Chapter Ten

The Internet

Data Communications and Computer Networks: A Business User's Approach

Eighth Edition

After reading this chapter, you should be able to:

- Discuss the responsibilities of the Internet Protocol (IP) and how IP can be used to create a connection between networks
- Identify both IPv4 and IPv6 addresses
- Discuss the responsibilities of the Transmission Control Protocol (TCP) and how it can be used to create a reliable, end-to-end network connection

After reading this chapter, you should be able to (continued):

- Identify the relationships between TCP/IP and the protocols ICMP, UDP, ARP, DHCP, NAT, and tunneling protocols
- Describe the responsibility of the Domain Name System and how it converts a URL into a dotted decimal IP address

After reading this chapter, you should be able to (continued):

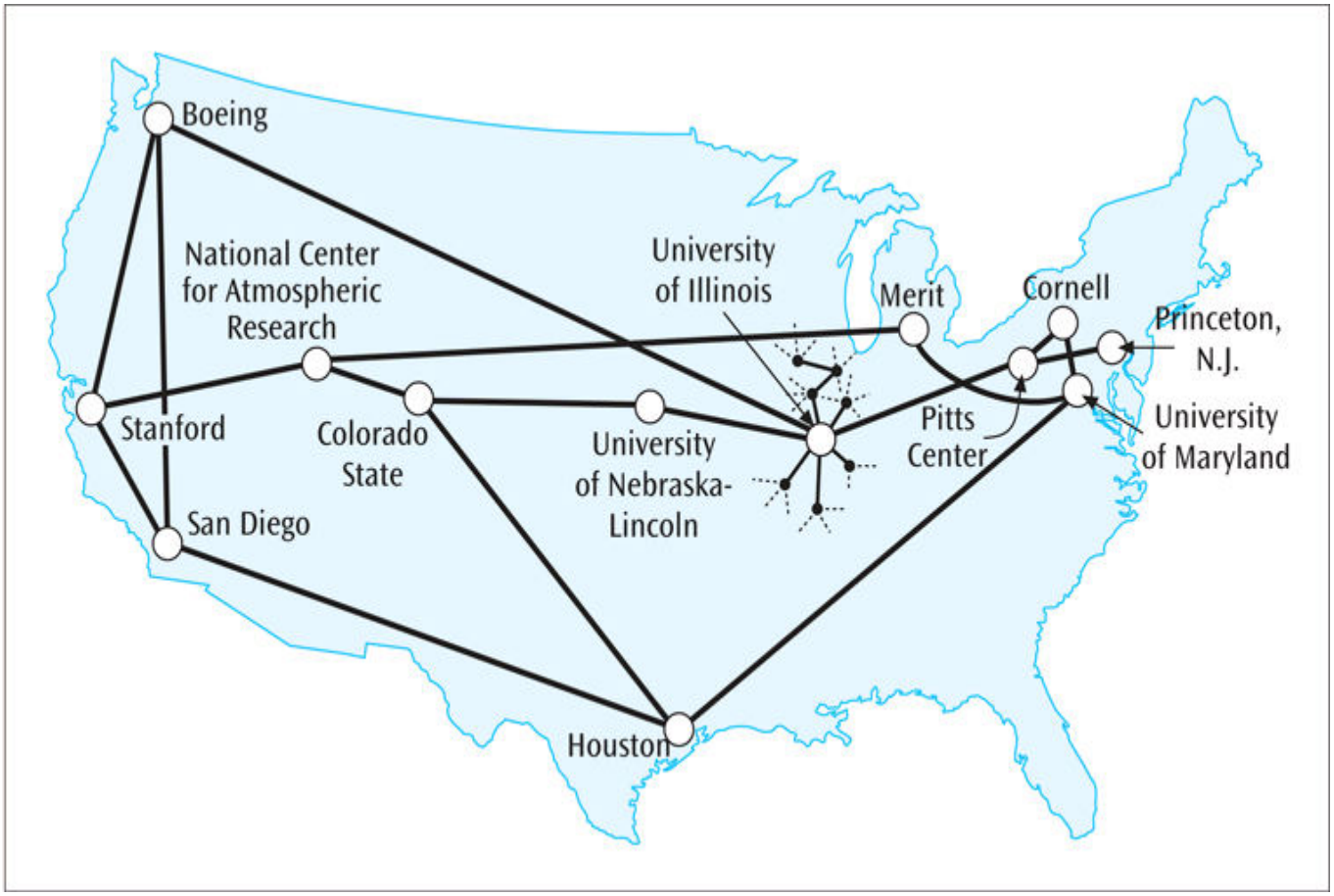
- Describe the major Internet applications and services
- Recognize that the Internet is constantly evolving and that IPv6 and Internet2 demonstrate that evolution

Introduction

- Today's present Internet is a vast collection of thousands of networks and their attached devices
- The Internet began as ARPANET during the 1960s
- One high-speed backbone connected several university, government, and research sites
  - Backbone was capable of supporting 56 kbps transmission speeds and eventually became financed by the National Science Foundation (NSF)

Introduction (continued)

Figure 10-1
Old NSFnet backbone and connecting mid-level and campus networks



Internet Protocols

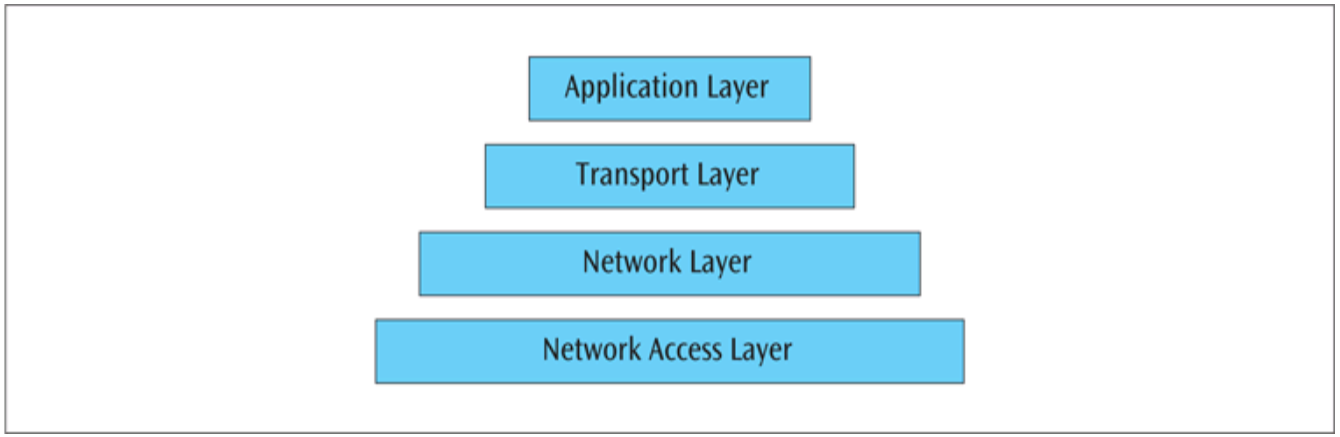
- To support the Internet and all its services, many protocols are necessary
- Some of the protocols that we will look at:
  - Internet Protocol (IP)
  - Transmission Control Protocol (TCP)
  - Address Resolution Protocol (ARP)
  - Dynamic Host Configuration Protocol (DHCP)
  - Network Address Translation (NAT)

