1 Internetworking

THE CCNA EXAM TOPICS COVERED IN THIS CHAPTER INCLUDE THE FOLLOWING:

- ./ **Describe the benefits of a layered model**
- ./ **Describe the main benefit of the OSI reference model**
- ./ **Understand each of the seven layers of the OSI reference model and what they provide application developers**
- ./ **Describe flow control and how it is used within an internetwork**
- ./ **Understand how the Transport layer flow control mechanism works**
- ./ **Describe how the OSI's Network layer provides routing in an internetwork environment**
- ./ **List the five conversion steps of data encapsulation**

Welcome to the exciting world of internetworking. This first chapter will help you understand the basics of internetworking and how to connect networks using Cisco routers and switches.

The Open Systems Interconnection (OSI) model will be discussed in detail in this chapter. The OSI model has seven hierarchical layers that were devel- oped to help different companies communicate between their disparate sys- tems. It is important to understand the OSI model as Cisco sees it, and that is how I will present the seven layers of the OSI model to you.

Cisco has created a three-layer hierarchical network model that can help you build, implement, and maintain networks. By understanding this model, you can effectively build, maintain, and troubleshoot any size network. This chapter will give you both an introduction to the Cisco three-layer model and the details of each layer.

Different types of devices are specified at different layers of the OSI model. It is important to understand the different types of cables and con- nectors used to connect these devices to a network. Cabling Cisco devices will be discussed with Ethernet LANs, WAN technologies, and even connect- ing a router or switch with a console connection.

Cisco makes a large range of router, hub, and switch products. By under- standing the different products available from Cisco, you can understand which devices can meet the business requirements for your network. The product line for Cisco hubs, routers, and switches is discussed at the end of this chapter.

Internetworking Models

When networks first came into being, computers could typically com- municate only with computers from the same manufacturer. For example, companies ran either a complete DECnet solution or an IBM solution—not
both together. In the late 1970s, the *OSI (Open Systems Interconnection) model* was created by the International Organization for Standardization (ISO) to break this barrier. The OSI model was meant to help vendors create interoperable network devices. Like world peace, it'll probably never happen completely, but it's still a great goal.

The OSI model is the primary architectural model for networks. It describes how data and network information are communicated from appli- cations on one computer, through the network media, to an application
on another computer. The OSI reference model breaks this approach into layers.

Cisco has also created a three-layer model that is used to help design, implement, and maintain any size network. By understanding the three-layer model, you will gain an understanding of how Cisco views internetworking. Also, by having a fundamental understanding of the devices used at each layer of the model, you can effectively design and purchase the correct Cisco equipment to meet your business needs. This chapter will cover both the OSI model and the Cisco three-layer hierarchical model.

The Layered Approach

A *reference model* is a conceptual blueprint of how communications should take place. It addresses all the processes required for effective communication and divides these processes into logical groupings called *layers*. When a communication system is designed in this manner, it's known as *layered architecture*.

Think of it like this: You and some friends want to start a company. One of the first things you'd do is sit down and think through what must be done, who will do them, what order they will be done in, and how they relate to each other. Ultimately, you might group these tasks into departments. Let's say you decide to have an order-taking department, an inventory depart- ment, and a shipping department. Each of your departments has its own unique tasks, keeping its staff members busy and requiring them to focus on only their own duties.

In this scenario, departments are a metaphor for the layers in a communication system. For things to run smoothly, the staff of each department will have to both trust and rely heavily on the others to do their jobs and competently handle their unique responsibilities. In your planning sessions, you would probably take notes, recording the entire process to facilitate later discussions about standards of operation that will serve as your business blueprint, or reference model.

Once your business is launched, your department heads, armed with the part of the blueprint relating to their department, will need to develop prac- tical methods to implement their assigned tasks. These practical methods, or protocols, will need to be compiled into a standard operating procedures manual and followed closely. Each of the various procedures in your manual will have been included for different reasons and have varying degrees of importance and implementation. If you form a partnership or acquire another company, it will be imperative for its business protocols—its busi- ness blueprint—to match, or be compatible with, yours.

Similarly, software developers can use a reference model to understand computer communication processes and to see what types of functions need to be accomplished on any one layer. If they are developing a protocol for a certain layer, all they need to concern themselves with is the specific layer's functions, not those of any other layer. Another layer and protocol will han- dle the other functions. The technical term for this idea is *binding*. The com- munication processes that are related to each other are bound, or grouped together, at a particular layer.

Advantages of Reference Models

The OSI model, like the Cisco three-layer model you will learn about later, is hierarchical, and the same benefits and advantages can apply to any layered model. The primary purpose of all models, and especially the OSI model, is to allow different vendors to interoperate. The benefits of the OSI and Cisco models include, but are not limited to, the following:

- Dividing the complex network operation into more manageable layers
- Changing one layer without having to change all layers. This allows application developers to specialize in design and development.
- Defining the standard interface for the "plug-and-play" multivendor integration

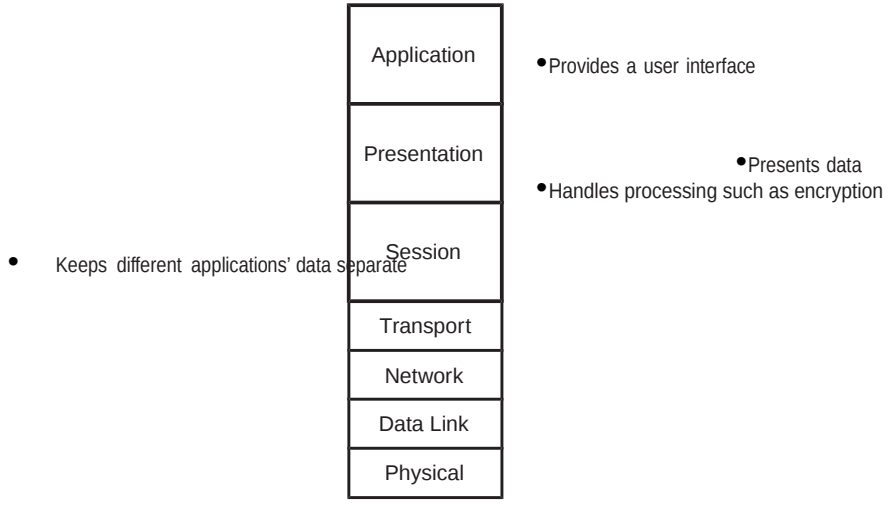
The OSI Reference Model

The OSI reference model was created in the late 1970s to help facilitate data transfer between network nodes. One of the greatest functions of the OSI specifications is to assist in data transfer between disparate hosts. This means you can transfer data between a Unix host and a PC, for example.

The OSI is not physical; rather, it is a set of guidelines that application developers can use to create and implement applications that run on a network. It also provides a framework for creating and implementing network- ing standards, devices, and internetworking schemes.

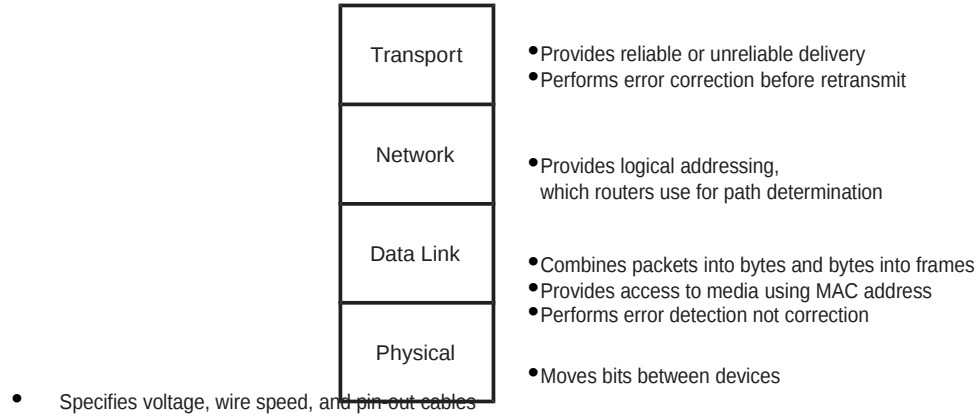
The OSI has seven different layers, which are divided into two groups. The top three layers define how the applications within the end stations will com- municate with each other and with users. The bottom four layers define how data is transmitted end-to-end. Figure 1.1 shows the three upper layers and their functions, and Figure 1.2 shows the four lower layers and their functions.

FIGURE 1.1 The upper layers



In Figure 1.1, you can see that the user interfaces with the computer at the application layer, and also that the upper layers are responsible for applications communicating between hosts. Remember that none of the upper layers know anything about networking or network addresses. That is the responsibility of the four bottom layers, which are shown in Figure 1.2.

FIGURE 1.2 The lower layers



The four bottom layers define how data is transferred through a physical wire or through switches and routers, and how to rebuild a data stream from a transmitting host to a destination host's application.

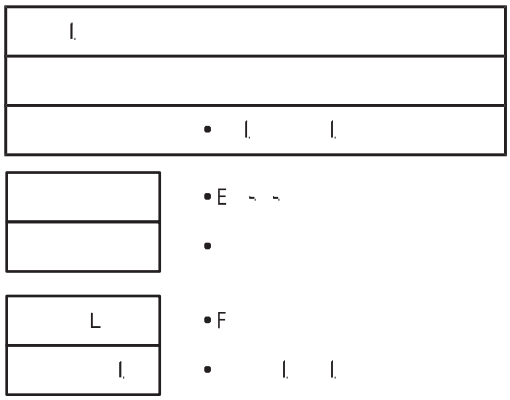
The OSI Layers

The International Organization for Standardization (ISO) is the Emily Post of the network protocol world. Just like Ms. Post, who wrote the book set- ting the standards—or protocols—for human social interaction, the ISO developed the OSI reference model as the precedent and guide for an open network protocol set. Defining the etiquette of communication models, it remains today the most popular means of comparison for protocol suites. The OSI reference model has seven layers:

- The Application layer
- The Presentation layer
- The Session layer
- The Transport layer
- The Network layer
- The Data Link layer
- The Physical layer

Figure 1.3 shows the functions defined at each layer of the OSI model. The following pages discuss this in detail.

FIGURE 1.3 Layer functions



The Application Layer

The *Application layer* of the OSI model is where users communicate to the computer. The Application layer is responsible for identifying and establishing the availability of the intended communication partner and determining if sufficient resources for the intended communication exist.

Although computer applications sometimes require only desktop resources, applications may unite communicating components from more than one network application; for example, file transfers, e-mail, remote access, network management activities, client/server processes, and infor- mation location. Many network applications provide services for communi- cation over enterprise networks, but for present and future internetworking, the need is fast developing to reach beyond their limits. Today, transactions and information exchanges between organizations are broadening to require internetworking applications like the following:

World Wide Web (WWW) Connects countless servers (the number seems to grow with each passing day) presenting diverse formats. Most are multimedia and include some or all of the following: graphics, text, video, and even sound. Netscape Navigator, Internet Explorer, and other browsers like Mosaic simplify both accessing and viewing Web sites.

E-mail gateways Are versatile and can use Simple Mail Transfer Protocol (SMTP) or the X.400 standard to deliver messages between different e-mail applications.

