CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

CECS 303: Networks and Network Security

Network Overview (cont'd)

Chris Samayoa

Week 3 – 1st Lecture
2/1/2022

Course Information

CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

- CECS 303
  - Networks and Network Security – 3.0 units
- Class meeting schedule
  - TuTH 5:00PM to 7:15PM
  - Lecture Room: VEC 402
  - Lab Room: ECS 413
- Class communication
  - chris.samayoa@csulb.edu
  - Cell: 562-706-2196
- Office hours
  - Thursdays 4pm-5pm
  - Other times by appointment only

Common Network Uses

- E-mail
- Printer sharing
- File sharing
- Internet access and website delivery
- Remote access capabilities
- Voice (telephone) and video services
- Network management
- Network and host monitoring

File and Print Services

- File services
  - Capability of server to share data file, applications, and disk storage space
- A file server provides file services
- File services provided the foundational need for networking
- Print services
  - Share printers across network
  - Saves time and money – particularly for an organization

Access Services

- Allow a remote user access to internal network resources
- Remote user
  - Computer user on a different network and/or in a different geographical location from LAN's servers
- Allow network users to connect to machines outside of their LAN
- Operating systems include many built-in access services
- Allows external administrators to diagnose and troubleshoot network issues
- Can provide "local" desktop access to remote users

Mail Servers

- Host responsible for e-mail storage and transfer of messages
- Additional tasks of mail servers
  - Intercept spam
  - Handle objectionable content
  - Route messages according to rules
  - Provide Web-based client for checking e-mail
  - Notify administrators or users if certain events occur
  - Schedule e-mail transmission, retrieval, storage, maintenance
  - Communicate with mail servers on other networks
- Specialized software is needed in order to function as a mail server

Internet Services

- Web server
  - Host running specialized software that allows it to serve web pages to various clients
- Other network services
  - File transfer capabilities
  - Internet addressing schemes
  - Security filters
  - Means for directly logging on to other networked computers

Management Services

- Traffic monitoring and control
- Load balancing
- Hardware diagnosis and failure alert
- Asset management
- License tracking
- Security auditing
- Address management
- Backup and restoration of data

CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

CECS 303: Networks and Network Security

TCP/IP

Chris Samayoa

Week 3 – 1st Lecture
2/1/2022

Objectives

- Identify and explain the functions of the core TCP/IP protocols
- Explain the TCP/IP model and how it corresponds to the OSI model
- Discuss addressing schemes for TCP/IP in IPv4 and IPv6

TCP/IP Model

- Four Layers
  - Application layer
  - Transport layer
  - Internet layer
  - Network access layer (or Link layer)

TCP/IP Model (cont'd)

