CCNA HANDBOOK

LEARN CCNA FROM BASIC TO ADVANCE

Network

- A group of two or more device that connect together to share information between each other.

Networking

- A process of using the connection between two devices purposefully to make that sharing of information possible.

Intranet

- Communication inside a organization , domain
- Private Communication

Internet

- Communication with world wide web

NETWORK BULLS WHERE CAREERS
infoogy

Type of Network

- On the basis of host role
- On the basis of geographical Area
- On the basis of participation

1) On the basis of host role:
    - Client →
        - That request for the services
        - Cannot provide services.
    - Server→
        - That provide the services
        - Cannot request for the services.

- Peer to peer →
    - Devices which can request and respond to or for a service at the same time.

Server& client	PEER to PEER
Client cannot know that what other client are connected to server	Every peer known that which other parts they are connected to
Data is centralized	Data is distributed
Since data is centralized client do not require other client to get any data download	Since data is distributed , peer require another peer to get a particular data download
Single point of failure	Any one peer file failure other data can still we can download

2) On the basis of geographical area
    - LAN- Local Area Network
        - **A computer network that links devices within a building or group of adjacent buildings, especially one with a radius of less than 1 km.**

    - WAN- Wide Area Network
        - A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs). The largest WAN in existence is the Internet.

    - MAN- Metropolitan Area Network
        - A **metropolitan area network** (MAN) is similar to a local **area network** (LAN) but spans an entire city or campus. MANs are

formed by connecting multiple LANs. Thus, MANs are larger than LANs but smaller than wide **area** networks (WAN).

- CAN- Campus Area Network
  - A **Campus Area Network** (CAN) is a computer **network** that links the buildings and consists of two or more local **area networks** (LANs) within the limited geographical **area**.

3) On the Basis Of Participation:

- Private network
  - ➢ Where data is shared only authorized Users.
  - ➢ Network which can be used by authorized Users.
- Public Network
  - ➢ Network which can be used by authorized as well as unauthorized user.
- VPN
  - ➢ Virtual private Network

➢ A logical network which is connected physical through ISP(Internet Service Provider).

➢ A private Network over Public Network

Type of Communication

i) Unicast
- One to one.

ii) Multicast
- one too many

- Only two intended group of people.

iii) Broadcast

- One to all
- Not only intended but also to unintended group of people.

Notes→the type of communication may differ on the basis of sender and receiver.

Modes of communication

i) Simplex

- One way Communication.

ii) Half Duplex

- Two way communication but one at a time.

iii) Full Duplex

- Two way communication but concurrently.
- Two way communication but simultaneously.
- Two way communication but at the same time.

Network components

A) <u>Physical Components.</u>

i) At least two network devices.

ii) NIC Card (Network Interface Card)

a) Wired

b) Wireless

iii) Transmission Media

a) Wired → cables

b) Wireless→Radio frequencies

B) Logical Components.

i) Protocols

a) Rules or Standard that defines how communication will or should take place.

ii) IP →Internet Protocols

1) Topologies

- Design of a network
  - How devices are connected

- Physical Topologies
  - How devices are physical Connected.

- Logical Topologies
  - How Data flows between Devices.

Bus, Ring, Star, Extended Star, Mesh, Mesh (Partial Mesh, Full Mesh)

Devices

1) Hub
2) Bridge
3) Switch
4) Router

a) HUB →

- It is a dumb devices
- Every PC can communicate with each other.
- It always works on Half Duplex.

➢ Dumb Devices

- It does not have any memory to decide where to send the packet

- Traffic Received on One port of a hub will be forwarded to another "active ports, accepts the port on which it was received.
- It two devices sends the traffic at the same time over a hub than the data will collide.

➢ Collision Domain

A segment on which two devices are connected with each other and send data at the same time which can collide with each other, then those devices are said to be in a single collision domain.

➢ CSMA/CD (Carrier Sense Multiple Access/Collision Detection)

- It Will Sense the carrier if any collision occurs.
- When Collision occurs, CSMA/CD activates then, it will send a jam signal to all devices to notify about the collision and instructing the devices to stop the transmission.
- CSMA/CD will let at the devices to transmit at random interval of time, so that collision should not occur again.

Solution →

- All segments in switch and router works in full duplex.
- Every Segment is separated by separated or isolated fibre on the motherboard.

CSMA/CD will work if the devices work in Half Duplex.

- Hub :-
  i) All Ports of a hub are in collision Domain
  ii) All these Four ports are in single Collision Domain

b) Switch :-

i) Multiport Bridge
ii) It has memory to store mac address and form mac table accordingly.
iii) It has multiple ports so that we can connect many devices 5,6,12,24,48..etc

iv) Ports by default works in full duplex
v) 1 segments = 2 circuits
vi) TX→Transmission
vii) RX →Receiving
viii) Switch forms collision domain on per ports basis
ix) Router also forms collision domain on per ports basis.
x) It is used to connect a single network.

c) <u>Router:-</u>

i) Internal structure is same on switch.
ii) It is used to connect to different LANs.
iii) Routers can be used in LANS but most-commonly used in WANs.
iv) It is used to connect two different Networks.
v) Works on the basis of IP address.
vi) No mac table is maintained
vii) Routing table maintained

NETWORK BULLS CAREERS FLY
nfoogy

➢ <u>Broadcast Domain</u>

- Group of devices that receives the same broadcast sent by on one devices
- All the devices are said to be in single broadcast domain
- Broadcast received on one port of a hub and switch will be sent to all other active ports accepts the port on which it was received.
- All ports of a hub and switch are in single broadcast domain.

Router → forms per port broadcast domain

→Broadcast received on one port of a router will never be forwarded on other ports of the same router.

d) **Repeater** – It work on first layer (physical layer) in OSI Model. It is used to connect devices together when signal of network is getting weak so with the help of repeater, we regenerate the signal.

e) **Firewall** – It is a Security Device, which is used to secure network. It works in Network Layer in OSI Model. A device give access to authorized user, with help of this device unauthorized user can not access in our network. Secure our inbound traffic.

- **Software →** Window, Antivirus.
- **Hardware →** vendor (Cisco, Juniper).

f) Access Point

- It is a wireless network device which is used to connect different devices like Computer, Laptop, Switch, etc. to make communication possible and Share data.

NETWORK BULLS WHERE CAREERS FLY infoogy

MAC ADDRESS

- 48 bits physical device/NIC address
- Is denoted by hexadecimal from
- 1 digit = 4bit
- 1 MAC ADD= 12 digit
- 12 digit = 12x4 = 48 bits
- Window →hyphen → aa-aa-aa-bb-bb-bb
- Cisco→dots → aaaa.aabb.bbbb
- Linux→colons→aa:aa:aa:bb:bb:bb
- First 24 bits = OUI (Organisational Unique Identifier)
  - To which organisation this first 24 bits is assigned
  - Assigned by IEEE
- Last 24 bits = Vendor specified (NIC card)
- 7th bit (2nd digit)
  - In mac add = U (Universal)/ L(Local)
  - 7th bit 0 = vendor assigned (unspoofed)
  - 7th bit 1=locally administered (Spoofed)
- 8th bit = I (Individual)/ G(Group)
- 8th bit 0= mac is individual (unicast)
- 8th bit 1 = mac in group (broadcast / multicast)

IANA→ APNIC (RIR) →ISP →Client

APNIC→ Asia Pacific Network Information Centre
Pronounced→A-P-NIC
IANA→Internet Assigned Number Authority
RIR→Regional Internet Registry

IP Address

- An IPv4 address is a 32 bit address use to uniquely identify each device on the network. A core function of IP is to provide logical addressing for hosts. IP Sec optional
- An IP address is most often represented in dotted decimal format.
    - Example: 156.89.24.15
- It is divided in 2 parts
    - Network Bits
        - These bits must be same in a LAN network.
        - We cannot change these bits.
    - Hosts bits
        - There bits can be change be different or unique in a LAN network.
        - We can change these bits.
- An IP address is comprised of four octets, separated by dot: First Octet. Second Octet. Third Octet. Fourth Octet ex. 158 .80 .164. 3 **IPv4 Addressing** each octet is an 8-bit number, resulting in a 32-bit IP address. The smallest possible value of an octet is 0, or 00000000 in binary. The largest possible value of an octet is 255, or 11111111 in binary.

