CHAPTER 13:
Ethernet and TCP-IP Networking

The Architecture of Computer Hardware, Systems Software & Networking:

An Information Technology Approach

4th Edition, Irv Englander

John Wiley and Sons ©2010

Chapter Example

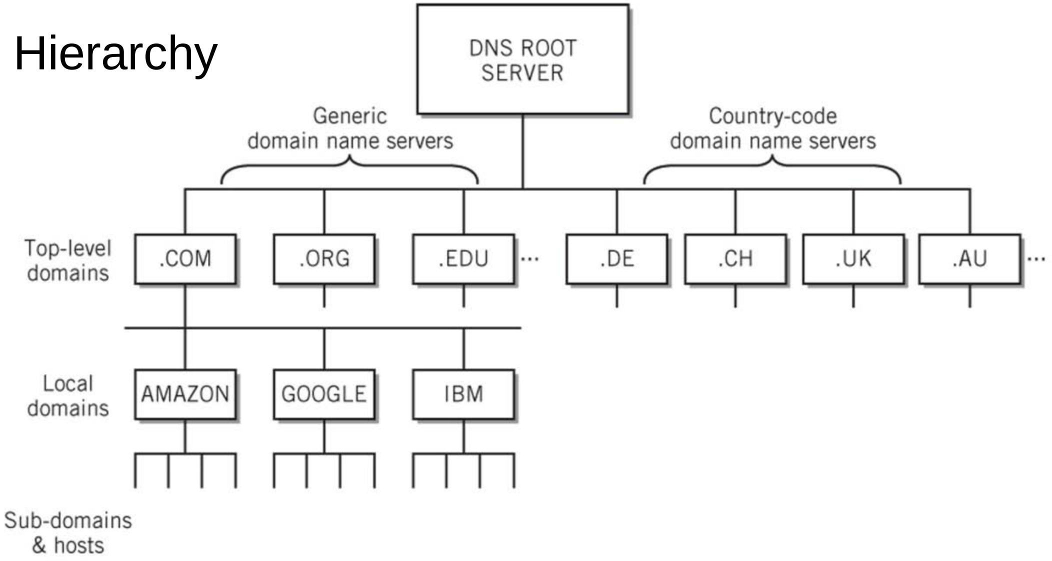
- User sitting at a computer types a URL that contains a domain name into a web browser
- First, HTTP client obtains the IP address of the Web server
- Then HTTP client initiates the process with a request to the TCP socket to establish a logical connection with the HTTP server at the destination site

Domain Names and DNS Services

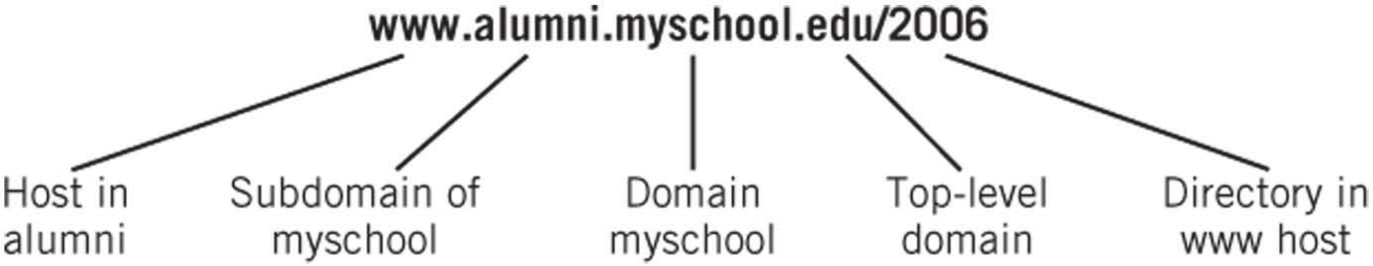
- Domain Names
  - Hierarchical system of network address identifiers used throughout the Internet and on local area networks, intranets and extranets
  - Created so users would not have to memorize IP addresses
- Domain Name System (DNS)
  - Domain name resolution – translates domain names into IP addresses
  - Uses a massive distributed database containing a directory system of servers
  - Each entry contains a domain name and an associated IP address

Domain Name System (DNS)