Electronic Data Interchange (EDI) Is a composite of specialized standards and processes that facilitates the flow of tasks such as accounting, shipping/receiving, and order and inventory tracking between businesses.

Special interest bulletin boards Include the many Internet chat rooms where people can connect and communicate with each other either by posting messages or by typing a live conversation. They can also share public domain software.

Internet navigation utilities Include applications like Gopher and WAIS, as well as search engines like Yahoo!, Excite, and Alta Vista, which help users locate the resources and information they need on the Internet.

Financial transaction services Target the financial community. They gather and sell information pertaining to investments, market trading, commodities, currency exchange rates, and credit data to their subscribers.

The Presentation Layer

The *Presentation layer* gets its name from its purpose: It presents data to the Application layer. It's essentially a translator and provides coding and conversion functions. A successful data transfer technique is to adapt the data into a standard format before transmission. Computers are configured to receive this generically formatted data and then convert the data back into its native format for actual reading (for example, EBCDIC to ASCII). By providing translation services, the Presentation layer ensures that data transferred from the Application layer of one system can be read by the Application layer of another host.

The OSI has protocol standards that define how standard data should be formatted. Tasks like data compression, decompression, encryption, and decryption are associated with this layer. Some Presentation layer standards are involved in multimedia operations. The following serve to direct graphic and visual image presentation:

PICT This is picture format used by Macintosh or PowerPC programs for transferring QuickDraw graphics.

TIFF The Tagged Image File Format is a standard graphics format for high-resolution, bitmapped images.

JPEG The Joint Photographic Experts Group brings these photo stan- dards to us.

Other standards guide movies and sound:

MIDI The Musical Instrument Digital Interface is used for digitized music.

MPEG The Moving Picture Experts Group's standard for the compression and coding of motion video for CDs is increasingly popular. It provides digital storage and bit rates up to 1.5Mbps.

QuickTime This is for use with Macintosh or PowerPC programs; it manages audio and video applications.

The Session Layer

The *Session layer* is responsible for setting up, managing, and then tearing down sessions between Presentation layer entities. The Session layer also provides dialog control between devices, or nodes. It coordinates communication between systems and serves to organize their communication by offering three different modes: *simplex*, *half-duplex*, and *full-duplex*. The Session layer basically keeps different applications' data separate from other applications' data.

The following are some examples of Session-layer protocols and interfaces (according to Cisco):

Network File System (NFS) Was developed by Sun Microsystems and used with TCP/IP and Unix workstations to allow transparent access to remote resources.

Structured Query Language (SQL) Was developed by IBM to provide users with a simpler way to define their information requirements on both local and remote systems.

Remote Procedure Call (RPC) Is a broad client/server redirection tool used for disparate service environments. Its procedures are created on clients and performed on servers.

X Window Is widely used by intelligent terminals for communicating with remote Unix computers, allowing them to operate as though they were locally attached monitors.

AppleTalk Session Protocol (ASP) Is another client/server mechanism, which both establishes and maintains sessions between AppleTalk client and server machines.

Digital Network Architecture Session Control Protocol (DNA SCP) Is a DECnet Session-layer protocol.

The Transport Layer

Services located in the *Transport layer* both segment and reassemble data from upper-layer applications and unite it onto the same data stream. They provide end-to-end data transport services and can establish a logical connection between the sending host and destination host on an internetwork.

Some of you might already be familiar with TCP and UDP (which you will learn about in Chapter 3) and know that TCP is a reliable service and UDP is not. Application developers have their choice of the two protocols when working with TCP/IP protocols.

The Transport layer is responsible for providing mechanisms for multi- plexing upper-layer application, session establishment, and teardown of vir- tual circuits. It also hides details of any network-dependent information from the higher layers by providing transparent data transfer.

Flow Control

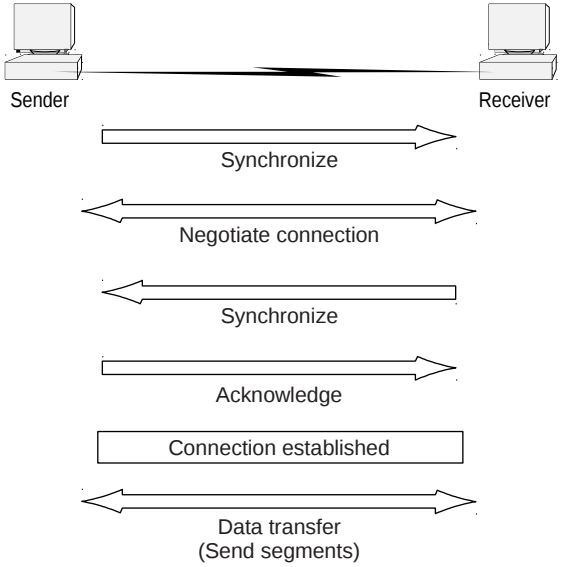
Data integrity is ensured at the Transport layer by maintaining flow control and allowing users the option of requesting reliable data transport between systems. *Flow control* prevents a sending host on one side of the connection from overflowing the buffers in the receiving host—an event that can result in lost data. Reliable data transport employs a connection-oriented communications session between systems, and the protocols involved ensure the fol- lowing will be achieved:

- The segments delivered are acknowledged back to the sender upon their reception.
    - Any segments not acknowledged are retransmitted.
- Segments are sequenced back into their proper order upon arrival at their destination.
- A manageable data flow is maintained in order to avoid congestion, overloading, and data loss.

Connection-Oriented Communication

In reliable transport operation, one device first establishes a connection-oriented session with its peer system. Figure 1.4 portrays a typical reliable session taking place between sending and receiving systems. In it, both hosts' application programs begin by notifying their individual operating systems that a connection is about to be initiated. The two operating systems com- municate by sending messages over the network confirming that the transfer is approved and that both sides are ready for it to take place. Once the required synchronization is complete, a connection is fully established and the data transfer begins. Cisco sometimes refers to this as a three-way handshake.

FIGURE 1.4 Establishing a connection-oriented session



While the information is being transferred between hosts, the two machines periodically check in with each other, communicating through their protocol software to ensure that all is going well and that the data is being received properly.

The following summarizes the steps in the connection-oriented session pictured in Figure 1.4:

- The first “connection agreement” segment is a request for synchronization.
- The second and third segments acknowledge the request and establish connection parameters between hosts.
- The final segment is also an acknowledgment. It notifies the destina- tion host that the connection agreement is accepted and that the actual connection has been established. Data transfer can now begin.

During a transfer, congestion can occur because a high-speed computer is generating data traffic faster than the network can transfer it or because many computers are simultaneously sending datagrams through a single gateway or destination. In the latter case, a gateway or destination can become congested even though no single source caused the problem. In either case, the problem is basically akin to a freeway bottleneck—too much traffic for too small a capacity. Usually, no one car is the problem; there are simply too many cars on that freeway.

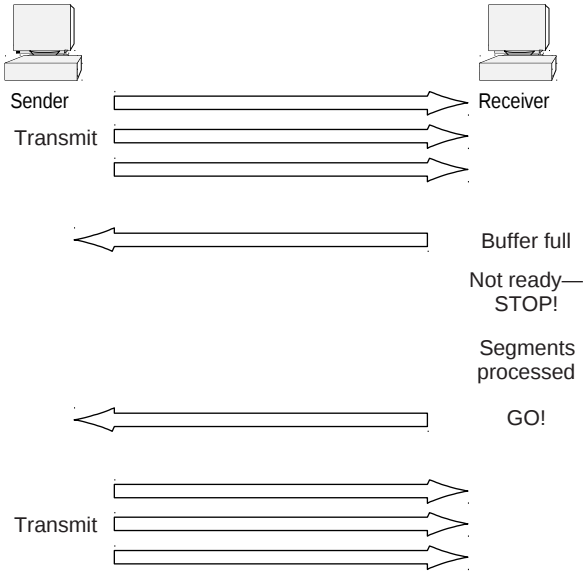
When a machine receives a flood of datagrams too quickly for it to process, it stores them in a memory section called a *buffer*. This buffering action solves the problem only if the datagrams are part of a small burst. However, if the datagram deluge continues, a device’s memory will eventually be exhausted, its flood capacity will be exceeded, and it will discard any additional datagrams that arrive.

But, no worries—because of the transport function, network flood control systems work quite well. Instead of dumping resources and allowing data to be lost, the transport can issue a “not ready” indicator to the sender, or source, of the flood (as shown in Figure 1.5). This mechanism works kind of like a stoplight, signaling the sending device to stop transmitting segment traffic to its overwhelmed peer. After the peer receiver processes the segments already in its memory reservoir, it sends out a “ready” transport indicator. When the machine waiting to transmit the rest of its datagrams receives this “go” indictor, it then resumes its transmission.

In fundamental, reliable, connection-oriented data transfer, datagrams are delivered to the receiving host in exactly the same sequence they’re trans- mitted; the transmission fails if this order is breached. If any data segments are lost, duplicated, or damaged along the way, a failure will transmit. The

answer to the problem is to have the receiving host acknowledge receiving each and every data segment.

FIGURE 1.5 Transmitting segments with flow control



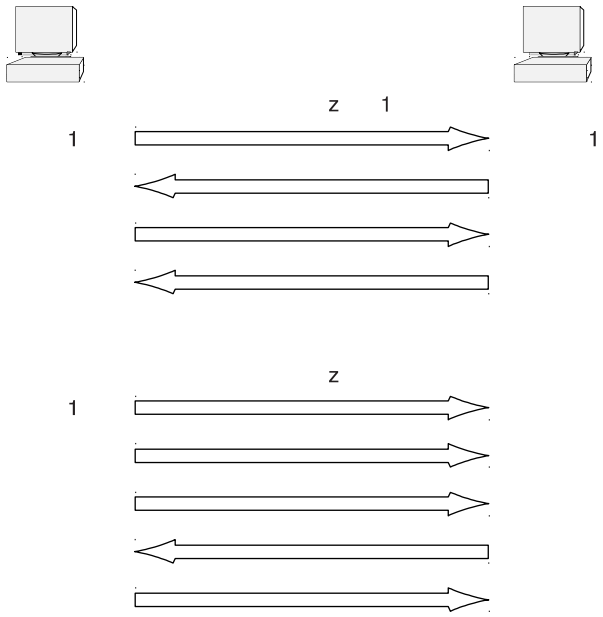
Windowing

Data throughput would be low if the transmitting machine had to wait for an acknowledgment after sending each segment. Because there's time available after the sender transmits the data segment and before it finishes processing acknowledgments from the receiving machine, the sender uses the break to transmit more data. The quantity of data segments the transmitting machine is allowed to send without receiving an acknowledgment for them is called a *window*.

Windowing controls how much information is transferred from one end to the other. While some protocols quantify information by observing the number of packets, TCP/IP measures it by counting the number of bytes. In Figure 1.6, there is a window size of 1 and a window size of 3. When a window size of 1 is configured, the sending machine waits for an acknowledgment for each data segment it transmits before transmitting another.

Configured to a window size of 3, it's allowed to transmit three data segments before an acknowledgment is received. In our simplified example, both the sending and receiving machines are workstations. Reality is rarely that simple, and most often acknowledgments and packets will commingle as they travel over the network and pass through routers. Routing complicates things, but not to worry, you'll learn about applied routing later in the book.

