

# INTRODUCTION

**Exam Code: 640-802**

## **Certifications:**

**Cisco Certified Network Associate (CCNA)**

## **Prerequisites:**

None

## **About This Study Guide**

This Study Guide is based on the current pool of exam questions for the Cisco CCNA 640-802 composite exam. As such it provides all the information required to pass the 640-802 exam and is organized around the specific skills that are tested in that exam. Thus, the information contained in this Study Guide is specific to the 640-802 exam and does not represent a complete reference work on the subject of Interconnecting Cisco Networking Devices. Topics covered in this Study Guide includes: Designing or Modifying a simple Local Area Network (LAN) using Cisco Products; Designing an IP Addressing Scheme; Selecting Appropriate Routing Protocols; Designing a simple Internetwork using Cisco products; Developing an Access List to Meet User Specifications; Choosing Wide Area Network (WAN) Services; Managing System Image and Device Configuration Files Performing an Initial Configuration on a Switch; Configuring Routing Protocols; Configuring IP Addresses, Subnet Masks, and Gateway Addresses on Routers and Hosts; Configuring a Router for Additional Administrative Functionality; Configuring a Switch with Virtual LANs (VLANs) and Inter-switch Communication; Implementing a LAN; Customizing a Switch Configuration; Implementing Access Lists; Implementing Simple WAN Protocols; Utilizing the OSI Reference Model as a Guide for Systematic Network Troubleshooting; Performing LAN and VLAN Troubleshooting; Troubleshooting Routing Protocols; Troubleshooting IP Addressing and Host Configuration; Troubleshooting a Device as Part of a Working Network; Troubleshooting an Access List; Performing Simple WAN Troubleshooting; Understanding Network Communications based on Layered Models; Understanding the Components of Network Devices; Understanding the Spanning Tree Process; Evaluating the Characteristics of LAN Environments; Evaluating the TCP/IP Communication Process and its Associated Protocols; Evaluating the Characteristics of Routing Protocols; Evaluating Rules for Packet Control; and Evaluating Key Characteristics of WANs.

## **Intended Audience**

This Study Guide is targeted specifically at people who wish to take the Cisco CCNA 640-802 Composite exam. This information in this Study Guide is specific to the exam. It is not a complete reference work. Although our Study Guides are aimed at new comers to the world of IT, the concepts dealt with in this Study Guide are complex. Knowledge of CompTIA's A+ and Network+ courses would be advantageous.

**Note:** Because the 640-802 exam is a composite of the 640-822 and 640-816 exams, there is a fair amount of overlap between this Study Guide and the 640-822 and 640-816 Study Guides. However, this Study Guide does not

combine the 640-822 and 640-816 Study Guides but addresses the 640-802 exam specifically. As such, we would not advise using this Study Guide for the 640-822 exam and/or the 640-816 exam.

### **How To Use This Study Guide**

To benefit from this Study Guide we recommend that you:

- Study each chapter carefully until you fully understand the information. This will require regular and disciplined work. Where possible, attempt to implement the information in a lab setup.
- Be sure that you have studied and understand the entire Study Guide before you take the exam.

**Note:** Remember to pay special attention to these note boxes as they contain important additional information that is specific to the exam.

Good luck!

# Topic 1: Networking Fundamentals

## Section 1.1: The OSI Reference Model

The OSI is the Open System Interconnection reference model for communications. As illustrated in Figure 1.1, the OSI reference model consists of seven layers, each of which can have several sublayers. The upper layers of the OSI reference model define functions focused on the application, while the lower three layers define functions focused on end-to-end delivery of the data.

- The **Application Layer (Layer 7)** refers to communications services to applications and is the interface between the network and the application. Examples include: Telnet, HTTP, FTP, Internet browsers, NFS, SMTP gateways, SNMP, X.400 mail, and FTAM.
- The **Presentation Layer (Layer 6)** defining data formats, such as ASCII text, EBCDIC text, binary, BCD, and JPEG. Encryption also is defined as a presentation layer service. Examples include: JPEG, ASCII, EBCDIC, TIFF, GIF, PICT, encryption, MPEG, and MIDI.
- The **Session Layer (Layer 5)** defines how to start, control, and end communication sessions. This includes the control and management of multiple bidirectional messages so that the application can be notified if only some of a series of messages are completed. This allows the presentation layer to have a seamless view of an incoming stream of data. The presentation layer can be presented with data if all flows occur in some cases. Examples include: RPC, SQL, NFS, NetBios names, AppleTalk ASP, and DECnet SCP
- The **Transport Layer (Layer 4)** defines several functions, including the choice of protocols. The most important Layer 4 functions are error recovery and flow control. The transport layer may provide for retransmission, i.e., error recovery, and may use flow control to prevent unnecessary congestion by attempting to send data at a rate that the network can accommodate, or it might not, depending on the choice of protocols. Multiplexing of incoming data for different flows to applications on the same host is also performed. Reordering of the incoming data stream when packets arrive out of order is included. Examples include: TCP, UDP, and SPX.
- The **Network Layer (Layer 3)** defines end-to-end delivery of packets and defines logical addressing to accomplish this. It also defines how routing works and how routes are learned; and how to fragment a packet into smaller packets to accommodate media with smaller maximum transmission unit sizes. Examples include: IP, IPX, AppleTalk DDP, and ICMP. Both IP and IPX define logical addressing, routing, the learning of routing information, and end-to-end delivery rules. The IP and IPX protocols most closely match the OSI network layer (Layer 3) and are called Layer 3 protocols because their functions most closely match OSI's Layer 3.
- The **Data Link Layer (Layer 2)** is concerned with getting data across one particular link or medium. The data link protocols define delivery across an individual link. These protocols are necessarily concerned with the type of media in use. Examples include: IEEE 802.3/802.2, HDLC, Frame Relay, PPP, ATM, and IEEE 802.5/802.2.
- The **Physical Layer (Layer 1)** deals with the physical characteristics of the transmission medium. Connectors, pins, use of pins, electrical currents, encoding, and light modulation are all part of different

