CA169: Week 3

Layered Architectures, OSI & TCP/IP

The Need for a Layered Architecture

- Think about everything that has to happen when you load a webpage
- There are a lot of parts at play
    - Chrome
    - Operating System
    - LAN/Wifi
    - The internet
    - Servers

Layered Architecture

- To accomplish all of this we break the problem into different parts
- E.g. your network card turns 1's and 0's into something understandable
- Your router knows where it needs to send your requests to
- Chrome knows how to load and display a webpage
- We call this setup a layered architecture
- The bottom layer is the 1's and 0's
- The top layer is a webpage
- And there are many parts in-between
- In networking there are two main architectures you need to know
- OSI (Opsn Systems Interconnection) Model
- TCP/IP Model
- One is real the other is theoretical

OSI

- OSI is not real
- It is more a blueprint on how to build a network architecture from scratch
- There are 7 layers to the OSI model
- These will be on your exam !
- (They also come up in job interviews!)

OSI Model

7. Application Layer (Top Layer)
6. Presentation Layer
5. Session Layer
4. Transport Layer
3. Network Layer
2. Data Link Layer
1. Physical Layer (Bottom Layer)

OSI Application Layer

- Represents the level at which applications access network services.
- This layer represents the services that directly support applications such as software for file transfers, database access, electronic mail.
- TLDR; Applications that use the web; chrome, mobile apps etc…

OSI Presentation Layer

- Translates data from the Application layer into an intermediary format.
- This layer also manages security issues by providing services such as data encryption.
- It also provides compressed data so that fewer bits need to be transferred on the network.

OSI Session Layer

- Allows two applications on different computers to establish, use, and end a session.
- This layer establishes dialog control between the two computers in a session, regulating which side transmits, plus when and how long it transmits

OSI Transport Layer

- Handles error recognition and recovery.
- Repackages long messages when necessary into small packets for transmission and, at the receiving end, rebuilds packets into the original message.
- The receiving Transport layer also sends receipt acknowledgments.

OSI Network Layer

- Addresses messages and translates logical addresses and names into physical addresses.
- It also determines the route from the source to the destination computer
- Manages traffic problems, such as switching, routing, and controlling the congestion of data packets.

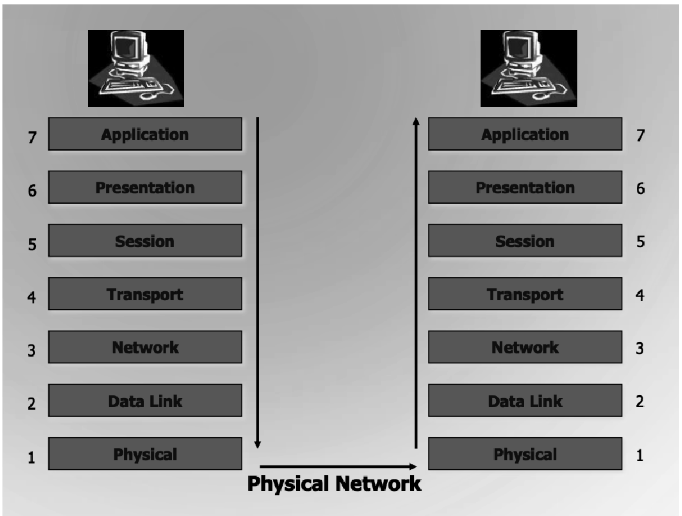
OSI Data Link Layer

- Packages raw bits from the Physical layer into frames (logical, structured packets for data).
- This layer is responsible for transferring frames from one computer to another, without errors.
- After sending a frame, it waits for an acknowledgment from the receiving computer

OSI Physical Layer

- Transmits bits from one computer to another and regulates the transmission of a stream of bits over a physical medium.
- This layer defines how the cable is attached to the network adapter and what transmission technique is used to send data over the cable.
- TLDR: What we covered last week!