FIGURE 1.6 Windowing



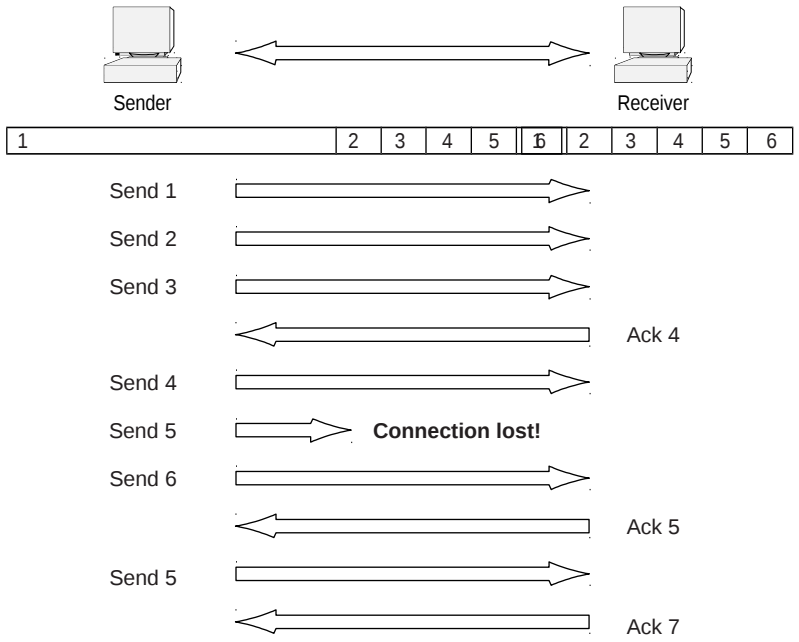
Acknowledgments

Reliable data delivery ensures the integrity of a stream of data sent from one machine to the other through a fully functional data link. It guarantees the data won't be duplicated or lost. The method that achieves this is known as *positive acknowledgment with retransmission.* This technique requires a receiving machine to communicate with the transmitting source by sending an acknowledgment message back to the sender when it receives data. The sender documents each segment it sends and waits for this acknowledgment

before sending the next segment. When it sends a segment, the transmitting machine starts a timer and retransmits if it expires before an acknowledgment is returned from the receiving end.

In Figure 1.7, the sending machine transmits segments 1, 2, and 3. The receiv- ing node acknowledges it has received them by requesting segment 4. When it receives the acknowledgment, the sender then transmits segments 4, 5, and 6. If segment 5 doesn't make it to the destination, the receiving node acknowledges that event with a request for the segment to be resent. The sending machine will then resend the lost segment and wait for an acknowledgment, which it must receive in order to move on to the transmission of segment 7.

FIGURE 1.7 Transport layer reliable delivery



The Network Layer

The *Network layer* is responsible for routing through an internetwork and for network addressing. This means that the Network layer is responsible for transporting traffic between devices that are not locally attached. *Routers*, or

other layer-3 devices, are specified at the Network layer and provide the routing services in an internetwork.

When a packet is received on a router interface, the destination IP address is checked. If the packet is not destined for the router, then the router will look up the destination network address in the routing table. Once an exit interface is chosen, the packet will be sent to the interface to be framed and sent out on the local network. If the entry for the destination network is not found in the routing table, the router drops the packet.

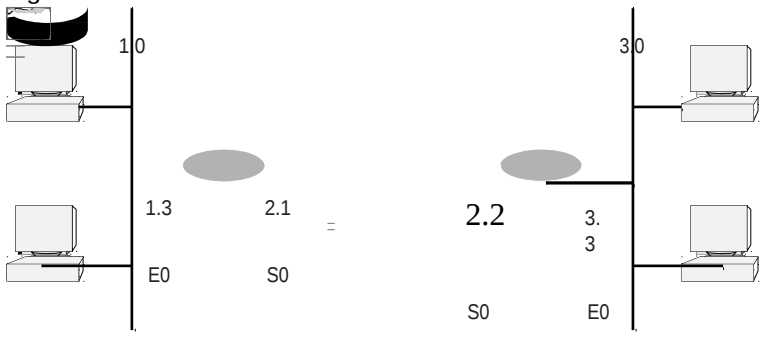
Two types of packets are used at the network layer: data and route updates.

Data packets Are used to transport user data through the internetwork, and protocols used to support data traffic are called routed protocols. Examples of routed protocols are IP and IPX. You'll learn about IP addressing in Chapter 3 and IPX addressing in Chapter 8.

Route update packets Are used to update neighbor routers about networks connected to routers in the internetwork. Protocols that send route update packets are called routing protocols, and examples are RIP, EIGRP, and OSPF, to name a few. Routing update packets are used to help build and maintain routing tables on each router.

Figure 1.8 shows an example of a routing table.

FIGURE 1.8 Routing table used in a router



Routing Table

NET	INT	Metric
1	E0	0
2	S0	0
3	S0	1

Routing Table

NET	INT	Metric
1	S0	1
2	S0	0
3	E0	0

The routing table used in a router includes the following information:

Network addresses Protocol-specific network addresses. A router must maintain a routing table for individual routing protocols because each routing protocol keeps track of a network with a different addressing scheme. Think of it as a street sign in each of the different languages spoken by the residents on a street.

Interface The exit interface a packet will take when destined for a specific network.

Metric The distance to the remote network. Different routing protocols use different methods of computing this distance. Routing protocols are covered in Chapter 5, but you need to understand that some routing protocols use hop count (the number of routers a packet passes through when routing to a remote network), while others use bandwidth, delay of the line, or even tick count (1/18 of a second).

Routers break up *broadcast domains*. This means, by default, that broadcasts are not forwarded through a router. This is good. Routers also break up collision domains, but this can also accomplished through layer-2 switches. Each interface in a router is a separate network and must be assigned unique network identification numbers. Each host on the network connected to that router must use that same network number.

Some points about routers that you must remember:

- Routers, by default, will not forward any broadcast or multicast packets.
- Routers use the logical address in a network layer header to determine the next hop router to forward the packet to.
- Routers can use access lists, created by an administrator, to control security on packets trying to either enter or exit an interface.
- Routers can provide layer-2 bridging functions if needed and can simultaneously route through the same interface.
- Layer-3 devices (routers in this case) provide connections between Vir- tual LANs (VLANs).

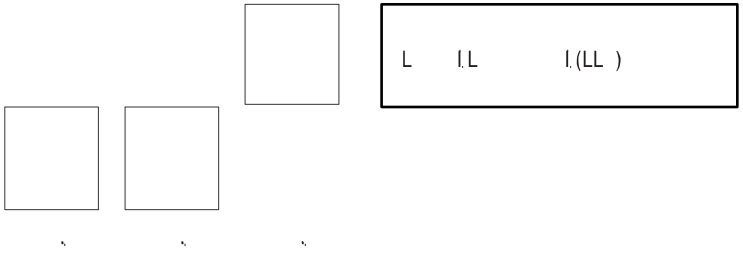
Switching and VLANs and are covered in Chapters 2 and 6, respectively.

- Routers can provide Quality of Service (QoS) for specific types of net- work traffic.

The Data Link Layer

The *Data Link layer* ensures that messages are delivered to the proper device and translates messages from the Network layer into bits for the Physical layer to transmit. It formats the message into *data frames* and adds a customized header containing the hardware destination and source address. This added information forms a sort of capsule that surrounds the original message in much the same way that engines, navigational devices, and other tools were attached to the lunar modules of the Apollo project. These various pieces of equipment were useful only during certain stages of space flight and were stripped off the module and discarded when their designated stage was complete. Data traveling through networks is similar. Figure 1.9 shows the Data Link layer with the Ethernet and IEEE specifications. Notice in the fig- ure that the IEEE 802.2 standard is used in conjunction with the other IEEE standards, adding functionality to the existing IEEE standards.

FIGURE 1.9 Data Link layer



You need to understand that routers, which work at the Network layer, do not care about where a host is located but only where networks are located. They also keep track of the best way to get to a remote network. The Data Link layer is responsible for uniquely identifying each device on a local network.

For a host to send packets to individual hosts and between routers, the Data Link layer uses hardware addressing. Each time a packet is sent between routers, it is framed with control information at the Data Link layer, but that information is stripped off at the receiving router and only the original packet is left completely intact. This framing of the packet continues for each hop until the packet is finally delivered to the receiving host. It is important to understand that the packet was never altered along the route, only encapsulated with the type of control information to be passed on to the different media types.

The IEEE Ethernet Data Link layer has two sublayers:

Media Access Control (MAC) 802.3 This defines how packets are placed on the media. Contention media access is first come, first served access where everyone shares the same bandwidth. Physical addressing is defined here, as well as logical topologies. Logical topology is the signal path through a physical topology. Line discipline, error notification (not correction), ordered delivery of frames, and optional flow control can also be used at this sublayer.

Logical Link Control (LLC) 802.2 This sublayer is responsible for iden- tifying Network layer protocols and then encapsulating them. An LLC header tells the Data Link layer what to do with 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. The LLC can also provide flow control and sequencing of control bits.

Switches and Bridges at the Data Link Layer

Switches and *bridges* both work at the Data link layer and filter the network using hardware (MAC) addresses. Layer-2 switching is considered hardware-based bridging because it uses a specialized hardware called *Application-Specific Integrated Circuits (ASICs)*. ASICs can run up to gigabit speeds with very low latency.

Bridges and switches read each frame as it passes through the network. The layer-2 device then puts the source hardware address in a filter table and keeps track of which port it was received on. This tells the switch where that device is located.

After a filter table is built on the layer-2 device, the device will only forward frames to the segment where the destination hardware address is located. If the destination device is on the same segment as the frame, the

layer-2 device will block the frame from going to any other segments. If the destination is on another segment, the frame is only transmitted to that seg- ment. This is called transparent bridging.

When a layer-2 device (switch) interface receives a frame and the destina- tion hardware address is unknown to the device's filter table, it will forward the frame to all connected segments. If the unknown device replies to this forwarding of the frame, the switch updates the filter table on that device's location. However, the destination address of the transmitting frame may be a broadcast address, in which case the switch will forward all broadcasts to every connected segment by default.

All devices that the broadcast is forwarded to are considered to be in the same broadcast domain. Layer-2 devices propagate layer-2 broadcast storms. The only way to stop a broadcast storm from propagating through an internetwork is with a layer-3 device (router).

The biggest benefit of using switches instead of hubs in your internetwork is that each switch port is its own collision domain, whereas a hub creates one large collision domain. However, switches and bridges do not break up broadcast domains, instead forwarding all broadcasts.

Another benefit of LAN switching over hub implementations is that each device on every segment plugged into a switch can transmit simultaneously because each segment is its own collision domain. Hubs allow only one device per network to communicate at a time.

Switches cannot translate between different media types. In other words, each device connected to the switch must use an Ethernet frame type. If you wanted to connect to a Token Ring switch or LAN, you would need a router to provide the translation services.

The Physical Layer

The *Physical layer* has two responsibilities: it sends bits and receives bits. Bits come only in values of 1 or 0—a Morse code with numerical values. The Physical layer communicates directly with the various types of actual com- munication media. Different kinds of media represent these bit values in dif- ferent ways. Some use audio tones, while others employ *state transitions*— changes in voltage from high to low and low to high. Specific protocols are needed for each type of media to describe the proper bit patterns to be used, how data is encoded into media signals, and the various qualities of the phys- ical media's attachment interface.

