v Hosts = end systems (last point connected to internet)

- Run network apps (YT, netflix, etc;)

Communication links

- fiber, copper, radio, satellite

- Transmission rate: bandwidth

Packet switches: Forwards packets

- Routers, switches

Interet: “network of networks”

-Protocols control sending, receiving of messages and content

Ex: TCP, HTTP, IP< SKype, 802.11

End devices: laptop, desktop computer, printers, etc;

Intermediary devices: router, ln switch, firewall appearances

Network media: wireless media, LAN media, WAN media

**2 ways to connect to internet:**

Client server model (centralized): server that all end devices connect to, and server must stay on to keep devices

connected/allow access of media and other info to end devices.

Peer 2 Peer model: gets rid of server, decentralized. Allows end devices to connect to each other to

share media and other information

**Advantage of Peer 2 Peer:**

* Easy to set up
* Less complexity
* Lowers cost since network devices and dedicated servers are not needed
* Can be used for simple tasks like transferring files and sharing pics

**Disadvantages of Peer 2 Peer:**

* No centralized administration
* Not as secure
* Not scalable
* Devices act as both client and server which can slow their performance down

**Bits:**

What can a network transmitter do?

Sends bits (0 and 1)

Everything that is sent across a network is represented by numbs, text, audio, video

8 bits = 1 byte

Transmitters send bits across a physical link

Data travels over many links or hops to reach a destination

Bit rate: the number of bits I can send in a second

BPS + bits per second

Capacity- Theoretical maximum bit rate based on cable type and distance

(the longer the distance, the lower the capacity)

Line rate- the actual constant bit rate for a particular link

\* Assume this is fixed for class

Throughput - end-to-end bit rate achieved over a particular connection

**Prefixes:**

**K - kilo (10^3)**

**M = mega (10^6)**

**G = giga (10^9)**

**T = tera (10^12)**

**m = milli (10^-3)**

**U = micro (10^-6)**

**n = nano (10^-9)**

If talking about file size, use base of 2 with power of 10

**2^10 = K**

**2^20 = M**

**2^30 = G**

**2^40 = T**

\*When doing file transfer problem, remember to multiply by 8 if in bytes, to get number in bits

Internet end to end model

**Transmission Time = Data Size (in bits) / Line Rate**

Client-subnet-router-subnet-router-subnet-router-subnet

Data packets travel from router to router across subnets (subnets basically link between routers)

**Network Types**

**Body Area Networks**

**- Connects wearables**

**- Antt, bluetooth lone energy**

**Personal Area Networks**

**- Interconnect personal devices (cellphones, portable game module, pc) within 30 ft or so**

**Local Area Networks**

**- Interconnect devices within a single business or building EX: Ethernet**

**Metropolitan Area Networks**

**- Interconnect customer sites controlled by a single telecommunication carrier within a metropolitan geographic region**

**EX: metro ethernet within Chicago area**

**Wide Area Networks**

**- LANs separated by geographic distance are connected by a network known as a WAN**

**-A large network that encompasses multiple states, countries, and the world**

**Wi-Fi = Wireless Fidelity**

4 characteristics of Network Architecture

Fault redundancy: Making sure user operations remain functional, in the case that a link fails, and that there are alternative paths to reach the desired system

Scalability: Making sure that users can join and leave the said service, and be connected with multiple other users all while performance isn’t hindered

QoS- Prioritizes apps/communication services. Usually managed by router to ensure smooth user experience w/ apps that are more data hungry such as streaming services

Security: makes sure that users on the network are protected from cyberattacks and makes sure their data is safe

Packets contain:

Source IP address

Destination IP address

Packet headers

A packet is a string of bits sent over a link containing:

- initial set of bytes called the packet headers, which contain control information about how and where to transmit the packet across the network

- the application data

Typically 1 “request” generates multiple “responses”

**Maximum packet size**

Packets are capped by a maximum transition unit

Maximum ethernet packet size = 1500 bytes

**IP Addresses**

IP routers can deliver any packet that contains an Internet Protocol Header

Within the IP header are two IP addresses corresponding to the sender and receiver of the packet

Source IP

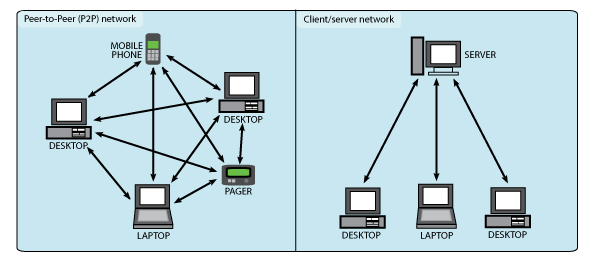
Destination IP

Each active network connection on every device is assigned an IP address

The same way as mail is addressed to a particular address

IPv4 addresses are 32 bits long and are written in dotted decimal notation

4 values between 0-255 with dots between them

Each value represents an 8-bit value

EX: 150.21.39.52

**Number Notations**

Sometimes IP addresses must be examined at the bit level to understand routing and subnetting

**Internet Backbone**

Routers on the IB are typically densely connected by hyperspeed fiber optic links

ISPs manage one or more access lines for each customer to connect them to the backbone

Customers connect LANs to access links through an Access Networks

Routers look up each packet’s destination IP in routing table to forward packet

IP routers provide what is known as “best effort data deliver”

