Week 4 - Lecture 4

Friday, 18 March 2016 2:01 PM

Topologies:

Simple Physical Topologies:

- Physical topology
    - ○ Physical network nodes layout
    - ○ Depicts broad scope
    - ○ Does not specify
        - ▪ Device types
        - ▪ Connectivity methods
        - ▪ Addressing schemes
    - ○ Fundamental shapes
        - ▪ Bus, ring, star
        - ▪ Hybrid
    - ○ Bus:
        - ▪ Single cable-connects all network nodes
        - ▪ No intervening connectivity devices
        - ▪ One shared communication channel
        - ▪ Advantages:
            - □ Relatively inexpensive
        - ▪ Disadvantages:
            - □ Does not scale well
            - □ Difficult to troubleshoot
            - □ Not very fault tolerant
    - ○ Ring:
        - ▪ Node connects to nearest two nodes
        - ▪ Circular network
        - ▪ One direction (unidirectional) data transmission
        - ▪ Physical medium
            - □ Twisted pair or fiber-optic cabling
        - ▪ Drawbacks:
            - □ Malfunctioning workstation can disable network
            - □ Not very flexible or scalable
    - ○ Star:
        - ▪ Node connects through central device
            - □ Router or switch
        - ▪ Physical medium
            - □ Twisted pair of fiber-optic cablnig
        - ▪ Single cable connects only two devices
        - ▪ Most popular fundamental layout
        - ▪ Advantage
            - □ Fault tolerant
            - □ Flexible
        - ▪ Disadvantage:
            - □ More expensive

- Hybrid Topologies
    - ○ Pure bus, ring and star topologies rarely exist because they are too restrictive
    - ○ Hybrid topology
        - ▪ More likely
        - ▪ Complex combination of pure topologies
        - ▪ Several options

- Logical Topologies
    - ○ Refers to way data transmitted between nodes
        - ▪ Rather than physical layout
    - ○ Does not necessarily match physical topology
    - ○ Most common: bus and ring
    - ○ Broadcast domain (more later)
        - ▪ All nodes connected to single repeating device or switch

Ethernet Fundamentals:

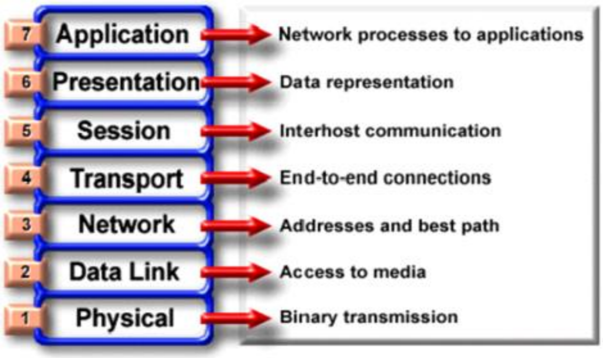
Ethernet:

- Ethernet is a bus network in which multiple computers

share a single transmission medium
- While one computer transmits a frame to another. All other computers must wait.
- Ethernet is the dominant LAN technology in the world.

Types of Ethernet:
- 10-Mbps Ethernet
- 100 Mbps Fast Ethernet
- Gigabit Ethernet
- 10 Gigabit Ethernet
- 10BASE5, 10BASE2, and 10BASE-T Ethernet are now considered Legacy Ethernet

OSI Model Revision:



Ethernet operates in two areas of the OSI model:
1. The lower half of the data link layer, known as the MAC sub layer
2. And the physical layer

Layer 1 - The physical Layer
- Defines standards for: physical media types, connectors, voltages, bit rates

Layer 2 - The Data Link Layer
- Physical addressing
  - As opposed to network, or logical addressing at layer 3
  - Media access control which provide reliable transition of data across a physical link

Data Link Layer - Two sublayers
- Logical Link Control (LLC):
  - The logical link control (LLC) sublayer remains relatively independent of the physical equipment
- Media Access Control (MAC):
  - The MAC sub-layer is concerned with the **physical components** that will be used to communicate information
  - Who can access the network when multiple computers are trying to access it simultaneously
  - Physical addressing (MAC addresses) and access control methods
  - Ethernet sub-layer

IEEE Ethernet Standards:

