

Cisco Academy Semester 2

1.1 The OSI Reference Model and the Problems it Solves

1.1.1 The layered network model: The OSI reference model

Network models use layers to simplify the networking functions. The separation of networking functions is called layering. To understand the importance of layering, let's consider the OSI reference model, a layered model for understanding and implementing computer communications. By using layers, the OSI reference model simplifies the tasks required for two computers to communicate with each other.

Each layer can be focused on specific functions, thereby allowing the networking designer to choose the right networking devices and functions for the layer. In the OSI reference model, each of the seven numbered layers indicates a distinct function. The reasons for this division of network functions include the following:

- Layers divide the aspects of network operation into less complex elements.
- Layers define standard interfaces for plug-and-play compatibility.
- Layers enable engineers to specialize design and development efforts on modular functions.
- Layers promote symmetry in the different network modular functions so that they work together.
- Layers prevent changes in one area from affecting other areas, so each area can evolve more quickly.
- Layers divide the complexity of networking into separate, easy to learn operations.

1.1.2 The OSI model layers

Each layer of the OSI reference model serves a specific function:

- Application layer (Layer 7) -This layer provides network services to user applications. For example, a word processing application is serviced by file transfer services at this layer.
- Presentation layer (Layer 6) -This layer provides data representation and code formatting, along with the negotiation of data transfer syntax. It ensures that the data that arrives from the network can be used by the application, and it ensures that information sent by the application can be transmitted on the network.
- Session layer (Layer 5) -This layer establishes, maintains, and manages sessions between applications.
- Transport layer (Layer 4) -This layer segments and reassembles data into a data stream. The transport layer has the potential to guarantee a connection and offer reliable transport.
- Network layer (Layer 3) -This layer determines the best way to move data from one place to another. The router operates at this layer. This layer uses logical addressing schemes that can be managed by an administrator. This layer uses the Internet Protocol (IP) addressing scheme, along with Apple-Talk, DECnet, VINES, and IPX addressing schemes.
- Data link layer (Layer 2) -This layer provides physical transmission across the medium. It handles error notification, network topology, and flow control. This layer uses Media Access Control (MAC) addresses, which also are referred to as physical or hardware addresses.
- Physical layer (Layer 1) -This layer provides the electrical, mechanical, procedural, and functional means for activating and maintaining the physical link between systems. This layer uses such physical media as twisted-pair, coaxial, and fiber-optic cable.

Cisco Academy Semester 2

1.1.3 Peer-to-peer communications

The OSI reference model describes how information makes its way from application programs on different computers through a network medium. As the information to be sent descends through the layers of a given system, it looks less and less like a human language and more and more like the ones and zeros that a computer understands. Each layer uses its own layer protocol to communicate with its peer layer in the other system. Each layer's protocol exchanges information, called protocol data units (PDUs), between peer layers. The figure shows an example of OSI-type communication. Host A has information to send to Host B. The application program in Host A communicates with Host A's application layer, which communicates with Host A's presentation layer, which communicates with Host A's session layer, and so on, until Host A's physical layer is reached. The physical layer puts information on (and takes information off) the physical network medium. After the information traverses the physical network medium and is picked up by Host B, it ascends through Host B's layers in reverse order (first the physical layer, then the data link layer, and so on) until it finally reaches Host B's application layer.

Although each Host A layer communicates with its adjacent layers, each layer in a host has a primary task it must perform. The primary task of each layer is to communicate with its peer layer in Host B. That is, the task of Layer 1 in Host A is to communicate with Layer 1 in Host B; Layer 2 in Host A communicates with Layer 2 in Host B, and so on.

The OSI reference model's layering prohibits direct communication between peer layers in different hosts. Each layer in Host A must therefore rely on services provided by adjacent Host A layers to help achieve communication with its Host B peer. Assume that Layer 4 in Host A must communicate with Layer 4 in Host B. To do this, Layer 4 in Host A must use the services of Layer 3 in Host A. Layer 4 is said to be the service user, and Layer 3 is the service provider. Layer 3 services are provided to Layer 4 at a service access point (SAP), which is a location at which Layer 4 can request Layer 3 services.

