Computer Networking Course - Network Engineering (CompTIA Network+) Part 8

Common Network Security Issues

Security issues caused by misconfigurations

Misconfigured firewall and access control list (ACL)

- A misconfigured firewall and ACL can result in 3 different categories of security issues:
  - traffic that should be blocked isn't, allowing threats in
  - traffic that shouldn't be blocked is, prevent receiving vital updates
  - all traffic is blocked, this isn't necessarily a security issue per se but is still a misconfiguration
- to protect against a misconfigured firewall or ACL, thoroughly test them before putting them into action

Misconfigured application

- A misconfigured application may become a security threat
  - a web application that does not perform proper validation of input may lead to a buffer overflow attack. This may lead to a successful attack on the web server on which it is hosted.
- thoroughly testing applications before placing them into service will mitigate the threat

Unpatched OS or firmware

- the manufacturers of OSs and hardware firmware will often produce security patches for vulnerabilities as they become known.
  - an unpatched OS or firmware becomes very vulnerable in short order and may become a threat to the nw.
- most software makers have an updating service; subscribing to that service will help to mitigate the threat

Open TCP/IP ports

- open ports on nws are listening for requests for or by services, applications, or protocols
  - all open ports are a security vulnerability and there are 65535 possible ports that may be open.
- the best practice for nw security is to specifically close all unnecessary ports to harden a nw

Misconfigured authentication services

- the **TACACS+** and **RADIUS** services are often used to authenticate devices and users on nws
  - a misconfiguration of either may lead to a security issue that allows malicious users to be authenticated to use nw resources
- thoroughly reviewing the configuration of authentication services will help to mitigate the problem. In addition, all default local accounts should be disabled (these may present a slight opening for a malicious user to exploit authentication services)

Active default usernames and passwords

- almost all devices and applications come with default usernames and passwords to ease the setup process
    - if left active, these defaults create a security issue
- a best practice is to disable all default usernames and passwords after setting up the device or application

Other network security issues

Malicious users

- malicious users may be the single biggest security issue facing any nw and they will fall into 1 of 2 categories:
    - an **untrusted malicious user**: an outside entity that has exploited a security weakness to gain access to nw resources (e.g., a hacker who has breached a database's security features to gain access to valuable info)
    - an **trusted malicious user**: a person or entity that has been explicitly granted access to nw resources that then exploits this trusted position for malicious purposes.
- a best practice is to review log files on a regular basis to see what resources are being accessed and by whom to help maintain security

Packet sniffers

- examine nw traffic at a very basic level and can be used to help in the administration of a nw
    - may also be used by malicious users to see what protocols and activities are allowed on the nw. This may help them in further attacking the nw.

Malware

- usually defined as malicious software that has the intent of causing harm. As a category, malware covers any code based threat to a nw or system.
    - examples: viruses, Trojans, and spyware
- to protect against malware, anti-malware applications should be running on every device. To be proactive, end user education should also be in place to teach them to recognize the dangers.

ICMP (Internet Control Messaging Protocol) related issues

- ICMP can be a valuable tool for diagnosing issues on nws, but it can also become a security vulnerability.
    - can be exploited in a DoS type of attack
    - can be used to redirect legitimate users to a new malicious default gateway, possibly resulting in loss of data or sensitive info
- it is now a best practice to deny ICMP requests on a router's outward facing interfaces

DoS or distributed DoS (DDoS)

- in an attempt to bring down a nw or website, malicious users will often send thousands of requests for services
    - the attacker's goal is to make that resource unreachable by legitimate users
- many modern firewalls and other nw appliances have been configured to recognize the signature of such an attack and can take steps to mitigate the results

Unintended backdoor access

- when creating applications, developers often create backdoors into the programs. Backdoors are a method of accessing an application or service while bypassing the normal authentication process. These backdoors are sometimes left open after the development process has been completed.
    - in most cases, the application is listening on a specific port for a request for access
- the best mitigation tech is to close all unnecessary ports on a nw.

Jamming(干扰)

- all wireless nws use RF channels to transmit data on the nw. It is possible to create enough interference on the RF channel that it is no longer useable on the nw.
    - an attacker will often use jamming when performing a DoS type attack;
    - it can also be used to perform an evil twin type attack
- many of the modern nwing standards and devices employ tech to mitigate the threat of jamming

Banner grabbing

- many nw devices display banners (displayed messages) when users are signing into or requesting services from nw devices. These banners can impart info about the type of device or the type of service that is being requested.
    - this info may be used by a hacker to research possible exploits.
- the best practice is to disable all unnecessary services and banners on nw devices

Common WAN Components and Issues

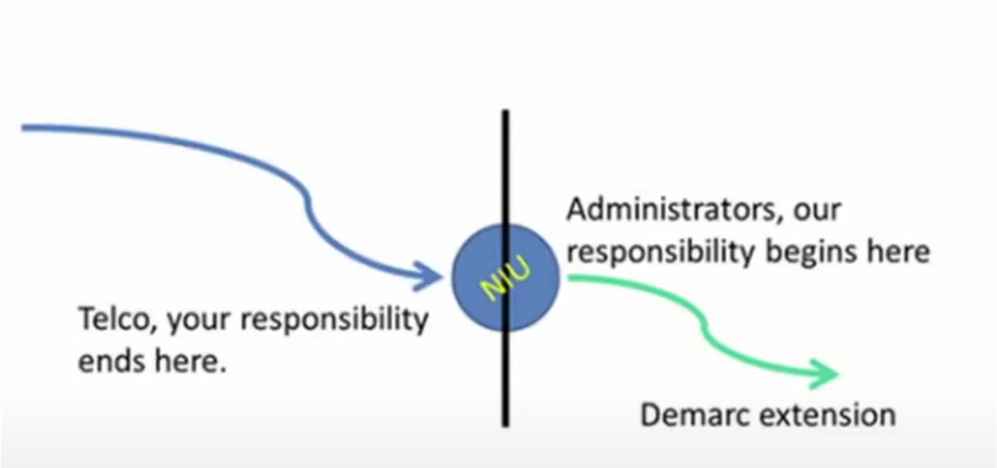
Common WAN components

Copper line drivers or repeaters

- these are used to allow nw traffic to go farther distances over copper wire type nw. (e.g., PSTN nw)
    - they take an incoming signal and regenerate it (boosting the strength) and then send it back out, thus reducing attenuation

Demarc

- Demarc = the demarcation point: the physical point where the telecommunication company's (Telco's) responsibility ends and the customer's begins
    - the Telco takes care of the upstream end of the nw
- the demarc may be simple or very complex, depending on the size of the organization and the required services
-


Administrators, our responsibility begins here
NIU
Telco, your responsibility ends here.
Demarc extension

Network interface unit (NIU)

- in the SOHO env, the NIU is usually the demarc
- in the SOHO env, the NIU is usually provided by the internet service provider (ISP)
    - an NIU can be a cable modern, a DSL modem, or another piece of hardware that connects the customer to the ISP

SmartJack

- an NIU that can provide feedback on conditions to the ISP
    - SmarJack can help the ISP determine if a problem exists on its end of the demarc through the use of remote loopback capabilities
    - many SmartJack can provide translation between protocols (e.g., translating a serial PPP communication stream into Ethernet)

Channel Service Unit/Digital Service Unit (CSU/DSU)

- the interface that provides the connection between a point-to-point line (T1) and the device that is directing nw traffic, usually a router.
    - the CSU/DSU may be an external device, or it may be a removable module inside a router
    - only two CSU/DSUs may exist on a single point-to-point line ---- one at either end of the connection

Common WAN issues

Loss of Internet connectivity issues

- many factors can lead to a loss of connectivity --- on both sides of the demarc
    - before contacting the WAN provider, check the local area nw (LAN) equipment for its operation. If the issue is not found to be on the LAN side, contact the WAN provider.
    - one of the tests that WAN provider will conduct is a loopback test to check its line for interference.