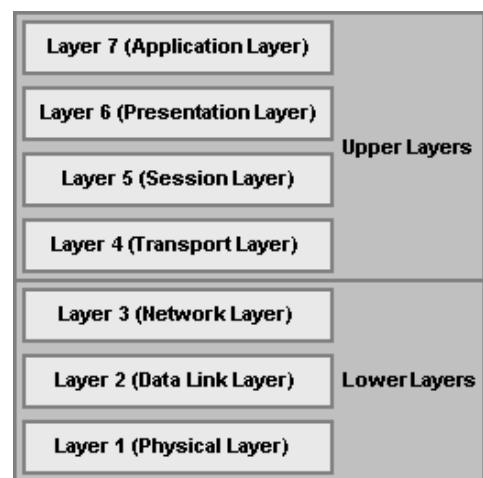


Figure 1.1: The OSI Reference Model

physical layer specifications. Examples includes: EIA/TIA-232, V.35, EIA/TIA-449, V.24, RJ-45, Ethernet, 802.3, 802.5, NRZI, NRZ, and B8ZS.

The upper layers of the OSI reference model, i.e., the Application Layer (Layer 7), the Presentation Layer (Layer 6), and the Session Layer (Layer 5), define functions focused on the application. The lower four layers, i.e., the Transport Layer (Layer 4), the Network Layer (Layer 3), the Data Link Layer (Layer 2), and the Physical Layer (Layer 1), define functions focused on end-to-end delivery of the data. As a Cisco Certified Network Associate, you will deal mainly with the lower layers, particularly the data link layer (Layer 2) upon which switching is based, and the network layer (Layer 3) upon which routing is based.

### 1.1.1: Interaction Between OSI Layers

When a host receives a data transmission from another host on the network, that data is processed at each of the OSI layers to the next higher layer, in order to render the data transmission useful to the end-user. To facilitate this processing, headers and trailers are created by the sending host's software or hardware, that are placed before or after the data given to the next higher layer. Thus, each layer has a header and trailer, typically in each data packet that comprises the data flow. The sequence of processing at each OSI layer, i.e., the processing between adjacent OSI layers, is as follows:

- The **Physical Layer** (Layer 1) ensures **bit synchronization** and places the received binary pattern into a buffer. It notifies the Data Link Layer (Layer 2) that a frame has been received after decoding the incoming signal into a bit stream. Thus, Layer 1 provides delivery of a stream of bits across the medium.
- The **Data Link Layer** (Layer 2) examines the **frame check sequence (FCS)** in the trailer to determine whether errors occurred in transmission, providing **error detection**. If an error has occurred, the frame is discarded. The current host examines data link address is examined to determine if the data is addressed to it or whether to process the data further. If the data is addressed to the host, the data between the Layer 2 header and trailer is handed over to the Network Layer (Layer 3) software. Thus, the data link layer delivers data across the link.
- The **Network Layer** (Layer 3) examines the destination address. If the address is the current host's address, processing continues and the data after the Layer 3 header is handed over to the Transport Layer (Layer 4) software. Thus, Layer 3 provides end-to-end delivery.
- If error recovery was an option chosen for the **Transport Layer** (Layer 4), the counters identifying this piece of data are encoded in the Layer 4 header along with acknowledgment information, which is called **error recovery**. After error recovery and reordering of the incoming data, the data is given to the Session Layer (Layer 5).
- The **Session Layer** (Layer 5) ensures that a series of messages is completed. The Layer 5 header includes fields signifying sequence of the packet in the data stream, indicating the position of the data packet in the flow. After the session layer ensures that all flows are completed, it passes the data after the Layer 5 header to the Presentation Layer (Layer 6) software.
- The **Presentation Layer** (Layer 6) defines and manipulates the data format of the data transmission. It converts the data to the proper format specified in the Layer 6 header. Typically, this header is included only for initialization flows, not with every data packet being transmitted. After the data formats have been converted, the data after the Layer 6 header is passed to the Application Layer (Layer 7) software.
- The **Application Layer** (Layer 7) processes the final header and examines the end-user data. This header signifies agreement to operating parameters by the applications on the two hosts. The headers are used to signal the values for all parameters; therefore, the header typically is sent and received at application initialization time only.

