WEEK 2

Day 6 : Ethernet LAN Switching (Part 2)

The Preamble + SFD is usually not considered part of the Ethernet header.

Thus ⇒ Size of Ethernet header + Trailer = 18 bytes
(6 + 6 + 2 + 4)

Minimum size for an Ethernet frame (Header + Payload [Packet] + Trailer) is 64 bytes
64 bytes − 18 bytes (header + trailer size) = 46 bytes

Minimum payload (Packet) size = 46 bytes

ARP (Address Resolution Protocol) is used to discover the layer 2 address (MAC address) of a known layer 3 address (IP address)

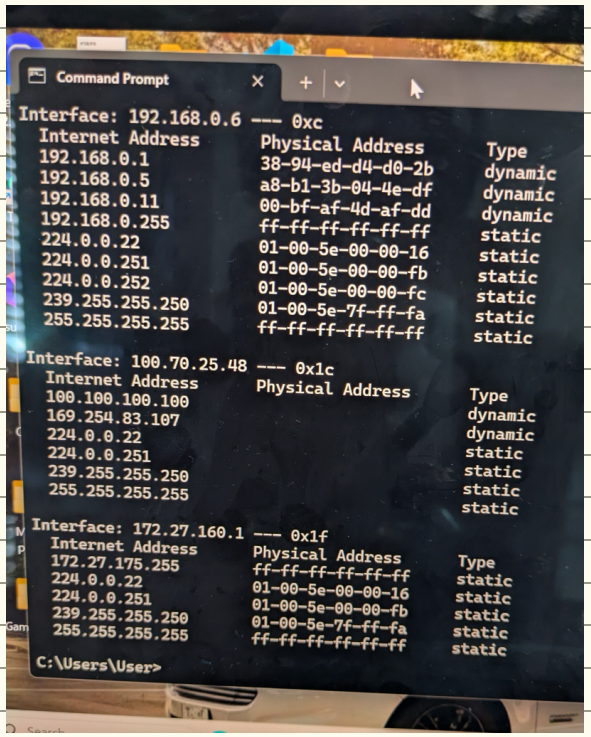
ARP → ARP Request
ARP → ARP Reply

ARP Request is broadcast

ARP Request Dest. Mac : FF:FF:FF:FF:FF:FF

PING : - A network utility that is used to test reachability.
- Measures round-trip time
- Uses 2 messages : ICMP Echo Request
ICMP Echo Reply

Command to use PING : ping (ip-address)



- Use arp -a to view the ARP table
- Internet Address = IP address (Layer 3 address)
- Physical Address = MAC address (Layer 2 address)
- Type static = default entry
- Type dynamic = learned via ARP

By default: - a ping in CISCO IOS sends 5 ICMP Echo Requests
- get 5 ICMP echo Replies back.

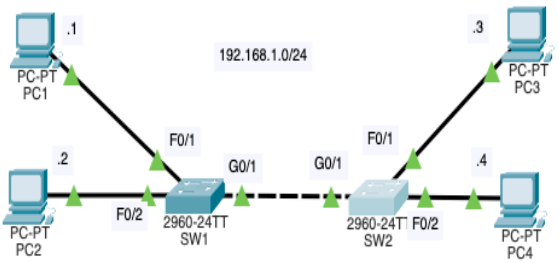
default size = 100 bytes.

Ports = Interfaces

Switches do not separate different Network, they connect and expand Network

Switches @ Layer 2 ⇒ OSI Model

Day 6 Lab : Analyzing Ethernet Switching



Both switches have an empty MAC address table, and all PCs have an empty ARP table.

1. If PC1 pings to PC3, what messages will be sent over the network, and which devices will receive them?
2. Send the ping and use Packet Tracer's 'simulation mode' to verify your answer.
3. Use pings to generate network traffic and allow the switches to learn the MAC addresses of all PCs on the network.
4. Use 'show' commands on the switches to identify the MAC address of each PC.
5. Clear the dynamic MAC addresses from the MAC address table of each switch.

Step 1:

1. ARP Request (Received by PC_2, PC_3, P_4)
2. ARP Reply (Received by PC_1)
3. ICMP Echo Request (Received by PC_3)
4. ICMP Echo Reply (Received by PC_1)

Step 2 :

Day 7: IPv4 Addressing (Part 1)

Layer 3: Network Layer

- Provides connectivity between end hosts on different networks
- Provides logical addressing (IP addresses)
- Provides path selection between source & destinat°
- Routers Operate at Layer 3.

Routing

IPV4 are writen using *Dotted Decimal*

4 bytes = 8 bits each.

