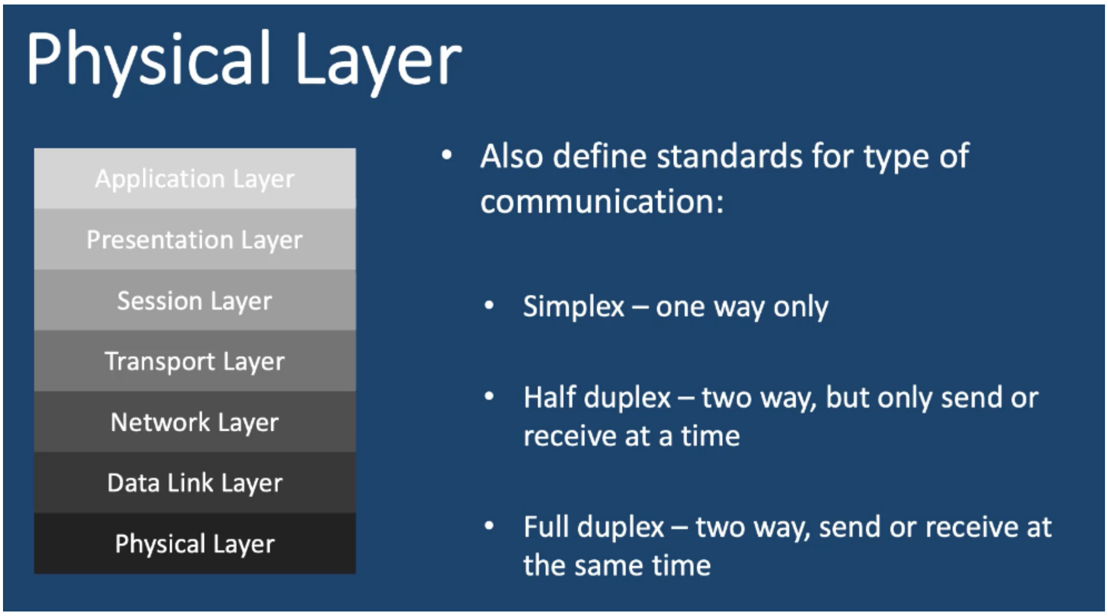
Network Basics



Collision Domains, Broadcast Domains, and VLANs

Collision Domains
- A hub is a single collision domain
- On a switch, each port is its own collision domain
- On a router, each port is its own collision domain

Broadcast Domains //ip
- A hub is a single broadcast domain
- A switch is a single broadcast domain
- On a router, each port is its own broadcast domain

VLAN
- VLAN is a logical separation of devices on the same LAN (switch)
- It allows you to divide a LAN segment into multiple logical LANs
- Each VLAN is a different network with a separate layer three addressing
- Different policies can be applied to traffic coming from different VLANs
- Each VLAN is identified by a unique IEEE 802.1Q ID (aka Tag)

Network Devices

Repeater (layer 1 device)
- used to repeat signals
- it receives a signal and retransmit it

Hub (layer 1 device)

- Operates in half duplex mode - can only send or receive data at any time
- Has multiple input and output ports allowing multiple devices to connect
- Data received on one port is forwarded out all other ports
- Has no intelligence of its own so it cannot learn MAC addresses

Bridge (layer 2 device)
- Learns MAC addresses
- Uses a CAM table to store port and MAC address information
- Frame forwarding is software-based.
- **how CAM table works**
- When a frame is received for the first time the source port and MAC address is added to the CAM table
- The frame is then forwarded out all ports other than the one on which it was received, because it is not known on which port the destination is connected.
- Once a response is received, the destination port and the MAC address is added to the CAM table
- Next time a frame is received for which the port is known, it is only forwarded out that port.

Switch (layer 2 device)
- learns MAC addresses
- specialized chips are used for frame forwarding, resulting in better performance.
- supports VLANs

Router (layer 3 device)
- routes packets between different networks
- use routing table to make routing decisions

Layer 2 Addressing

MAC address - layer 2 address, identifies a device on the local network
IP address - layer 3 address, identifies a device outside the local network

MAC Address
- Stands for media access control
- 48-bit address that is burned on the network interface
- represented as 6 groups of 2 hexadecimal digits, separated by colons
- the first 3 groups known as the **Organization Unit Identifier (OUI)**
- OUT identifies the manufacturer of the network equipment

Broadcast MAC address
- Consists of all F (all 1s in binary)
- Frames sent with the destination set as the broadcast MAC address will reach all hosts on the same network

Intro IPv4

- 32 bits logical address assigned to a network device
- format with 4 octets (8 binary bits) separated by dots