The Physical layer specifications specify the electrical, mechanical, proce- dural, and functional requirements for activating, maintaining, and deacti- vating a physical link between end systems.

At the Physical layer, the interface between the Data Terminal Equipment, or DTE, and the Data Circuit-Terminating Equipment, or DCE, is identified. The DCE is usually located at the service provider, while the DTE is the attached device. The services available to the DTE are most often accessed via a modem or Channel Service Unit/Data Service Unit (CSU/DSU).

The Physical layer's connectors and different physical topologies are defined by the OSI as standards, allowing disparate systems to communicate. The CCNA course and exam are only interested in the Ethernet standards.

Hubs at the Physical Layer

Hubs are really multiple port repeaters. A repeater receives a digital signal and reamplifies it or regenerates the digital signal, then forwards the digital signal out all active ports without looking at any data. An Active hub does the same thing. Any digital signal received from a segment on a hub port is regenerated or reamplified and transmitted out all ports on the hub. This means all devices plugged into a hub are in the same collision domain as well as in the same broadcast domain. A broadcast domain is defined as all devices on a network segment that hear all broadcasts sent on that segment.

Hubs, like repeaters, do not look at any traffic as they enter and are trans- mitted out to the other parts of the physical media. Hubs create a physical star network where the hub is a central device and cables extend in all direc- tions, creating the physical star effect. However, Ethernet networks use a logical bus topology. This means that the signal has to run from end to end of the network. Every device connected to the hub, or hubs, must listen if a device transmits.

Ethernet Networking

E*thernet* is a contention media access method that allows all hosts on a network to share the same bandwidth of a link. Ethernet is popular because it is easy to implement, troubleshoot, and add new technologies, like Fast-
Ethernet and Gigabit Ethernet, to existing network infrastructures. Ethernet uses the Data Link and Physical layer specifications, and this section of the chapter will give you both the Data Link and Physical layer information you

need to effectively implement, troubleshoot, and maintain an Ethernet network.

Ethernet networking uses what is called *Carrier Sense Multiple Access with Collision Detect (CSMA/CD)*, which helps devices share the bandwidth evenly without having two devices transmit at the same time on the network medium. CSMA/CD was created to overcome the problem of collisions that occur when packets are transmitted simultaneously from different nodes. Good collision management is important, because when a node transmits in a CSMA/CD network, all the other nodes on the network receive and examine that transmission. Only bridges and routers effectively prevent a transmission from propagating through the entire network.

The CSMA/CD protocol works like this: When a host wants to transmit over the network, it first checks for the presence of a digital signal on the wire. If all is clear (no other host is transmitting), the host will then proceed with its transmission. And it doesn't stop there. The transmitting host con- stantly monitors the wire to make sure no other hosts begin transmitting. If the host detects another signal on the wire, it sends out an extended jam sig- nal that causes all nodes on the segment to stop sending data. The nodes respond to that jam signal by waiting a while before attempting to transmit again. Backoff algorithms determine when the colliding stations retransmit. If after 15 tries collisions keep occurring, the nodes attempting to transmit will then time-out.

Half- and Full-Duplex Ethernet

Half-duplex Ethernet is defined in the original 802.3 Ethernet and uses only one wire pair with a digital signal running in both directions on the wire. It also uses the CSMA/CD protocol to help prevent collisions and retransmit if a collision does occur. If a hub is attached to a switch, it must operate
in half-duplex mode because the end stations must be able to detect collisions. Half-duplex Ethernet, typically 10BaseT, is only about 50 to 60 percent efficient, as Cisco sees it. However, you typically will only get 3- to 4Mbps, at most, in a large 10BaseT network.

Full-duplex Ethernet uses two pairs of wires, instead of one wire pair like half duplex. Full duplex uses a point-to-point connection between the trans- mitter of the transmitting device and the receiver of the receiving device. There are no collisions because it's as if we now have a freeway with multiple lanes instead of the single-lane road associated with half duplex. Full-duplex

Ethernet is supposed to offer 100 percent efficiency in both directions. This means that you can get 20Mbps with a 10Mbps Ethernet running full duplex, or 200Mbps for FastEthernet. This is called an aggregate rate, but it essentially means "you're supposed to get" 100 percent efficiency, though no one is certain.

When a full-duplex Ethernet port is powered on, it connects to the remote end and then negotiates with the other end of the FastEthernet link. This is called an auto-detect mechanism. This mechanism first decides on the exchange capability, which means it checks to see if it can run at 10 or 100Mbps. It then checks to see if it can run full duplex. If it cannot, then it will run half duplex.

Ethernet at the Data Link Layer

Ethernet at the Data Link layer is responsible for Ethernet addressing, which is typically called hardware addressing or MAC addressing. Ethernet is also responsible for framing packets received from the Network layer and preparing them for transmission on the local network through the Ethernet contention media access method. There are four different types of Ethernet frames available:

- Ethernet_II
- IEEE 802.3
- IEEE 802.2
- SNAP

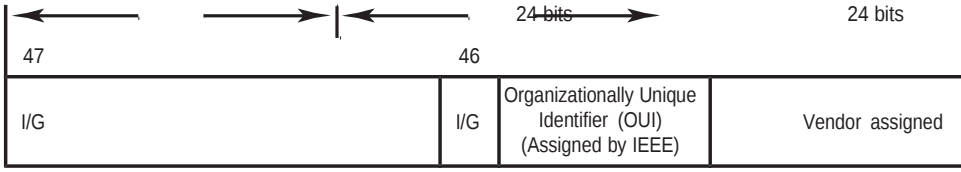
I will discuss all four of the available Ethernet frames in the upcoming sections.

Ethernet Addressing

Ethernet addressing uses the *Media Access Control (MAC) address* burned into each and every Ethernet Network Interface Card (NIC). The MAC address, sometimes referred to as a hardware address, is a 48-bit address written in a canonical format to ensure that addresses are at least written in the same format, even if different LAN technologies are used.

Figure 1.10 shows the 48-bit MAC addresses and how the bits are divided.

FIGURE 1.10 Ethernet addressing using MAC addresses



The *Organizationally Unique Identifier (OUI)* is assigned by the IEEE to an organization (24 bits or 3 bytes). The organization, in turn, assigns a globally administered address (24 bits or 3 bytes) that is unique (supposedly) to each and every adapter they manufacturer. Notice bit 46. Bit 46 must be 0 if it is a globally assigned bit from the manufacturer and 1 if it is locally administered from the network administrator.

Ethernet Frames

The Data Link layer is responsible for combining bits into bytes and bytes into *frames*. Frames are used at the Data Link layer to encapsulate packets handed down from the Network layer for transmission on a type of media access. There are three types of media access methods: contention (Ethernet), token passing (Token Ring and FDDI), and polling (IBM Mainframes and 100VGAnylan). This CCNA exam covers primarily Ethernet (contention) media access.

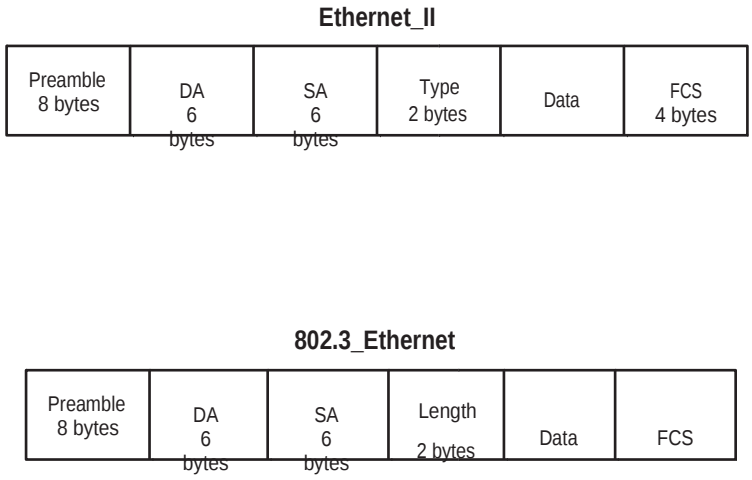
The function of Ethernet stations is to pass data frames between each other using a group of bits known as a MAC frame format. This provides error detection from a cyclic redundancy check (CRC). However, remember that this is error detection, not error correction. The 802.3 frames and Ether- net frame are shown in Figure 1.11.

The following bullet points detail the different fields in the 802.3 and Ethernet frame types.

Preamble An alternating 1,0 pattern provides a 5MHz clock at the start of each packet, which allows the receiving devices to lock the incoming bit stream. The preamble uses either an SFD or synch field to indicate to the receiving station that the data portion of the message will follow.

Start Frame Delimiter (SFD)/Synch SFD is 1,0,1,0,1,0, etc., and the synch field is all 1s. The preamble and SFD/synch field are 64 bits long.

FIGURE 1.11 802.3 and Ethernet frame formats



Destination Address (DA) This transmits a 48-bit value using the Least Significant Bit (LSB) first. DA is used by receiving stations to determine if an incoming packet is addressed to a particular node. The destination address can be an individual address, or a broadcast or multicast
MAC address. Remember that a broadcast is all 1s or Fs in hex and is sent to all devices, whereas a multicast is sent to only a similar subset of nodes on a network.

Hex is short for hexadecimal, which is a numbering system that uses the first six letters of the alphabet (A through F) to extend beyond the available 10 dig- its in the decimal system. Hexadecimal has a total of 16 digits.

Source Address (SA) SA is a 48-bit MAC address supplied by the transmitting device. It uses the Least Significant Bit (LSB) first. Broadcast and multicast address formats are illegal within the SA field.

Length or Type field 802.3 uses a length field, whereas the Ethernet frame uses a type field to identify the Network layer protocol. 802.3 cannot identify the upper-layer protocol and must be used with a proprietary LAN, for example, IPX.

Data This is a packet sent down to the Data Link layer from the Network layer. The size can vary from 46–1500 bytes.

Frame Check Sequence (FCS) FCS is a field at the end of the frame that is used to store the cyclic redundancy check (CRC).

Let's take a look at some frames caught on our trusty Etherpeek network analyzer. The frame below has only three fields: a destination, source, and type field. This is an Ethernet_II frame. Notice the type field is IP, or 08-00 in hexadecimal.

```
Destination:     00:60:f5:00:1f:27
Source:          00:60:f5:00:1f:2c
Protocol Type:08-00  IP
```

The next frame has the same fields, so it must also be an Ethernet_II frame. We included this one so you could see that the frame can carry more than just IP: It can also carry IPX, or 81-37h. Notice that this frame was a broadcast. You can tell because the destination hardware address is all 1s in binary, or all Fs in hexadecimal.

```
Destination:  ff:ff:ff:ff:ff:ff  Ethernet  Broadcast
Source:       02:07:01:22:de:a4
Protocol  Type:81-37    NetWare
```

Notice the length field in the next frame. This must be an 802.3 frame. Which protocol is this going to be handed to at the Network layer? It doesn't specify in the frame, so it must be IPX. Why? Because when Novell created the 802.3 frame type (before the IEEE did and called it 802.3 Raw), Novell was pretty much the only LAN server out there. So, Novell was assuming that if you're running a LAN, it must be IPX.

```
Flags:           0x80  802.3
Status:          0x00
Packet Length:64
Timestamp:       12:45:45.192000  06/26/1998
Destination:  ff:ff:ff:ff:ff:ff  Ethernet  Broadcast
Source:          08:00:11:07:57:28
Length:          34
```

802.2 and SNAP

Remember that the 802.3 Ethernet frame cannot by itself identify the upper-layer (Network) protocol; it needs help. The IEEE defined the 802.2 LLC specifications to provide this function and more. Figure 1.12 shows the IEEE 802.3 with LLC (802.2) and the Subnetwork Architecture Protocol (SNAP) frame types.