32 bits ⇒ Splits into 4 Octects

221 = 11011101

128	64	32	16	8	4	2	1
1	1	0	1	1	1	0	1

11000000101010000000000111111110

11000000 10101000 00000000 11111110

192 . 168 . 1 . 254 /24

24 bits of IP address represent the Network portion of the Address and remaining 8 Represents the End-host.

10011010 . 01001110 . 01101111 . 00100000

↓

154 . 78 . 111 . 32 / 16

00001100 . 10000000 . 11111011 . 00010111

12 . 128 . 251 . 23 / 8

IPv4 Address Class

Class	First Octect	First Octet # Range
A	0	0 - ~~127~~ 126
B	10	128 - 191
C	11	192 - 223
D	111	224 - 239
E	1111	240 - 255

D → MultiCast Address

E → Reserved (Experimental)

Loopback Address

Address Range 127.0.0.0 - 127.255.255.255

Used to test the Network Stack (think of OSI, TCP/IP model) on the local device.

If Host portion of the address = 0's ⇒ Network Address

" " " " = 1's ⇒ Broadcast Address

Prefix / Netmasks

Day 8: IPv4 Addressing (Part 2)

* Subnet Mask

Instead of /24, you can write 255.255.255.0

So 192.168.1.10/24 = 192.168.1.10 255.255.255.0

/24 is CIDR Notation

* What does /24 actually means?

IPv4 has 32 bits

If we have: /24 that means:

- 24 networks bits

&

- 8 host bits.

Thus ⇒

Network bits	Host bits
11111111.11111111.11111111.	00000000
24 bits	8 bits

that's why /24 = 255.255.255.0

* How Many Hosts can /24 have?

You have 8 host bits

⇒ $2^8 = 256$ addresses.

But you normally cannot use 2 of them for Hosts:

* Network address
* Broadcast address

⇒ 256 - 2 = 254 usable hosts

/24 → 254 usable hosts

Broadcast Address: Is used to communicate with everyone on the network

E.g: 192.168.1.0/24

Broadcast = 192.168.1.255

So

Network address = 192.168.1.0

Usable adress = 192.168.1.1 = 192.168.1.254

Broadcast = 192.168.1.255

Subnetting = Taking a big Network & breaking it into smaller Networks.

* Why Subnet ?

Suppose you have: 192.168.1.0/24 ⇒

You have 254 usable hosts → Company only needs 50 computers per department. Instead of putting everyone on one giant network, you can divide it.

192.168.1.0/26 192.168.128/26

192.168.1.64/26 192.168.1.192/26

CIDR	Subnet Mask	Block Size	Usable Hosts
/24	255.255.255.0	256	254
/25	255.255.255.128	128	126
/26	255.255.255.192	64	62
/27	255.255.255.224	32	30
/28	255.255.255.240	16	14
/29	255.255.255.248	8	6
/30	255.255.255.252	4	2

Eg: /26 ⇒ 255.255.255.192

256 - 192 = 64

Thus the size block is 64 (The Networks occur every 64:)

⇒

192.168.1.0 /26 ⇒ 192.168.1.64/26

⇒ 192.168.1.128/26 ⇒ 192.168.1.192/26

Another Example: What is the Network address of 192.168.1.70/26 ?

First thing to do ⇒ Find the block size of /26 ⇒ 255.255.255.192

⇒ 256-192 = 64

Thus Networks : 0, 64, 128, 192

If we take 70 it fall between 64-70 ⇒ 128

Therefore

Network: 192.168.1.64

BroddCast : 192.168.1.127

And usable hosts 192.168.1.65 - 192.168.1.126

Day 8 Lab : Configuring IP Addresses

Day 9: Switch Interfaces

. Interface Speed & duplex.

- Speed & duplex negotiation
- Interface status
- interface counters & errors

Switch interfaces don't have the shutdown command applied by default.

= will be in the up/up state if connected to another device OR in the down/down state if not connected to another device.

Router interfaces have the shutdown command applied by defaut

= will be in the administratively down/down state by default

Show interfaces status: to check on Switch interfaces.

* Full / Half Duplex:

- Half duplex: The device cannot send and receive data at the same time. If it is receiving a frame, it must wait before sending a frame.
- Full duplex: The device can send & receive data at the same time. It does not have to wait.

Carrier Service Multiple Access with collision detection (CSMA/CD) ⇒ Hub (layer 1)

- Before sending frames, devices "listen" to the collision domain until they detect that other devices are not sending.
- If a collision does occur, the device sends a jamming signal to inform the other devices that a collision happened.
- Each device will wait random period of time before sending frames again.
- The process repeats.