DNS issues

- may look like a loss of internet connectivity, but it isn't. (e.g., users cannot connect to www.google.ca)
- if using a local DNS server, verify the settings and make corrections accordingly.

- if using the WAN provider's DNS settings, attempt to ping the IP address; if that works, there is a WAN connection
  - if you use the ping utility with the fully qualified domain name and this fails, contact the WAN provider to resolve this issue.

Interface issues

- Errors on a router's WAN interface can indicate several different issues. Monitoring an interface's status and reading the error reports may provide a clue as to the issue.
- the most common issue that prevents a good connection is a speed or duplex mismatch
  - a speed mismatch between the interfaces will prevent a link from being established
  - a duplex mismatch between the interfaces will create errors (e.g., output and input errors)
- discards and packet drops
  - if the device is discarding incoming packets, then, more than likely, the device's CPU is being overutilized
  - if the device is dropping outgoing packets, then there is a bw congestion issue (which may be caused by interference on the line)

Router configuration issues

- a common problem when establishing a new WAN connection
  - a misconfiguration of the WAN interface of a router will lead to a WAN connection issue
  - if this is suspected, verify the proper configuration settings with the WAN provider

Company policy and practice issues

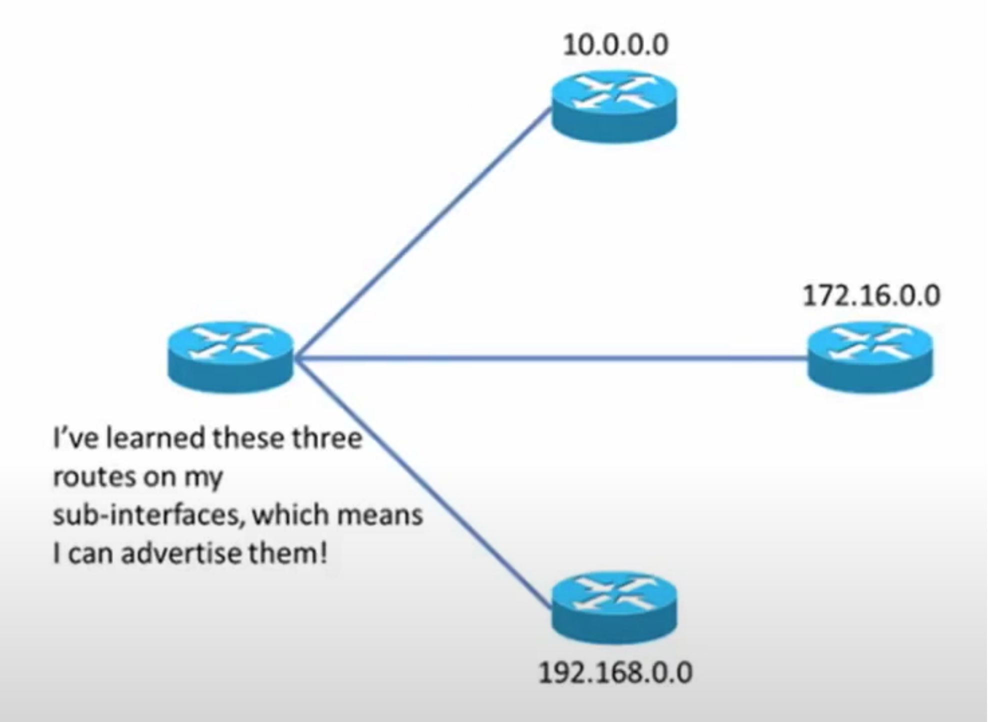
- there are some company policies and practices that may appear to end users as WAN connection issues
  - some applications may be throttled (have their available bw reduced for QoS reasons), leading to slow servers (a perceived WAN issue)
  - acceptable use policies may restrict or block access to certain sites or types of sites, which may appear to the end user as a WAN issue

Satellite issues

- if a satellite WAN connection is used, latency will increase due to the distances covered.
  - *latency* is the measure of time between the sending of data and the receiving of data
  - careful application of QoS techniques may mitigate the effects of latency on some applications

Split horizon issues

- A technique used in routing to help prevent routing loops
  - with split horizon, a router will not advertise a route to another nw out of the interface it learned the route on
- with a point-to-multipoint WAN connection, the router may have difficulty with split horizon
  - it will learn all of the routes on the same interface, but can't advertise those routes back out of the interface
- creating logical sub-interfaces on the WAN interface will usually resolve this issue
  - the logical sub-interfaces appear to the router as individual interfaces, allowing the router to advertise the routes back out of the WAN interface.

- 
  10.0.0.0
172.16.0.0
192.168.0.0
I've learned these three routes on my sub-interfaces, which means I can advertise them!

The OSI Networking Reference Model

A brief history

OSI: Open Systems Interconnection

- a conceptual model with 2 major components:
  - an abstract model of nwing --- a seven layer model
  - a set of specific protocols --- allow differing computing systems to communicate with one another despite their different architectures

Why a nwing model was required

- early nws could only communicate with like systems

TCP/IP reference model

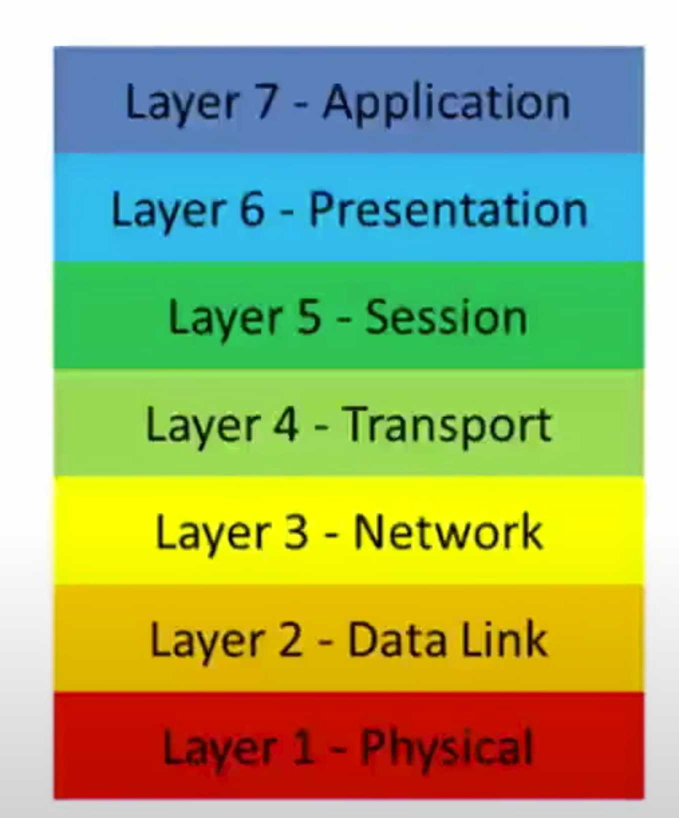
- Transmission Control Protocol/Internet Protocol
- adopted by the big players beginning in 1984