- 802.1 - Standards introduction
- **802.2 - Logical Link Control (LLC)**
- **802.3 – Ethernet**
- 802.4 - Token Bus - 75 ohm CATV coax or Fibre
- **802.5 - Token Ring**
- 802.6 - MAN (Metropolitan Area Network) - similar to FDDI
- 802.7 - Broadband
- 802.8 - Fibre Optics
- 802.9 - Integrated Voice and Data
- 802.10 - LAN Security

- **802.11 - Wireless**
- 802.12 - 100 VG AnyLAN
- 802.15 - Bluetooth
- 802.16 - WiMax

1000-Mbps Ethernet - Gigabit:

- Gigabit ethernet standards represent transmission using both fiber optic and copper media
- IEEE 802.3z
  - Specifies 1Gbps full duplex over optical fiber
  - The 1000BASE-LX and SX standard
  - Where LX is long wave and SX is short wave frequencies of light travelling
- IEEE 802.3ab
  - Specifies 1Gbps full duplex over twisted pair copper cable
  - The 1000BASE-X standard

The MAC address:

- 48-bit flat address that never changes
- Every node on a network has a unique MAC address
- Consists of 12 hex digits (48 bits)
  - First 6 digits (assigned by the IEEE)
- First 6 digits represent the Organizational Unique Identifier (OUI) which identifies the manufacturer
- The last 6 are assigned by the manufacturer and represent a unique hardware ID number for the NIC

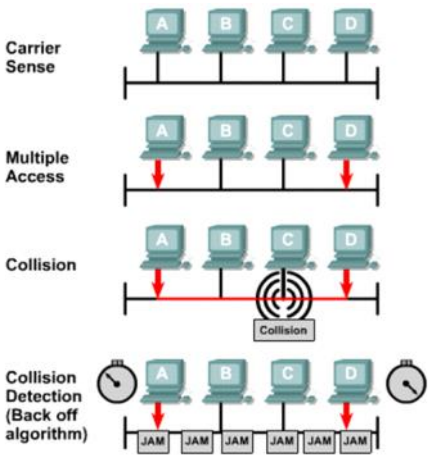
Ethernet:

- Ethernet performs three functions:

1. **Transmitting and receiving data frames**
   - Uses CSMA/CD (non-deterministic)
   - CSMA/CD - Carrier Sense Multiple Access/ Collision Detection
2. **Decoding data frames and checking them for valid MAC addresses**
   - Before passing them to the upper layers of the OSI model
3. **Detecting errors within data frames** or on the network
   - Note that Ethernet performs error detection but NOT error correction
   - Any frame with an incorrect checksum is an error
   - Also any frame under 64 bytes in length is an error

(EXAM) CSMA/CD MAC Rules and Collision:

Detection/ back off



-Computers send signal at same time

-

- When a collision is detected, the computers that sent the signals transmit a transmit a 'jam signal' that stops all computers from transmitting. They then start transmitting at random times afterwards to prevent another collision.

Full and Half Duplex:

- Half duplex hosts can only send or receive at any one time
    - Share the same medium (wire, radio frequency) for transmit and receive
- Full duplex allows hosts to send and receive simultaneously
    - Requires 2 pairs of wires (one for send and one for receive)
    - Doubles the bandwidth

Network Devices:

Layer 1 devices (refresh):

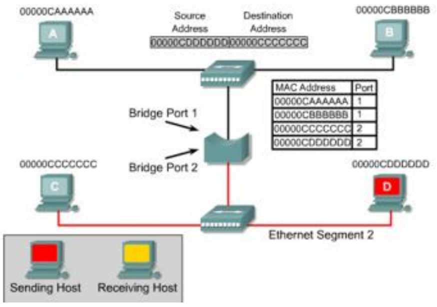
- Transceiver - Something that can transmit and receive.
- Repeaters and hubs.

Layer 2 devices:

- Bridges
    - Divides a network into segments
    - Contains collisions in these segments (**collision domains**)

Layer 2 bridging tables:

- Bridge creates smaller **collision domains**
- Still called a single broadcast domain
- Source MAC addresses of a frame and the associated incoming switch port are added to the address table to allow filtering of frames
- e.g.



MAC Address	Port
00000CAAAAAA	1
00000CBBBBBB	1
00000CCCCCCC	2
00000CDDDDDD	2

Layer 2 Devices (cont.)