OSI Model



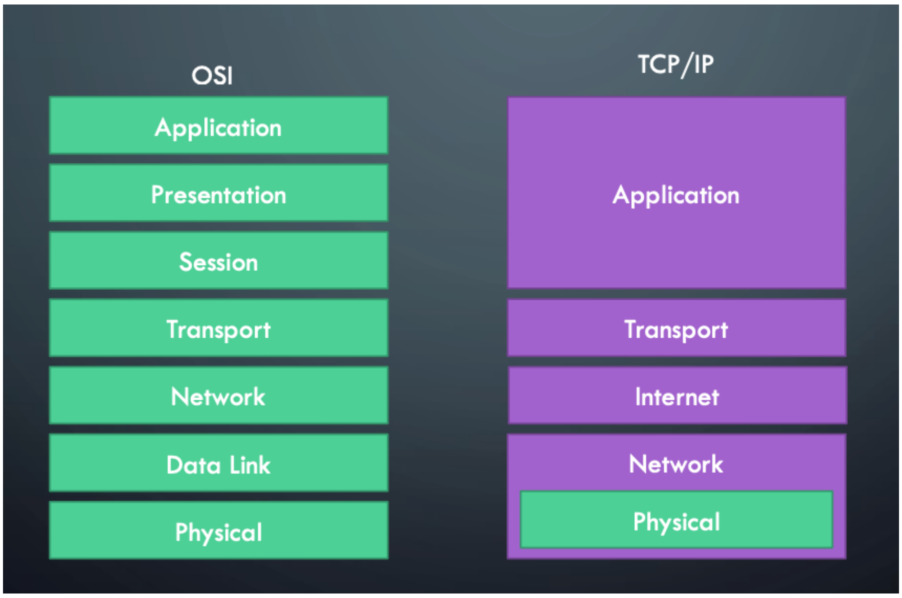
OSI Summed Up

- 7 Layers
- Guidebook on how to build a network from
- scratch
- Not real !
- Will be on your exam !

TCP/IP

- OSI is a theoretical architecture for building a network
- TCP/IP is the real version
- TCP/IP is how the internet works
- The OSI model has 7 layers
- The TCP/IP model has 5 layers
- This is because some layers in the TCP/IP model can do the work of two layers in the OSI model
-

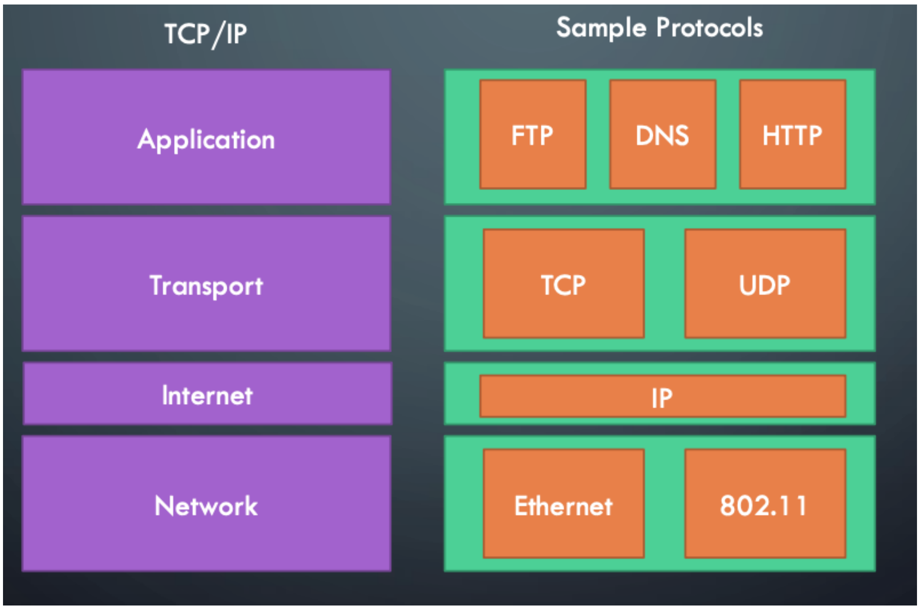
TCP/IP v OSI



TCP/IP & OSI

- Transmission Control Protocol / Internet Protocol (TCP/IP) is the protocol on which the Internet is based upon.
- It has five layers and they are related to the OSI model.
- Information is transmitted around the Internet in packets.
- These packets contain among other things the destination and source addresses of the packet and the data
- The protocol used is TCP/IP.
- Internet Protocol is protocol, which sends packets around the Internet.
- TCP sits on top of IP and it guarantees reliable delivery of packets for applications such as FTP and Telnet.
- An end-to-end connection is open for the delivery session between two applications

TCP/IP Family



Why Have Two Models

- OSI concepts
  - Services (definition)
  - Interfaces (how to access)
  - Protocols (peer protocols, private)
- Kind of OO approach, encapsulation.
- Prescriptive & Descriptive origins
  - Simple services, interfaces, protocols

