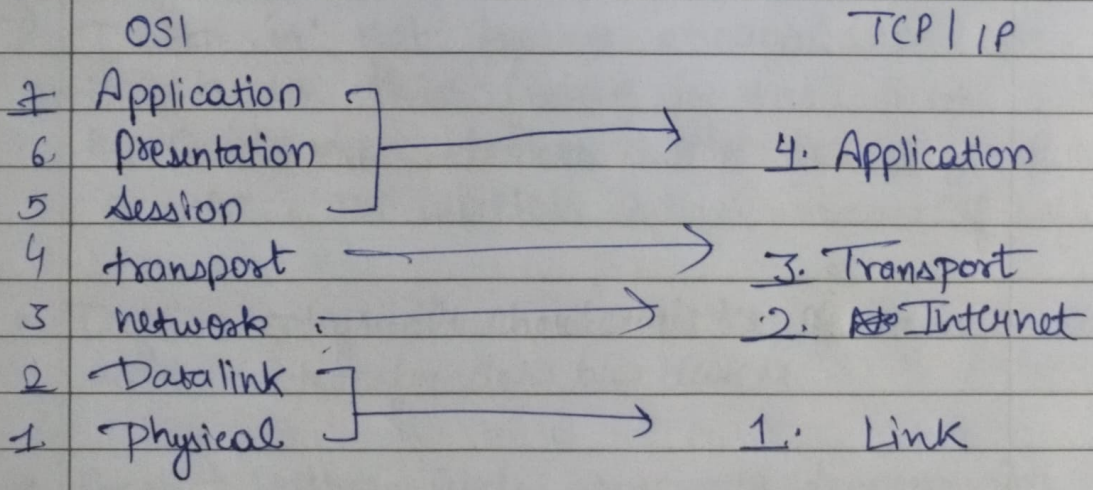
TCP/IP Suite / Model

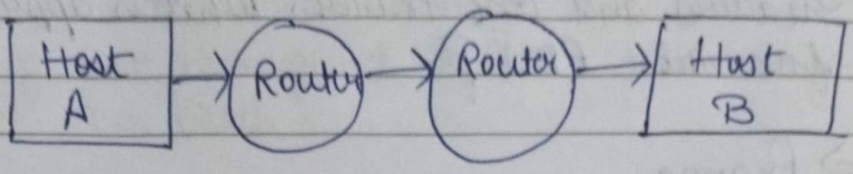
__/__/__

- Conceptual model and set of Communication protocols used in the internet and other networkes.
- known as TCP/IP bcoz those are two of the foundational protocols in the suite.
- Developed by the united states department of Defense through DARPA (Defense Advanced Research Projects Agency).
- Illy structure to the OSI model, but with fewer layers.
- this is the model actually in use in modern technology (modern networkes).
- Note: The OSI model still influences how network engineers think and talk about networks.