The above IP address represented in binary would look as follows:

First Octet. Second Octet. Third Octet. Fourth Octet

10011110. 01010000. 10100100. 00000011

- A subnet mask is used to determine to which network a particular IP address belongs to.
- The IPv4 address space has been structured into five classes. The value of the first octet of an address determines the class of the network:
    - Example of a Class A address: 64.32.254.100 255.0.0.0
    - Example of a Class B address: 152.41.12.195 255.255.0.0
    - Example of a Class C address: 207.79.233.6 255.255.255.0

- Example of a Class D address: 224.0.0.10
- The IP address is 32 bits represent address so, 2 ^32 = 4.3 billion (Approx)

- IP address is divided in 5 classes:
  a) Class A = 0-127
  b) Class B = 128-191
  c) Class C= 192-223
  d) Class D= 224-239
  e) Class E= 240 – 255

A) Class A : The range of this class is 0- 127

- 0.0.0.0 is use for default routing and wildcard mask/DHCP
- The range is start from 0.0.0.1- 0.255.255.255
- 127 is use for NIC testing / TCP-IP testing. Range is 127.0.0.0 to 127.255.255.255
- Useable Octets = 1-126
- Private IPs for class A = 10.0.0.0 to 10.255.255.255/8
- Public IPs for class A = 1 – 9 and 11-126
- First 8 bits for network
- Last 24 bits for Host

B) Class B : The range of this class is 128- 191

- Reserved IPs are
  a) APIPA – Automatic Private IP Addressing are 169.254.0.0 to 169.254.255.255
  b) Private IPs – 172.16.0.0 to 172.31.255.255 /12
  c) First 16 bits for network
  d) Last 16 bits for Host

C) Class C : The range of this class is 192-223

- Private IPs- 192.168.0.0 to 192.168.255.255 /16
- First 24 bits for network

- Last 8 bits for Host

D) Class D: The range of class D is 224 -239. This is use for Multicast address.
E) Class E: The range of Class E is 240 - 255. This is use for Experimental and Research purposes

Private IP	Public IP
It is provided by Network Admin	It is provided by ISP(Internet services Provider)
It is locally unique IP and provide by network Admin	It is globally unique and used for WAN communication
Unregistered	Registered
Free of cost	Paid
Range → class A → 10.0.0.0 to 10.255.255.255 Class B →172.16.0.0 to 172.31.255.255 Class C → 192.168.0.0 to 192.168.255.255	Range →Those IP which are not private IP are terms as public IP.

- **Subnet mask**
  - It's also 32 bits dotted long decimal address.
  - It's also writing in 4 octets.
  - On bits in subnet is used to define network bits in IP address
  - Off bits in subnet is used to define hosts bits in IP address.
- Class A → 255.0.0.0 (N.H.H.H)
- Class B→ 255.255.0.0 (N.N.H.H)
- Class C → 255.255.255.0 (N.N.N.H)

- **Subnetting -** Dividing a large number of network into multiple sub-networks. To reduce more wastage of IPs.

- How to find Number of subnet?
  - No. of Network = 2^n (Number of extra on bits/Borrow bits)
- How to find Number of Host per subnet?

- No. of host = 2^n – 2 (Number of Off bits)
- Network Bits ID =
    - This is first IP address of network.
    - Turn off all host bits in IP address.
    - It is used to represent a network on a router on Globally
- Broadcast ID=
    - This is a last IP address of a network
    - It's used to send Broadcast to everyone in a LAN Network.
    - Turn on all host bits to calculate broadcast ID.
- Class Full
    - When we use default network and default subnet mask is called class full
- Class Less
    - When we use different network with Different subnet mask is called class less.
    - It is used to prevent wastage of ip address in class full
    - Here we can use any subnet mask with any class.

(Classless Inter-Domain Routing) CIDR

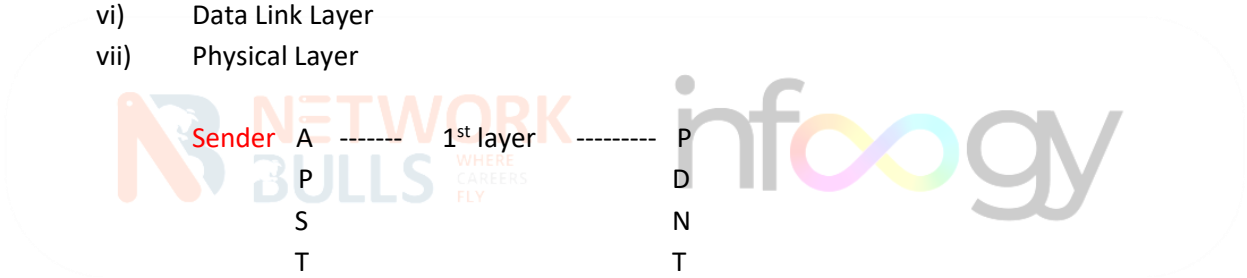
It is a method by which you can represent subnet mask. With the help of user to easily identify number of ON bits (1) and OFF bits (0). For example, a subnet mask of 255.255.248.0 would be represented as follows in binary:

11111111.11111111.11111000.00000000

The first /21 bits are ON bits and last /11 bits are OFF bits, so CIDR value of this network is 21.

OSI (Open System Interconnection)

1) It is invented by ISO(International Standard Organisation)
2) It is invented in 1984
3) Defines how communication will take place between devices from source to destination.
4) It provides common standard for developing all network devices.
5) It helps in different vendor device to interoperate with each other.
6) It helps in easy trouble shooting.
7) It helps any network Engineer to identify the problem of one layer without affecting other layer.
8) OSI is divided into seven Layers.
   i) Application Layer
   ii) Presentation Layer
   iii) Session Layer
   iv) Transport Layer
   v) Network Layer
   vi) Data Link Layer
   vii) Physical Layer



Sender	A	------- 1st layer ---------		P
	P			D
	S			N
	T			T
	N			S
	D			P
	P			A------ Last Layer Receiver

Logical Components --- Sender/Receiver.

1) Application Layer→

a) Interface→Communication with company.

b) Communication Resources check

Application layer gives an interface where we can communicate with our machines for the desire destination. Its acts an Interface between User and services. It checks the resource available for communication.

If the communication Resources are unavailable it informs us.

Services	Protocols
WEB	HTTP (80), HTTPS (443)
Remote	Telnet (23), SSH (22)
Mail	POP3 (110), IMAP (143)
File	FTP (20, 21), TFTP (69)
Domain	DNS (53), DHCP (67, 68)

2) Presentation Layer→ The Presentation layer gives us the encoded data from the source and we decoded this data at the destination. This algorithm use for encoding and decoding must be same at source as well as destination otherwise your data will not be properly Receive or Interoperated.

File Type	Format
Audio	MP3, WMA
Video	MP4,WMV,AVI
Picture	JPEG,BMP
Text	DOC,PDF

- Compression, Decompression, Encryption, Decryption

3) Session Layer →Session layer is used to create, maintain or terminate session between client and Server.

- Number of sessions depends upon Number of Ports
- Port Number→16 bits →2^16 = 65536 = 0 – 65535 per LAN
  - In a single LAN two User Cannot be assigned the same session Id for same destination but can be assigned for different destination.
  - Session layer is also responsible for Dialog Control
    - Mode of communication

- Simplex, Half Duplex, Full Duplex

4) Transport Layer→ to check end to end Connectivity.

There are some parameters that we use in Transport layer.

a) Segmentation→

1. Breaking up of big crunch of data into small-2 stream so that the transmission loses can be minimizing. How big the each segments will be it is depended upon the maximum segments size.(by default –1460)

b) Sequencing →

i) Numbering of the data at sender's end.

ii) At receiver's end these numbers will be used to rearrange the data into correct order.

iii) It is a kind of identification for rearrangement of data.

2^32=4.3 billion

c) Acknowledgements→

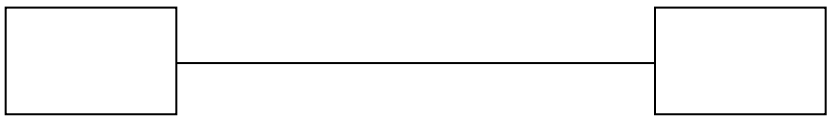
1. It is kind of receipts received by sender upon successful delivery of data.

NETWORK BULLS WHERE CAREERS FLY infoogy

d) Connection Orientation→

1. To provide reliable Connection between Source and Destination.

- TCP Provide 3-WAY HANDSHAKE PROCESS



1→Syn (Synchronisation) (0)

To ask for connection Parameters

2→SYN (10) + ACK (1)

- If connection parameters are acceptable by receiver then in Reply its sends the same connection parameters

- If connection parameters are not acceptable then in reply it will send its own connection parameters

3→ACK (11)

- Connection Oriented process is only maintain by tcp
- Transmission Control Protocols→belongs to transport layer
    1. TCP use protocols number 6
    1. In this SYN packet we try to matches some parameters
    2. MSS(MAXIMUM SEGMENT SIZE)
    3. Window SIZE
    4. Source Port=Random
    5. Destination Port=Predefine
    6. Selective Acknowledgement technique
    7. Congestion Technique

- MSS (Maximum Segment Size) → this is MSS which include the TCP information plus the data. When we start the Synchronisation Process we first negotiate the MSS between the Sender and Receiver lowest.

MSS = IPMTU- [TCP header + IP header]

=1500-[20+20] = 1460 bytes

- Buffer Size → Storage that is used to store the data before process

- Window Size→The empty size of buffer on a device is known as window size
    1. Window Size are two types
    a) Sending window
    b) Receiving Window

    We always negotiate the receiving window is lowest among the sender and receiver.

- Congestion Technique→

Sender----------xxxxxxx----------Receiver

Congestion technique in the TCP is negotiated using a flag explicit congestion ECHO this flag is negotiated at the time of 3-way handshaking Process. If we no negotiate this flag that we are not going use that Congestion technique.

- Selective Acknowledgement→ Is the process where if any segment is missing in the transmission we can ask for only that selective segments to be retransmitted not the all the data this technique is only available in TCP.
- Connection Less→
  →User datagram protocols (UDP)
  →UDP protocol number is 17
  →Unreliable connection
- No 3 – way handshake
- Infact, this protocols only cores to send the data but do not guarantee the delivery of data.
- It does not support acknowledgement
  - TCP is used in that process where reliability (data) is more important rather than speed.
  - UDP is used those process where speed is more important rather than reliability (Data).