OSI reference model

- published in 1983
- define the relationships between differing protocols, between protocols and hardware

Networking reference models

The OSI reference model



Layer 7 - Application

Layer 6 - Presentation

Layer 5 - Session

Layer 4 - Transport

Layer 3 - Network

Layer 2 - Data Link

Layer 1 - Physical

L1, physical layer

- standardizes the electrical signal the nws use; defines cable standards and how bits are places on the physical media
  - nw cables and hubs are part of L1

L2, Data Link

- identify the individual nodes (both sending and receiving); introduces an error correction method known as **frame check sequence (FCS).**
- is composed of 2 sub-layers:
  - the **logical link control (LLC)** layer: flow control and error correction
  - the **media access control (MAC)** layer: node addressing
- switches and bridges are L2 devices

L3, Network

- routing functions between nws; identifies nodes and nws.
- routers are L3 devices

L4, Transport

- breaking the data into smaller pieces for the lower layers and for the actual data transport protocols ---- TCP and UDP (User Datagram Protocol); may be required to confirm the actual delivery of the data stream and error correction

L5, Session

- establishing the initial parameters between 2 systems; set up and tears down the communication channel

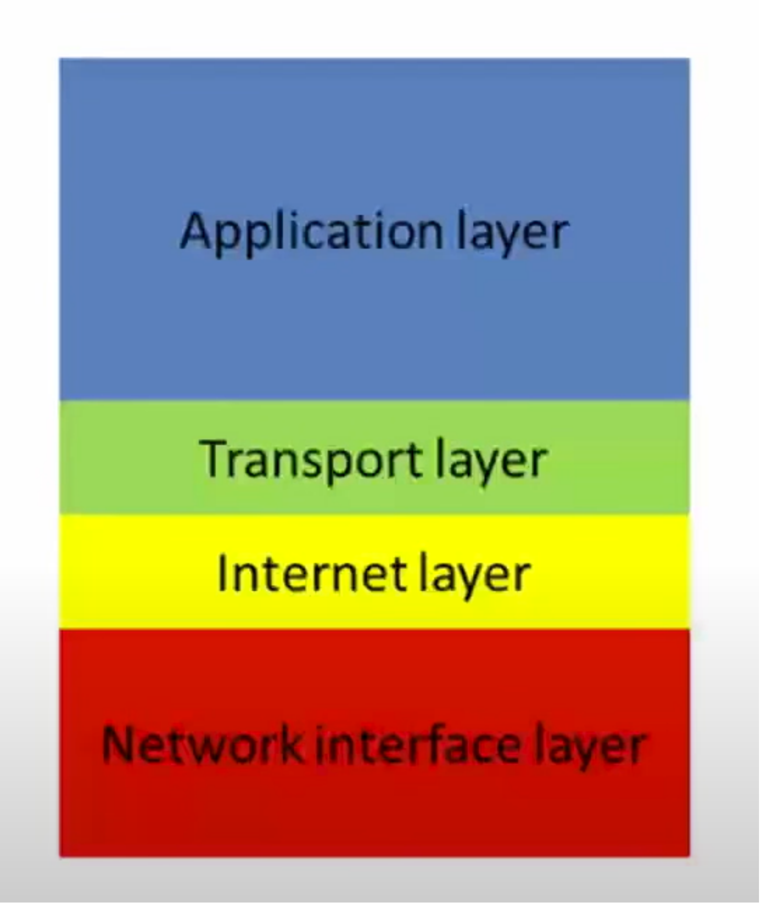
L6, Presentation

- taking data and converting it from a machine dependent language to a machine independent language; as well as encryption between nws.

L7, Application

- responsible for the protocols that request services or functions from other systems; may not be the actual application (e.g., IE is an application that uses HTTP at L7 to request web pages)

TCP/IP reference model



Network interface layer (a.k.a. Link layer)

- handles electrical signaling, flow control, error detection, node addressing

Internet layer

- handles routing functions and identifies nw systems and nodes

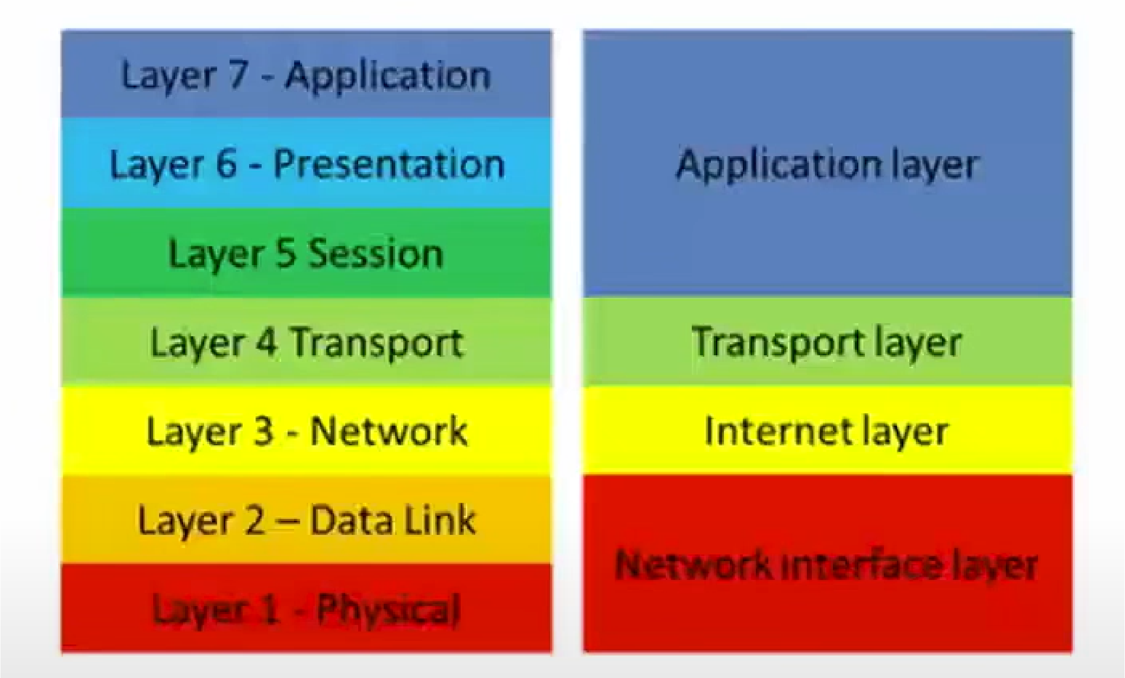
Transport layer

- handles breaking the data into more manageable chunks for lower layers; responsible for the delivery method, either reliable or unreliable, and error correction for reliable delivery

Application layer

- handles requests for services from applications, translation to machine independent languages and encryption; sets up and tears down sessions

OSI and TCP/IP comparison



Layer 7 - Application

Layer 6 - Presentation

Layer 5 Session

Layer 4 Transport

Layer 3 - Network

Layer 2 – Data Link

Layer 1 - Physical

Application layer

Transport layer

Internet layer

Network interface layer

- TCP/IP is used in real-life application, OSI is used for communicating issues with other technicians.
- both models are references only, not mandatory to be followed. Developers determine their own way of implementing nw models.