Switches (modern network switches) do not use CSMA/CD during normal operation because each switch port creates its own isolated collision domain.

Switches : - Full-duplex mode
- No Share medium.

* Speed / Duplex Autonegotiation : allows two connected network devices (like a computer & a switch) to automatically talk to each other, compare their capabilities, an choose the fastest possible speed and duplex setting they both support.

Interface Errors:

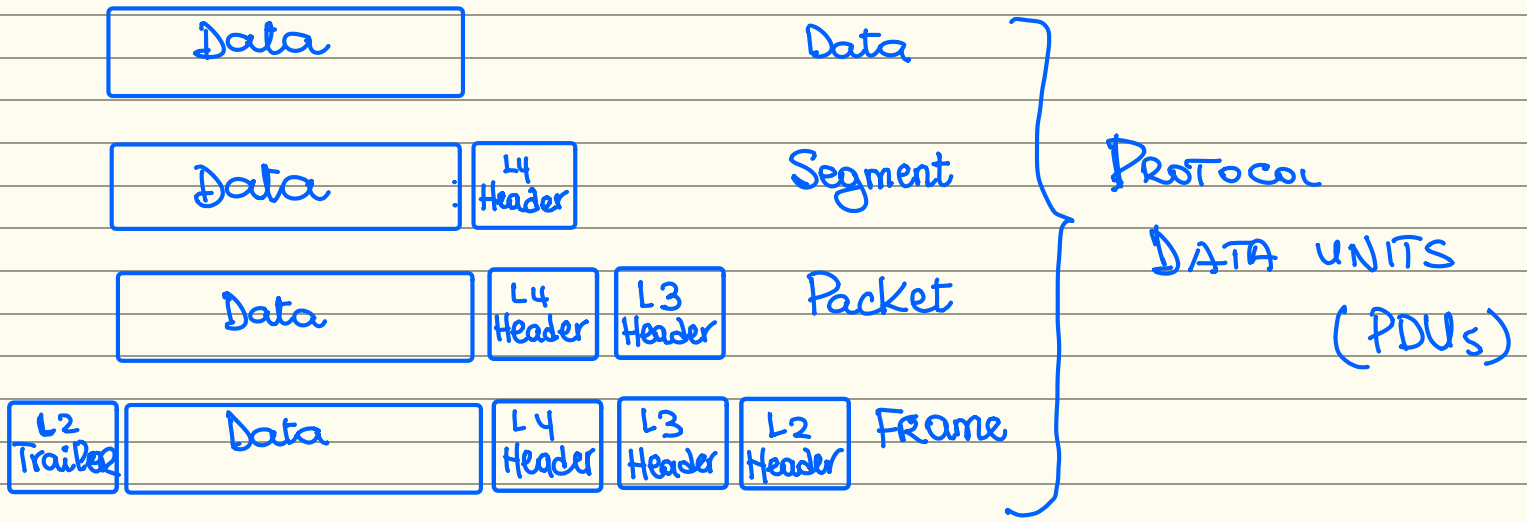
- Runts: Frame that are Smaller than the minimum frame size (64 bytes)
- Giants: Frame that are larger than the maximum frame size (1518 bytes)
- CRC: Frame that failed the CRC check (in the ethernet FCS trailer)
- Frame: Frame that have an incorrect format (due to an error)
- Input errors: Total of various counters, such as the above four
- Output errors: Frames the switch tried to send, but failed due to an error.

Show interfaces cmd: Shows various counters of errors detected on an interface.

