DCF255 Test 1 Review

Week 1: Overview

Terminology

- A computer is a programmable machine that can perform various computations, store data, and create documents by following a set of prerecorded instructions called a program. The data generated or stored by the computer is a collection of zeros and ones.
- Data communications is the sending of signals that represent zeros and ones over a point-to-point circuit between two computers.
- Networking begins when point-to-point circuits are joined together into a collection of computers for the exchange information and the sharing of resources.

Why should a programmer understand data communications?

1. Build better applications if you understand how network is organized and what happens in the network cloud as data is forwarded from host to host
2. Build better application if you understand how hackers can take advantage of a mobile app for malicious purposes
3. The "Network is now the computer"(John Gage). Programming started with data and code installed on the same machine. Using Internet technology, the cloud through virtualization can be used to host software (SaaS), platform (PaaS) and infrastructure (IaaS) . The cloud is now a platform for developing mobile applications and will increase in useage over time

History of Computing:

1. Host to mainframe – powerful centralizaed processing connected to dumb terminals
2. Client Server- powerfull distributed processing connected to PCs. Lower cost than mainframe
3. Internet – increased the usage of client server architecture and lead to n-Tier programming with separate user presentation frontend, a logic processing web services in the middle, linked to a database backend.
4. Cloud computing – extension of client server using virtualization to provide software, infrastructure or platfrom as a service.- changin the way IT dept and business function.

Week 2: Standards

Standards

For applications to share resources, communication standards must be worked out in advance called standards. National, International, Professional and Independent standard making bodies.

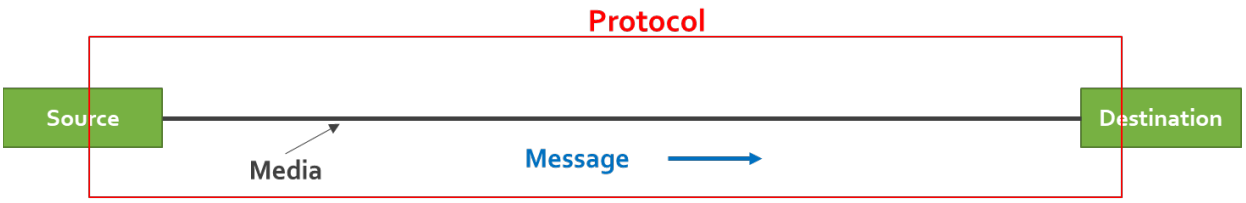
-1980's vendor lock in made computer networking expensive – no body happy – users not getting applcations they wanted, businesses had to buy software and hardware from same vendor, vendors not happy had to share source code with programmers to write applications – danger of intellectual theft.

-led to the ISO (International Organization for Standardization) to create a task force called the OSI (Open System Interconnection) to develop a set of protocols, to make interoperability of software and hardware purchased from different vendors.

Layers & Protocol - Data Communication

- The components involved in data communication are: Source, Destination, Media, Protocol and the message exchanged between the source and the destination.

- **Protocol-**The rules that allow two entities (source, destination) to exchange some message (text, audio, video) using a physical quantity (medium-wired/wireless).
- Protocols provide the common standardization and flexible interconnection of communication among different platforms and different kinds of computing equipment (interoperability) around the globe and locally.
- **Layer** - specific piece of software following some pre-defined rules of functioning in data communications.
- Layers are implemented at the source and destination and any piece of hardware which provides interfacing between the two.
- The task of the layer is to ensure that data is physically delivered to the destination without any errors.



Layered Model

-developed a layered architecture – each layer works independently of the other

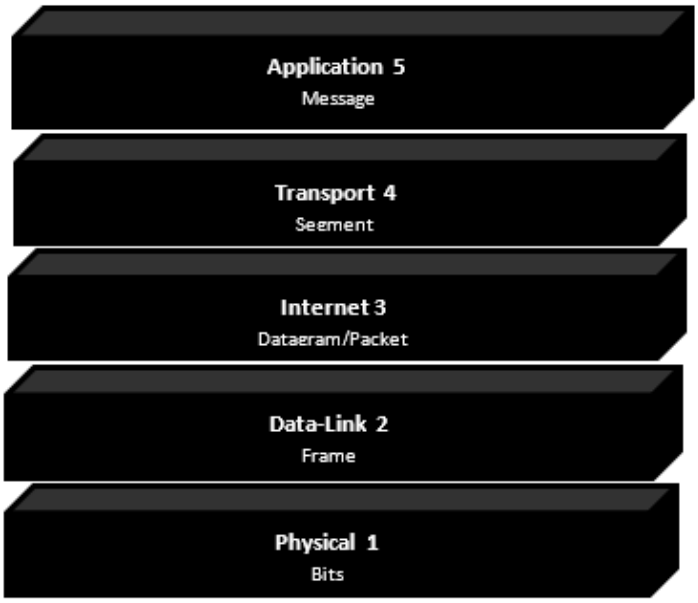
-each layer below provides a service to the layer above. – results in modular coding and specialization.