OSI - TCP/IP Physical & Network Layers

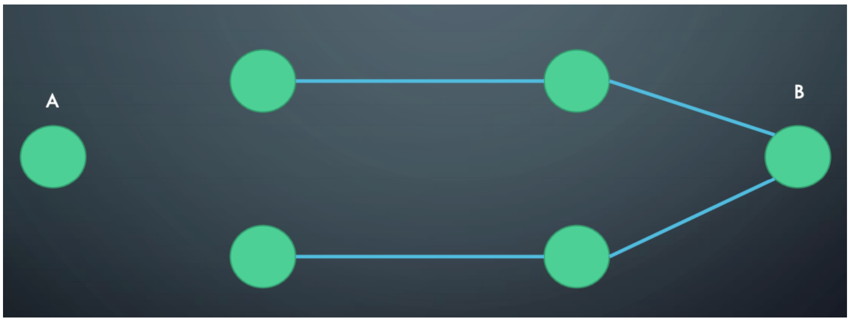
- Last week we looked at how we can transmit data
- We learned how modems turn electrical signals into digital and vice versa
- We looked at how we can detect errors, and why we need protocols
- Finally we looked at the sliding window solution for packets arriving out of order
- Now we are going to examine how a packet travels across the internet
- We will look at real world physical and network layer protocols
- 802.3 LAN
- 802.11 WiFi

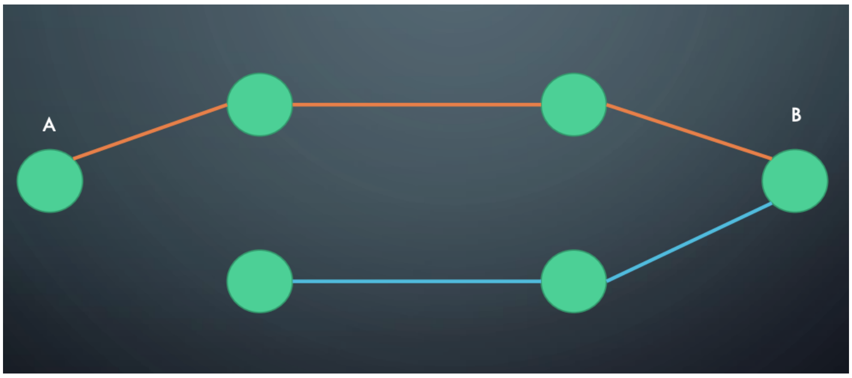
Switching

- When you send a packet across a network, how does it actually get to its destination
- This process is called switching
- There are three kinds of switching:
    - Circuit Switching
    - Message Switching
    - Packet Switching

Circuit Switching

- Like old fashioned terrestrial telephone system.
- Try to form dedicated physical path from source to destination.
- Path remains dedicated until session is terminated.
- Not typical operation of bursty comms.





Message Switching

- No physical path established.
- Large bursts of data transmitted from sender to receiver.
- Each burst stored and forwarded from host to host throughout network.
- No limit to burst size, may encounter memory\buffering and link availability problems.
- Not really used anymore
- Data is sent as one large “chunk” across the network
- Used in older technologies
    - E.g. telegrams, teletype

Packet Switching

- Upper limit set on size of blocks to be transmitted.
- Ideal for bursty computer communications.
- May utilise pipelining to improve throughput.
- Large packet size will emulate message switching, small emulates circuit switching.

Packet vs Circuit Switching

Item	Circuit Switched	Packet-Switched
Call Setup	Required	No
Dedicated Physical Path	Yes	No
Each packet follows same route	Yes	No
Packets arrive in order	Yes	No
Is crash fatal?	Yes	No
Bandwidth Available	Fixed	Dynamic
When can congestion occur	During Setup	On every packet
Potentially wasted bandwidth	Yes	No
Store and forward information	No	Yes
Transparency	Yes	No
Charging	Yes	No

Local Area Networks and 802

- IEEE formulated 802 standard for LAN.
- ITU (CCITT) adopted 802 as 8802
- Common media types are UTP and Co-axial cable.
- Topologies may be Ring\ Bus\ Star or Wireless.

802 Organisation

- Layered within the Data-link and Physical layers of OSI protocol stack.
- Composed of
    - Physical Medium Dependent (PMD) layer.
    - Medium Access Control (MAC) layer.
    - Logic Link Control (LLC) layer.