Means routers fone guarantee delivery -packets may drop

Not guaranteed that packets will be delivered in the same order they were sent

**ISPs**

Each ISP typically owns and operates many routers that are a part of the Internet Backbone

An autonomous system is a contiguous set of routers owned by a particular ISP

Each Autonomous System is assigned a unique number

No one runs the internet it is:

Decentralized, distributed, and has chaotic growth

To talk to an end device, we need its IP address which is gathered by its DNS name

SInce people remember names more easily than numbers, there are Domain Name Systems (DNS) servers on the internet that translate DNS names into IP addresses

DNS top-level domains

Top level domains (TLDs) controlled by ICANN)

A protocol defines format and order of messages sent and received among network entities and actions taken on a message transmission and receipt

Client and servers must follow a protocol which determines:

Packet format

- Permissible requests and responses

- Format of header info and data

- Packet ordering and timing

Protocol standards are documents that define protocols

For internet apps, protocol standards are called request for comments (RFCs)

Protocol layers

----Hosts

----Routers

----Links of various media

----Applications

----Protocols

----Hardware, software

Why layering?

In dealing w/ complex systems:

Explicit structure

Identification and relationship of complex pieces

Modularization eases maintenance, updating of system

Change of implementation layer’s service transparent to rest of system

EX change in airplane gate procedure doesn’t affect rest of the system

**Internet Protocol Stack**

5) Application: supporting network apps

FTS, SMTP, HTTP

4) Transport: Process-process data transfer

-TCP, UPP

3) Network: Routing of datagrams from source to destination

IP, routing protocols

2) Link: Data transfer between neighboring network elements

Ethernet, Wi-Fi, PPP(Point 2 Point Protocol), ARP

1) Physical: Bits “on the wire”

**Programs vs process**

Programs have multiple processes running in the background

**What do we address?**

Send message directed to a specific process ID, not a program or IP address

Uses the port number which is addressed to a certain process

**Network VS transport layer example**

Transport layer talks between the port numbers of the 2 devices

Network layer uses the IP address to talk over the internet (IP of each device)

The original layered protocol model was the 7-layer Open Systems Interconnect model (1977)

**OSI reference model**

7) Application

6) Presentation: Allows applications to interpret meaning of data

EX: encryption

5) Session: Synchronization, checkpointing, recovery of data exchange

**Layers 4-1 are same as Internet Protocol Stack**

Internet stack “missing” layers 5 and 6

Moved into the application layer

Removed from the internet stack because not all applications needed them

**Traversing through the OSI Track**

The Protocol Data Unit (PDU) grows in size due to the headers added in each layer as it travels “down the stack

The PDU reduces in size and it travels “up” the stack

Layer 2 PDU referred as a frame

Layer 3 PDU referred as a packet

Layer 4 PDU referred as a segment

Layer 5 PDU referred as a message (payload)

**Process Communicating**

Process: Program running within a host

Within same host, two processes communicate using inter-process communication

Processes in different host communicate by exchanging messages

Note: applications with peer-to-peer architecture typically have both client processes and server processes

**Sockets**

Process sends/receives messages to/from its socket

(Like a mailbox for a process)

A socket is analogous to a door

Sending process shoves the message out the door

Sending process relies on transport infrastructure on other side of door to deliver messages to a socket a receiving process

**Addressing Processes**

To receive messages, processes must have an identifier

Host device has unique 32-bit IP address, but cannot be used as address to send messages to processes

You need the port # of a process to deliver messages to a specific process

Identifier includes both IP address and port address associated with process on host

**TCP/UDP Ports**

TCP and UDP headers contain two 2-byte port numbers

Source Port

Destination Port

A port number identifies a particular software process running on a host

When a client process (like a browser window) starts up, it is assigned an unused private port number

When a server process(like a Web server) starts up, it is binded to a well-known or registered port number based on its function

**Port Number Ranges**

Well-known (0-1023)

Specific to certain processes (assigned by IANA) no one can use these port numbers

Registered (1024-49151)

Assigned by software vendors for new server processes

Private (49152-65535)

Assigned locally to client processes

**IP Addresses**

IP addressing is “hierarchical”

In classful addressing an IP address contains 3 parts:

An **IP Network** part that is used by Internet Backbone routers to deliver packets to a particular IP Network. IP Network values are assigned by IANA to guarantee uniqueness

An **IP Subnet** part that is used by Internal Routers within an IP Network to deliver packets to a particular subnet. Subnet address values are assigned by local network administration

An **IP Host** part that identifies a particular individual device on the subnet. Chosen by network admin or randomly assigned from subnet address pool by DHCP server

IPv6 increases the number of address bits by a factor of 4, from 32 bits to 128 bits

A 128 bit IPv6 address is written using up to 32 hexadecimal digits, written as 8 groups of 4 hex digits each- “coloned hex format”

\* you can remove any left hand zeros present in each group

**Data-Link/MAC Addresses**

Every Ethernet interface has a 6-byte address stored in the interface hardware called:

Physical address

MAC (medium access control) address

Data-link address

Set as a serial number by the manufacturer

Values written in hexadecimal notation

Address information for a network connection can be found in Network details or by running “ipconfig/all”

Every Ethernet interface (NIC) has a 6-byte physical

address or MAC (medium access control) address

assigned and burned into the interface hardware when it

is manufactured

MAC address is like a serial number.