- Switches:

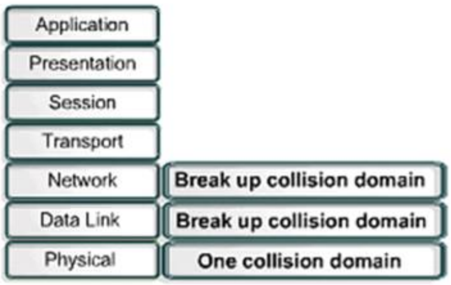
- Multiport bridges
- Creates more than two collision domains
- These days every device gets its own collision domain
- Also uses bridging tables
- Will only send frames out of the ports that the frames are addressed to

- Forwarding Decisions:
  - Store and Forward
    - Holds the frame and checks it for errors, will drop it if faulty. Can be slow.
  - Cut through
    - Once it knows the address it starts forwarding frames. Does not do error checking. Very fast switching.
  - Fragment free
    - Checks that frame is at least the minimum size (64 bits) before sending it on. Better checking than 'cut through' but not as good as 'store and forward'. Midway point in speed.

Collisions in collision Domain:

- If you internet router has a hub instead of a switch, this is why it slows down when you connect a few extra computers. On a hub, a frame sent to the hub gets sent out of every port on the hub.

Collision Domain segmentation:



Increasing a Collision Domain:

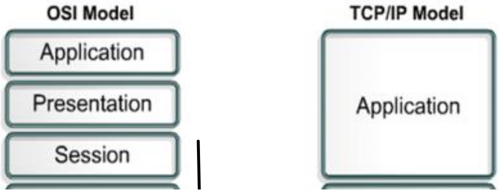
Layer 1 devices extend collision domains
- e.g. HUB

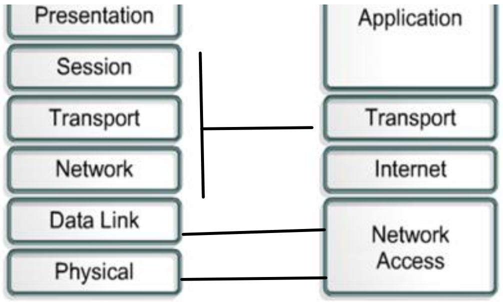
Layer 2 devices break up collision domains
- e.g. Bridge, switch, router

Layer 3:
- Routers connect networks
- Routers building routing tables to all known destination networks by exchanging their routing tables with adjacent routers
- Routers select the best path for incoming data packets to reach their destination networks

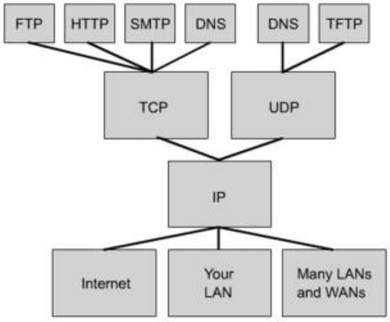
Broadcast domain segmentation
- Routers break up broadcast domains. Layer three devices are the only devices that contain broadcasts.

TCP/IP Reference Model:
Transport Layer





TCP/IP Protocol Graph:



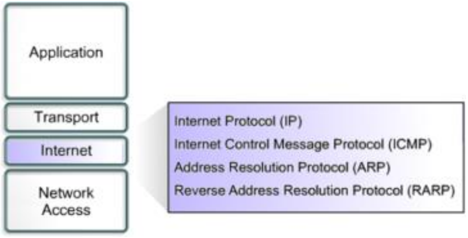
Application Layer

Transport Layer

Network Layer

Physical Layer

Internet Layer Protocols:


Application
Transport
Internet
Network Access
Internet Protocol (IP)
Internet Control Message Protocol (ICMP)
Address Resolution Protocol (ARP)
Reverse Address Resolution Protocol (RARP)

IP protocol is responsible for:
- Defining packet format and the IP addressing scheme
- Routing packets to remote hosts (best path selection)
- Transferring data between the internet layer and the network access layer

Internet Layer Protocols:
- IP (Internet protocol)
  - Connectionless, best-effort delivery routing of packets
- ICMP (Internet control message protocol)
  - Control and messaging capabilities
- ARP (Address resolution protocol)
  - Determines the data link layer address for known IP addresses
  - ARP is often considered to sit between layer 2 and 3
    - Not in layer 2.