- Port Assignment →

Ports = 16 bits = 0 – 65535
0 --- 1023 (Well known Ports)
1024 – 65535 (User Ports)

- Well known Ports → which are Pre- defined for any protocols
- User Ports →which can be used by any user randomly.

- Application ports number is pre--defined

HTTP	TCP	80
HTTPS	TCP	443
TELNET	TCP	23
SSH	TCP	22
POP	TCP	110
IMAP	TCP	143
SMTP	TCP	25
SNMP	TCP	161/162
DNS	TCP/UDP	53
DHCP	UDP	67,68
TFTP	UDP	69
FTP	TCP	20,21

- Flow Control→ Instead of losing the data, Client sends a not ready to the server in order to indicate that buffer memory is full and cannot receive any more data. After the processing of all received data, client sends a ready message now to indicate server that data transmission can be continued.
- Windowing →
  1) Before windowing, any segment sent must receive acknowledgement and the next segment will not be sent until the ack is received.
  2) If within 5 sec, ack is not received then the same segment will be sent again this process is known as Retransmission.
  3) This process makes any transmission very slow.

- Windowing→"How many segments can be sent at once against a single acknowledgement?"
  1. By default = 4128 bytes
  2. Ex- Window Size = 3

5) Network layer →
   a. It 3rd layer of OSI Model
   b. It is used to add ip address with Segment
   c. There are two types of address is added, source and destination address.
   d. It is layer is used to find best path from source to destination

- IP addressing →Subnetting
  →Summarization
- Path determination→ calculating the entire path between source and destination.
- Path selection→ calculating best path among the entire path available between source and destination.
- Routing protocols (OSPF , EIGRP , RIP , BGP)
- Routing protocols→ Protocols which carries routing protocols to determination and selection of best path from source to destination.

Encapsulation and Decapsulation

- Encapsulation → Adding some control information in each layer one by one.
- Decapsulation→ removing some control information in each layer one by one

6) Data link layer →
    a. This layer is used to add MAC address with packet
- LLC (link layer control)
    1. LLC is used to encapsulate the packet into the frame.
    2. This layer is used to identify layer 2 protocols
    3. STP,VTP,DTP
- MAC→ MAC is emended on NIC card, and NIC works in physical layer.
- Error detection
    1. Frame check Sequence
    2. To run CRC (Cyclic redundancy check).data + Header
- Error Correction and error detect support only in transport layer (data + Header)

7) Physical layer→
    a. Converting the frame into bits/binary and vice versa.
    b. Data convert digital to electrical and vice versa.
    c. It will make communicate b/w software and Hardware.

NETWORK BULLS WHERE CAREERS FLY infoogy

TCP/IP MODEL

- OSI MODEL
    1. ISO
    2. Layer 7
    3. Reference Model
    4. How communication will take place at each layer.

- TCP/IP MODEL
    1. DOD(Department of Defence)
    2. Layer 5
    3. Practical Model
    4. Defines what are the protocols that will be used to make this communication possible.

TCP/IP model has 5 layers:-

1) Application Layer
2) Transport layer/ Host to host layer
3) Network layer / Internet layer
4) Data link layer
5) Physical layer.

Protocols

- Application layer → HTTP , HTTPS, DNS , DHCP , TELNET , SSH , FTP , TFTP
- Transport layer→ TCP header / UDP header
- Internet layer → IP header , ICMP
- Data link layer→ ethernet header , ARP header , MAC address ,CDP

NETWORK BULLS WHERE CAREERS FLY infoogy

HTTP (Hyper text transfer protocols)

- To exchange web pages b/w client and server
- Encapsulate in TCP with port number 80.
- It is not encrypted or secure
- All data is sent in clear text form

HTTPS (HTTP secure)

- Encapsulate in TCP with port number 443
- All data is encrypted
- Encryption is done for HTTPS will be done by presentation layer in OSI model.
- To secure the data, the circuit through which data is transmitted is done by SSL (Secure socket layer.)

FTP(FILE TRANSFER PROTOCOLS)

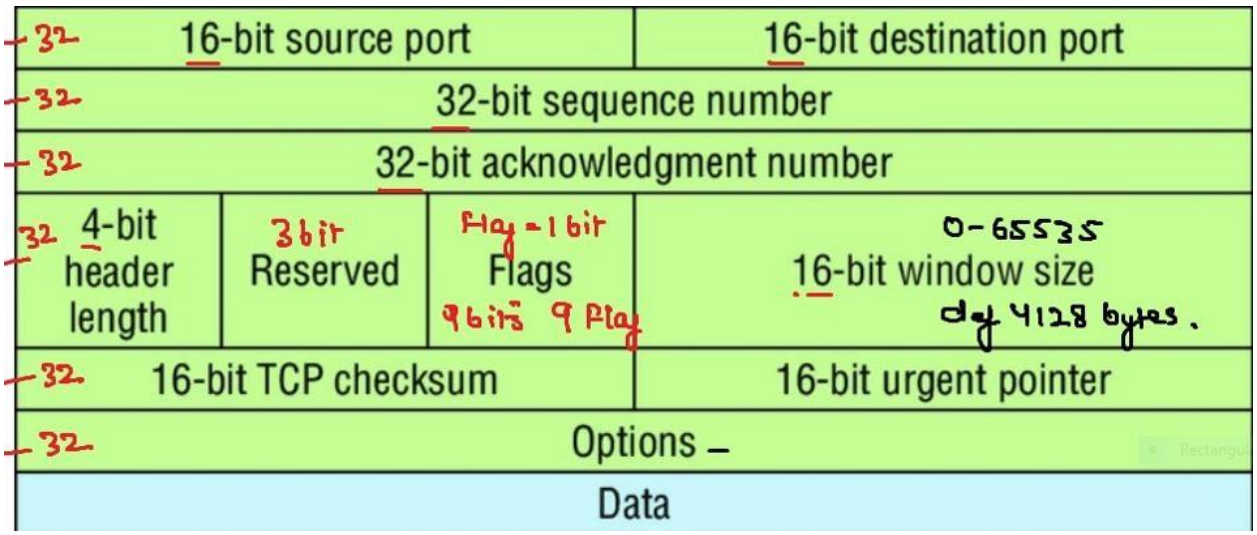
- It is used to transfer data b/w client and server.
- Encapsulates in TCP port number 20,21
- Data is unsecured. (secured version of FTP is SFTP (SECURE FTP)
- We can browse through files and folders.
- It can give ability to download but not to enter or view.
- IF the size is less than 512 bytes then it use port number 20
- Support authentication
- If the size is more than 512 bytes than it use port number 21.

TFTP(Trivial FTP)

- You cannot browse through files + folders, Infact you have to type exact file name to get the data download.
- Encapsulate in UDP port number 69
- No authentication
- Data is unsecured and cannot be secured in any way
- In order to secure any file, it is recommended to assign a typical file name.

NETWORK BULLS WHERE CAREERS FLY
infoogy

Tcp header



1) Options fields carry parameters of 3-ways handshake.
2) After 3-way handshake --- Actual data is sent

SYN – It is used to exchange these parameters, so for SYN, your tcp header will be of 24 bytes.

- Rest of all TCP Packets are of 20 bytes--- 5 fields = 5 *4 = 20 bytes.

SYN ------→ 24 bytes

24 bytes ←-------- SYN + Ack

Ack -----→ 20 bytes

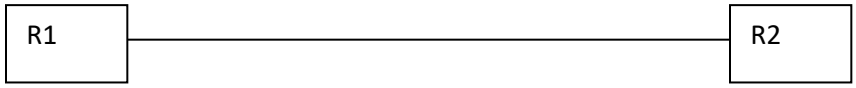
Actual data ←-----→

1) Source Port → Source field is a 16 bit filed. It is identifies the port of the sending Application ports. Port Number from services request sent.

2) Destination port → Destination Port is a 16 bit filed. It is identified the port of the receiving application. Port number which is used to identify service requested by user.

3) Sequence Number→ It is not only used to rearrange the data in correct order but also carry the size of data inside the segments. It is also used for retransmission if any segment is lost.

"Seq num is a 32 bit field"



10.0.0.1 10.0.0.2

←-------- SYN Seq = 0(MSS = 1460, WIN= 4128, LEN=0)

SYN (Seq=0) +ACK (Seq=1) (MSS = 1460, WIN= 4128, LEN=0) ---------→

←---------ACK (Seq =1) (MSS = 1460, WIN= 4128, LEN=0)

NETWORK BULLS WHERE CAREERS FLY infoogy

←----------Telnet data = 12 bytes (LEN)

Last Seq=1

Next Seq num= 12+1 = 13

ACK = (Seq) 1

Telnet data = 12 bytes (LEN) ----------→

Last Seq =1

Next Seq= 13

Ack = 13 (data + last seq number)

←----------Telnet data = 3 bytes (LEN)

Last seq = 13

Next Seq num = 13+3 = 16

Ack= 13 (Last data received by R1)

←----------Telnet data = 3 bytes (LEN)

Last seq = 16

Next Seq num = 16+3 = 19

Ack= 13 (Last data received by R1)

Telnet data = 42 bytes (LEN) ----------→

Last Seq =13

Next Seq= 42+13 = 55

Ack = 20 (data + last seq number)

4) Acknowledgement Number →
   a) Acknowledgement num is 32 bit field.
   b) It tells the sender to send the next data with this sequence number.
   c) It is always sequence number of the last received data bytes increment by 1.

5) Header length → SIZE OF HEADER
   Bit= 4* [value]
   1) Header length is a 4 bit field.
   2) It contains the length of tcp header.
   3) It helps in knowing from where the actual data begins.