Internet Protocols (continued)

- Recall that the Internet with all its protocols follows the TCP/IP protocol suite (Internet model)
  - An application, such as e-mail, resides at the highest layer
  - A transport protocol, such as TCP, resides at the transport layer
  - The Internet Protocol (IP) resides at the Internet or network layer
  - A particular media and its framing resides at the network access (or data link) layer

Internet Protocols (continued)

Figure 10-2
Hierarchy of layers as created by the Department of Defense



The Internet Protocol (IP)

- IP prepares a packet for transmission across the Internet
- The IP header is encapsulated onto a transport data packet
- The IP packet is then passed to the next layer where further network information is encapsulated onto it

The Internet Protocol (IP) (continued)

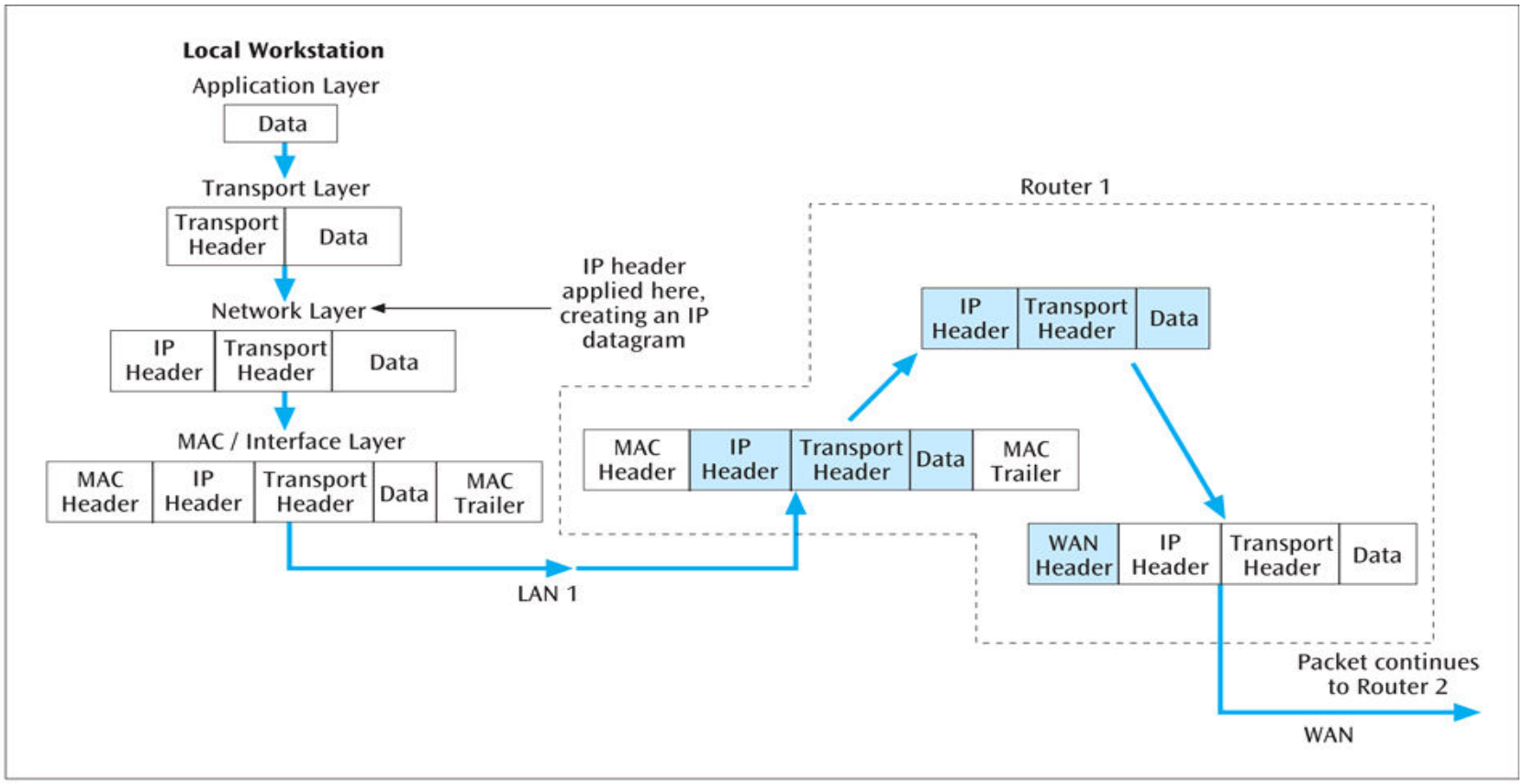


Figure 10-3
Progression of a packet from one network to another

The Internet Protocol (IP) (continued)