Thus, the TCP segments become part of the network layer packets (also called datagrams) exchanged between IP peers. In turn, the IP packets must become part of the data link frames exchanged between directly connected devices. Ultimately, these frames must become bits as the data is finally transmitted by the physical-layer protocol using hardware.

1.1.4 Encapsulation

How does Layer 4 in Host B know what Layer 4 in Host A wants? Layer 4's specific requests are stored as control information, which is passed between peer layers in a header block that is attached to the actual application information. Each layer depends on the service function of the OSI reference model layer below it. To provide this service, the lower layer uses encapsulation to put the PDU from the upper layer into its data field; then, it can add whatever headers and trailers the layer will use to perform its function.

The concept of a header and data is relative, depending on the layer currently analyzing the information unit. For example, to Layer 3, an information unit consists of a Layer 3 header and the data that follows. Layer 3's data, however, can potentially contain headers from Layers 4, 5, 6, and 7. Further, Layer 3's header is simply data to Layer 2. This concept is illustrated in the Figure. Finally, not all layers need to append headers. Some layers simply perform a transformation on the actual data they receive to make the data readable to their adjacent layers.

For example, the network layer provides a service to the transport layer, and the transport layer presents data to the network layer. The network layer then encapsulates the data within a header. This header contains information required to complete the transfer, such as source and destination logical addresses. The data link layer, in turn, provides a service to the network layer encapsulating

Cisco Academy Semester 2

the network layer information in a frame. The frame header contains information required to complete the data link functions. For example, the frame header contains physical addresses. The physical layer also provides a service to the data link layer by encoding the data link frame into a pattern of ones and zeros for transmission on the medium. For example, let's assume that Host A wants to send the following e-mail to Host B:

The small gray cat ran up the wall to try to catch the red bird.

Five conversion steps occur during data encapsulation, which enables the transmission of the e-mail to the appropriate destination:

Step 1

As a user sends an e-mail message, its alphanumeric characters are converted to data, starting at Layer 7 down through Layer 5, and are sent over the network.

Step 2

By using segments at Layer 4, the transport function packages data for the network transport and ensures that the message hosts at both ends of the e-mail system can reliably communicate.

Step 3

The data is placed into a packet (or datagram) at Layer 3 that contains a network header with source and destination logical addresses. Then, the network devices send the packets across the network along a chosen path.

Step 4

Each network device must put the packet into a frame at Layer 2. The frame allows connection to the next directly connected network device on the link. Each device in the chosen network path requires framing to connect to the next device.

Step 5

The frame must be converted into a pattern of ones and zeros for transmission on the medium (often copper wire or optical fiber) at Layer 1. A clocking function enables the devices to distinguish these bits as they traverse the medium. The medium on the physical network can vary along the path used. For example, the e-mail message can originate on a LAN, cross a campus backbone, and go out a WAN link until it reaches its destination on another remote LAN

1.2 The Physical Layer of the OSI Reference Model

1.2.1 Three categories of Ethernet

Together, Ethernet and IEEE 802.3 currently maintain the greatest share of any local-area network (LAN) protocol used. Today, the term Ethernet is often used to refer to all carrier sense multiple access collision detect (CSMA/CD) LANs that generally conform to Ethernet specifications, including IEEE 802.3.

When it was developed, Ethernet was designed to fill the middle ground between long-distance, low-speed networks and specialized, computer room networks carrying data at high speeds for very limited distances. Ethernet is good for applications where a local communication medium must carry sporadic, occasionally heavy traffic at high-peak data rates.

The term Ethernet refers to the family of LAN implementations that includes three principal categories:

Cisco Academy Semester 2

- Ethernet and IEEE 802.3-LAN specifications, which operate at 10 Mbps over coaxial and twisted-pair cable.
- 100-Mbps Ethernet--A single LAN specification, also known as Fast Ethernet, which operates at 100 Mbps over twisted-pair cable.
- 1000-Mbps Ethernet --A single LAN specification, also known as Gigabit Ethernet, which operates at 1000 Mbps (1 Gbps) over fiber and twisted-pair cables.