The transport layer plus ICMP

TCP and UDP

Transport layer

- receives data from L5 and determines what method of delivery is required for the data; then hands the data with the instructions for method of delivery to L3.
- 2 main protocols: TCP and UDP

Intro to TCP

- uses a reliable method to deliver nw packets
- helps to set up the connection session
- establishes error control
- helps to tear down the nw session
- used when not sensitive to latency issues

Reliable delivery method

- uses a three-way handshake
  - request the connection
  - receives the response from the other end
  - sends an ACK back that sets the sequence number that will be used
- every packet that gets sent must be acknowledged by the receiver. If the sender doesn't receive the ACK of a packet, the sender will re-send the packet

Intro to UDP

- uses an unreliable method to deliver nw packets
- doesn't help to set up connection session, establish error control, tear down the nw session
- used when speed is more important, e.g., VoIP

Unreliable delivery method

- could be described as a "best effort" delivery method
- sends the data stream to the destination, trusting that the destination is:
  - listening for the data stream
  - willing to accept the data stream
- data stream flows with no ACK of it being received

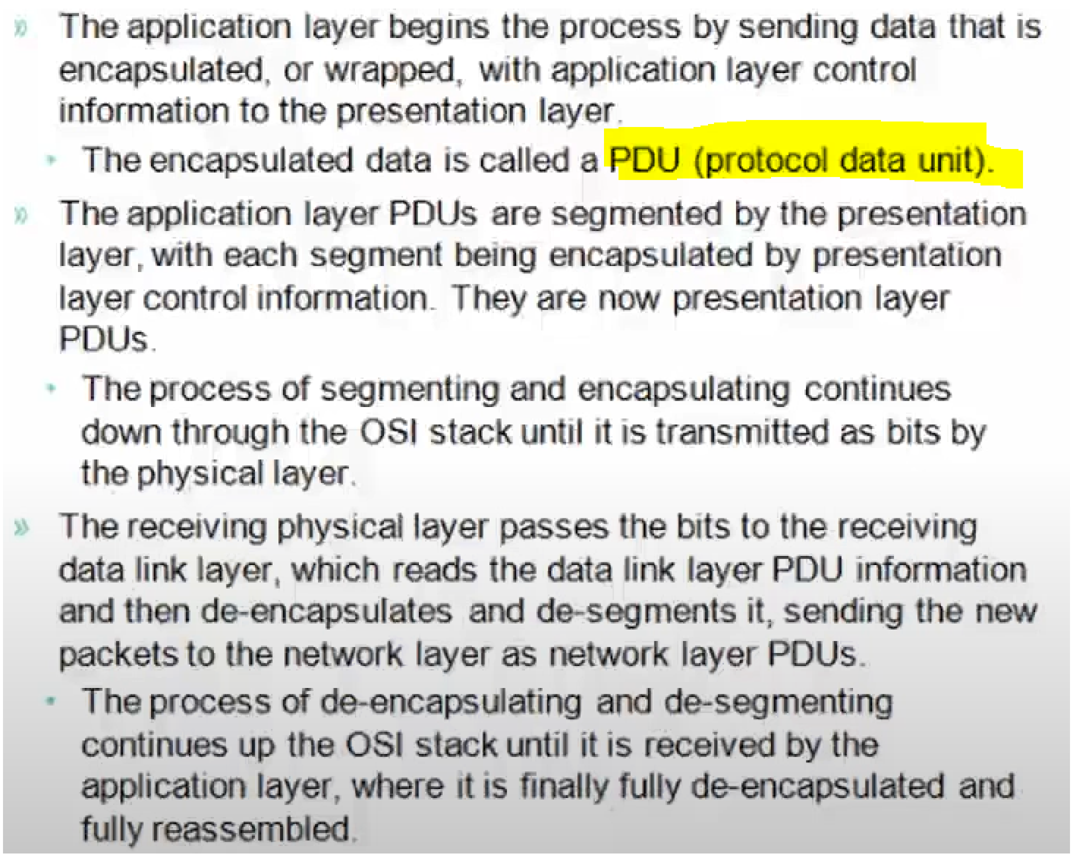
ICMP (Internet Control Message Protocol)

- works at L3, or L2; used by IP to perform several services
- its packets are carried as encapsulated IP datagrams; provides info about nwing issues
- the **ping** utility uses ICMP to test for ent-to-end connectivity between 2 devices using ICMP echo request packets
- the **tracert** utility uses a combination of ICMP echo requests and dst unreachable packets to map the actual route between 2 endpoints
- a router is under full memory buffer will use ICMP messages to inform other routers to slow down to avoid packets loss

Basic network concepts

Encapsulation

- as data flows down from the L7 through to the L1, it is encapsulated --- layer info is wrapped around the data --- at each layer with info to help the corresponding layer at the other end of the communication line understand what is happening
- as data is received at the other end, it is de-encapsulated (unwrapped) as it moves up the OSI stack
- keyword: **PDU (Protocol data unit)**

- 

  - The application layer begins the process by sending data that is encapsulated, or wrapped, with application layer control information to the presentation layer.
    - The encapsulated data is called a PDU (protocol data unit).
  - The application layer PDUs are segmented by the presentation layer, with each segment being encapsulated by presentation layer control information. They are now presentation layer PDUs.
    - The process of segmenting and encapsulating continues down through the OSI stack until it is transmitted as bits by the physical layer.
  - The receiving physical layer passes the bits to the receiving data link layer, which reads the data link layer PDU information and then de-encapsulates and de-segments it, sending the new packets to the network layer as network layer PDUs.
    - The process of de-encapsulating and de-segmenting continues up the OSI stack until it is received by the application layer, where it is finally fully de-encapsulated and fully reassembled.

Modulation (Encode)

- how does physical layer transmit data across the media? (physical layer transmits bits --- literal zeros and ones --- of data)
  - the bits of data are modulated (or encoded) by the L1 and placed on the **carrier signal** (also called **carrier channel**) of the media, which carries the modulated data on to its next dest.
  - once the bits are received, they are de-modulated (un-encoded) by the receiving L1