In addition to processing between adjacent OSI layers, the various layers must also interact with the same layer on another computer to successfully implement its functions. To interact with the same layer on another computer, each layer defines additional data bits in the header and, in some cases, trailer that is created by the sending host's software or hardware. The layer on the receiving host interprets the headers and trailers created by the corresponding layer on the sending host to determine how that layer's processing is being defined, and how to interact within that framework.

## Section 1.2: TCP/IP and the OSI Reference Model

As illustrated in Figure 1.2, the Transmission Control Protocol/Internet Protocol (TCP/IP) model consists of four layers, each of which can have several sublayers. These layers correlate roughly to layers in the OSI reference model and define similar functions. Some of the TCP/IP layers correspond directly with layers in the OSI reference model while others span several OSI layers. The four TCP/IP layers are:

- The **TCP/IP Application Layer** refers to communications services to applications and is the interface between the network and the application. It is also responsible for presentation and controlling communication sessions. It spans the Application Layer, Presentation Layer and Session Layer of the OSI reference model. Examples include: HTTP, POP3, and SNMP.
- The **TCP/IP Transport Layer** defines several functions, including the choice of protocols, error recovery and flow control. The transport layer may provide for retransmission, i.e., error recovery, and may use flow control to prevent unnecessary congestion by attempting to send data at a rate that the network can accommodate, or it might not, depending on the choice of protocols. Multiplexing of incoming data for different flows to applications on the same host is also performed. Reordering of the incoming data stream when packets arrive out of order is included. It correlates with the Transport Layer of the OSI reference model. Examples include: TCP and UDP, which are called Transport Layer, or Layer 4, protocols.
- The **TCP/IP Internetwork Layer** defines end-to-end delivery of packets and defines logical addressing to accomplish this. It also defines how routing works and how routes are learned; and how to fragment a packet into smaller packets to accommodate media with smaller maximum transmission unit sizes. It correlates with the Network Layer of the OSI reference model. Examples include: IP and ICMP.
- The **TCP/IP Network Interface Layer** is concerned with the physical characteristics of the transmission medium as well as getting data across one particular link or medium. This layer defines delivery across an individual link as well as the physical layer specifications. It spans the Data Link Layer and Physical Layer of the OSI reference model. Examples include: Ethernet and Frame Relay.

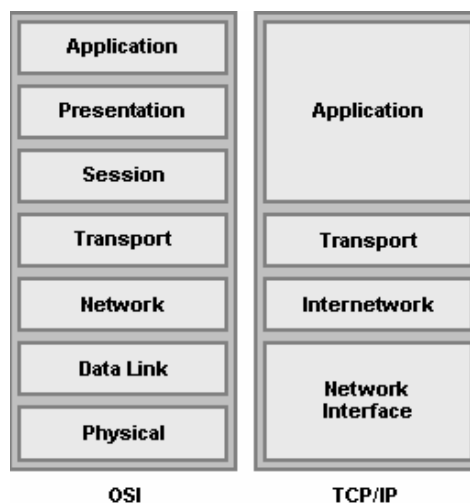


Figure 1.2: OSI and TCP/IP Models

### 1.2.1: The TCP/IP Protocol Architecture

TCP/IP defines a large collection of protocols that allow computers to communicate. Table 1.1 outlines the protocols and the TCP/IP architectural layer to which they belong. TCP/IP defines the details of each of these protocols in **Requests For Comments (RFC)** documents. By implementing the required protocols defined in TCP/IP RFCs, a computer that implements the standard networking protocols defined by TCP/IP can communicate with other computers that also use the TCP/IP standards.

Table 1.1: The TCP/IP Architectural Model and Protocols

TCP/IP Architecture Layer	Protocols
Application	HTTP, POP3, SMTP
Transport	TCP, UDP
Internetwork	IP
Network interface	Ethernet, Frame Relay

### 1.2.2: TCP/IP Data Encapsulation

The term encapsulation describes the process of putting headers and trailers around some data. A computer that needs to send data encapsulates the data in headers of the correct format so that the receiving computer will know how to interpret the received data. Data encapsulation with TCP/IP consists of five-steps:

**Step 1:** Create the application data and headers.

**Step 2:** Package the data for transport, which is performed by the transport layer (TCP or UDP). The Transport Layer creates the transport header and places the data behind it.

**Step 3:** Add the destination and source network layer addresses to the data, which is performed by the Internetwork Layer. The Internetwork Layer creates the network header, which includes the network layer addresses, and places the data behind it.

**Step 4:** Add the destination and source data link layer addresses to the data, which is performed by the Network Interface Layer. The Network Interface Layer creates the data link header, places the data behind it, and places the data link trailer at the end.

**Step 5:** Transmit the bits, which is performed by the Network Interface Layer. The Network Interface Layer encodes a signal onto the medium to transmit the frame.

### Section 1.3: Networks

A network is defined as a group of two or more computers linked together for the purpose of communicating and sharing information and other resources, such as printers and applications. Most networks are constructed around a cable connection that links the computers, however, modern wireless networks that use radio wave or infrared connections are also becoming quite prevalent. These connections permit the computers to communicate via the wires in the cable, radio wave or infrared signal. For a network to function it must provide connections, communications, and services.