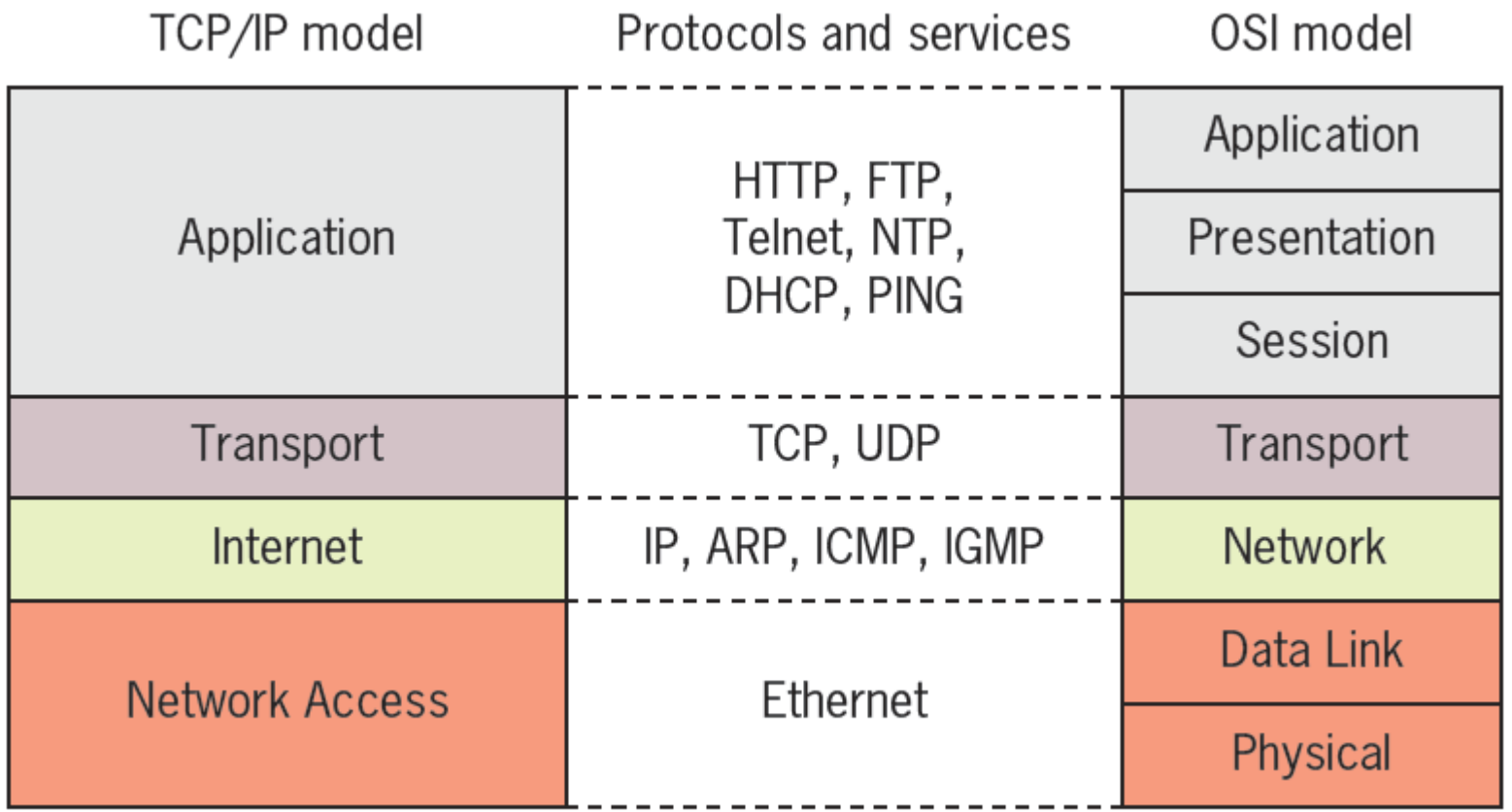

Image: Course Technology / Cengage learning

TCP/IP Overview

- TCP/IP = Transmission Control Protocol / Internet Protocol
- Protocol Suite
  - Commonly referred to as “IP” or “TCP/IP”
  - Subprotocols include TCP, IP, UDP, and ARP
  - Internet layer
  - Network access layer (or Link layer)
- Developed by US Department of Defense
  - Specifically DARPA (Defense Advanced Research Projects Agency)
  - ARPANET (developed in late 1960s) was precursor to TCP/IP protocol suite and internet as a whole

Advantages of TCP/IP

- Open Standard
  - Available on IETF website as RFCs
- Flexible
  - Runs on virtually any platform
  - Connects dissimilar operating systems and devices
- Routable
  - Transmissions carry Network layer addressing information
  - Suitable for small AND large networks

TCP/IP Core

- TCP/IP suite subprotocols
- Mainly operates in Transport or Network layers of OSI model
- Provide basic services to protocols in other layers
- Most significant protocols in TCP/IP suite
  - TCP
  - IP

TCP

- TCP = Transmission Control Protocol
  - Transport layer protocol
- Provides reliable data delivery services
  - Connection-oriented subprotocol
    - Establish connection before transmitting
- Uses sequencing and checksums
- Provides flow control
- TCP segment format
  - Encapsulated by IP packet in Network layer
    - Becomes IP packet's "data"