Carrier Signal defined

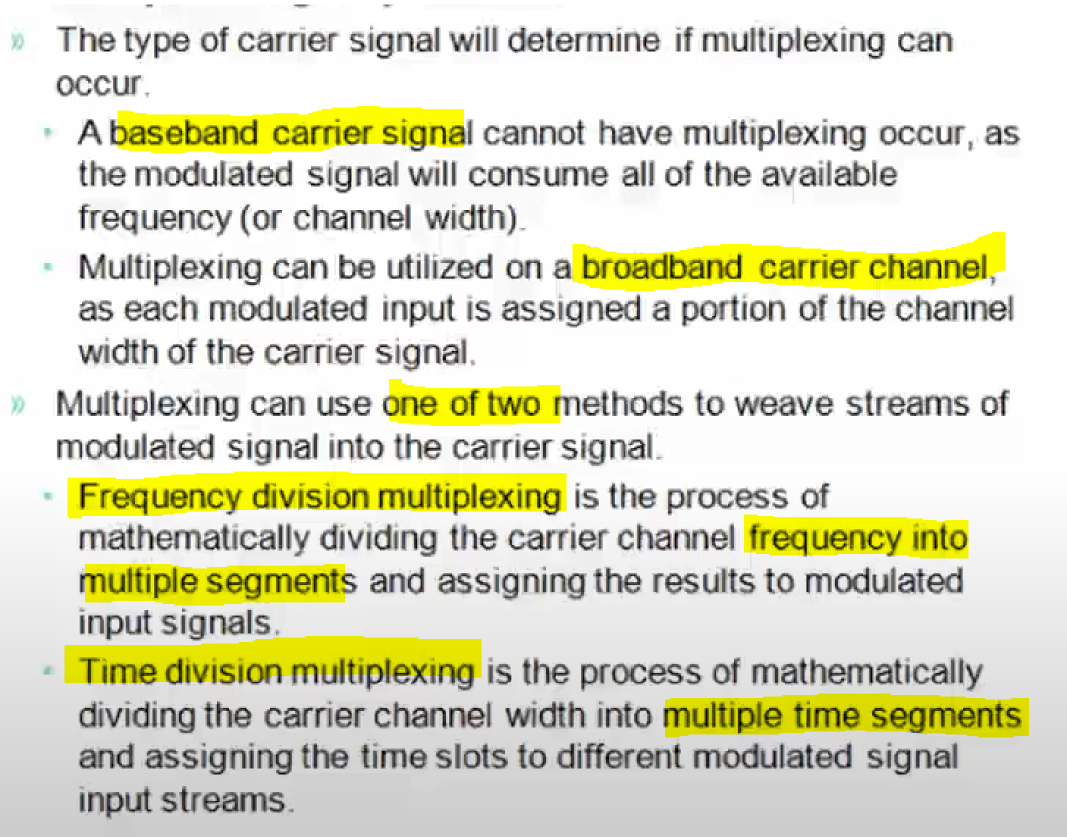
- a standard waveform, usually in the form of a sine wave, that is used as the base carrier of another input signal

Modulation defined

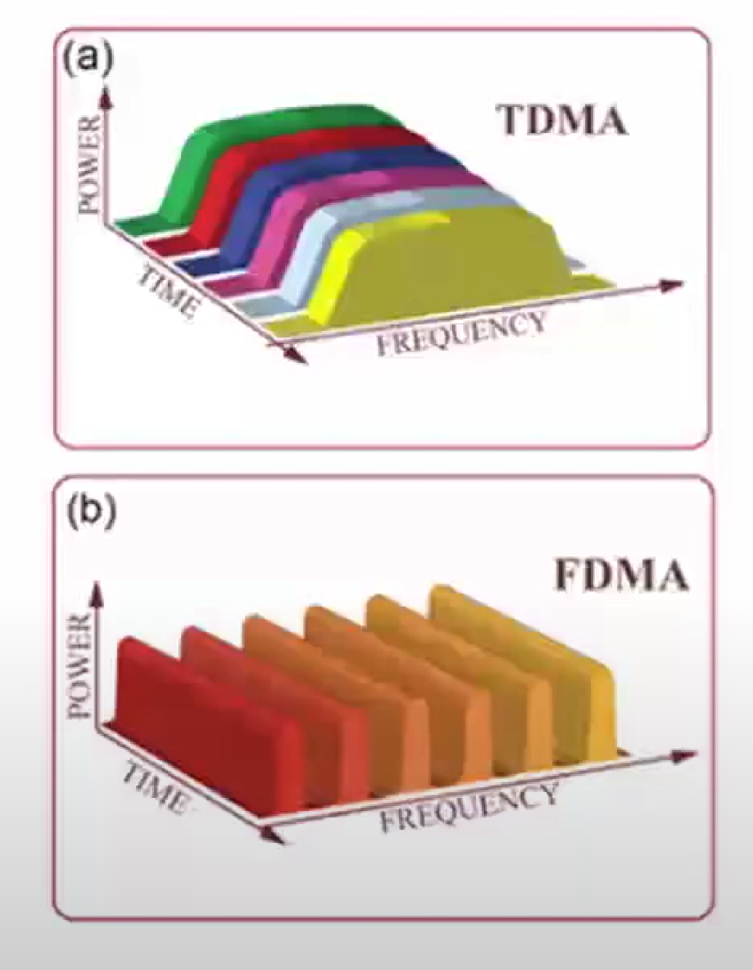
- the process of varying one or more properties of a carrier signal with an input signal --- usually for the purpose of conveying info.
- can be used to encode digital nw traffic onto media that uses a digital carrier signal
- can be used to encode a digital signal onto a media that uses an analog carrier signal --- digital nw traffic traveling over the public switched telephone nw (PSTN)
- **multiplexing** can be used to increase the number of modulated signals that can be placed onto a carrier signal

Multiplexing explained

- keywords: Frequency division multiplexing, Time division multiplexing



- The type of carrier signal will determine if multiplexing can occur.
  - A baseband carrier signal cannot have multiplexing occur, as the modulated signal will consume all of the available frequency (or channel width).
  - Multiplexing can be utilized on a broadband carrier channel, as each modulated input is assigned a portion of the channel width of the carrier signal.
- Multiplexing can use one of two methods to weave streams of modulated signal into the carrier signal.
  - Frequency division multiplexing is the process of mathematically dividing the carrier channel frequency into multiple segments and assigning the results to modulated input signals.
  - Time division multiplexing is the process of mathematically dividing the carrier channel width into multiple time segments and assigning the time slots to different modulated signal input streams.



Baseband

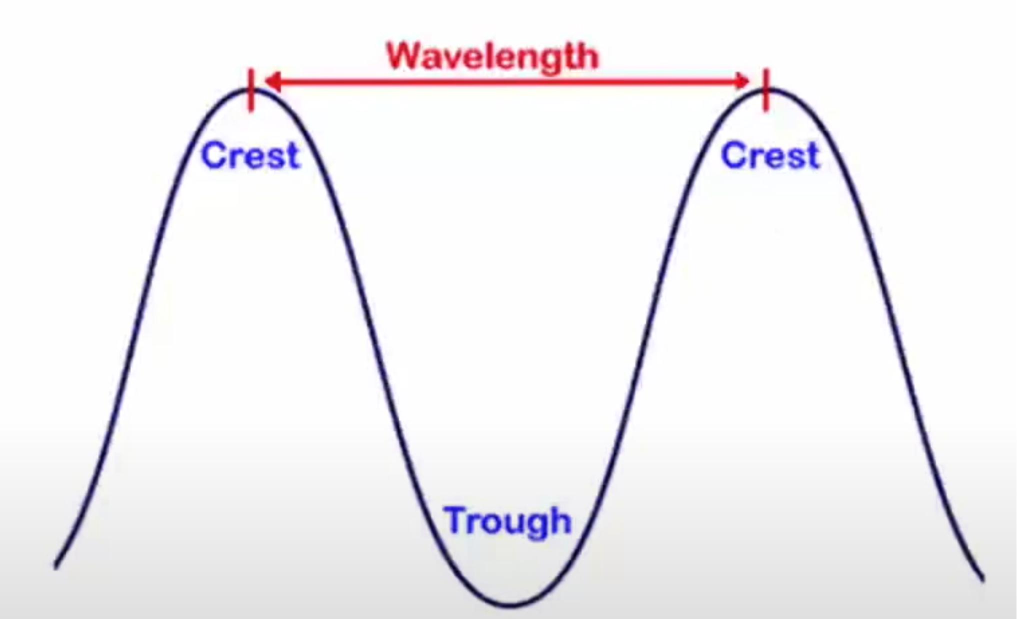
- a stream of data that is sent over a carrier channel as a **digital modulated signal**
  - the digital signal will take all of the carrier signal's available frequency or time
  - while the modulated input does take all of the carrier channel's available frequency, the communication is bidirectional

Broadband

- a stream of data that is sent over a carrier channel as an **analog modulated signal**
  - the analog signal will be assigned a portion of either the carrier channel's available frequency or time
  - while the modulated input doesn't take all of the carrier channel's available frequency, the communication is *not* bidirectional.
  - for two way communication to take place, multiplexed channels must be created

Network Transmission Concepts

Wavelength

- a measurement of the distance between peaks in the wave patterns emitted by electromagnetic radiation (e.g., light, radio, microwave)
- each type of electromagnetic radiation falls into a specific range of wavelengths. By modifying a wavelength, data can be encoded into the wavelength and transmitted to a receiving device, which then decodes the transmission.
- 

Baud rate and bit rate

Baud rate

- originally used to measure the speed of a telegraph transmission. It is a measure of the number of state changes in a given period of time.
  - the usual state change that was measured was electricity (voltage change)

Bit rate

- a measure of the number of zeros and ones that can be transmitted across a medium in a given period of time. (bps)
  - a more accurate measure of transmission throughput than the baud rate.