Minimum & Maximum header length

- The length of TCP header always lies in the Range [20 bytes, 60 bytes]
- The initials 5th rows of the tcp header are always used.
- So, minimum length of tcp header= 5*4 = 20 bytes.
- The Size of the 6th row representing the options field.
- So, minimum length of tcp header = 6*4=24 bytes
- The size of options fields can go up to 40 bytes.
- So, maximum length of tcp header = 20 bytes+ 40 bytes= 60 bytes

Concepts of scaling factor

- Header Length is a 4bit field
- So, the range of decimal value that can be represent in [5 , 15]
- But, the range of header length is [20,60]
- So, to represent the header length, we use a scaling factor of 4 In general

Header length = Header length field value x 4

a) If header length field contains decimal value 5 (represent as 0101), then
Header length = 5x4 = 20 bytes

NOTES→ it is important to note.

a) Header length and header length field value are two different things.
b) The range of header length field value is always [5,15]
c) The range of header length is always [20,60]

6) Reserved Bits

a) The 3 bits are reserved.
b) These bits are not used.

7) Flags →

a) Urgent [URG bit] →
   i) If bit is 1→ data will not wait into buffer and will get proceed immediately.
   ii) If bit is 0→ data is not urgent

b) ACK bit→
   i) If bit is 1→the packet is an acknowledgement packet.
   ii) If bit is 0→the packet is not acknowledge packet.

c) Push→to make the data stream speedily.
   i) 1→to speed up the data stream.
   ii) 0→not need to speed up data stream.

Notes:

i) Unlike URG bit, PSH bit does not prioritize the data.

ii) It just causes all the segments in the buffer to be pushed immediately to the receiving application.

iii) The same order is maintained in which the segments arrived.

iv) It is not good to set PUSH bit=1

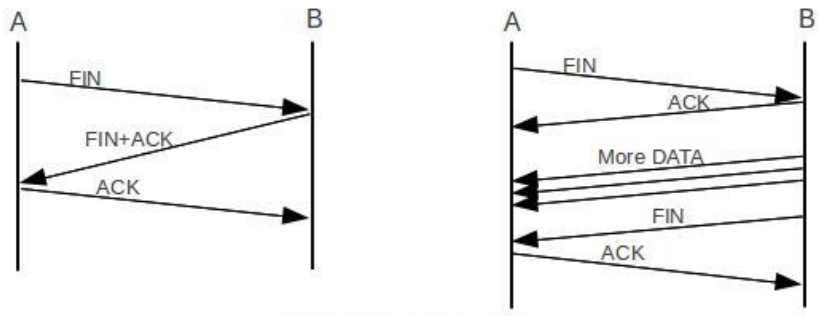
v) This is bcoz it disrupts the working of receiving CPU and forces it to take an action immediately.

d) RST Bit→

- RST bit is used to reset the TCP Connection
- When RST bit is set to 1.
- It is indicate session has been expired.
- When Destination port for which service is required is not available.
- For both these cases flag will be 1(set)
- Otherwise flag will be ZERO

e) FIN BIT→ FIN bit is used to terminate the TCP Connection

- Session has been logout



Two TCP close scenarios

f) SYN→ Segment in which you want to share connection parameters

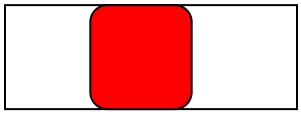
8) Option →MSS (max segment Size)

- MSS= MTU – tcp header-IP header

  1500-20 bytes-20 bytes

  1460 bytes

9) Urgent Pointer→urgent flag = 1



46:10 46 from where urgent data is start

10 size of urgent data (bytes)

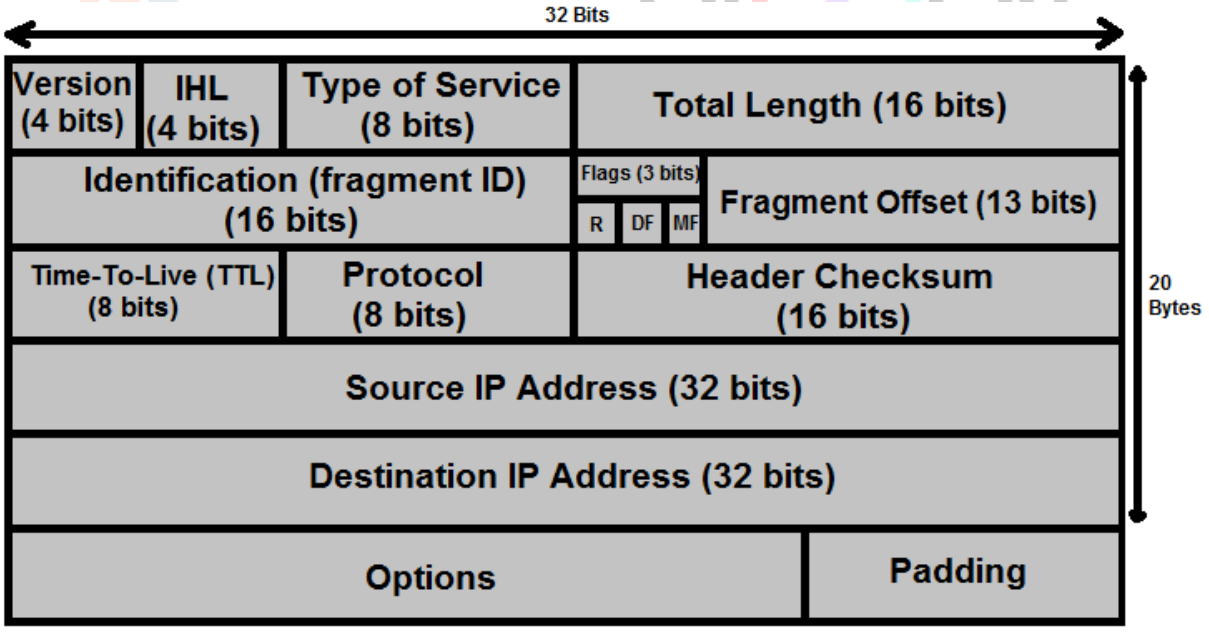
- When URG flag is set (1). It indicate that URGENT data has to send immediately to wire from sender side and on receiving and the urgent data has to be sent immediately to application.

- Urgent Pointer in TCP segment is used to indicate that amount of urgent data present in TCP segment.

10) Checksum → Represent in HEXADECIMAL FORM.

- Header Checksum
- Both will be verified (Data + Header)
- One algorithm will run on the Header, and will come with a checksum value in hex format when their again verified by receiver.
- The receiver will again run algorithm on the header received.
- IF value of the receiver and sender matches then the data will be accepted otherwise will be dropped.

IP header



1) Version – Only for IPV4 Address family →IPV4 and IPv6
2) Header Length →

- Minimum- 20 bytes
- Maximum – 60 bytes

3) Type of services→for prioritising the traffic. It is replaced by DSCP (Differentiated Services Code Point) with additional features.
    a. Range (0-7) = 0 Least IMP
4) Total length → Data(segment) + header Length
5) Fragmentation→dividing large data into smaller part called fragmentation
    - Data can be generated from two layers of OSI MODEL.
    - Application layer
    - Network layer

- What is the difference between segmentation and fragmentation?
    - Segmentation can be done for the data generated from APP. Layer
    - Fragmentation can be done for the data generated from Network layer

6) IDENTIFICATION → This field is used to differentiate fragments of one data from another data.
    16 bits field = hex from
    1 digit hex = 4 bits Total = 4 digit
    - Fragment of single data will have same identification number.
7) Flags→3 bit
    - 1 bit = Reserved
    - DF →Don't fragment
    - If bit is 0 →fragmentations can be done.
    - IF bit is 1→ fragmentation cannot be done.
    - MF→More fragment
    - IF bit is 1→still more fragment to receive
    - IF bit is 0→this is still last fragmentation received.

8) Fragmentation offset →is used to reassemble the data into correct order.
    - Packet = 5000 byte (includes IP header)
    - Actual data = 4980 bytes
    - IP header = 20 bytes
    - Payload= 1st fragmentation = 1480 +20 = 0-1479 = 0
        2nd fragmentation = 1480 +20 = 1480 – 2959 = 1480
        3rd fragmentation = 1480 + 20 = 2960 – 4439 = 2960
        4th fragmentation = 540 +20 = 4440 – 4979 = 4440

    Total Length = Data (Payload) + IP Header

	Data + header	Data + header	Data + header	Data + header
Total Length	1480+20	1480+20	1480+20	540+20
Identification	0x0001	0x0001	0x0001	0x0001
Frag. OFF.	0	1480	2960	4440

➔ IP is a connectionless Protocols
➔ No re-transmission
➔ No ack.

9) TTL(Time to live)→ 8 bits = 2^8 = 256 = 0-255
- How far or how many routers/broadcast domains a packet can cross from source to destination.
- TTL value is assigned by n/w layer.
- Whenever a packet crosses a broadcast domain from one interface of a router to another interface of same router then TTL will be decrement by 1 (one)
- How many routers we can assign a single line.
- It is used to identify how many routers are there b/w source & destination.
- Tracing
- Cisco—255
- Window—128
- Linux → 64

NETWORK BULLS WHERE CAREERS FLY infoogy

10) Protocols (8 bits) = Protocols num = 2 ^ 8 = 256 = 0 -255
- Which upper and n/w layer protocols are encapsulated in IP header
- Protocols number →
  - TCP=6
  - GRE=47
  - UDP=17
  - EIGRP =88
  - OSPF =89
  - ICMP=1

1) What is the different between protocols number & port number?