Classes of IPv4

- Class A - 0.0.0.0 to 127.255.255.255
- Class B - 128.0.0.0 to 191.255.255.255
- Class C - 192.0.0.0 to 223.255.255.255
- Class D - 224.0.0.0 to 239.255.255.255 (reserved for multicast purposes)
- Class E - 240.0.0.0 to 255.255.255.255 (reserved for experimental purposes)

RFC 1918 Address

- In each class A,B,C, a block of IP addresses has been reserved as private IP addresses
- These are not routable over the internet, hence known as private IP addresses.
- Not able to route packets over the internet.
- help to conserve the IP address pace by allowing organizations to use these private addresses for internal addressing.
- RFC 1918 Address
- Class A - 10.0.0.0 to 10.255.255.255 (10.0.0.0/8)
- Class B - 172.16.0.0 to 172.31.255.255 (172.16.0.0/12)
- Class C - 192.168.0.0 to 192.168.255.255 (192168.0.0/16)

Loopback address

- the entire 127.0.0.0/8 address block is reserved called loopback address
- 127.0.0.1 is localhost

Link Local Address:

- APIPA (Automatic private IP address) in IPv4
- APIPA range in IPv4 is 169.254.0.0/16
- Used for communicating over the LAN, cannot be used to route packets over to other LANs

Subnet Mask

Every IP address has two parts - network portion and host portion
Every IP address is accompanied by a subnet mask
Subnet mask is a 32-bit number that helps you separate the network portion from the host portion

Two ways to denote a subnet mask

- 10.0.0.0/8   (meaning 8 bits are 1)
- 10.0.0.0/255.0.0.0

When the subnet mask is converted to binary, the **1s denote the network portion** while **0s denote the host portion**

10.0.0.0/255.0.0.0

- Decimal: 255.0.0.0
- Binary: 11111111.00000000.00000000.00000000

The first 8 bits are made up of 1’s, that is the network portion

Hence the notation 10.0.0.0/8 – the number after the slash indicates the network portion

Default Subnet Mask
- Class A has a default subnet mask of /8
- Class B has a default subnet mask of /16
- Class C has a default subnet mask of /24

Total Number of Hosts
- possible host = 2^H, usable host = 2^H-2
- H represents the number of host bits (zeros) in a subnet mask
- -2 because, the first address is the network address and the last address is the broadcast address of the network
    - example: 192.168.1.0/24
    - 1st: 192.168.1.0
    - 2nd: 192.168.1.255
    - usable hosts: 2^8-2

Why do we need Subnetting?

- Consider a /30 subnet mask
- Total usable IP addresses = $2^2 - 2 = 2$
- Subnetting allows efficient use of IP addresses

Subnet Examples

Steps:
1. Convert the subnet mask into binary format
2. Determine the number of host bits to be borrowed

3. Determine the increment
4. Add increment to get the new subnets

Divide 192.168.1.0/24 into <u>5 networks</u>

- <u>Step1</u>
- 11111111.11111111.11111111.00000000
- <u>Step2</u>
- 192.168.1.0/24 is one network, if we need more networks we need more network bits
- 2^x >= 5   x>=3, we need to borrow 3 host bits
- 11111111.11111111.11111111.11100000
- /27 = 255.255.255.224
- <u>Step3</u>
- the increment is the power of 2 corresponding to the least significant bit = 2^5=32
- <u>Step4</u>
- increment should be added to the octet from which bits were borrowed, in this case, 4th octet
- 192.168.1.32
- 192.168.1.64
- 192.168.1.96
- 192.168.1.128
- 192.168.1.160
- 192.168.1.192
- 192.168.1.224
- all above with subnet /27

Divide 124.0.0.0/8 such that each network has <u>500 hosts</u>

1. Convert the subnet mask into binary format
   - Decimal: /8 – 255.0.0.0
   - Binary: 11111111.00000000.00000000.00000000

2. Determine the number of host bits to be **fixed**

   Instead of borrowing host bits to convert them to network bits, we'll fix the host bits that will remain unchanged

   $2^X \geq$ required number of hosts + 2

   $2^X \geq 500 + 2$

   X = 9 will give you 512 (2^9) subnets which is greater than or equal to 500

   Total number of bits to **fix** = 9

2. Determine the number of host bits to be fixed

/8 = 11111111.00000000.00000000.00000000

After fixing 9 host bits, remaining network bits are 23

/23 = 11111111.11111111.11111110.00000000

new subnet mask = /23 = 255.255.254.0
3. increment 1^2 = 2 at 3 octet

4. Add increment to get new subnets

124.0.0.0	.
124.0.2.0	.
124.0.4.0	124.254.0.0
.	124.254.2.0
124.0.254.0	.
124.1.0.0	.
124.1.2.0	124.254.254.0

Total number of subnets = 2^N = 2^15 = 32768 (N total number of bit borrow)
Total hosts per subnet = 2^H = 2^9 = 512, usable host per subnet = 512-2=510

Which subnet does 200.1.1.10/29 belong to?