Sampling size

- when converting from an analog audio signal to a digital signal, a computer captures the analog audio waveform and mathematically converts into different wavelengths (which is how we get the discrete sounds). This occurs over a specific period of time, which is called the size of the sample.

Carrier detect and carrier sense

Carrier detect

- when a device can only tell when a carrier signal or channel is present by the reception(反应) of a control signal.
  - the presence of the control signal signifies that transmissions can occur
  - the control signal controls the order of transmissions, so data collisions are not possible
  - the control signal can be used to establish the maximum speed of the transmission can be used

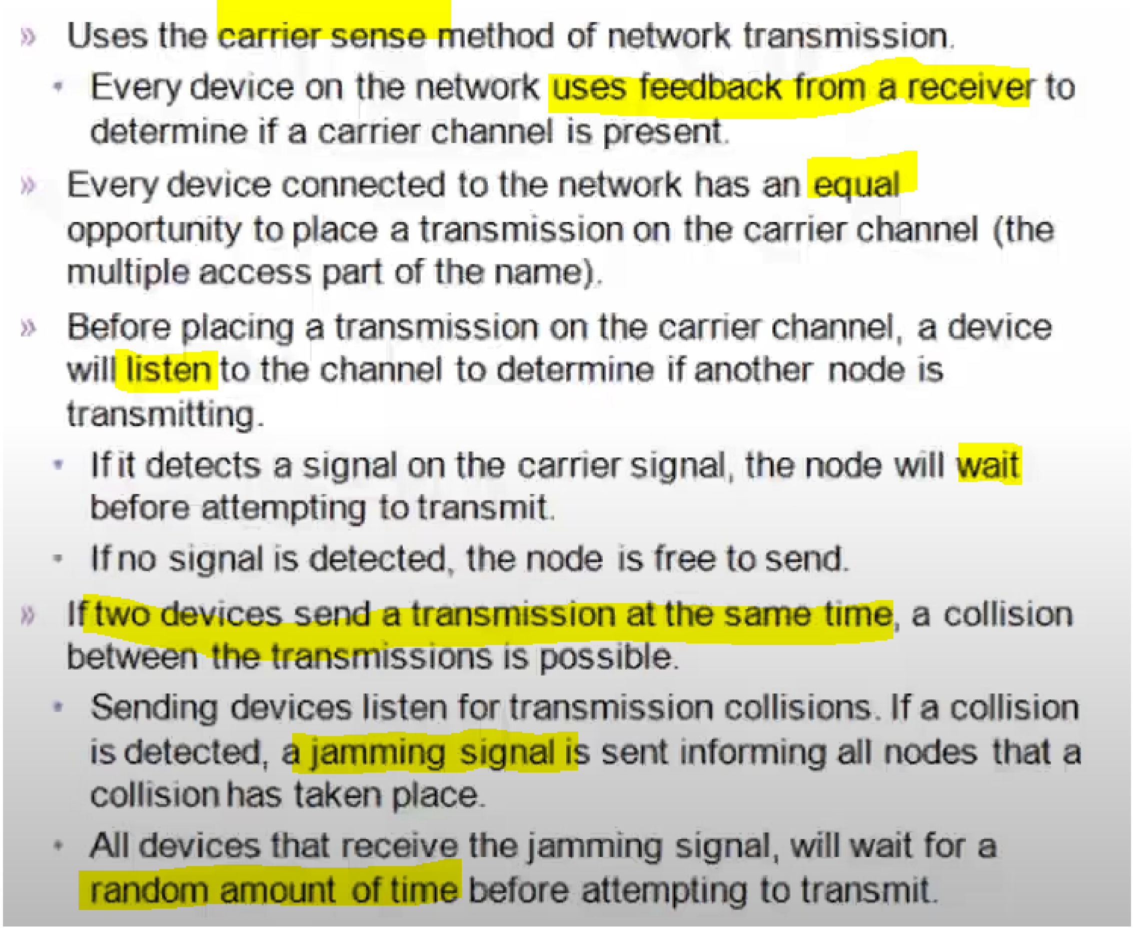
Carrier sense

- when a device uses feedback from a receiver to determine if a carrier channel is present.
  - if a carrier signal is detected, the device can send transmissions.
  - data transmission collisions are possible with carrier sense

CSMA/CD and CSMA/CA

As the number of nodes increases, the efficiency of carrier detect method decrease, and the carrier sense method becomes more efficient.

CSMA/CD (Carrier sense multiple access with collision detection)

- 

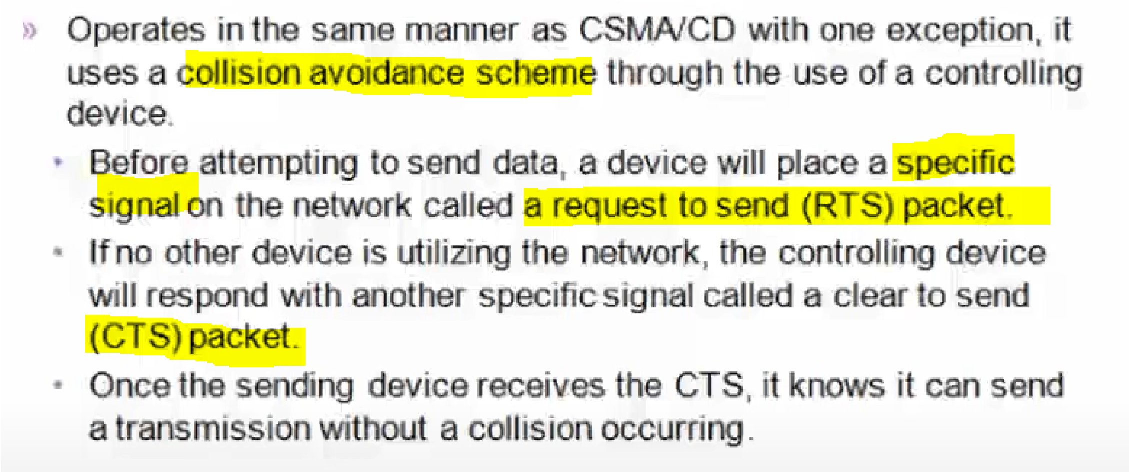
» Uses the carrier sense method of network transmission.
- Every device on the network uses feedback from a receiver to determine if a carrier channel is present.

» Every device connected to the network has an equal opportunity to place a transmission on the carrier channel (the multiple access part of the name).