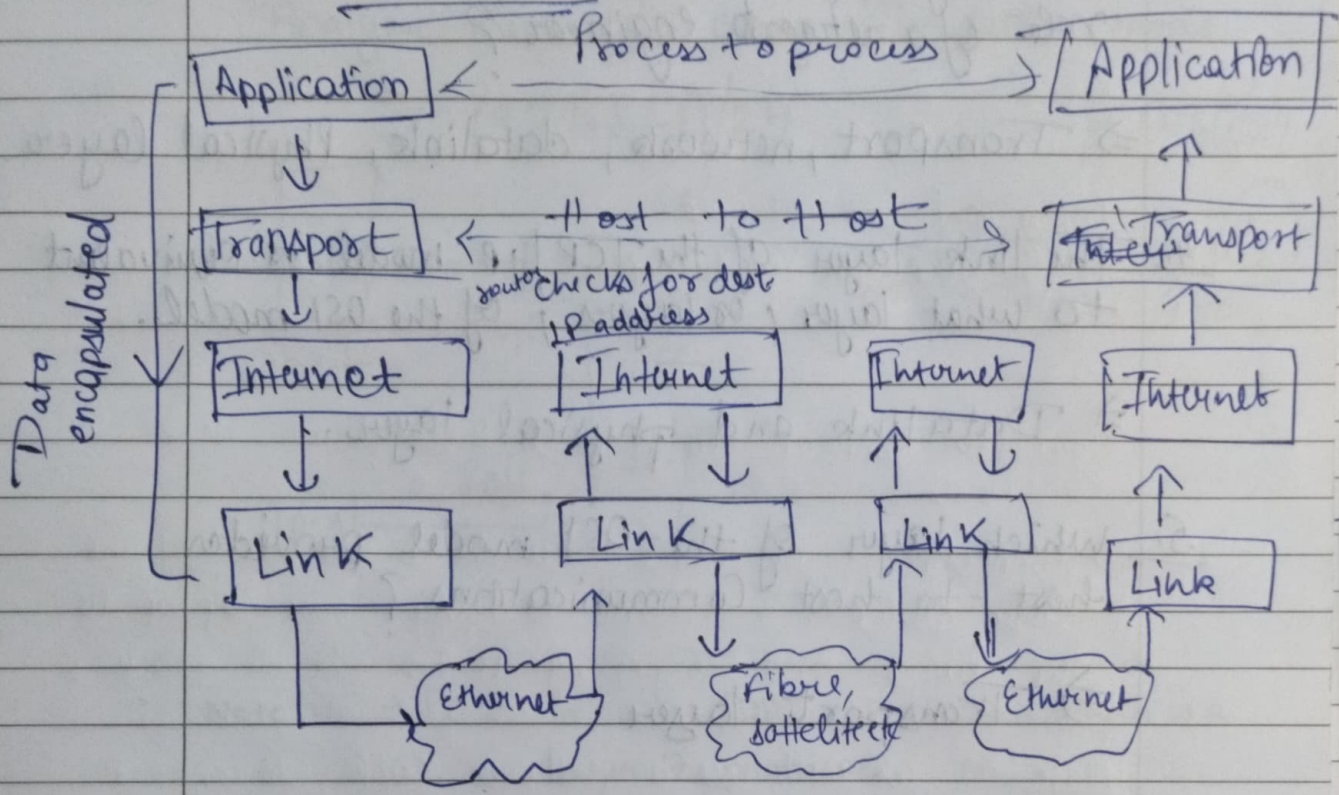


TCP/IP

Network Topology



Data flow



Note ⇒
Any type of device like dell can connect to any other like MAC etc.

Quiz

1 HTTP data sent from a youtube web server is displayed via your web browser. this is an example of what?

⇒ Same-layer Interaction

__/__/__

2. HTTP data has been encapsulated with three separate headers and one trailer, what is appropriate name for this PDU?

⇒ frame

3. Which layers of OSI model are most relevant to the role of a network engineer?

⇒ Transport, network, datalink, Physical layer.

4. The link layer of the TCP/IP model is equivalent to what layer (or layers) of the OSI model.

⇒ Datalink and physical layer..

5. Which layer of the OSI model provides host-to-host communications?

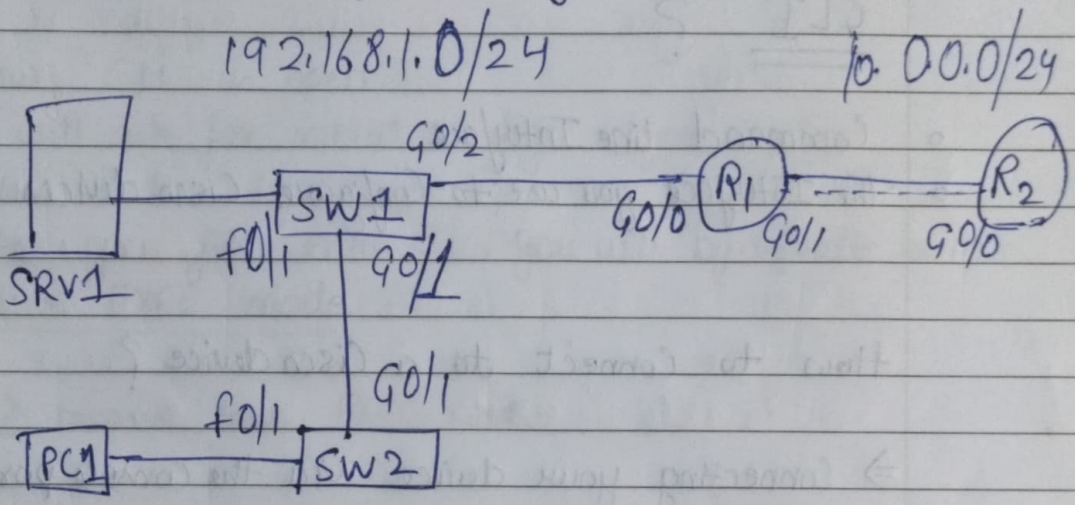
⇒ Transport layer.

__/__/__

Lab

1. Use 'simulation mode' to analyze the various traffic being sent throughout network. What layers of OSI are used.

2. Release and renew PC1's IP address to generate some Layer 7 traffic.
Analyze the traffic using simulation mode.



Note ⇒ ⇒ PC1 is using DHCP protocol which is a Layer 7 protocol.
⇒ PC1 is automatically recieving an IP address through DHCP
⇒ To generate some DHCP traffic.
⇒ PC1 get to release its IP address and then renew it.

Click on PC1 → Desktop → Cmd prompt
→ ipConfig to release ip address
→ ipConfig /release.
now, renew it.
→ ipconfig /renew.

Intro to CLI

CISCO IOS CLI

CiscoIos is the operating system used on cisco devices like windows on a PC, or mac OS on an IMAC

CLI ?

- Command line Interface
- The Interface you use to Configure Cisco devices

How to Connect to a Cisco device ?

⇒ Connecting your device via the Console port of the other device. it means bringing your laptop to the device and connecting it to Console port.

Note ⇒ we will use a roll over cable to connect the PC to RJ-45 port in Console port in the switch.

So, after that we will need a terminal emulator to connect to CLI.

Use Putty to get to the CLI

Open putty → Serial → open.

you will be able to Connect to the CLI

__/__/__

⇒ You will be connected to CLI using default settings.

You can down on left side → click on serial option → to change the default settings.

Speed = 9600 bits per sec.
Data bits = 8
Stop bits = 1

Now, CLI is open.
it will ask for initial Config. type 'no'.

⇒ when you first enter CLI, you will by default be in User EXEC mode.