A) Port number →
   a. Are assigned at transport layer for the data generated from application layer.

B) Protocols Number→
   a. It is used to identify data received from transport layer and assigned for the data generated from network layer itself.

ICMP (Internet Control Messaging Protocols)

- It is used to verify connectivity b/w source and destination.
- Utilities / Tools
- Ping → Packet Internet Groper
- Trace route → tracing the path between Source and destination.
- Message → 1) Query →Echo Request →(Type code 8)
    - Echo Reply (Type code 0)

2) Error →Destination Unreachable →type 3

→Request time out →types 11

→Since R1 does not know the route to reach Network of 20

→R1 will generate a new ICMP Message notifying PC1 that the destination is unreachable.

→User→Window → 5 sec timeout

→Cisco →2 sec timeout

Window →by def = 4 packet

Cisco → by def = 5 packet

→Window → by def = 32 bytes of data

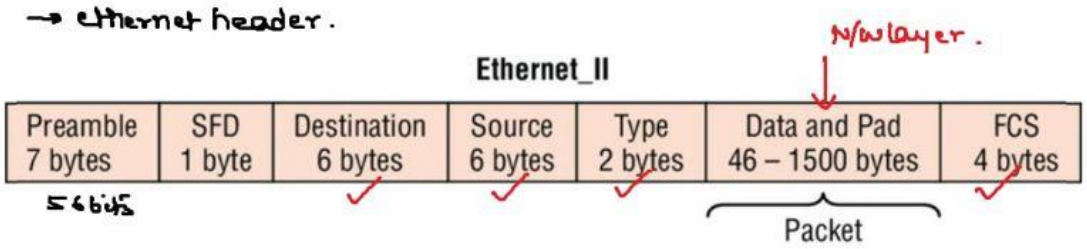
→Cisco →by def → 100 bytes of data

→Cisco → ! → Success

U→Unreachable

. →RTO

Ethernet Header



1) Preamble →
   - FLP (Fast link Pulses)
     - Ethernet frame starts with 7-Bytes Preamble. This is a pattern of alternative 0's and 1's which indicates starting of the frame and allows sender and receiver to establish bit synchronization. Initially, PRE (Preamble) was introduced to allow for the loss of a few bits due to signal delays. But today's high-speed Ethernet don't need Preamble to protect the frame bits.
     - PRE (Preamble) indicates the receivers that frame is coming and allow the receiver to lock onto the data stream before the actual frame begins.

2) SFD (Start frame delimiter)
   - The last two bits will be set as 11 to notify the adjacent devices that to stop sending FLPs and Start receiving data. This is a 1-Byte field which is always set to 10101011. SFD indicates that upcoming bits are starting of the frame, which is the destination address. Sometimes SFD is considered the part of PRE, this is the reason Preamble is described as 8 Bytes in many places. The SFD warns station or stations that this is the last chance for synchronization.

→ These fields are never attached with any data.

3) Destination MAC→this is 6-Byte field which contains the MAC address of machine for which data is destined.

4) Source MAC→
   - This is a 6-Byte field which contains the MAC address of source machine. As Source Address is always an individual address (Unicast), the least significant bit of first byte is always 0.

5) Type→
   a. To identify Upper and data link layer protocols.
   i) IPV4 → 0X0800
   ii) IPV6 → 0X86DD
   iii) ARP →0X0806
   iv) Dot 1.q → 0X8100
6) FCS(Frame Check Sequence)
   - ALGO
     - Data link layer =CRC (Cyclic Redundancy Check)
   - Like checksum which not only verify header but data inside the headers.
   - This layer is used to perform error detection.
   - Whatever the value is calculated by CRC will be copied into FCS.

7) Data and Padding (46 min to max 1500)
   a. MTU does not include eth header Size
   - Ethernet header = 18 bytes.
   - Frame = data (packet) from network layer + eth header.
   - Min frame size = 64 bytes
   - Max frame size = 1522 bytes
   - Frame < 64 bytes –> RUNTS
   - Frame>1522 → GIANTS

NETWORK BULLS WHERE CAREERS FLY infoogy

Wire/cables

1) Serial Cable →
   - This is used to connect Router.
   - It is also known as point to point Cable.
   - Speed is 1.544 Mbps.

2) Co-axial Cable →
   - It is used for T.V communication
   - In 1970's it is used for computer communication.
   - Made by Copper
   - Single core

3) Ethernet Cable →This is used for LAN communication

- There are two types of Ethernet Cable

a) STP → Shielded Twisted Pair → Protect with multiple layer
b) UTP → Unshielded Twisted Pair → Only one layer
c) There is total 4 pair → means there are 8 wires in Ethernet.
d) Solid → Green , Blue, Orange, Brown
e) Mixed→White Green , White Blue , White Orange , White Brown

4) Crossover cable → blue colour

- To attach / connect similar devices.
    a. Router --- Router
    b. Switch---Switch
    c. PC-----PC
    d. Router---PC

5) Straight through cable (Yellow cable)→To attach/connect dissimilar devices.

- Router----Switch
- Switch-----Router
- Pc----Switch

GW	Green white
G	Green
O	Orange
OW	Orange White
B	Blue
BW	Blue White
Br	Brown
Br w	Brown White

- IEEE provide some standard

T568A	T568B
Gw	OW
G	O
OW	GW
B	B
BW	BW
O	G
BRW	BRW
BR	BR

Straight cable→

T568A	T568A
Gw	GW
G	G
OW	OW
B	B
BW	BW
O	O
BRW	BRW
BR	BR

T568B	T568B
OW	OW
O	O
GW	GW
B	B
BW	BW
G	G
BRW	BRW
BR	BR

Cross cable:-

T568A	T568B
GW	OW
G	O
OW	GW
B	B
BW	BW
O	G
BRW	BRW
BR	BR

T568B	T568A
OW	GW
O	G
GW	OW
B	B
BW	BW
G	O
BRW	BRW
BR	BR

Router/PC	Switch
1 Tx	1 Rx
2 Tx	2 Rx
3 Rx	3 Tx
6 Rx	6 Tx

NETWORK BULLS WHERE CAREERS FLY
infoogy

Router/PC (T568A)	Switch (T568A)
1 Tx GW	1 Rx GW
2 Tx G	2 Rx G
3 Rx OW	3 Tx OW
6 Rx O	6 Tx O

Router /PC (T568A)	Switch (T568B)
1 Tx GW	1 Tx OW
2 Tx G	2 Tx O
3 Rx OW	3 Rx GW
6 Rx O	6 Rx G

Switch (T568B)	Router /PC (T568A)
1 Tx OW	1 Tx GW
2 Tx O	2 Tx G
3 Rx GW	3 Rx OW
6 Rx G	6 Rx O

6) Auto mdx: - This Feature is used on latest devices interface that help to change sending and receiving pins according to cable.
7) Fiber Optical Cable: - Form of light
    a) Single mode Fiber: - In which data will travel in single Beam of Light. Mostly used in Wan
    - Distance 1-40 km
    - Speed 1-2 gig
    b) Multi mode Fiber: - In which multiple beams of light can travel.
    - Distance – 1-2 km
    - Speed – 1-10 gig
8) SFP: - modules →Ethernet , Fiber
9) Console Cable = this is used to take CLI of device or for Physical Access.

Hardware on Devices

1) ROM (Read Only Memory)
    - This is defined Boot Sequence of a devices.
2) RAM(Random Access Memory)
    - All configuration or task of devices is working in RAM
    - All running Configuration is available in RAM
3) NVRAM(Non-Volatile RAM)
    - Saved configuration is available in NVRAM that is known as Start-up configuration.
4) Flash= that is kind of hard drive. That is used to store IOS (Internetwork Operating System) of device. IOS version – 12.x, 15.x.

Bootstrap Process

1) POST(Power on Self Test) :- IN which devices will check all hardware component (RAM, CPU, Interface Slot)
2) IOS :- flash → Boot IOS
3) NVRAM: - Check Startup Configuration → then Copy in Running Configuration.
4) RAM :- Running Configuration

Access Device

1) Physical Access: - Console Access

2) Remote Access: - Telnet, SSH

1) CLI: - Command line Interface: - In which all configure is done through Command Prompt.
2) GUI: - Graphical User Interface: - In which all configurations is done by GUI.

Router Ports

a) Console port → This is used to access CLI (command Line Interface) of the devices
b) Ethernet → distance → 80 m

- ethernet = 10 mbps(e) (Mbps →mega bits per second)
- fastethernet =100 mbps(Fe)
- Gigabit ethernet= 1000mbps(Ge)
- 10 gig. = 10,000mbps

Bits = 0 or 1	1 bytes (B) = 8 bits
Kilobits = 1024 bits	kilobytes = 1024 bytes
Megabits = 1024 kb	Megabytes= 1024 kilobytes (KB)
Gigabits = 1024 Mb	Gigabytes= 1024 Megabytes (MB)
Terabits = 1024 Gb	Terabytes=1024 Gigabytes (GB)

Ports no. (Interfaces)

1. Line card number → always start from 1
2. Slot number → always start from 0
3. Port number → router start with 0 , Switch start with 1
4. Ex fa1/1/2 ---- line/slot/Port num
5. Routers does not have line number
6. Switch may or may not have line number.

