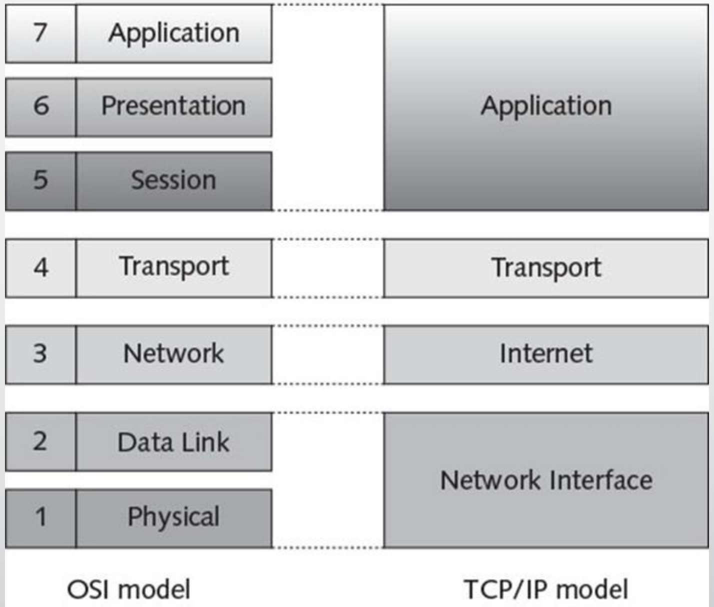
TCP /IP Fundamentals

Mr. Cantu

OSI Model and TCP/IP Model Comparison



	OSI model	TCP/IP model
7	Application	Application
6	Presentation	
5	Session	
4	Transport	Transport
3	Network	Internet
2	Data Link	Network Interface
1	Physical	

Figure 8-1 OSI model vs. TCP/IP model

TCP / IP Protocols (Application Layer)

- The TCP/IP subprotocols listed in this layer are services that support a number of network functions:
  - HTTP
  - DNS
  - DHCP
  - FTP
  - SNMP
  - Telnet
  - IMAP, SMTP, and POP

TCP / IP Addressing (Network layer)

- Internet Protocol Version 4 (IPv4)
  - 32 bits of data
  - Each address is divided into four groups called octets
    - Each octet contains 8 bits of data
  - Binary IP address example:
    - 10000000.00100110.00101100.11100010
  - Binary is difficult for people to understand

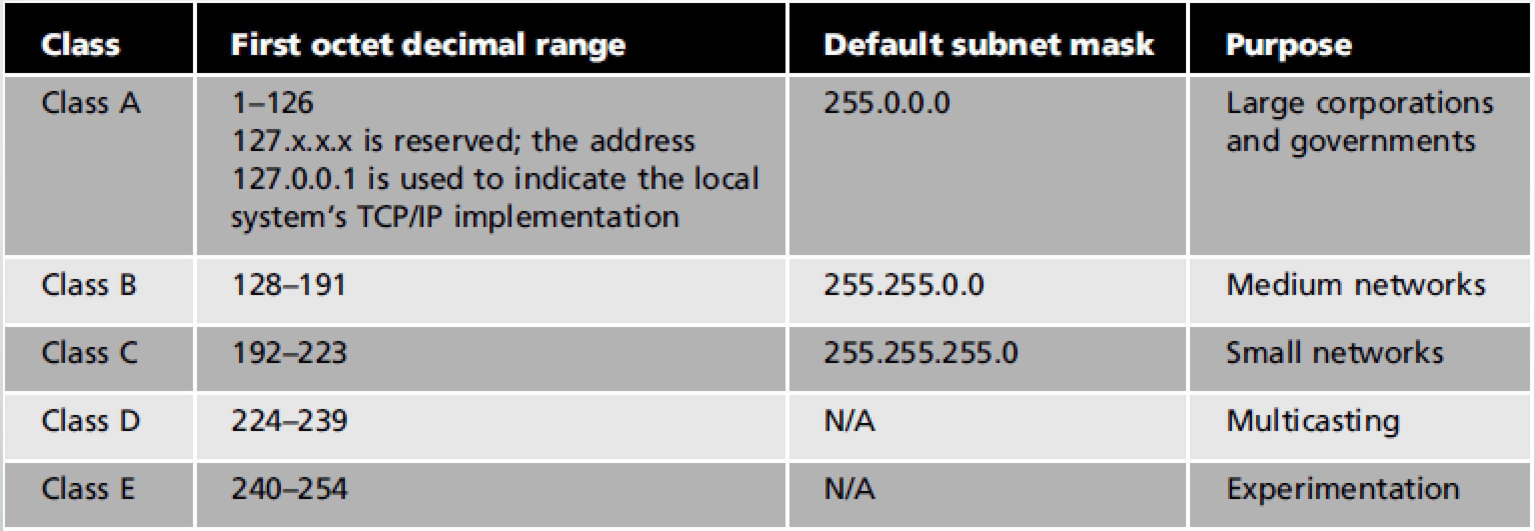
TCP / IP Addressing (Network layer) Cont.

