Intro to Networking

Offensive Network Security
Florida State University
Spring 2014

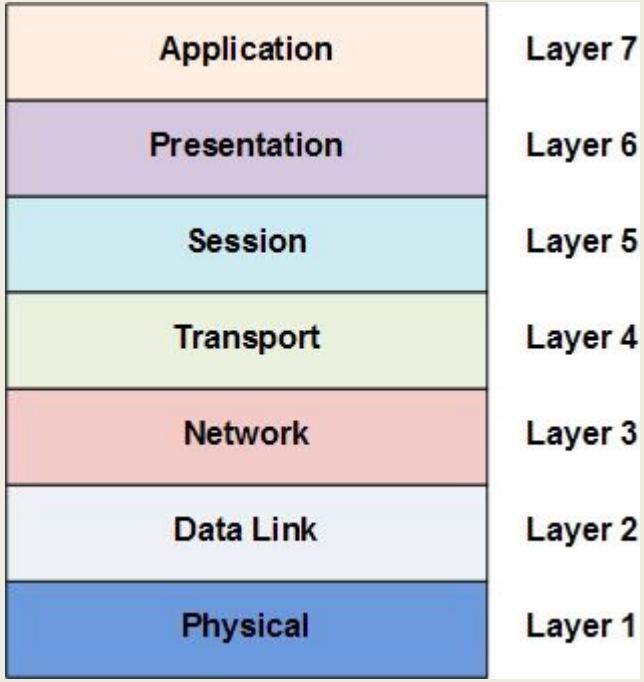
Outline

- A look into the layers of computer network communication
- Understand
  - Switched Ethernet
  - Internet Protocol
  - Transmission Control Protocol
  - User Datagram Protocol
- Get to know these protocols so we know how to manipulate/exploit for our needs

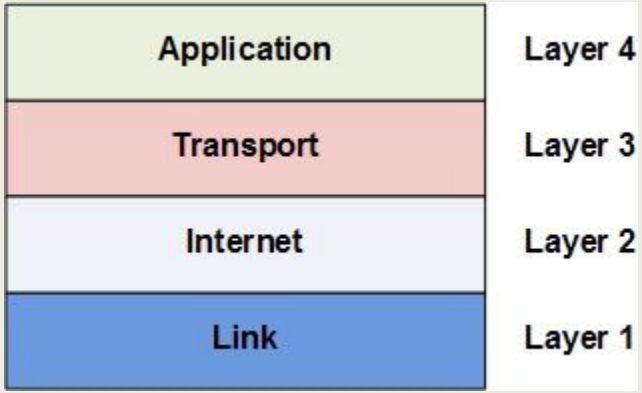
Network Terms (General)

- Host (end-node): the sending or receiving end
- Frame: data transmission which utilizes synchronization
- Packet: a unit of data sent through a network
- Port: an abstract end-point used to specify where an application is listening, sending, or receiving
- Protocol: a set of rules that governs how communication will occur
- Topology: the structure of a network
- Local Area Network (LAN): a small interconnected network which commonly uses Switched Ethernet topology
- Wide Area Network (WAN): a large geographical network which utilize routers for communication