FIGURE 1.12 802.2 and SNAP

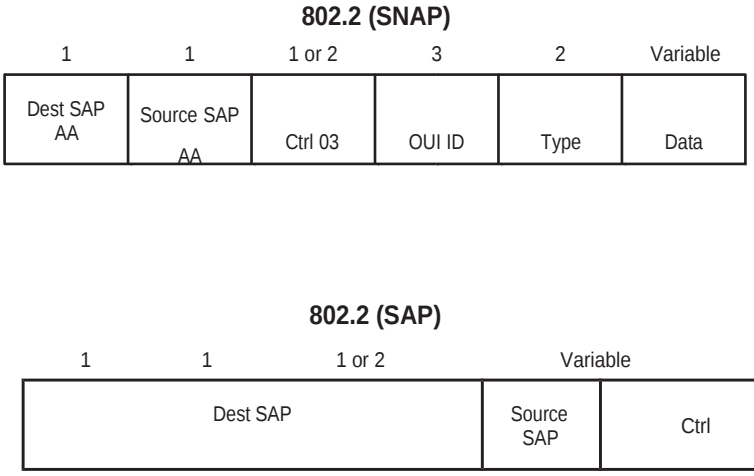


Figure 1.12 shows how the LLC header information is added to the data portion of the frame.

Now, let's take a look at an 802.2 frame and SNAP captured from our analyzer.

802.2 Frame

The following is an 802.2 frame captured with a protocol analyzer. Notice that the first frame has a length field, so it's probably an 802.3, right? But look again; it also has a DSAP and an SSAP, so it has to be an 802.2 frame. (Remember that an 802.2 frame is an 802.3 frame with the LLC information

in the data field of the header, so we know what the upper-layer protocol is.) Here is the frame:

```
Flags:          0x80  802.3
Status:         0x02  Truncated
Packet Length:64
Slice Length:   51
Timestamp:      12:42:00.592000  03/26/1998
Destination:    ff:ff:ff:ff:ff:ff Ethernet Broadcast
Source:         00:80:c7:a8:f0:3d
LLC Length:     37
Dest. SAP:      0xe0  NetWare
Source SAP:     0xe0  NetWare  Individual  LLC  Sublayer
Management Function
Command:        0x03  Unnumbered  Information
```

SNAP Frame

The SNAP frame has its own protocol field to identify the upper-layer protocol. This is really a way to allow an Ethernet_II frame to be used in an 802.3 frame. Even though the following network trace shows a protocol field, it is really an Ethernet_II type (ether-type) field.

```
Flags:          0x80  802.3
Status:         0x00
Packet Length:78
Timestamp:      09:32:48.264000  01/04/2000
802.3 Header
Destination:    09:00:07:FF:FF:FF   AT Ph 2 Broadcast
Source:         00:00:86:10:C1:6F
LLC Length:     60
802.2 Logical Link Control (LLC) Header
Dest. SAP:      0xAA  SNAP
Source SAP:     0xAA  SNAP
Command:        0x03  Unnumbered  Information
Protocol:       0x080007809B  AppleTalk
```

You can identify a SNAP frame because the DSAP and SSAP fields are always AA, and the command field is always 3. The reason this frame type was created is because not all protocols worked well with the 802.3 Ethernet frame, which didn't have an ether-type field. To allow the proprietary pro- tocols created by application developers to be used in the LLC frame, the IEEE defined the SNAP format. It is not used that often and is mostly seen only with AppleTalk and proprietary frames. Cisco uses a SNAP frame with their proprietary protocol Cisco Discovery Protocol (CDP), which is covered in Chapter 7.

Ethernet at the Physical Layer

In a shared-hub Ethernet environment, if one station sends a frame, then all devices must synchronize to the digital signal being transmitted and extract the frame from the wire. All devices that use the same physical media and listen to each frame are considered to be in the same collision domain. This means that only one device can transmit at any given time, and any other device on the network segment must synchronize with the signal and extract the frame. If two stations try to transmit at the same time, a collision will occur. In 1984, the IEEE Ethernet committee released the Carrier Sense Multiple Access with Collision Detect (CSMA/CD) protocol. This basically tells all stations to constantly listen for any other device trying to transmit at the same time they are and to stop and wait for a predetermined time if they do sense a collision.

Ethernet uses a bus topology, which means that whenever a device transmits, the signal must run from one end of the segment to the other. Ethernet also defined baseband technology, which means that when a station does transmit, it will use the entire bandwidth on the wire and will not share it. Here are the original IEEE 802.3 standards:

10Base2 10Mbps, baseband technology, up to 185 meters in length. Known as thinnet and can support up to 30 workstations on a single seg- ment.

10Base5 10Mbps, baseband technology, up to 500 meters in length. Known as thicknet.

10BaseT 10Mbps using category-3 twisted-pair wiring. Unlike the 10Base2 and 10Base5 networks, each device must connect into a hub or switch, and you can only have one host per segment or wire.

Each of the 802.3 standards defines an Attachment Unit Interface (AUI), which allows a one-bit-at-a-time transfer to the Physical layer from the Data Link media access method. This allows the MAC to remain constant but means the Physical layer can support any existing and new technologies. The original AUI interface was a 15-pin connector, which allowed a transceiver (transmitter/receiver) that provided a 15-pin–to–twisted-pair conversion. Typically, the AUI has a built-in transceiver, and the connections are now usually just RJ-45 connections.

However, the AUI interface cannot support 100Mbps Ethernet because of the high frequencies involved. 100BaseT needed a new interface, and the 802.3u specifications created one called the Media Independent Interface (MII), which provides 100Mbps throughput. The MII uses a nibble, which is defined as four bits. Gigabit Ethernet uses a Gigabit Media Independent Interface (GMII), which is eight bits at a time.

Data Encapsulation

When a host transmits data across a network to another device, the data is *encapsulated* with protocol information at each layer of the OSI model. Each layer communicates only with its peer layer on the receiving device.

To communicate and exchange information, each layer uses what are called *Protocol Data Units (PDUs)*. These hold the control information attached to the data at each layer of the model, which is typically attached to the header of the data field but can also be in the trailer, or end of the data field.

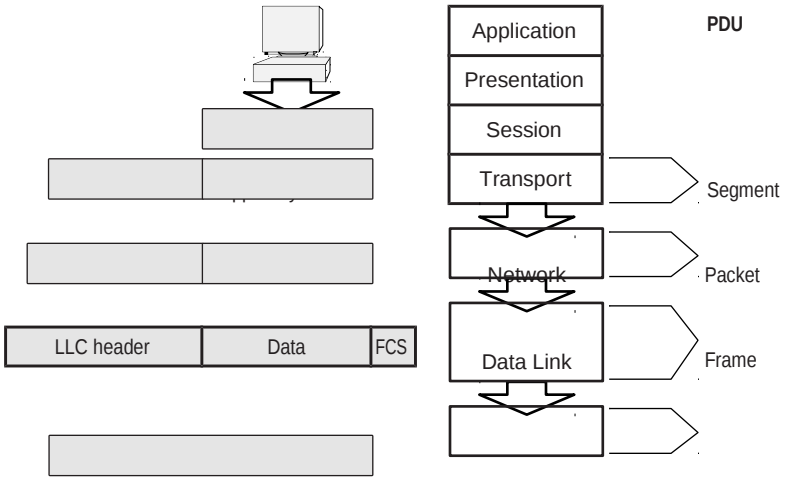
Each PDU is attached to the data by encapsulating it at each layer of the OSI model. Each PDU has a specific name depending on the information each header has. This PDU information is only read by the peer layer on the receiving device and then is stripped off and the data is handed to the next upper layer.

Figure 1.13 shows the PDUs and how they attach control information to each layer.

This figure shows how the upper-layer user data is converted for transmission on the network. The data stream is then handed down to the Transport layer, which sets up a virtual circuit to the receiving device by sending a synch packet. The data stream is then broken up into smaller pieces, and a Transport layer header (PDU) is created and called a segment. The header control information is attached to the header of the data field. Each segment

is sequenced so the data stream can be put back together on the receiving side exactly as transmitted.

FIGURE 1.13 Data encapsulation



Each segment is then handed to the Network layer for network addressing and routing through an internetwork. Logical addressing, for example, IP, is used to get each segment to the correct network. The Network-layer proto- col adds a control header to the segment handed down from the Transport layer, and it is now called a packet or datagram. Remember that the Trans- port and Network layers work together to rebuild a data stream on a receiv- ing host. However, they have no responsibility for placing their PDUs on a local network segment, which is the only way to get the information to a router or host.

The Data Link layer is responsible for taking packets from the Network layer and placing them on the network medium (cable or wireless). The Data Link layer encapsulates each packet in a frame, and the frame's header car- ries the hardware address of the source and destination hosts. If the device is on a remote network, then the frame is sent to a router to be routed through an internetwork. Once it gets to the destination network, a new frame is used to get the packet to the destination host.

To put this frame on the network, it must first be put into a digital signal. Since a frame is really a logical group of 1s and 0s, the Physical layer is responsible for encapsulating these digits into a digital signal, which is read

by devices on the same local network. The receiving devices will synchronize on the digital signal and extract the 1s and 0s from the digital signal. At this point the devices build the frames, run a cyclic redundancy check (CRC), and then check their answer against the answer in the frame's FCS field. If it matches, the packet is pulled from the frame, and the frame is discarded. This process is called de-encapsulation. The packet is handed to the Network layer, where the address is checked. If the address matches, the segment is pulled from the packet, and the packet is discarded. The segment is processed at the Transport layer, which rebuilds the data stream and acknowledges to the transmitting station that it received each piece. It then happily hands the data stream to the upper-layer application.

At a transmitting device, the data encapsulation method works as follows:

1. User information is converted to data for transmission on the network.
2. Data is converted to segments and a reliable connection is set up between the transmitting and receiving hosts.
3. Segments are converted to packets or datagrams, and a logical address is placed in the header so each packet can be routed through an inter- network.
4. Packets or datagrams are converted to frames for transmission on the local network. Hardware (Ethernet) addresses are used to uniquely identify hosts on a local network segment.
5. Frames are converted to bits, and a digital encoding and clocking scheme is used.