> means user EXEC mode

Router >
↳ hostname of the device.

- User EXEC mode is very limited.
- User can look at some things but can't make changes to the Configuration.
- Also called 'user mode'.

let's move to mode with more power to make changes to the device.

Router > enable → you will be moved to privilaged exec mode.
Router #
↓
privilage exec mode.

Note ⇒ there are much more commands in privilaged mode than in user mode. you can see list of cmd's by just typing ? ← to view available Cmd's.

- we can write en → then press tab. it will automatically write the whole cmd. enable.
- or type en → press enter it will also work.

- if we just type e → it will return % Ambiguous cmd : "e"

- type e? ← it will show cmds starts with e.
  > enable exit

⇒ To make changes to the router Configure we need to enter ' global configuration mode'

cmd = #Configure terminal
or
conf t (in short)

Enable Password

Router (config) # enable password?
password

without space? shows all possible terms related to alphabets you wrote.

Router (config) # enable password ?

with space.
will show the options for setting the passwords.

7 Line Level → Like this

Router> enable
Password: ____
Router #

enable password "write password" ?

to see more options.

enable password CCNA.

Now, your password is set.
type exit, then you can test it.

incorrect passwd → "% Bad secrets"

running-config / startup-config

- there are two separate configuration files kept on the device at once.
- Running-config = the current, active configuration file on the device. As you enter cmd's in the CLI, you edit the active config.
- Startup-config = the ~~conf~~ config. file that will be loaded upon restart of the device.

In terminal

⇒ Router # Show running-config

→ to view the current running config. files

Router # Show startup-config.
it will show
Startup-config is not present.
"bcoz we haven't save any running-config. files."

⇒ Saving the config. file.

we are in privilage exec mode. Currently,

Router # write
Building configuration...
[OK]
Router # write memory.
Building Con——— ~~
[OK]
→ to indicate Config. was saved.

Router # copy running-config startup-config
Destination filename [Startup-config]?
Building Configuration ...
[OK]
Router #.

Copying running config to startup-config. and doing the same work as above two.

Now, type
Router # Show Startup-Config

⇒ it displays the same config. as we have seen in running-config.

__/__/____

⇒ when we type show running-config or startup-config. it is clearly showing our password so anyone can easily steal that password easily and can get access to privilage exec mode.

⇒ So, to make it more secure, we need to use 'service password-encryption' command in global configuration mode.

Router # conf t ↓ we have entered global conf. mode
Router (config) # service password-encryption.

Now, if you type show running-config.
it will show password as.

enable password 7 0802 6f 6028
↑
type of encryption.

but this type of encryption can be decrypt easily by just search on google.

So, there is a more secure and complex encryption. the cmd for that is

Router (Config) # enable secret Cisco
↑ Password

do sh run
↑ ↑ show running-config
for using ~~global config~~ privilage exec mode cmd's in global config. mode

Now, you will see passwd as.

enable secret 5 1mERx$YLCkLMcTYWwKf1
Cendtll.

5 = MD5 encryption.

Note ⇒ when enable secret "Password" is set than enable password "password" will be ignored

⇒ How to Cancel or delete a Cmd that you've entered?

Just type "no" in front of cmd.

Ex.

Router (config) #no Service password-encryption.

- previous passwd will not be affected
- but when we set new passwords they will be without encryption.

Service password - encryption.

if enable ⇒
- Current pass will be encrypted
- future pass will be encrypted
- the enable secret will not be affected.

if disable ⇒
- Curr pass will not be decrypted.
- future pass will not be encrypted.
- the enable secret will not be affected.

__/__/__

Quiz

1. What kind of cable is used to connect to a Cisco device via the RJ45 console port?

⇒ Roll-over Cable

2. You type enable to enter privileged exec mode on your Cisco router, however the pass you enter is not accepted. What could be the problem?

⇒ Capslock is on.

3. What is the most secure method to protect access to privileged EXEC mode?

⇒ the enable secret command.

4. if both the enable password and the enable secret cmd are configured, what will happen when you use enable to enter privileged EXEC mode?

⇒ You must enter the enable secret only.

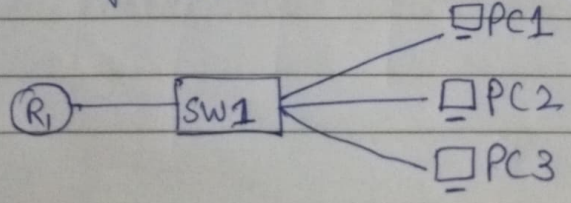
5. You enter conf t command to enter global config. mode. What is the full length version of the command.

⇒ Configure terminal.

__/__/____

Lab

1. Change the hostnames of the router and switch to the appropiate names (R1, SW1)
   ## use the 'hostname' cmd in global config. mode ##
2. Config. an unencrypted enable password of 'CCNA' on both sides.
3. Exit back to user EXEC mode and test the password
4. View the password in the running Config.
5. Ensure that the current password and all the future passwords are encrypted.
6. View the password in the running Config.
7. Config. a more secure, encrypted enable password of 'Cisco' on bothe devices.
8. Exit back to the User-Exec mode and then return to the privilaged exec mode. which password ?
9. View the pass. in the running Config.
   what encryption type number is used for the encrypted enable pass and enable secret?
10. Save the running Config. to startup Config.