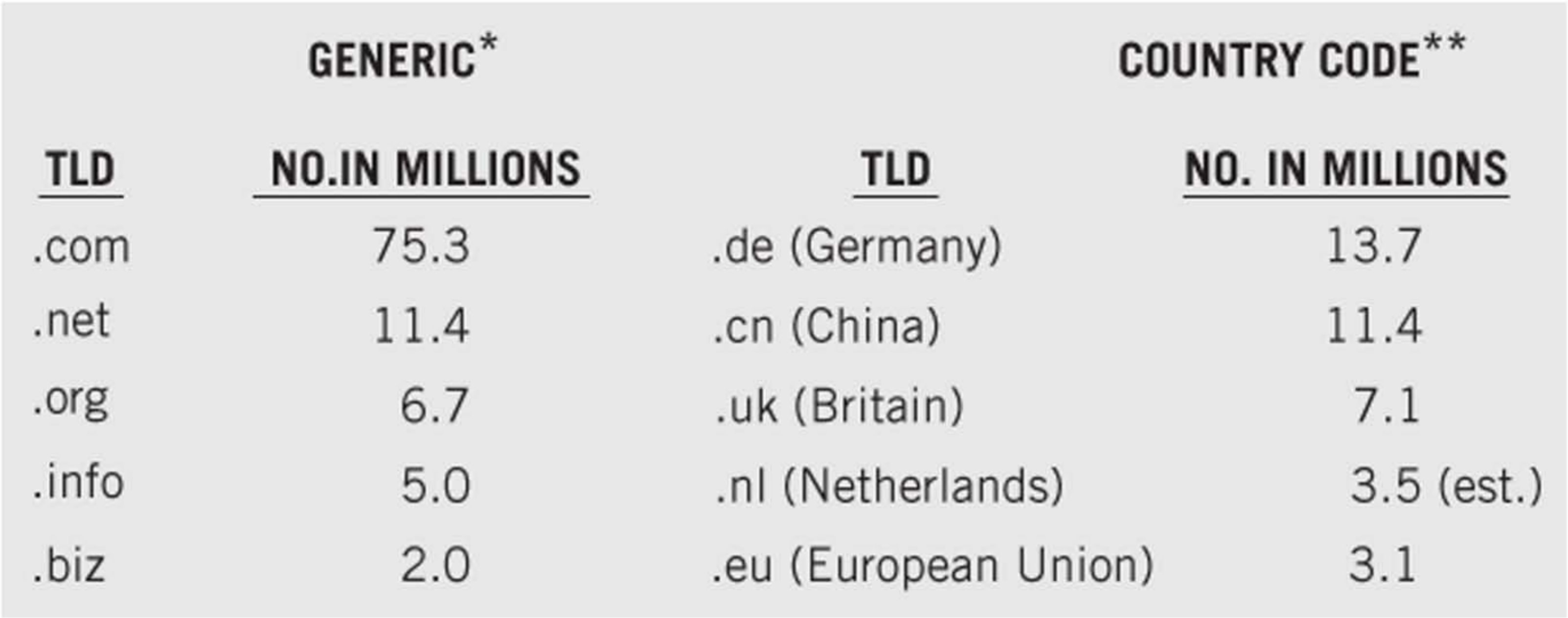
DNS Server Hierarchy



The Elements of a Domain Name

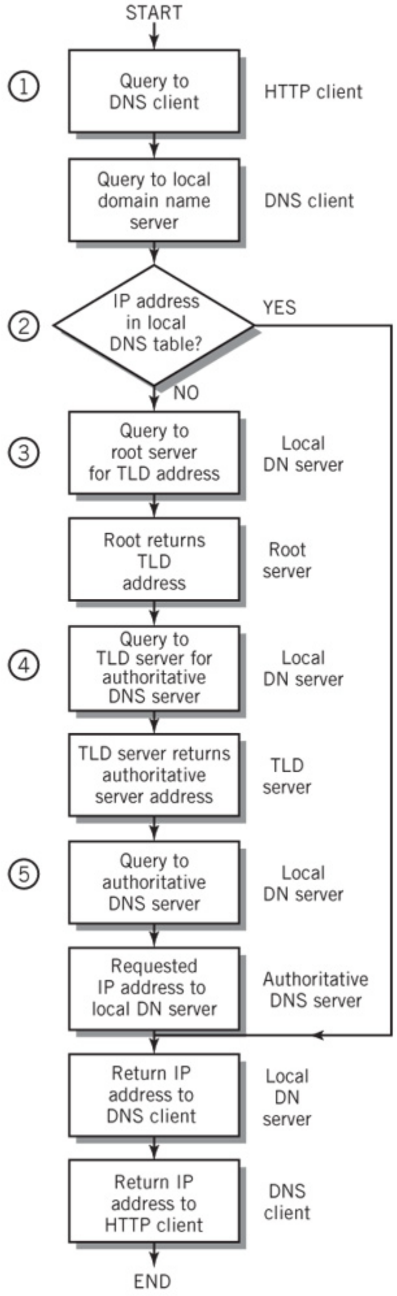


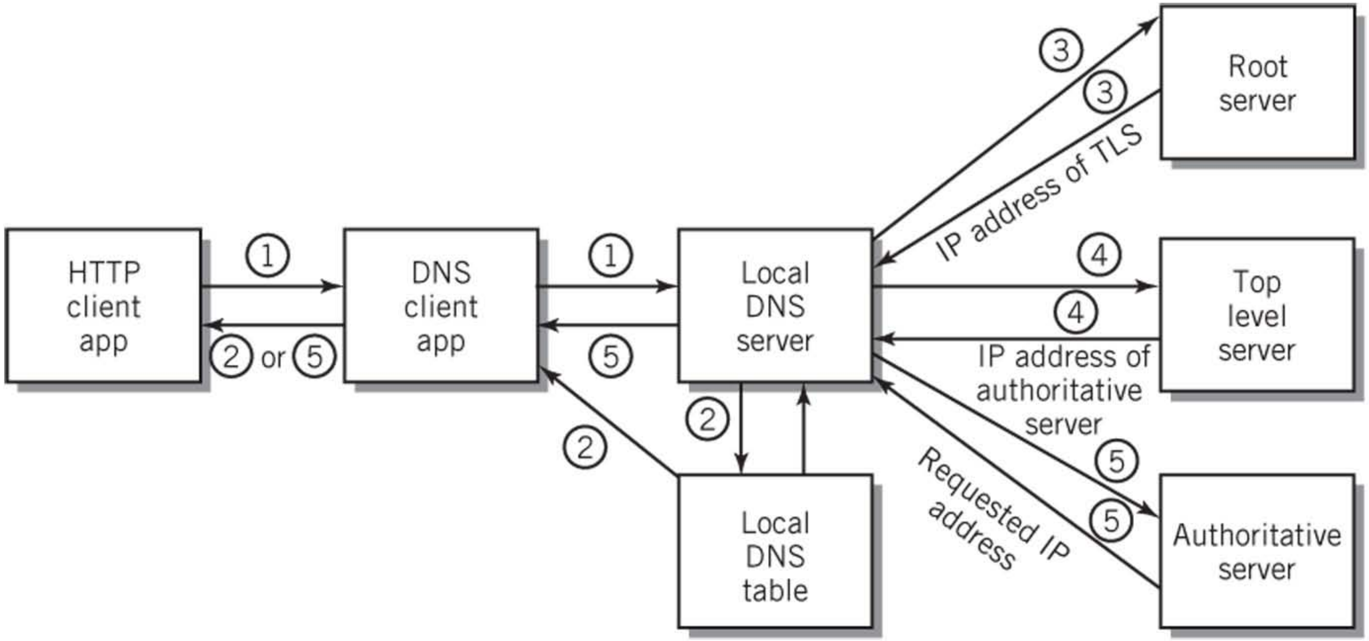
Top Domain Name Registrations



GENERIC*		COUNTRY CODE**	
TLD	NO.IN MILLIONS	TLD	NO. IN MILLIONS
.com	75.3	.de (Germany)	13.7
.net	11.4	.cn (China)	11.4
.org	6.7	.uk (Britain)	7.1
.info	5.0	.nl (Netherlands)	3.5 (est.)
.biz	2.0	.eu (European Union)	3.1