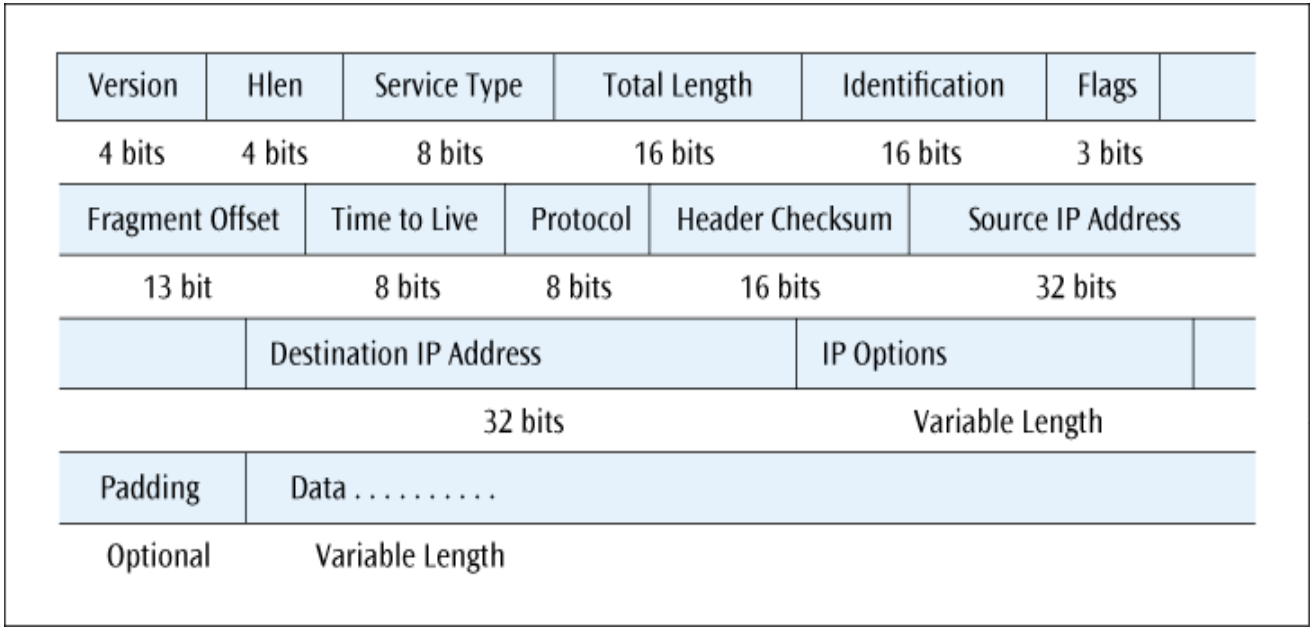
- There are currently two versions of IP:
  - Version 4, which has been in existence for many years
  - Version 6, which has been available for several years but is only now starting to see a substantial move towards replacing version 4
  - Let's take a look at both versions

IPv4

- Using IPv4, a router:
  - Makes routing decisions based on the 32-bit destination address
  - May have to fragment the datagram into smaller datagrams using Fragment Offset
  - May determine that current datagram has been hopping around the network too long and delete it (Time to Live)

The IPv4 Header/Datagram

Figure 10-4
Format of the IPv4 datagram



IPv4

- Fragmenting an IPv4 datagram is performed by the Offset and More fields. Offset value is in multiples of 8 bytes

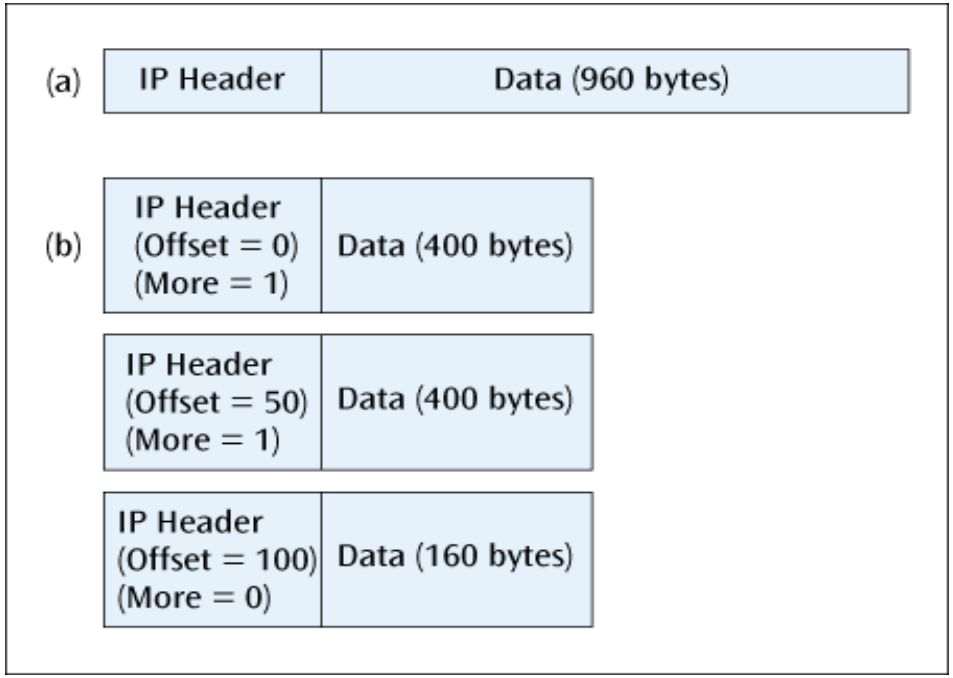


Figure 10-5
Division of an IPv4 datagram into three fragments

IPv4 Addresses

- All devices connected to Internet have a 32-bit IP address
- Think of the IP address as a logical address (possibly temporary), while the 48-bit address on every NIC is the physical, or permanent address
- Computers, networks and routers use the 32-bit binary address, but a more readable form is the dotted decimal notation

IPv4 Addresses (continued)

- For example, the 32-bit binary address

  10000000 10011100 00001110 00000111

  translates to

  128.156.14.7

  in dotted decimal notation

IPv4 Addresses (continued)

- When IP addresses were originally created, they were called classful addresses
  - That is, each IP address fell into particular class
  - A particular class address has a unique network address size and a unique host address size
  - There are basically five types of IP addresses: Classes A, B, C, D and E

IPv4 Addresses (continued)

Table 10-1

Five basic forms of a 32-bit IP address

Address Type	Beginning Bit Pattern	Network Address (net ID)	Host Address (host ID)
Class A	0	128 addresses (7 bits)	16,777,216 addresses (24 bits)
Class B	10	16,384 addresses (14 bits)	65,536 addresses (16 bits)
Class C	110	2,097,152 addresses (21 bits)	256 addresses (8 bits)
Class D	1110	Multicast address	
Class E	1111	Reserved addresses	

IPv4 Addresses (continued)

- When you examine the first decimal value in the dotted decimal notation:
  - All Class A addresses are in the range 0 - 127
  - All Class B addresses are in the range 128 - 191
  - All Class C addresses are in the range 192 – 223
  - All Class D addresses are in the range 224 – 239
  - All Class E addresses are in the range 240 - 255

IPv4 Addresses (continued)