OSI and TCP/IP Model



OSI Model

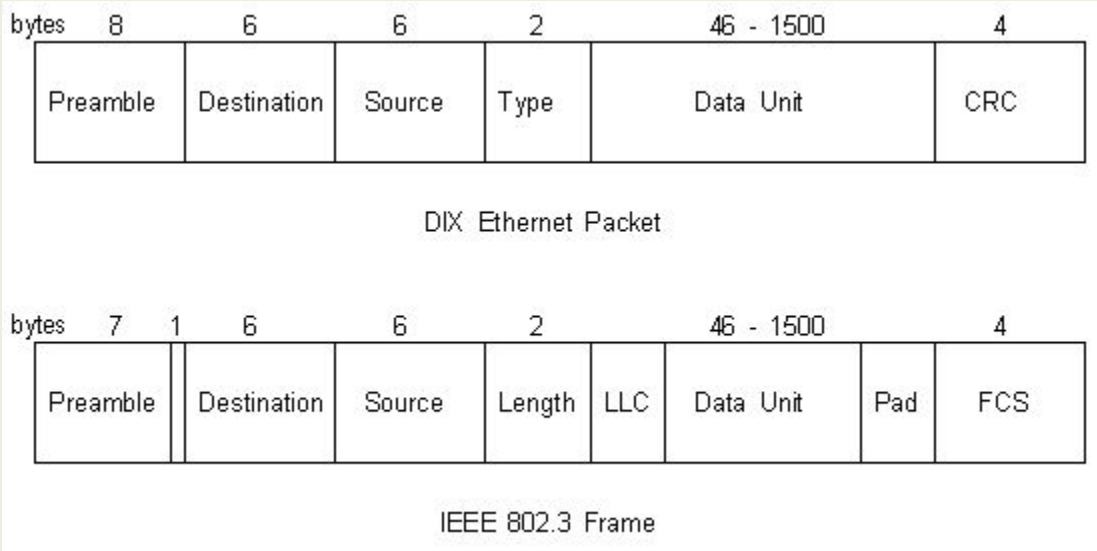


TCP/IP Model

Switched Ethernet

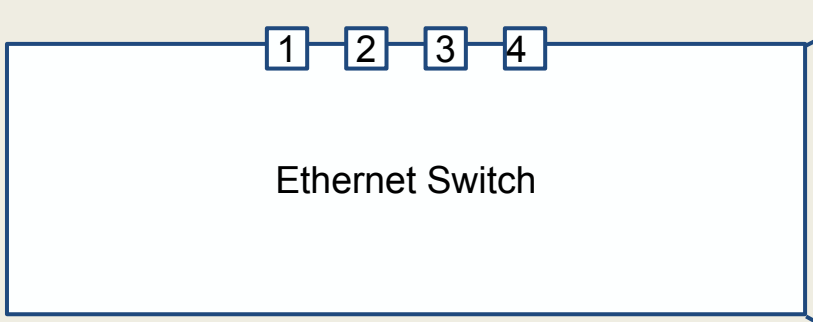
- Most common LAN technology
- Considered Layer-1 and Layer-2 technology
- IEEE 802.3 (standardized)
- Utilizes 48-bit MAC addresses to “uniquely” identify each physical socket on a Network Interface Controller (NIC)
- Uses frames to send and receive data
- No loops in topology / Spanning Tree Protocol
- Ethernet types
  - Address Resolution Protocol (ARP) (0x0806)
  - Internet Protocol (IP) (0x0800)
  - GOOSE (IEC 61850)
  - SV (IEC 61850)

Ethernet Frame



Ethernet Switch

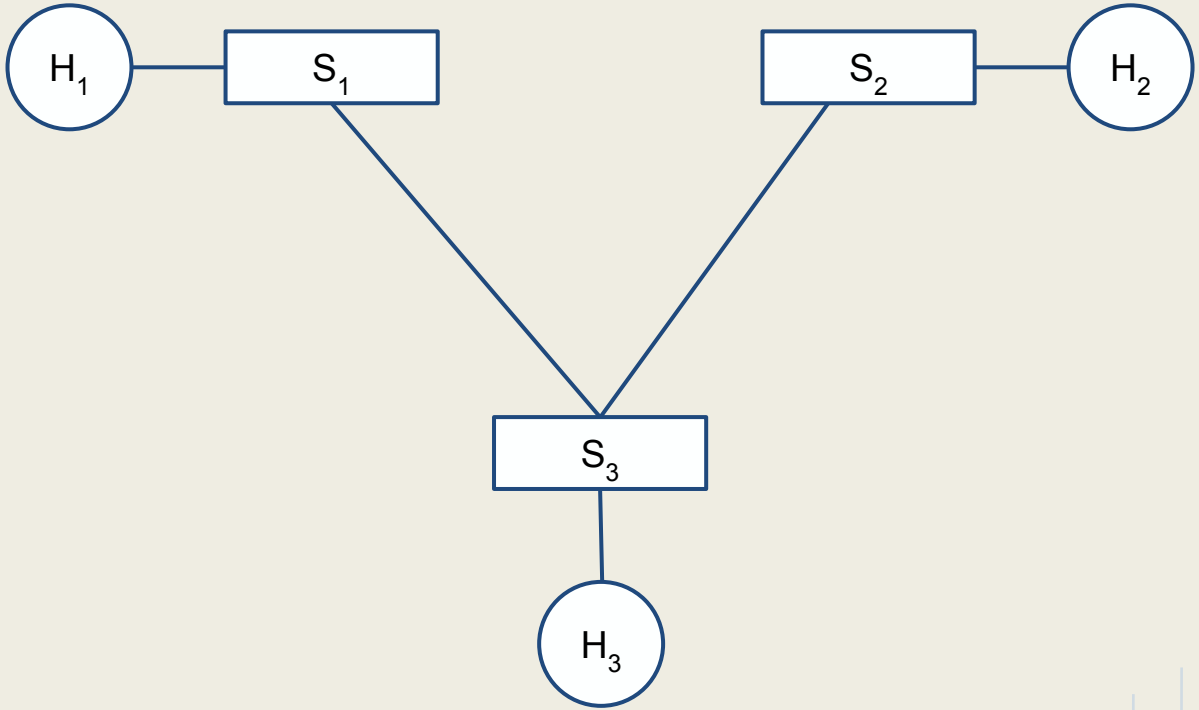
- Layer-2 Device
- Uses store-and-forward
  - Buffer each frame
  - Save sending MAC & port
- Broadcast frame if no match in table



