Business Data Communications & Networking:

12th Edition

Chapter 5: Transport and Network Layer

Sadiq M. Sait, PhD
Professor
College of Computer Sciences and Engineering
Director, Office of Planning & Quality

November 2023

NETWORK AND TRANSPORT LAYER

- The network layer and transport layer are responsible for moving messages from **end to end** in a network.
- They are closely tied together and are usually discussed together.
- **The transport layer (layer 4) performs three functions:**
  - linking the application layer to the network,
  - segmenting (breaking long messages into smaller packets for transmission), and
  - session management (establishing an end-to-end connection between the sender and receiver).
- The network layer (layer 3) performs two functions:
  - routing and
  - addressing (finding the address of that next computer).
  - Only one protocol is in widespread use today: Transmission Control Protocol/Internet Protocol (**TCP/IP**), the protocol used on the Internet.

Introduction

- ❑ The transport layer links the application software in the application layer with the network and is responsible for the end-to-end delivery of the message.
- ❑ The transport layer accepts outgoing messages from the application layer (e.g., Web, email, and so on) and **segments** them for transmission.
- ❑ Figure 5-1 shows the application layer software producing an SMTP packet that is **split into two smaller** TCP segments by the transport layer.
- ❑ The Protocol Data Unit (PDU) at the transport layer is called a **segment**.
- ❑ The network layer takes the messages from the transport layer and routes them through the network by selecting the best path from computer to computer through the network (and adds an IP packet).
- ❑ The data link layer adds an Ethernet frame and instructs the physical layer hardware when to transmit.
- ❑ Each layer in the network has its own set of protocols that are used to hold the data generated by higher layers, much like a set of matryoshka (nested Russian dolls).

Introduction

- The network and transport layers also accept incoming messages from the data link layer and organize them into coherent messages that are passed to the application layer.
- For example, as in Figure 5-1, a large email message might require several data link layer frames to transmit.
    - the **transport** layer at the sender would ***break*** the message into several smaller segments and give them to
    - the **network layer** to **route**, which in turn gives them to
    - the **data link** layer to **transmit**.
- The network layer at the receiver would
    - receive the individual packets from the data link layer,
    - process them, and pass them to the transport layer, which would reassemble them into one email message
    - before giving it to the application layer.

Introduction

- The network and transport layers also accept incoming messages from the data link layer and organize them into coherent messages that are passed to the application layer.
- For example, as in Figure 5-1, a large email message might require several data link layer frames to transmit.
  - the **transport** layer at the sender would ***break*** the message into several smaller segments and give them to
  - the **network layer** to **route**, which in turn gives them to
  - the **data link** layer to **transmit**.
- The network layer at the receiver would
  - receive the individual packets from the data link layer,
  - process them, and pass them to the transport layer, which would reassemble them into one email message
  - before giving it to the application layer.

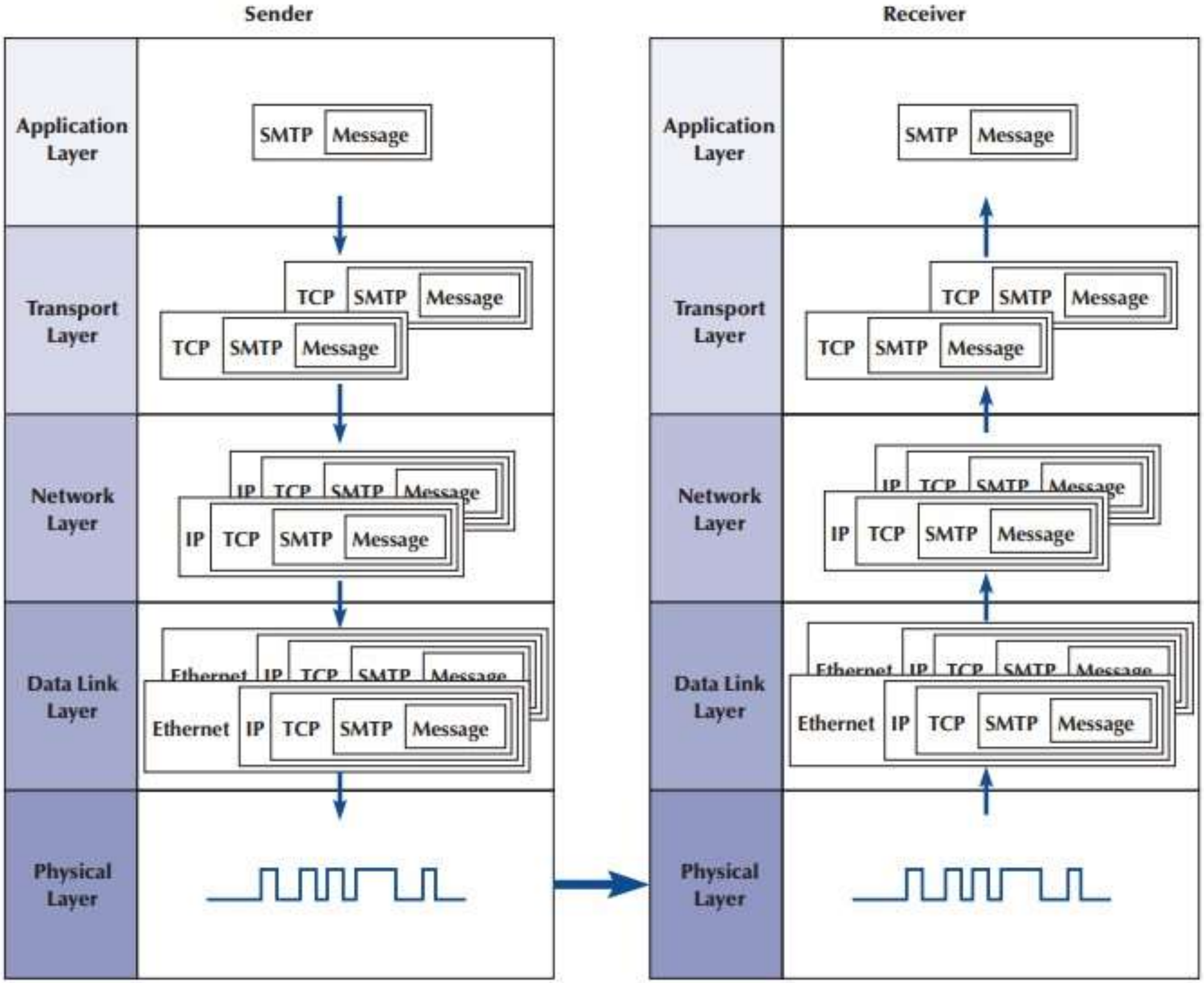


FIGURE 5-1 Message transmission using layers. HTTP = Hypertext Transfer Protocol; IP = Internet Protocol; TCP = Transmission Control Protocol

5.2.1 TCP Protocol

- A typical TCP segment has a 192-bit header (24 bytes) of control information (Figure 5-2).
- Among other fields, it contains
  - the source and destination port identifier. The destination port tells the TCP software the destination to which application layer program the application layer packet should be sent, whereas the source port tells the receiver which application layer program the packet is from.
  - The TCP segment also provides **a sequence number** so that the TCP software at the destination can **assemble** the segments into the correct order and make sure that no segments have been lost.
  - The options field is optional and rarely used. Therefore this results in a 20-byte-long TCP header.
  - The header **length** field is used to tell the receiver how long the TCP packet is—that is, whether the options field is included.

5.2.1 TCP Protocol (contd)

- ❑ TCP/IP has a second type of transport layer protocol called **User Datagram Protocol** (UDP).
- ❑ UDP PDUs are called datagrams.
- ❑ UDP is used when the sender needs to send a single small packet to the receiver (e.g., for a DNS request, which we discuss later in this chapter).
- ❑ When there is only one small packet to be sent, the transport layer doesn’t need to worry about segmenting the outgoing messages or reassembling them upon receipt, so transmission can be faster.
- ❑ A UDP datagram has only four fields (8 bytes of overhead) plus the application layer packet: source port, destination port, length, and a CRC-16.
- ❑ Unlike TCP, UDP does not check for lost messages, so occasionally a UDP datagram is lost, and the message must be resent.
- ❑ Interestingly, it is not the transport layer that decides whether TCP or UDP is going to be used. This decision is left to the engineer who is writing the application.

5.2.2 IP--- Internet Protocol

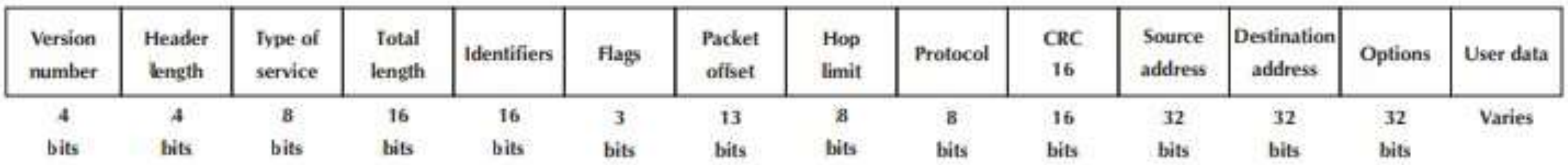
- This is a Network Layer Protocol
- Network layer PDUs are called packets.
- Two forms of IP are currently in use.
- The older form is IP version 4 (IPv4), which also has a 192-bit header (24 bytes) (Figure 5-3).
    - This header contains **source** and **destination** addresses, **packet length**, and **packet number**. Similar to the TCP header, the **options field is rarely used**, and therefore the header is usually 20 bytes long.
- IP version 4 is being replaced by IPv6
    - This has a 320-bit header (40 bytes) (Figure 5-4).
    - The primary reason for the increase in the packet size is an increase in the address size from 32 bits to 128 bits.
    - IPv6's simpler packet structure makes it easier to perform routing and supports a variety of new approaches to addressing and routing.