Ethernet has survived as an essential media technology because of its tremendous flexibility and because it is simple to implement and understand. Although other technologies have been promoted as likely replacements, network managers have turned to Ethernet and its derivatives as effective solutions for a range of campus implementation requirements. To resolve Ethernet's limitations, creative users (and standards organizations) have created bigger and bigger Ethernet pipes. Critics might dismiss Ethernet as a technology that cannot grow, but its underlying transmission scheme continues to be one of the principal means of transporting data for contemporary campus applications.

1.2.2 Three varieties of 10Mbps Ethernet

The Ethernet and IEEE 802.3 wiring standards define a bus topology LAN that operates at 10 Mbps. The Figure illustrates the three defined wiring standards:

- 10BASE2--Known as thin Ethernet, 10BASE2 allows network segments up to 185 meters on coaxial cable.
- 10BASE5--Known as thick Ethernet, 10BASE5 allows network segments up to 500 meters on coaxial cable.
- 10BASE-T--10BASE-T carries Ethernet frames on inexpensive twisted-pair wiring.

Ethernet and IEEE 802.3 wiring standards specify a bus topology network with a connecting cable between the end stations and the actual network medium. In the case of Ethernet, that cable is called a transceiver cable. The transceiver cable connects to a transceiver device attached to the physical network medium. The IEEE 802.3 configuration is much the same, except that the connecting cable is referred to as an attachment unit interface (AUI), and the transceiver is called a media attachment unit (MAU). In both cases, the connecting cable attaches to an interface board (or interface circuitry) within the end station.

Stations are attached to the segment by a cable that runs from an AUI in the station to an MAU that is directly attached to the Ethernet coaxial cable. Because the 10BASE-T standard provides access for a single station only, stations attached to an Ethernet LAN by 10BASE-T are almost always connected to a hub or a LAN switch.

1.3 The Data Link Layer of the OSI Reference Model

1.3.1 Lock analogy for NICs

Access to the networking media occurs at the data link layer of the OSI reference model. The data link layer, where the MAC address is located, is adjacent to the physical layer. No two MAC addresses are ever alike. Thus, on a network, the network interface card (NIC) is where a device connects to the medium, and each NIC has a unique MAC address.

Before each NIC leaves the factory, the hardware manufacturer assigns it a MAC address. This address is programmed into a chip on the NIC. Because the MAC address is located on the NIC, if a computer's NIC is replaced, the physical address of the station changes to that of the new NIC's MAC address. MAC addresses are written using a base 16 (hexadecimal) number system. There are two formats for MAC addresses: 0000.0c12.3456 and 00-00-0c-12-34-56.

Cisco Academy Semester 2

Imagine that you operate a motel. Room 207 has a lock called Lock A. Key A will open the door to Room 207. Room 410 has a lock called Lock F. Key F will open the door to Room 410. You decide to swap the locks on Rooms 207 and 410. After you switch the two locks, Key A opens the door of Room 410, and Key F opens the door to Room 207. In this analogy, the locks are like NICs. When the NICs are swapped, the matching keys also must be changed. In this analogy, the keys are like the MAC addresses.

On an Ethernet network, when one device wants to send data to another device, it can open a communication pathway to the other device by using its MAC address. When data is sent out on a network by a source, it carries the MAC address of its intended destination. As this data travels along the network media, the NIC in each device on the network checks to see if its MAC address matches the physical destination address carried by the frame. If no match is made, the NIC ignores the frame, and the frame continues along the network to the next station. However, when a match is made, the NIC makes a copy of the frame, which it places in the computer where it resides at the data link layer. Even though this copy has been made by the NIC and placed on the computer, the original frame continues along the network, where other NICs will be able to look at it to determine whether a match can be made.

1.3.2 Data transport across the physical link connecting hosts, routers, and other devices

The Ethernet and 802.3 data links provide data transport across the physical link joining two devices. For example, the three devices can be directly attached to each other over the Ethernet LAN. The Apple Macintosh on the left and the Intel-based PC in the middle show MAC addresses used by the data link layer. The router on the right also uses MAC addresses for each of its LAN-side interfaces.