Mode of Router/ Switch

1) Router> User mode/Exec mode = this mode is used to check output of devices or for show command but we can't check full configuration of device.
2) Router# Enable mode / Privilege mode = In this mode we can check all show commands.
3) Router(config)# Global Configuration Mode = This mode is used to configure everything on device,

1) Status → whether Physical port is Up or down
→Up → Port is enabled/ no shut
→Adm. Down → Port is disabled / shut

2) Protocols →Physical connectivity
→Down → devices are not physically connected with other devices
→UP →Devices are connected

Telnet

1. Teletype Network
2. For remote access of other devices
3. That device of which you want to telnet must be enabled with telnet services.
4. Encapsulation in TCP with port number 23
5. Line vty 0 4
6. Line → how many users can access a server at the same time.
7. Vty →virtual terminal
8. All the data that is transmitted through telnet is in clear text form.
9. Router(config)#line vty 0 4

SSH (Secure Shell)

➔ Almost function on telnet.
➔ All data is encrypted.
➔ Encapsulated in TCP with port number 22

- Step for SSH Commands
- Line vty 0 4
- Login Local
- Username/Password
- Domain name
- Hostname any other than router
- Crypto key generate.

NETWORK BULLS WHERE CAREERS FLY
infoogy

Router

- Routing protocols→ Protocols which carries routing protocols to determination and selection of best path from source to destination.
- Routing table → this table is used to share route information.
- R1#show ip route (by the help of this command you will check routing table)

- C- Connected route
- S- Static route
- *S-Default Route
- R-RIP
- D- Eigrp
- O- OSPF
- B- BGP

Connected Routes→

- A valid IP should be available on Interface.
- Interface status and protocols should be UP
- do show ip route (to check routing table)

1) We have two ways to configure path on router
    - Static Routing
    - Dynamic Routing

Static Routing

- Route which needs to be assigned manually/statically
- Exit Interface
    - Ip route <Destination Prefix ><destination subnet mask><exit interface>
    - ip route < 30.0.0.0>< 255.0.0.0>< fastethernet 0/1>
- Next Hop
- Exit interface + Next hop
    - When route is assigned through exit interface
        - Problem →Proxy ARP
        - Solution → no recursive Lookup
    - When Route is assigned through next hop
        - Solution →no proxy ARP
        - Problem → recursive Lookup
- Recursive Lookup
    - Repetition of routing table lookup for a single destination.
- Proxy Arp
    - An ARP reply is given on behalf of other devices.
- Serial Link →
    - Does not Support ARP
    - Serial Link Does not have mac address
    - Static route can be assigned through exit interface if that interface is serial → so that will no problem of proxy ARP.

Route Preference criteria

- Purpose → Redundancy (Backup)
  - Primary path
  - Secondary Path
- When there are multiple paths for a single destination, so router should prefer any one path to reach that destination.
- Highest Prefix length (CIDR)
  - Higher the prefix , less the number of host IPs
  - Less the number of host IPs, lesser the cup utilization.
  - When multiple routes are assigned on a single router, both the routers will be installed in routing table.
- Lowest administrative Distance (AD)→ 8 bit (0-255)
  - When prefix (CIDR) is length is same.
  - Measure of trustworthiness.
  - Lower the AD value, the higher the trust/Preference.
  - Connected = 0 (always)
  - Static = 1 (always)
  - RIP= 120
  - EIGRP=90 , 170
  - OSPF=110
  - BGP=20,200
  - 255= route will be considered as invalid.
  - Router having lower AD value will only get into routing table.
- Lowest metric
  - If AD value is also same then
  - Connected and static route does not have metric = always (0)
  - It is useful in dynamic
  - RIP →Hop count
  - EIGRP→Composite metric weights
  - OSPF →Cost
- When all criteria are same then routers will perform “Load Balancing”
- Both the routes will be installed in routing table.
- Packets will be distributed among both the routes equally and alternating.

Floating Static routing

- Where you can manipulated the path from source to destination on the basis of
  - Highest prefix length
  - Lower AD value

DHCP (Dynamic Host Configuration Protocols)

- Automatic IP assignment on host devices
- Time consumption is less.
- Administrative overhead will be less.
- Productivity will increase.
- Human error will decrease.
- Encapsulate in UDP
- Port Number 67 – Server , 68 – Client
- Multiple parameters can be assigned along with IP address
  - Subnet Mask
  - Default Gateway
  - DNS
    1. Primary DNS
    2. Secondary DNS
  - Lease - Duration Of IP assigned to a user

DHCP works through a process called DORA (Discover Offer Request Acknowledgement)

a. Discover – whenever you enable DHCP on a client it start to find out any DHCP sever available.
b. Offer- DHCP server will offer an IP to the client. IP is assigned from a pool.
c. Requesting – Requesting for the IP offered by the Server.
d. ACK- When a client receives the ack, the client will assign the IP on the system.

- DHCPSERVER(config)#ip dhcp pool abs
- DHCPSERVER(dhcp-config)#network 10.0.0.0 255.0.0.0
- DHCPSERVER(dhcp-config)#default-router 10.0.0.1

- DHCPSERVER(dhcp-config)#exit
- DHCPSERVER(config)R2(config-if)#ip address dhcp
- DHCPSERVER(config)ip dhcp excluded-address 10.0.0.3 10.0.0.5

Default Gateway –

1- A L3 interface through which any LAN user can Communicates outside the LAN.
2- The IP assigned on to the interface connected to the LAN will be your default gateway IP.

Relay agent –

- It is used when the DHCP Server is in remote location. Since the DORA messages are broadcasted, they cannot cross their domain. So, we need an agent who could relay the messages between the server and the DHCP Client. Basically it converts broadcast packet into unicast and then relay to the dhcp server with relay agent information.

- R3(config-if)#ip helper-address 10.0.0.1

NETWORK BULLS WHERE CAREERS FLY
infoogy

DHCP Snooping

- Rogue DHCP Server
- Man in the middle Attack
- IP DHCP SNOOPING
- IP DHCP SNOOPING VLAN 1
- Show ip DHCP SNOOPING
  - Trusted→ received OFFER / ACK
  - Untrusted → not received offer / ack-- deny
- By default all port are untrusted
- DHCP SNOOPING BINDING TABLE

IP address	MAC	Lease	Int
10.0.0.1	OA	24	1
10.0.0.2	OB	24	2
10.0.0.3	OC	24	3

- Ip dhcp pool cisco
- Network 10.1.1.0 255.255.255.0
- Default-router 10.1.1.1
- IP dhcp snooping
- IP dhcp Snooping vlan 1,10,20
- Switch(config)#int e0/2
- Switch(config-if)#ip dhcp snooping trust
- Switch(config)#no ip dhcp snooping information option(to disable option 82)
- Switch(config)#do Sh ip dhcp snooping binding
- DHCP_SERVER#debug ip dhcp server events

DAI (Dynamic Arp Inspection)

- DOS (Denial of Services) ATTACK
- Per second 1000 ICMP msg
    - CPU Utilization high
- When you enable DAI your port will become untrusted
- Those Port who are untrusted that port will not resolve ARP they DROP ARP
- Only resolve ARP for those who have entry in DHCP BINDING TABLE
- Those ports that are connected with router that port you have to manually make trusted.

- Switch(config)#ip arp inspection vlan 1
- Switch(config)#int e0/2
- Switch(config-if)#ip arp inspection trust

Dynamic Routing

- Routing in which routes are maintained and calculate automatically.
- Routers automatically exchange the routes b/w each other.

- Some packets are there for each protocol which is advertised by routing protocols to get the routes from their neighbouring routers→ Directly Connected Routers.
- Dynamic Routing
    - IGP(Interior Gateway Protocols)
    - EGP(Exterior Gateway Protocols)
- IGP→Routing Protocols that share routes among same autonomous system.
    - Ex→ RIP , EIGRP , OSPF
- EGP→Routing Protocols that share routes between different autonomous systems.
    - BGP
- Autonomous System Numbers(IANA)
    - Group of router or network in single administration is called AS number
    - It is identify by decimal number
    - 16 bit (0-65535) 0 & 65535
    - 1-64511(public AS)
    - 64512-65534(Private AS)
- IGP(Interior Gateway Protocols)
    - RIP(Routing Information Protocols)
    - EIGRP(Enhanced Interior Gateway Protocols)
    - OSPF(Open Shortest Path First)

NETWORK BULLS WHERE CAREERS FLY
infoogy

OSPF (Open Shortest Path First)

- Link State Routing Protocols (LSRP)
- Link →how many links are their between Routers.
- State → How many routers are connected with each link
- In ospf, routes are not advertised Infact complete database in the form of link state advertisements(LSA) are advertised among the complete topology
- Routers calculate their best path themselves.
- OSPF metric = cost = Reference bandwidth /link bandwidth
- Reference Bandwidth (100 mbps)→default
- OPSF create a map of complete topology on the basis of “AREAS”
- Area ID = 32 bit = 0- 4.3 billion
- Backbone area (area id =0)