Domain Name Resolution

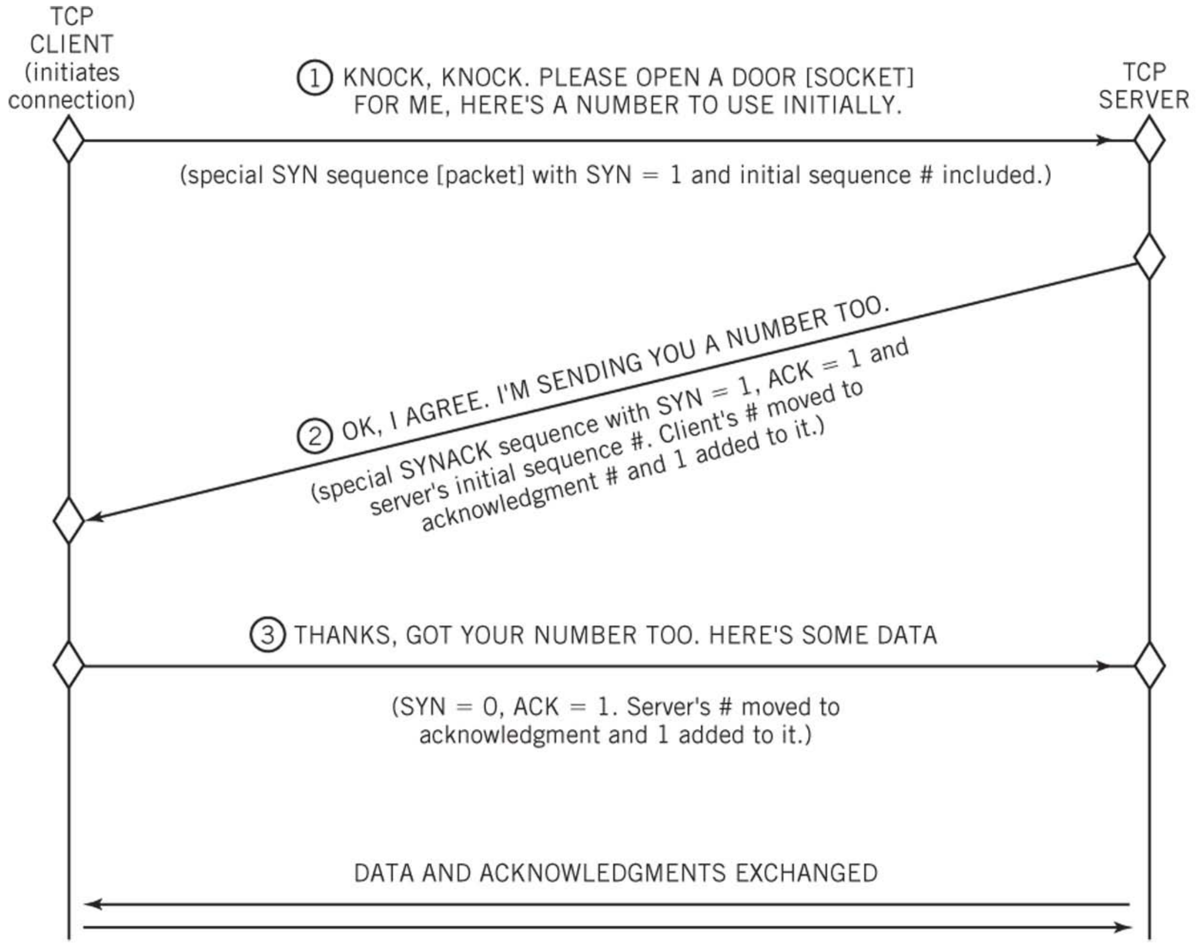

START
1
Query to DNS client
HTTP client
Query to local domain name server
DNS client
2
IP address in local DNS table?
YES
NO
3
Query to root server for TLD address
Local DN server
Root returns TLD address
Root server
4
Query to TLD server for authoritative DNS server
Local DN server
TLD server returns authoritative server address
TLD server
5
Query to authoritative DNS server
Local DN server
Requested IP address to local DN server
Authoritative DNS server
Return IP address to DNS client
Local DN server
Return IP address to HTTP client
DNS client
END