A TCP Segment

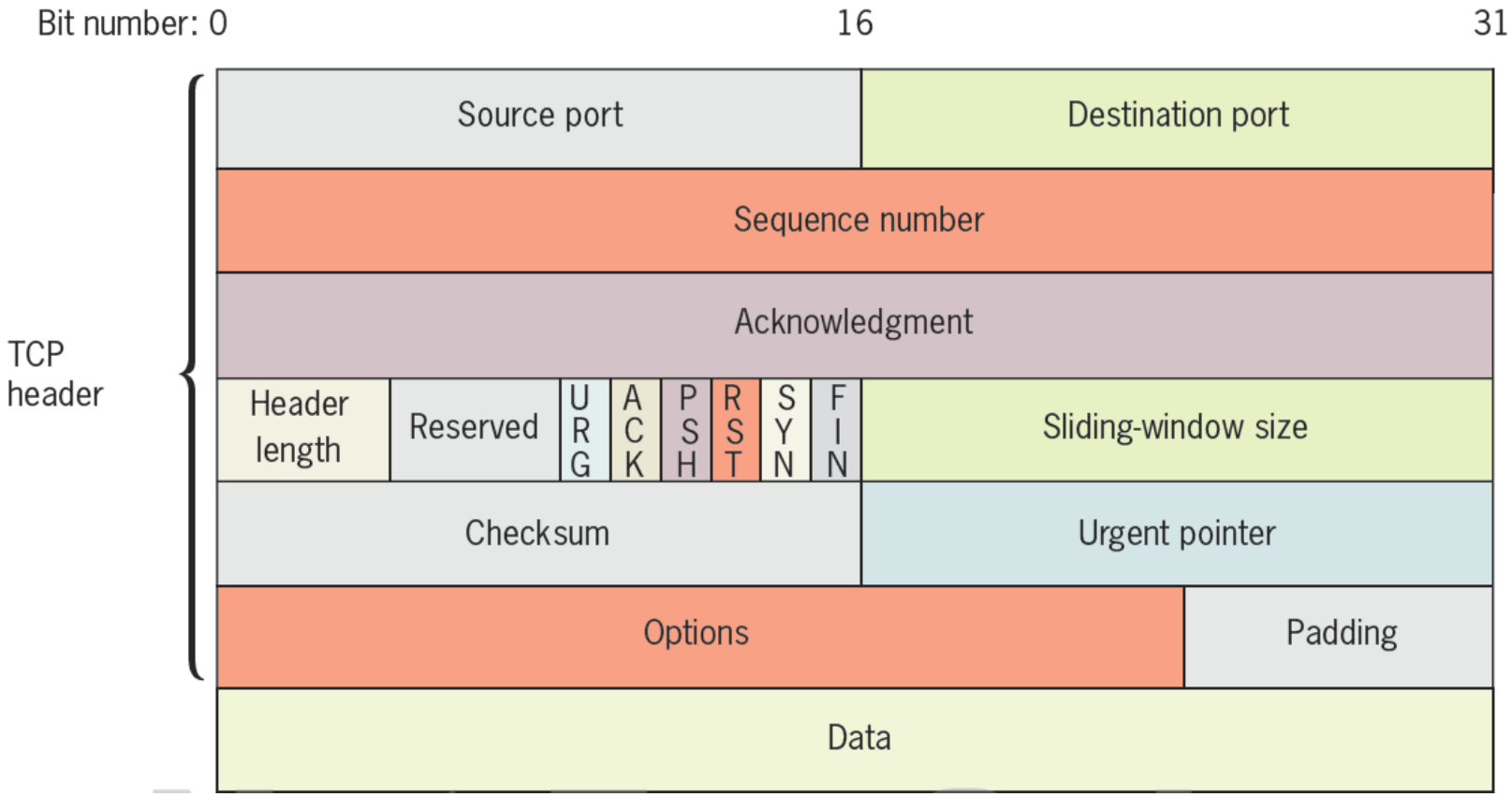

Image: Course Technology / Cengage learning

TCP Segment Fields

Field	Length	Function
Source port	16 bits	Indicates the port number at the source node. A **port number** is the address on a host where an application makes itself available to incoming or outgoing data.
Destination port	16 bits	Indicates the port number at the destination node.
Sequence number	32 bits	Identifies the data segment's position in the stream of data segments already sent.
Acknowledgment number (ACK)	32 bits	Confirms receipt of the data via a return message to the sender.
TCP header length	4 bits	Indicates the length of the TCP header.
Reserved	6 bits	A field reserved for later use.
Flags	6 bits	A collection of six 1-bit fields that signal special conditions through flags. The following flags are available for the sender's use: • URG—If set to *1*, the Urgent pointer field contains information for the receiver. • ACK—If set to *1*, the Acknowledgment field contains information for the receiver. (If set to *0*, the receiver will ignore the Acknowledgment field.) • PSH—If set to *1*, it indicates that data should be sent to an application without buffering. • RST—If set to *1*, the sender is requesting that the connection be reset. • SYN—If set to *1*, the sender is requesting a synchronization of the sequence numbers between the two nodes. This code is used when TCP requests a connection to set the initial sequence number. • FIN—If set to *1*, the segment is the last in a sequence and the connection should be closed.
Sliding-window size (or window)	16 bits	Indicates how many bytes the sender can issue to a receiver while acknowledgment for this segment is outstanding. This field performs flow control, preventing the receiver from being deluged with bytes. For example, suppose a server indicates a sliding window size of 4000 bytes. Also suppose the client has already issued 1000 bytes, 250 of which have been received and acknowledged by the server. That means that the server is still buffering 750 bytes. Therefore, the client can only issue 3250 additional bytes before it receives acknowledgment from the server for the 750 bytes.
Checksum	16 bits	Allows the receiving node to determine whether the TCP segment became corrupted during transmission.
Urgent pointer	16 bits	Indicates a location in the data field where urgent data resides.
Options	0–32 bits	Specifies special options, such as the maximum segment size a network can handle.
Padding	Variable	Contains filler information to ensure that the size of the TCP header is a multiple of 32 bits.
Data	Variable	Contains data originally sent by the source node. The size of the Data field depends on how much data need to be transmitted, the constraints on the TCP segment size imposed by the network type, and the limitation that the segment must fit within an IP packet.