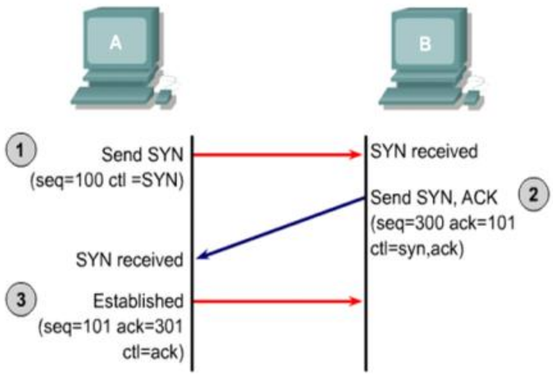
Transport Layer Protocols:
- TCP (Transmission Control Protocol)
  - Connection-Oriented
- UDP (User datagram protocol)
  - Connectionless

Transport Layer:
- The primary duties of the transport layer, are to transport and regulate the flow of information for the source to the destination, reliably and accurately
- End-to-end control and reliability are provided by sliding windows, sequencing numbers, and acknowledgements.

TCP Services:
- Segmenting upper-layer application data
- Establishing, maintaining and terminating end-to-end connections
- Transporting segments from one end host to another end host
- Re-assembling upper-layer application data
- Reliability of data delivery using sequence numbers, acknowledgements and retransmission
- **Flow control**

Establishing a TCP connection:

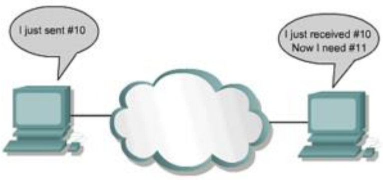
TCP three way handshake:



- TCP requires **connection establishment** before data transfer begins.
- The algorithm used to establish and terminate the connection is called the Three Way Handshake
- For a connection to be established or initialized:
    - Hosts must synchronise their **Initial Sequence Numbers (ISN)**
    - Synchronisation is done through an exchange of connection establishing segments that carry a control bit called **SYN**, for synchronise, and the **Initial Sequence Numbers**
    - The connection is established when each side has received the ISN from the other side and sent confirming **ACK**.

Transport Layer - Reliability

- Reliability through acknowledgment



- If receipt of a segment is not acknowledged within a set time the source resends the segment
- This provides a façade of reliability

Reliability through acknowledgments:

- Positive acknowledgment requires a recipient to communicate with the source, sending back an acknowledgment message when it receives data
    - Sender keeps a record of each data segment that it sends and expects an acknowledgment
    - The sender also starts a time when it sends a segment and will retransmit a segment if the timer expires before an acknowledgment arrives
    - TCP reassembles the segments into a complete message. If a sequence number is missing in the series, that segment is retransmitted

Transport Layer - Flow Control (Windowing):

- Sometimes the receiving host is unable to process data as quickly as it arrives which could result in data loss
- Flow control allows the two hosts to establish a data-transfer rate that is agreeable to both

General Principle of Flow Control:

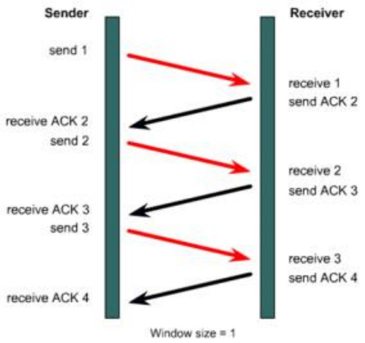
- When data arrives too quickly for a host to process, they are **temporarily stored in memory**
- If the traffic continues, the host eventually exhausts its memory and must **discard the additional data that arrives**
- Instead of allowing data to be lost, flow control allows the receiver to issue a **"not ready"** indicator to the sender
- The sending host stops transmission until it receives a **"ready"** signal from the receiver

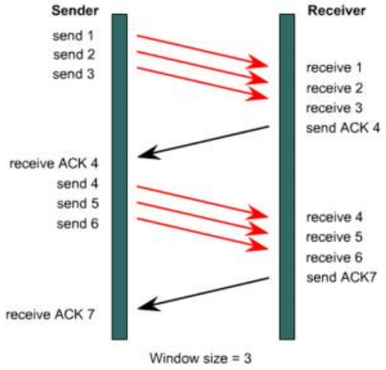
Windowing (TCP flow control mechanism):