- IP address consist of two parts:
  - Network Identifier - the part of an IP address shared among computers in a network segment
  - Host Identifier - is unique to each computer on the network segment
- Two identifiers are defined by another dotted decimal value called the **Subnet Mask**.

Network Address Translation (NAT)

- Translate your private network’s internal addresses into the address of the NAT server’s external interface connected to the Internet.
  - Private addresses are not routable on the Internet
  - Increase security
  - Used due to limited public addresses

IP Address Classes



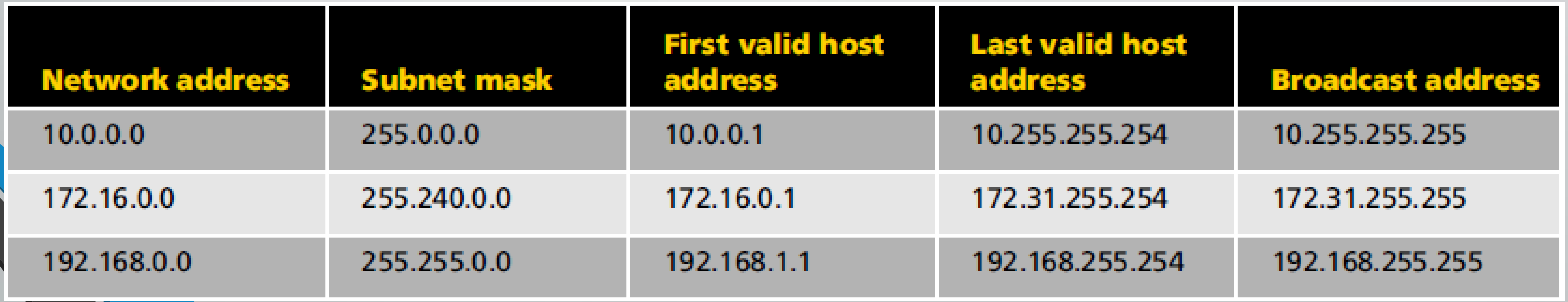
Class	First octet decimal range	Default subnet mask	Purpose
Class A	1–126 127.x.x.x is reserved; the address 127.0.0.1 is used to indicate the local system's TCP/IP implementation	255.0.0.0	Large corporations and governments
Class B	128–191	255.255.0.0	Medium networks
Class C	192–223	255.255.255.0	Small networks
Class D	224–239	N/A	Multicasting
Class E	240–254	N/A	Experimentation

IP Address Classes Cont.