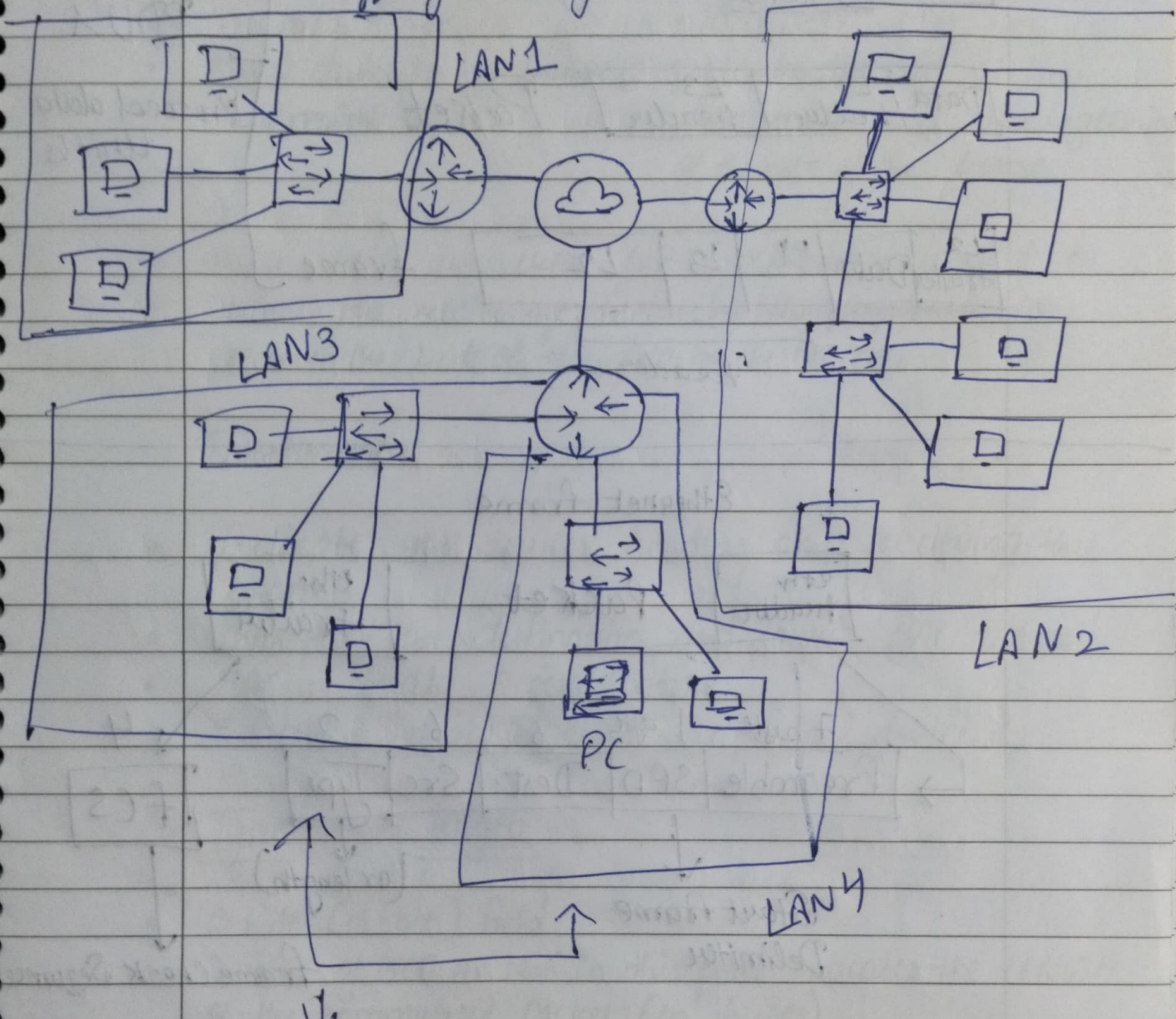


__/__/__

Ethernet Switching Part 1

Local Area Networks (LAN's)