MAC/Port Table

Port	MAC
1	AA:AA:AA:DD:EE:FF
3	BB:BB:BB:DD:FF:FF
2	CC:CC:CC:BB:CC:DD

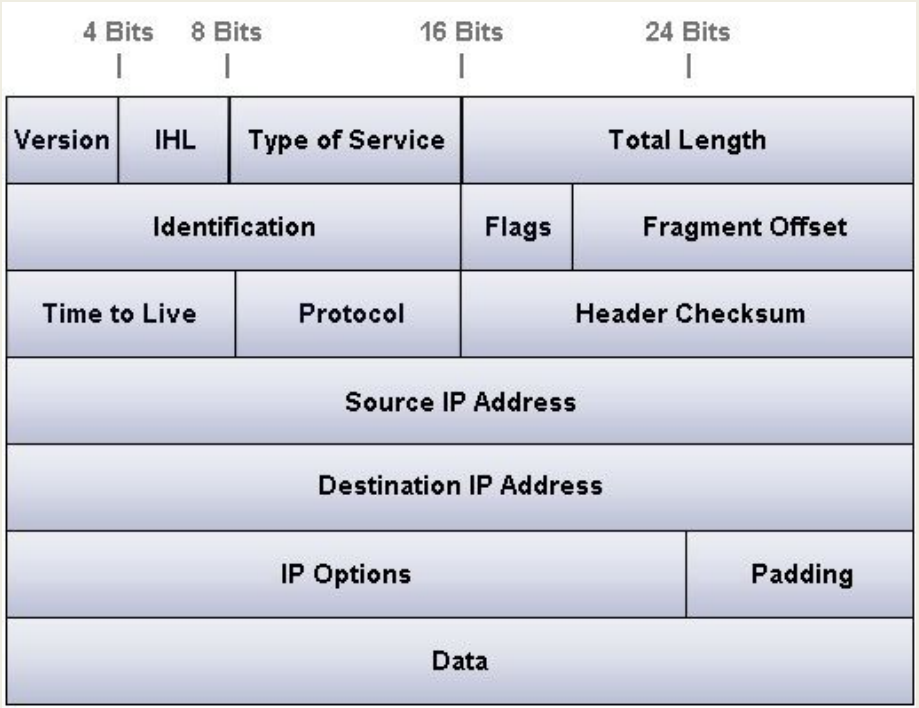
Switched Ethernet Topology



Internet Protocol v4

- Most popular protocol to route internet traffic
- Stateless and connectionless protocol
- Uses 32-bit (4-bytes) addresses
  - Addresses fully exhausted
  - Uses to NAT to combat IP exhaustion
- Private IP ranges
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16
- Reserved
  - 127.0.0.0/8
  - 224.0.0.0/4

IP Packet


4 Bits
8 Bits
16 Bits
24 Bits
Version
IHL
Type of Service
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source IP Address
Destination IP Address
IP Options
Padding
Data