5.2.2 IPv6--- Internet Protocol

- Development of the IPv6 came about because IP addresses were being depleted on the Internet.
- IPv4 has a 4-byte address field, which means there is a theoretical maximum of about 4.294 billion addresses.
- However, about 500 million of these addresses are reserved and cannot be used, and the way addresses were assigned in the early days of the Internet means that a small number of companies received several million addresses, even when they didn’t need all of them.
- With the increased growth in Internet users, and the explosion in mobile Internet devices, we ran out of IPv4 addresses in 2011.
- Internet Protocol version 6 uses a 16-byte-long address which provides a theoretical maximum of 3.4^{1038} addresses—more than enough for the foreseeable future.
- Addresses are eight sets of 2-byte numbers (e.g., 2001:0890:0600:00d1:0000:0000:abcd:f010), but because this can be long to write, there is a IPv6 “compressed notation” that eliminates the leading zeros within each block and blocks that are all zeros.
- So the preceding IPv6 address could also be written as 2001:890:600:d1: :abcd:f010.

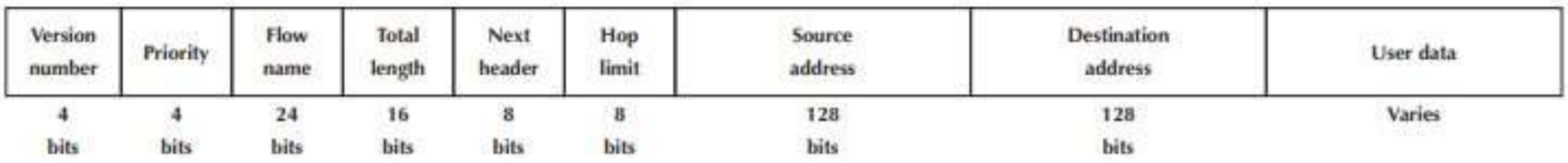
5.2.2 IPv6--- Internet Protocol

- ❑ The size of the message field depends on the data link layer protocol used.
- ❑ TCP/IP is commonly combined with Ethernet.
- ❑ Ethernet has a maximum packet size of 1,492 bytes, so the maximum size of a TCP message field if IPv4 is used is 1,492 − 24 (the size of the TCP header) − 24 (the size of the IPv4 header) = 1,444.



Version number	Header length	Type of service	Total length	Identifiers	Flags	Packet offset	Hop limit	Protocol	CRC 16	Source address	Destination address	Options	User data
4 bits	4 bits	8 bits	16 bits	16 bits	3 bits	13 bits	8 bits	8 bits	16 bits	32 bits	32 bits	32 bits	Varies

FIGURE 5-3 Internet Protocol (IP) packet (version 4). CRC = cyclical redundancy check



Version number	Priority	Flow name	Total length	Next header	Hop limit	Source address	Destination address	User data
4 bits	4 bits	24 bits	16 bits	8 bits	8 bits	128 bits	128 bits	Varies

FIGURE 5-4 Internet Protocol (IP) packet (version 6)

5.3 TRANSPORT LAYER FUNCTIONS

- The transport layer:
  - Links the application software in the application layer with the network and
  - Is responsible for segmenting large messages into smaller ones for transmission and
  - For managing the session (the end-to-end delivery of the message).
  - One of the first issues facing the application layer is to find the numeric network address of the destination computer.
    - Different protocols use different methods to find this address.
    - Depending on the protocol ——finding the destination address can be classified as a transport layer function, a network layer function, a data link layer function, or an application layer function with help from the operating system.
  - The three unique functions performed by the transport layer are:
    - linking the application layer to the network layer
    - segmenting, and
    - session management

5.3.1 Linking to The Application Layer

- Users use many applications at the same time (Browsing, FTP, mail, etc).
- Likewise many servers act as web servers
- When the transport layer receives an incoming message, it must decide to which application program it should be delivered.
- With TCP/IP each application layer software has a unique **port address**.
- Any message sent to a computer must tell TCP (the transport layer software) the application layer port address that is to receive the message.
- Therefore, when an application layer program generates an outgoing message, it tells the TCP software its own port address (i.e., the source port address) and the port address at the destination computer (i.e., the destination port address).
- These two port addresses are placed in the first two fields in the TCP segment (see Figure 5-2).
- On the Internet, all port addresses for popular services such as the Web, email, and FTP have been standardized (**Web server port address is 80, which is called the well-known port. Web browsers, therefore, automatically generate a port address of 80 for any Web page you click on. FTP servers use port 21, SMTP 25, and so on**)

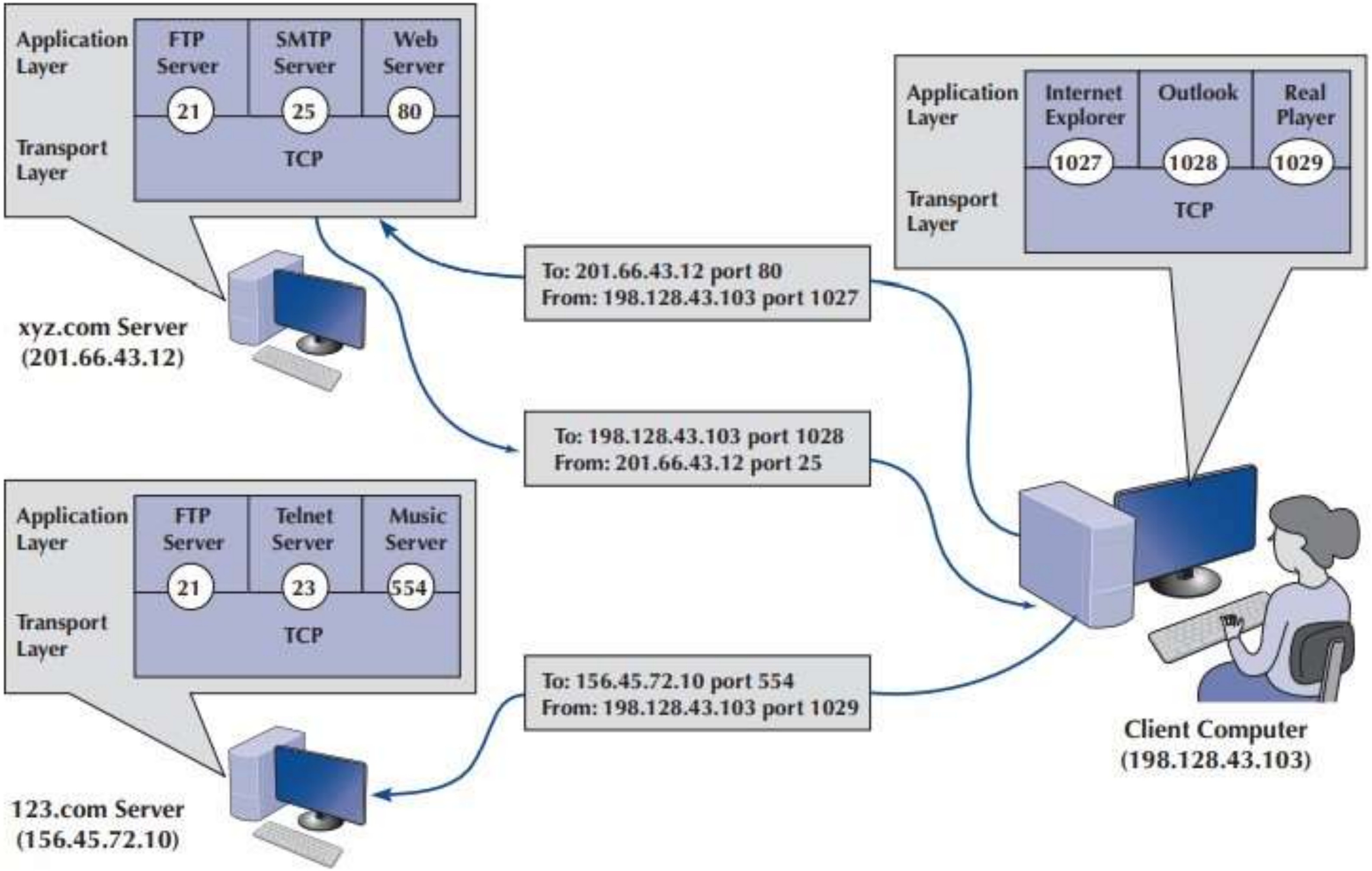


FIGURE 5-5 Linking to application layer services

5.3.1 Linking to The Application Layer (contd)

- ❑ Figure 5-5 shows a user running three applications on the client (Internet Explorer, Outlook, and RealPlayer), **each of which has been assigned a different port number**, called a **temporary** port number (1027, 1028, and 7070, respectively).
- ❑ Each of these can simultaneously send and receive data to and from different servers and different applications on the same server.
- ❑ In this case, we see a message sent by Internet Explorer on the client (port 1027) to the Web server software on the xyz.com server (port 80).
- ❑ We also see a message sent by the mail server software on port 25 to the email client on port 1028.
- ❑ At the same time, the RealPlayer software on the client is sending a request to the music server software (port 554) at 123.com