- **Connections** are defined by the hardware or physical components that are required to connect a computer to the network. This includes the **network medium**, which refers to the hardware that physically connects one computer to another, i.e., the network cable or a wireless connection; and the **network interface**, which refers to the hardware that attaches a computer to the network medium and is usually a network interface card (NIC).
- **Communications** refers to the network protocols that are used to establish the rules governing network communication between the networked computers. Network protocols allow computers running different operating systems and software to communicate with each.
- **Services** define the resources, such as files or printers, that a computer shares with the rest of the networked computers.

### 1.3.1: Network Definitions

Computer networks can be classified and defined according to geographical area that the network covers. There are four network definitions: a Local Area Network (LAN), a Campus Area Network (CAN), a Metropolitan Area Network (MAN), and a Wide Area Network (WAN). There are three additional network definitions, namely the Internet, an intranet and an Internetwork. These network definitions are discussed in Table 1.2.

Table 1.2: Network Definitions

Definition	Description
Local Area Network (LAN)	A LAN is defined as a network that is contained within a closed environment and does not exceed a distance of 1.25 mile (2 km). Computers and peripherals on a LAN are typically joined by a network cable or by a wireless network connection. A LAN that consists of wireless connections is referred to as a <b>Wireless LAN (WLAN)</b> .
Campus Area Network (CAN)	A CAN is limited to a single geographical area but may exceed the size of a LAN
Metropolitan Area Network (MAN)	A MAN is defined as a network that covers the geographical area of a city that is less than 100 miles.
Wide Area Network (WAN)	A WAN is defined as a network that exceeds 1.25 miles. A WAN often consists of a number of LANs that have been joined together. A CAN and a MAN is also a WAN. WANs typically connected numerous LANs through the internet via telephone lines, T1 lines, Integrated Services Digital Network (ISDN) lines, radio waves, cable or satellite links.
Internet	The Internet is a world wide web of networks that are based on the TCP/IP protocol and is not own by a single company or organization.
Intranet	An intranet uses that same technology as the Internet but is owned and managed by a company or organization. A LAN or a WAN s usually an intranet.
Internetwork	An internetwork consists of a number of networks that are joined by routers. The Internet is the largest example of an internetwork.

Of these network definitions, the most common are the Internet, the LAN and the WAN.

### 1.3.2: Types of Networks

These network definitions can be divided into two types of networks, based on how information is stored on the network, how network security is handled, and how the computers on the network interact. These two types are: **Peer-To-Peer (P2P) Networks** and **Server/Client Networks**. The latter is often also called Server networks.

- On a **Peer-To-Peer (P2P) Network**, there is no hierarchy of computers; instead each computer acts as either a server which shares its data or services with other computers, or as a client which uses data or services on another computer. Furthermore, each user establishes the security on their own computers and determines which of their resources are made available to other users. These networks are typically limited to between 15 and 20 computers. Microsoft Windows for Workgroups, Windows 95, Windows 98, Windows ME, Windows NT Workstation, Windows 2000, Novell's NetWare, UNIX, and Linux are some operating systems that support peer-to-peer networking.
- A **Server/Client Network** consists of one or more dedicated computers configured as servers. This server manages access to all shared files and peripherals. The server runs the network operating system (NOS) manages security and administers access to resources. The client computers or workstations connect to the network and use the available resources. Among the most common network operating systems are Microsoft's Windows NT Server 4, Windows 2000 Server, and Novell's NetWare. Before the release of Windows NT, most dedicated servers worked only as hosts. Windows NT allows these servers to operate as an individual workstation as well.

### 1.3.3: Network Topologies

The layout of a LAN design is called its topology. There are three basic types of topologies: the star topology, the bus topology, and the ring topology. Hybrid combinations of these topologies also exist.

- In a network based on the **star topology**, all computers and devices are connected to a centrally located hub or switch. The hub or switch collects and distributes the flow of data within the network. When a hub is used, data from the sending host are sent to the hub and are then transmitted to all hosts on the network except the sending host. Switches can be thought of as intelligent hubs. When switches are used rather than hubs, data from the sending host are sent to the switch which transmits the data to the intended recipient rather than to all hosts on the network.
- In a network based on the **bus topology**, all computers and devices are connected in series to a single linear cable called a trunk. The trunk is also known as a backbone or a segment. Both ends of the trunk must be terminated to stop the signal from bouncing back up the cable. Because a bus network does not have a central point, it is more difficult to troubleshoot than a star network. Furthermore, a break or problem at any point along the bus can cause the entire network to go down.