MAC address of every Ethernet device is guaranteed to be

globally unique.

Layer 2 Ethernet MAC address is a 48-bit binary value

expressed as 12 hexadecimal digits.

IEEE requires vendor to follow 2 simple rules:

Must use vendor's assigned 01\_11 as first 3 bytes.

All MAC addresses With the same OUI must be assigned a unique value in last 3

ARP is a broadcast protocol used to determine the MAC

address corresponding to a known IP address

ARP Request packet containing an IP address is broadcast

on a subnet (using the MAC all Is broadcast destination address).

ARP Reply is sent by device that recognizes its IP address in the ARP Request.

**Unicast MAC Address**

Sending a message to a specific device on a network

**Broadcast MAC Address**

Sending a message to everyone on a network

**Multicast**

Sending a message to a group of devices, and all devices must respond to the message

**Anycast**

Sending a message to a group of devices, but looking for a response from at least one device

**ARP Table**

IP Address/MAC Address pairs are stored in the ARP Table (also called ARP cache)

by the sender so the ARP Request does not need to be re-sent.

**Removing Entries from an ARP Table**

ARP cache timer removes ARP entries that have not been used for a specified period of time.

Commands may also be used to manually remove all or some of the entries in the ARP table.

**Two Types of Ethernets**

**Shared Ethernets**

Computers connected via cable (no hubs) through Ethernet hubs.

Data is broadcast from single sender to all stations on LAN.

**Switched Ethernets**

Computers connected through Ethernet switches.

Data is forwarded by intelligent switches based on Destination MAC address

**Ethernet Transmission**

**Shared Ethernets**

Can only have one sender at a time.

CSMA/CD used to ensure single sender.

Collisions and retransmissions occur when multiple stations try

to send simultaneously.

**Switched Ethernets**

Can have multiple senders. Collisions can be eliminated.

Data may be buffered in switches when multiple stations try to send simultaneously.

**Protocols for multiple access links**

2 types of "links"

**point-to-point**

PPP for dial-up access

point-to-point link betvæen Ethernet switch, host

**broadcast (shared wire or medium)**

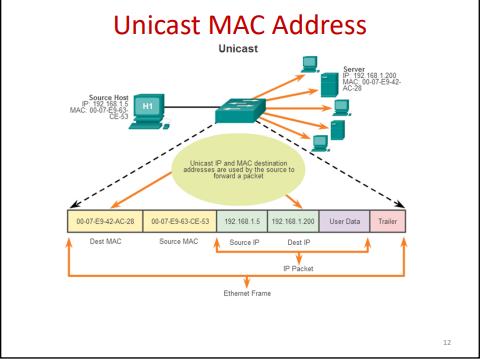
Old-fashioned Ethernet

upstream HFC

802.11 wireless LAN

**Multiple access protocols**

Single shared broadcast channel

two or more simultaneous transmissions by nodes: interference 

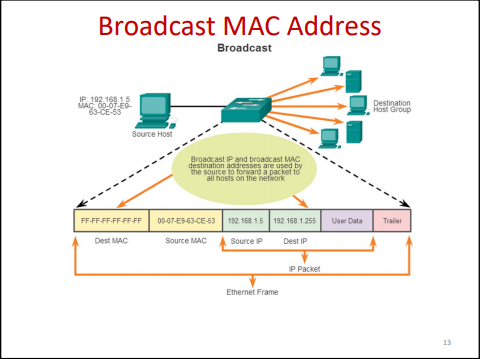
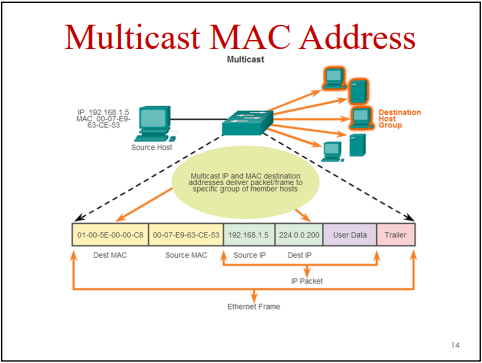
multiple access protocol

distributed algorithm that determines how nodes share channel,

i.e., determine when node can transmit

Communication about channel sharing must use the channel itself!

no out-of-band channel for coordination

Converting Binary to Hexadecimal - gHacks Tech News

**MAC Protocols- Three broad classes**

**Channel Partitioning**

- Divide channel into smaller “pieces”

(time slots, frequency, code)

- Allocate piece-t-node for exclusive use

**Random Access**

- Channel not divided, allows collisions

- “Recover” from collisions

**Taking Turns**

- Nodes take turns, but nodes with more data to send can take longer turns

**CSMA (Carrier Sense Multiple Access)**

- Listen before you transmit

- If channel is idle: transmit entire frame

- If channel is busy: defer transmission

**CSMA Collisions**

- Propagation delay means that two noes may not hear each other’s transmission

- Collisions: entire packet transmission time wasted

- Distance and propagation delay play a role in determining collision probability

**CSMA with Collision Detections**

- On shared ethernets, only 1 station can transmit at any one time

- CSMA/CD protocol used to resolve contention if multiple stations want to transmit at same time

- Not needed in switched ethernets in which the central switch stores data if multiple stations send at same time