Image: Course Technology / Cengage learning

TCP Segment Capture

CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

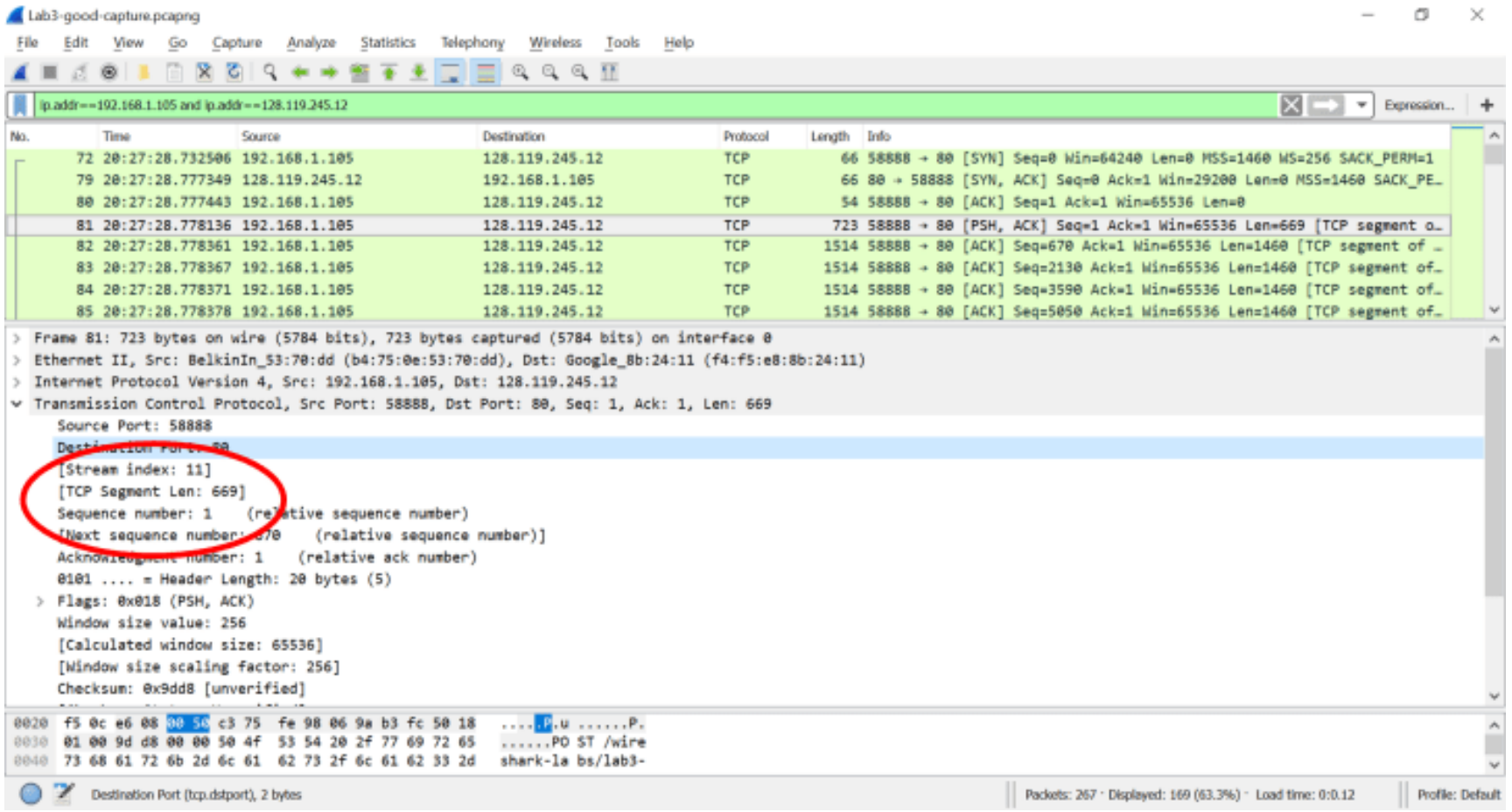

Image: MadPackets *(https://madpackets.com/2018/04/25/tcp-sequence-and-acknowledgement-numbers-explained/)*

TCP 3-Way Handshake

- Three segments establish a connection
- Host A issues message to Host B
  - Sends segment with SYN bit set
    - SYN field: Random synchronize sequence number
- Host B receives message
  - Sends segment
    - ACK field: sequence number Host A sent plus 1
    - SYN field: Computer B random number
- Host A responds
  - Sends segment
    - ACK field: sequence number Host B sent plus 1
- FIN flag indicates transmission end

3-Way Handshake (cont'd)