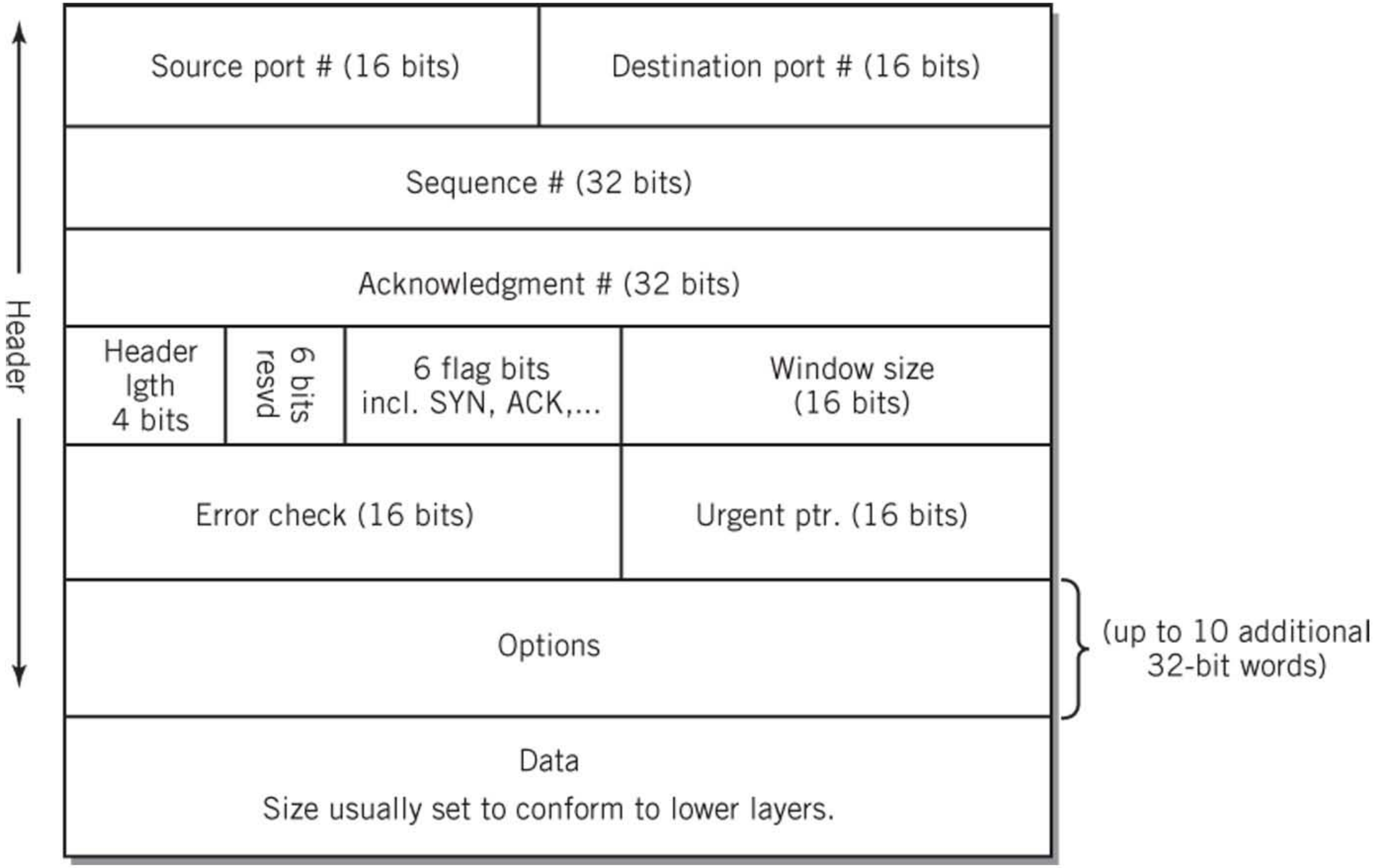
Transport Layer

- TCP protocol
  - Sends a packet to TCP at the destination site, requesting a connection
  - Handshaking – back and forth series of requests and acknowledgments
  - If handshaking negotiations are successful, a connection is opened
  - Connection is logically full-duplex

Three-Way TCP Connection Handshake


TCP
CLIENT
(initiates
connection)
TCP
SERVER
1 KNOCK, KNOCK. PLEASE OPEN A DOOR [SOCKET] FOR ME, HERE'S A NUMBER TO USE INITIALLY.
(special SYN sequence [packet] with SYN = 1 and initial sequence # included.)
2 OK, I AGREE. I'M SENDING YOU A NUMBER TOO.
(special SYNACK sequence with SYN = 1, ACK = 1 and server's initial sequence #. Client's # moved to acknowledgment # and 1 added to it.)
3 THANKS, GOT YOUR NUMBER TOO. HERE'S SOME DATA
(SYN = 0, ACK = 1. Server's # moved to acknowledgment and 1 added to it.)
DATA AND ACKNOWLEDGMENTS EXCHANGED

TCP Segment Format



Source port # (16 bits)

Destination port # (16 bits)

Sequence # (32 bits)

Acknowledgment # (32 bits)

Header lgth 4 bits

6 bits resvd

6 flag bits incl. SYN, ACK,...

Window size (16 bits)

Error check (16 bits)

Urgent ptr. (16 bits)

Options

(up to 10 additional 32-bit words)

Data

Size usually set to conform to lower layers.