**CSMA/CA**

- 802.11 LANs use CSMA with Collision Avoidance (CA)

- When an 802.11 station wants to transmit:

- Wait until the frequency band is idle (CSMA). Wait a random time to avoid collisions (CA)

- If still idle, (optionally) send Request-to-send msg to AP, wait for Clear-to-send msg from the AP for reserved time on channel

- Transmit data frame and start ACK timer

- Access point sends back ACK frame

- Sender retransmits data if no ACK within timeout

**Wi-Fi LANs**

- IEEE 802.11 committee has created multiple standards for transmitting wireless data within shared frequency bands

- 802.11a, 802.11b, 802.11g, 802.11n, 902.11ac

- Configurations

- Infrastructure- access points act as hubs for all WiDi devices that join a common SSID

- Ad-hoc- A group of WiFI devices can talk without an AP (SSID = Service Set Identifier)

**Service Set Identifier (SSID)**

- The SSID is a name (up to 32 characters) for a BSS or ESS

- A **Basic Service Set** (BSS) is an 802.11 Access Point and associated stations. The AP uses its 48-bit MAC address as the BSS identifier

- An **Extended Service Set** (ESS) consists of multiple APs on same Ethernet LAN that all use the same SSID and same security credentials

**Frequencies Used**

- Devices connect to a wireless LAN using 2.4 gHz or 5 gHz frequency bands

- A “Hertz” is the term for a unit of frequency, as defined by the international system of units

- Lower frequencies (2.4 GHz) can travel **farther**, can pass through most objects, and carry lower data rates

- Higher frequencies (5.0 GHz) can carry **higher data rates**, but cannot travel as far and are blocked by more types of materials (walls,etc)

**802.11 Frequency Channels**

**2.4 GHz band (802.11 b/g/n)**

- There are up to 14 frequency channels, 22 MHz each- but each channel overlaps with up to 2 channels on each side.

- There are only 3 non-overlapping channels (1, 6, 11).

- Overlapping channels = interference = decreased data rates

**5 GHz band (802.11 a/n)**

- In the US there are 12 non-overlapping frequency channels of 20 MHz each

**Mixed Mode Operations**

- In an organization with different kinds of devices, access points must operate in mixed-mode, supporting old and new devices simultaneously

- But mixed-mode operation decreases 802.11n client throughput by about 30%!

**MIMO for improving Mixed-operation**

- Employ dual-antenna units that use separate antennas at 2.4 GHz (for old 802.11g clients) and at 5.0 GHz (for new 802.11n clients)

**Adaptive Coding**

- All Wi-Fi LAN Access Points utilize adaptive coding, meaning transmission speeds can change based on network conditions

- APs are continuously evaluating signal quality (power levels, signal interference, noise levels, etc) and adjusting their data rate based on conditions

- For example an 802.11n AP that normally sends at 72.2 Mbps may down-shift to 65 Mbps, 57 Mbps, 29 Mbps, or even lower speeds (down to 7 Mbps) if signal interference occurs

**Wi-Fi = Shared Network**

802.11 LANs are shared networks, meaning:

- Only one device can send at a time

- As more devices are added to LAN, throughputs of each device gets slower

**Two Types of Ethernets**

**Shared Ethernets**

- Computers connected via coaxial cable or through Ethernet hubs

- Data is broadcasted from single sender to all stations on LAN

**Switched Ethernets**

- Computers connected through ethernet switched

- Data is forwarded by intelligent switched based on Destination MAC address

**Switched Ethernet Data Delivery**

- Forwarding Table in switch contains, for each LAN device

- The MAC Address of that device

- The switch port that connects out to that device

- Incoming data packets are then simply sent out the switch port associated with the destination address in the packet

**Two Switch Modes**

**Store-and-Forward Mode**

+ No erroneous frames are forwarded

- Must wait until each frame is completely buffered before starting to re-transmit

EX 2 complete frame transmission times required to go through 1 switch

**Cut-Through Mode**

+ Minimizes delay in switch

+ Used in high performance networks (trading)

- Switch may forward erroneous frames

**Half Duplex Ethernet**

-Like a walkie talkie where one person at a time can talk and receive messages without interference

**Full Duplex Ethernet**

- Full-Duplex Ethernet allows a workstation to send and receive data simultaneously

- Requirements

- Must have a full-duplex Ethernet interface

- Must be connected to ethernet switch

**Switch Operations**

- Data frame arrives on switch interface (port) x:

- If destination address = FF:FF:FF:FF:FF:FF (broadcast) then the frame is re-transmitted out all ports except port x

- Else switch looks up destination address in forwarding table and finds associated port = y

- If x not equal to y then send frame out port y

- Else if x = y, drop the frame

- If there is no entry for destination address in Forwarding Table, then forward frame out all ports except port x (that is, broadcast the frame)

**Building Forwarding Table**

**Switch Learning**

- For each arriving data frame, switch examines source address and adds/updates its entry in forwarding table containing: Source address (6 byte format), Port that this frame arrived on, and Frame arrival time\

**Timing out Table Entries**

Table Entry Removal

- If the source address of an arriving frame is already in the Forwarding Table, switch will simply update the Update time to the current time.