- Class A addresses
  - 8 bits for the network portion of the address and 24 bits for the host
- Class B addresses
  - 16 bits for the network portion of the address and 16 bits for the host
- Class C addresses
  - 24 bits for the network portion of the address and 8 bits for the host

Private IP Address Ranges

- To obtain a public IP address, individuals and organizations must register and pay a fee for each address.
- RFC (Request for Comments) 1918 defined ranges of reserved private IP addresses
- Lowest address -> Network Address Highest -> Broadcast Address



Network address	Subnet mask	First valid host address	Last valid host address	Broadcast address
10.0.0.0	255.0.0.0	10.0.0.1	10.255.255.254	10.255.255.255
172.16.0.0	255.240.0.0	172.16.0.1	172.31.255.254	172.31.255.255
192.168.0.0	255.255.0.0	192.168.1.1	192.168.255.254	192.168.255.255

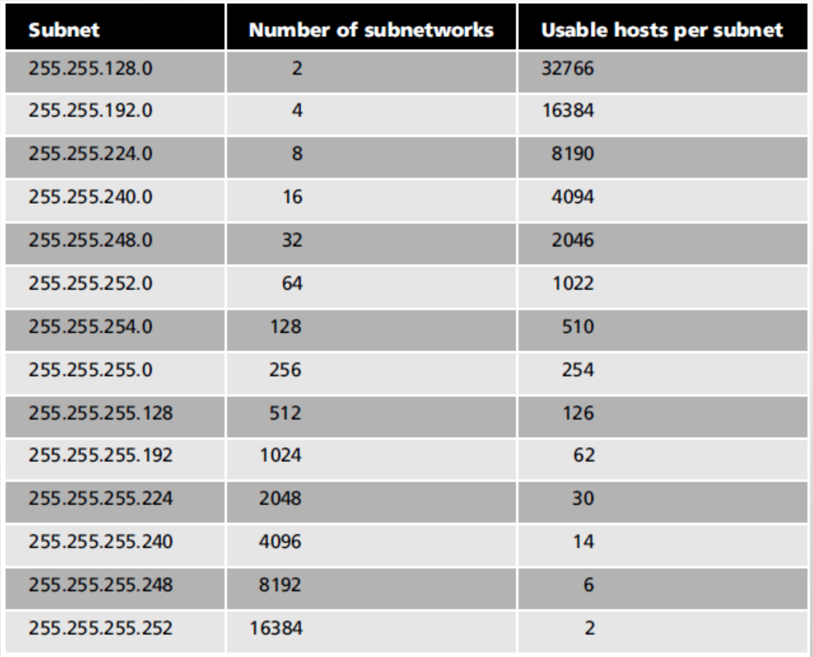
Subnetting

- Subnetting is used to segment internal networks logically
- Can also be used for the following:
  - Mirroring the organization’s physical layout
  - Mirroring the organization’s administrative structure
  - Planning for future growth
  - Reducing and controlling network traffic
  - Increasing network security

Subnetting Cont.

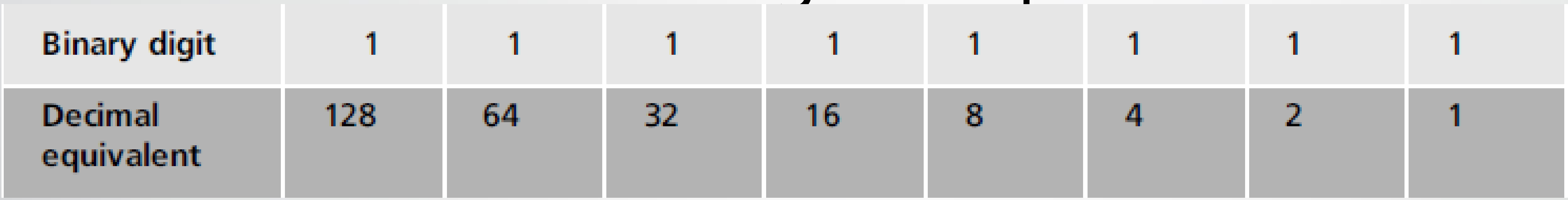
- Bits borrowed from the host portion of the IP address to make a set of subnetworks
- Some addresses are lost
- Calculated in binary