1.4 Network Layer Functions

1.4.1 Layer 3 protocols of the TCP/IP stack

Several protocols operate at the OSI reference model network layer:

- IP provides connectionless, best-effort delivery routing of datagrams. It is not concerned with the content of the datagrams (packets); instead, it looks for a way to move the datagrams (packets) to their destinations.
- Internet Control Message Protocol (ICMP) provides control and messaging capabilities.
- Address Resolution Protocol (ARP) determines the data link layer addresses for known IP addresses.
- Reverse ARP (RARP) determines network addresses when data link layer addresses are known.

1.4.2 Network and subnetwork addresses in the IP

In a TCP/IP environment, end stations communicate with servers, hosts, or other end stations. This occurs because each node using the TCP/IP protocol suite has a unique 32-bit logical address, known as the IP address. In addition, within a TCP/IP environment, each network is seen as a single unique address. That address must be reached before an individual host within that network can be contacted.

Networks can be segmented into a series of smaller networks called subnetworks. Thus, an IP address is broken up into the network number, the subnetwork number, and the host number. Subnets use unique 32-bit subnet addresses that are created by borrowing bits from the host field. Subnet addresses are visible to other devices on the same network, but they are not visible to outside

Cisco Academy Semester 2

networks. Subnetworks are not visible to outside networks because the outside networks can only reference the subnet's whole network address.

With subnets, network address use is more efficient. There is no change to how the outside world sees the network, but within the organization, there is additional structure. In Figure network 172.16.0.0 is subdivided into four subnets: 172.16.1.0, 172.16.2.0, 172.16.3.0, and 172.16.4.0.

1.4.3 Path determination in the contexts of packets and routers

Path determination is the path traffic should take through the network cloud. Routers evaluate the best known path for traffic. Path determination occurs at Layer 3, the network layer. Routing services use network topology information when evaluating network paths. This information can be configured by the network administrator or collected through dynamic processes running in the network.

The network layer connects to networks and provides best-effort end-to-end packet delivery services to its user, the transport layer. The network layer sends packets from the source network to the destination network based on the IP routing table. After the router determines which path to use, it can proceed with switching the packet. Switching involves taking the packet the router accepted on one interface and forwarding it to another interface or port that reflects the best path to the packet's destination.

1.4.4 Why Layer 3 addresses must contain both path and host information

For path communication to be truly practical, a network must consistently represent the paths available between routers. Each line between the routers in Figure has a number that represents the subnetwork address that can be used by a routing process.

The network address contains both a path and a host portion. The path portion identifies a path part used by the router within the network cloud; the host portion identifies a specific device on the network. The router uses the network address to identify the source or destination network of a packet. Figure shows three network numbers coming from the router and three hosts sharing the network number 1. For some network layer protocols, a network administrator establishes this relationship by assigning network addresses ahead of time according to a network-addressing plan. For other network layer protocols, assigning addresses is partially or completely dynamic.

The consistency of Layer 3 addresses across the entire network also improves the use of bandwidth by preventing unnecessary broadcasts. Broadcasts cause unnecessary traffic and waste capacity on any devices or links that do not need to receive the broadcasts. By using consistent end-to-end addressing to represent the path of media connections, the network layer can find a path to the destination without unnecessary use of devices or links on the network

1.4.5 Types of ICMP messages

ICMP messages are carried in IP datagrams and are used to send error and control messages. ICMP uses the following types of defined messages; others exist, but are not included on this list:

- Destination unreachable
- Time exceeded
- Parameter problem
- Source quench
- Redirect
- Echo
- Echo reply

Cisco Academy Semester 2

- Timestamp
- Timestamp reply
- Information request
- Information reply
- Address request
- Address reply

1.4.6 ping command

Figure shows a router receiving a packet that it is unable to deliver to its ultimate destination; because of this the router sends an ICMP host unreachable message to the source. The message might be undeliverable because there is no known route to the destination. On the other hand, Figure shows an echo reply that is a successful reply to a `ping` command.

1.4.7 ARP

To communicate on an Ethernet network, the source station must know the destination station's IP and MAC addresses.