802 Standards

• 802.2 LLC (HDLC based)
• 802.3 CSMA/CD Bus (Ethernet)
• 802.4 Token Bus
• 802.5 Token Ring
• 802.6 DQDB
• 802.7 Broadband LAN using Coaxial Cable (disbanded)
• 802.8 Fiber Optic TAG (disbanded)
• 802.9 Integrated Services LAN (disbanded)
• 802.10 Interoperable LAN Security (disbanded)
• 802.11 WiFi
• 802.12 demand priority (disbanded)
• 802.13 Not used (officially)
• 802.13ah Defines "Copper for the first mile" for Metro Area Networks (proposed)
• 802.14 Cable modems (disbanded)
• 802.15 Wireless PAN
• 802.15.1 Bluetooth certification
• 802.15.2 coexistance of 802.15 and 802.11
• 802.15.1 (Bluetooth certification)
• 802.15.4 (ZigBee certification)
• 802.16 Broadband Wireless Access (WiMAX certification)
• 802.16e (Mobile) Broadband Wireless Access
• 802.16.1 Local Multipoint Distribution Service
• 802.17 Resilient packet ring
• 802.18 Radio Regulatory TAG
• 802.19 Coexistence TAG
• 802.20 Mobile Broadband Wireless Access
• 802.21 Media Independent Handoff
• 802.22 Wireless Regional Area Network

Ethernet Networks 802.3

- May operate over several cable types.
- 10 Base 2 Thin wire coax, bus topology.
- 10 Base 5 Thick wire coax, bus topology.
- 10 Base T Twisted pair, star topology.
- 10 Base F Optical fibre, star topology.
- 100BASE-TX fast Ethernet over 100Mbps 802.3u
- 1000BASE-T Gbit/s Ethernet over twisted pair
- Today many types of Gbps versions over fiber depending on type of lasers used.

Ethernet Uses MAC Addresses

- 48 bit unique identifier
- Tied to a network card
- Written in hexadecimal
- Written as: D4-3B-04-1F-AD-88

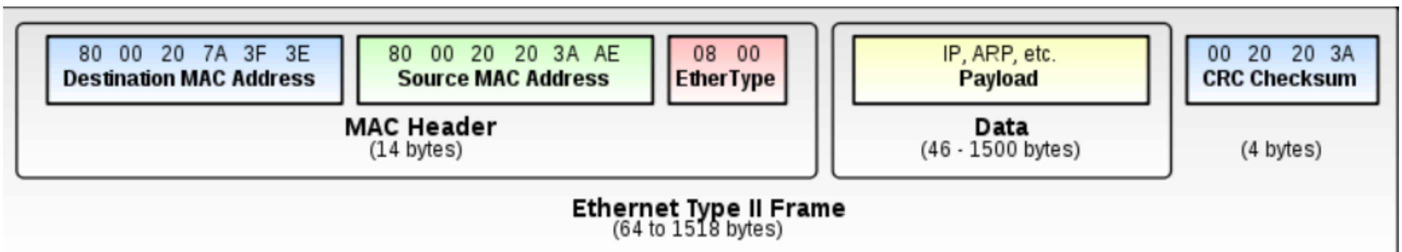
802 Frame Format

Preamble	SD	Dest Addr	Src Addr	LD	Data	Pad	CRC

- Preamble (7 bytes): Sine wave, clock synch.
- SFD – Start Frame Delimiter (1 byte): 10101011 denoted.
- Dest Addr: 6 byte unique 802 address.
- Src Address: 6 byte address, 248 possible.
- LD: Size of payload.
- Data: Payload max 1500 bytes.
- Pad: Ensures min size of 64 bytes.
- CRC: As discussed previously.

Ethernet II or DIX Frames

- Defines the 2 octet Type field (LD previously), defining the upper layer protocol encapsulating the frame data
- 0x0800 indicates IP V4
- 0x0806 is ARP
- 0x06DD is IP V6
- Must be greater than 0x0600 (1,536 decimal, > 0x05DC or 150010 the max payload of Ethernet)



Coexistence of Ethernet & Etherent II

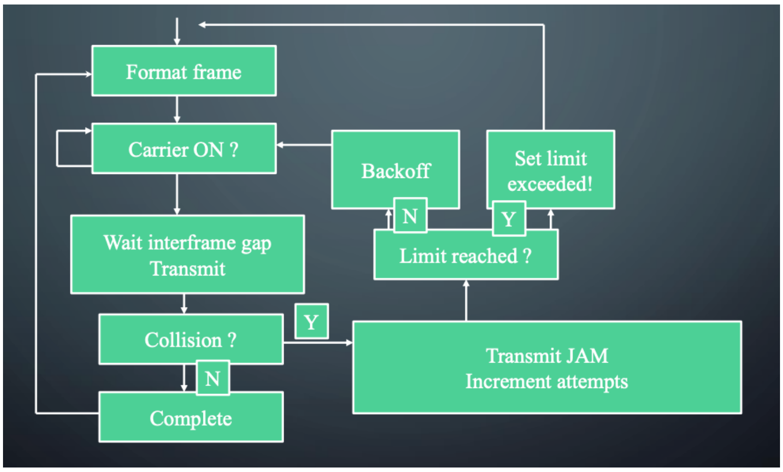
- Both types can exist on the same Ethernet network.
- Distinguish V1 and V2 by value in type field
- For V2, value in type field must be >=1,53610 or 0x600
- Maximum payload for Ethernet is 0x05DC or 1,50010
- For V1, value must be <= 150010 or 0x05DC