The Cisco Three-Layer Hierarchical Model

Most of us were exposed to hierarchy early in life. Anyone with older siblings learned what it was like to be at the bottom of the hierarchy! Regard- less of where you first discovered hierarchy, today most of us experience it
in many aspects of our lives. *Hierarchy* helps us understand where things belong, how things fit together, and what functions go where. It brings order and understandability to otherwise complex models. If you want a pay raise,

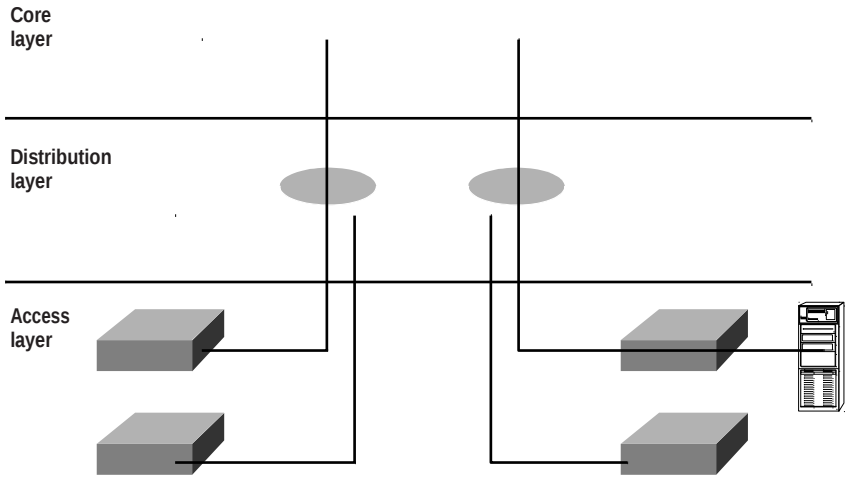
for instance, hierarchy dictates that you ask your boss, not your subordinate. That is the person whose role it is to grant (or deny) your request.

Hierarchy has many of the same benefits in network design that it does in other areas of life. When used properly, it makes networks more predictable. It helps us define at which levels of hierarchy we should perform certain functions. Likewise, you can use tools such as access lists at certain levels in hierarchical networks and avoid them at others.

Let's face it, large networks can be extremely complicated, with multiple protocols, detailed configurations, and diverse technologies. Hierarchy helps us summarize a complex collection of details into an understandable model. Then, as specific configurations are needed, the model dictates the appropriate manner to apply them.

The Cisco hierarchical model can help you design, implement, and maintain a scalable, reliable, cost-effective hierarchical internetwork. Cisco defines three layers of hierarchy, as shown in Figure 1.14, each with specific functions.

FIGURE 1.14 The Cisco hierarchical model



The following are the three layers:

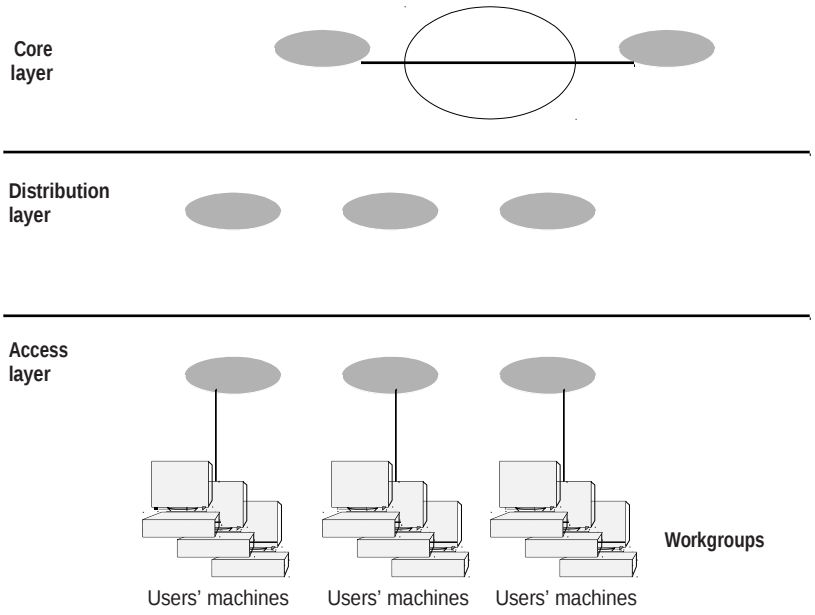
- The Core layer
- The Distribution layer
- The Access layer

Each layer has specific responsibilities. Remember, however, that the three layers are logical and are not necessarily physical devices. Consider the OSI model, another logical hierarchy. The seven layers describe functions but not necessarily protocols, right? Sometimes a protocol maps to more than one layer of the OSI model, and sometimes multiple protocols commu- nicate within a single layer. In the same way, when we build physical imple- mentations of hierarchical networks, we may have many devices in a single layer, or we might have a single device performing functions at two layers. The definition of the layers is logical, not physical.

Before you learn about these layers and their functions, consider a common hierarchical design as shown in Figure 1.15. The phrase "keep local traffic local" has almost become a cliché in the networking world; however, the underlying concept has merit. Hierarchical design lends itself perfectly to fulfilling this concept.

Now, let's take a closer look at each of the layers.

FIGURE 1.15 Hierarchical network design



The Core Layer

The *core layer* is literally the core of the network. At the top of the hierarchy, the core layer is responsible for transporting large amounts of traffic both reliably and quickly. The only purpose of the network's core layer is to switch traffic as fast as possible. The traffic transported across the core is common to a majority of users. However, remember that user data is processed at the dis- tribution layer, which forwards the requests to the core if needed.

If there is a failure in the core, *every single user* can be affected. Therefore, fault tolerance at this layer is an issue. The core is likely to see large volumes of traffic, so speed and latency are driving concerns here. Given the function of the core, we can now consider some design specifics. Let's start with some things we don't want to do.

- Don't do anything to slow down traffic. This includes using access lists, routing between virtual local area networks (VLANs), and packet filtering.
- Don't support workgroup access here.
- Avoid expanding the core when the internetwork grows (i.e., adding routers). If performance becomes an issue in the core, give preference to upgrades over expansion.

Now, there are a few things that we want to do as we design the core. They include the following:

- Design the core for high reliability. Consider data-link technologies that facilitate both speed and redundancy, such as FDDI, Fast Ether- net (with redundant links), or even ATM.
- Design with speed in mind. The core should have very little latency.
- Select routing protocols with lower convergence times. Fast and redundant data-link connectivity is no help if your routing tables are shot!

The Distribution Layer

The *distribution layer* is sometimes referred to as the workgroup layer and is the communication point between the access layer and the core. The pri- mary function of the distribution layer is to provide routing, filtering, and WAN access and to determine how packets can access the core, if needed.

The distribution layer must determine the fastest way that network service requests are handled; for example, how a file request is forwarded to a server. After the distribution layer determines the best path, it forwards the request to the core layer. The core layer then quickly transports the request to the correct service.

The distribution layer is the place to implement policies for the network. Here you can exercise considerable flexibility in defining network operation. There are several items that generally should be done at the distribution layer. They include the following:

- Implementation of tools such as access lists, of packet filtering, and of queuing
- Implementation of security and network policies, including address translation and firewalls
- Redistribution between routing protocols, including static routing
- Routing between VLANs and other workgroup support functions
- Definitions of broadcast and multicast domains

Things to avoid at the distribution layer are limited to those functions that exclusively belong to one of the other layers.

The Access Layer

The *access layer* controls user and workgroup access to internetwork resources. The access layer is sometimes referred to as the desktop layer. The network resources most users need will be available locally. The distribution layer handles any traffic for remote services. The following are some of the functions to be included at the access layer:

- Continued (from distribution layer) access control and policies
- Creation of separate collision domains (segmentation)
- Workgroup connectivity into the distribution layer

Technologies such as DDR and Ethernet switching are frequently seen in the access layer. Static routing (instead of dynamic routing protocols) is seen here as well.

As already noted, three separate levels does not imply three separate routers. It could be fewer, or it could be more. Remember, this is a *layered* approach.

Assembling and Cabling Cisco Devices

In this section, I'll address the corporate environment and the different types of cabling required to connect an internetwork. To understand
the types of cabling used to assemble and cable Cisco devices, you need to understand the LAN Physical layer implementation of Ethernet.

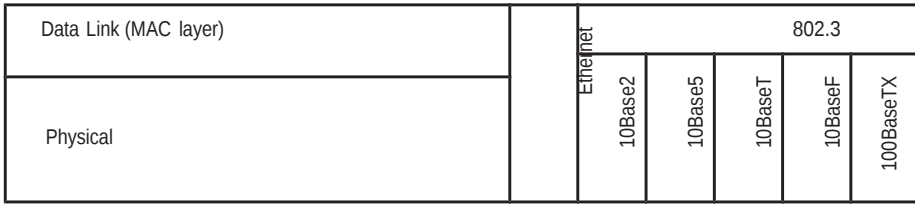
Ethernet is a media access method that is specified at the Data Link layer and uses specific Physical layer cabling and signaling techniques. It is impor- tant to be able to differentiate between the types of connectors that can be used to connect an Ethernet network together. I'll discuss the different unshielded twisted-pair cabling used today in an Ethernet LAN.

Cabling the Ethernet Local Area Network

Ethernet was first implemented by a group called DIX (Digital, Intel, and Xerox). They created and implemented the first Ethernet LAN specification, which the IEEE used to create the IEEE 802.3 committee. This was a 10Mbps network that ran on coax, twisted-pair, and fiber physical media.

The IEEE extended the 802.3 committee to two new committees known as 802.3u (FastEthernet) and 802.3q (Gigabit Ethernet). These are both specified on twisted-pair and fiber physical media. Figure 1.16 shows the IEEE 802.3 and original Ethernet Physical layer specifications.

FIGURE 1.16 Ethernet Physical layer specifications



When designing your LAN, it is important to understand the different types of Ethernet media available. It would certainly be great to run Gigabit Ethernet to each desktop and 10Gbps between switches, and although this might happen one day, it is unrealistic to think you can justify the cost of that network today. By mixing and matching the different types of Ethernet

media methods today, you can create a cost-effective network that works great.

The following bullet points provide a general understanding of where you can use the different Ethernet media in your hierarchical network:

- Use 10Mbps switches at the access layer to provide good performance at a low price. 100Mbps links can be used for high-bandwidth– consuming clients or servers. No servers should be at 10Mbps if possible.
- Use FastEthernet between access layer and distribution layer switches. 10Mbps links would create a bottleneck.
- Use FastEthernet (or Gigabit if applicable) between distribution layer switches and the core. Also, you should be implementing the fastest media you can afford between the core switches. Dual links between distribution and core switches are recommended for redundancy and load balancing.

Ethernet Media and Connector Requirements

It's important to understand the difference between the media access speeds Ethernet provides. However, it's also important to understand the connector requirements for each implementation before making any decision.

The EIA/TIA (Electronic Industries Association and the newer Telecommunications Industry Association) is the standards body that creates the Physical layer specifications for Ethernet. The EIA/TIA specifies that Ethernet use a *registered jack (RJ) connector* with a 4 5 wiring sequence on *unshielded twisted-pair (UTP)* cabling (RJ-45). The following bullet points outline the different Ethernet media requirements:

10Base2 50-ohm coax, called *thinnet*. Up to 185 meters and 30 hosts per segment. Uses a physical and logical bus with AUI connectors.

10Base5 50-ohm coax called *thicknet*. Up to 500 meters and 208 users per segment. Uses a physical and logical bus with AUI connectors. Up to 2500 meters with repeaters and 1024 users for all segments.