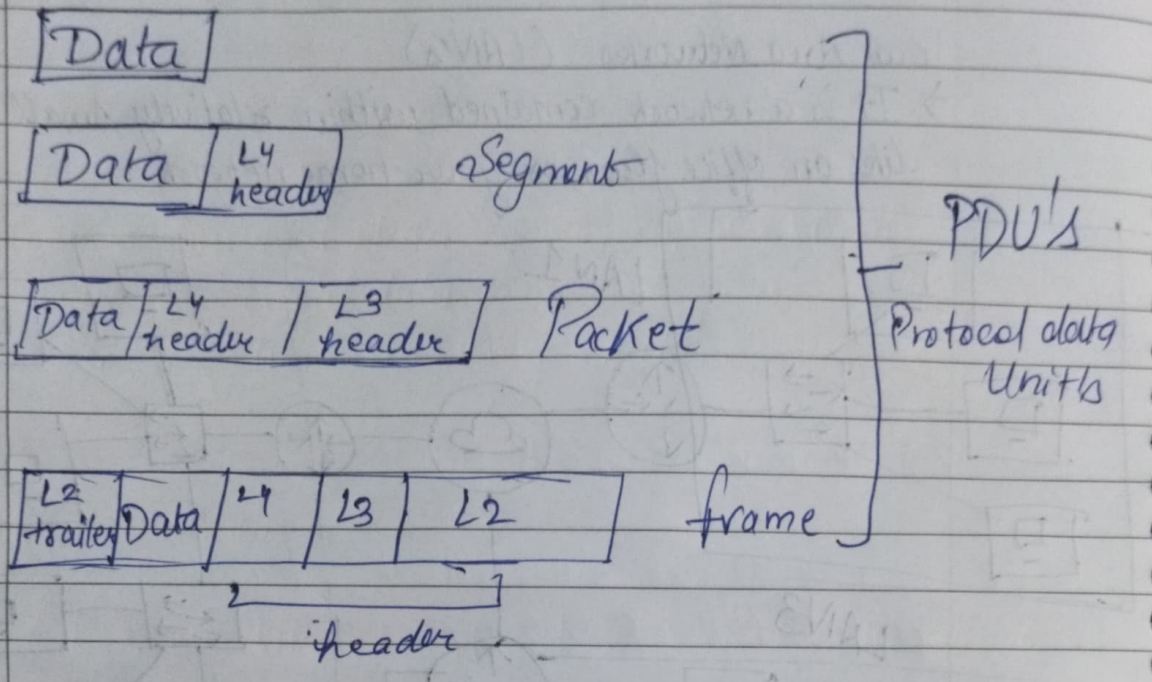
⇒ It is a network contained within relatively small area like an office floor or your home network



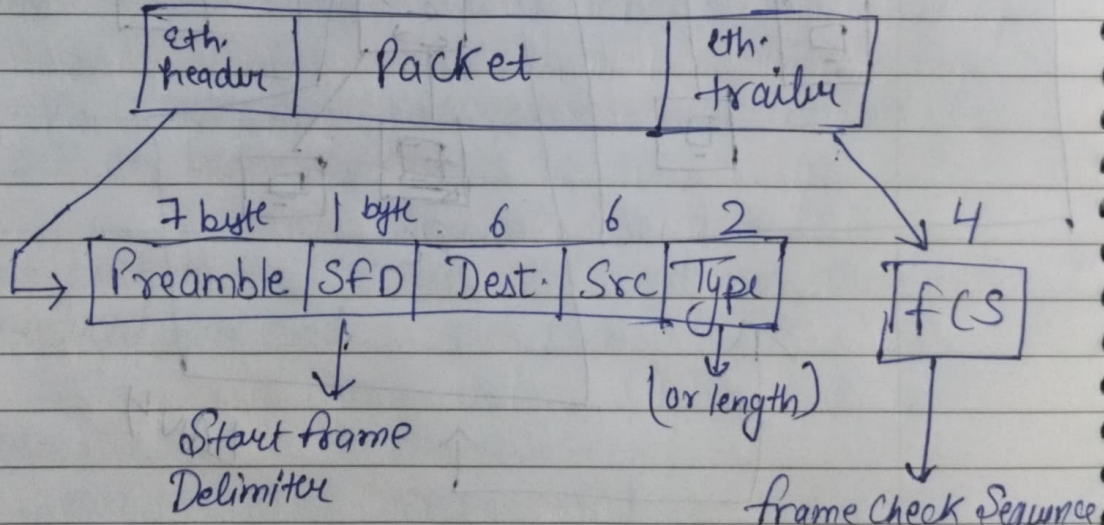
↓

as the switches are not connected to each other so they are separate LAN's

OSI Model - PDUs



Ethernet frame



= 26 bytes (header + trailer)

Ethernet Header

__/__/__

Preamble

- length 7 bytes (56 bits)
- Alternating 1's and 0's
- 10101010 * 7
- Allows device to synchronize their recieve clocks

SFD

- Start frame Delimiter
- length: 1 byte (8 bits)
- 10101011
- Marks the end of the preamble and the beginning of the rest of the frame.

- these both are used for synchronization and to allow the recieving device to be prepared to recieve the rest of the data in the frame.

Destination

- Indicate the devices sending and recieving the frame.
- Consist of the destination and source 'MAC address'
- MAC = Media Access Control.
- = 6 byte (48-bit) address of the physical device.

Source

Type or length

- 2 byte (16-bit) field
- A value of 1500 or less in this field indicates the LENGTH of the encapsulated packet (in bytes).
- A value of 1536 or greater in this field indicates the type of the encapsulated packet (usually IPv4 or IPv6) and the length is determined via other methods.

IPv4 = 0x0800 (hexa decimal) (2048 in decimal).

IPv6 = 0x86DD (Hexa decimal) (34525 in decimal)

