**OSI Model vs TCP/IP (what we use in class)**

-Application: Many - HTTP. Everything application specific

-Presentation: Only in OSI. Presentation of data.

-Session: Only in OSI. Multiple related connections, e.g. audio + video go together.

-Transport: few – 99% TCP or UDP - End to end, not concerning middle devices. Security, error checking allowing endpoint to do error checking

-Network: one-ish - IPv4 or IPv6 - Getting from one device to another. IP addressing, routing, forwarding

-Link: Many, roughly same as physical- Ethernet II. - getting from one device to next device. MAC addressing, identify start/end of packet (framing), error detection.

-Physical: Many- physical representation of bits, structure of cables. Bit representation, cable standards, multiplexing

There are security protocols at all levels. Link- wifi securing, Network- vpn, Application- app specific

**Groups Responsible for Protocols**

IEEE- Institute of Electrical and Electronics Engineers

IETF- Internet Engineering Task Force

ICANN- Internet Corporation for Assigned Names and Numbers

IANA- Internet Assigned Numbers Authority

**Processing Time**

Propagation Time = distance/speed = time for a bit to travel

Processing Time = time for devices to process

Transmit Time = size/data rate = time from putting first bit on line to putting last bit on line

Queueing Time = time stuck in traffic

**Max Data Rate Formulas**

β = Bandwidth

V = Signal Levels, e.g. 2 would be 0 or 1, 4 would be 11, 10, 01, or 00 2 bits per signal

S/N = Signal Noise Ratio- Signal Power/ Noise Power

*C* is the channel capacity in bits per second, a theoretical upper bound on the net bit rate (information rate, sometimes denoted *I*) excluding error-correction codes;

*B* is the bandwidth of the channel in hertz (passband bandwidth in case of a bandpass signal);

*S* is the average received signal power over the bandwidth (in case of a carrier-modulated passband transmission, often denoted *C*), measured in watts (or volts squared);

*N* is the average power of the noise and interference over the bandwidth, measured in watts (or volts squared); and

*S/N* is the signal-to-noise ratio (SNR) or the carrier-to-noise ratio (CNR) of the communication signal to the noise and interference at the receiver (expressed as a linear power ratio, not as logarithmic decibels).

**Shannon’s Theorem - Look at more in depth tomorrow**

C = β \* log2(1 + S/N)

**Nyquist Theorem - Look at more in depth tomorrow**

C = 2 \* β \* log2(V)

a noiseless 3-kHz channel cannot transmit binary (i.e., two-level) signals at a rate exceeding 6000 bps.

a channel of 3000-Hz bandwidth with a signal to thermal noise ratio of 30 dB (typical parameters of the analog part of the telephone system) can never transmit much more than 30,000 bps

The minimum of both of these is the allowable rate

**Bit Encoding Methods**

Baseline Wander- baseline is average voltage. If it gets too high, what is meant to be a high could fall below the baseline. If it gets too low, what is meant to be low could go above the baseline. Use 4b/5b encoding to ensure wander doesn’t get terrible.

Baud Rate- number of symbol changes or pulses per second. Different from Bit Rate is multiple bits per symbol, i.e. signal level over 2.

NRZ- Non Return Zero- 0s are low, 1s are high

Manchester- Reads multiple times per bit to detect changes and to see if baud rate is right. 0 is high to low, 1 is low to high.

NRZi- changes voltage on 1s and stays same on 0. No baud rate increase is necessary like in Manchester. Tons of 0s will skew baseline and mess up clock. Changing voltage on 0 and staying same on 1s is opposite, but also called NRZi.

AMI- uses 4b/5b encoding. 0 is a middle signal level. A 1 is a high signal, then the next 1 is a low signal, next is high, next is low, etc. 0s are in between.

4b/5b encoding- 4 bits of data becomes 5 bit code word. No code word has more than 1 leading 0 or more than 2 trailing 0s. This ensures there will be a 1 at least every 4 bits.

**QAM** Quadrature Amplitude Modulation

On Cartesian plane, used like radians. Phase is angle, and amplitude is radius.