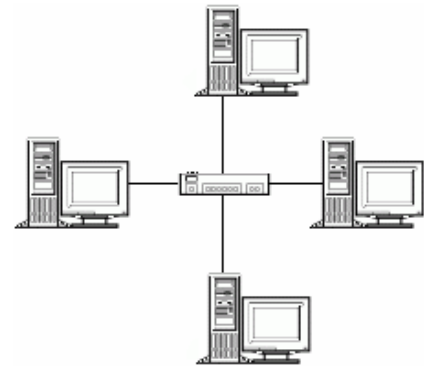
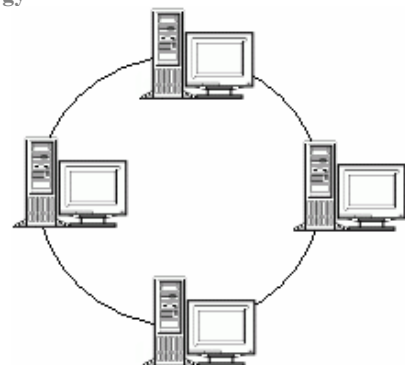


Figure 1.3: The Star Topology



Figure 1.4: The Bus Topology



- In a network based on a **ring topology**, all computers and devices are connected to cable that forms a closed loop. On such networks there are no terminating ends; therefore, if one computer fails, the entire network will go down. Each computer on such a network acts like a repeater and boosts the signal before sending it to the next station. This type of network transmits data by passing a “token” around the network. If the token is free of data, a computer waiting to send data grabs it, attaches the data and the electronic address to the token, and sends it on its way. When the token reaches its destination computer, the data is removed and the token is sent on. Hence this type of network is commonly called a token ring network.

Figure 1.5: The Ring Topology

Of these three network topologies, the star topology is the most predominant network type and is based on the Ethernet standard.

### 1.3.4: Network Technologies

Various network technologies can be used to establish network connections, including Ethernet, Fiber Distribution Data Interface (FDDI), Copper Distribution Data Interface (CDDI), Token Ring, and Asynchronous Transfer Mode (ATM). Of these, Ethernet is the most popular choice in installed networks because of its low cost, availability, and scalability to higher bandwidths.

#### 1.3.4.1: Ethernet

Ethernet is based on the Institute of Electrical and Electronics Engineers (IEEE) 802.3 standard and offers a bandwidth of 10 Mbps between end users. Ethernet is based on the carrier sense multiple access collision detect (CSMA/CD) technology, which requires that transmitting stations back off for a random period of time when a collision occurs.

Coaxial cable was the first media system specified in the Ethernet standard. Coaxial Ethernet cable comes in two major categories: **Thicknet** (10Base5) and **Thinnet** (10Base2). These cables differed in their size and their length limitation. Although Ethernet coaxial cable lengths can be quite long, they are susceptible to electromagnetic interference (EMI) and eavesdropping.

Table 1.3: Coaxial Cable for Ethernet

Cable	Diameter	Resistance	Bandwidth	Length
Thinnet (10Base2)	10 mm	50 ohms	10 Mbps	185 m
Thicknet (10Base5)	5 mm	50 ohms	10 Mbps	500 m

Today most wired networks use twisted-pair media for connections to the desktop. Twisted-pair also comes in two major categories: **Unshielded twisted-pair (UTP)** and **Shielded twisted-pair (STP)**. One pair of insulated copper wires twisted about each other forms a twisted-pair. The pairs are twisted to reduce interference and crosstalk. Both STP and UTP suffer from high attenuation, therefore these lines are usually restricted to an end-to-end distance of 100 meters between active devices. Furthermore, these cables are sensitive to EMI and eavesdropping. Most networks use 10BaseT UTP cable.

An alternative to twisted-pair cable is fiber optic cable (10BaseFL), which transmits light signals, generated either by light emitting diodes (LEDs) or laser diodes (LDs), instead of electrical signals. These cables support higher transmission speeds and longer distances but are more expensive. Because they do not carry electrical signals, fiber optic cables are immune to EMI and eavesdropping. They also have low attenuation

which means they can be used to connect active devices that are up to 2 km apart. However, fiber optic devices are not cost effective while cable installation is complex.

Table 1.4: Twisted-Pair and Fiber Optic Cable for Ethernet

Cable	Technology	Bandwidth	Cable Length
Twisted-Pair	(10BaseT)	10 Mbps	100 m
Fiber Optic	(10BaseFL)	10 Mbps	2,000 m

#### 1.3.4.2: Fast Ethernet

Fast Ethernet operates at 100 Mbps and is based on the IEEE 802.3u standard. The Ethernet cabling schemes, CSMA/CD operation, and all upper-layer protocol operations have been maintained with Fast Ethernet. Fast Ethernet is also backward compatible with 10 Mbps Ethernet. Compatibility is possible because the two devices at each end of a network connection can automatically negotiate link capabilities so that they both can operate at a common level. This negotiation involves the detection and selection of the highest available bandwidth and half-duplex or full-duplex operation. For this reason, Fast Ethernet is also referred to as **10/100 Mbps Ethernet**.

Cabling for Fast Ethernet can be either UTP or fiber optic. Specifications for these cables are shown in Table 1.5.