-OSI developed 7 layer model –Application, Presentation, Session, Transport, Internet, Data Link and Physical – it was expected that this new model would replace TCP/IP as the Internet protocol

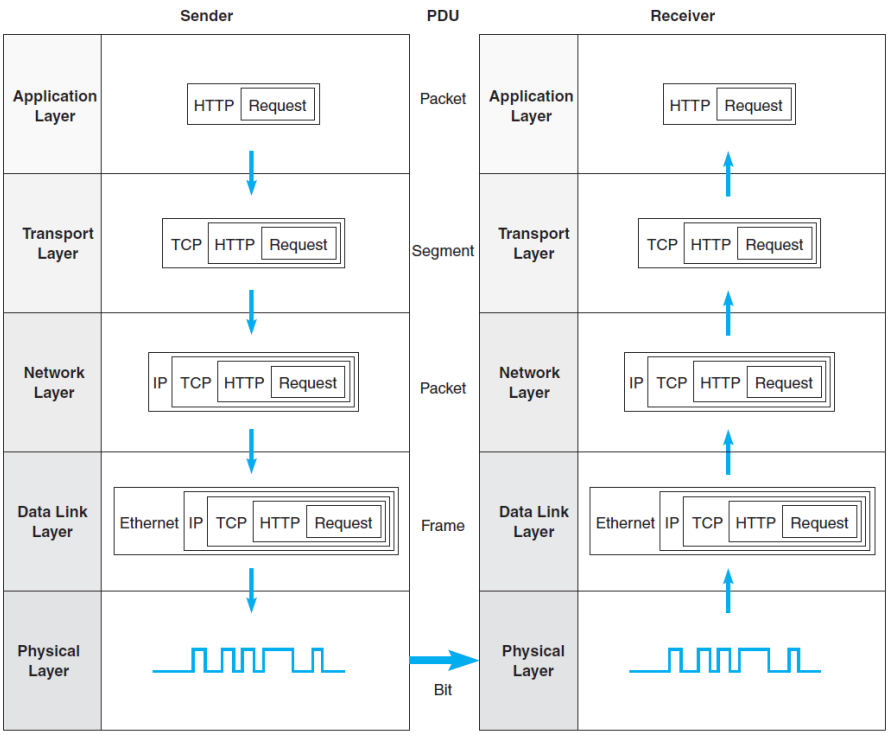
-did not happen because – OSI reported in 1993, the web was developed in 1991 and explosive growth by businesses, for email, web page sales, etc.

-also improvements in network speed and realibility, made the 7 layer model overly complex and cumbersome – consequently TCP/IP remains the dominant protocol for network communication

-but OSI dominates the bottom 2 layers, Data link and Physical –consequently we have a hybrid 5 layer model – TCP/IP top 3 layers, dealing with networking issues and bottom 2 layers OSI dealing with data communication issues. Appplications, Transport, Internet, Data Link, Physical



Message Transmission using Layers



The application layer defines the protocols to exchange data and specifies how applications can access the services of the other layers using sockets. A socket is an IP address and a port number, separated by a colon, such as **137.234.56.15:25**

Protocol Specification:

Protocol specification 4 parts: example http-- message type

-message syntax

-message sequence

-type of connection

Message Type – GET – go get the file on the server and POST – here is the file to process

Message Sequence – who speaks first – only client can begin communication

Message Syntax – the organization of the message. – header added to front of data –trailer added to end of data

HTTP Request Message

The syntax of the HTTP request message is fairly simple. The screen shot shows the message sent to retrieve a web site called “danny.roy” on a server called people in a domain called “senecac.on.ca”.

```
GET /danny.roy/ HTTP/1.1\r\n
Host: people.senecac.on.ca\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
\r\n
```

- The first line specifies the GET method which requests a path to a file for retrieval and the version of HTTP used by the sender. Notice this line and all other lines end with a character return and a new line [CRLF]
- The second line specifies the host to which the request is sent people.senecac.on.ca
- The third line specifies the host browser and operating system used to send the request
- The fourth line specifies the language to be used in this case English US
- The fifth line specifies the type of compression to use, such as gzip or deflate
- The sixth line specifies the type of TCP connection in this case “keep-alive” means to keep the connection active over multiple request-response cycles. Without this, the TCP connection would end after each request-response cycle and would have to be re-established. Notice, the 2 blank lines at the end of the request; these lines are required and indicate the end of the header field. The data field is empty.

HTTP Response Message

The HTTP Response to the request contains the file requested in the data portion of the packet (not shown).

```
HTTP/1.1 200 OK\r\n
Server: Sun-Java-System-Web-Server/7.0\r\n
Date: Thu, 18 Feb 2016 00:03:37 GMT\r\n
Content-type: image/x-icon\r\n
Content-length: 1406\r\n
\r\n
```

- The first line begins with HTTP/1.1 which indicates the server has a compatible version. The 200 is a success code that the desired file is returned. The browser actually ignores this code; it is designed for humans to indicate the request was successful.
- The next line indicates the server that returned the request
- The next line gives the date and time the request was returned.
- The next heading specifies the content type which was returned, in this case an image file.
- Again, the end of the header is marked with 2 blank lines followed by the content returned in the data field (not shown). There is no trailer.

Type of Connection – determines the protocol to use – connection oriented –TCP – connectionless UDP

Character Encoding

Application Layer responsible for digital encoding of the message.