Ethernet Trailer

1/1

FCS

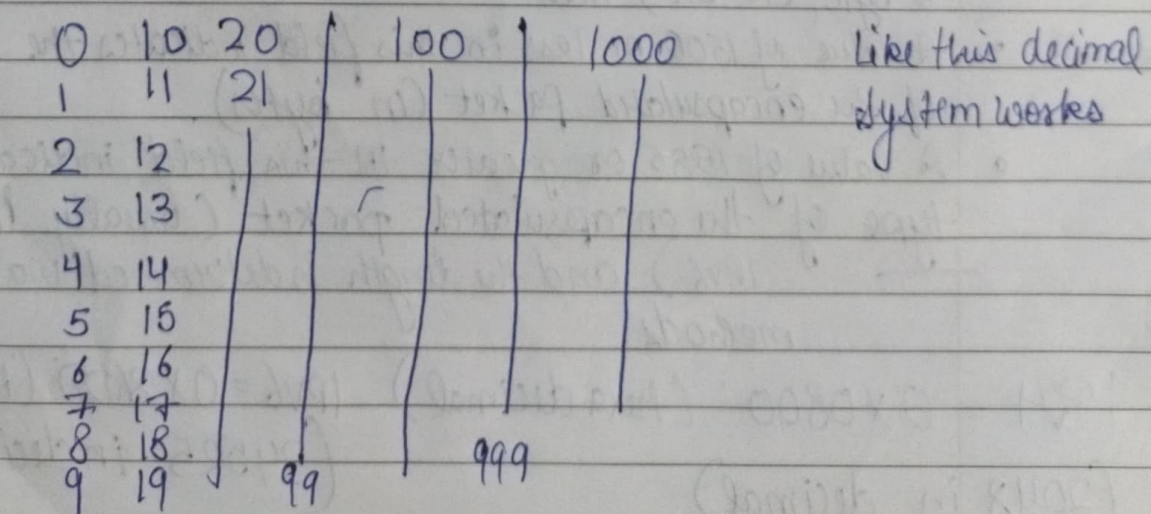
- Frame Check Sequence
- 4 bytes (32 bits) in length
- Detects corrupted data by running a 'CRC' algorithm over the recieved data
- CRC = 'Cyclic Redundancy Check'

MAC address

- 6 byte (48-bit) physical address assigned to the device which it is made
- A.K.A. 'Burned-in Address' (BIA)
- is globally unique
- the first 3 bytes are the OUI (Organizationally Unique Identifier), which is assigned to the company making the device
- the last 3 bytes are unique to device itself.
- written as 12 hexadecimal characters.

Decimal

Uses 10 possible digits: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9

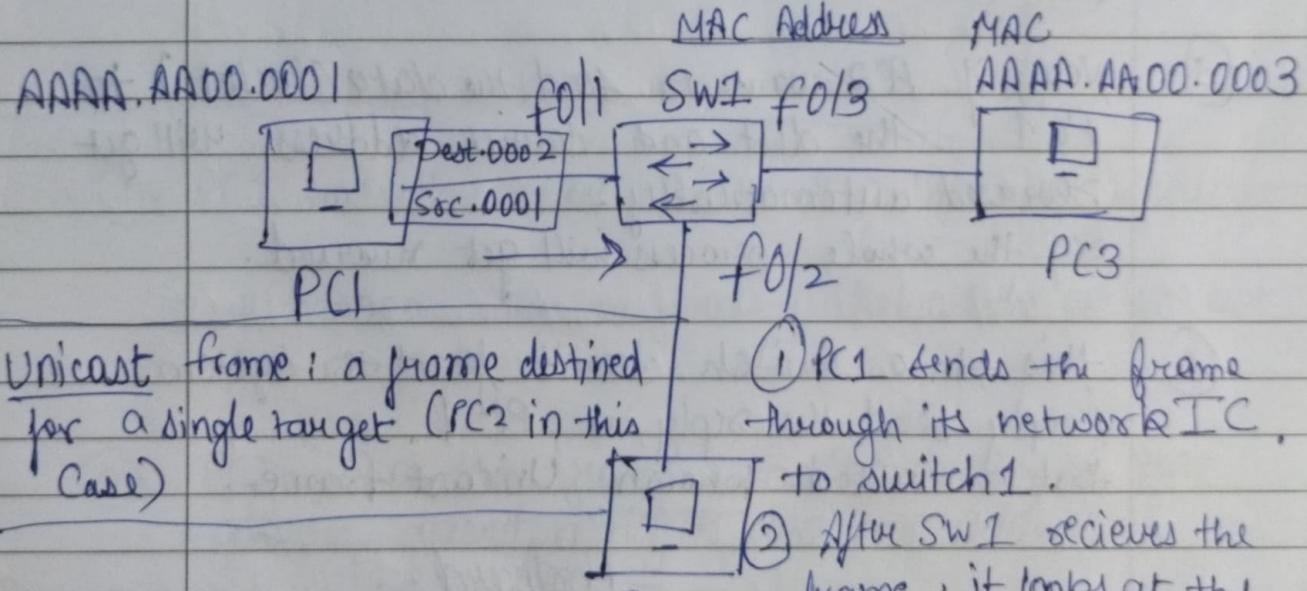


Hexadecimal

Uses 16 possible digits.

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, f
10 11 12 13 14 15

DEC	HEX	DEC	HEX
16	10	24	18
17	11	25	19
18	12	26	1A
19	13	27	1B
20	14	28	1C
21	16	29	1D
22	16	30	1E
23	17	31	1F



Unicast frame : a frame destined for a single target (PC2 in this Case)

① PC1 sends the frame through its network IC, to switch 1.

② After SW1 recieves the frame, it looks at the source mac address field of the frame - and use that information to learn where that PC1 is.

③ Now, SW1 doesn't know about where is the destination (.0002) is., so, it is called unknown unicast frame a frame for which SW1 doesn't have a ~~entry~~ in its MAC address table.