» Before placing a transmission on the carrier channel, a device will listen to the channel to determine if another node is transmitting.
- If it detects a signal on the carrier signal, the node will wait before attempting to transmit.
- If no signal is detected, the node is free to send.

» If two devices send a transmission at the same time, a collision between the transmissions is possible.
- Sending devices listen for transmission collisions. If a collision is detected, a jamming signal is sent informing all nodes that a collision has taken place.
- All devices that receive the jamming signal, will wait for a random amount of time before attempting to transmit.

CSMA/CA (Carrier sense multiple access with collision avoidance)

- 

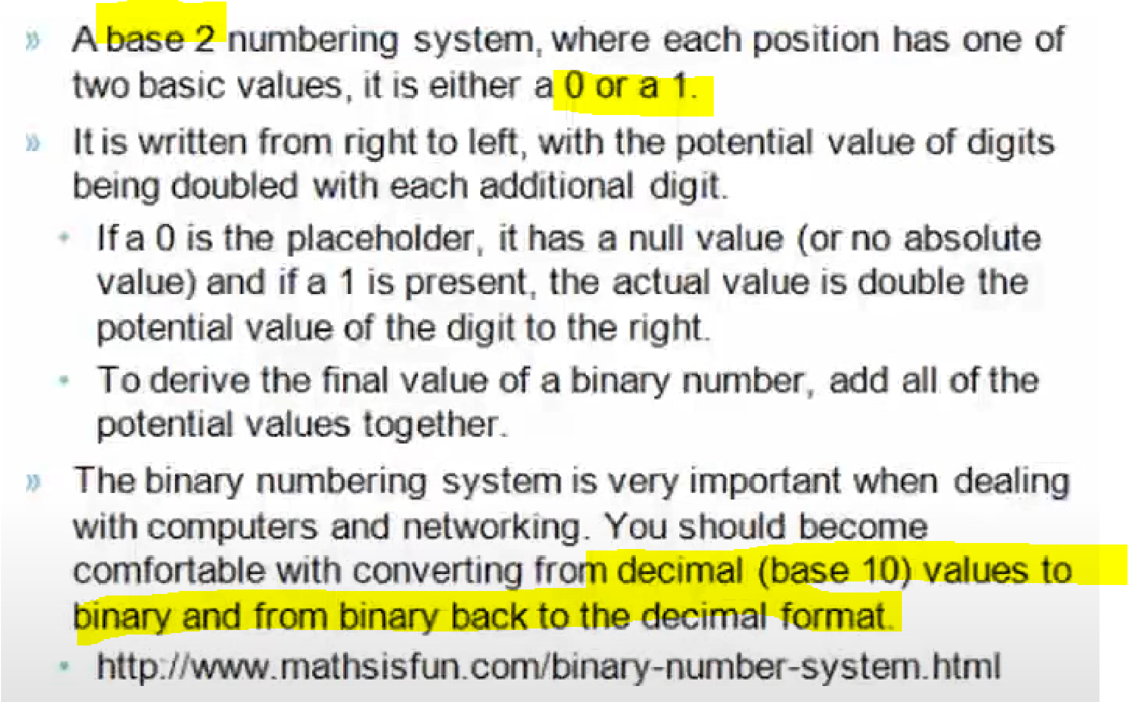
  - Operates in the same manner as CSMA/CD with one exception, it uses a collision avoidance scheme through the use of a controlling device.
    - Before attempting to send data, a device will place a specific signal on the network called a request to send (RTS) packet.
    - If no other device is utilizing the network, the controlling device will respond with another specific signal called a clear to send (CTS) packet.
    - Once the sending device receives the CTS, it knows it can send a transmission without a collision occurring.

CSMA/CD vs. CSMA/CA

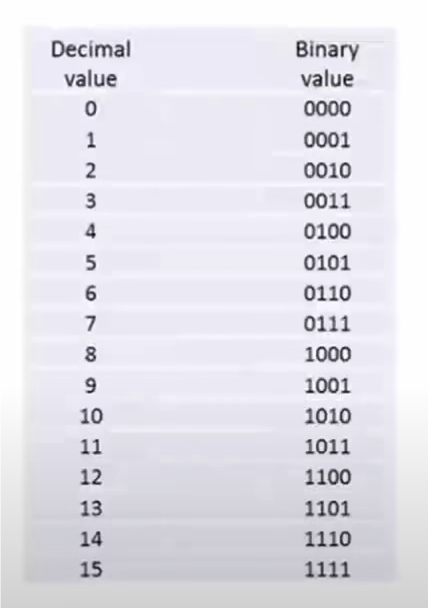
- CSMA/CD:
  - better suited for high speed,
  - high throughput nws
  - is the specified nw transmission standard (as it has a low amount of nw overhead)
- CSMA/CA:
  - better suited for lower speed
  - lower throughput type of nws where the possibility of data collisions is higher
  - is the specified standard for 802.3 wireless (Wi-Fi) nws

Numbering systems

Binary

- 

  - A base 2 numbering system, where each position has one of two basic values, it is either a 0 or a 1.
  - It is written from right to left, with the potential value of digits being doubled with each additional digit.
    - If a 0 is the placeholder, it has a null value (or no absolute value) and if a 1 is present, the actual value is double the potential value of the digit to the right.
    - To derive the final value of a binary number, add all of the potential values together.
  - The binary numbering system is very important when dealing with computers and networking. You should become comfortable with converting from decimal (base 10) values to binary and from binary back to the decimal format.
    - http://www.mathsisfun.com/binary-number-system.html
-



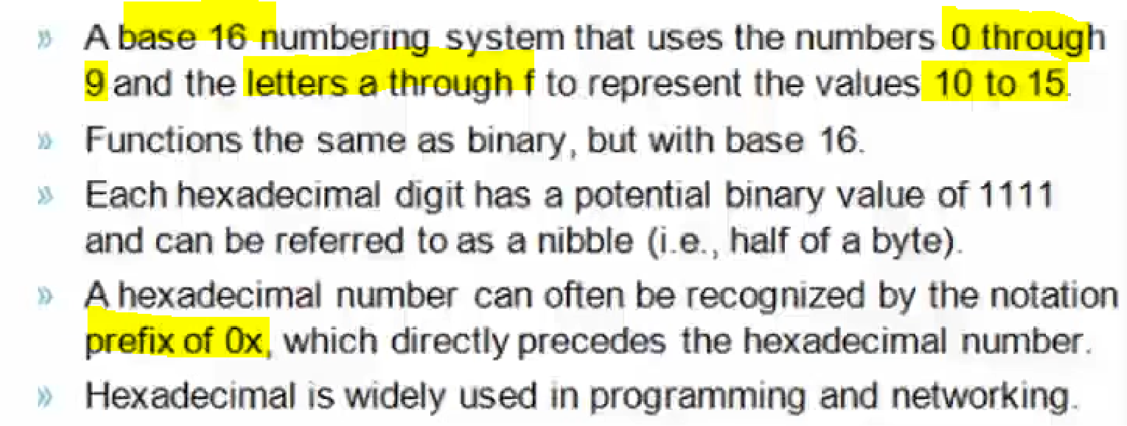
Decimal value	Binary value
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
10	1010
11	1011
12	1100
13	1101
14	1110
15	1111