5.3.2 Segmenting

- The data link layer can transmit only messages of certain lengths.
- It is therefore up to the sender’s transport layer to break into segments.
- The receiver’s transport layer must receive **(from where? The Network Layer)** and recombine the segments.
- Depending on what the application layer software chooses, the incoming packets can either be delivered
  - one at a time (web browsers, as they arrive)
  - or held until all packets have arrived and the message is complete (email)
- The TCP is also responsible for ensuring that the receiver has actually received all segments that have been sent. TCP, therefore, uses continuous ARQ (see Chapter 4).
- The challenge at the transport layer is deciding the segment size.
  - When transport layer software is set up, it is told what size segments it should use to make the best use of its own data link layer protocols (or it chooses the default size of 536).
  - The transport layer at the sender negotiates with the transport layer at the receiver to settle on the best segment sizes to use. This negotiation is done by establishing a TCP connection between the sender and receiver.

5.3.3 Session Management

- A session can be thought of as a conversation between two computers.
- The sender transmits the segments in sequence until the conversation is done, and then the sender ends the session.
- This approach to session management is called
  - connection-oriented messaging.
  - connectionless messaging is when the sender only wants to send one short information message or a request. (In this case, the sender may choose not to start a session but just send one quick message and move on).

5.3.3 Connection-Oriented Messaging

- Here, to establish a connection, the transport layer on both the sender (client) and the receiver (server) must send a SYN and receive a ACK segment.
- This process starts with
  - The sender sending a SYN to the receiver
  - The server responds with an ACK for the sender's/client's SYN
  - And then sends its own SYN.
- SYN is usually a randomly generated number that identifies a packet.
- The last step is when the client sends an ACK for the server's SYN.
- This is called the three-way handshake, and this process also contains the segment size negotiation.
- Once the connection is established, the segments flow using the continuous ARQ (sliding window) technique 4 to make sure that all segments arrive and also to provide flow control.
- When the transmission is complete, the session is terminated using a four-way handshake.
- Because TCP/IP connection is a full-duplex connection, each side of the session has to terminate the connection independently.
  - The sender will start by sending with a FIN to the receiver (i.e., the server) that is finished sending data, and the server sends an ACK.
  - Then the server sends a FIN to the client. The connection is successfully terminated when the server receives the ACK for its FIN

5.3.3 Connectionless Messaging

- ❑ Here, each packet is treated separately and makes its own way through the network.
- ❑ No connection is established.
- ❑ The sender simply sends the packets as separate, unrelated entities, and it is possible that different packets will take different routes through the network.
- ❑ Packets may arrive out of sequence at their destination.
- ❑ The sender’s network layer, therefore, puts a sequence number on each packet, in addition to information about the message stream to which the packet belongs.
- ❑ The network layer must reassemble them in the correct order before passing the message to the application layer.
- ❑ TCP/IP can operate either as connection oriented or connectionless.
- ❑ When connection-oriented messaging is desired, TCP is used.

5.3.3 Connectionless Messaging ---- UDP

- When connectionless messaging is desired, the TCP segment is replaced with a User Datagram Protocol (UDP) packet.
- The UDP header is much smaller than the TCP header (only 8 bytes).
- Connectionless is most commonly used when the application data or message can fit into **one single message**.
- You might expect, for example, that because **HTTP requests are often very short**, they might use UDP connectionless rather than TCP connection-oriented messaging. **However, HTTP always uses TCP**.
- All of the application layer software we have discussed so far use TCP (HTTP, SMTP, FTP, Telnet).
- UDP is most commonly used for **control messages** such as
  - addressing (DHCP [Dynamic Host Configuration Protocol], discussed later),
  - routing control messages (RIP [Routing Information Protocol], discussed later), and
  - network management (SNMP [Simple Network Management Protocol], discussed in Chapter 12).

5.3.3 Quality of Service (QoS)t

- ❑ QoS routing is a special type of connection-oriented messaging in which different connections are assigned different priorities.
  - ❑ For example, videoconferencing requires fast delivery of packets to ensure that the images and voices appear smooth and continuous; they are very time dependent because delays in routing seriously affect the quality of the service provided.
  - ❑ Email packets, conversely, have no such requirements. Although everyone would like to receive email as fast as possible, a 10-second delay in transmitting an email message does not have the same consequences as a 10-second delay in a videoconferencing packet.
  - ❑ With QoS routing, different classes of service are defined, each with different priorities.
  - ❑ When the transport layer software attempts to establish a connection (i.e., a session), it specifies the class of service that connection requires.
  - ❑ Each path through the network is designed to support a different number and mix of service classes.
  - ❑ When a connection is established, the network ensures that no connections are established that exceed the maximum number of that class on a given circuit.

5.3.3 Quality of Service (QoS) (contd) t

- QoS routing is common in certain types of networks (e.g., ATM, Ch 8).
- The Internet provides several QoS protocols that can work in a TCP/IP environment.
  - Resource Reservation Protocol (**RSVP**) and Real-Time Streaming Protocol (**RTSP**) both permit application layer software to request connections that have certain minimum data transfer capabilities.
    - RTSP is geared toward audio/video streaming applications,
    - RSVP is more general purpose.
  - Both RSVP and RTSP, are used to create a connection (or session) and request a certain minimum guaranteed data rate.
  - Once the connection has been established, they use Real-Time Transport Protocol (**RTP**) to send packets across the connection.
  - **RTP contains information about the sending application, a packet sequence number, and a time stamp.**
  - RTP is combined with UDP. (**RTP does not provide source and destination port addresses.**)
  - This means that each real-time packet is first created using RTP and then surrounded by a UDP datagram, before being handed to the IP software at the network layer.

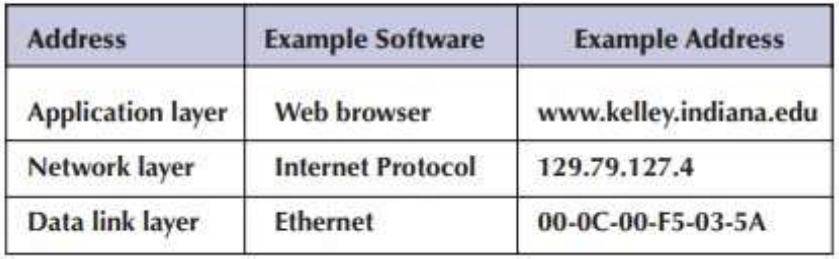
5.4 ADDRESSING t

- Before you can send a message, you must know the destination address.
- It is extremely important to understand that **each computer has several addresses**, **each used by a different layer.**
- **One address is used by the data link layer, another by the network layer, and still another by the application layer.**
  - www.indiana.edu is an application layer address (or a server name).
  - When request is passed on to the network layer software, it uses a network layer address.
  - The network layer protocol used on the Internet is IP, so this Web address (www.indiana.edu) is translated into an IP address (e.g., 129.79.127.4) (Figure 5-6).
  - This process is similar to using a phone book to go from someone’s name to his or her phone number.
  - The network layer then determines the best route through the network to the final destination.
  - **On the basis of this routing, the network layer identifies the data link layer address of the next computer to which the message should be sent.**
  - If the data link layer is running Ethernet, then the network layer IP address would be translated into an Ethernet address.

5.4 ADDRESSING (contd) t

- Ethernet addresses are 6 bytes in length, so a possible address might be 00-0F-00-81-14-00 (Ethernet addresses are usually expressed in hexadecimal) (Figure 5-6).
- Data link layer addresses are needed only on multipoint circuits that have more than one computer on them.
- For example, many WANs are built with point-to-point circuits that use PPP as the data link layer protocol.
- These networks do not have data link layer addresses

FIGURE 5-6
Types of addresses



Address	Example Software	Example Address
Application layer	Web browser	www.kelley.indiana.edu
Network layer	Internet Protocol	129.79.127.4
Data link layer	Ethernet	00-0C-00-F5-03-5A

5.4 ADDRESSING: MAC Address t

- ❑ This address is part of the hardware (e.g., Ethernet card) and can never be changed.
- ❑ Hardware manufacturers have an agreement that assigns each manufacturer a unique set of permitted addresses, so even if you buy hardware from different companies, it will never have the same address.
- ❑ Whenever you install a network card into a computer, it immediately has its own data link layer address that uniquely identifies it from every other computer in the world.
- ❑ Network layer addresses are generally assigned by software.
- ❑ Every network layer software package usually has a **configuration file** that specifies the network layer address for that computer. Network managers can assign any network layer addresses they want. It is important to ensure that every computer on the same network has a unique network layer address so that every network has a standards group that defines what network layer addresses can be used by each organization.
- ❑ Application layer addresses (or server names) are also assigned by a software configuration file.