- Non backbone area (1-4.3 billion)/Normal Area
- Routers identify with in area
    - Backbone Routers
    - Non backbone Routers/Normal routers
    - ABR(area Border Routers)
    - ASBR(Autonomous System Boundary Routers)
- Backbone Routers→ Router have All interface in AREA 0
- Non backbone → Router have All interface in non backbone area
- Complete database is exchanged between routers within area only.
- Area Border routers(ABR)
    - This connected to different area together.
    - A router will be ABR only when at least one interface of that is connected to A0
    - ABR will automatically exchanged best routes of one area into another area without redistribution
    - ABR's will have the complete database of each area they are connected to.
    - OSPF work in hierarchical structure(tree)
        - Root
        - Stems/Branches
    - A0 should be centralized located between all non backbone areas
    - There should not be more than one area 0 in ospf domain.
- Algorithm = SPF(Shortest path first)
- AD=110
- Metric = Cost
- ASBR(Autonomous System Boundary Router)
    - At least one interface should be in ospf
- Neighbour ship
    - Area Id should be same
    - Subnet and subnet mask should same
    - Hello & dead timers should be same
    - Router id should be unique within area
    - Authentication should match

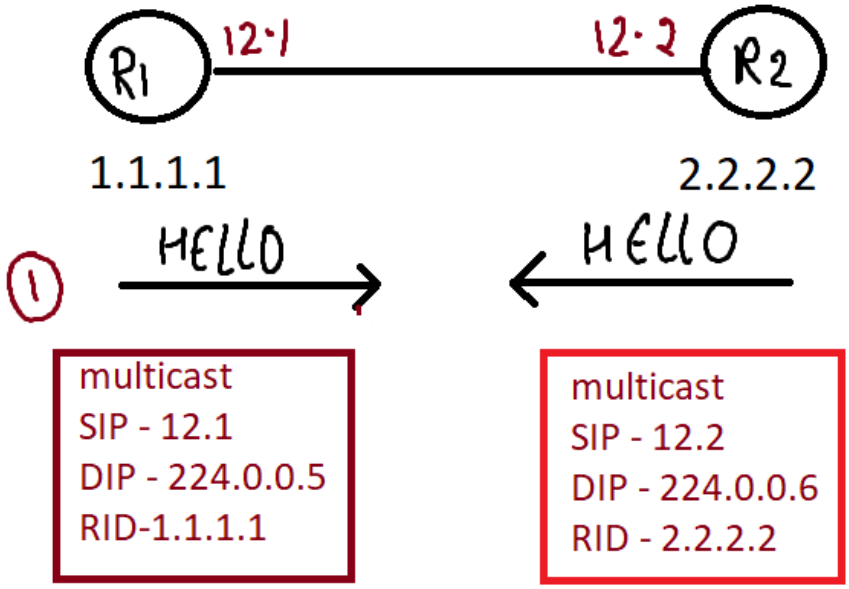
- Process ID → Locally significant (1-65535)
    - You can have same or different process ids on different routers.
    - Never advertises into updates.
- Router-id →to differentiate between routers within an area
    - Should be unique within area of all routers
    - Must not be unique among routers of different areas.

- Election of RID
  - Manual
  - Highest loopback IP
  - Highest physical int ip no matter that int is enabled with ospf or not
- Hello = 10 sec
- Hold = 40 sec
- OSPF tables
  - Neighbour table
  - Routing table
  - Database table
- OSPF message / packets
  - Hello
  - DBD(data base description)
  - LSR (Link state Request)
  - LSU (Link state Update)
  - LSACK(Link state ACK)

NETWORK BULLS WHERE CAREERS FLY
infoogy

OSPF state

- Down
  - No hello will be sent or received
- Init
  - Hello is sent but not received in return
  - Active neighbour ship



ACTIVE NEIGHBOUR FIELD

NETWORK BULLS WHERE CAREERS FLY infoogy

- 2-way
  - hello is sent and received
- Exstart
  - Null DBD is exchanged between to verify bidirectional connectivity for updates.
  - Master/Slaves (Election)
    - Highest RID
  - To decide who will start sending the database first
  - Once the election will be completed they will move to " exchange" state
  - Seq number
  - MTU size negotiate
- Exchange
  - Asking about each other's database.
  - LSA header send from master
  - Then slave will send LSA header in response
  - But will not have network information in that DBD.
- Loading

- Master will send LSR to ask detail information about LSA Header.
- Slave will send LSU
- Master will send LSACK
- When the database is completely synchronised they will move to full state and will said to form “adjacency”
- Neighbour ship / adjacency -> 40 sec (wait timer)

2 –Way State

- Network type
  - BMA (Broadcast Multi Access)
  - P2P (Point to point)

- Number of Neighbour ship = n (n-1)/2 n= Number of router

- To reduce the number of adjacencies, router will elect DR & BDR between the router
- DR(Designated Router)
- BDR(Backup Designated Router)
- Election Criteria
  - HIGHEST Priority (def=1) = 0 -255
  - Highest RID

- One broadcast domain can have only one DR and one BDR
  - Every DRother will form adjacency with DR and BDR both.
  - DR and BDR will form adjacency with each other.
  - DRother will never form adjacency with DRother.
- 224.0.0.5 → Whenever DR send any update all will received from this multicast add. Every router of ospf can accept that.
- 224.0.0.6→Only DR and BDR can accept the update.
- Clear IP OSPF PROCESS (Y) → Simultaneously with in msec
  - DR (only two router in one BMA) currently
  - DR/BDR (when more than two router in BMA)
  - No election takes place of DR and BDR on P2p Segment.

LSA 1(Router LSA) → with in Area

- Generated by each router with in an area.
- LSID →RID of router generated the LSA
- Adv. Router→RID of Router generated the LSA
  - Number of router LSA = Number of router in an area
  - Link count = Broadcast (BMA)= 1 segment = 1 link count
  - P2P = 1 Segment = 2 link count
  - Per loopback = 1 link count

LSA2 (NETWORK LSA) → with in area

- Generated by DR
- LSID =DR physical interface IP
- Adv. Router= DR RID
- Number of DR within AREA = number of broadcast multi Access segment
- Number of network LSA = Number of DR

LSA3 (Summary LSA) → to advertise best routes of one area into another area.

- Generated by ABR
- LSID= network ID of router
- ADV. Router= ABR RID
- Number of summary LSA= number of routes of another area.

LSA 5 (AS-External LSA)

- Generated by ASBR when external AS other than ospf are redistributed into OSPF.
- Number of LSA 5 = Number of external routers adv into ospf
- LSID = network id of external routes
- Adv router= ASBR RID
- RID of ASBR does not change throughout ospf domain in LSA 5

LSA 4 (Summary – ASBR LSA)

- Generated by ABR
- To let other router to know how to reach ASBR
- LSID = ASBR RID
- ADV. RID = ABR RID
- Number of LSA 4 = Number of ASBR in OSPF Domain
- LSA 4 exists in those areas where router LSA of ASBR does not exist.

Switch

- It is a layer 2 device which forwards the traffic on the basis of mac address.
  - MAC address
  - ARP Packet flow
    - Switch Function

1. Address learning
2. Forwarding
3. Filtering
4. Loop Avoidance

1. <u>Address learning :-</u>
   - Whenever a switch receives any frame, it learns the mac add from source mac address field in ethernet header.
   - Mac address will be learned and stores in a table called Mac-address table.

2. <u>Forwarding:-</u>
   - A switch forwards a frame on the basis of destination mac in ethernet header.
   - Source mac address – Will always be unicast
   - Destination mac address →

- Unicast →
  - When destination mac is unicast then switch will check its mac table and whatever the port that mac address is learned on, the frame will only be forwarded in the port.
- Multicast→
  - Routing / protocols
- Broadcast →
  - when destination mac is broadcast then switch will copy the frame according to the number of active ports and then frame will be forwarded to those ports
- Switch will never forward the frames on the port on which it was received.

- Any end devices keep the Arp entry in its table for 4 hrs
- Switch stores mac entry in mac add tables for 300 sec/ 5 min – Idle time out

Aging time out → 0 -300 sec

- Unknown unicast flooding
  - When the frame is sent as unicast and the destination mac is no more present in mac table then switch will copy the frame and sent it to all active ports except the port on which it was received.

Ques: - Difference between broadcasting and flooding?

- Broadcasting →
  - When the frame is intensely sent as broadcast
- Flooding→
  - When the frame is unintensely sent as broadcast but unicast.

3) Filtering →on the basis of VLANS (virtual LANs)

- Since a switch has only one broadcast domain for all ports.
- Vlans are used to divide broadcast domains logically on a switch
- Vlans = 12 bits = 4096 = 0-- 4095
  - 0 & 4095 (Reserved)
- Standard vlan = 1 – 1005
- Extended Vlan = 1006 – 4094
- One vlan = one broadcast domain
- By default, all ports of a switch are in vlan 1
- Vlan 1 cannot be deleting or modified.

1. Standard range → vlan 1 default
   a. 1002 →FDDI
   b. 1003→token ring
   c. 1004 →FDDI-net
   d. 1005→token ring – net cannot be deleted or modified. (Older technology which are no more in use).

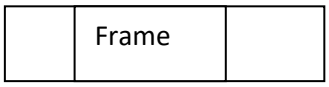
Useable vlan /User vlan →1 – 1001

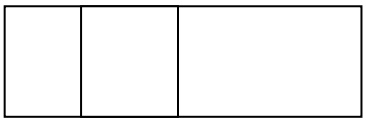
- Broadcast frame received by a switch on a particular port of a particular vlan will be forwarded to all other ports of same vlan only.
  - ❖ Switch ports
    - Access port →
      - Port which can be members of one vlan at a time.
      - Ports which should be connected to end devices/Routers
    - Trunk Ports→
      - Ports which can be members of all vlan at a time
      - Ports which should be connected to other switch / routers
  - ❖ Tag can be done or removed on trunks ports only
  - ❖ Access ports does not support tag

- Ingress –
  - From where switch can receive traffic is known as ingress interface.
- Egress
  - From where switch can send traffic is known as egress interface.
- Switch maintain mac table in CAM table.