- One packet and one acknowledgement at a time results in a low throughput
- However if multiple packets are sent the receiver may not be able to process them and some may be lost
- To address this problem TCP uses a flow control mechanism called **Windowing**
- Windowing allows the receiving node to inform the sender of the maximum amount of segments it can receive in a block
- Windowing allows a sequence of packets to be sent sequentially in a block without waiting for an individual ACK for each segment
- The receiver then sends a single ACK for the block of segments making the transfer more efficient

Window Size:

- Window size - How many bites of data can the receiver get in one chunk
- TCP **window sizes are variable** during the lifetime of a connection
- Window size is varied by the receiver to flag the amount of data it can accommodate in its receiver buffer
- Larger window size increases communication efficiency.





TCP and UDP:

Transmission Control Protocol (TCP)

- Summary
  - TCP is a **connection-oriented** transport layer protocol that provides reliable full-duplex data transmission
  - Supports **sequence numbers and acknowledgments** in an attempt to provide **"guaranteed" delivery**, and also provides **flow control** using **sliding windows**.
  - Protocols that use TCP include:
    - FTP (File transfer Protocol)
    - HTTP (Hypertext Transfer Protocol)
    - SMTP (Simple Mail Transfer Protocol)
    - Telnet

User Datagram Protocol (UDP)

- Summary
  - The TCP model is not the OSI model and breaks some of the rules
  - The TCP/IP model has 2 transport layer protocols TCP and UDP
  - Although TCP conforms to the OSI Transport layer functionality, UDP does not
  - UDP is a simple, fast, best effort transport layer protocol designed for real time applications that do not require retransmission of lost segments
  - Protocols that use UDP:
    - TFTP (Trivial File Transfer Protocol)
    - SNMP (Simple Network Management Protocol)
    - DHCP (Dynamic Host Control Protocol)
    - DNS (Domain Name System)

- Simplified Summary
  - Much simpler
  - Connectionless
  - No windowing (No acknowledgments, window sizes)
  - For things that can handle a few lost packets such as video streaming

Port Numbers:

Multiplexing of upper-layer conversations:

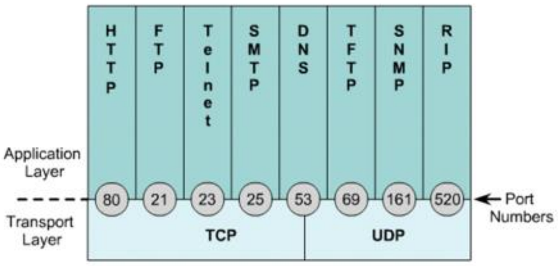
- Transport layer can simultaneously send and receive data streams for different applications
- Streams are differentiated by allocating each TCP/IP application (email, web server…) its own **port number** which is included in the transport layer segment header

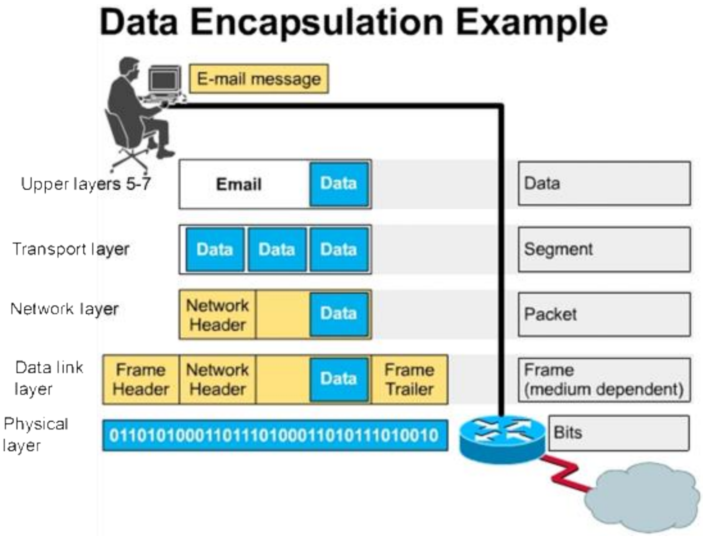
TCP and UDP port numbers:

- Each TCP/IP application gets a port number (email, google chrome)
- Port numbers 255 and below are assigned to specific services
  - e.g. Any conversation bound for a web server uses the standard port number 80.
- Port numbers (as well as IP addresses and domain names) are managed by the international organisation ICANN

- From 256-1023 are assigned to companies for marketable applications
- Port numbers from 1024 are dynamically assigned

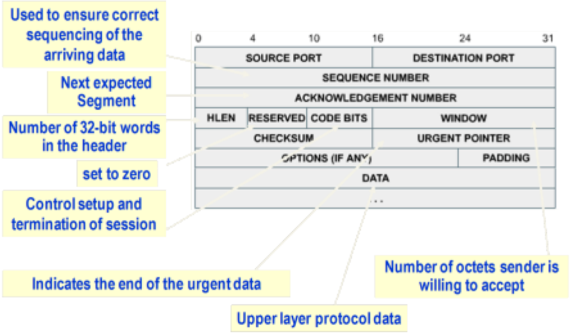
- Know TCP and UDP port numbers for services:

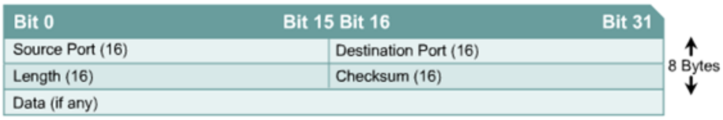




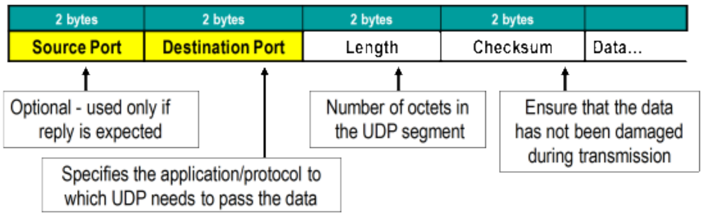
- THE IP ADDRESS IS DEFINING THE DEVICE YOU ARE TALKING TO.
- THE PORT NUMBER IS DEFINING THE APPLICATION ON THE DEVICE THAT YOU ARE TALKING TO.

TCP and UDP segment formats:


Used to ensure correct sequencing of the arriving data
Next expected Segment
Number of 32-bit words in the header
set to zero
Control setup and termination of session
0
4
10
16
24
31
SOURCE PORT
DESTINATION PORT
SEQUENCE NUMBER
ACKNOWLEDGEMENT NUMBER
HLEN
RESERVED
CODE BITS
WINDOW
CHECKSUM
URGENT POINTER
OPTIONS (IF ANY)
PADDING
DATA
...
Indicates the end of the urgent data
Number of octets sender is willing to accept
Upper layer protocol data



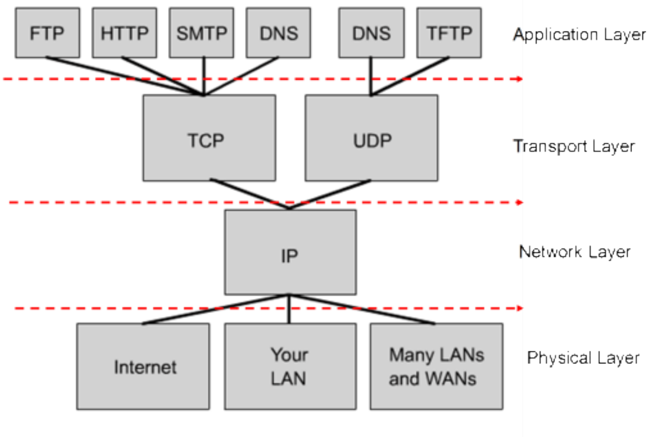
Bit 0	Bit 15 Bit 16	Bit 31
Source Port (16)	Destination Port (16)	
Length (16)	Checksum (16)	
Data (if any)		



2 bytes	2 bytes	2 bytes	2 bytes	
Source Port	Destination Port	Length	Checksum	Data...

Optional - used only if reply is expected
Specifies the application/protocol to which UDP needs to pass the data
Number of octets in the UDP segment
Ensure that the data has not been damaged during transmission

Protocol Graph: TCP/IP


FTP
HTTP
SMTP
DNS
DNS
TFTP
Application Layer
TCP
UDP
Transport Layer
IP
Network Layer
Internet
Your LAN
Many LANs and WANs
Physical Layer