10BaseT EIA/TIA category 3, 4, or 5, using two-pair unshielded twisted-pair (UTP) wiring. One user per segment; up to 100 meters long. Uses an RJ-45 connector with a physical star topology and a logical bus.

100BaseTX EIA/TIA category 5, 6, or 7 UTP two-pair wiring. One user per segment; up to 100 meters long. Uses an RJ-45 MII connector with a physical star topology and a logical bus.

100BaseFX Uses fiber cabling 62.5/125-micron multimode fiber. Point-to-point topology; up to 400 meters long. Uses an ST or SC connector, which are duplex media-interface connectors.

1000BaseCX Copper shielded twisted-pair that can only run up to 25 meters.

1000BaseT Category 5, four-pair UTP wiring up to 100 meters long.

1000BaseSX MMF using 62.5 and 50-micron core; uses a 780-nanometer laser and can go up to 260 meters.

1000BaseLX Single-mode fiber that uses a 9-micron core, 1300-nanometer laser and can go from 3 km up to 10 km.

100VG-AnyLAN is a twisted-pair technology that was the first 100Mbps LAN. However, since it was incompatible with Ethernet signaling techniques (it used a polling media access method), it was not typically used and is essen- tially dead.

UTP Connections (RJ-45)

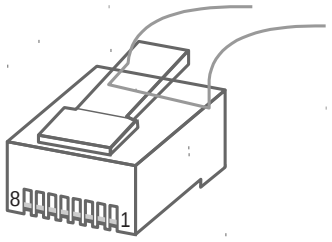
The RJ-45 connector is clear so you can see the eight colored wires that connect to the connector's pins. These wires are twisted into four pairs. Four wires (two pairs) carry the voltage and are considered *tip*. The other four wires are grounded and are called *ring*. The RJ-45 connector is crimped onto the end of the wire, and the pin locations of the connector are numbered from the left, 8 to 1.

Figure 1.17 shows a UTP cable with an RJ-45 connector attached.

The UTP cable has twisted wires inside that eliminate cross talk. Unshielded cable can be used since digital signal protection comes from the twists in the wire. The more twists per inch, the farther the digital signal can supposedly travel without interference. For example, categories 5 and 6 have many more twists per inch than category 3 UTP does.

FIGURE 1.17 UTP wire with an RJ-45 connector attached

Pin	Wire Pair (T Is Tip; R Is Ring)
1	Pair 2 T2
2	Pair 2 R2
3	Pair 3 T3
4	Pair 1 R1
5	Pair 1 T1
6	Pair 3 R3
7	Pair 4 T4
8	Pair 4 R4



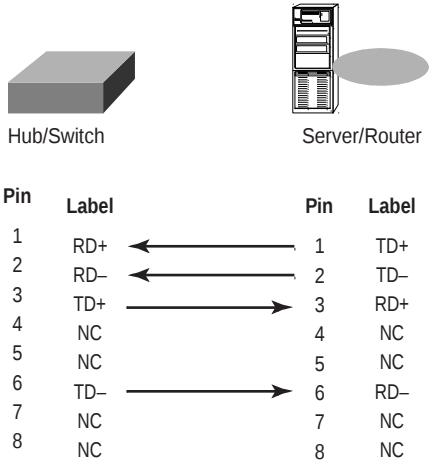
RJ-45 connector

Different types of wiring are used when building internetworks. You will need to use either a straight-through or crossover cable.

Straight-Through

In a UTP implementation of a straight-through cable, the wires on both cable ends are in the same order. Figure 1.18 shows the pinouts of the straight- through cable.

FIGURE 1.18 UTP straight-through pinouts



You can determine that the wiring is a straight-through cable by holding both ends of the UTP cable side by side and seeing that the order of the wires on both ends is identical.

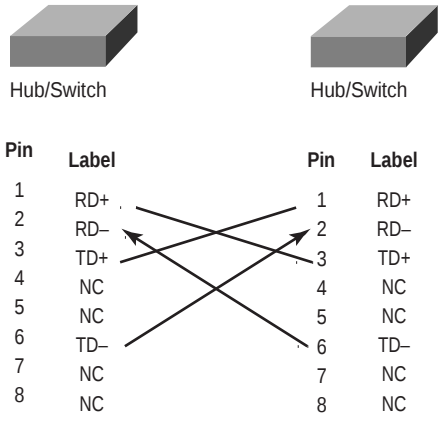
You can use a straight-through cable for the following tasks:

- Connecting a router to a hub or switch
- Connecting a server to a hub or switch
- Connecting workstations to a hub or switch

Crossover

In the implementation of a crossover, the wires on each end of the cable are crossed. Transmit to Receive and Receive to Transmit on each side, for both tip and ring. Figure 1.19 shows the UTP crossover implementation.

FIGURE 1.19 UTP crossover implementation



Notice that pin 1 on one side connects to pin 3 on the other side, and pin 2 connects to pin 6 on the opposite end.

You can use a crossover cable for the following tasks:

- Connecting uplinks between switches
- Connecting hubs to switches
- Connecting a hub to another hub

- Connecting a router interface to another router interface
- Connecting two PCs together without a hub or switch

When trying to determine the type of cable needed for a port, look at the port and see if it is marked with an "X." Use a straight-through cable when only one port is designated with an "X." Use a crossover when both ports are des- ignated with an "X" or when neither port has an "X."

Cabling the Wide Area Network

To connect your *wide area network (WAN)*, you need to understand the WAN Physical layer implementation provided by Cisco as well as the different WAN serial connectors. In this section, I will give you that information, along with the cabling requirements for ISDN BRI connections.

Cisco serial connections support almost any type of WAN service. The typical WAN connections are dedicated leased lines using High-Level Data Link Control (HDLC), Point-to-Point Protocol (PPP), Integrated Services Digital Network (ISDN), and Frame Relay. Typical speeds are anywhere from 2400bps to 1.544Mbps (T1).

All of these WAN types are discussed in detail in Chapter 10.

HDLC, PPP, and Frame Relay can use the same Physical layer specifications, but ISDN has different pinouts and specifications at the Physical layer.

Serial Transmission

WAN serial connectors use *serial transmission*, which is one bit at a time, over a single channel. *Parallel transmission* can pass at least 8 bits at a time. All WANs use serial transmission.

Cisco routers use a proprietary 60-pin serial connector, which you must buy from Cisco or a provider of Cisco equipment. The type of connector you have on the other end of the cable depends on your service provider or end-device requirements. The different ends available are EIA/TIA-232, EIA/TIA-449, V.35 (used to connect to a CSU/DSU), X.21 (used in X.25), and EIA-530.

Serial links are described in frequency or cycles-per-second (hertz). The amount of data that can be carried within these frequencies is called *bandwidth*. Bandwidth is the amount of data in bits-per-second that the serial channel can carry.

Data Terminal Equipment and Data Communication Equipment

Router interfaces are, by default, *Data Terminal Equipment (DTE)* and connect into *Data Communication Equipment (DCE)*, for example, a *Channel Service Unit/Data Service Unit (CSU/DSU)*. The CSU/DSU then plugs into a demarcation location (demarc) and is the service provider's last responsibility. Typically, the demarc is a jack that has an RJ-45 female connector located close to your equipment. If you report a problem to your service provider, they'll always tell you it tests fine up to the demarc and that the problem must be the CPE, or Customer Premise Equipment, which is your responsibility.

The idea behind a WAN is to be able to connect two DTE networks together through a DCE network. The DCE network includes the CSU/DSU, through the provider's wiring and switches, all the way to the CSU/DSU at the other end. The network's DCE device provides clocking to the DTE-connected interface (the router's serial interface).

Fixed and Modular Interfaces

Some routers Cisco sells have fixed interfaces, while others are modular. The fixed routers, such as the 2500 series, have set interfaces that can't be changed. The 2501 router has two serial connections and one 10BaseT AUI interface. If you need to add a third serial interface, then you need to buy a new router—ouch! However, the 1600, 1700, 2600, 3600, and higher routers have modular interfaces that allow you to buy what you need now and add almost any type of interface you may need later. The 1600 and 1700 are limited and have both fixed and modular ports, but the 2600 and up provide many serials, FastEthernet, and even voice-module availability.

Integrated Services Digital Network (ISDN) Connections

Integrated Services Digital Network (ISDN) Basic Rate Interface (BRI) is two B (Bearer) channels of 64k each and one D (Data) channel of 16k for signaling and clocking.

ISDN BRI routers come with either a U interface or what is known as an S/T interface. The difference between the two is that the U interface is already a two-wire ISDN convention that can plug right into the ISDN local loop. The S/T interface is a four-wire interface and needs a Network Termination type 1 (NT 1) to convert from a four-wire to the two-wire ISDN specification.

ISDN is covered in depth in Chapter 10.

The U interface has a built-in NT 1 device. If your service provider uses an NT 1 device, then you need to buy a router that has an S/T interface. Most Cisco router BRI interfaces are marked with a U or an S/T. When in doubt, ask Cisco or the salesperson you bought it from.

Primary Rate Interface (PRI) provides T1 speeds (1.544Mbps) in the U.S. and E1 speeds (2.048) in Europe. PRI is not discussed further in this course.

The ISDN BRI interface uses an RJ-45, category 5, straight-through cable. It is important to avoid plugging a console cable or other LAN cable into a BRI interface on a router, because it will probably ruin the interface. Cisco says it *will* ruin it, but I have students do it every week and haven't lost one yet (I probably shouldn't have said that…now I will probably lose one next week).

Console Connections

All Cisco devices are shipped with console cables and connectors, which allow you to connect to a device and configure, verify, and monitor it. The cable used to connect between a PC is a rollover cable with RJ-45 connectors.

The pinouts for a rollover cable are as follows:

1–8

2–7

3–6

4–5

5–4

6–3

7–2

8–1

You can see that you just take a straight-through RJ-45 cable, cut the end off, flip it over, and reattach a new connector.

Typically, you will use the DB9 connector to attach to your PC and use a com port to communicate via HyperTerminal. Most Cisco devices now sup- port RJ-45 console connections. However, the Catalyst 5000 series switch still uses a DB25 connector.

Set up the terminal emulation program to run 9600bps, 8 data bits, no parity, 1 stop bit, and no flow control. On some routers, you need to verify that the terminal emulation program is emulating a VT100 dumb-terminal mode, not an auto-sense mode, or it won't work.

Most routers also have an aux port, which is an auxiliary port used to connect a modem. You can then dial this modem and connect the router to the aux port. This will give you console access to a remote router that might be down and that you cannot telnet into. The console port and aux port are considered out-of-band management since you are configuring the router "out of the network." Telnet is considered in-band.

Selecting Cisco Products

You can use the Cisco three-layer model to determine what type of product to buy for your internetwork. By understanding the services
required at each layer and what functions the internetworking devices per- form, you can then match Cisco products to your business requirements. To select the correct Cisco products for your network, start by gathering infor- mation about where devices need to operate in the internetworking hierar- chy, and then consider issues like ease of installation, port-capacity requirements, and other features.

If you have remote offices or other WAN needs, you need to first find out what type of service is available. It won't do you any good to design a large Frame Relay network only to discover that Frame Relay is only supported in half the locations you need. After you research and find out about the

different options available through your service provider, you can choose the Cisco product that fits your business requirements.