Each adjacent point to a given point only varies by one bit.

Grey coding allows for minimal error in this way.

**Framing** Identifying start/end of a frame or a packet

Start- a flag.

PPP (Point to Point Protocol) used by dialup uses a 1 byte flag 01111110

Ethernet uses 8 byte flag 01010101x7 01010111

End a flag

PPP- 01111110

**Byte Stuffing**

Sender, any time flag (01111110) is in data use escape character of 01111101 preceding flag

Sender, any time escape character is in data, send escape character before that

Receiver, any time escape character is in data, remove it and read the next byte as data

**Bit Stuffing**

Sender, any time there are 5 1s in a row, insert a 0 after it

Receiver, any time there are 5 1s in a row, then a 0, remove the 0.

Any time there are 6 1s in a row, that is the flag

**Error Checking**

Done in multiple layers. These check for accidental random errors introduced.

Error Correcting is not widely used. Used when re-sending packets would be expensive. E.g. Mars Rover

Error Detecting is widely used. Packet can be re-requested or dropped if acknowledgements are being used.

Parity: send 9 bits for every byte. Make # of 1s even using the last bit. Can’t detect when an even number of bits are changed. XOR all bits together to get parity bit.

**Reliability**

Acknowledgements allow sender to know what packets were received.

Stop-and-Wait: Sender sends single packet. Receiver sends acknowledgement. If sender gets ack, move on to next packet. Essentially sliding-window with window size 1.

Sequence Number: each packet has a sequence number so the receiver can know if a duplicate is received. Range of sequence numbers needs to be 2x window size.

Sliding-Window: Window size is known by sender and receiver. Sender sends window of packets. Receiver acknowledges any packets it receives. If sender receives ack for 1st packet in window, slide forward, send new packets in window. Receiver has a buffer for the packets. If a packet is received, space is left for it in the buffer so they are placed in order.

Cumulative Acknowledgement: sending an acknowledgement for 3 means packets 1-3 were received. Don’t need to send as many acknowledgements this way.

**Sharing Transmission Medium**

TDMA - Time Division Medium Access - devices get timeslots – can only send in your timeslot, might not have stuff to send when it’s your timeslot.

FDMA - Frequency Division Medium Access - giving certain devices certain frequencies

CDMA - Code Division Medium Access

**CSMA** - Carrier Sense Medium Access

1-Persistent CSMA used by Ethernet (CSMA/CD[collision detection]). Check if line is idle. If yes, send. If no, wait for idle, then send immediately.

Non-persistent CSMA Check if line is idle. If yes, send. If no, sleep random time, then repeat.

P-persistent CSMA Check if line is idle. If yes, send w/ probability P. If probability fails, repeat. If line not idle, wait for idle, then send w/ probability P. Ex. With p = 0.05. Generate rand num 0-1. If less than 0.05, send packet. If miss, sleep rand time and check again. 1-persistent is P-persistent with p = 1.

**CSMA/CD**

Simple collision checking would be seeing if acknowledgement was received. Ethernet does not have acknowledgements though.

Ethernet can send and receive at the same time. If what was received differs from what was sent, there was a collision. Transmission time must be ≥ 2 \* propagation time to detect collision.

**Exponential Backoff**

When to resend after collision detected. N = number of collisions experienced for current message. Choose random k ∈ 0…2N. Wait k \* 512 bit times (a bit time is time necessary to put a bit on the line. E.g. 10 Mb = 10 million bits per second, 1 10 millionth of a second bit time)

**Ethernet Frame**

(start of frame)8B\_(dest addr)6B\_(src addr)6B\_(type)2B\_(data)\_(CRC)4B

Type indicates IPv4 or IPv6

CRC (Cyclic Redundancy Check) for error checking

Start of frame is 01010101(x7) 01010111, indicating frame start

Ethernet frame doesn’t say data length, so we check in network layer for the length

These addresses are MAC addresses.

No acknowledgements or requests with packets. Packets with errors are just discarded.