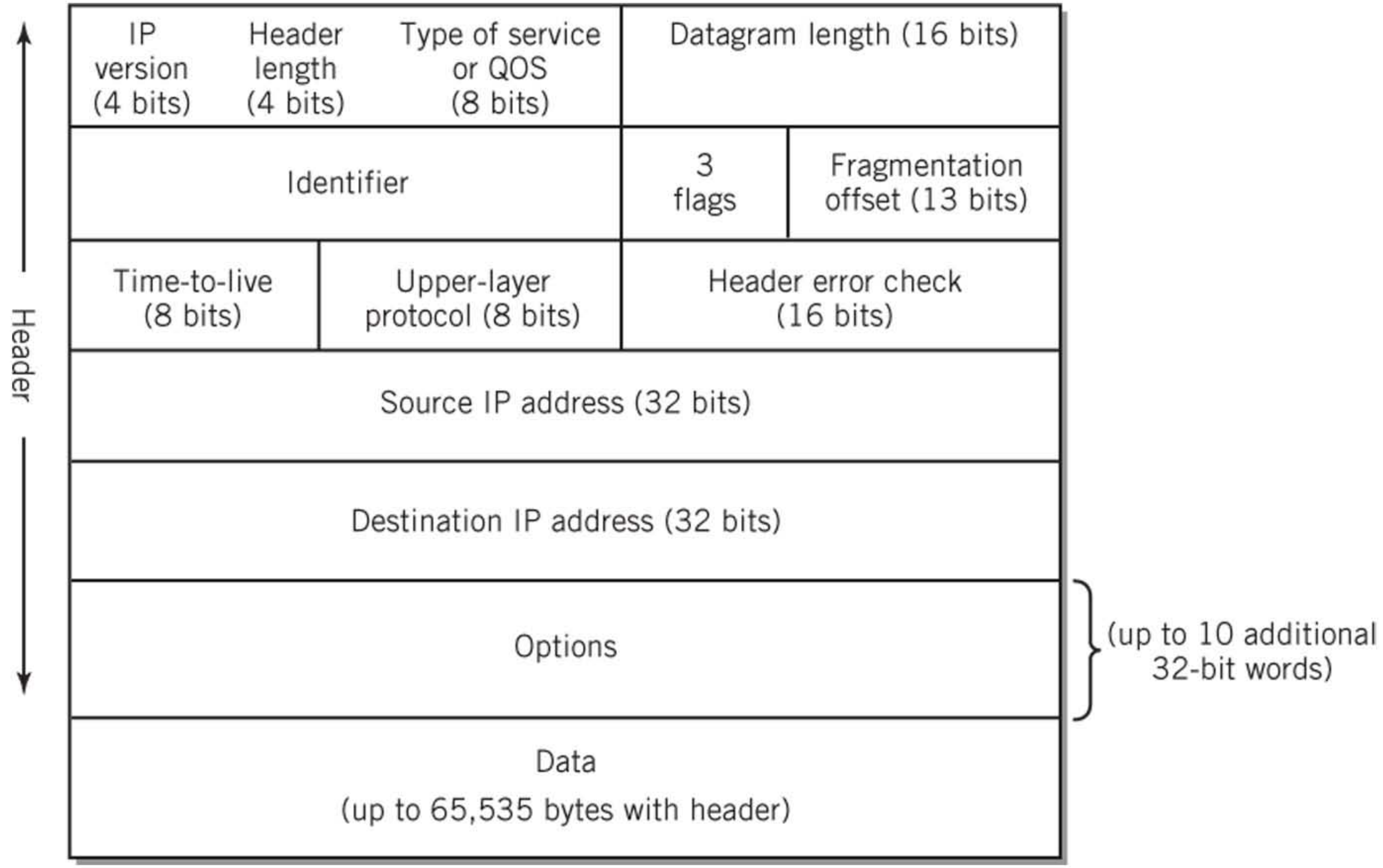
Network Layer

- IP protocol
  - Responsible for relaying packets from the source end node to the destination end node through intermediate nodes
  - Performed using datagram packet switching and logical IP addresses
  - Best-attempt unreliable service
  - Size of datagram ranges from 20 to 65,536 bytes
  - Header size between 20 and 60 bytes

IPv4 Addresses

- Registered and allocated by ICANN
- 32 bits long divided into 4 octets
- Assigned in blocks of contiguous addresses
  - Number of addresses is a power of two
- Divided into three levels
  - Network address
  - Subnetworks (subnets)
  - Hosts (nodes)
- Masks
  - Used to separate the different parts of the address

IPv4 Datagram Format



IP version (4 bits)

Header length (4 bits)

Type of service or QOS (8 bits)

Datagram length (16 bits)

Identifier

3 flags

Fragmentation offset (13 bits)

Time-to-live (8 bits)

Upper-layer protocol (8 bits)

Header error check (16 bits)

Source IP address (32 bits)

Destination IP address (32 bits)

Options

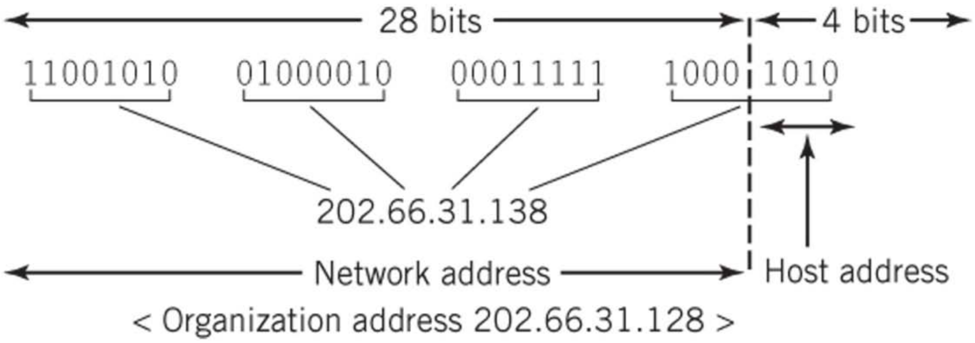
(up to 10 additional 32-bit words)

Data

(up to 65,535 bytes with header)