-unicode (universal encoding) can represent all of the worlds languages

-UTF-8 – Universal Coded Character Set + Transformation Format – 8-bit. Most popular web encoding system because it is fully compatible with ASCII)

a variable-length encoding system using 1 to 4 “octets” (1 byte is called an octet). The first octet representing the first 128 values is identical to ASCII, making UTF-8 a superset of ASCII and safe to use with programming languages that interpret only one byte encoded characters

Bits	Decimal Range	First Code Point	Last Code Point	Bytes used	Byte1	Byte2	Byte3	Byte 4
7	0-127	U+0000	U+007F	1	**0**xxxxxxx			
11	128-2,047	U+0080	U+07FF	2	**110**xxxxx	**10**xxxxxx		
16	2,048-65,535	U+0800	U+FFFF	3	**1110**xxxx	**10**xxxxxx	**10**xxxxxx	
21	65,536-1,112,064	U+10000	U+1FFFFF	4	**11110**xxx	**10**xxxxxx	**10**xxxxxx	**10**xxxxxx

-must demonstrate conversion – decimal to binary
-must demonstrate conversion – binary to hexadecimal
-must demonstrate conversion-hexadecimal to Unicode

-must demonstrate conversion- Unicode to UTF-8

1. What is the binary value of the decimal value 579? __ _____
2. What is the hexadecial value of the binary string 001001000011?_____
4. What is the decimal value of 1123 in Unicode? _____
5. What is the UTF-8 hexadecimal encoding of the Unicode value U+03FF?_____

Week 3: Physcial Layer

Electromagnetic Field – a moving magnet generates electricity and electricity generates a magnetic field accoring to the right hand rule.

Characteristics of Sigals – all signals have –

1. Amplitude – height of the waveform – measured in volts
2. Frequency – number of completed cycles of the waveform in 1 sec.
3. Phase – position of the waveform a specific point in time.

Types of Signals

1. Analog –continuous rising and falling of voltage – sine wave
2. Digital – discrete square waveform with threshold values

   Analog – can carry more signals than digital\

   Digital – less affected by noise

Digital Data Carried by Digital Signal

- NRZI – non return to zero inverted – very efficient – change in voltage at beginning of clock cycle is a 1 no change in voltage is a 0 – baud rate ½ bit rate on average
- 4B/5B – converts 4 bits of original data into a special 5 bit transmission code which has no more than 2 consecutive 0s. – the 5 bit code is encoded using NRZI. – used on GigE and fiber optic cables

Analog Data Carried by Analog Signal

- AM radio – example –music signal is added to a powerful carrier signal set to a licensed Amplitude. –Tune radio to the amplitude and get the music signal

Digital Data Carried by Analog Signal

- ASK – Amplitue Shift Keying – uses different heights of the waveform to represent 0 and 1
- FSK –Frequency Shift Keying –uses different frequencies of the waveform to represent 0 and 1- used extensively on cable TV systems
- PSK – Phase Shift Keying – uses different phases of the waveform to represent 0 and 1

Analog Data Carried by Digital Signal

- 3 step process
- Analog data waveform is "sampled" – measures the amplitude at fixed internals
- Sampled amplitude – converted to a 7 bit digital value
- To play back the digital value, a special chip on audio card called PAM (Pulse Code Modulation) reads the digital value and recreates the amplitude waveform
- Not perfect representation – CD quality means that waveform must be sampled 2X highest frequency (Nyquist's theorem) – 700 Hz – wave –needs to be sampled 1400 times per second to get a good representation of the waveform
- Can loose sound in original or create noise not in the original

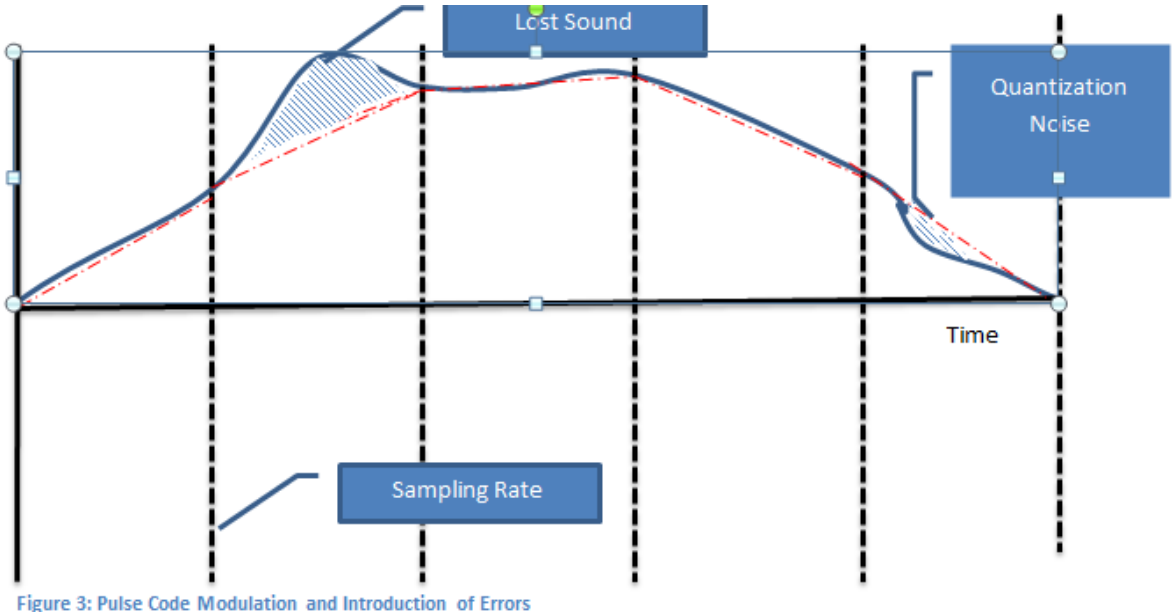


Figure 3: Pulse Code Modulation and Introduction of Errors

Relationship between Frequency and Bit Rate

- To increse network speed must increase the frequency of the wave to send more bits
- Or keep the frequency the same and send more bits per clock cycle.
- Shannon's Theorem is used to calculate the maximum of an analog signal with any number of signal levels based on the level of the noise.