  - 14 = 2^3 + 2^2 + 2^1 + 2^0

Bit, byte and nibble

- Bit: a single 0 or 1
- Byte/**Octet**: eight (8) bits
- Nibble: half of a byte or 4 bits

Hexadecimal

- 

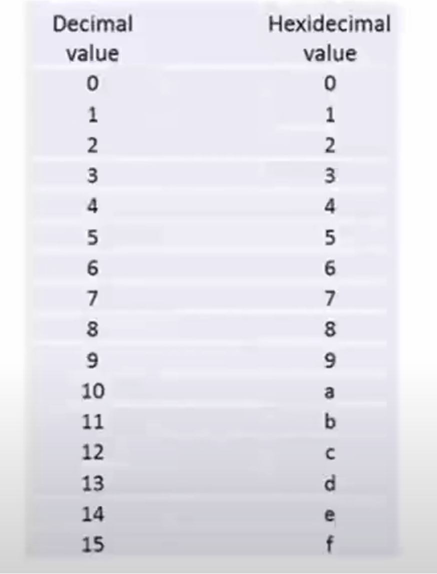
  » A base 16 numbering system that uses the numbers 0 through 9 and the letters a through f to represent the values 10 to 15.

  » Functions the same as binary, but with base 16.

  » Each hexadecimal digit has a potential binary value of 1111 and can be referred to as a nibble (i.e., half of a byte).

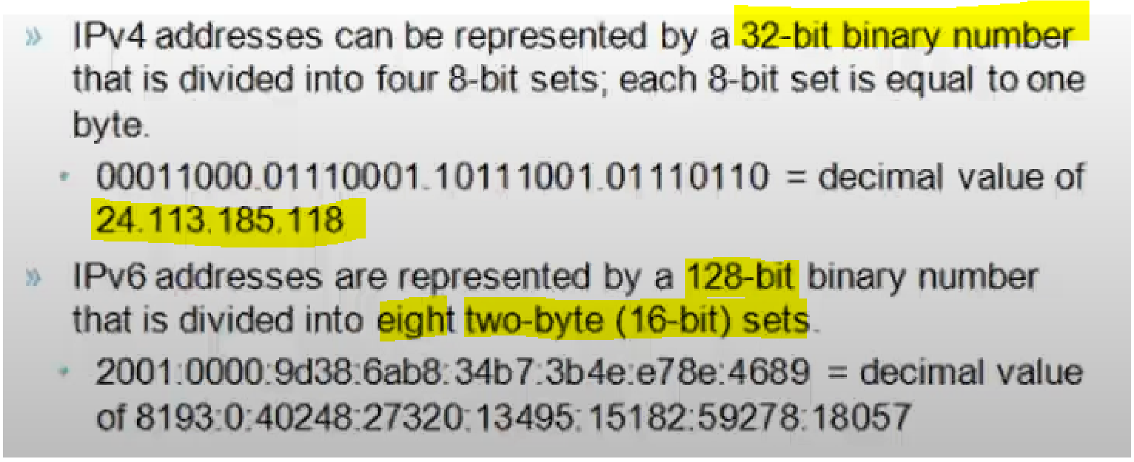
  » A hexadecimal number can often be recognized by the notation prefix of 0x, which directly precedes the hexadecimal number.

  » Hexadecimal is widely used in programming and networking.

- 

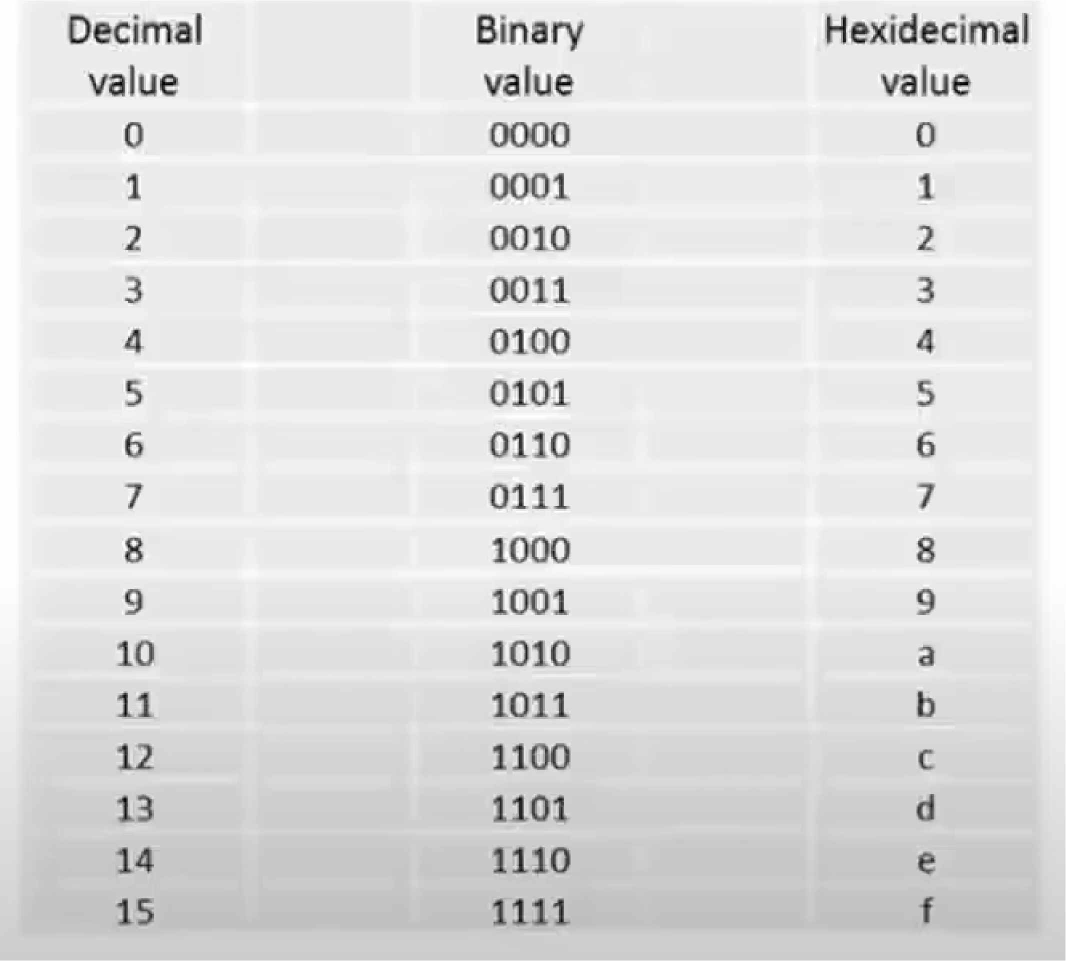
Decimal value	Hexidecimal value
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
10	a
11	b
12	c
13	d
14	e
15	f

Examples of binary and hexadecimal use

- 

  - IPv4 addresses can be represented by a 32-bit binary number that is divided into four 8-bit sets; each 8-bit set is equal to one byte.
    - 00011000.01110001.10111001.01110110 = decimal value of 24.113.185.118
  - IPv6 addresses are represented by a 128-bit binary number that is divided into eight two-byte (16-bit) sets.
    - 2001:0000:9d38:6ab8:34b7:3b4e:e78e:4689 = decimal value of 8193:0:40248:27320:13495:15182:59278:18057

Conversion tables

- 

Decimal value	Binary value	Hexidecimal value
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	a
11	1011	b
12	1100	c
13	1101	d
14	1110	e
15	1111	f