5.4 ADDRESSING: MAC Address (contd) t

- ❑ Virtually all servers have an application layer address, but most client computers do not.
- ❑ As with network layer addresses, network managers can assign any application layer address they want, but a network standards group must approve application layer addresses **to ensure that no two computers have the same application layer address**.
- ❑ Network layer addresses and application layer addresses go hand in hand, **so the same standards group usually assigns both** (e.g., www.indiana.edu at the application layer means **129.79.78.4** at the NW layer.
- ❑ It is possible to have **several** application layer addresses for the same computer. For example, one of the Web servers in the Kelley School of Business at Indiana University is called both www.kelley.indiana.edu and www.kelley.iu.edu

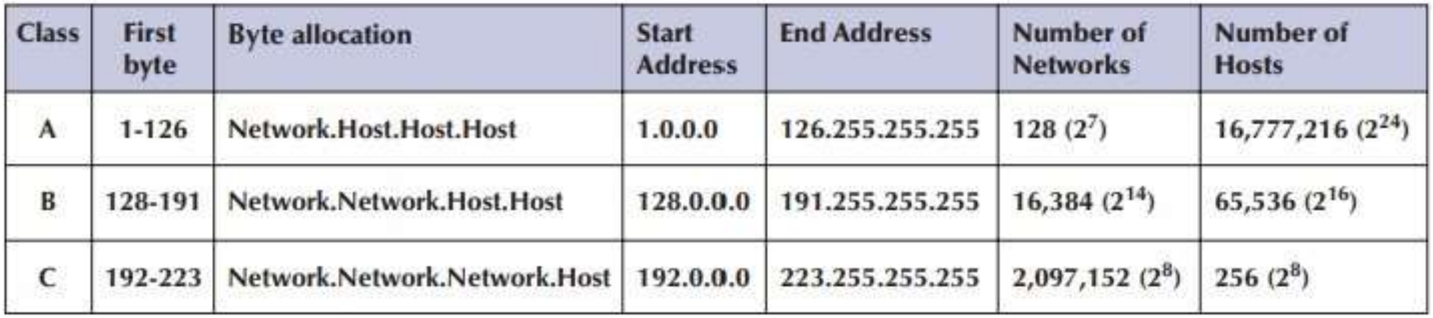
- ❑ **NOTE: All public IPs assigned to Routers of ISPs or Routers connecting to Internet are unique. but private IPs of two hosts can be the same if both are connected to different public networks. So the combination of public and private IP identifies your device uniquely.**

5.4 Internet Addresses t

- ❑ No one is permitted to operate unless he or she uses approved addresses.
- ❑ ICANN (Internet Corporation for Assigned Names and Numbers) is responsible for managing the assignment of IP addresses and application layer addresses (e.g., www.indiana.edu).
- ❑ ICANN sets the rules by which new domain names (e.g., .com, .org, .ca, .uk) are created and IP address numbers are assigned to users.
- ❑ Once authorized, a registrar can approve requests
- ❑ IP addresses are often assigned in groups, so that one organization receives a set of numerically similar addresses for use on its computers. For example, Indiana University has been assigned the set of application layer addresses that end in indiana.edu and iu.edu and the set of IP addresses in the 129.79.x.x range (i.e., all IP addresses that start with the numbers 129.79).
- ❑ Size of the Address Space? In general, if a protocol uses N bits to define an address, the available space is 2^{N}
- ❑ Specifically, IPv4 uses 32 bits (4 bytes) to define an address, and therefore the number of available addresses is 2^{32} = 4,294,967,296, or approximately 4.3 billion. These 4.3 billion addresses in the IPv4 address space are divided into Internet address classes.

5.4 Internet Address Classes

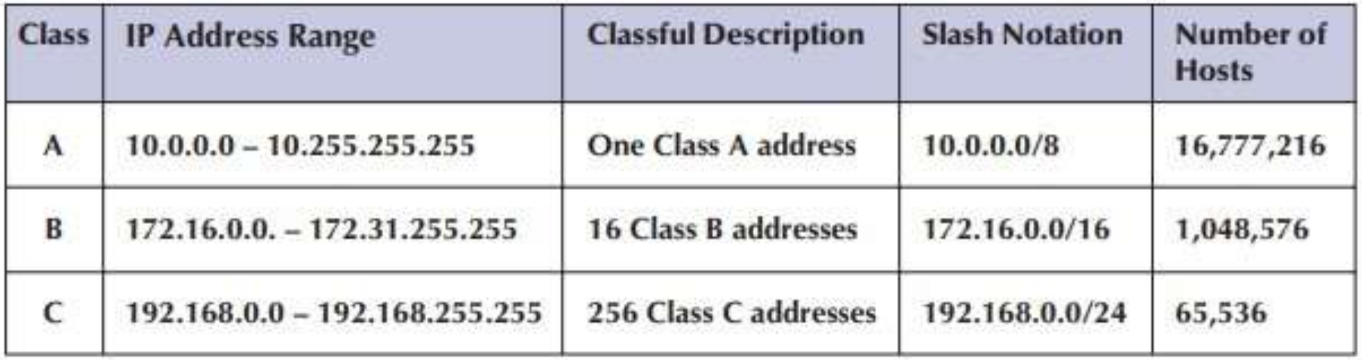
- There is an address ranges for each class (A, B or C) of addresses depending on the value of the first byte.
  - For example, Class A addresses can have any number between 1 and 126 in the first byte.
  - Figure 5-7 shows that there are some numbers in the first byte range that are not assigned to any address range.
  - An address starting with 0 is not allowed.
  - The 127 address range is reserved for a computer to communicate with itself and is called the loopback (used for testing software)
  - Addresses starting from 224 are reserved addresses that should not be used on IP networks.
  - Addresses from 224 to 239 belong to Class D and are reserved for multicasting, which is sending messages to a group of computers rather than to one computer (which is normal) or every computer on a network (called broadcast).
  - Addresses from 240 to 254 belong to Class E and are reserved for experimental use. Some companies use the Class E addresses for multicasting internal content in addition to the Class D addresses.
  - Addresses starting with 255 are reserved for broadcast messages



Class	First byte	Byte allocation	Start Address	End Address	Number of Networks	Number of Hosts
A	1-126	Network.Host.Host.Host	1.0.0.0	126.255.255.255	128 (2^7)	16,777,216 (2^{24})
B	128-191	Network.Network.Host.Host	128.0.0.0	191.255.255.255	16,384 (2^{14})	65,536 (2^{16})
C	192-223	Network.Network.Network.Host	192.0.0.0	223.255.255.255	2,097,152 (2^8)	256 (2^8)

FIGURE 5-7 IPv4 public address space

FIGURE 5-8
IPv4 private address space

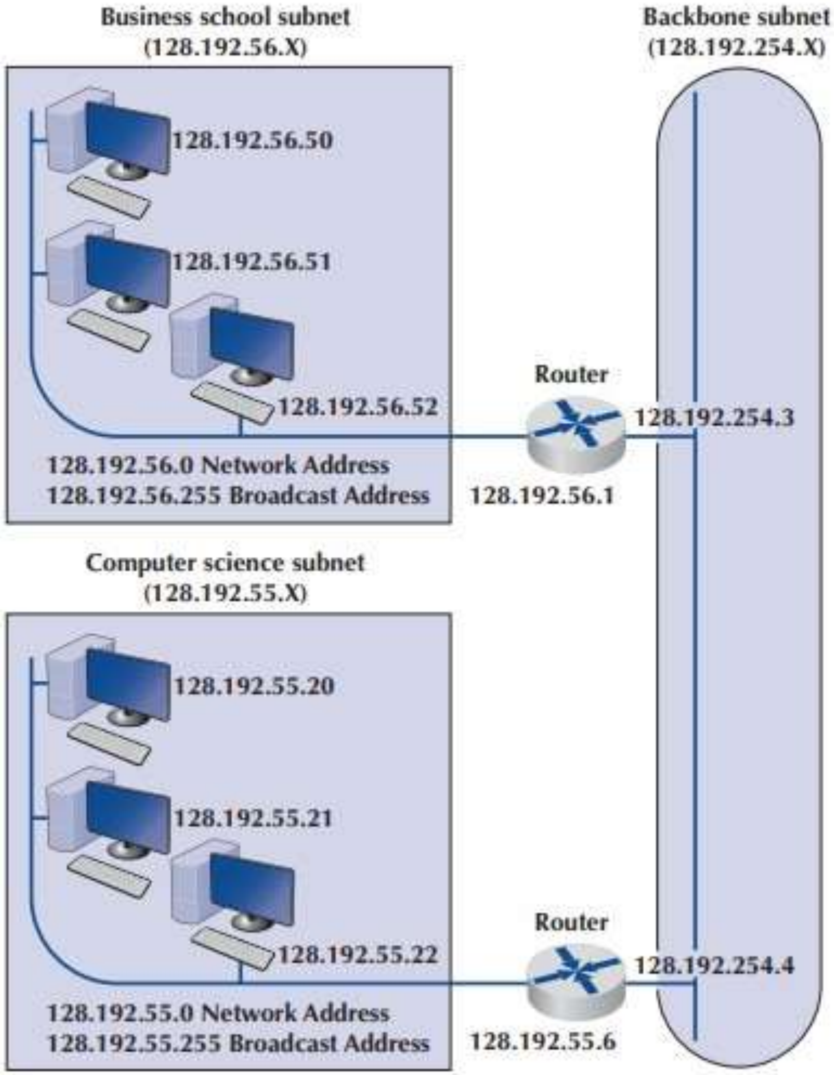


Class	IP Address Range	Classful Description	Slash Notation	Number of Hosts
A	10.0.0.0 – 10.255.255.255	One Class A address	10.0.0.0/8	16,777,216
B	172.16.0.0. – 172.31.255.255	16 Class B addresses	172.16.0.0/16	1,048,576
C	192.168.0.0 – 192.168.255.255	256 Class C addresses	192.168.0.0/24	65,536