Data Rate = f X $\log_2$ (1 + S/N)

f – bandwidth of the signal

S – power of the signal in watts

N – power of the noise in watts

Programming in Analog

With analog signals being a continuous rising and falling of voltage, the programmer would have to make a decision as to the amplitude to use. Analog signals are affected by noise, so if noise entered the system, the receiving computer may miss interpret the amplitute.

Metric Notation

Prefix	Name	Example	Description
P	Peta	1,000,000,000,000,000	One thousand trillion
T	Tera	1,000,000,000,000	One trillion
G	Giga	1,000,000,000	One billion
M	Mega	1,000,000	One million
K	kilo	1,000	One thousand

- If youu are converting from a smaller unit to a larger unit (moving upward in the table shown above), move the decimal place to the left in the number you are converting (dividing by 1000).
- If you are converting from a larger unit to a smaller unit (moving down in the table), move the decimal to the right (multiple by 1000).
- The number of places you move the decimal corresponds to the number of rows you are crossing in the table. For example, let's say you want to convert 8,500,000 bps to Mbps. Mega is two rows up so the decimal should be moved six places to the left to create 8.5 Mbps.
- Proper notation should always have one to three digits before the decimal point. So 8.5Mbps is good (1 place), but 8,500.0 kbps is bad (4 places.).

- You place a space between the number and the metric prefix, but not between the metric prefix and the base unit. For example, writing 8.5 Mbps is good, but writing 8.5M bps or 8.5Mbps is improper

Types of Cable

1. **UTP/STP**

- UTP refers to "Unshielded Twisted Pair" cable.
- Four pairs of wires each twisted around the other, inside a PVC protective jacket. Two wires carry equal but opposite signals; with the cables twisted, the flow of electrons generates opposite electro-magnetic fields minimizing crosstalk.
- STP stands for "Shielded Twisted Pair" where the wires are wrapped in a shielding which protects the signal from external EMI and increases attenuation by having electrons bounce back to the center of the cable.
- The most popular network cables today are CAT5e and CAT6 cables
- UTPs' popularity is a result of its ease of use and expandability using the RJ45 connector

2. **Coaxial**

Figure 1: UTP and STP cables (htt)

- Coaxial cable conducts electrical signal using a solid copper wire surrounded by an insulating layer and all enclosed by a shield of woven metallic braid which are soldered at the ends to the BNC connectors.
- The shield protects the signal from outside EMI and preventing electron leakage from the centre of the cable.
- This property makes coaxial cable a good choice for carrying weak signals Coaxial cable is commonly used in CATV and RF installations.

3. **Fiber Optic**

- A single fiber optic cable can carry about 90,000 TV stations, or 3 million full duplex telephone conversationFiber optic cables are bundles of glass fibers, smaller than a human hair, which are combined into a single cable.

    - Core - Thin glass center of the fiber where the light travels
    - Cladding - Outer optical material surrounding the core that reflects the light back into the core
    - Buffer coating - Plastic coating that protects the fiber from damage and moisture
- Light travels in a straight line and only in one direction at a time.
- The inside of the cable is like a mirror; so that light can travel down the core.
- Advantage - the light wave can travel great distances and is impervious to EMI and wiretapping.

Types of Connections

1. DSL – Digital Subscriber Line – dedicated circuit to Telcom – always on and provides high speed internet using UTP

- Speed decreases the fartheryou are from switching centre
- DLS is multiplexed using a DSLAM – DSL Access Multiplexer
- Modem converts digital signal to discrete analog signal
- Assymetric – fast download, slower upload

2. Cable Modem

- Used CATV cable to provide internet access – uses coaxial
- The broadband signal splits CATV channels from the Internet channel.
- Assymetric speed like DSL
- Unlike DSL cable bandwidth shared - as traffic increases overall throughput decreases.
- Each cable modem uses Ethernet to connect to the local network providing DHCP services to local hosts. The cable modem works with the service provider's cable modem termination system (CMTS) at the head office.
- The CMTS is responsible for connecting a group of customers to an Internet Service Provider (ISP) for connection to the internet. Downloaded Internet content is demodulated using QAM converting the radio frequency into a unique binary value.
- The upstream content is modulated using Quadrapture Phase Shift-Keying (QPSK). This modulation technique moves 2 bits at a time. A zero is represented as a 90 degree shift change and a 1 is the same waveform

3. Bell Fibe

- An all-digital IPTV streaming service,
- and delivered on Bell's high-speed fiber optic network. On the customer end is the IPTV modem which connects PVR which contains 1 TB hard drive for recording programs. The PVR includes an integrated TV receiver which can be connected via coaxial cable, Category 5 cable or wirelessly using 5 GHz – 802.11n.
- each packet leaves the server only once, but is sent simultaneously to many different destinations using the IGMP (IP Group Membership Protocol)
- This means one server can send information to many clients as easily as to a single client using the RTSP (Real-Time Streaming Protocol).
- Changing channels is changing IPGP groups of users.
- Unlike Cable TV which sends the entire TV spectrum to the setup box which decodes appropriate channels, IP multicasting is more efficient in bandwidth because it sends only the selected channel to the appropriate IP group.