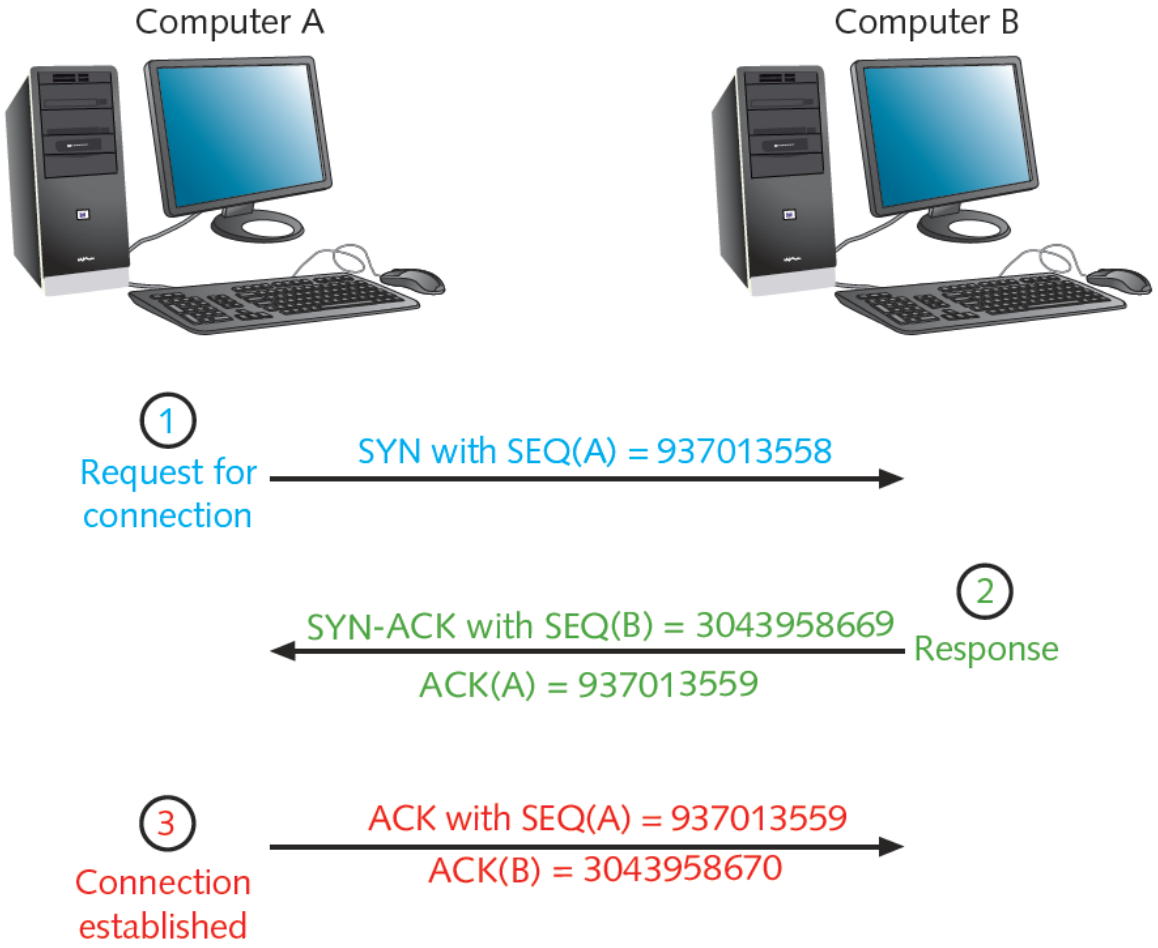

Image: Course Technology / Cengage learning

UDP

- UDP = User Datagram Protocol
  - Transport layer protocol
- Provides unreliable data delivery services
  - Connectionless transport service
  - No assurance packets received in correct sequence
  - No guarantee packets received at all
  - No error checking, sequencing
  - Lacks sophistication
    - More efficient than TCP
- Useful situations
  - Great volume of data transferred quickly

A UDP Segment

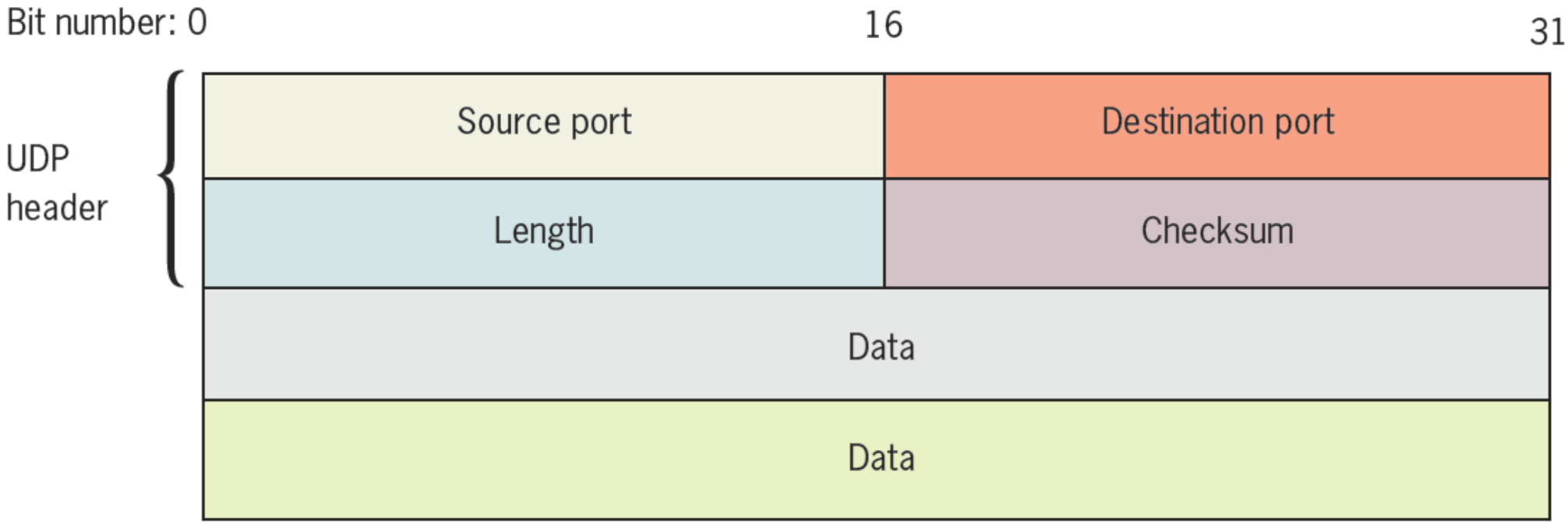

Image: Course Technology / Cengage learning

IP (Internet Protocol)

- Network layer protocol
  - How and where data delivered, including:
    - Data's source and destination addresses
- Enables TCP/IP to internetwork
  - Traverse more than one LAN segment
    - More than one network type through router
- Network layer data formed into packets
  - IP packet
    - Data envelope
    - Contains information for routers to transfer data between different LAN segments

IP (cont'd)

- Versions
  - IPv4: unreliable, connectionless protocol
  - IPv6: connectionless or connection-oriented
- "Newer" version of IP protocol
  - IP next generation
  - Released in 1998
- Advantages of IPv6
  - Provides trillions of additional IP addresses
  - Better security and prioritization provisions