1. /29=255.255.255.248
   11111111.11111111.11111111.11111000
2. –
3. increment is 2^3 = 8
4. 200.1.1.0
   200.1.1.8
   200.1.1.16

   ans = 200.1.1.8/29
   network address: 200.1.1.8
   broadcast: 200.1.1.15

Supernetting

- Allows you to represent smaller networks as a single larger network
- Helps with route summarization

Which supernet do these belong to?

- 10.4.0.0/16
- 10.5.0.0/16
- 10.6.0.0/16
- 10.7.0.0/16

Determine the common bits

- 10.4.0.0 – 00001010.00000100.00000000.00000000
- 10.5.0.0 – 00001010.00000101.00000000.00000000
- 10.6.0.0 – 00001010.00000110.00000000.00000000
- 10.7.0.0 – 00001010.00000111.00000000.00000000

Supernet address – 10.4.0.0

Use the new mask to determine the supernet

11111111.11111100.00000000.00000000

Supernet is 10.4.0.0/14

To derive subnets from the supernet

00001010.00000100.00000000.00000000 - 10.4.0.0/16

00001010.00000101.00000000.00000000 - 10.5.0.0/16

00001010.00000110.00000000.00000000 - 10.6.0.0/16

00001010.00000111.00000000.00000000 - 10.7.0.0/16

IPv6

- IPv6 addresses are 128 bits in length, resulting in a much larger address space
- broadcast removed
- not compatible with IPv4
- 8 groups separated by colons

IPv4 has three types of communication - unicast, multicast, broadcast
IPv6 introduces a new type of communication - Anycast

Anycast
- similar to multicast but it reaches the nearest node in the group

Stateless Address Auto Configuration

- An IPv6 device can generate a unique address that can be used to communicate over the network (on the fly even not assigned)

Rules of writing IPv6 addresses

1. leading zeros in a group can be discarded
2. any group of two or more zeroes can be replaced with :: (but only one)

- Applying rule 1 - 2001:0:0:0:48b5:0:0:9177
- Applying rule 2, there are two possibilities:
  - 2001::48b5:0:0:9177
  - 2001:0:0:0:48b5::9177

Types of IPv6

Unspecified Address

- used when a computer boots up and has no address assigned
- If the computer is on DHCP-enabled network, this address is used before it gets an address via DHCP
- denoted by ::/128, which is all zeros

Loopbacl Address

- denoted by ::1/128

Link Local Address

- Assigned by the computer to itself from the FE80::/10 range
- unique on the subnet
- helps the host with automatic address configuration when no static address is assigned and no DHCP server is present

Unique Local Address

- Unique and local addresses used for communicating inside the LAN
- Similar to RFC 1918 addresses in IPv4
- Cannot route over internet
- Range is FC00::/7

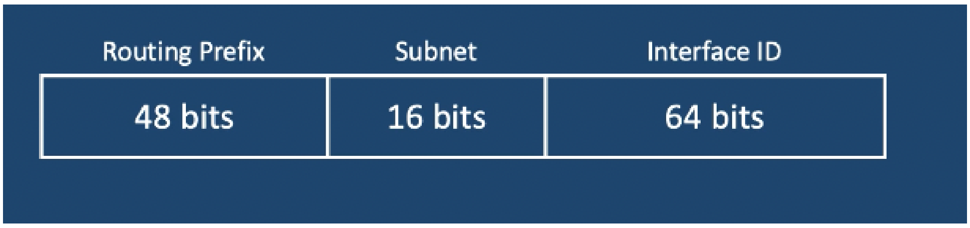
Global Unicast Address

- Public address
- range 2000::/3 to 3FFF::/3

Multicast address

- range FF00::/8
- used for destination address

IPv6 Subnetting



Routing Prefix assigned by the ISP
Interface ID aka host bits

Class of Service

Class of service allows you to assign traffic to classes and define their service levels
CoS allow you to provide differentiated services when **best effort delivery is insufficient**
With Cos, we can configure classes of service for different applications
Implemented using 6 bits in the IPv4 and IPv6 headers
Known as DSCP (differentiated service code point)

Jitter is defined as a variation in the delay of received packets and is generally caused by congestion in the IP network

Connection-oriented protocols vs Connectionless protocols

Connection-oriented protocols

- requires a connection to be established before exchanging data
- tcp - three way handshake connection (http, ftp, Talnet)

connection less protocols

- UDP (DNS
- lower overhead compared