Table 1.5: Fast Ethernet Cabling and Distance Limitations

Technology	Wiring Type	Pairs	Cable Length
100BaseTX	EIA/TIA Category 5 UTP	2	100 m
100BaseT2	EIA/TIA Category 3,4,5 UTP	2	100 m
100BaseT4	EIA/TIA Category 3,4,5 UTP	4	100 m
100BaseFX	Multimode fiber (MMF) with 62.5 micron core; 1300 nm laser	1	400 m (half-duplex) 2,000 m (full-duplex)
	Single-mode fiber (SMF) with 62.5 micron core; 1300 nm laser	1	10,000 m

#### 1.3.4.3: Gigabit Ethernet

Gigabit Ethernet is an escalation of the Fast Ethernet standard using the same IEEE 802.3 Ethernet frame format. Gigabit Ethernet offers a throughput of 1,000 Mbps (1 Gbps). Like Fast Ethernet, Gigabit Ethernet is compatible with earlier Ethernet standards. However, the physical layer has been modified to increase data transmission speeds: The IEEE 802.3 Ethernet standard and the American National Standards Institute (ANSI) X3T11 FibreChannel. IEEE 802.3 provided the foundation of frame format, CSMA/CD, full duplex, and other characteristics of Ethernet. FibreChannel provided a base of high-speed ASICs, optical components, and encoding/decoding and serialization mechanisms. The resulting protocol is termed IEEE 802.3z Gigabit Ethernet.

Gigabit Ethernet supports several cabling types, referred to as 1000BaseX. Table 1.6 lists the cabling specifications for each type.

Table 1.6: Gigabit Ethernet Cabling and Distance Limitations

Technology	Wiring Type	Pairs	Cable Length
1000BaseCX	Shielded Twisted Pair (STP)	1	25 m
1000BaseT	EIA/TIA Category 5 UTP	4	100 m
1000BaseSX	Multimode fiber (MMF) with 62.5 micron core; 850 nm laser	1	275 m
	Multimode fiber (MMF) with 50 micron core; 1300 nm laser	1	550 m
1000BaseLX/LH	Multimode fiber (MMF) with 62.5 micron core; 1300 nm laser	1	550 m
	Single-mode fiber (SMF) with 50 micron core; 1300 nm laser	1	550 m
	Single-mode fiber (SMF) with 9 micron core; 1300 nm laser	1	10 km
1000BaseZX	Single-mode fiber (SMF) with 9 micron core; 1550 nm laser	1	70 km
	Single-mode fiber (SMF) with 8 micron core; 1550 nm laser	1	100 km

### 1.3.5: Network Addressing

Network addressing identifies either individual devices or groups of devices on a LAN. A pair of network devices that transmit frames between each other use a source and destination address field to identify each other. These addresses are called **unicast** addresses, or individual addresses, because they identify an individual network interface card (NIC).

The IEEE defines the format and assignment of network addresses by requiring manufacturers to encode globally unique unicast Media Access Control (MAC) addresses on all NICs. The first half of the MAC address identifies the manufacturer of the card and is called the **organizationally unique identifier (OUI)**.

### 1.3.6: Bridging

Bridging is used to connect two network segments. This alleviates congestion problems on a single Ethernet segment and extends allowed cabling distances because the segments on each side of the bridge conformed to the same distance limitation as a single segment. This bridge is called “**transparent bridging**” because the end-point devices do not need to know that the bridge exists.

Transparent bridges forward frames only when necessary and, thus, reduces network overhead. To accomplish this, transparent bridges learning MAC addresses by examining the source MAC address of each frame received by the bridge; decides when to forward a frame or when to filter a frame, based on the destination MAC address; and creates a loop-free environment with other bridges by using the Spanning-Tree Protocol.

Generally, broadcasts and multicast frames are forwarded by the bridge in networks that use bridges. In addition, transparent bridges perform switching of frames using Layer 2 headers and Layer 2 logic and are

Layer 3 protocol-independent. Store-and-forward operation, which means that the entire frame is received before the first bit of the frame is forwarded, is also typical in transparent bridging devices. However, the transparent bridge must perform processing on the frame, which also can increase latency.

A transparent bridge operates in the following manner:

- The bridge has **no initial knowledge** of the location of any end device; therefore, the bridge must listen to frames coming into each of its ports to figure out on which network a device resides.
- The bridge constantly **updates its bridging table** upon detecting the presence of a new MAC address or upon detecting a MAC address that has changed location from one bridge port to another. The bridge is then able to forward frames by looking at the destination address, looking up the address in the bridge table, and sending the frame out the port where the destination device is located.
- If a frame arrives with the broadcast address as the destination address, the bridge must **forward** or flood the frame **out all available ports**. However, the frame is not forwarded out the port that initially received the frame. Hence, broadcasts are able to reach all available networks. A bridge only segments collision domains but does not segment broadcast domains.
- If a frame arrives with a **destination address that is not found** in the bridge table, the bridge is unable to determine which port to forward the frame to for transmission. This is known as an **unknown unicast**. In this case, the bridge treats the frame as if it was a broadcast and forwards it out all remaining ports. After a reply to that frame is received, the bridge will learn the location of the unknown station and add it to the bridge table.
- Frames that are forwarded across the bridge **cannot be modified**.

### 1.3.7: LAN Switching

An Ethernet switch uses the same logic as a transparent bridge, but performs more functions, has more features, and has more physical ports. Switches use hardware to learn MAC addresses and to make forwarding and filtering decisions, whereas bridges use software.