5.4 Subnets t

- ❑ Subnetworks or subnets are designed on the network that subdivide the network into logical pieces.
- ❑ For example, suppose a university has just received a set of addresses starting with 128.192.x.x.
- ❑ One subnet ID for this LAN then is 128.192.56.
- ❑ Two addresses on this subnet cannot be assigned as IP address to any computer.
  - ❑ The first address is 128.192.56.0, and this is the network address.
  - ❑ The second address is 128.192.56.255, which is the broadcast address.
- ❑ Another LAN might be assigned 128.192.55.x, and likewise, all the other LANs at the university and the BN that connects them would have a different set of numbers.
- ❑ Routers connect two or more subnets so they have a separate address on each subnet. Without routers, the two subnets would not be able to communicate.
- ❑ The routers in Figure 5-9, for example, have **two** addresses each because they connect two subnets and must have one address in each subnet.
- ❑ Although it is customary to use the first 3 bytes of the IP address to indicate different subnets, it is not required.
- ❑ Any portion of the IP address can be designated as a subnet by using a subnet mask. Every computer in a TCP/IP network is given a **subnet mask.**
  - ❑ Every computer in a TCP/IP network is given a subnet mask to enable it to determine which computers are on the same subnet (i.e., LAN) that it is on and which computers are outside of its subnet

FIGURE 5-9
Address subnets



5.4 Dynamic Addressing t

- Here, a server is designated to supply a network layer address to a computer each time the computer connects to the network.
- This is commonly done for client computers but usually not for servers
- The most common standard for dynamic addressing is Dynamic Host Configuration Protocol (DHCP).
- DHCP does not provide a network layer address in a configuration file.
- Instead, there is a special software package installed on the client that instructs it to contact a DHCP server to obtain an address.
- The **DHCP** server can be configured to assign the same network layer address to the computer (on the basis of its data link layer address) each time it requests an address, or it can lease the address to the computer by picking the "next available" network layer address from a list of authorized addresses.

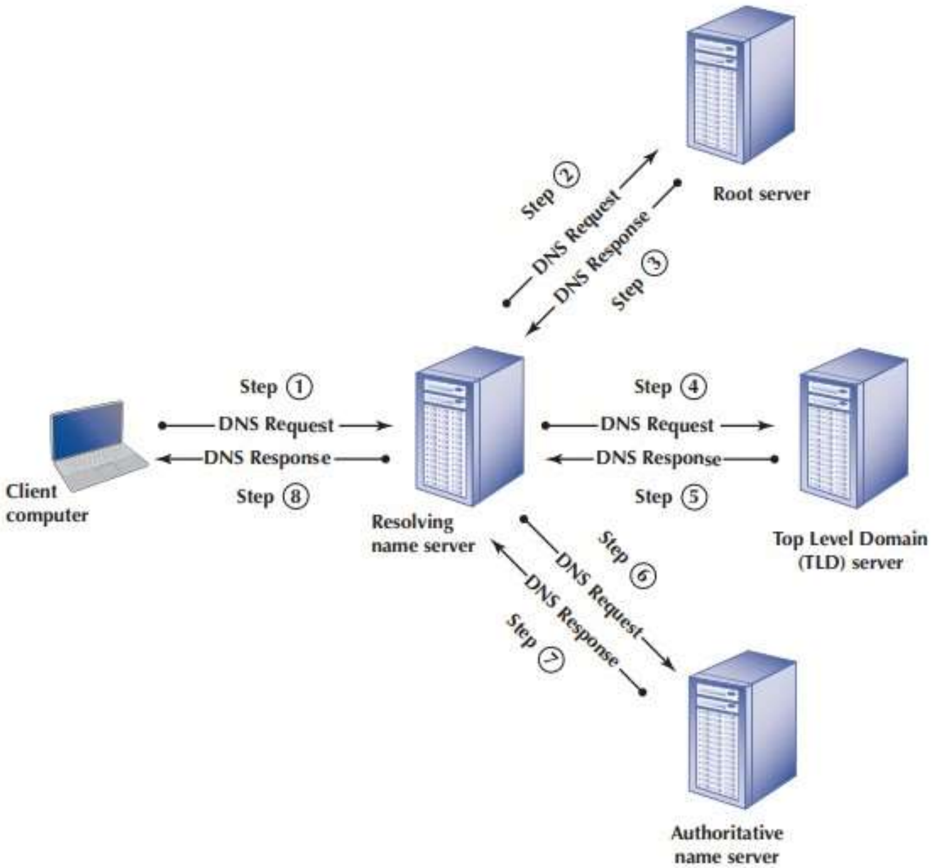
5.4 Server Name Resolution and DNS

- ❑ Server name resolution is the translation of application layer addresses into network layer addresses (e.g., translating an Internet address such as www.yahoo.com into an IP address such as 204.71.200.74).
- ❑ This is done using the Domain Name Service (DNS).
- ❑ Throughout the Internet a series of computers called name servers provides DNS services.
- ❑ These name servers ("directory assistance" for the Internet) have address databases that store thousands of Internet addresses and their corresponding IP addresses.
- ❑ Anytime a computer does not know the IP number for a computer, it sends a message to the name server requesting the IP number.
- ❑ Whenever you register an Internet application layer address, you must inform the registrar of the IP address of the name server that will provide DNS information for all addresses in that name range.
- ❑ DNS servers are maintained by network managers, who update their address information as the network changes.
- ❑ DNS servers can also exchange information about new and changed addresses among themselves, a process called **replication**.

5.4 Server Name Resolution and DNS (contd)

- When a computer needs to translate an application layer address into an IP address, it sends a special DNS request packet to its DNS server.

FIGURE 5-10
How the DNS system works



- Once your application layer software receives an IP address, it is stored on your computer in a DNS cache.

5.5 ROUTING

- ❑ Routers are usually found at the edge of subnets (they connect subnets).
- ❑ Figure 5-11 shows a small network with two routers, R1 and R2 (this network has five subnets, each router has 4 interfaces, plus a connection to the Internet).
- ❑ Every router has a routing table (generally 2-columns) that specifies how messages will travel through the network.

5.4 ROUTING

FIGURE 5-11
A small corporate network

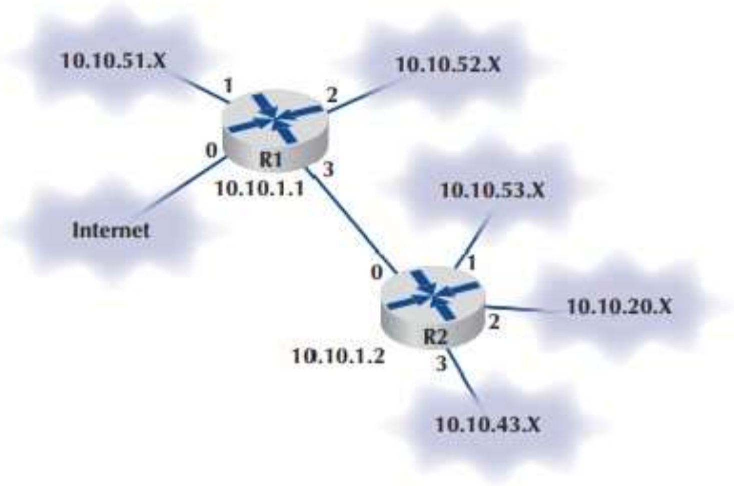
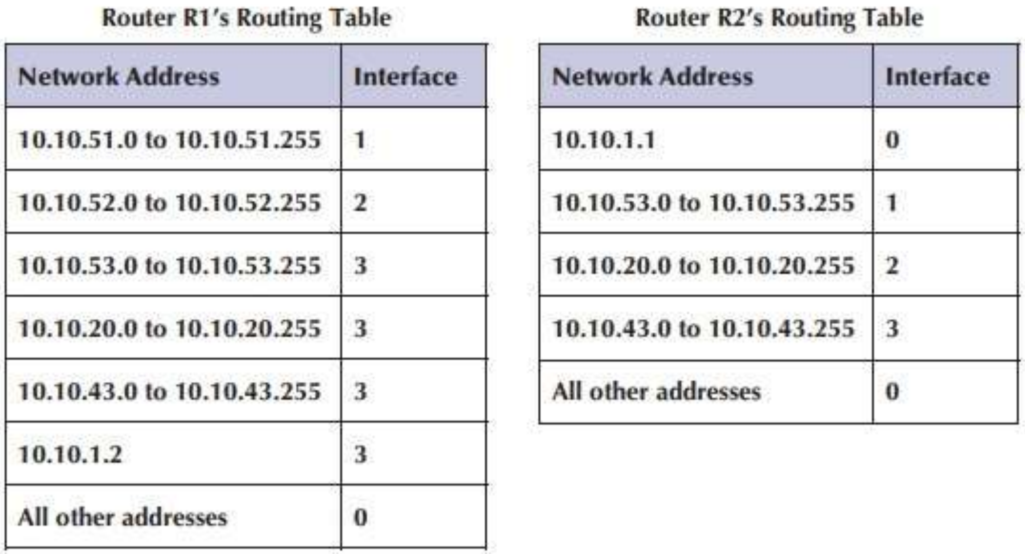