IP Addresses

IP Block Addresses



28 bits

4 bits

11001010 01000010 00011111 1000 1010

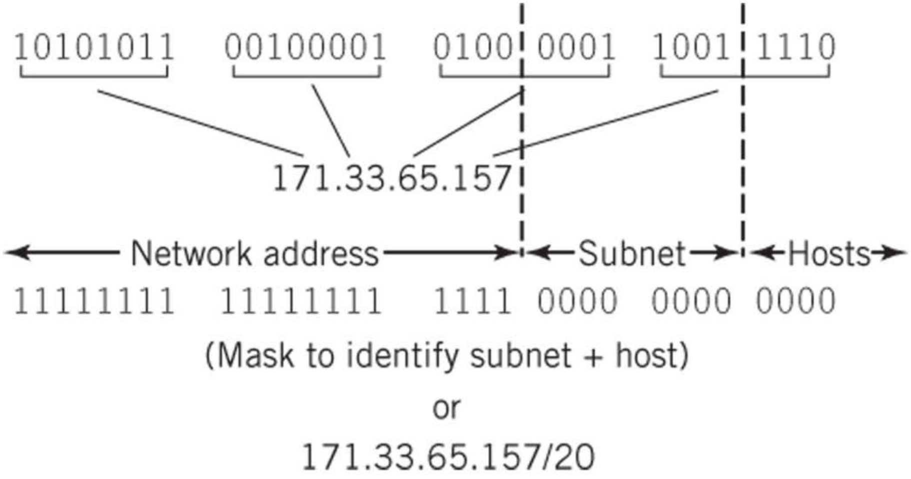
202.66.31.138

Network address

Host address

< Organization address 202.66.31.128 >

IP Hierarchy and Subnet Mask



10101011 00100001 0100 0001 1001 1110

171.33.65.157

Network address

Subnet

Hosts

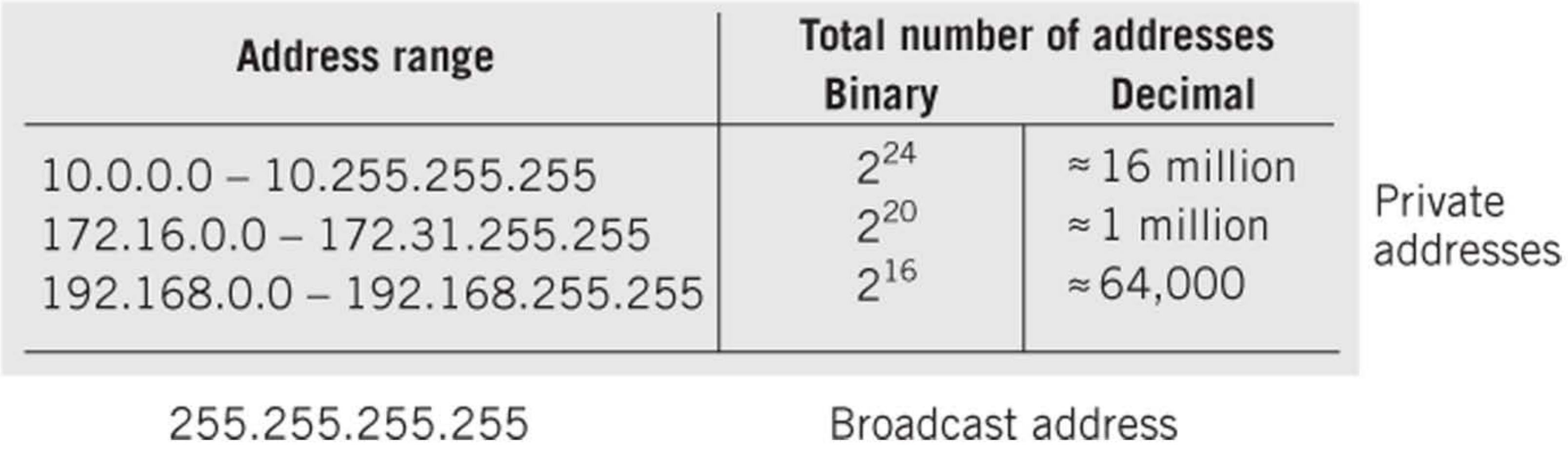
11111111 11111111 1111 0000 0000 0000

(Mask to identify subnet + host)

or

171.33.65.157/20

Resever IP Addresses



Address range	Total number of addresses		
	Binary	Decimal	
10.0.0.0 – 10.255.255.255	2^{24}	≈ 16 million	Private addresses
172.16.0.0 – 172.31.255.255	2^{20}	≈ 1 million	
192.168.0.0 – 192.168.255.255	2^{16}	≈ 64,000	

255.255.255.255 Broadcast address

DHCP

Two methods to distribute IP addresses more efficiently:

1. Use of private network IP addresses behind a router
   - The router must readdress traffic passing between the Internet and the local network
   - Management of readdressing becomes difficult with large networks
2. Dynamic Host Configuration Protocol (DHCP)
   - Maintain a bank of available IP addresses and assign them dynamically to computers for use when the computers are attached to the network
   - Method often used by large organizations, DSL and cable providers
   - DHCP client on computer or network device broadcasts a query to locate the DHCP server
   - DHCP server responds with a lease which includes an IP address, domain name of network, IP address of DNS server, subnet mask, IP address of gateway and other configuration parameters