- Any entry not updated within a specific timeout period (typically 5 mins) is erased from the Forwarding Table

**Allowing Multiple Paths**

- Only one active data path can exist between any pair of LAN switches (o.w. Address learning gets messed up)

- However, we want multiple paths for backup in case of transmission line failure

- Activating the *Spanning Tree Protocol* allows loops to exist in the network

**Virtual LANs**

- If we connect many switches together, we can get scalability problems

- **Problem:** Broadcasts can start to consume a lot of bandwidth since each broadcast fram gets copied to every device on every switch

- **Problem:** We may not want broadcasts sent everywhere due to security concerns

**Solutions?**

- A network can be split by a network manager into several Virtual LANs (VLANs)

- Each VLAN is it’s own broadcast domain

**VLAN Implementation**

- Sets of switch ports can be grouped into Virtual LANs by an admin

- Broadcast frame sent by any station are only set out to other ports on the same VLAN

- It works as if each VLAN is a separate switch

**VLAN Advantages**

- Less broadcast traffic = better performance, better security

- Network manager can control which resources each VLAN device “sees” when it broadcasts

- Different priorities may be assigned to different VLAN IDs, giving multiple levels of service

- Each VLAN is a separate IP subnet

**Overview of VLANs**

- A VLAN is a logical partition of a layer 2 network

- Multiple partitions can be created, allowing for multiple VLANs to co-exist

- Each VLAN is a broadcast domain, usually with its own IP network

- VLANs are mutually isolated and packets can only pass between then via a router

- The partitioning of the layer 2 network takes place inside a layer 2 device, usually via a switch

- The hosts grouped within a VLAN are unaware of the VLANs existence

**Additional Header Bytes IEEE 802.1Q sub-headers**

- Optional 802.1Q subheader adds 2 bytes between Ethernet and IP headers

- Priority (3 bits)

- Virtual LAN (13 bits)

- This subheader can be used by switches and servers to mark Ethernet frames with VLAN and Priority information

**Ethernet Frame Priorities**

- With 3 priority bits, an Ethernet frame can be assigned to any one of 8 (ex 2^3) priority classes:

Priority 7: Network-critical traffic, such as routing table update messages

Priority 5, 6: Delay-sensitive traffic, such as interactive video or voice

Priority 4: Business-critical traffic, such as streaming data, SAP data, transaction processing

Priority 2-3: Less critical business data

Priority 0-1: Best-effort traffic, such as non-essential e-mails and file transfers

- Switches use these bits to prioritize data frame transfer through the switch

**IPv4 Header**

- IPv4 adds 20 bytes of *IPv4 Header* to every data packet

- These 20 bytes include all information required by IP routers to direct this packet to its destination

**IPv4 Header Fields**

- **Version:** IP protocol version. Value = “4” for IPv4 header

- **IP Header Length:** Length of IP header in 32-bit words

**- Type of Service:** Indicates whether this packet should be low or high priority

**- Total Length:** Length of IP packet in bytes

**- Identification / Fragment Offset:** used to identify and reassemble **fragments** that are formed when routers break IP packets into smaller packets

**- Time to Live:** Max number of routers this IP packet may pass through. If exceeded, packet will be discarded

**- Protocol:** Identifies the protocol carried inside the *next header* after this IPv4 header-typically TCP or UDP

**- Header Checksum:** Allows error checking of IP packets

**- Source Address:** 4 byte IPv4 source address for the packet

**- Destination Address:** 4-byte IPv4 destination address for this packet

**Dynamic Host Configuration Protocol (DHCP)**

- Network admin can set static or dynamic address

- For dynamic, device will broadcast to the DHCP server

- DHCP server will return the following values required to sent IPv4 data

- IP Address

- Subnet Mask

- Default gateway address

- DNS server address

-Lease access time

**DHCP Server**

- DHCP server maintains pool of free IP addresses for each subnet and allocates with a *lease time*

- Device must renew IP address before lease time is up or the DHCP will reclaim it

**What’s a Router?**

- A router is a device with multiple network interfaces

- Ethernet interfaces connect the router to ethernet switches

- Serial interfaces connect routers to other router over point-to-point links

- Each interface has its own IP address and subnet mask

- Each interface connects to an *IP Subnet* of devices

- For us subnet = Ethernet LAn or a point-to-point link

**A Router’s Job**

Simply, forward packets from one IP subnet to another IP subnet

- It receives packets on one interface

- It looks up the packet’s IP destination address in routing table

- It ***retransmits*** the packet out another interface to get it closer to its destination

**Types of Routers**

**Wireless Home Routers**

- Combine a Wi-Fi access point, an Ethernet switch and a simple access router into a single box for home networking and Internet access across a DSL or Cable Modem connection

**Enterprise Routers**

- Interconnect Ethernets within a business organization

**Access Routers**

- Used to connect home or business LANs to an Internet access link to an Internet Service Provider (ISP)

**Backbone Routers**

- transport packets across the Internet backbone

**What’s a Subnet?**

- A subnet is a group of devices that can all send packets to each other *without* going through a router

- An Ethernet LAN is an example of a subnet

- PCs that can send packets to each other through any combination of Ethernet hubs and switches are members of the same subnet

- Every device in a subnet is allocated an IP address from a group of addresses called an **IP Subnet**

**What’s a Routing Table?**

- Each router stores a routing table that tells it how to forward packets to different IP address destinations

**Routing Table**

This routing table is somewhat like the Forwarding Table in an Ethernet switch **except**