Network card chops off start of frame and CRC before OS sees packet. OS doesn’t create CRC, this is done by the NIC (network interface controller).

**MAC Addresses**

Every MAC address on a network should be unique. To ensure they are locally unique, they are made globally unique. Every network card manufactured is given a unique MAC address. First 3 bytes indicate manufacturer. Last 3 bytes assigned by manufacturer. MAC address can be changed on a device.

**WIFI Frames**

Data

Management

Beacon- sent by access points so devices can find networks

Association Request- request to connect to network

Association Response- response to request

Authentication Request- send password to authenticate

Authentication Response- response from router to requesting device

Control

RTS- request to send- used for medium access for collision avoidance

CTS- clear to send- used for medium access for collision avoidance

ACK- acknowledgement

Wireless is less reliable (huge possibility for interference), so there is need for acknowledgements.

**WIFI Frequencies**

FCC controls what frequencies are used for TV, Radio, Cell Phones, etc.

WIFI frequencies- 2.4GHz and 5 GHz, not controlled by FCC, used by other things as well

**802.11 IEEE Specifications**

802.11b- 2.4GHz, spread spectrum

802.11a- 5GHz, no spread spectrum, faster than b, but less range

802.11g- 2.4Ghz, no spread spectrum, faster than b, more range than a

802.11ac- 2 antennae at once, signals interfere, but the interference is mathematically dissected to reveal the original signals

**WIFI Protocol**

Power Management Bit- notifies devices via the beacon frame if there is data waiting. If sent to router, lets router know that we are participating in power management.

**WIFI Connections**

Hub- physical layer device, receives a message in 1 interface and broadcasts on all others. Increased collisions due to not directing traffic. Cheap and easy to implement.

Switch/Bridge- link layer device, directs traffic based on MAC address. Requires no configuration to work, but not scalable (only supports on the order of tens or hundreds of devices).

Router- network layer device, directs traffic based on IP address. Scalable, must be configured with network information.

**Switch Network Configuring**

A network of switches must create a spanning tree to remove loops. Switches send out configuration method containing, here’s who I think the root is, here’s who I am, here’s my distance from the root. (MAC addr, MAC addr, # of hops). They must use the same algorithm for choosing the root, so the use the device with the lowest serial number.

**Network Layer IPv4 and IPv6**

Versions 1-3 are obsolete, used only in 70s. Version 5 was skipped.

**IPv4** 32 bits, 5 classes of addresses

Class- first bits- network bits- host bits;

A- 0- 7- 24;

B- 10- 14- 16;

C- 110- 21- 8;

D- 1110- multicast;

E- 1111- reserved for future use;

**CIDR** Classless Inter-Domain Routing

Any size prefix is allowed (prefix determines the network.

1.2.0.0/16 notation means first 16 bits signify network. Network is any IP starting with 1.2

When allocating addresses, the first address has to have all 0s in the host bits.

A company wants 1000, so the get 1024, 210. First address 1.2.0.0, last address 1.2.3.255, prefix would be 1.2.0.0/22.

Next company wants 498, so they get 512, 29. First address 1.2.4.0, last address 1.2.5.255, prefix would be 1.2.4.0/23.

Next company wants 1001, so they get 1024, 210. First address can’t be 1.2.4.0. It won’t fit and the host bits wouldn’t all be 0. They would instead start at 1.2.8.0 and go to 1.2.11.255, prefix 1.2.8.0/22

**IPv4 Header**

TTL- Time to Live, number of forwards before the packet is dropped (to prevent endless loops). Typically, a packet takes 16-20 hops to reach other side of world. TTL is set by OS to 32, 64, or 128.

TOS- Type of Service, or Quality of Service, provides different levels of priority.

Protocol- tells what protocol is used at transport layer (TDP or UDP)

IHL- Header Length, variable, extra options can be specified at end, but common case is no extra options- supported in hardware so faster.