FIGURE 5-12
Sample routing tables



Router R1's Routing Table

Network Address	Interface
10.10.51.0 to 10.10.51.255	1
10.10.52.0 to 10.10.52.255	2
10.10.53.0 to 10.10.53.255	3
10.10.20.0 to 10.10.20.255	3
10.10.43.0 to 10.10.43.255	3
10.10.1.2	3
All other addresses	0

Router R2's Routing Table

Network Address	Interface
10.10.1.1	0
10.10.53.0 to 10.10.53.255	1
10.10.20.0 to 10.10.20.255	2
10.10.43.0 to 10.10.43.255	3
All other addresses	0

5.5.1 Types of Routing

- There are three fundamental approaches to routing: centralized routing, static routing, and dynamic routing. Internet uses all three of them.
  - Centralized Routing: All routing decisions are made by one central computer or router. Centralized routing is commonly used in host-based networks.
  - Static Routing: Is decentralized. All computers or routers in the network make their own routing decisions.
  - Dynamic Routing: AKA adaptive routing, routing decisions are made in a decentralized manner by individual computers.
    - This approach is used when there are **multiple routes** through a network, and it is important to select the best route. Dynamic routing attempts to improve network performance by routing over the fastest possible route, away from busy circuits and busy computers.
    - An initial routing table is developed by the network manager but is **continuously updated** by the computers themselves to reflect changing network conditions.

5.5.2. Routing Protocols

- ❑ A routing protocol is used to exchange information among computers to enable them to **build** and maintain their routing tables.
- ❑ When new paths are added or broken and cannot be used, messages are sent among computers using the routing protocol.
- ❑ It can be useful to know all possible routes to a given destination. However, as a network gets quite large, knowing all possible routes becomes impractical; there are simply too many possible routes. For this reason, networks are often subdivided into autonomous systems of networks. An autonomous system is simply a network operated by one organization.
- ❑ If an autonomous system grows too large, it can be split into smaller parts.
- ❑ The routing protocols used inside an autonomous system are called interior routing protocols. Protocols used between autonomous systems are called exterior routing protocols.
- ❑ Usually, exterior protocols provide information about only the preferred or the best routes rather than all possible routes.

5.5.2. Routing Protocols

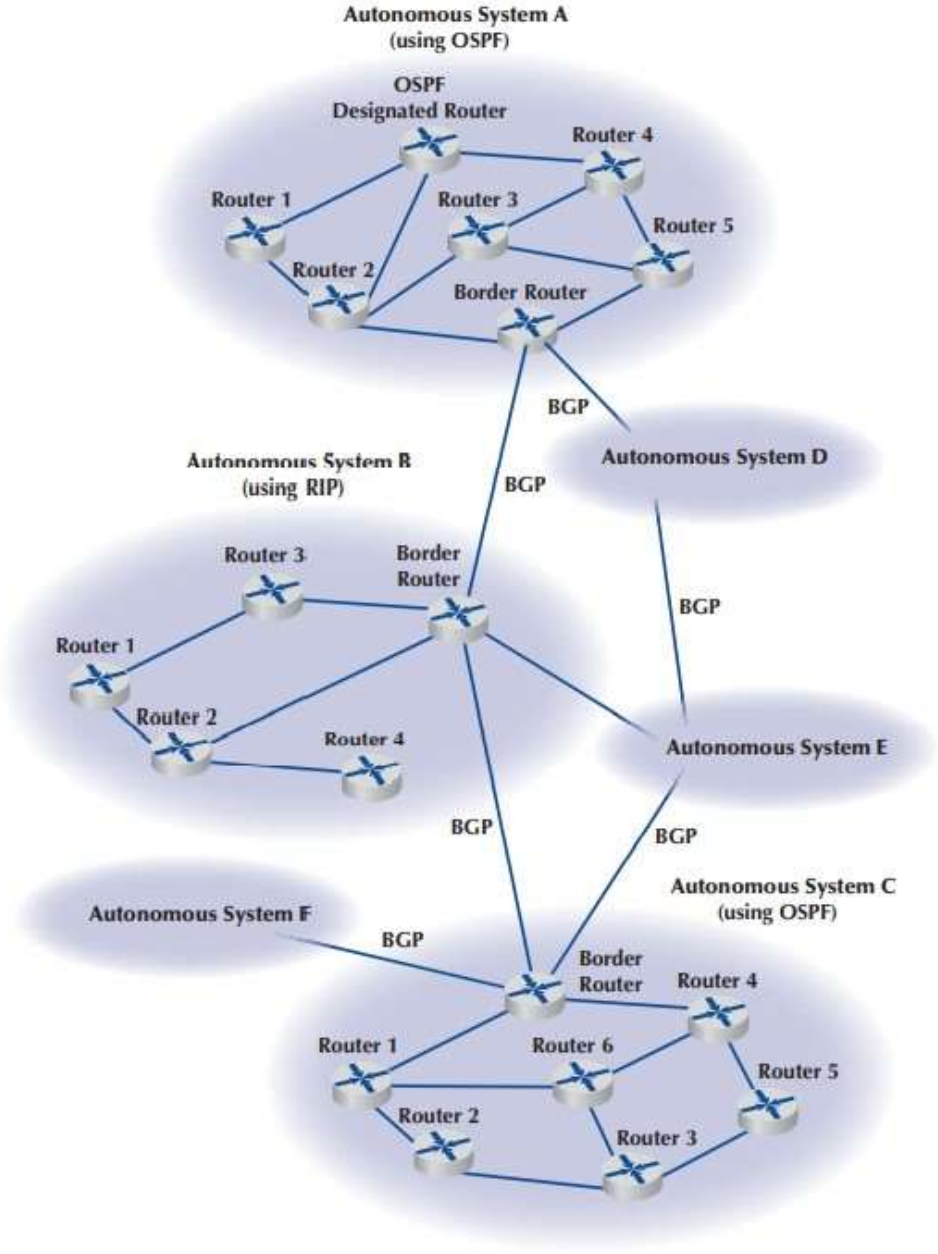
- ❑ There are many different protocols that are used to exchange routing information. Five are commonly used on the Internet:
  - ❑ Border Gateway Protocol (BGP)
  - ❑ Internet Control Message Protocol (ICMP)
  - ❑ Routing Information Protocol (RIP)
  - ❑ Intermediate System to Intermediate System (IS-IS)
  - ❑ Open Shortest Path First (OSPF), and
  - ❑ Enhanced Interior Gateway Routing Protocol (EIGRP).
- ❑ Border Gateway Protocol (BGP) is used on the Internet to exchange routing information between autonomous systems—that is, large sections of the Internet. Although BGP is preferred it is seldom used inside companies because it is large, complex, and often hard to administer.
- ❑ Internet Control Message Protocol (ICMP) is the simplest. ICMP is simply an error-reporting protocol that enables computers to report routing errors to message senders. ICMP also has a very limited ability to update routing tables.

5.5.2. Routing Protocols (contd)

- Routing Information Protocol (RIP) is a dynamic distance vector interior routing protocol that is commonly used in smaller networks,
  - The network manager uses RIP to develop the routing table. When new computers are added, RIP simply counts the number of computers in the possible routes to the destination and selects the shortest. Intermediate
- System to Intermediate System (IS-IS) is a link state interior routing protocol that is commonly used in large networks.
- Open Shortest Path First (OSPF) is a dynamic hybrid interior routing protocol that is commonly used on the Internet.
  - It uses the number of computers in a route, network traffic and error rates to select the best route.
  - OSPF is more efficient than RIP because it normally doesn’t use broadcast messages.
  - OSPF is the preferred interior routing protocol used by TCP/IP
- Enhanced Interior Gateway Routing Protocol (EIGRP) is a dynamic hybrid interior routing protocol (by Cisco) and is used inside organizations.
  - EIGRP records information about a route’s transmission capacity, delay, reliability, and load. EIGRP is unique in that computers or routers store their own routing tables as well as the routing tables for all of their neighbors, so they have a more accurate understanding of the network.

FIGURE 5-13

Routing on the Internet with Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP)



5.5.3 Multicasting

- The most common is the transmission between two computers.
    - One sends a message to another computer (e.g., a client requesting a Web page). This is called a **unicast** message.
    - Broadcast message that is sent to all computers on a specific LAN or subnet.
    - Multicast is used to send the same message to a **group** of computers.
        - Computers wishing to participate in multicast send a message to the sending computer using a special type of packet called Internet Group Management Protocol (IGMP).
        - Each multicast group is assigned a special IP address
        - Each requesting computer must inform its data link layer software to process incoming messages with this multicast data link layer address.
        - When the multicast session ends the multicast group is removed.