- Forwards to IP subnets rather than Ethernet addresses

- Each IP subnet is a group of IP addresses

- Note that the routers are more scalable than switches, since each routing table entry is for an entire subnet of devices, while each switch forwarding table entry is for one individual device

- Routing tables can have a default route. If a packet destination doesn’t match any other routes in the table, it is forwarded over the default route

- *How do we keep addresses current?*

- Neighboring router periodically exchange Router Table Update messages to keep their tables up-to-date

**What’s in a Routing Table?**

Each entry in a routing table contains the following

**- Destination IP Subnet** - This identifies a group of IP addresses

**- Outgoing Interface** - The router interface the packet should be sent out to forward it towards the destination IP subnet

**- Next Hop -** The IP address of the next router this packet needs to go through, if any

**Router forwarding operation**: For each arriving packet

- Find the destination IP Subnet in the routing table that contains the IP destination address in the packet header

- Send packet out the corresponding Outgoing Interface to the Next Hop router

**Keeping Router Tables Up-to-Date**

How is a routing table set up and maintained?

- Initially, a network administrator specifies an IP address and subnet mask for each router interface

- This creates routing table entries for directly connected subnets

- In static routing, the network administrator manually enters routes for remote subnets into the routing table

- In dynamic routing, the router exchanges Routing Protocol messages with all neighbor routers

-Each router creates and updates remote subnet routes in its routing table based on information in Routing Protocol messages

**IP vs. MAC Addresses**

IP addresses are global

- The IP address of a device can be used by any other device on the entire Internet to communicate with it

- IP addresses are easily discoverable via DNS lookup, hyperlinks or scanning

MAC addresses are local to their subnet

- The MAC address or a computer or server is only known to other devices on the same IP subnet (EX the same LAN)

- MAC addresses never cross routers- there is no way to discover the MAC address of a device in a different subnet

**How a PC sends an IP packet**

When a device wants to send an IP packet, it must first determine whether the Destination IP is on the same subnet as the sending PC or on a different subnet

- If the destination is on the same subnet, then the PC adds an Ethernet header with Destination PC’s MAC address in the Ethernet Destination field

- If the destination is on a different IP subnet, then the PC adds an Ethernet header with the MAC address of the default gateway in the Ethernet Destination field.

**MAC Header Swapping**

When forwarding a packet, a router will:

1. Remove the MAC header of arriving packets

2. Determine the outgoing interface from Routing Table

3. Create a new MAC header for outgoing packet that has MAC source and destination addresses for next subnet

- The MAC header is either Ethernet (for Ethernet interfaces) or PPP header (for point-to-point interface)

- Thus, the TCP and IP headers stay unchanged end-to-end, but the layer 2 header changes at each router (hop) and local MAC addresses are never seen in packets outside the local subnet

*How does the router know all these MAC addresses?*

- Sends ARP request packets to learn them and stores them in a router ARP Table

**How’s the Routing Table used?**

For each arriving packet, the router will:

1. Remove the MAC header from the arriving packet

2. Look up the destination IP address from the packet in the Routing Table to determine both Interface and Next Hop (if present)

3. Create a new MAC header of the appropriate type (either Ethernet or PPP) of the selected interface

4. If there is a Next Hop value then

- If Ethernet interface, look in ARP Table to find MAC Address corresponding to Next Hop and put that into Destination Field of the new MAC header

5. If there is no Next Hop

- Look in ARP Table to find MAC address corresponding to Dest IP in packet and put that into Destination Field of the new MAC header

**IP Address Subnets**

An IP Address subnet is a group of IP addresses

- The size of the subnet (number of IP addresses) must be a power of 2

- All IP addresses within a subnet must be identical in the first n bits

- Value ‘n’ is called the Prefix Length, written “/n”

- Size of the subnet it 2^(32-n)

- First n bits of IP address are Routing Prefix Bits

- Last (32-n) bits of IP address are Host Bits

- The first IP in a subnet is called the **Network Address.** All Host bits in the Network Address must be 0

**A Device Subnet**

- A device subnet is a set of devices that can communicate with each other without going through a router

An Ethernet LAN is an example of a device subnet

- All devices in Subnet must be allocated IP addresses that are from the same IP address subnet

- Each interface on a router connects to a different subnet

- Thus, a router forwards packets from one subnet to another

**Subnet Notation**

IP Subnets are written as:

<Network Address>/<prefix length>

- This is called a Subnet ID

- This refers to the full group of addresses

- Example: 130.88.55.0/24 refers to a group of 256 IP addresses

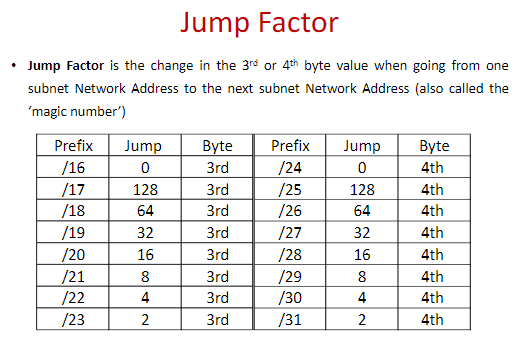
**Assignable Host Addresses**

In any subnet, there are **2 IP addresses** that cannot be assigned to any device:

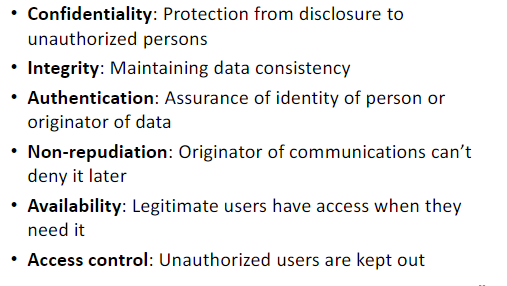
- The **first address** in the subnet (host bits are all 0s) is the Network Address and cannot be assigned to any device

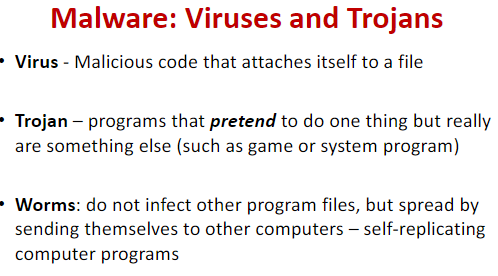
- The **last address** in the subnet (host bits are all 1s) is the Subnet Broadcast Address and cannot be assigned to any device

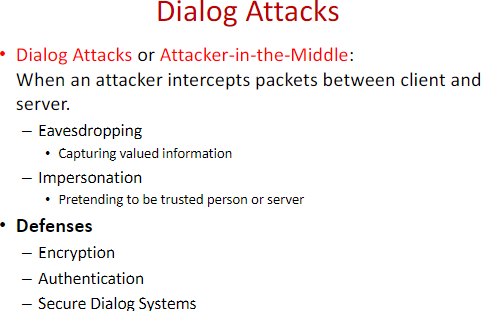
- So the maximum number of assignable host addresses (also called valid host addresses) is **2 less than the subnet size**

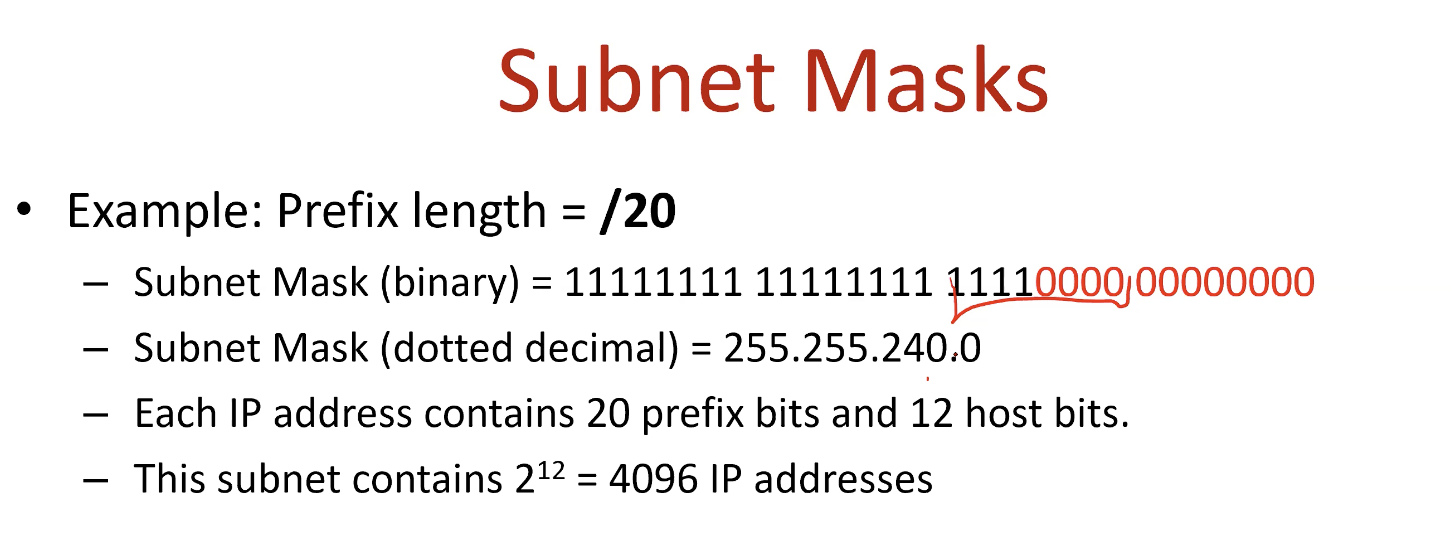
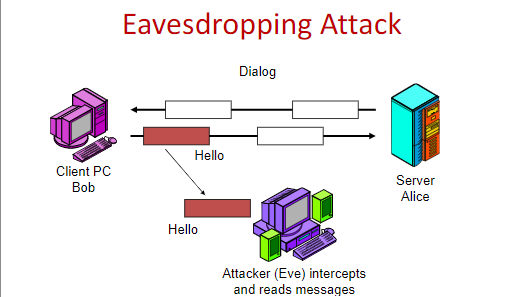