MAC Address table

MAC	Interface
.0001	f0/1
.0002	f0/2

Dynamically learned MAC address or Dynamic MAC address (bcoz switch learn about it itself).

(4) So, Now, only one option is left to flood the system. that means to send the data to all the interfaces except the source.

PC3 rejects the packet bcoz dest. macaddress doesn't match the given address.

PC2 accepts the packet and processes it normally up the OSI stack.

(5) Now, if PC2 wants to send the data (Packet) to PC1. the dest and source address will get reversed automatically.
So, the whole process will get reversed.

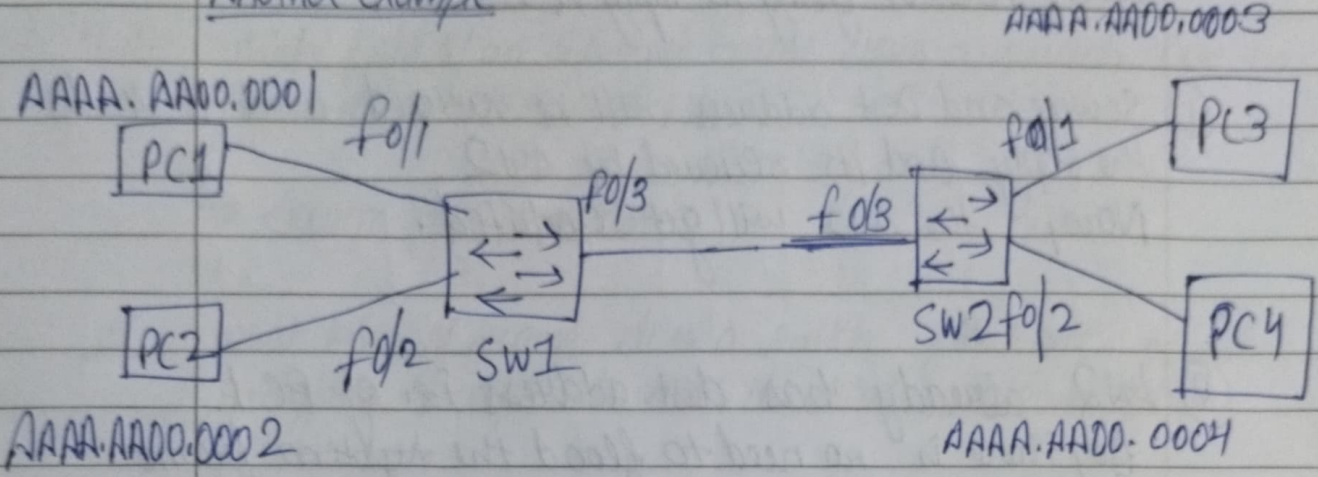
(6) this time Switch doesn't flood the system. simply send the reply to PC1.
that is called known Unicast frame.

= forward.

Note. ⇒ Dynamic MAC addresses are removed from the MAC address table after 5 minutes of inactivity.

__/__/__

Another example



SW1 MAC Address table

MAC	Interface
.0001	f0/1
.0003	f0/3

SW2 MAC address table

MAC	Interface
.0001	f0/3
.0003	f0/1

(1) PC1 sends the packet SW1, then Unknown Unicast frame = flood will happen. then it floods packet all the ports except source port.

(2) PC2 drops the frame bcoz the destination MAC address doesn't match its own mac address.

(3) Now, Packet is on SW2. SW2 did the same thing as SW1, It will floods the data further.

(4) PC3 recieves the frame as mac address is same as dest. mac address.

Now, PC3 is going to reply PC1.

① Source and Dest address will be reversed and it sends the reply and its recieved by SW2.
Now, the SW2 will get updated.

② SW2 already has dest. address i.e. of PC1.
So, there is no need to flood the ~~system~~ frame.
instead it is forwarded normally out the corresponding interface in the MAC address table f0/3.

③ the frame is recieved by SW1, which adds the entry for PC3's mac address in its table.

④ So, now SW1 mac address table has the dest. address in its interface, so, it sends the ~~packet~~ frame directly to PC1 mac address. and it reaches the destination. i.e. PC1.

Quiz

1. which field of an Ethernet frame provides reciever clock synchronization?

⇒ Preamble

2. How long is the physical address of a network device?

⇒ 48 bits.

3. What is the OUI of this MAC address? E8BA.70 11 or 2874

⇒ E8BA.70

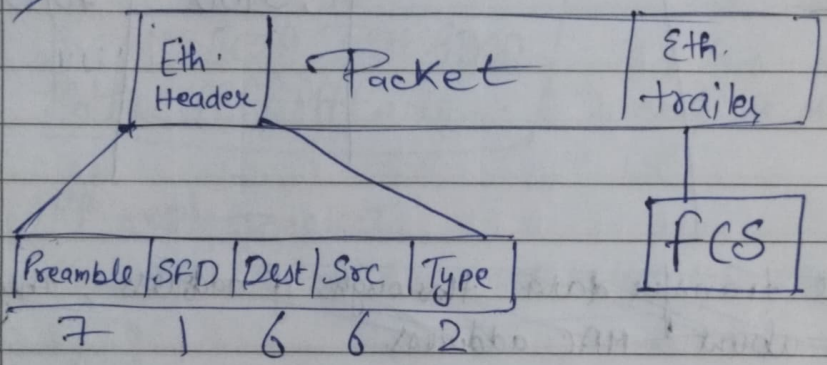
4.0. which field of an Ethernet frame does a switch use to populate its MAC address?