IPv4 Packet

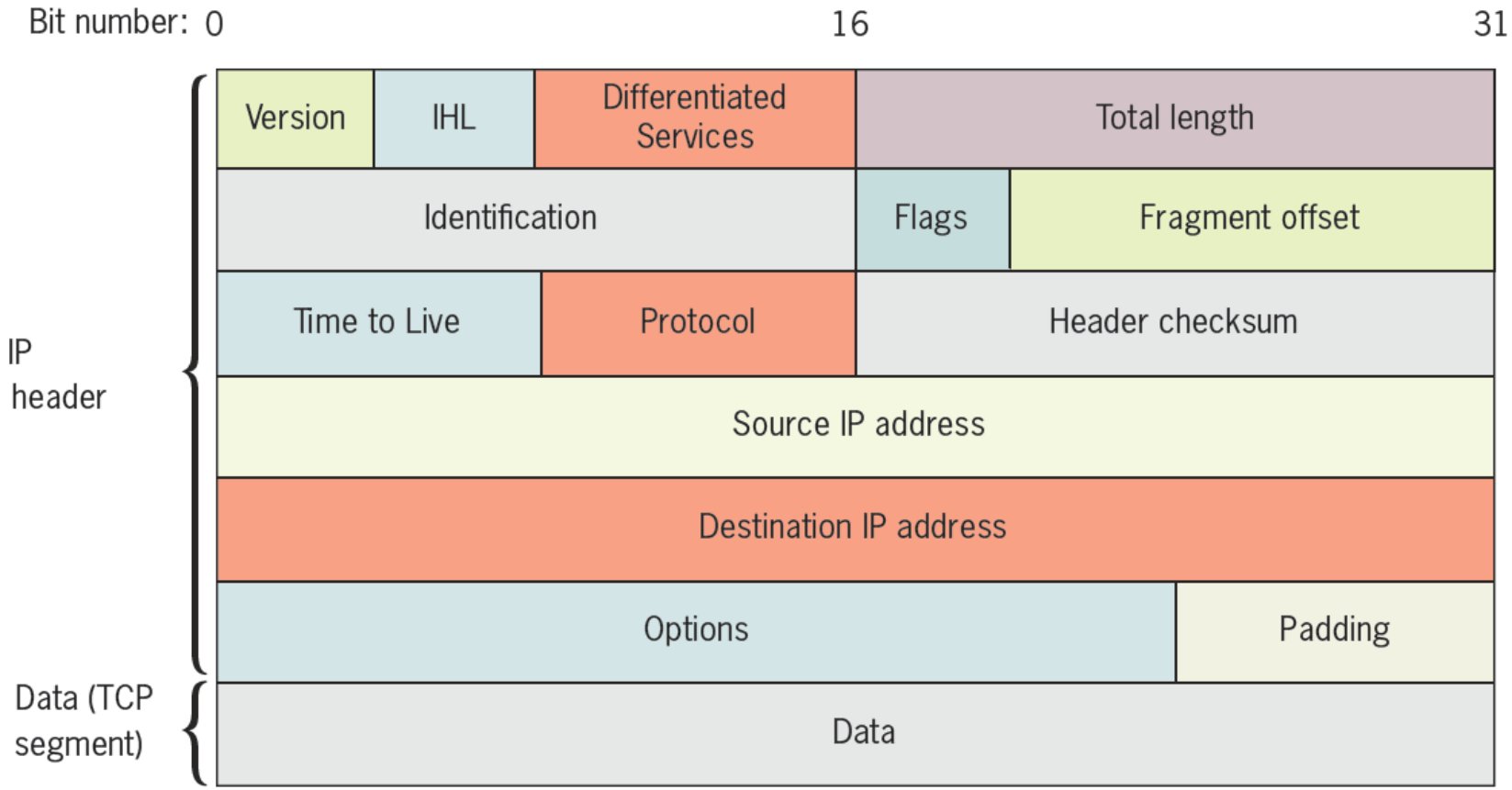

Image: Course Technology / Cengage learning

IPv6 Packet Header

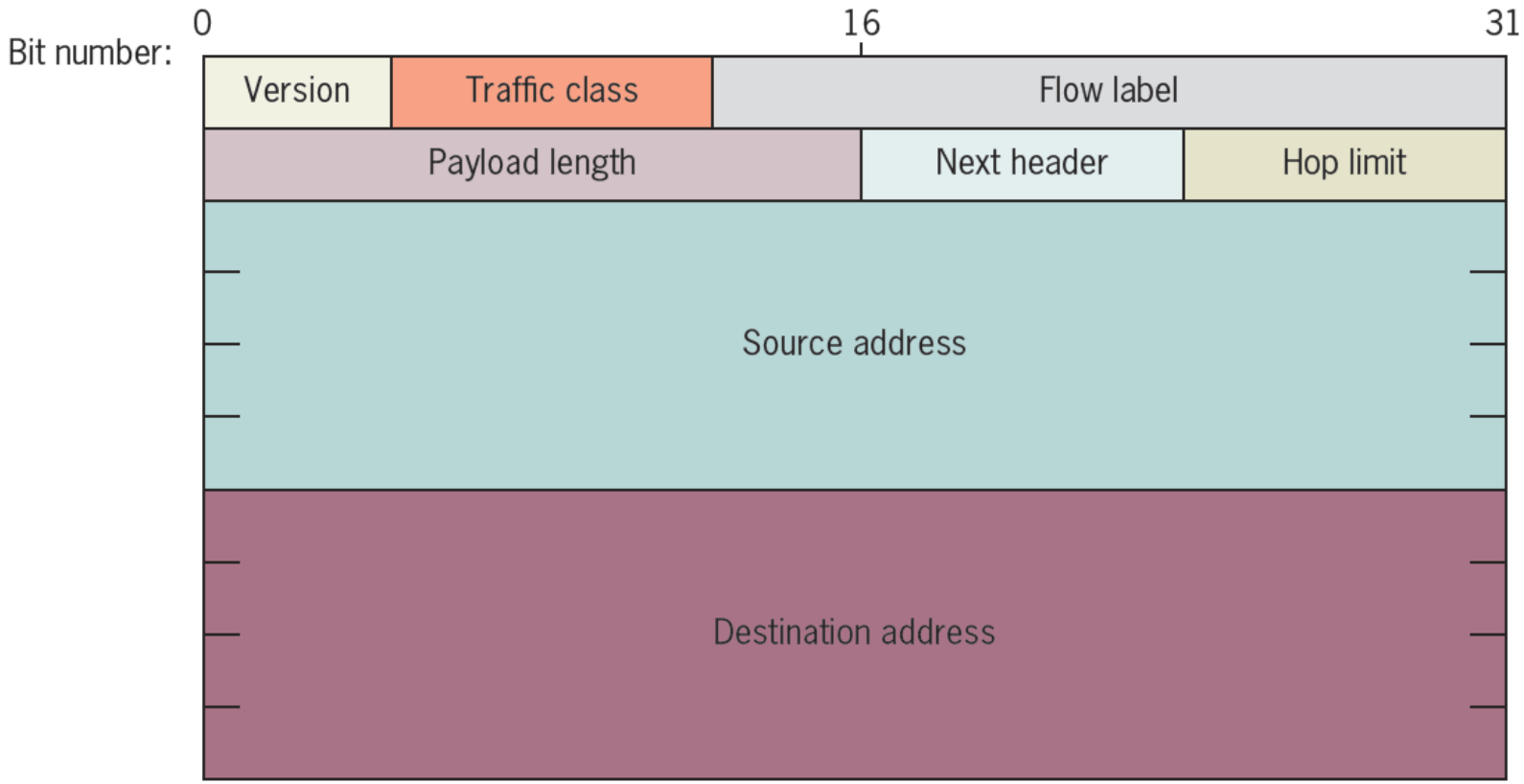

Image: Course Technology / Cengage learning

IGMP

- IGMP = Internet Group Management Protocol
- Operates at Network layer of OSI model
- Manages multicasting on networks running IPv4
- Multicasting
  - Point-to-multipoint transmission method
  - One node sends data to a group of nodes
  - Sometimes used for internet teleconferencing or video-conferencing (needs tunnel to function over public internet)

ARP

- ARP = Address Resolution Protocol
- Network layer protocol
- Used with IPv4
- Obtains MAC (physical) address of host or node
- Creates database that maps MAC to host's IP address
- ARP table
  - Table of recognized MAC-to-IP address mappings
  - Saved on network device's local storage (host, network switch, etc.)
  - Increases efficiency
  - Contains dynamic and static entries

ICMP

- ICMP = Internet Control Message Protocol
- Network layer protocol
  - Reports on data delivery success or failure
- Announces transmission failures to sender
  - Network congestion
  - Data fails to reach destination
  - Data discarded: TTL expired
- ICMP cannot correct errors
  - Provides critical network problem troubleshooting information