Subnetting Class B table



Subnet	Number of subnetworks	Usable hosts per subnet
255.255.128.0	2	32766
255.255.192.0	4	16384
255.255.224.0	8	8190
255.255.240.0	16	4094
255.255.248.0	32	2046
255.255.252.0	64	1022
255.255.254.0	128	510
255.255.255.0	256	254
255.255.255.128	512	126
255.255.255.192	1024	62
255.255.255.224	2048	30
255.255.255.240	4096	14
255.255.255.248	8192	6
255.255.255.252	16384	2

Subnetting Example



Binary digit	1	1	1	1	1	1	1	1
Decimal equivalent	128	64	32	16	8	4	2	1

Number of Subnets = $2^{\text{Number of Subnet Bits or 1s}}$
Number of Valid Hosts = $2^{\text{Number of Host Bits or 1s}} – 2$

Example:

192.168.1.0
255.255.255.240 (/28)
11111111.11111111.11111111.11110000

Subnetting Example Cont.

192.168.1.0 -> is a class C address

255.255.255.240 (/28) <- is the number of 1s

11111111.11111111.11111111.11110000

Never Changes	Never Changes	Never Changes	Subnet Bits	Host Bits

Number of Subnets = 2^4 = (2x2x2x2) = 16

Number of Valid Hosts = 2^4 = 16 – 2 =14

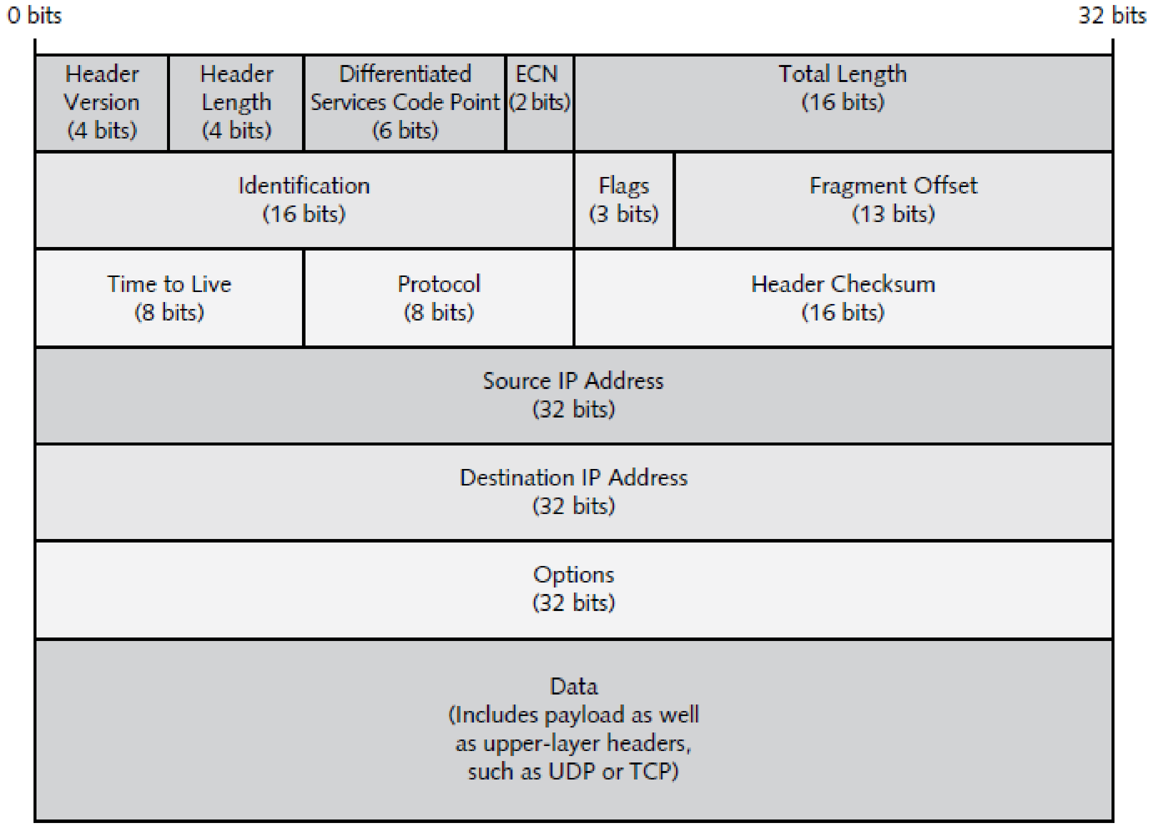
Unicast, Multicasting, and Broadcasting

- unicast transmission, one packet is sent from a server computer to each client computer that requests a file or an application, such as a streaming video presentation.
- multicast transmission means the server can treat all five clients as a group and send one transmission that reaches all of them.
- broadcast sends a communication to all points on a specific network.
  - Flooded broadcasts are sent to any subnet.
  - Directed broadcasts are sent to a specific subnet

IPv4 in Detail

- The portion of the packet that IP is responsible for routing through networks is called an **IP datagram**.