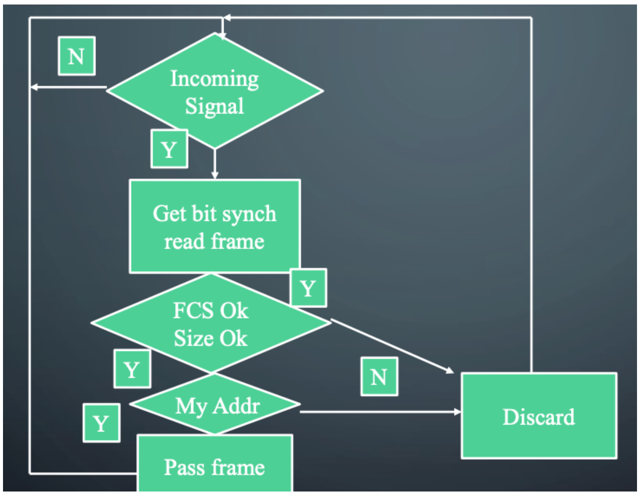
Ethernet II Types

- EtherType value
- 0x0800 signals that the frame contains an IPv4 datagram
- 0x0806 indicates an ARP frame,
- 0x8100 indicates an IEEE 802.1Q frame (Virtual Lan)
- 0x86DD indicates an IPv6 frame.

802.3 MAC

- Carrier Sense Multiple Access with Collision Detection CSMA\CD
- Allows multiple stations to share transmission medium.
- Senses carrier to see if medium is quiet.
- Be able to detect if another station is interfering by continuing to listen to carrier while transmitting.





Truncated Binary Exponential Backoff

- When collision is detected, two stations wish to transmit simultaneously.
- Need to prevent continuous collisions between this pair.
- Better to have graceful degradation of throughput.

Algorithm

- The number of slot times before the Nth retransmission attempt is chosen as a uniformly distributed random integer in the range
  - $0 \le R \le 2^k$
  - where K = min(N, backoff limit),
  - e.g. for a backoff limit of 20, possible ranges of K will be 0..2, 0..4, 0..8, 0..16, 0..20, 0..20, 0..20 for successive attempts at retransmission up to a maximum number of attempts.
- The backoff limit of 20 is imposed and prevents the series continuing 8, 16, 32, 64, etc, etc and thus the heuristic is called truncated binary exponential backoff.

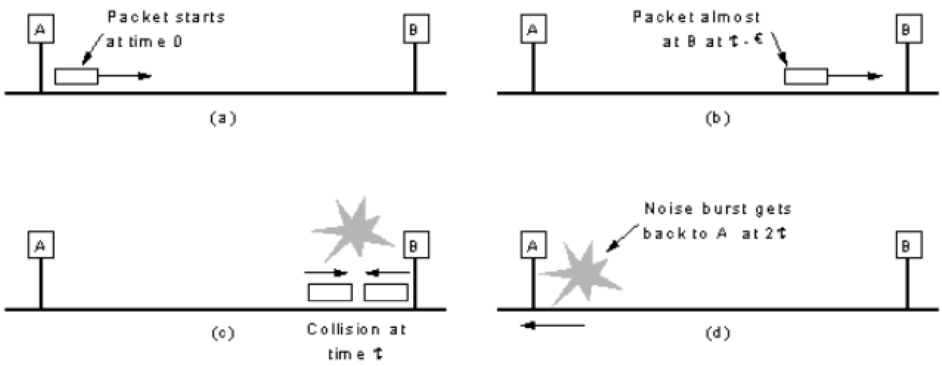


Fig. 4-22. Collision detection can take as long as 2τ.

802.3 Modern Implementations

- Most modern implementations of Ethernet use Switched Ethernet.
- There are almost no collisions
- Packet paths can cross over the switch without colliding, provided each "conversation" has no receivers in common
- Improved throughput and better utilisation

A Switch