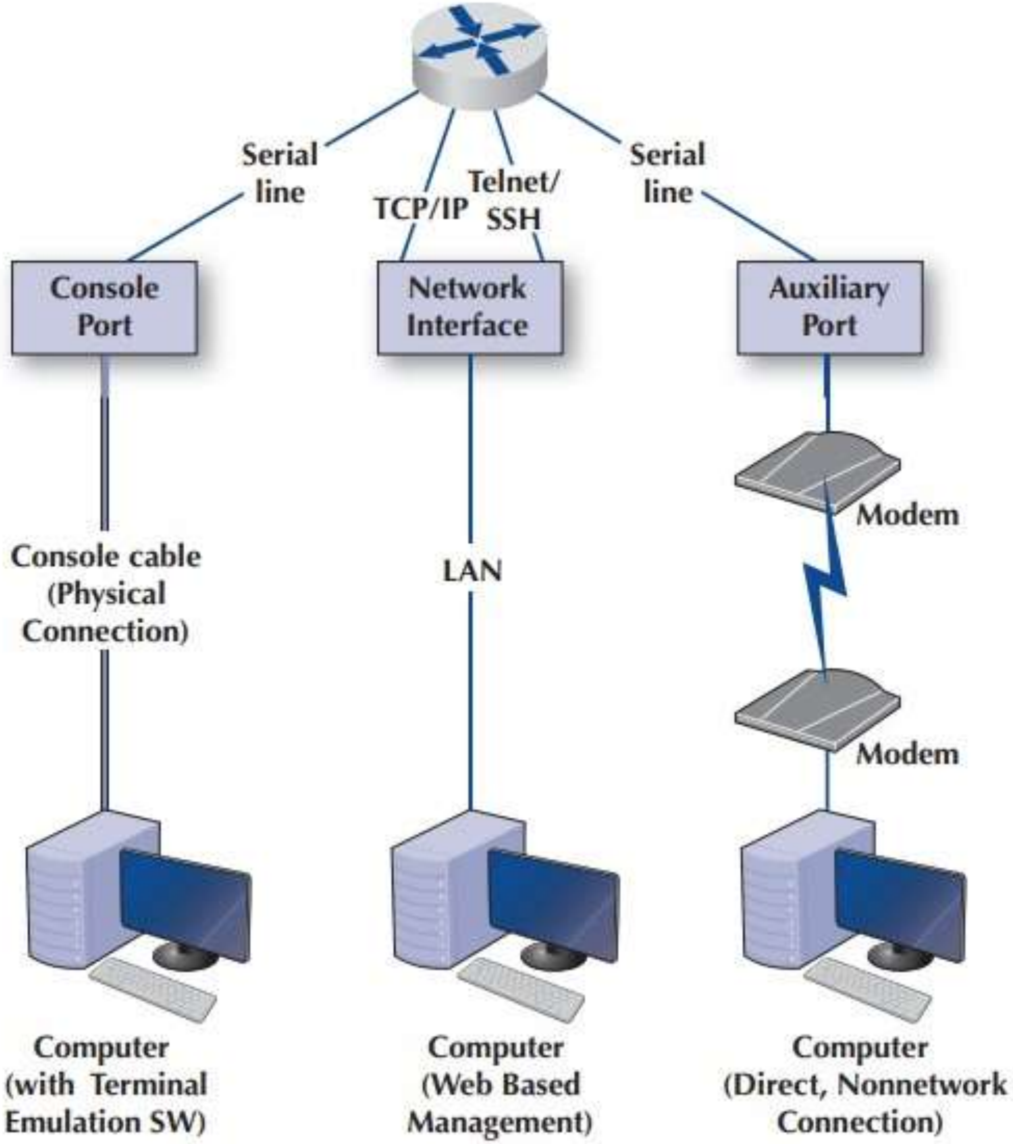
5.5.4 The Anatomy of a Router

- There is a huge array of software and hardware that makes the Internet work, but the one device that is indispensable is the **router**.
- The router has three main functions:
  - it determines a path for a packet to travel over,
  - it transmits the packet across the path, and
  - it supports communication between a wide variety of devices and protocols.
- We will look inside a router to see how these three functions are supported by hardware and software.
  - Routers are essentially special-purpose computers that consist of a CPU (central processing unit), memory (both volatile and nonvolatile), and ports or interfaces that connect them to the network and/or other devices **so that a network administrator can communicate with them**.
  - Routers are computers which are **diskless** and they don't come with a **monitor**, **keyboard**, and **mouse**.
  - They don't have these because they were designed to move data rather than display it.

5.5.4 The Anatomy of a Router (contd)

- ❑ There are three ways that a network manager can connect to a router and configure and maintain it: (1) console port, (2) network interface port, and (3) auxiliary port (see Figure 5-14).
- ❑ When the router is turned on for the very first time, it does not have an IP address assigned, so it cannot communicate on the network.
- ❑ Because of this, the **console port, also called the management port**, is used to configure it.
- ❑ A network manager would use a blue rollover cable (not the Ethernet cable) to connect the router’s console port to a computer that has **terminal emulation software** on it.
- ❑ The network manager would use this software to communicate with the router and perform the basic setup (e.g., IP address assignment, routing protocol selection).
- ❑ Once the basic setup is done, the network manager can log in to the router from any computer using the network interface using TCP/IP and Telnet with Secure Shell (SSH).
- ❑ A router, just like a computer, must have an operating system so that it can be configured.

FIGURE 5-14
Anatomy of a router


Serial line
TCP/IP
Telnet/ SSH
Serial line
Console Port
Network Interface
Auxiliary Port
Modem
Console cable (Physical Connection)
LAN
Modem
Computer (with Terminal Emulation SW)
Computer (Web Based Management)
Computer (Direct, Nonnetwork Connection)

5.6 TCP/IP Example

- We discussed the functions of the transport and network layers: linking to the application layer, segmenting, session management, addressing, and routing.
- Now we will tie all of these concepts together to take a closer look at how these functions actually work using TCP/IP.
- When a computer is installed on a TCP/IP network (or dials into a TCP/IP network),
  - it must be given four pieces of network layer addressing and routing information before it can operate.
  - This information can be provided by a configuration file, or via a DHCP server.
  - The (minimum required) information is:
    1. Its IP address
    2. A subnet mask
    - The IP address of a DNS server, so it can translate application layer addresses into IP addresses
    - The IP address of an IP gateway (commonly called a router) leading outside of its subnet

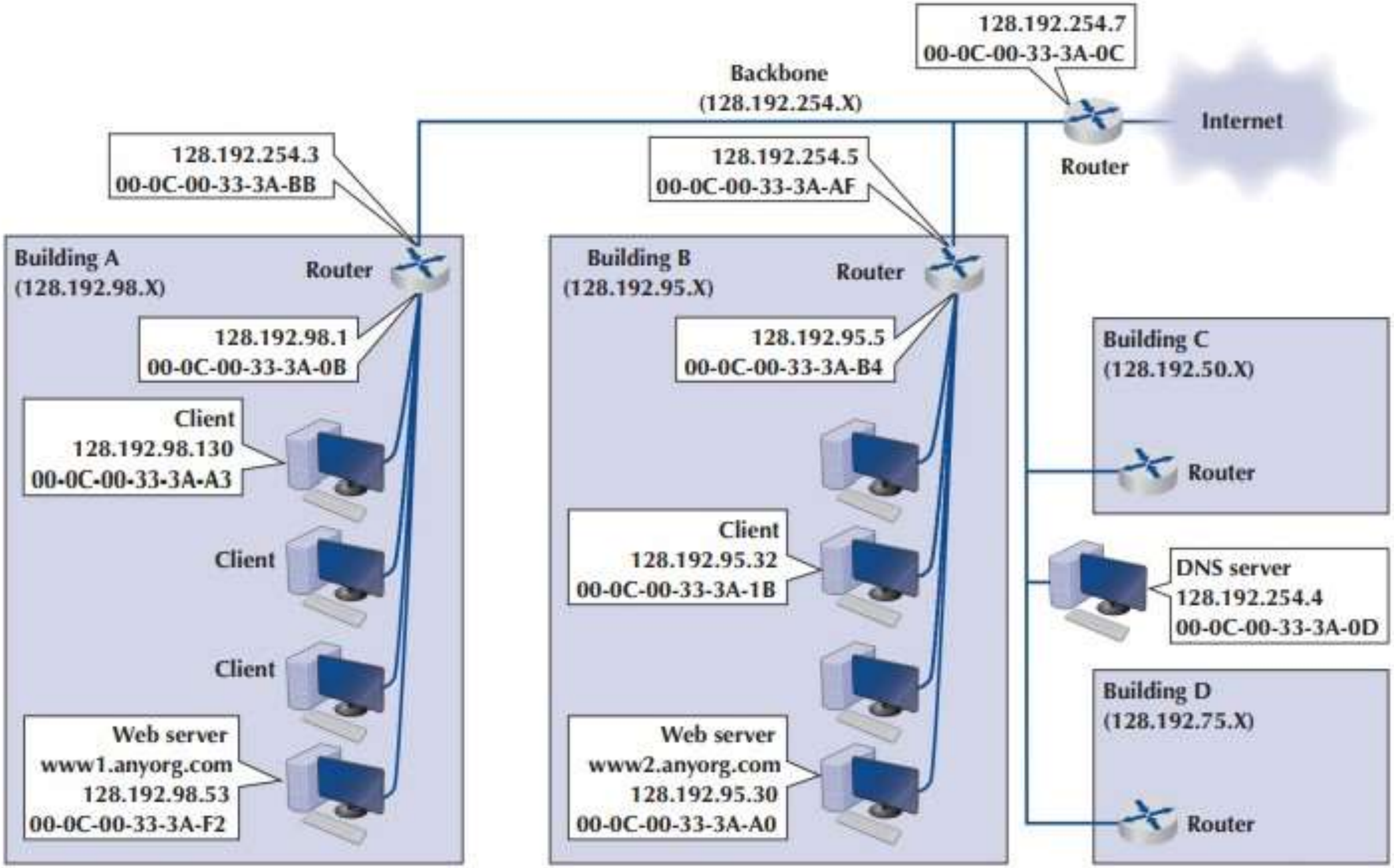


FIGURE 5-15 Example Transmission Control Protocol/Internet Protocol (TCP/IP) network