When the source has determined the IP address for the destination, the source's Internet Protocol looks into its ARP table to locate the MAC address for the destination. If the Internet Protocol locates a mapping of destination IP address to destination MAC address in its table, it binds the IP address with the MAC address and uses them to encapsulate the data. The data packet is then sent out over the networking media to be picked up by the destination.

If the MAC address is not known, the source must send out an ARP request. To determine a destination address for a datagram, the ARP table on the router is checked. If the address is not in the table, ARP sends a broadcast looking for the destination station. Every station on the network receives the broadcast.

The term local ARP is used when both the requesting host and the destination host share the same medium, or wire. Prior to issuing the ARP, the subnet mask was consulted. The mask determined that the nodes are on the same subnet.

1.5 Routing and the Different Classes of Routing Protocols

1.5.1 Routing in a mixed LAN-media environment

The network layer must relate to and interface with various lower layers. Routers must be capable of seamlessly handling packets encapsulated into different lower level frames without changing the packets' Layer 3 addressing. The figure shows an example of this using LAN-to-LAN routing. In this example, packet traffic from Host 4 on Ethernet Network 1 needs a path to Host 5 on Network 2.

When the router checks its routing table entries, it discovers that the best path to Network 2 uses outgoing Port To0, the interface to a Token Ring LAN. Although the lower layer framing must change as the router switches packet traffic from Ethernet on Network 1 to Token Ring on Network 2, the Layer 3 addressing for source and destination remains the same. The destination address remains Network 2, Host 5, despite the different lower layer encapsulations.

1.5.2 Two basic operations a router performs

Routers generally relay a packet from one data link to another. To relay a packet, a router uses two basic functions: a path determination function and a switching function. The figure illustrates how a router uses addressing for routing and switching functions.

Cisco Academy Semester 2

The switching function allows a router to accept a packet on one interface and forward it on a second interface. The path determination function enables the router to select the most appropriate interface for forwarding a packet. The node portion of the address refers to a specific port on the router that leads to an adjacent router in that direction.

When a host application needs to send a packet to a destination on a different network, a data link frame is received on one of a router's interfaces. The network - layer process examines the header to determine the destination network and then references the routing table that associates networks to outgoing interfaces. The original frame is stripped off and discarded. The packet is again encapsulated in the data link frame for the selected interface and stored in a queue for delivery to the next hop in the path.

This process occurs each time the packet switches through another router. At the router connected to the network containing the destination host, the packet is again encapsulated in the destination LAN's data link frame type and delivered to the destination host.

1.5.3 Static and dynamic routes

Static routing is administered manually. A network administrator enters route into the router's configuration. The administrator must manually update this static route entry whenever a network topology change requires an update. Static routing reduces overhead because routing updates are not sent (in the case of RIP, every 30 seconds).

Dynamic routing works differently. After the network administrator enters configuration commands to start dynamic routing, route knowledge is updated automatically by a routing process whenever new information is received from the network. Changes in dynamic knowledge are exchanged between routers as part of the update process.

Static routing has several useful applications. It allows a network administrator to specify what is to be advertised about restricted partitions. For security reasons, the administrator can hide parts of a network. Dynamic routing tends to reveal everything known about a network. Additionally, when a network is accessible by only one path, a static route to the network can be sufficient. This type of partition is called a stub network. Configuring static routing to a stub network avoids the overhead of dynamic routing because routing updates are not sent.

1.5.4 Default route

The Figure shows a use for a default route: a routing table entry that is used to direct packets for which the next hop is not explicitly listed in the routing table. In this example, Company X routers possess specific knowledge of the topology of the Company X network, but not of other networks. Maintaining knowledge of every other network accessible by way of the Internet cloud is unnecessary and unreasonable, if not impossible.

Instead of maintaining specific network knowledge, each router in Company X is informed by the default route that it can reach any unknown destination by directing the packet to the Internet.