  - Network of OSI model
  - Divided into sections
    - Header, data, and footer

IP Header Structure



0 bits 32 bits

<table>
<tr><td colspan="4">Header Version (4 bits)</td><td colspan="4">Header Length (4 bits)</td><td colspan="6">Differentiated Services Code Point (6 bits)</td><td colspan="2">ECN (2 bits)</td><td colspan="16">Total Length (16 bits)</td></tr>
<tr><td colspan="16">Identification (16 bits)</td><td colspan="3">Flags (3 bits)</td><td colspan="13">Fragment Offset (13 bits)</td></tr>
<tr><td colspan="8">Time to Live (8 bits)</td><td colspan="8">Protocol (8 bits)</td><td colspan="16">Header Checksum (16 bits)</td></tr>
<tr><td colspan="32">Source IP Address (32 bits)</td></tr>
<tr><td colspan="32">Destination IP Address (32 bits)</td></tr>
<tr><td colspan="32">Options (32 bits)</td></tr>
<tr><td colspan="32">Data (Includes payload as well as upper-layer headers, such as UDP or TCP)</td></tr>
</table>

IP Header Structure

- **Header Version:** 4-bit field identifies the IP version
- Header Length: length of the header in 32-bit words, and is a 4-bit value
- **Differential Services Code Point (DSCP):** This 6-bit field expresses the quality of service
- **Explicit Congestion Notification (ECN):** 2-bit field allows ECN-compliant routers on ECN-compliant network infrastructures to signal congestion minimize dropping of packets.
- **Total Length:** 16-bit field specifies the datagram’s total length to a maximum of 65,535 bytes
- **Identification:** 16-bit value helps divide the data stream into packets
  - receiving computer reassembles packets in correct order

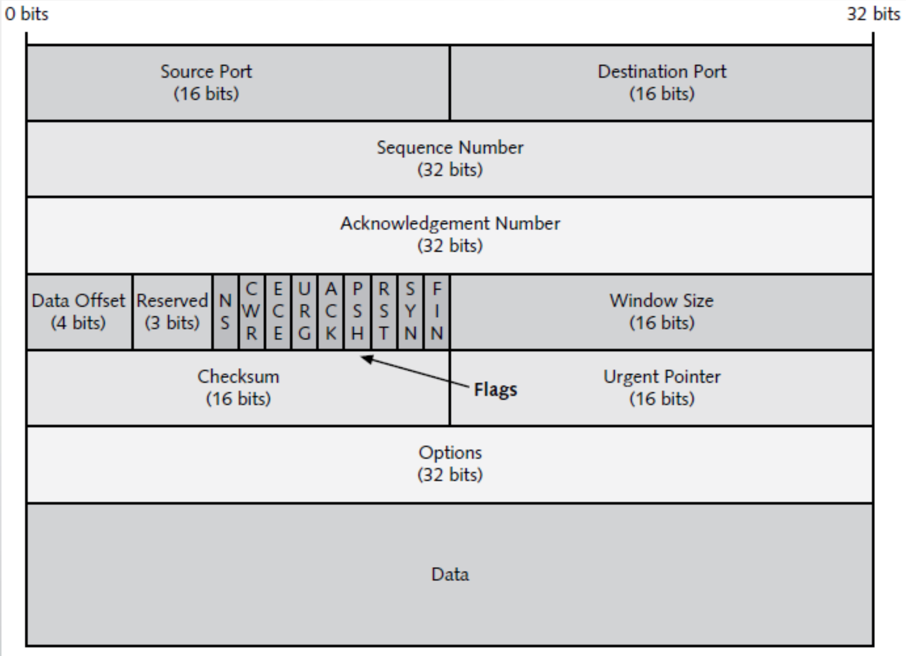
IP Header Structure Cont.