A switch listens for frames that enter all its interfaces. After receiving a frame, a switch decides whether to forward a frame and out which port(s). To perform these functions, switches perform three tasks:

- **Learning**, which means that the switch learns MAC addresses by examining the source MAC address of each frame the bridge receives. Switches dynamically learn the MAC addresses in the network to build its MAC address table. With a full, accurate MAC address table, the switch can make accurate forwarding and filtering decisions. Switches build the MAC address table by listening to incoming frames and examining the frame's source MAC address. If a frame enters the switch, and the source MAC address is not in the address table, the switch creates an entry in the table. The MAC address is placed in the table, along with the interface in which the frame arrived. This allows the switch to make good forwarding choices in the future. Switches also forward unknown unicast frames, which are frames whose destination MAC addresses are not yet in the bridging table, out all ports, which is called **flooding**, with the hope that the unknown device will be on some other Ethernet segment and will reply. When the unknown device does reply, the switch will build an entry for that device in the address table.
- **Forwarding or filtering**, which means that the switch decides when to forward a frame or when to filter it, i.e., not to forward it, based on the destination MAC address. Switches reduce network overhead by forwarding traffic from one segment to another only when necessary. To decide whether to forward a frame, the switch uses a dynamically built table called a **bridge table** or **MAC address table**. The switch looks at the previously learned MAC addresses in an address table to decide where to forward the frames.

- **Loop prevention**, which means that the switch creates a loop-free environment with other bridges by using **Spanning-Tree Protocol (STP)**. Having physically redundant links helps LAN availability, and STP prevents the switch logic from letting frames loop around the network indefinitely, congesting the LAN.

Frames sent to unicast addresses are destined for a single device; frames sent to a broadcast address are sent to all devices on the LAN. Frames sent to multicast addresses are meant for all devices that care to receive the frame. Thus, when a switch receives a frame, it checks if the address is a unicast address, a broadcast address or a multicast address. If the address is unicast, and the address is in the address table, and if the interface connecting the switch to the destination device is not the same interface on which the frame arrived, the switch forwards the frame to the destination device. If the address is not in the address table, the switch forwards the frame on all ports. If the address is a broadcast or multicast address, the switch also forwards the frame on all ports.

The internal processing on a switch can decrease latency for frames. Switches can use store-and-forward processing as well as **cut-through** processing logic. With cut-through processing, the first bits of the frame are sent out the outbound port before the last bit of the incoming frame is received. However, because the frame check sequence (FCS) is in the Ethernet trailer, a cut-through forwarded frame might have bit errors that the switch will not notice before sending most of the frame..

### 1.3.8: Wireless Networks

Conventional Ethernet networks require cables connected computers via hubs and switches. This has the effect of restricting the computer's mobility and requires that even portable computers be physically connected to a hub or switch to access the network. An alternative to cabled networking is wireless networking. The first wireless network was developed at the University of Hawaii in 1971 to link computers on four islands without using telephone wires. Wireless networking entered the realm of personal computing in the 1980s, with the advent to networking computers. However, it was only in the early 1990s that wireless networks started to gain momentum when CPU processing power became sufficient to manage data transmitted and received over wireless connections.

Wireless networks use network cards, called Wireless Network Adapters, that rely radio signals or infrared (IR) signals to transmit and receive data via a Wireless Access Point (WAP). The WAP uses has an RJ-45 port that can be attached to attach to a 10BASE-T or 10/100BASE-T Ethernet hub or switch and contains a radio transceiver, encryption, and communications software. It translates conventional Ethernet signals into wireless Ethernet signals it broadcasts to wireless network adapters on the network and performs the same role in reverse to transfer signals from wireless network adapters to the conventional Ethernet network. WAP devices come in many variations, with some providing the Cable Modem Router and Switch functions in addition to the wireless connectivity.

**Note:** Access points are not necessary for direct peer-to-peer networking, which is called ad hoc mode, but they are required for a shared Internet connection or a connection with another network. When access points are used, the network is operating in the infrastructure mode.

#### 1.3.8.1: Wireless Network Standards

In the absence of an industry standard, the early forms of wireless networking were single-vendor proprietary solutions that could not communicate with wireless network products from other vendors. In

1997, the computer industry developed the IEEE 802.11 wireless Ethernet standard. Wireless network products based on this standard are capable of multivendor interoperability.

The IEEE 802.11 wireless Ethernet standard consists of the IEEE 802.11b standard, the IEEE 802.11a standard, and the newer IEEE 802.11g standard.

**Note:** The Bluetooth standard for short-range wireless networking is designed to complement, rather than rival, IEEE 802.11-based wireless networks.

- **IEEE 802.11** was the original standard for wireless networks that was ratified in 1997. It operated at a maximum speed of 2 Mbps and ensured interoperability between wireless products from various vendors. However, the standard had a few ambiguities allowed for potential problems with compatibility between devices. To ensure compatibility, a group of companies formed the Wireless Ethernet Compatibility Alliance (WECA), which has come to be known as the **Wi-Fi Alliance**, to ensure that their products would work together. The term **Wi-Fi** is now used to refer to any IEEE 802.11 wireless network products that have passed the Wi-Fi Alliance certification tests.
- **IEEE 802.11b**, which is also called 11 Mbps Wi-Fi, operates at a maximum speed of 11 Mbps and is thus slightly faster than 10BASE-T Ethernet. Most IEEE 802.11b hardware is designed to operate at four speeds, using three different data-encoding methods depending on the speed range. It operates at 11 Mbps using quaternary phase-shift keying/complimentary code keying (QPSK/CCK); at 5.5 Mbps also using QPSK/CCK; at 2 Mbps using differential quaternary phase-shift keying (DQPSK); and at 1 Mbps using differential binary phase-shift keying (DBPSK). As distances change and signal strength increases or decreases, IEEE 802.11b hardware switches to the most suitable data-encoding method.