1.5.5 Routed and routing protocols

Confusion often exists between the similar terms routed protocol and routing protocol:

- Routed protocol--Any network protocol that provides enough information in its network layer address to allow a packet to be forwarded from host to host based on the addressing scheme. Routed protocols define the format and use of the fields within a packet. Packets

Cisco Academy Semester 2

generally are conveyed from end system to end system. IP is an example of a routed protocol.

- Routing protocol--A protocol that supports a routed protocol by providing mechanisms for sharing routing information. Routing protocol messages move between the routers. A routing protocol allows the routers to communicate with other routers to update and maintain tables. TCP/IP examples of routing protocols are Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Enhanced Interior Gateway Routing Protocol (Enhanced IGRP), and Open Shortest Path First (OSPF) protocol.

1.5.6 Information that routers use to perform their basic functions

The success of dynamic routing depends on two basic router functions:

- Maintenance of a routing table
- Timely distribution of knowledge in the form of routing updates to other routers

Dynamic routing relies on a routing protocol to share knowledge. A routing protocol defines the set of rules used by a router when it communicates with neighboring routers. For example, a routing protocol describes:

- How updates are sent
- What knowledge is contained in these updates
- When to send this knowledge
- How to locate recipients of the updates

Exterior routing protocols are used to communicate between autonomous systems. Interior routing protocols are used within a single autonomous system.

1.5.7 IP routing protocols

At the network layer (Layer 3) of the OSI reference model, a router can use IP routing protocols to accomplish routing through the implementation of a specific routing protocol. Examples of IP routing protocols include:

- RIP-A distance-vector routing protocol
- IGRP-Cisco's distance-vector routing protocol
- OSPF-A link-state routing protocol
- EIGRP-A balanced-hybrid routing protocol

Most routing protocols can be classified as one of two basic types: distance vector or link state. The distance-vector routing protocol determines the direction (vector) and distance to any link in the network. The link-state routing protocol (also called the shortest path first [SPF] protocol) approach re-creates the exact topology of the entire network (or at least the partition in which the router is situated). A third type of protocol, the balanced-hybrid protocol, combines aspects of the link-state and distance-vector protocols.

1.5.8 Network convergence

Routing protocols, which are used to determine the best route for traffic from a particular source to a particular destination, are fundamental to dynamic routing. Whenever the topology of the network changes because of growth, reconfiguration, or failure, the network knowledge base also must

Cisco Academy Semester 2

change. The knowledge needs to reflect an accurate, consistent view of the new topology. This accurate, consistent view is called convergence.

When all routers in a network are operating with the same knowledge, the network is said to have converged. Fast convergence is a desirable network feature because it reduces the period of time that routers have outdated knowledge for making routing decisions that could be incorrect, wasteful, or both.

1.5.9 Distance vector routing

Distance-vector routing protocols pass periodic copies of a routing table from router to router. Each router receives a routing table from its direct neighbor. For example, Router B receives information from Router A. Router B adds a distance-vector number (such as a number of hops), increases the distance vector, and then passes the routing table to its other neighbor, Router C. This same step-by-step process occurs in all directions between direct-neighbor routers. In this way, the protocol accumulates network distances so it can maintain a database of network topology information. Distance-vector protocols do not allow a router to know the exact topology of a network.

1.5.10 Link-state routing

The second basic protocol used for routing is the link-state protocol. Link-state routing protocols maintain a complex database of topology information. Whereas the distance-vector protocol has nonspecific information about distant networks and no knowledge of distant routers, a link-state routing protocol maintains full knowledge of distant routers and how they interconnect.

Link-state routing uses link-state advertisements (LSAs), a topological database, the SPF protocol, the resulting SPF tree, and finally, a routing table of paths and ports to each network. Engineers have implemented this link-state concept in OSPF routing.

1.5.11 Distance vector and link state routing

You can compare distance-vector routing to link-state routing in several key areas:

- Distance-vector routing gets all topological data from the routing table information of its neighbors. Link-state routing obtains a complete view of the network topology by accumulating information from LSAs from both neighboring and distant routers.
- Distance-vector routing determines the best path by adding to the metric value it receives from tables moving from router to router. For link-state routing, each router works separately to calculate its own shortest path to destinations.
- With most distance-vector routing protocols, updates for topology changes come in periodic table updates. These tables pass from router to router, often resulting in slower convergence. With link-state routing protocols, updates usually are triggered by topology changes. Relatively small LSAs passed to all other routers usually result in faster time to converge on any network topology change.