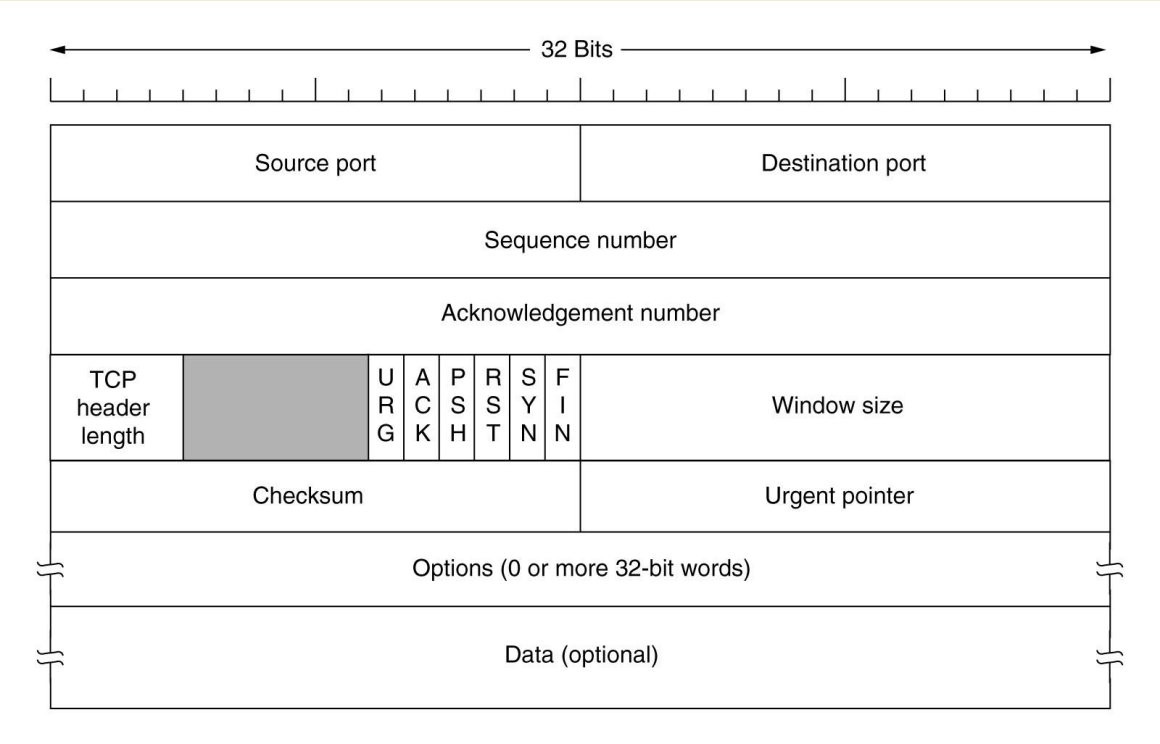
TCP

- RFCs: 675, 793, 1122, 2581
- Transport layer (layer-4)
- Provides
  - Reliable connection
  - Ordered delivery
  - Error check
- Exchanges data packets (header + body)
- Flags
  - URG -- urgent
  - ACK -- acknowledgement
  - PSH -- push data
  - RST -- reset connection
  - SYN -- synchronize protocol (sequence numbers)
  - FIN -- sender is finished sending data

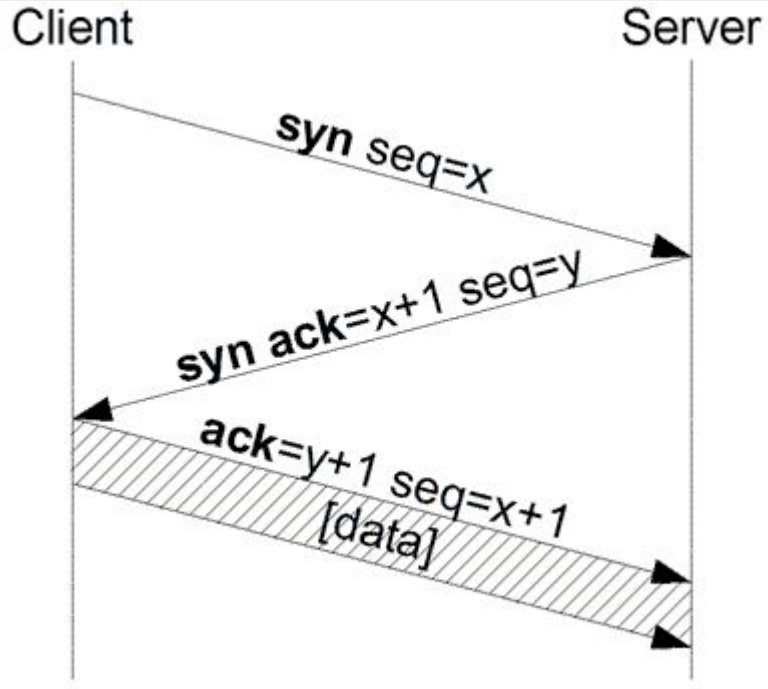
TCP cont...