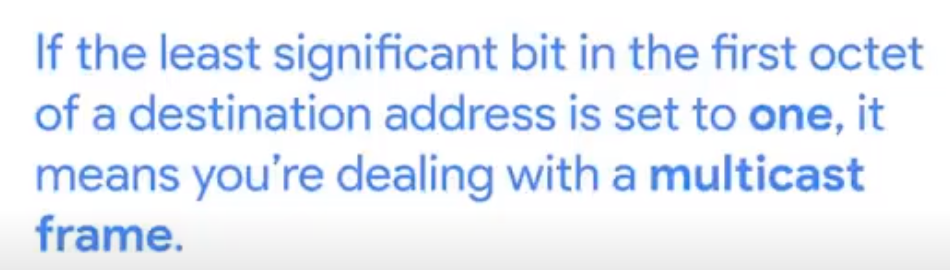


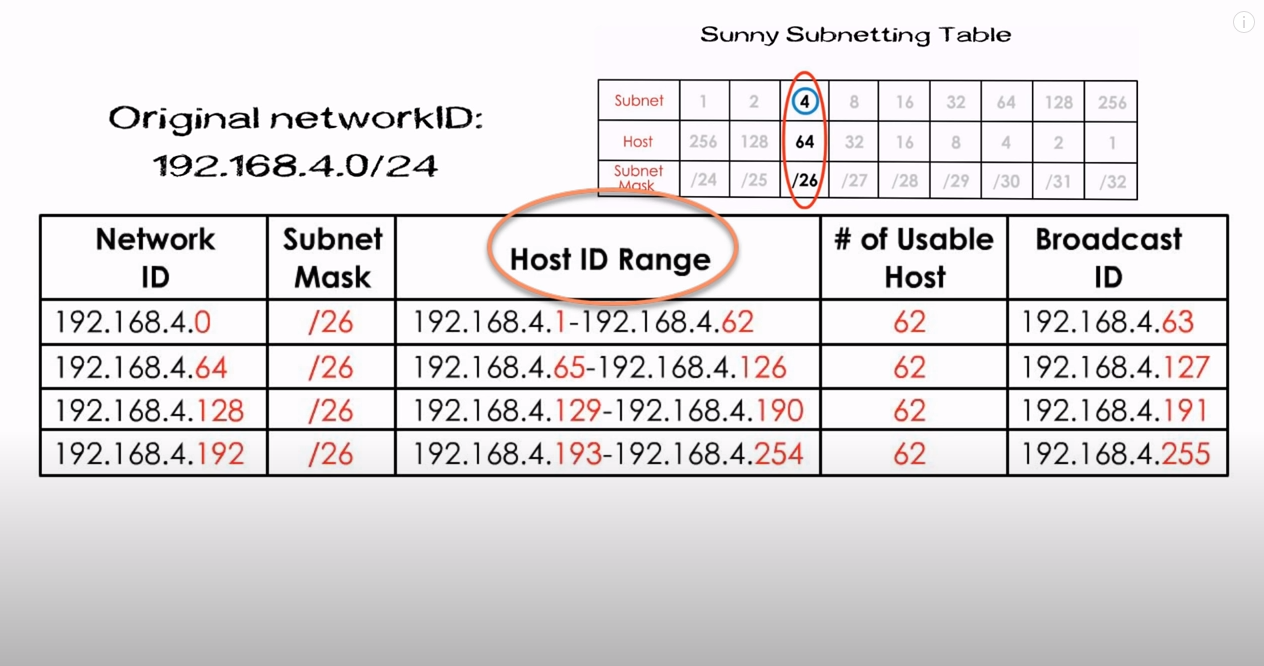


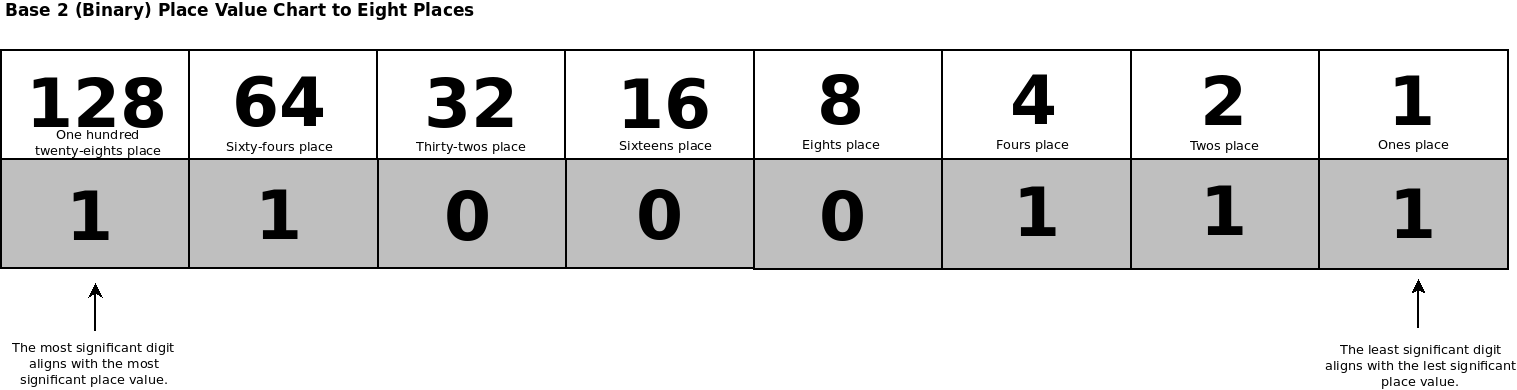










8 bits per slot in IP address -> 00000000.00000000.00000000.00000000 (ex: 140.192.18.0 -> 10001100.11000000.00010010.00000000)