- IP subnet masking
  - Sometimes you have a large number of IP addresses to manage
  - By using subnet masking, you can break the host ID portion of the address into a subnet ID and host ID
  - Example – subnet mask 255.255.255.0 applied to a class B address will break the host ID (normally 16 bits) into an 8-bit subnet ID and an 8-bit host ID

IPv4 Addresses (continued)

- Today, IP addresses are considered classless addresses
  - With classless addressing, companies (users) do not apply for particular class of addresses
    - Instead, company will get its IP addresses from an Internet service provider (ISP)
    - Most ISPs have already applied for a large number of IP addresses and are willing to lease those addresses to companies

IPv4 Addresses (continued)

- Example – instead of applying for two Class C addresses, a company could contact an ISP, which would lease 500 IP addresses to the company
- The addresses are not identified by any class – they are simply a contiguous block of IP addresses
- Classless addressing has led to a much more efficient allocation of the IP address space
  - A company can lease only as many addresses as it needs

Classless IPv4 Addresses

- An IP address in *slash notation* has all the info we need about the block of addresses assigned to a user/company
- For example, one address in a block of addresses is 167.199.170.82/27
  - 27 bits belong to the network ID, and 5 bits belong to the host ID (IPv4 addresses have 32 bits)
  - The network mask has 27 1s followed by 5 0s. In dotted decimal notation that is 255.255.255.224.
  - The number of addresses in the block is $2^5 = 32$

Classless IPv4 Addresses

- To find the first address, AND the address (167.199.170.82) with the network mask (255.255.255.224)

Address: 10100111 11000111 10101010 01010010

Mask: 11111111 11111111 11111111 11100000

Result: 10100111 11000111 10101010 01000000

Which in decimal is 167.199.170.64/27

The last address is 31 addresses past the first, or 167.199.170.95/27

IPv6

- The next version of the Internet Protocol
- Main features include:
  - Simpler header
  - 128-bit IP addresses
  - Priority levels and quality of service parameters
  - No fragmentation

IPv6 (continued)

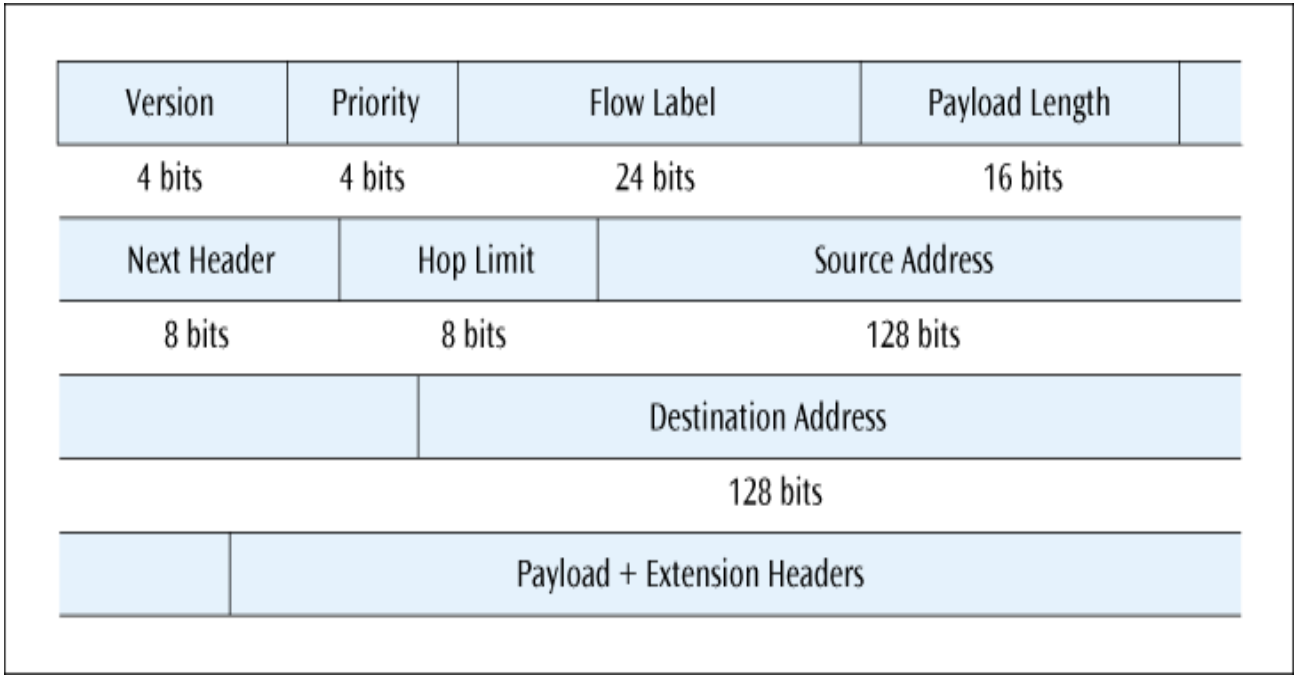


Figure 10-6
The fields in the IPv6 header

IPv6 Addresses

- IPv6 addresses are 128-bits in size (2^{128} is a very large number!)
- They are also classless addresses, similar to IPv4 addresses
- Because of their size, a number of conventions have been adopted:

IPv6 Addresses

- Binary addresses are written using the short-hand hexadecimal form:

0110 1010 0011 1110 1011 1010 … 1110 1111

6A3E : BA91 : 7221 : 0000 : 01FC : 922C : 877B : FFEF

- Four hex 0s in a row are truncated as follows:

6A3E : BA91 : 7221 : 0 : 01FC : 922C : 877B : FFEF

IPv6 Addresses

- Longer strings of 0s can be abbreviated further. For example,

  6A3E : BA91 : 0 : 0 : 0 : 0 : 877B : FFEF

- can be abbreviated as

  6A3E : BA91 : : 877B : FFEF

The Transmission Control Protocol (TCP)

- TCP layer creates connection between sender and receiver using port numbers
  - The port number identifies a particular application on a particular device (IP address)
- TCP can multiplex multiple connections (using port numbers) over a single IP line

The Transmission Control Protocol (TCP) (continued)

- The TCP layer can ensure that the receiver is not overrun with data (end-to-end flow control) using the Window field
- TCP can perform end-to-end error correction
  - Checksum
- TCP allows for the sending of high priority data
  - Urgent Pointer

The Transmission Control Protocol (TCP) (continued)