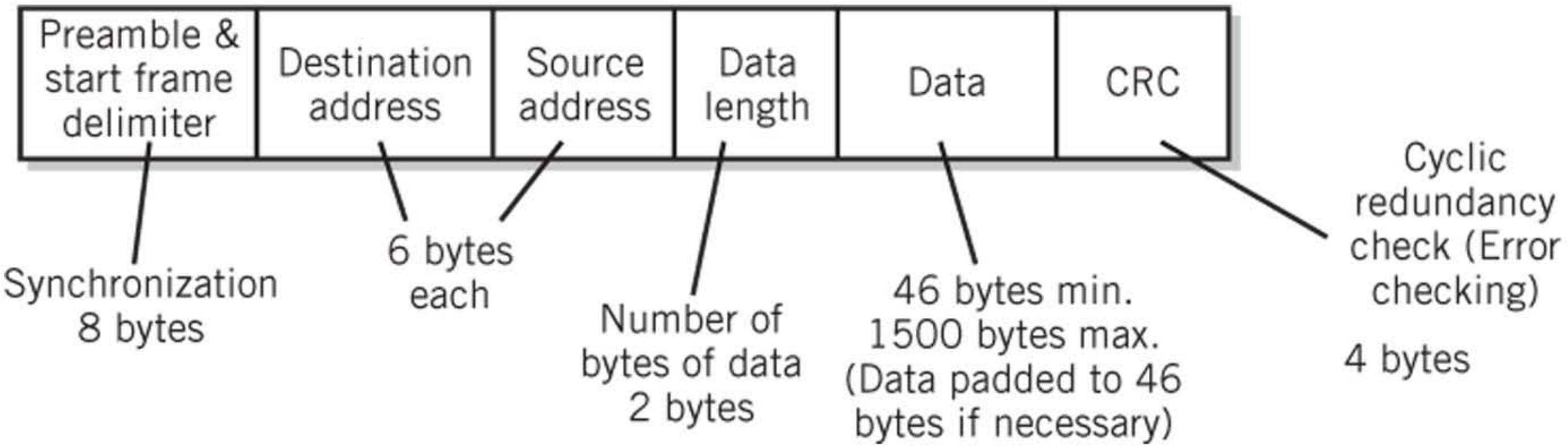
Operation of IP

- Two major functions
  - Routes datagrams from node to node until they reach their destination node
  - Translates IP addresses to physical addresses before it passes the packets to the data link later for delivery
- Address Resolution Protocol (ARP)
  - Implemented at the network layer
  - Translation of IP address to physical address at each intermediate node until destination is reached
  - A broadcast of the IP address is sent to every node on the network. The matching node responds with a physical address
  - Physical address (MAC address in the case of Ethernet) is sent in frame to the data link layer
  - At final destination, the packet is passed up to the transport layer for deployment to the application layer

Data Link Layer

- Layer responsible for transmitting a packet from one node to the next node
- Node access defined by the medium access control (MAC) protocol
  - Steer data to its destination
  - Detect errors
  - Prevent collisions
- Ethernet (CSMA-CD)
  - Predominant medium-access protocol for local area networks
  - Standard Ethernet packet is a frame (see next slide)

Ethernet Frame



Preamble & start frame delimiter

Destination address

Source address

Data length

Data

CRC

Synchronization
8 bytes

6 bytes
each

Number of
bytes of data
2 bytes

46 bytes min.
1500 bytes max.
(Data padded to 46
bytes if necessary)

Cyclic
redundancy
check (Error
checking)

4 bytes

Hub-Based Ethernet

- Simple means of wiring a bussed Ethernet together
- Logically still a bus network
- CSMA-CD
- Collision
  - Occurs when multiple nodes access the network in such a way that their messages become mixed and garbled
- Network propagation delay
  - Amount of time that it takes for one packet to get from one end of the network to the other
- Adequate for networks with light traffic

Switched Ethernet

- Permits point-to-point connection of any pair of nodes
- Multiple pairs can be connected simultaneously
- Possible to connect nodes in full-duplex mode
- Each pair of connections operates at the maximum bit rate of the network
- Why can’t there be any collisions in a switched Ethernet network?

Quality of Service (QoS)

1. Methods to reserve and prioritize channel capacity to favor packets that require special treatment
2. Service guarantees from contract carrier services that specify particular levels of throughput, delay and jitter
   - Jitter – variation in delay from packet to packet

- Differentiated service (DiffServ)
  - 8-bit (DS) field in IP header
  - Set by the application at the sender or by the first node
  - Diffserv capable nodes such as routers can then prioritize and route packets based on the packet class

Network Security Categories

1. Intrusion
   - Keeping network and system resources free from intruders
2. Confidentiality
   - Keeping the content of data private
3. Authentication
   - Verifying the identity of a source of data being received
4. Data integrity and non-repudiation
   - Protecting the content of data communication against changes and verifying the source of the message
5. Assuring network availability and access control
   - Keep network resources operational and restricting access to those permitted to use them

Network Security

- Network intrusions
  - Packet sniffers read data in a packet as it passes through a network
  - Probing attacks to uncover IP address / port numbers that accept data packets
- Physical and Logical Restriction
  - Limit access to wiring and network equipment
  - Firewall
  - Private networks
- Encryption
  - Symmetric key cryptography
    - Both key used for encryption and decryption
    - Both sender and receiver use the same key which makes security difficult
  - Public key cryptography
    - Two different keys are used for encryption and decryption

Alternative Protocols to TCP/IP

- MPLS (Multi-Protocol Label Switching)
  - Creates a virtual circuit over packet switched networks to improve forwarding speed of datagrams
- ATM (Asynchronous Transfer Mode)
  - Partial-mesh network technology in which data passes through the network in cells (53-byte packets)
- SONET (Synchronous Optical Network) and

  SDH (Synchronous Digital Hierarchy)
  - Protocol that uses fiber optic to create wide area networks with very high bit rates over long distances
- Frame Relay
  - Slow, wide area network standard