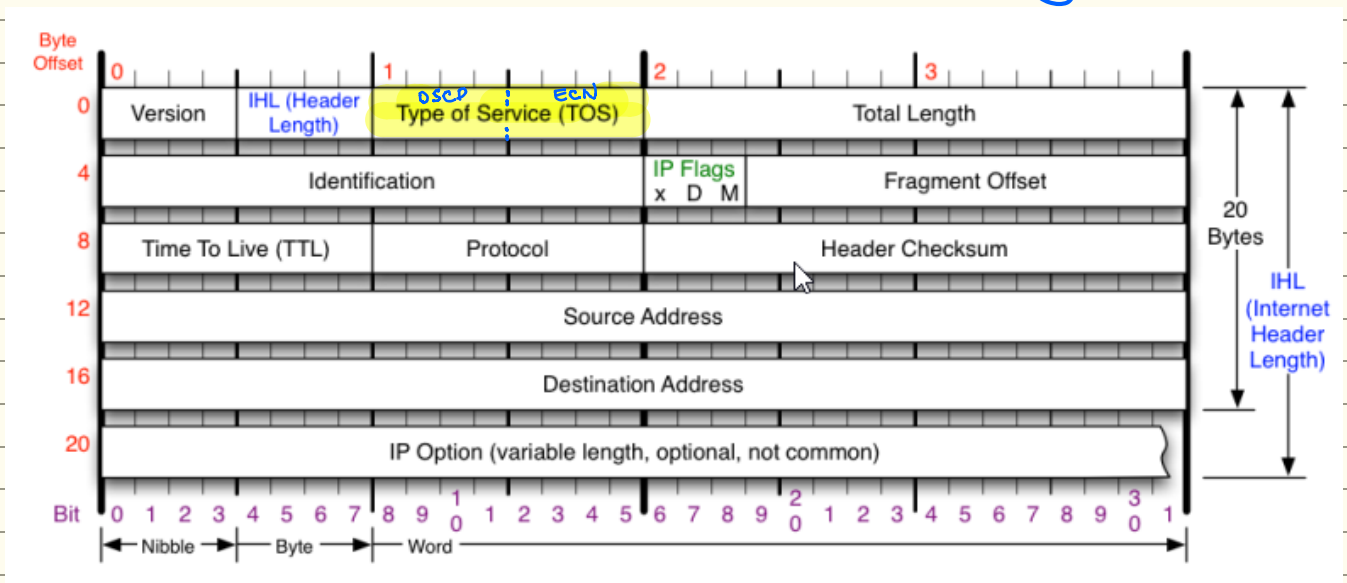
Day 10: The IPV4 Header

Layer 3: help send data between devices on different network.

- IPV4 packet Structure
- Fields of the IPV4 Header



L3 - Header => IPV4 Header => Routing Packet



* Version field = 4 bits = Identifies the version field (0100)
* Internet Header Length / IHL fied = 4 bits (Identifies the length of the Header in 4-byte increments)

Final Field of the IPV4 header (Options is a variable or length = Identifies the length of the header in 4 byte increments.

Minimum IPV4 Header Length = 20 Bytes.

- Minimum value is 5 (= 20 bytes)
- Maximum value is 15 (15 x 4-bytes = 60 bytes)

* DSCP (Differentiated Services Code Point) ⇒ length = 6 bits
Used for QoS (Quality of service)
Essentialy Used to prioritize delay-sensitive data (streaming voice, video, etc ...)

* ECN field (Explicit Congestion Notification) ⇒ length = 2 bits.
Provides end-to-end (between two endpoints) notification
Network Congestion without dropping packets
Network busy = Congestion

* Total Length ⇒ Length : 16 bits = Total length of Packet

* Identification ⇒ Length : 16 bits
Packet are fragmented if larger than MTU (Maximum Transmission Unit) ⇒ usually 1500 bytes

* Flags ⇒ length 3 bits ⇒ Used to control / identify fragments
  - Bit 0 : Reserved, always set to 0
  - Bit 1 : Don't fragment (DF bit), used to indicate a packet that should not be fragmented
  - Bit 2 : More fragments (MF bit)

* Fragment offset ⇒ length 13 bits ⇒ used to indicate the position of the fragment within the original, unfragmented IP Packet

* Time to live ⇒ length : 8 bits

* Protocol ⇒ length : 8 bits ⇒ indicates the protocol of the encapsulated L4PDU

  - Value of 6 : TCP
  - Value of 17 : UDP
  - Value of 89 : OSPF (dynamic routing protocol)
  - Value of 1 : ICMP

* Header Checksum ⇒ length : 16 bits ⇒ used to check for errors only in the IPv4 header

* Source & Destination IP address ⇒ length 32 bits each

* Option ⇒ length 0 – 320 bits ⇒ Rarely used.
  if the IHL field is greater than 5, it means that options are present.

Summary:

- IPv4 packet structure
- Fields of the IPV4 header

Quiz:

Wich field will cause the packet to be dropped if it has a value of 0?

a) TTL (Time to Live) c) IHL

b) DSCP d) ECN

How are errors in an IPv4 packet's encapsulated data detected?

a) The IPv4 Header Checksum field checks for errors.

b) The encapsulated protocol (TCP, UDP) checks for errors.

c) Errors in the encapsulated data cannot be detected.

The IPv4 Header Checksum field only checks for errors in the IPv4 header itself. However, layer 4 protocols like TCP or UDP can use their checksum to check for errors in the encapsulated data.

Which field of an IPV4 header are variable in length.

Answers => Options