- ICMPv6 used with IPv6

IPv4 Addressing

- Networks recognize two addresses
  - Logical (Network layer)
  - Physical (MAC / hardware) addresses
- IP Protocol handles logical addressing
- Specific Parameters
  - Unique 32-bit number
    - Divided into four octets (sets of eight bits) separated by periods
    - Example: 192.168.1.1
  - Network class determined from first octet

Common IPv4 Classes

Network class	Beginning octet	Number of networks	Maximum addressable hosts per network
A	1–126	126	16,777,214
B	128–191	> 16,000	65,534
C	192–223	> 2,000,000	254

Image: Course Technology / Cengage learning

IPv4 Addressing (cont'd)

- Class D, Class E rarely used (never assign)
  - Class D: value between 224 and 239
    - Multicasting
  - Class E: value between 240 and 254
    - Experimental use
- Eight bits have 256 combinations
  - Networks use 1 through 254
  - 0: reserved as placeholder
  - 255: reserved for broadcast transmission

IPv4 Addressing (cont'd)

- Class A devices
  - Share same first octet (bits 0-7)
    - Network ID
  - Host: second through fourth octets (bits 8-31)
- Class B devices
  - Share same first two octet (bits 0-15)
  - Host: second through fourth octets (bits 16-31)
- Class C devices
  - Share same first three octet (bits 0-23)
  - Host: second through fourth octets (bits 24-31)