- Protocol States
  - listen -- waiting for connection
  - syn-sent -- first handshake packet sent / waiting SYN-ACK
  - syn-received -- first handshake packet received / waiting for ACK
  - established -- open connection between sender / receiver
  - fin-wait-1 -- closing, waiting for remote termination ACK
  - fin-wait-2 -- waiting for remote termination request
  - close-wait -- local user termination requested
  - closing -- waiting for termination request ACK
  - last-ack -- waiting for connection termination ACK
  - time-wait -- waiting specified time after connection close
  - closed -- connection gone

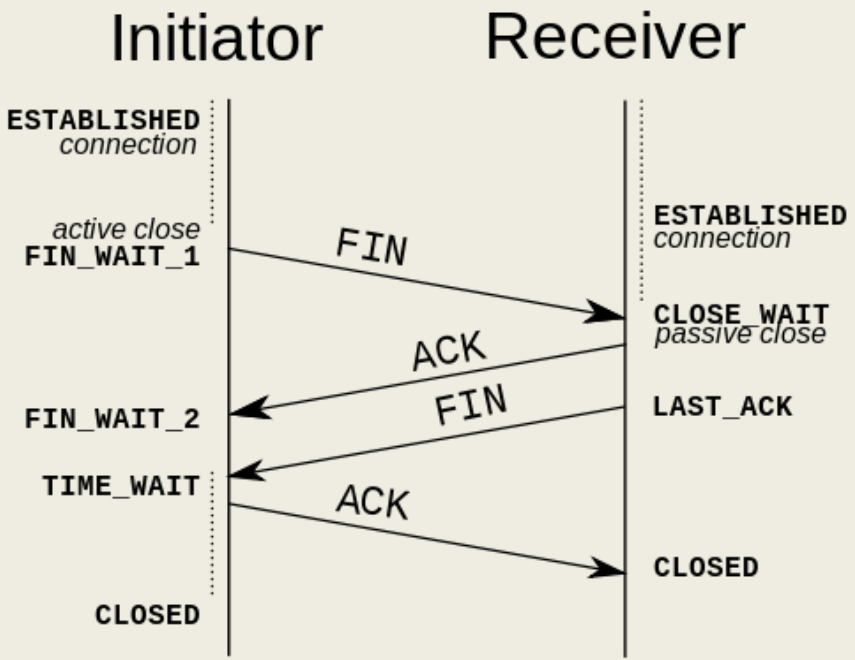
TCP Header


32 Bits
Source port
Destination port
Sequence number
Acknowledgement number
TCP header length
URG
ACK
PSH
RST
SYN
FIN
Window size
Checksum
Urgent pointer
Options (0 or more 32-bit words)
Data (optional)

TCP Three-way Handshake



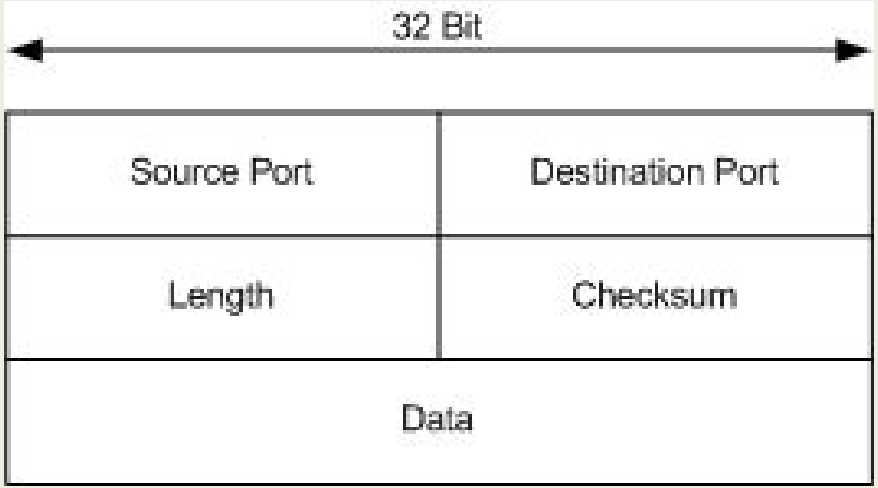
TCP Termination



UDP

- RFC 768
- Transport layer (layer-4)
- Connectionless
- Sends messages known as datagrams
- No handshakes
- No guarantee of delivery
- Stateless, possible duplicates

UDP Header



Reading Resources

- Tanenbaum, Andrew. “Computer Networks”. 5th ed., 2010.
  - Excellent introduction to computer networking
  - Covers all layers (Physical to Application)
  - Covers major protocols (i.e. HTTP, SMTP, etc.)
- Calvert, Kenneth L and Donahoo, Michael J. “TCP/IP Sockets in C, Second Edition: Practical Guide for Programmers”. 2nd ed., March 2009
- Neither books are required reading for this course but would be great additions to the library if interested in having reading references