Comparing Distance Vector Routing to Link-State Routing

Distance Vector	Link-State
Views net topology from neighbor's perspective	Gets common view of entire network topology
Adds distance vectors from router to router	Calculates the shortest path to other routers
Frequent, periodic updates: slow convergence	Event-triggered updates: faster convergence
Passes copies of routing table to neighbor routers	Pass link-state routing updates to other routers

Cisco Academy Semester 2

1.5.12 Enabling an IP routing process

The selection of IP as a routed protocol involves the setting of global parameters. Global parameters include selecting a routing protocol, such as RIP or IGRP, and assigning IP network numbers without specifying subnet values.

IP Address Configuration

The `ip address` command to establish the logical network address of the interface. You use the term `ip netmask-format` command to specify the format of network masks for the current session. Format options are bit count, dotted-decimal (the default), and hexadecimal.

Dynamic Routing Configuration

When using dynamic routing, routers send periodic routing update messages to each other. Each time such a message is received and it contains new information, the router recalculates the new best route and sends new update information to other routers. By using router configuration commands, a router can adjust to changing network conditions.

The table on the left shows the router commands that start routing processes. This table shows which `network` command is required because it allows the routing process to determine which interfaces will participate in the sending and receiving of routing updates.

1.5.13 Configuring RIP

Key characteristics of RIP include the following:

It is a distance-vector routing protocol.

- Hop count is used as the metric for path selection.
- The maximum allowable hop count is 15.
- Routing updates are broadcast every 30 seconds by default.

The `router rip` command selects RIP as the routing protocol. The `network` command assigns an IP-based network address range of a segment that is directly connected. The routing process associates interfaces with the proper addresses and begins packet processing on the specified networks.

- `router rip`--Selects RIP as the routing protocol.
- `network 1.0.0.0`--Specifies a directly connected network.
- `network 2.0.0.0`--Specifies a directly connected network.

The Cisco A router interfaces connected to networks 1.0.0.0 and 2.0.0.0 will send and receive RIP updates.

1.6 The Transport Layer of the OSI Reference Model

1.6.1 "Reliable" transport

As the transport layer sends its data segments, it can ensure the integrity of the data. One method of doing this is called flow control. Flow control avoids the problem of a host overflowing the buffers in the destination host. Overflows can present serious problems because they can result in the loss of data. Transport-layer services also allow users to request reliable data transport between hosts and destinations. To obtain such reliable transport of data, a connection-oriented relationship is used between the communicating end systems. Reliable transport can accomplish the following:

Cisco Academy Semester 2

- Segment upper-layer applications
- Establish a connection
- Transfer data
- Provide reliability with windowing
- Use acknowledgment techniques

1.6.2 Layer 4 segmentation

One reason for using a layered network model is so that several applications can share the same transport connection. Transport functionality is accomplished segment by segment. This means that different applications can send data segments on a first-come, first-served basis. Such segments can be intended for the same destination or for many different destinations.

1.6.3 The three-way handshake

To establish a connection, one machine places a call that must be accepted by the other. Protocol software modules in the two operating systems communicate by sending messages across the network to verify that the transfer is authorized and that both sides are ready. After all synchronization has occurred, a connection is established, and the transfer of data begins. During transfer, the two machines continue to communicate with their protocol software to verify that data is received correctly.

The figure depicts a typical connection between sending and receiving systems. When you first meet someone, you often greet the person by shaking his or her hand, the act of shaking hands is understood by both parties as a signal for a friendly greeting. We speak of connections on the network in the same way. The first handshake, or greeting, requests synchronization. The second and third handshakes acknowledge the initial synchronization request, as well as synchronize connection parameters in the opposite direction. The final handshake segment is an acknowledgment used to inform the destination that both sides agree that a connection has been established. After the connection has been established, data transfer begins.