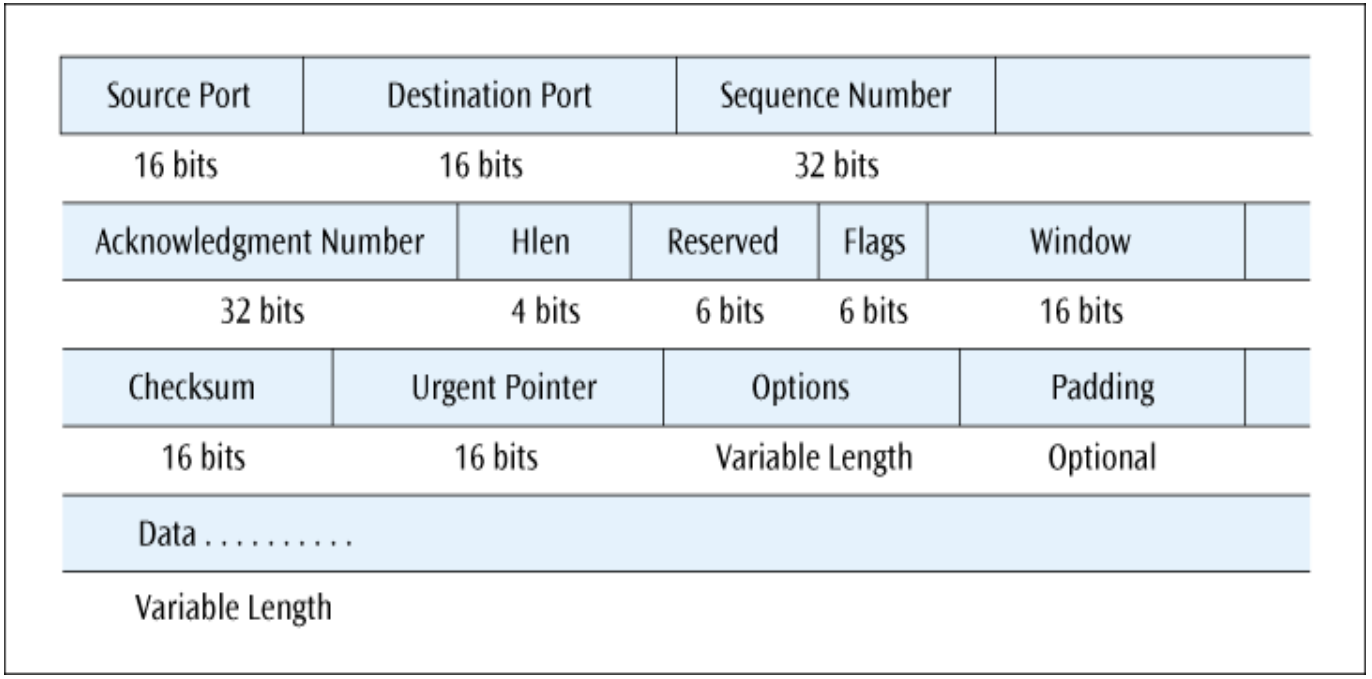


Figure 10-7
The fields of the TCP header

Internet Control Message Protocol (ICMP)

- ICMP
  - Used by routers and nodes
  - Performs error reporting for the Internet Protocol
    - ICMP reports errors such as invalid IP address, invalid port address, and the packet has hopped too many times

User Datagram Protocol (UDP)

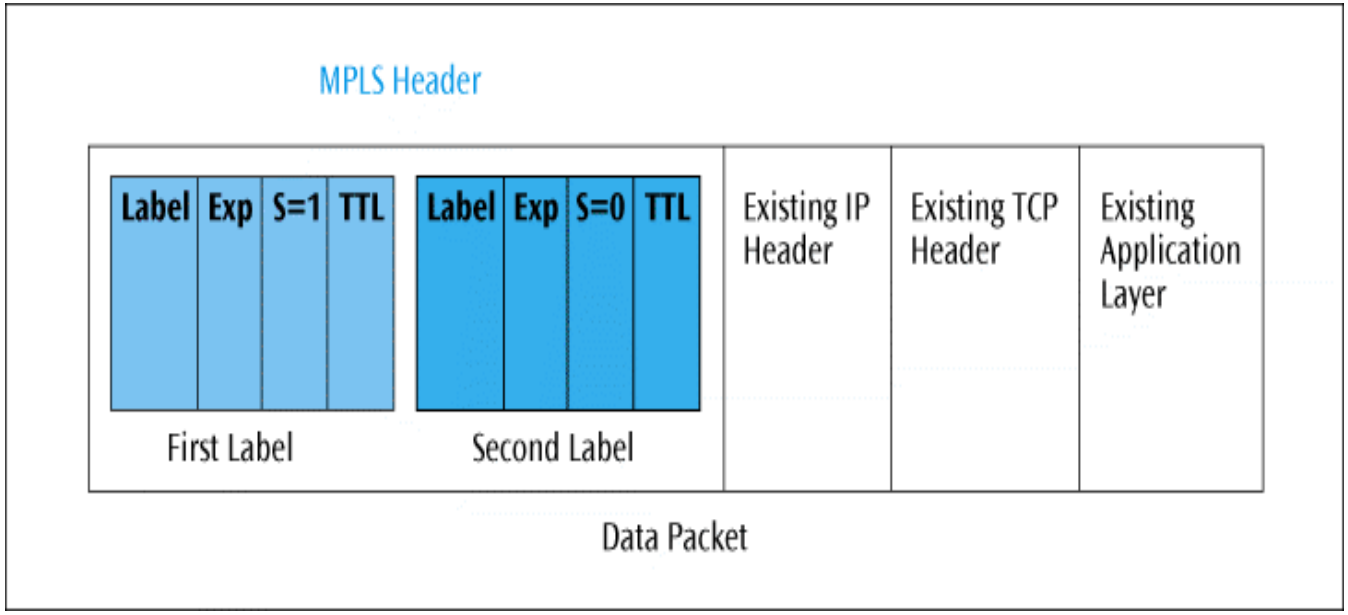
- A transport layer protocol used in place of TCP
- Where TCP supports a connection-oriented application, UDP is used with connectionless applications
- UDP also encapsulates a header onto an application packet but the header is much simpler than TCP (16-bit source port, 16-bit dest port, 16-bit length of entire packet, 16-bit checksum)

Multiprotocol Label Switching

- An additional layer often added above TCP
- Used to move Internet packets more quickly through routers
- By using the MPLS label, the router does not have to “dig in” so deep to retrieve IP address
- The 20-bit Label field is the key identifier that connects this packet with a particular flow of packets