Week 4: Data Link Layer

Data Link Layer Functions

1. Data Framing: The data link layer is responsible for the final encapsulation of higher-level messages into frames so it can be sent across a single switched network by the physical layer. And the synchronization of machines at each end of the link

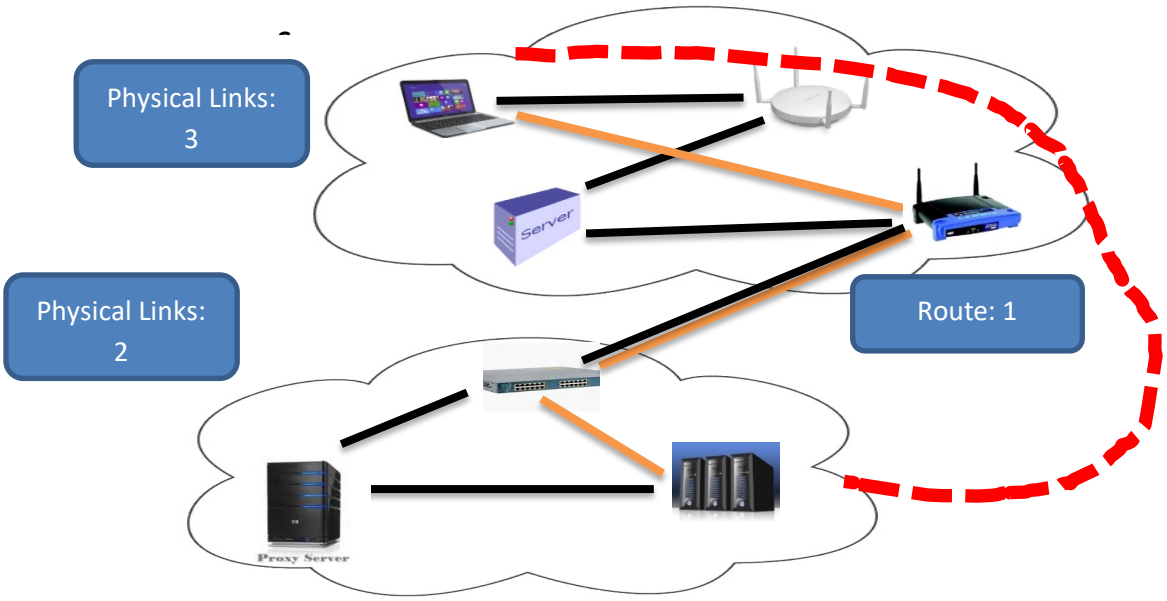
2. Media Access Control (MAC): On wireless networks or older non switched Ethernet networks, the DLL is responsible for setting rules to manage devices which share a common medium.

3. Addressing: Each device on a network has a unique number, usually called a hardware address or MAC address. The data link layer is responsible for adding the source and destination MAC addresses to the frame header to ensure proper delivery.

4. Flow Control: Some devices are faster processing in others, so the data link layer can control the speed of sending frames to avoid filling the receiving devices buffer capacity and lose frames.

Error Correction: The data link layer handles errors that occur in transmission using a Frame Check Sequence which allows the receiving host to detect if the data was received correctly

Seneca Case Study



The frame is forwarded link by link from Seneca Network to Microsoft's Network
Physical links – 6, (black)

Frames – 3 – a data llink is a path through one switched network to another. There are 3 data links – Host A to Seneca Router, Router to Router, Microsoft's router to Host B (orange)

The Data Link layer removes/adds frame headers and trailers at each data link so the frame can travel on the next link.

Packets – 1 Routes -1 There was only 1 packet sent and one route from Host A to Host B -logical

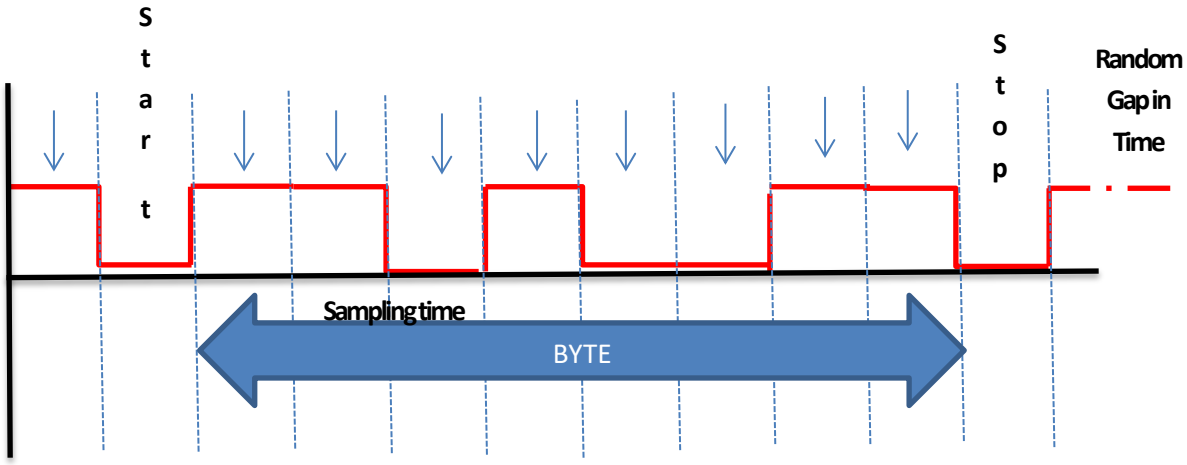
Synchronization Problem

Three methods have been developed to keep remote computers in time - even if they are in different parts of the world.

1. The best and most expensive way to keep computers in synch is to run a separate clocking wire to between them. Used on MANs and some WANs, expensive and not practical if great distance.

2. The second method is to develop an encoding system which is "self-clocking". Manchester encoding is self-clocking, but too inefficient for high speed. NRZI is more efficient

3. The third method is to transmit data asynchronously so that timing is less of an issue. applications like real time streaming or large data bases. Effecitive but too slow for data base or processor intensive applications.