IPv4 Classes

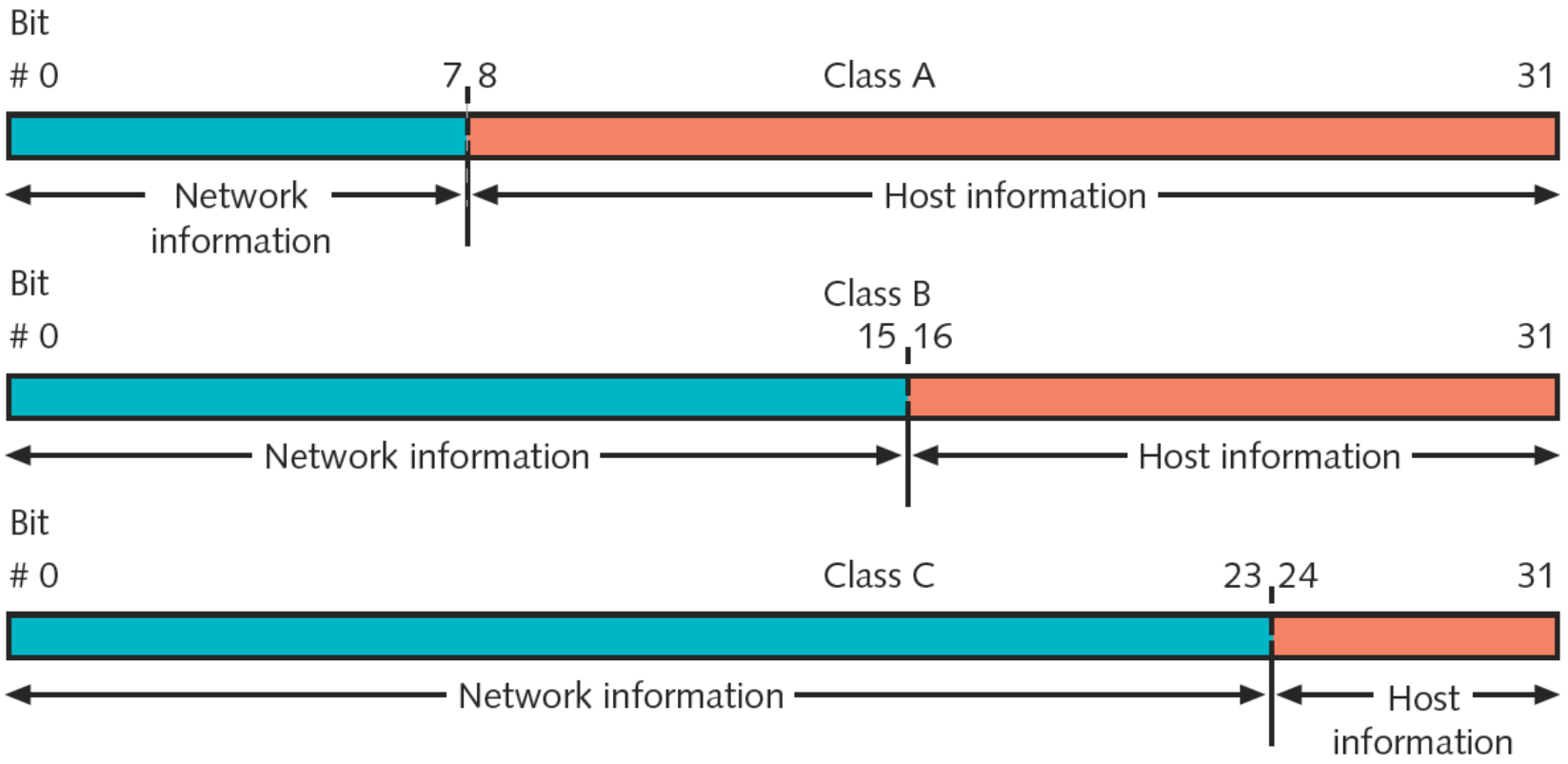

Image: Course Technology / Cengage learning

IPv4 Addressing (cont'd)

- Loopback address
  - First octet equals 127 (127.0.0.1)
- Loopback test
  - Attempting to connect to own machine
  - Useful for troubleshooting
- Windows
  - 'ipconfig' command
- Unix / Linux
  - 'ifconfig' command

Binary and Dotted Decimal Notation

- Dotted decimal notation
  - Common way of expressing IP addresses
  - Decimal number between 0 and 255 represents each octet
  - Period (dot) separates each decimal
- Dotted decimal address has binary equivalent
  - Convert each octet
  - Remove decimal points

Subnet Mask

- 32-bit number identifying a device's subnet
- Combines with device IP address
- Informs network about logical subdivision of IPs
- Four octets (32 bits)
  - Expressed in binary or dotted decimal notation
- Assigned same way as IP addresses
  - Manually or automatically (via DHCP)

Subnet Mask (cont'd)

Network class		Default subnet mask
A	1–126	255.0.0.0
B	128–191	255.255.0.0
C	192–223	255.255.255.0

Image: Course Technology / Cengage learning

IPv6 Addressing

- Composed of 128 bits
- Eight 16-bit fields
- Typically represented in hexadecimal numbers
  - Separated by a colon
  - Example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334
- Abbreviations for multiple fields with zero values
  - 00FF can be abbreviated FF
  - 0000 can be abbreviated 0
- Modern devices and operating systems can use both IPv4 and IPv6

Summary

- Protocols define standards for network communication
  - TCP/IP suite most popular
- TCP: connection-oriented subprotocol
- UDP: efficient, connectionless service
- IP provides information about how and where to deliver data
- IPv4 addresses: unique 32-bit numbers
- IPv6 addresses: unique 128-bit numbers - composed of eight 16-bit fields