Multiprotocol Label Switching

Figure 10-8
Two MPLS headers and their four fields



Address Resolution Protocol (ARP)

- When an IP packet has traversed the Internet and encounters the destination LAN, how does the packet find the destination workstation?
- Even though destination workstation may have an IP address, a LAN does not use IP addresses to deliver frames
  - A LAN uses MAC layer address
- ARP translates IP address into MAC layer address so frame can be delivered to proper workstation

Dynamic Host Configuration Protocol (DHCP)

- An IP address can be assigned to a workstation permanently (static assignment) or dynamically
  - Dynamic IP address assignment is a more efficient use of scarce IP addresses
  - When DHCP client issues an IP request, DHCP server looks in its static table
    - If no entry exists, server selects an IP address from available pool

Dynamic Host Configuration Protocol (DHCP) (continued)

- The address assigned by DHCP server is temporary
  - Part of agreement includes specific period of time
    - If no time period specified, the default is one hour
  - DHCP clients may negotiate for a renewal before the time period expires

Network Address Translation (NAT)

- NAT lets router represent entire local area network to Internet as single IP address
  - Thus, all traffic leaving LAN appears as originating from global IP address
  - All traffic coming into this LAN uses this global IP address
- This security feature allows a LAN to hide all the workstation IP addresses from the Internet

Network Address Translation (NAT) (continued)

- Since the outside world cannot see into LAN, you do not need to use registered IP addresses on inside LAN
- We can use the following blocks of addresses for private use:
  - 10.0.0.0 – 10.255.255.255
  - 172.16.0.0 – 172.31.255.255
  - 192.168.0.0 – 192.168.255.255

Network Address Translation (NAT) (continued)

- When a user on inside sends packet to outside, the NAT interface changes the user's inside address to global IP address
  - This change is stored in a cache
- When the response comes back, the NAT looks in cache and switches the addresses back
  - If not the packet is dropped
    - Unless NAT has a service table of fixed IP address mappings
      - This service table allows packets to originate from the outside

Tunneling Protocols and Virtual Private Networks (VPNs)

- The Internet is not normally a secure system
- If person wants to use Internet to access corporate computer system, how can a secure connection be created?
  - One possible technique is by creating a virtual private network (VPN)
    - VPN creates a secure connection through the Internet by using a tunneling protocol

The World Wide Web

- The World Wide Web (WWW) – immense collection of web pages and other resources that can be downloaded across the Internet and displayed on a workstation via a web browser and is the most popular service on the Internet
- Basic web pages are created with the Hypertext Markup Language (HTML)
- Hypertext Transport Protocol (HTTP) is protocol to transfer a web page

Locating a Document on the Internet

- Every document on the Internet has a unique Uniform Resource Locator (URL)
- All URLs consist of four parts:
  - Service type
  - Host or domain name
  - Directory or subdirectory information
  - Filename

Locating a Document on the Internet (continued)

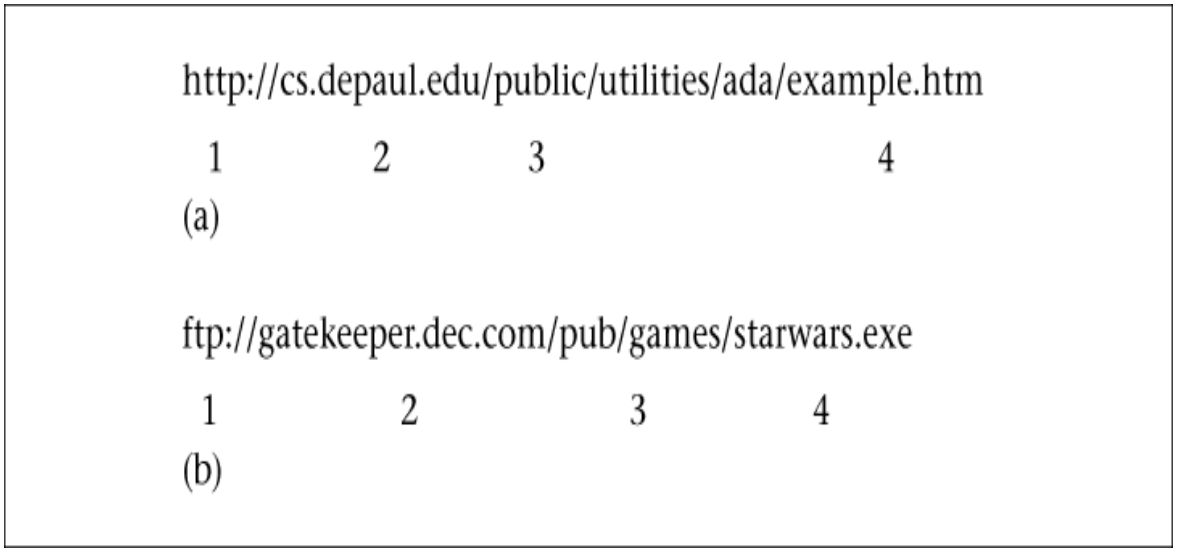


Figure 10-9
The parts of a Uniform Resource Locator (URL) for HTTP (a) and FTP (b)

Locating a Document on the Internet (continued)

- When a user, running a Web browser, enters a URL, how is URL translated into an IP address?
  - Domain Name System (DNS) – large, distributed database of URLs and IP addresses
    - The first operation performed by DNS is to query a local database for URL/IP address information
      - If local server does not recognize address, the server at next level will be queried
      - Eventually root server for URL/IP addresses will be queried
        - » If root server has answer, results are returned
        - » If root server recognizes domain name but not extension in front of domain name, root server will query server at domain name's location
        - » When domain's server returns results, they are passed back through chain of servers (and their caches)

Internet Services

- The Internet provides many types of services, including several very common ones:
  - Electronic mail (e-mail)
  - File transfer protocol (FTP)
  - Remote login (Telnet)
  - VoIP (Voice over IP)
  - Listservs
  - Streaming audio and video
  - Instant Messaging, Tweets, and Blogs

Electronic Mail (e-mail)

- E-mail programs can create, send, receive, and store e-mails, as well as reply to, forward, and attach non-text files
- Multipurpose Internet Mail Extension (MIME) is used to send e-mail attachments
- Simple Mail Transfer Protocol (SMTP) is used to transmit e-mail messages
- Post Office Protocol version 3 (POP3) and Internet Message Access Protocol (IMAP) are used to hold and later retrieve e-mail messages