4. The better approach is to create a synchronous transmission which is a large data block (for Ethernet the block is 1500 bytes – Payload is much larger than indicated in the diagram).

- The address field holds the MAC address of the sending and receiving devices.
- The Control field is one or more bytes and contains information about the type of frame
- The Payload of the frame is the data field sent from the higher layer and is completely transparent to the DLL.
- The CRC refers to the "Cyclical Redundancy Check" which is a two byte field. The value of these bytes is the result of polynomial arithmetic based on every bit of data between the flags. Detects 99.99% of all errors.

mission	Advantages	Disadvantages
Asynchronous	Simple, uses less hardware and programming. Equipment less expensive.	Low throughput because of high overhead and slower speed
Synchronous	High throughput because of less overhead and larger frame size	Requires more hardware and programming. Equipment more expensive

Data Link Layer Programming

Synchronous transmissions are the norm of network traffic.

- Each synchronous transmission has a flag of 126 in decimal or 7E in hexadecimal at the beginning and at the end of the frame. The flags are essential because they tell the receiving computer when a transmission starts and ends.
- The problem is if this value appears in anywhere else in the frame, the receiving computer could mistakenly interpret the value as the end of the frame. To avoid this program, the DLL layer has a build in programming routine called "bit stuffing".
- Data link layer counts the ones and if 5 adds a 0, the receiving host after removing the flags, counts the ones and if 5 ones followed by a 0, removes the 0.

Simplex Half Duplex and Full Duplex

- Simplex - the data can only travel in one direction receive or send, but not both
- Half-duplex- Send and receive but not at the same time
- Full duplex – send and receive simultaneously.

Common Transmission Errors:

- Noise is called "thermal noise. Or random "spikes" –EIA\TIA strick limits on cable lenth
- EMI causes errors when cabling is located too close to noise sources which generate their own electromagnetic field,
- Crosstalk is a special type of electromagnetic interference. Cables with electrons travelling in opposite directions can pull electrons off of one cable, and they travel on the other cable, in the opposite direction.
- Jitter occurs when two computers "drift" out of synch with each other. This can happen if the receiving computer begins to sample the voltage too near the end of a clock cycle, it can misinterpret the value.

Error Detection

- Parity -One extra bit is sent along with the original bits to make the number of 1s either even, in case of even parity, or odd, in case of odd parity. The sender counts the number of 1s and if the number of 1a is odd, the layer adds a bit to keep the parity even, if even parity is used(even parity is more common than odd parity)

- **Cyclic Redundancy Check (CRC) -** uses binary division combined with polynomial arithmetic to detect if the received frame contains - data. The divisor is generated using polynomials. The sender performs a division operation on the bits being sent and calculates the remainder. Before sending the actual bits, the sender adds the remainder at the end of the actual bits.

- The receiver performs a division operation using the same CRC divisor. If the remainder contains all zeros the data bits are accepted, otherwise it is considered as there some data corruption occurred in transit. The CRC seems complicated and slow, but it is very fast because it is built into the hardware. It all has the lowest overhead, less than 1% (16 check bits for a transmission of 1500 bytes). Lastly, studies have shown that the CRC can detect 99.99% of all errors.

Error Correction

In the digital world, error correction can be done in two ways:

- Backward Error Correction: When the receiver detects an error in the data received, it sends a requests back to the sender to retransmit the data unit.

- Forward Error Correction: When the receiver detects some error in the data received, it executes error-correcting code, which helps it to auto-recover and to correct some kinds of errors. –uses a combination of parity with hamming codes

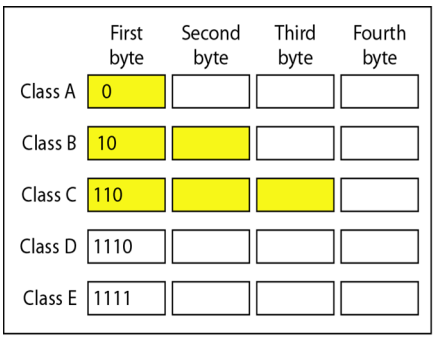
Week 5: Internet

The Internet layer accepts all input from the Transport layer as data. To the data, it adds a header which includes the IP address of the source and destination computer. The Internet layer is responsible for routing of the datagram from source to destination, deciding the best path among multiple paths. The path chosen to send the datagram is called the route.

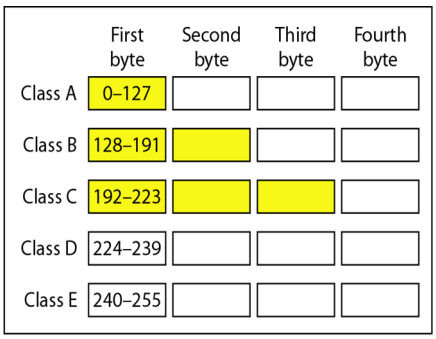
IPv4 and Changes to Preserve the Address Space

IPv4 is a classful addressing scheme and it has five classes as shown in the figure below. The first 3 classes A, B,C are used for one-to-one or unicast communication between source and destination. All internet communication is in general is unicast. Class D addresses are used for one to many known as multicast communication e.g. BellFibe and Rogers Ignite. The shaded yellow boxes in the figure below identifies the

network prefix or the number of bits used for network ID in each class, where the unshaded part represents the suffix or host ID.



a. Binary notation



b. Dotted-decimal notation

IPv4 addresses are 32-bit long, and written in dotted decimal notation. The total address space or the number of IPv4 addresses are **2^{32}=4.3** billion addresses

Subnet Mask

Hides, or "masks," the network part of a system's IP address and leaves only the host part as the machine identifier. It is used to identify the network segment to which packet belongs. If a machine's IP address and subnet mask/network prefix is known, then the network can be identified by doing a logical AND operation.