You have a few options, typically: dial-up asynchronous connections, leased lines up to 1.544Mbps, Frame Relay, and ISDN, which are the most popular WAN technologies. However, xDSL is the new front-runner to take over as the fastest, most reliable, cheapest WAN technology. You need to consider your usage before buying and implementing a technology. For example, if your users at a remote branch are connected to the corporate office more than three to four hours a day, then you need either Frame Relay or a leased line. If they connect infrequently, then you might get away with ISDN or dial-up connectivity.

The next sections discuss the different types of Cisco hubs, routers, and switches you can use to build a hierarchical network.

Cisco Hubs

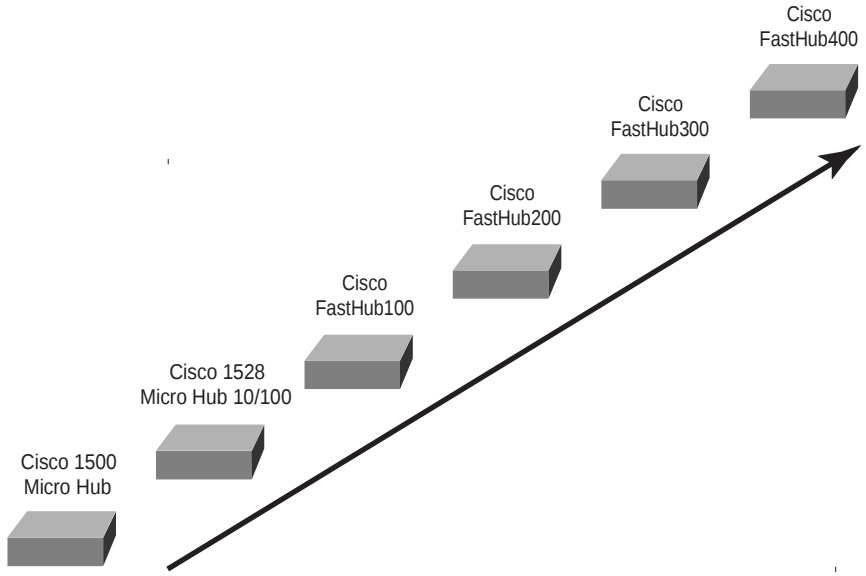
It is hard for me to imagine that you would call Cisco and ask to buy a hub, but I suppose it does happen or they wouldn't be selling them. Cisco actually has an extensive listing of hubs that address an amazing variety of selection issues.

Before you buy any hub, you need to know—not think you know, but actually know—which users can use a shared 10Mbps or shared 100Mbps network. The lower-end model of hubs Cisco offers supports only 10Mbps, while the middle-of-the-road one offers both 10- and 100Mbps auto-sensing ports. The higher-end hubs offer network-management port and console connections. If you are going to spend enough to buy a high-end hub, you should consider just buying a switch. Figure 1.20 shows the different hub products Cisco offers. Any of these hubs can be stacked together to give you more port density.

These are the selection issues you need to know:

- Business requirements for 10- or 100Mbps
- Port density
- Management
- Ease of operation

FIGURE 1.20 Cisco hub products



Cisco Routers

When you think of Cisco, what do you think of first? Hubs? I don't think so. You think of routers, of course. Cisco makes the best routers in the world. Everyone knows this, and it is also one of the reasons you are even reading this book.

It seems as though Cisco comes out with a new router almost every month. It is hard to keep up with their new offerings. A key criterion when selecting router products is knowing what feature sets you need to meet your business requirements. For example, do you need IP, Frame Relay, and VPN support? How about IPX, AppleTalk, and DECnet? Cisco has it all.

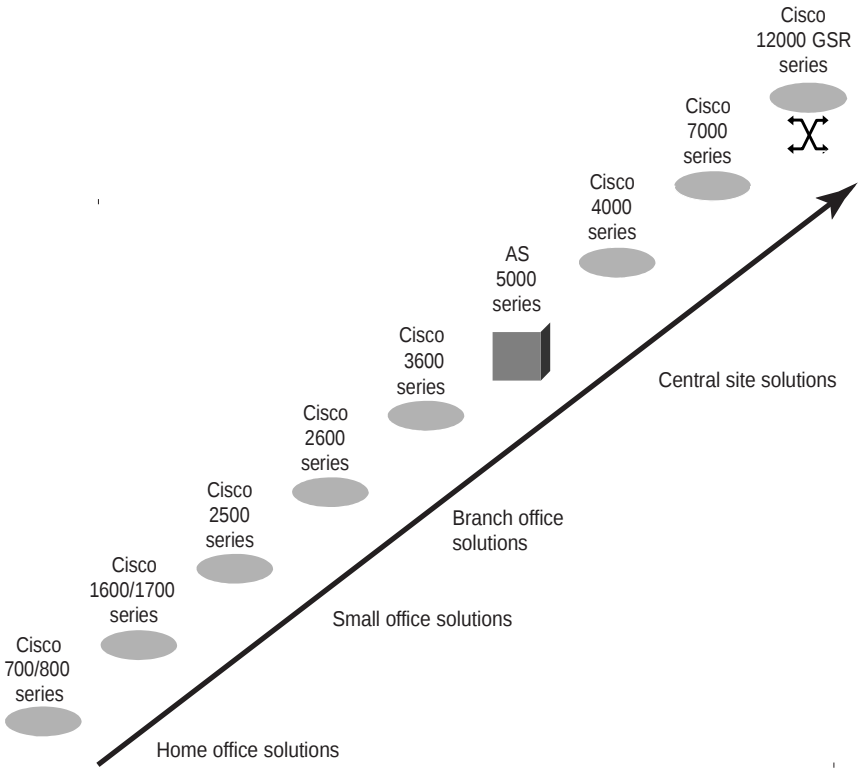
The other features you need to think about when considering different product-selection criteria are port density and interface speeds. As you get into the higher-end models, you see more ports and faster speeds. For example, the new 12000 series model is Cisco's first gigabit switch and has enormous capability and functionality.

You can tell how much a product is going to cost by looking at the model number. A stripped-down 12000 series switch with no cards or power sup- plies starts at about $12,000. The price can end up at well over $100,000 for a loaded system. Seems like a loaded 12000 series system would be great for my little home network.

You also need to think about WAN support when buying a router. You can get anything you want in a Cisco router, but you just have to be familiar with the service provided for your area.

Figure 1.21 shows some of the router products Cisco sells.

FIGURE 1.21 Cisco router products



The Cisco 800 series router has mostly replaced the Cisco 700 series because the 700 series does not run the Cisco IOS. In fact, I hope Cisco will soon stop selling the 700 series routers altogether. They are difficult to con- figure and maintain.

The main selections involved in choosing Cisco routers are listed below:

- Scale of routing features needed
- Port density and variety requirements
- Capacity and performance
- Common user interface

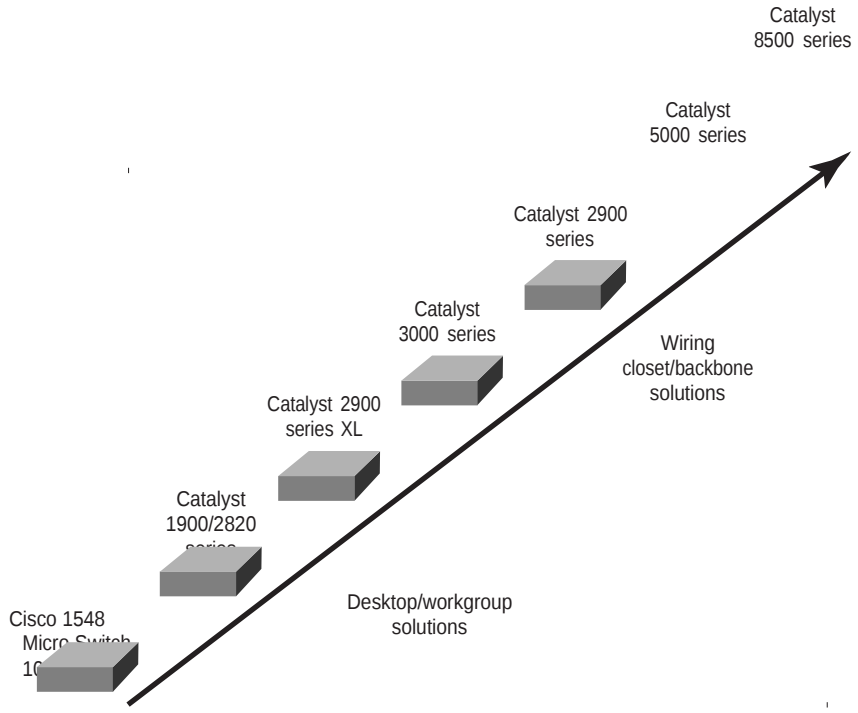
Cisco Switches

It seems like switch prices are dropping almost daily. I just received an e.mail from Cisco announcing that the Catalyst 2900 series switches have dropped in price 30 percent. About four years ago a 12-port 10/100 switch card for the Catalyst 5000 series switch was about $15,000. Now you can buy a complete Catalyst 5000 with a 10/100 card and supervisor module for about $7500 or so. My point is that with switch prices becoming rea- sonable, it is now easier to install switches in your network. Why buy hubs when you can use switches? I think every closet should have at least one switch.

Cisco has a huge assortment of switches to meet absolutely every busi- ness need. You must consider whether you need 10/100 or 1000Mbps for each desktop or to connect between switches. ATM (asynchronous trans- fer mode) is also a consideration; however, with Gigabit Ethernet out and 10Gbps links just around the corner, who needs ATM? The next criteria to consider are port density. The lower-end models start at 12 ports, and the higher-end models can provide hundreds of switched ports per switch.

Figure 1.22 shows the Cisco-switch product line.

FIGURE 1.22 Cisco Catalyst switch products



The selection issues you need to know when choosing a Cisco switch are listed below:

- Business requirements for 10,100 or even 1000Mbps
- Need for trunking and interswitch links
- Workgroup segmentation (VLANs)
- Port density needs
- Different user interfaces

Summary

This chapter began with a discussion of the OSI model, which is a seven-layer model used to help application developers design applications that can run on any type of system or network. I provided complete details of each layer and discussed how Cisco views the specifications of the model

Different types of devices are specified at each of the OSI model's layers. This chapter discussed the different types of devices, cables, and connectors used at each layer.

Also, I provided an introduction to the Cisco hierarchical network model, which was created to help administrators design and understand hierarchical networks. By using the Cisco three-layer model, you can effectively design, implement, and maintain any size network.

Cisco makes a large range of router, hub, and switch products. I discussed the different products Cisco creates and sells so that you can make more informed decisions when building your internetwork.

Key Terms

Before taking the exam, be sure you're familiar with the following terms.

access layer

Application layer

Application-Specific Integrated Circuits (ASICs)

Basic Rate Interface (BRI)

bridges

broadcast domain

buffer

Carrier Sense Multiple Access with Collision Detect (CSMA/CD)

Channel Service Unit/Data Service Unit (CSU/DSU)

core layer

Data Communication Equipment (DCE)

data frame

Data Link layer

Data Terminal Equipment (DTE)

distribution layer

encapsulation

Ethernet

flow control