- **Flags:** 3-bit value indicates whether the datagram is a fragment
- **Fragment Offset:** this value indicates where the fragment belongs in the sequence
- **Time to Live (TTL):** 8-bit value identifies the maximum amount of time the packet can remain in a network before it is dropped
- **Protocol:** type of protocol being carried
  - 1 = ICMP
  - 6 = TCP
  - 17 = UDP
- **Header Checksum:** Sum of the 16-bit values in the datagram header; it is calculated at every hop to ensure accuracy
- **Source IP Address:** device that sent the IP datagram
- **Destination IP Address:** that received the IP datagram
- **Options:** security field and several source routing fields

ICMP Messages

- Internet Control Message Protocol (ICMP) is designed to assist TCP/IP networks with troubleshooting communication problems.
  - Ping commands
  - ICMP Codes - https://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml

TCP Headers



0 bits

32 bits

Source Port
(16 bits)

Destination Port
(16 bits)

Sequence Number
(32 bits)

Acknowledgement Number
(32 bits)

Data Offset
(4 bits)

Reserved
(3 bits)

NS

CWR

ECE

URG

ACK

PSH

RST

SYN

FIN

Window Size
(16 bits)

Checksum
(16 bits)

Flags

Urgent Pointer
(16 bits)

Options
(32 bits)