**Fragmentation**- splitting the packet up to send on a link with a smaller maximum than the packet size.

ID = 1234, Length = 1500. 20 bytes IP header, so 1480 bytes of data. MF (more follow)= 0, DD (don’t fragment)= 0. Offset= 0. Offset is the number of bytes of data this packet is from the original start of the packet. MTU (Maximum Transmission Unit) = 532 bytes, 20 byte header + 512 data

Fragment- Length- Offset- MF;

1- 532- 0- 1;

2- 532- 64- 1;

3; 476; 128; 0;

Fragment 2 arrives at a link with MTU 280. We can’t send 280 because it would mess up offset, so we send 276.

Fragment- Length- Offset- MF;

a- 276- 64- 1;

b- 276- 96- 1; This more follows is true because fragment 3 follows.

**IPv6 Header**

128 bit addresses, as opposed to 32 bit with IPv4. 64 bit network prefix, 64 bits of addresses on each network. 264 is about 18 quintillion.

Flow Label- every packet belonging to same flow (transaction/communication) has same flow label.

Payload Length- length of data

Next Header- (TCP, UDP, ICMP) Transport Layer or Options header

Hop Limit- TTL Time to Live

What’s Missing:

Fragmentation: happens to very few packets. If fragmentation is possible, a fragmentation header is used in the next header field. New routers don’t do fragmentation because it decreases the workload on the router. The router drops the packet and sends an ICMP to the sender saying what size they need. The sender then makes the remaining packets the right size.

Variable Length: Use an Options header is options are to be used.

Check Sum: Reduces the work for the router. No error checking at network layer, but still exists at link layer and transport layer.

**ARP**

Used in IPv4, Address Resolution Protocol

**NDP**

Neighbor Discovery Protocol

**What these Are**

Way to get MAC address from IP address.

Ask the connections what the MAC address is belonging to that IP.

ARP has Ethernet Header which has Source MAC as self and Destination MAC as broadcast. ARP then has an ARP header which has Self MAC, Self IP, Target MAC = 0, and Target IP. ARP gets broadcast. If the target IP matches a device, the device caches the sender’s MAC and IP, make self MAC and self IP refer to device, target Mac and target IP refer to original sender, then swap the MAC address in the Ethernet Header and sends the ARP back.

NDP is similar in concept, different in implementation. Uses Ethernet Header, IPv6 Header, and ICMP Neighbor Discovery. NDP can’t be used by IPv4 devices, so most devices we use, use ARP.

**DHCP** Dynamic Host Configuration Protocol (uses DHCP server) used by IPv6

1. DHCP Discover- From Client to Server, destination= broadcast, source= 0, uses a specific port number

2. DHCP Offer- From Server to Client, source= Server’s IP address, contains offered IP address for the device that requested it. Also, IP addr of default router, IP addr of DNS server, and lease time.

3. DHCP Request- From Client to Server, same info as offer, client repeats to server to confirm. Destination = server’s IP addr, Source= The IP address offered

4. DHCP Acknowledgement- From Server to Client to confirm request.

Renewal process is just steps 3 and 4 done ½ way through lease time. If not on network at ½ way point, upon reconnect will try to renew.

**Stateless Auto Configuration** used by IPv6

1. Ask router what network prefix is.

2. Concatenate prefix | MAC addr to become the IP addr

3. Use Neighbor Discovery to check if addr already used.

**Line Coding**

Baseband- The baseband is defined as a transmission signal that contains more than just a single frequency from 0 Hz to the highest frequency component. In essence, the baseband is the original signal that is intended to be transmitted. However, this baseband frequency, when transmitted towards its target, can easily be slowed down or can pick up noise and distortion, which is why the original baseband signal must be transmitted into radio frequency. Radio frequency, however, also is at risk for transmission problems, creating the need for a band-pass filter.

Passband- The passband is the output of a band-pass filter. It is a signal that corresponds to the settings of the band-pass filter. While baseband is the original signal, passband is the filtered signal. Passband is more technically defined as the portion of the spectrum between limiting frequencies with minimum relative loss or maximum relative gain. Given the earlier example, a radio tuner set at 107.5 MHz will allow only 107.5 MHz to pass through. Anything below or above 107.5 MHz will be blocked by the filter