Class	Binary	Dotted Decimal	Prefix/CIDR
A	**1111111.00000000.00000000.00000000**	**255.0.0.0**	**/8**
B	**11111111.11111111.00000000.00000000**	**255.255.0.0**	**/16**
C	**11111111.11111111.11111111.00000000**	**255.255.255.0**	**/24**

Default Mask of Classful Addressing

IPv4 and Changes to Preserve the Address Space

The IPv4 address space, which we are all familiar with like, 192.168.0.1, is based on 4 octets, or 32 bit address. Each octet has a range of values from 0-255; thus, the maximum size of the address space is 256 X 256 X 256 X 256 or 4.3 billion addresses. The 32 bits can be divided into different classes to allocate network and host addresses. With the development of the World Wide Web, the growth of PCs, the use of smartphones, tablets, gaming systems, and VoIP systems, far more IP addresses were necessary than the founders envisaged. The new address space IPv6 uses 128-bit addresses and is

capable of 340 trillion, trillion, trillion addresses. How big is this number? If you assigned an IPv6 address to every atom on Earth, you would still have enough addresses to do another 100 Earths. It is not even remotely a possibility that we will run out of IPv6 addresses, before humans are extinct.

The depletion of IPv4 addresses was predicted in 1993 and steps where take to preserve the space as long as possible. The IETF instituted the following changes:

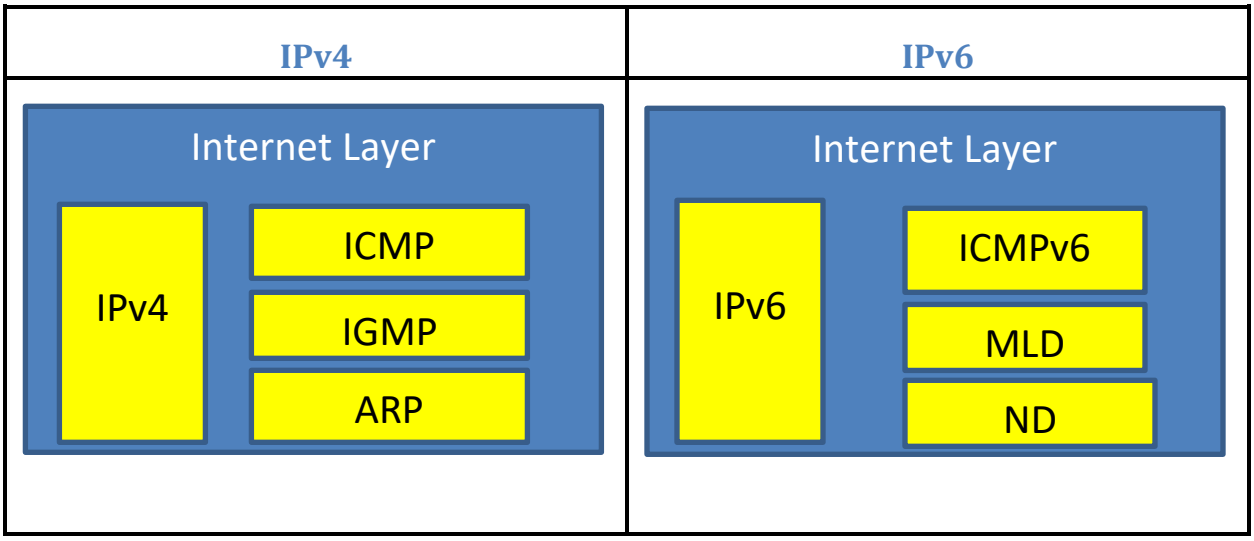
- Private address spaces where created to allow networks to create LAN addresses with approval of the Internet registry. However, hosts on the LAN can't communicate with the public Internet except through a proxy gateway.
- NAT, Network Address Translator, was created to act as a proxy gateway converting private host addresses to public addresses to access the Internet. Thus, many LAN hosts can share a single Internet address.
- DHCP, Dynamic Host Configuration Protocols was created to act as a server to allocate addresses from a pool of available LAN addresses. The address assigned to the host is "leased" from the server for a time and can be reallocated to another host when the lease expires. Thus, many hosts can share a pool of addresses.
- CIDR, Classless Inter-Domain Routing was a fundamental change in how IP addresses were assigned. The old class based system of allocating IPv4 addresses was discontinued for a classless system which used the 32 bit address space more efficiently, avoiding wasted IP addresses.

All of these network technologies we have heard before and are currently implemented on our home and Seneca networks. In North America, IPv4 will continue to be used for a long time. Networks won't convert to IPv6 until new hardware is required.

IPv6 addressing

IPv6 uses three types of addresses -- unicast, multicast, and anycast. Unicast and multicast addresses also existed in IPv4, but Anycast is a new type of address defined by IPv6.