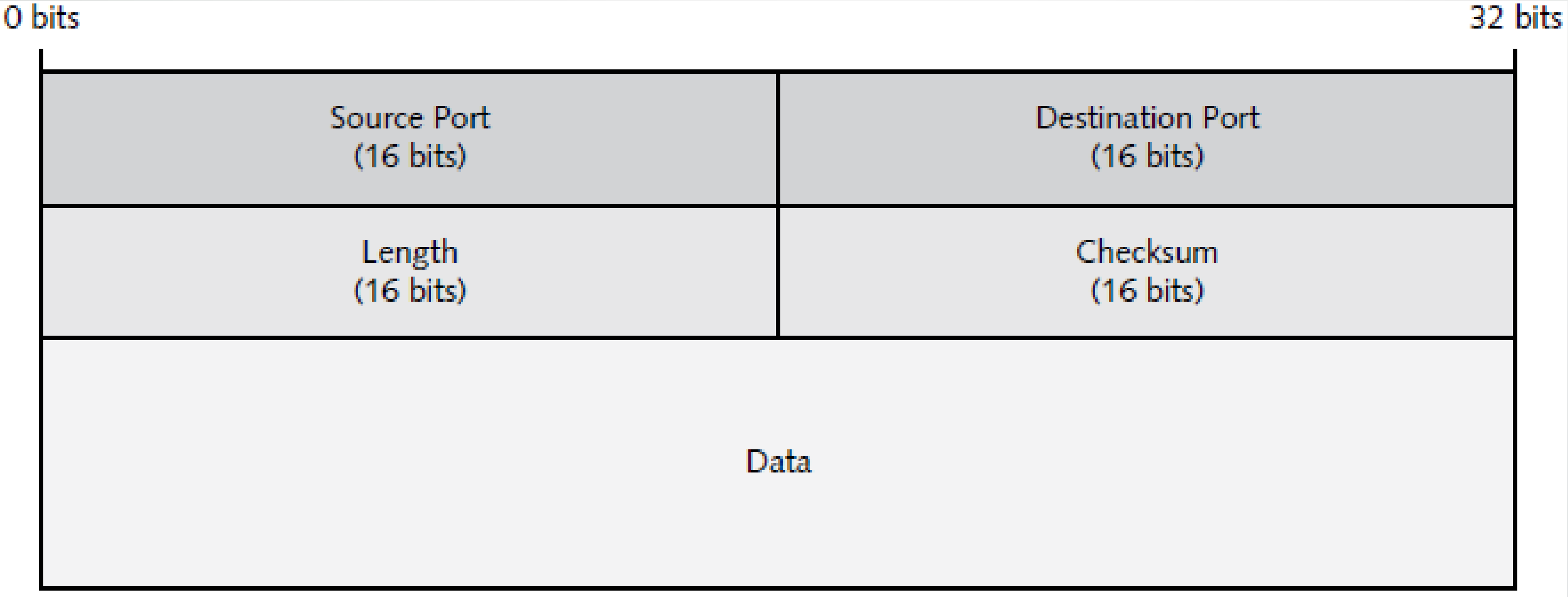
Data

TCP Flags

- NS (Nonce Sum)—Associated with ECN
- CWR (Congestion Window Reduced)—Associated with ECN
- ECE (ECN Echo)—Associated with ECN
- URG (Urgent)—When set to 1, data should be considered significant
- ACK (Acknowledgement)—Indicates that the previous packet was received
- PSH (Push)—Forces TCP to deliver data rather than buffer it on the receiver
- RST (Reset)—Resets the connection
- SYN (Synchronize)—Synchronizes the sequence numbers
- FIN (Finish)—Indicates that no more data will come from the sender