Wireless networks running IEEE 802.11b hardware use the 2.4 GHz radio frequency band that many portable phones, wireless speakers, security devices, microwave ovens, and the Bluetooth short-range networking products use. Although the increasing use of these products is a potential source of interference, the short range of wireless networks (indoor ranges up to 300 feet and outdoor ranges up to 1,500 feet, varying by product) minimizes the practical risks. Many devices use a spread-spectrum method of connecting with other products to minimize potential interference.

IEEE 802.11b networks can connect to wired Ethernet networks or be used as independent networks.

- **IEEE 802.11a** uses the 5 GHz frequency band, which allows for much higher speeds, reaching a maximum speed of 54 Mbps. The 5 GHz frequency band also helps avoid interference from devices that cause interference with lower-frequency IEEE 802.11b networks. IEEE 802.11a hardware maintains relatively high speeds at both short and relatively long distances.

Because IEEE 802.11a uses the 5 GHz frequency band rather than the 2.4 GHz frequency band used by IEEE 802.11b, standard IEEE 802.11a hardware cannot communicate with 802.11b hardware. A solution to this compatibility problem is the use of dual-band hardware. Dual-band hardware can work with either IEEE 802.11a or IEEE 802.11b networks, enabling you to move from an IEEE 802.11b wireless network at home or at Starbucks to a faster IEEE 802.11a office network.

- **IEEE 802.11g** is also known as Wireless-G and combines compatibility with IEEE 802.11b with the speed of IEEE 802.11a at longer distances. This standard was ratified in mid-2003, however, many network vendors were already selling products based on the draft IEEE 802.11g standard before the final standard was approved. These early IEEE 802.11g hardware was slower and less compatible than the specification promises. In some cases, problems with early-release IEEE 802.11g hardware can be solved through firmware upgrades.

### 1.3.8.2: Wireless Network Modes

Wireless networks work in one of two modes that are also referred to as topologies. These two modes are ad-hoc mode and infrastructure mode. The mode you implement depends on whether you want your computers to communicate directly with each other, or via a WAP.

- In **ad-hoc mode**, data is transferred to and from wireless network adapters connected to the computers. This cuts out the need to purchase a WAP. Throughput rates between two wireless network adapters are twice as fast as when you use a WAP. However, a network in ad-hoc mode cannot connect to a wired network as a WAP is required to provide connectivity to a wired network. An ad-hoc network is also called a peer-to-peer network.
- In **infrastructure mode**, data is transferred between computers via a WAP. Because a WAP is used in infrastructure mode, it provides connectivity with a wired network, allowing you to expand a wired network with wireless capability. Your wired and wirelessly networked computers can communicate with each other. In addition, a WAP can extend your wireless network's range as placing a WAP between two wireless network adapters doubles their range. Also, some WAPs have a built-in router and firewall. The router allows you to share Internet access between all your computers, and the firewall hides your network. Some of these multifunction access points include a hub with RJ-45 ports.

### 1.3.8.3: Security Features

Because wireless networks can be accessed by anyone with a compatible wireless network adapter, most models of wireless network adapters and WAPs provide for encryption options. Some devices with this feature enable you to set a security code known as an SSID on the wireless devices on your network. This seven-digit code prevents unauthorized users from accessing your network and acts as an additional layer of security along with your normal network authentication methods, such as user passwords. Other wireless network adapters and WAPs use a list of authorized MAC addresses to limit access to authorized devices only.

All Wi-Fi products support at least 40-bit encryption through the wired equivalent privacy (WEP) specification, but the minimum standard on newer products is 64-bit WEP encryption. Many vendors also offer 128-bit or 256-bit encryption on some of their products. However, the WEP specification is insecure. It is vulnerable to brute-force attacks at shorter key lengths, and it is also vulnerable to **differential cryptanalysis** attacks, which is the process of comparing an encrypted text with a known portion of the plain text and deriving the key by computing the difference between them. Because WEP encrypts TCP headers, hackers know what the headers should contain in many cases, and they can attempt to find patterns in a large body of collected WEP communications in order to decrypt the key. The attack is complex and difficult to automate, so it is unlikely to occur for most networks, especially at key lengths greater than 128 bits. Furthermore, WEP does not prevent an intruder from attaching a hidden WAP on the network and using it to exploit the network.

New network products introduced in 2003 and beyond now incorporate a new security standard known as Wi-Fi Protected Access (WPA). WPA is derived from the developing IEEE 802.11i security standard, which will not be completed until mid-decade. WPA-enabled hardware works with existing WEP-compliant devices, and software upgrades might be available for existing devices.