⇒ Source MAC address

5. what kind of frame does a switch flood out of all interfaces except the one it was recieved on?

⇒ Unknown unicast.

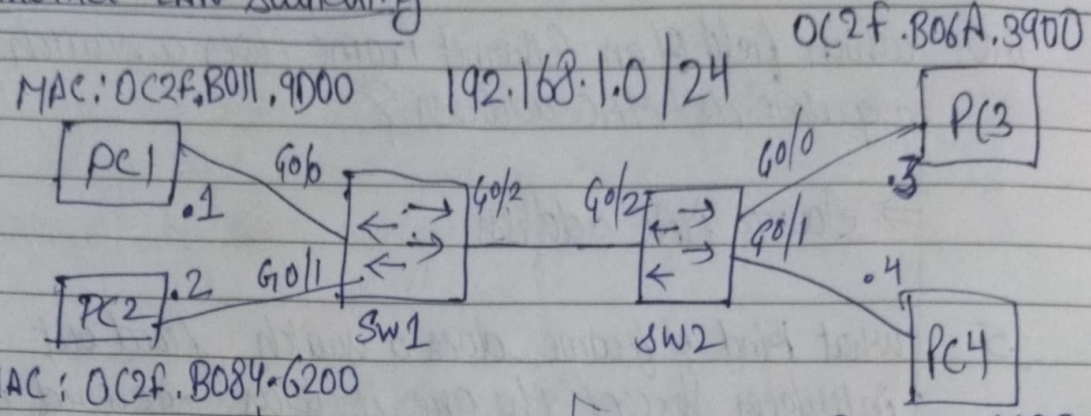
Extra ⇒



- The preamble + SfD is usually not considered part of the ethernet header.
- therefore the size of the Ethernet header + trailer is 18 bytes (6+6+2+4).

- the min. size for an Ethernet frame (Header + Payload [Packet] + trailer) is 64 bytes.
- so, 64 bytes − 18 bytes (header + trailer size) = 46 bytes
- therefore the minimum payload (packet size is 46 bytes.
- if packetsize is less than minimum size i.e. 46 bytes then padding bytes are added.
- ie. 34 byte packet + 12 byte padding = 46 bytes.

Ethernet LAN Switching



SW1 MAC address table

MAC	Interface
.9D00	Gi0/0
.3900	Gi0/2

SRC IP: 192.168.1.1
Dst IP: 192.168.1.3
Src MAC: .9D00
Dst MAC: ???

SW2 MAC address table

MAC	Interface
.9D00	Gi0/2
.3900	Gi0/0

- ~~Device transfer data through IP address, they don't know about MAC address.~~
- these switches are layer 2 devices, they don't operate at layer 3, so they need to use MAC address not ip addresses.

To find MAC address of PC3, ~~PC1~~ to connect PC1 to PC3, ~~to~~ to do so, it uses something called ARP. (Address resolution protocol)

ARP

- used to discover layer 2 address (i.e. MAC addresses) of a known layer 3 address (IP address)
- ~~Ex~~ Consist of two messages;

ARP request and reply

- ARP request is broadcast = sent to all hosts on the network. (the host that sent request)
- ARP reply is unicast = sent only to one host.

Actual frame

Src IP: 192.168.1.1
Dst IP: 192.168.1.3
Src MAC: .9D00
Dst MAC:

ARP request frame
(first frame that has sent into network by PC1)

ARP request
Src IP: 192.168.1.1
Dest. IP: 192.168.1.3
Src MAC: 0C2f.B011.9D00
Dst MAC: ffff.ffff.ffff

⇒ broadcast MAC address

ARP reply packet
(Now, the reply will sent back to the source)

ARP reply
SRC IP: 192.168.1.3
Dst. IP: 192.168.1.1
Src MAC: 0C2F.B06A.3900
Dst MAC: 0C2F.B011.9D00

← known unicast frame
= forward (not flood).

__/__/____

ARP table

Interface: 169.254.146.29 --- 0x9

Internet Address	physical Address	Type
169.254.255.255	ff-ff-ff-ff-ff-ff	Static
224.0.0.2	01-00-5e-00-00-02	static
224.0.0.22	01-00-5e-00-00-16	static
.251	01-00-5e-00-00-fb	static
.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-00-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

Interface: 192.168.0.167 ---0xd

Internet address	Physical Address	type
192.168.0.1	98-da-c4-dd-a8-e4	dynamic
192.168.0.255	ff-ff-ff-ff-ff-ff	Static
224.0.0.2	01-00-5e-00-00-02	
224.0.0.22	01-00-5e-00-00-16	
224.0.0.251	01-00-5e-00-00-fb	
224.0.0.252	01-00-5e-00-00-fc	
239.255.255.250	01-00-5e-7f-ff-fa	
255.255.255.255	ff-ff-ff-ff-ff-ff	

⇒ use arp-a to views the arp table, on any OS.

⇒ Internet address = IP address (Layer 3 address)

⇒ Physical Address = MAC address (Layer 2 address)

⇒ Type static = default entry

⇒ Type dynamic = Learned via ARP.