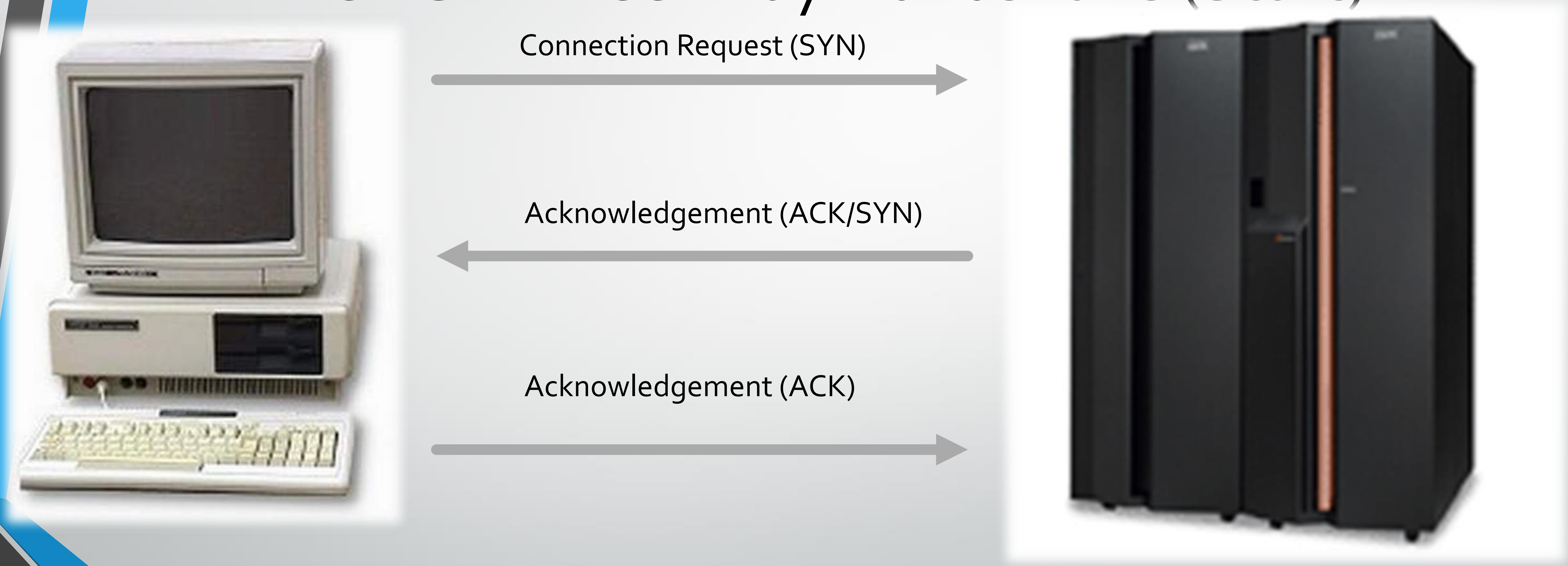
UDP Headers

- User Datagram Protocol (UDP), like TCP, is processed at the Transport layer of the OSI model.
- Considered unreliable because it is connectionless.
  - Real time streaming, speed over reliability



0 bits	32 bits
Source Port (16 bits)	Destination Port (16 bits)
Length (16 bits)	Checksum (16 bits)
Data	

The TCP Three-Way Handshake (Start)

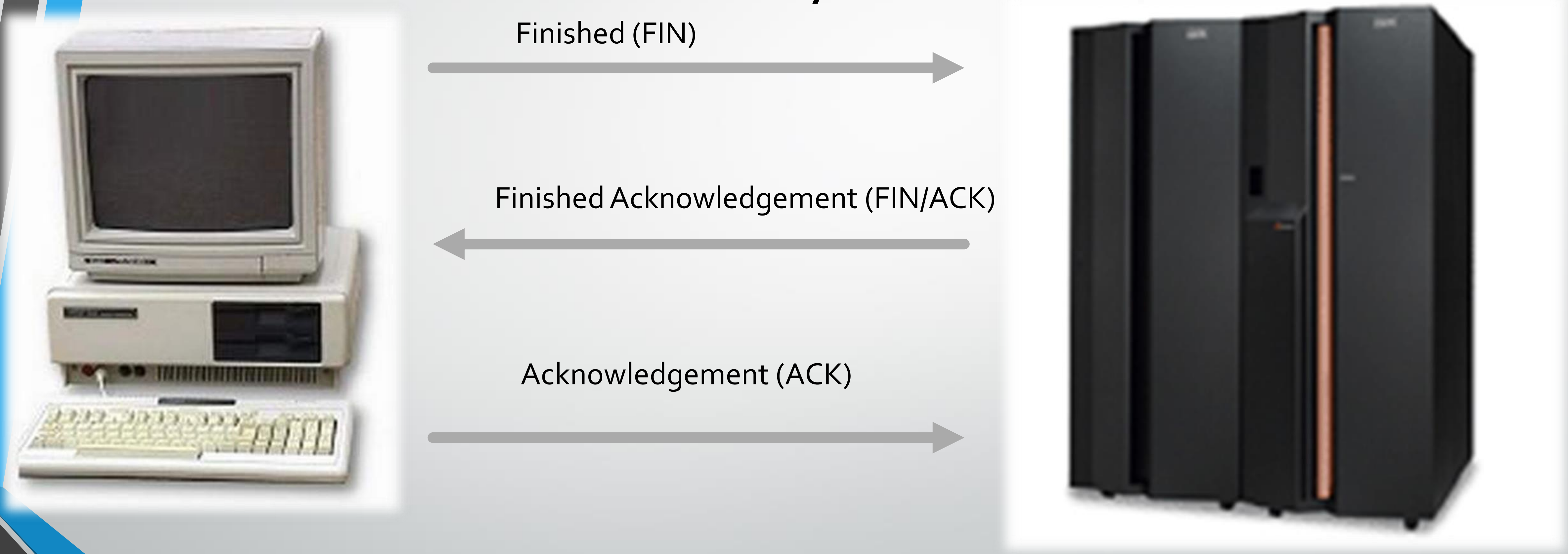


Connection Request (SYN)

Acknowledgement (ACK/SYN)

Acknowledgement (ACK)

The TCP Three-Way Handshake (End)



Finished (FIN)

Finished Acknowledgement (FIN/ACK)

Acknowledgement (ACK)

What would happen if you send a SYN and FIN at the start of the connection?