1.6.4 Why is a buffer used in data communications

When data transfer is in progress, congestion can arise for two different reasons. First, a high-speed computer might be able to generate traffic faster than a network can transfer it. Second, if many computers simultaneously need to send datagrams to a single destination, that destination can experience congestion, even though no single source caused the problem.

When datagrams arrive too quickly for a host or gateway to process, they are temporarily stored in memory. If the traffic continues, the host or gateway eventually exhausts its memory and must discard additional datagrams that arrive. Therefore an indicator acts like a stoplight and signals the sender to stop sending data. When the receiver can handle additional data, the receiver sends a "ready" transport indicator, which is like a "go" signal. When it receives this indicator, the sender can resume segment transmission.

1.6.5 Windowing

In the most basic form of reliable connection-oriented data transfer, data packets must be delivered to the recipient in the same order in which they were transmitted. The protocol fails if any data packets are lost, damaged, duplicated, or received in a different order. The basic solution is to have a recipient acknowledge the receipt of every data segment.

Cisco Academy Semester 2

If the sender has to wait for an acknowledgment after sending each segment, throughput is low. Because time is available after the sender finishes transmitting the data packet and before the sender finishes processing any received acknowledgment, the interval is used for transmitting more data. The number of data packets the sender is allowed to have outstanding without yet receiving an acknowledgment is known as the window.

Windowing is a method to control the amount of information transferred end-to-end. Some protocols measure information in terms of the number of packets; TCP/IP measures information in terms of the number of bytes.

1.6.6 Explain reliability via acknowledgment

Reliable delivery guarantees that a stream of data sent from one machine will be delivered through a data link to another machine without duplication or data loss. Positive acknowledgment with retransmission is one technique that guarantees reliable delivery of data streams. Positive acknowledgment requires a recipient to communicate with the source, sending back an acknowledgment message when it receives data. The sender keeps a record of each data packet it sends and waits for an acknowledgment before sending the next data packet. The sender also starts a timer when it sends a segment, and it retransmits a segment if the timer expires before an acknowledgment arrives.

The figure shows the sender transmitting Data Packets 1, 2, and 3. The receiver acknowledges receipt of the packets by requesting Packet 4. Upon receiving the acknowledgment, the sender sends Packets 4, 5, and 6. If Packet 5 does not arrive at the destination, the receiver acknowledges with a request to resend Segment 5. The sender resends Packet 5 and must receive an acknowledgment to continue with the transmission of Packet 7.

Chapter Summary

Now that you have completed this chapter, you should have a firm understanding of the following:

- By using layers, the OSI reference model simplifies the task required for two computers to communicate.
- Each layer's protocol exchanges information, called PDUs, between peer layers.
- Each layer depends on the service function of the OSI reference model layer below it. The lower layer uses encapsulation to put the PDU from the upper layer into its data field; then, it can add whatever headers and trailers the layer will use to perform its function.
- The term *Ethernet* is often used to refer to all CSMA/CD LANs that generally conform to Ethernet specifications, including IEEE 802.3.
- The Ethernet and 802.3 data links provide data transport across the physical link that joins two devices.
- IP provides connectionless, best-effort delivery routing of datagrams. It is not concerned with the content of the datagrams, but it looks for a way to move the datagrams to their destination.
- ICMP messages are carried in IP datagrams and are used to send error and control messages.
- ARP is used to map a known IP address to a MAC sublayer address to allow communication on a multiaccess medium, such as Ethernet.
- The switching function allows a router to accept a packet on one interface and forward it on a second interface.
- Routed protocols are network protocols that provide enough information in the network layer address to allow a packet to be forwarded from host to host based on the addressing scheme.

Cisco Academy Semester 2

- Routing protocol supports routed protocols by providing mechanisms for sharing routing information. Routing protocol messages move between the routers.
- Most routing protocols can be classified into one of two basic protocols: distance-vector or link-state.
- Routers must be capable of seamlessly handling packets encapsulated into different lower-level frames without changing the packets' Layer 3 addressing.
- Examples of IP routing protocols include RIP, IGRP, OSPF, and EIGRP.
- Transport -layer services allow users to request reliable data transport between hosts and destinations.