File Transfer Protocol (FTP)

- Used to transfer files across the Internet
- User can upload or download a file
- The URL for an FTP site begins with ftp://…
- The three most common ways to access an FTP site are:
  - Through a browser
  - Using a canned FTP program
  - Issuing FTP commands at a text-based command prompt

Remote Login (Telnet)

- Allows a user to remotely log in to a distant computer site
- User usually needs a login and password to access a remote computer site
- User saves money on long-distance telephone charges

Voice Over IP (VoIP)

- The transfer of voice signals using a packet-switched network and the IP protocol
- Voice over IP (VoIP) can be internal to a company (private VoIP) or can be external using the Internet
- VoIP consumes many resources and may not always work well, but can be cost-effective in certain situations

Voice Over IP (continued)

- Three basic ways to make a telephone call using VoIP:
  - PC to PC using sound cards and headsets (or speakers and microphone)
  - PC to telephone (need a gateway to convert IP addresses to telephone numbers)
  - Telephone to telephone (need gateways)

Voice Over IP (continued)

- Three functions necessary to support VoIP:
  - Voice must be digitized (PCM, 64 kbps, fairly standard)
  - 64 kbps voice must be compressed
  - Once the voice is compressed, the data must be transmitted

Voice Over IP (continued)

- How can we transport compressed voice?
  - H.323
    - Created in 1996 by ITU-T
    - Actually, H.323 created for a wide range of applications both audio and video, and not for TCP/IP networks
  - Session Initiation Protocol (SIP)
    - Created by IETF specifically for supporting the transfer of voice over the Internet
  - Many feel SIP will surpass H.323

Voice Over IP (continued)

- ENUM
  - A protocol that supports VoIP
  - Converts telephone numbers to fully qualified domain name addresses
  - Example – telephone number (312) 555-1212 will be converted to 2.1.2.1.5.5.5.2.1.3.1.e164.arpa

Listservs

- A popular software program used to create and manage Internet mailing lists
- When an individual sends an e-mail to a listserv, the listserv sends a copy of the message to all listserv members
- Listservs can be useful business tools for individuals trying to follow a particular area of study

Streaming Audio and Video

- The continuous download of a compressed audio or video file, which can be heard or viewed on the user's workstation
- Real-Time Protocol (RTP) and Real-Time Streaming Protocol (RTSP) support streaming audio and video
- Streaming audio and video consume a large amount of network resources

Instant Messaging, Tweets, and Blogs

- IM allows a user to see if people are currently logged in on the network and to send short messages in real time
- Consumes less resources than e-mail, and faster
- Tweets occur when you Twitter. Max 140 character messages
- Blogs are online web logs that people maintain

The Internet and Business

- E-Commerce – the buying and selling of goods and services via the Internet
- Many agree that e-commerce consists of four major areas:
  - E-retailing
  - Electronic data interchange (EDI)
  - Micro-marketing
  - Internet security

Cookies and State Information

- A cookie is data created by a Web server that is stored on the hard drive of a user's workstation
  - This state information is used to track a user's activity and to predict future needs
- Information on previous viewing habits stored in a cookie can also be used by other Web sites to provide customized content
- Many consider cookies to be an invasion of privacy

Intranets and Extranets

- An intranet is a TCP/IP network inside a company that allow employees to access the company's information resources through an Internet-like interface
- When an intranet is extended outside the corporate walls to include suppliers, customers, or other external agents, the intranet becomes an extranet

The Future of the Internet

- Various Internet committees are constantly working on new and improved protocols
- Examples include:
  - Internet Printing Protocol
  - Internet fax
  - Extensions to FTP
  - Common Name Resolution Protocol
  - WWW Distributed Authoring and Versioning

Internet2

- A new form of the Internet is being developed by a number of businesses and universities
- Internet2 will support very high-speed data streams
- Applications might include:
  - Digital library services
  - Tele-immersion
  - Virtual laboratories

The Internet In Action: A Company Creates a VPN

- A fictitious company wants to allow 3500 of its workers to work from home
- If all 3500 users used a dial-in service, the telephone costs would be very high

The Internet In Action: A Company Creates a VPN (continued)