5.6. TCP/IP Example (contd).

- ❑ Figure 5-15 to illustrate how TCP/IP works.
- ❑ This figure shows an organization that has four LANs connected by a BN.
- ❑ The BN also has a connection to the Internet.
- ❑ Each building is configured as a separate subnet.
- ❑ For example, Building A has the 128.192.98.x subnet, whereas Building B has the 128.192.95.x subnet.
- ❑ The BN is its own subnet: 128.192.254.x.
- ❑ Each building is connected to the BN via a router that has two IP addresses and two data link layer addresses, one for the connection into the building and one for the connection onto the BN.
- ❑ The organization has several Web servers spread throughout the four buildings.
- ❑ The DNS server and the router onto the Internet are located directly on the BN itself.
- ❑ For simplicity, we assume that all networks use Ethernet as the data link layer and only focus on Web requests at the application layer.

5.6.5 TCP/IP and Network Layers

- ❑ A final look at how messages flow through the layers.
- ❑ Figure 5-18 shows how a Web request message (an HTTP Packet) from a client computer in Building A on its way to the server in Building B.
- ❑ This packet is passed to the transport layer, which surrounds the HTTP packet with a TCP segment.
- ❑ This is then passed to the network layer, which surrounds it with an IP frame that includes the IP address of the final destination (128.192.95.30).
- ❑ This in turn is passed to the data link layer, which surrounds it within an Ethernet frame that also includes the Ethernet address of the **next** computer to which the message will be sent (00-0C-00-33-3A-0B).
- ❑ Finally, this is passed to the physical layer, which converts it into electrical impulses for transmission through the cable to its next stop—the router that serves as the gateway in Building A.
- ❑ When the message arrives at the router in Building A, its physical layer translates it from electrical impulses into digital data and passes the Ethernet frame to the data link layer.
- ❑ The data link layer checks to make sure that the Ethernet frame is addressed to the router, performs error detection, strips off the Ethernet frame, and passes its contents (the IP packet) to the network layer.

5.6.5 TCP/IP and Network Layers (contd).

- The routing software running at the network layer looks at the destination IP address, determines the next computer to which the packet should be sent, and passes the outgoing packet down to the data link layer for transmission.
- The data link layer surrounds the IP packet with a completely new Ethernet frame that contains the destination address of the next computer to which the packet will be sent (00-0C-00-33-3A-AF).
- In Figure 5-18, this new frame is shown in a different color.
- This is then passed to the physical layer, which transmits it through the network cable to its next stop—the router that serves as the gateway in Building B.
- When the message arrives at the router in Building B, it goes through the same process. The physical layer passes the incoming packet to the data link layer, which checks the destination Ethernet address, performs error detection, strips off the Ethernet frame, and passes the IP packet to the network layer software.
- The software determines the next destination and passes the IP packet back to the data link layer, which adds a completely new Ethernet frame with the destination address of its next stop (00-0C-00-33-3A-A0)—its final destination.

Finally

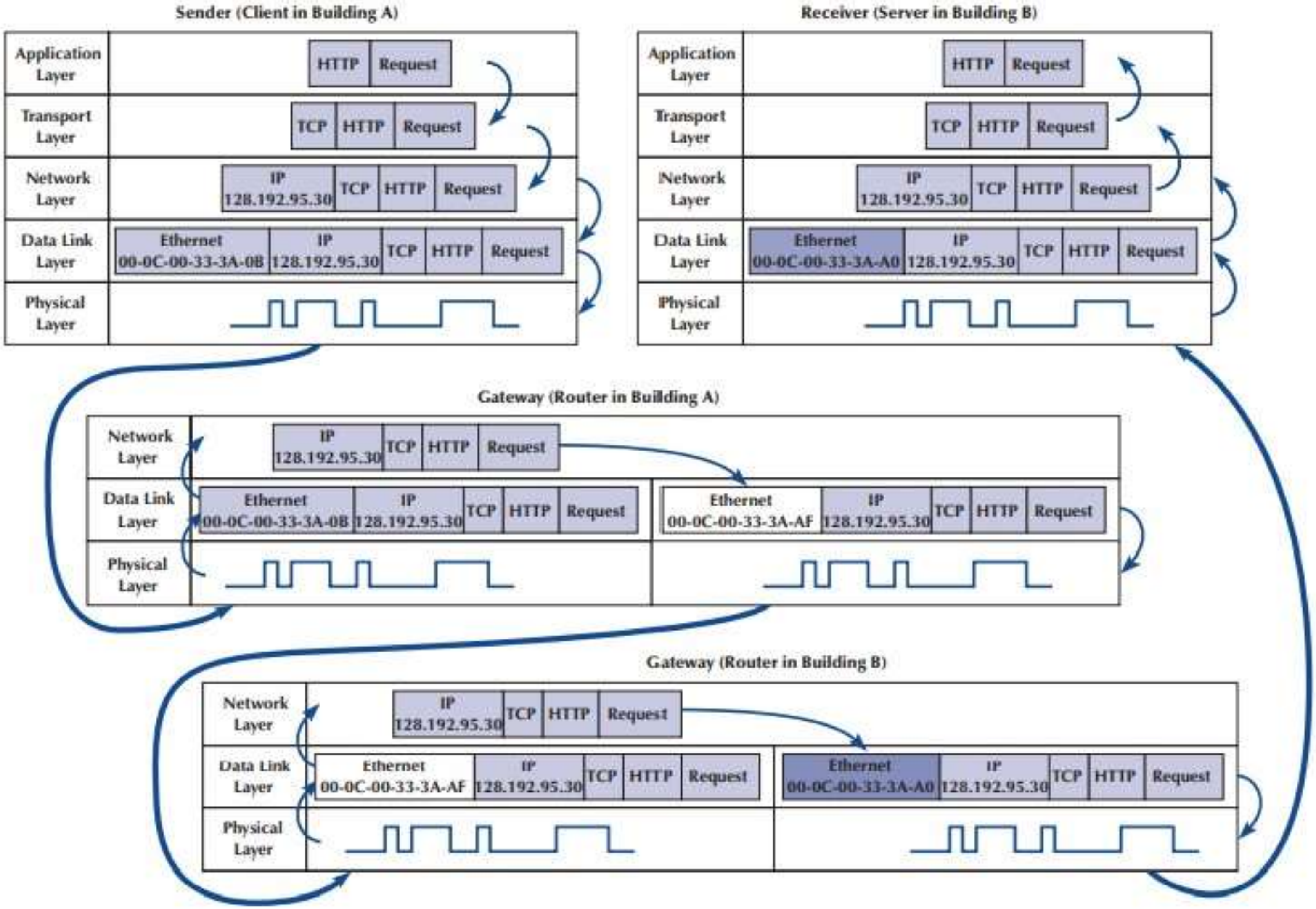

Sender (Client in Building A)
Application Layer
HTTP Request
Transport Layer
TCP HTTP Request
Network Layer
IP 128.192.95.30 TCP HTTP Request
Data Link Layer
Ethernet 00-0C-00-33-3A-0B IP 128.192.95.30 TCP HTTP Request
Physical Layer
Receiver (Server in Building B)
Application Layer
HTTP Request
Transport Layer
TCP HTTP Request
Network Layer
IP 128.192.95.30 TCP HTTP Request
Data Link Layer
Ethernet 00-0C-00-33-3A-A0 IP 128.192.95.30 TCP HTTP Request
Physical Layer
Gateway (Router in Building A)
Network Layer
IP 128.192.95.30 TCP HTTP Request
Data Link Layer
Ethernet 00-0C-00-33-3A-0B IP 128.192.95.30 TCP HTTP Request
Ethernet 00-0C-00-33-3A-AF IP 128.192.95.30 TCP HTTP Request
Physical Layer
Gateway (Router in Building B)
Network Layer
IP 128.192.95.30 TCP HTTP Request
Data Link Layer
Ethernet 00-0C-00-33-3A-AF IP 128.192.95.30 TCP HTTP Request
Ethernet 00-0C-00-33-3A-A0 IP 128.192.95.30 TCP HTTP Request
Physical Layer

FIGURE 5-18 How messages move through the network layers.
Note: The addresses in this example are destination addresses