1. **Unicast:** A unicast address is a one-to-one address. Packets send to a unicast address travel between two hosts on a single interface.
2. **Multicast:** A multicast address is a one-to-many address. Packets sent to a multicast address travel to all interfaces identified by the multicast group address.(this replaces the broadcast address used in IPv4)
3. **Anycast:** A anycast address is a one-to-one address sent to the nearest host. Packets sent to a anycast address are sent to a single interface of the nearest host identified by the address.
4. Both IPv4 and IPv6 are connectionless protocols. "best effort" delivery system
5. IP works with ICMP, (Internet Control Message Protocol) which is responsible for generating error messages when an error occurs during data transmission. The Transport layer protocols, namely TCP and UDP, decide to retransmit data based on the error message that is received. The table below is a comparison of the IPv4 and IPv6 layers and the protocol specifications of each layer.



The dual stack approach to IPv6 means that IPv4 will be around for a long time. IPv4 devices will continue to work in the foreseeable future. However, there are 3 reasons why businesses should plan to change to IPv6.

- **Inevitability**: At some point in the future, IPv4 will be no longer supported. Moving to IPv6 when hardware needs to be changed is a good approach
- **Efficiency:** IPv6 is better protocol than IPv4, with faster routing by removing the need to check packet integrity and fragment a packet. In IPv6, only the sending host performs fragmentation. If an IPv6 router cannot forward a packet because it is too large, the router sends an ICMPv6 Packet Too Big message to the sending host and discards the packet. NAT will no longer be needed, because each host will have a unique IP address on the public network, unless the network continues to use private addressing.
- **Security:** IPv6 has been built from the ground up with security in mind with builtin encryption.IPv6 encrypts traffic and checks packet integrity to provide VPN-like protection for standard Internet traffic.

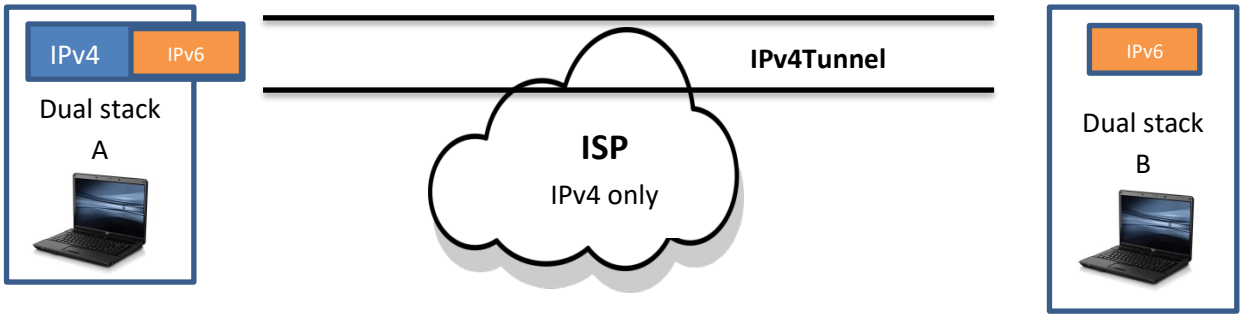
IPv6 Address Space

- IPv6 has a network address of 48 bits which is assigned by the Internet Society.
- Network prefix bits which businesses can use to divide their address space to match organizational needs.

- The remaining 64 bits are host bits.
- 128 bit address divided allow 8 16 bit blocks – then converted to hexadecimal
- 0s can be compressed using a "::" – but can be used only once in an address
- In dual environment special format for IPv4 used in low order bits ::192.168.2.1/96
- 127.0.0.1 represented as ::1/128

Tunnelling

- The dual stack approach is an important feature to ensure compatibility between IPv4 and IPv6 hosts. To allow packets to travel across IPv4 only device **IPv6 over IPv4 tunneling** has been defined.
- IPv6 packet encapsulated in IPv4 packet to pass through IPv4 only device.
- DNS records are used to determine if device IPv4 or IPv6 only or IPv4/v6
- IPv6 addresses are trued first, if fail try IPv4.



IPv6: A Programmer's Perspective

From a programmer's perspective IPv6 is very different that IPv4 programming and will present some new challenges.

1. **User Interface Design:** Unlike the IPv4 address space, the IPv6 address space is much larger and must be displayed in hexadecimal notation. An advantage of dotted decimal notation was that it was very predictable when displaying addresses. IPv6 on the other hand, with its truncated notation of using double colons to represent a series of zeros is less predictable. Lastly, GUI application Users will normally use DNS names to identify hosts not IP addresses. Thus, GUI applications which supply text boxes, such as TCP/IP properties, would be unnecessary and should be avoided given the complexity of IPv6 format over IPv4. However, applications used by administrators would need such text boxes.
    - Should number based or named base notation be used?

- Should the truncated addresses be used in the interface? The double colon is an optional method of notation to simplify the address, not a specification.
- Does the user need specific parts of the address, such as the subnet prefix, scope identifier or other subfields?

2. **IP Family Independent:** With a dual stack environment it is important not to write code that is family specific, such as IPv4 or IPv6. Family specific code can't be handled correctly in a dual stack environment. The best approach is to use data structures and functions that are family independent.

- **Determine IP Family Before Creating Socket:** When creating a socket, the common procedure in IPv4 was to create the socket, and bind the address family information to the socket. This procedure will not work in IPv6. The address family must be determined first, then create the socket and bind the family to it. In IPv4, a node normally has a single IPv4 address associated with it. In IPv6, it is normal to have multiple IP addresses onto a single node. More specifically, IPv6 addresses are assigned to interfaces, not to nodes. An interface can have multiple IPv6 addresses

- if the user is to enter an IPv6 address as part of the URL, the address must be enclosed in square brackets to avoid ambiguity with the port number which is also separated by a colon. For example: **http://[F380:DC28:ffff::1]:80/64**..