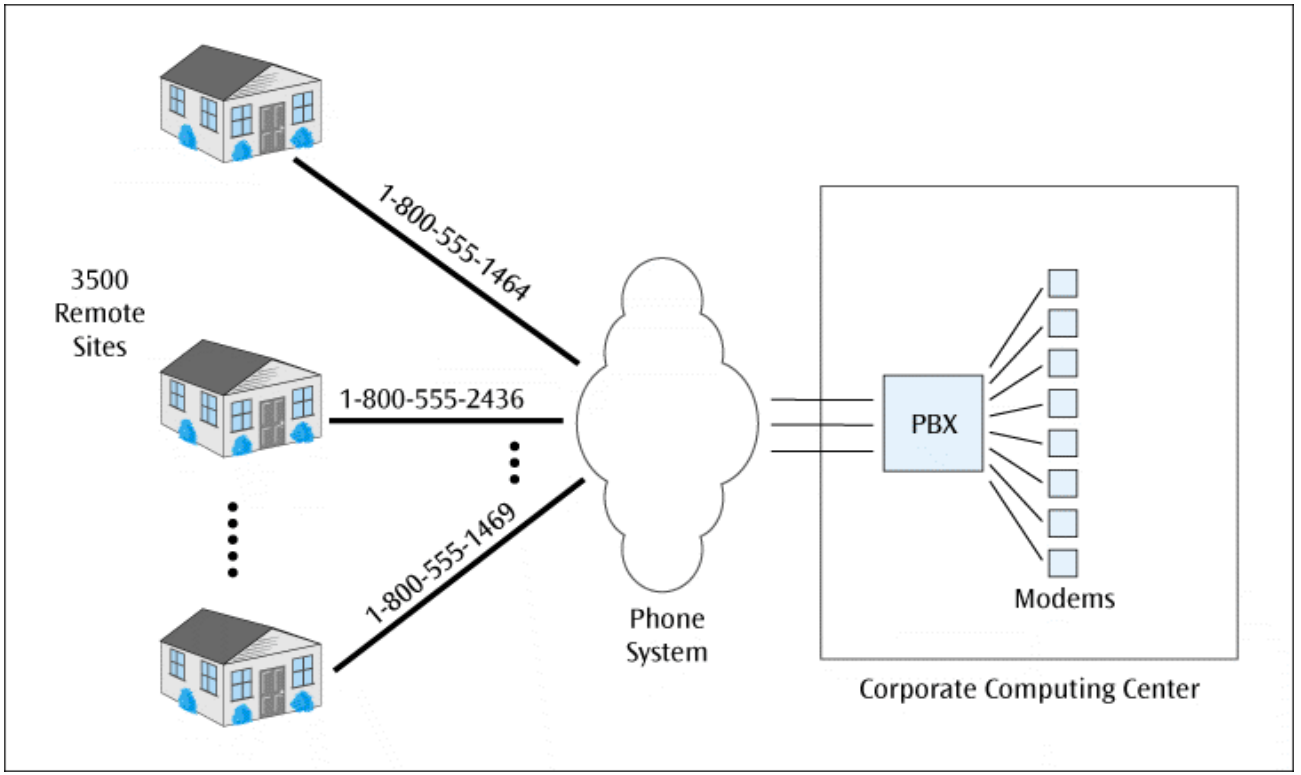


Figure 10-10
CompuCom employees dialing directly into the corporate computing center

The Internet In Action: A Company Creates a VPN (continued)

- Instead, the company will require each user to access the Internet via their local Internet service provider
  - This local access will help keep telephone costs low
  - Then, once on Internet, company will provide software to support virtual private networks
  - The virtual private networks will create secure connections from the users' homes into the corporate computer system

The Internet In Action: A Company Creates a VPN (continued)

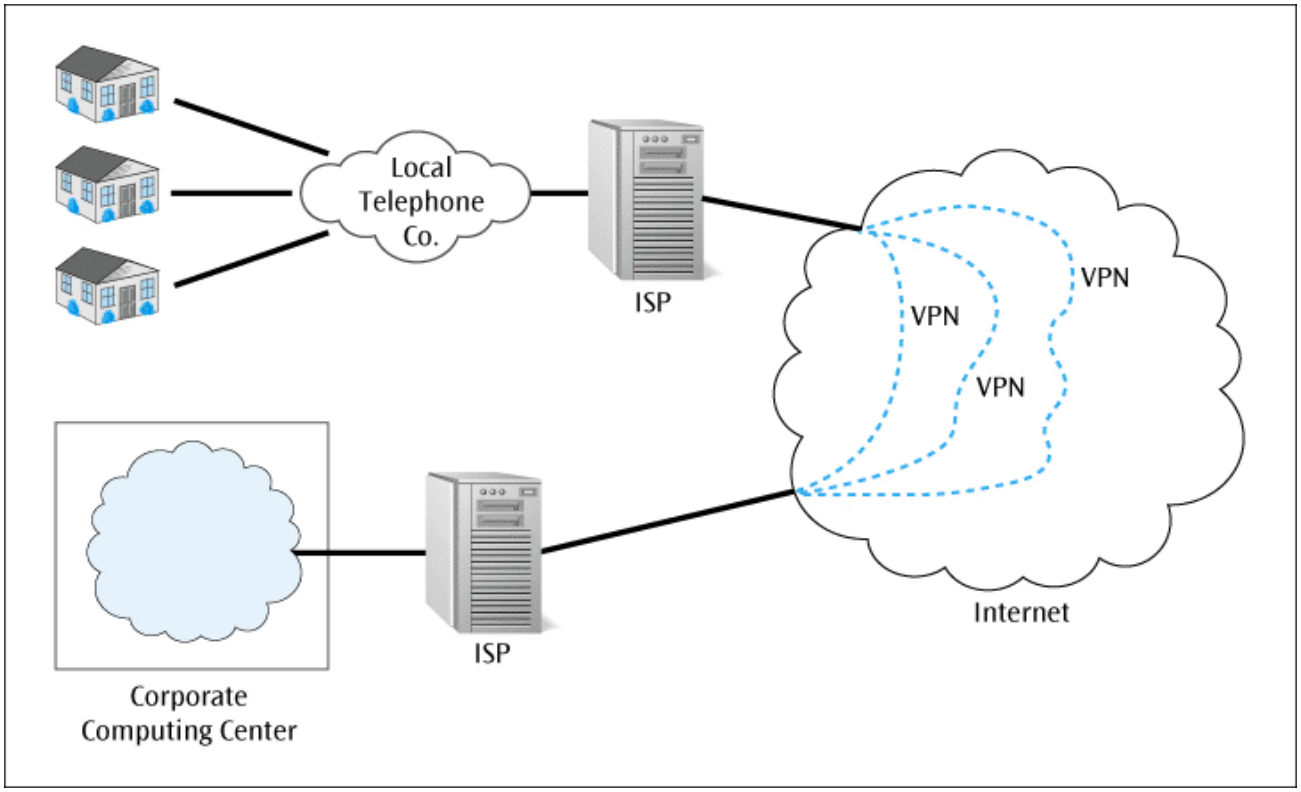


Figure 10-11
CompuCom's employees using a tunnel across the Internet into the corporate computing center

Summary

- To support Internet, many protocols, such as IP, TCP, ICMP, UDP, ARP, DHCP, and NAT, are necessary
- The Internet Protocol provides a connectionless transfer of data over a wide variety of networks
- There are currently two versions of IP: IPv4 and IPv6
- The Transmission Control Protocol (TCP) resides at the transport layer and provides an error-free, end-to-end connection
- The Internet Control Message Protocol (ICMP) performs error reporting for IP

Summary (continued)

- The User Datagram Protocol (UDP) provides a connectionless transport layer protocol in place of TCP
- The Address Resolution Protocol (ARP) translates an IP address into a CSMA/CD MAC address on a LAN
- The Dynamic Host Configuration Protocol (DHCP) allows a network to dynamically assign IP addresses to workstations as they are needed
- Network Address Translation (NAT) allows a network to replace local IP address with on global-type IP address

Summary (continued)

- Tunneling protocols allow a company to create virtual private network connections into a corporate computing system
- World Wide Web is vast collection of electronic documents containing text and images that can be accessed by simply clicking link within browser's Web page
- To locate document on Internet, you usually refer to its Uniform Resource Locator (URL)

Summary (continued)

- Internet consists of many commonly used network applications
- E-commerce is the buying and selling of goods and services electronically
- Cookies store state information on user's hard drive and provide a way for Web sites to track a user's Web-browsing patterns and preferences

Summary (continued)

- Intranet is in-house Internet with Web-like services that are available only to a company's employees or to customers and suppliers through an extranet
- The Internet continues to evolve with a completely new, higher-speed Internet2