Frame tagging

ISL (Inter Switch Link)	**802.1q**
Cisco proprietary	**Open Standard**
External Tagging	**Internal tagging**
Tag is attached outside the frame	**Tag is inserted into the frame**





30 bytes → ISL frame

max frame size= 1522

-18 bytes (ethernet header)
– 4 bytes (dot 1q header) =
1500 (MTU)

→26 bytes →Header

➔ 4 bytes → trailer
➔ 1522 (max size of ethernet header)

1522- 18 bytes – 30 bytes = 1474 bytes (MTU)

ISL is no more in USE

- Cisco l2 switch does not have support
- Cisco L3 switch does not have support

Native Vlan

- Native Vlan use to send traffic without tag
- Dot 1 q support native vlan
- ISL does not support native vlan
    - CDP is used to carry NV Vlan information; if NV is mismatched then it will only give you a log but will not block the traffic.
    - STP (BPDU) also carries NV information; if NV is mismatched then it will block the traffic completely.

Trunk port:-

- Static trunk →
    - Manually configure a port as trunk
    - Define encapsulation method
    - Make Port Trunk
    - #Switchport trunk Encapsulation Dot1Q
    - switch mode trunk
- Dynamic trunk

DTP (Dynamic Trunking Protocols)

- Cisco Proprietary
- Layer 2 protocols
- Hello timer = 30 sec
- Negotiation Protocols → negotiation for trunk

➔ Modes

- Dynamic Auto (default)

        - It will wait for Negotiate never start negotiation.
        - 3750 , 3850,above (Latest Switch)
    - Dynamic Desirable
        - This mode negotiate to form trunk port
        - 2950 , 3550, 3560 (Old Switch)

Auto ---- Auto (no trunk)

Auto --- desirable (trunk DTP dynamic MSG)

Desirable ---- Desirable (Trunk Dynamic)

Auto ---- manually trunk (trunk manually)

Desirable ---- manually trunk (trunk)

#switch Mode Access → Disable DTP on host access port

Switchport nonegotiate → Disable DTP on trunk port

➔ Access port →

- Dynamic access → port which are by default access but can from trunk if DTP negotiation received from adjacent switch.
- Static access → port which will always remain access no matter DTP negotiation is received or not.

CDP (Cisco Discovery Protocols)

- It is a layer 2 device
    - Will encapsulate in Ethernet Header.
- Cisco Proprietary Protocols
    - Can only run on cisco devices.
- By default
- To identify Physical topology
- To convert physical topology into logical topology
- Cdp Packet → these packets are advertised through each and every link between the devices.
- SMAC→
    - int Mac add
- DMAC →
    - Multicast add →0100.0ccc.cccc

- Cisco ID → 0100.0C → 24 bits
- CDP , DTP ,VTP,UDLD,PAGP →CC.CCCC – LAST 24 bits

➔ Timers →

- hello → 60 sec
- Hold → 180 sec

➔ show cdp entry *

STP (Spanning Tree Protocols)

- By default
- Layer 2 protocols
- IEEE Standard is 802.1d
- Loop avoidance
- multicast Address of BPDU is 0180.c200.0000

→STP Terminology

- Root Bridge
- Non Root Bridge
- BPDU
- Root Port
- Designated Port
- Cost
- Alternate Port/Blocking Port

➢ STP Performs three Major Election

- Root Bridge
- Root Port
- Designated Port

1) Root Bridge
   - Can only be one per topology
   - Criteria →
     - Lowest Bridge ID

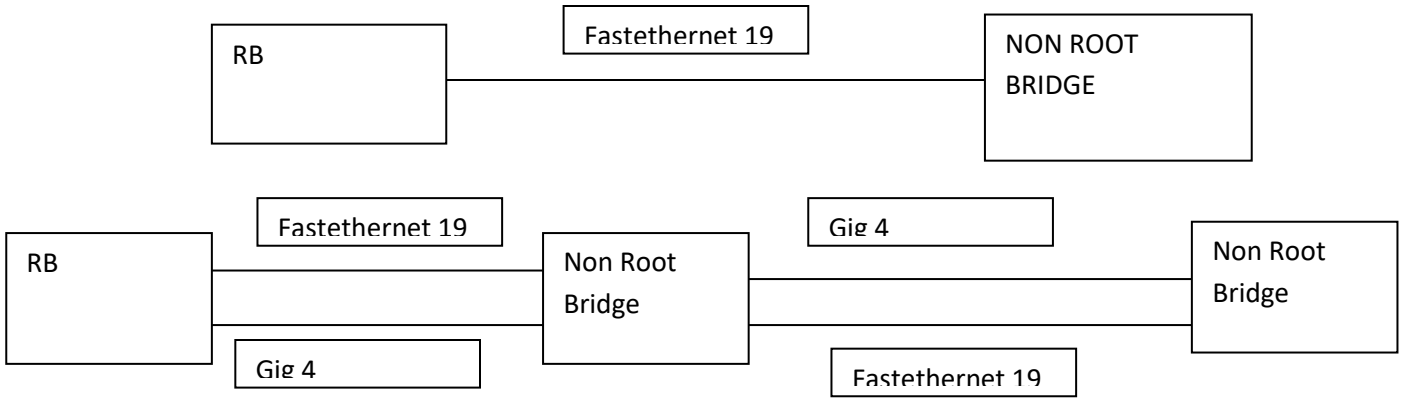
- 1)lowest Priority (0- 65535) default 32768
- 2)Lowest base Mac add
- Only RB can send BPDU
- BPDU will be sent through each & every port
- Any switch which connect to know that its priority or base mac add is higher will stop sending BPDU and not understand itself as RB. (Non-Root Bridge)

2) Root Port

- Root port is elected on Non-Root Bridge only.
- Root port is shortest path towards RB.
- Every Non-Root Bridge can have only one RP
- RP is only receive BPDU but cannot send BPDU.

Criteria:-

1. Lowest cost toward Root Bridge
   - Ethernet → 10 Mbps →100
   - Fastethernet → 100 mbps →19
   - 1gig →1000mbps → 4
   - 10 gig →10,000→2



→RB always sends the cost as 0.

3) Lowest Sender Bridge ID –
   - Root Bridge ID—Root Bridge
   - Sender Bridge ID --- Sending / forwarding BPDU
4) Lowest Sender port ID→
   - Port priority (def 128) = 0-255
   - Port number
5) Lowest Receiver Port ID→

3) Designated Port

- The port which is used to sent out the BPDU's
- Can be RB & Non –RB
- All Ports of RB are DP always
- Non-RB will elect the DP so that they can relay the BPDU's of RB to downstream Switches or to the switches which not directly connected to RB

1) Lowest Advertised Cost
- Every link (collision domain) between switches will have only one DP

2) Lowest advertised sender Bridge ID
3) Lowest advertised Sender Port ID

4) Blocked Port

- Ports which are not elected on RP & DP will be blocked port
- Blocked Port
  - Alternate blocking (redundant to RP)
  - Backup blocking (Redundant to DP)

STP States

a) Disable →When Port is Down

b) Blocking →To Prevent Loop
    - BPDU received only not send
    - Never Learn User MAC Address
    - NO User Data Forwarding
c) Listening→
    - BPDU send And Received Both
    - Election is Done in this State
    - 15 sec (by default) equal forward delay timer
    - NO User Data Forwarding
    - Never Learn User MAC Address
d) Learning→
    - BPDU send and Received Both
    - Learn user mac address
    - No user data forwarding
    - 15 sec (by default)
e) Forwarding →
    - BPDU received and Send Both
    - Learn user mac address
    - User data forwarding

BPDU (Bridge Protocols Data Unit)

- Root Bridge always generate a Hello msg after 2 sec that msg is known as BPDU
- It is used to Elect Root Bridge
- Configuration→is used for election
- TCN (Topology change Notification) →is used to notify any topology change b/w the switches so that re-election can take place.

Configuration

- Show Spanning Tre

CST (Common Spanning Tree)

- IEEE (open standard)
- Layer 2 protocols
- BPDU untagged
- Only one spanning tree topology.
- Only one Root Bridge for all VLANS.
- Only one spanning tree instance (logical Topology)
- To reduced the switch CPU load during STP calculations.
- It was open standard
- SM → Int MAC Address
- DM → 0180.c200.0000
- If active links never goes down this links will be considered as wastage of resource.

NETWORK BULLS WHERE CAREERS FLY
infoogy

PVST (Per VLAN Spanning Tree)

- Cisco Proprietary
- Per vlan Spanning tree Instance
- Instance are equal to number of Vlans
- 10 Vlans = 10 instance
- Number of vlan = Number of instance.
- Number of RB= No. of switches in topology
- Priority + System extended Id(vlan number)
- 32768 +1 = 32769
- It support only ISL
- SMAC→ Int MAC address
- DMAC →0100.0CCC.CCCD
- We can have multiple loop free topologies

        - Multiple Root Bridge in a single topology
        - Can be done on the basis of per vlan RB
    - Advantage
    - Load balancing
    - No wastage of resources
    - BPDU are being distributed b/w switches
- Disadvantage
    - CPU utilization high

Bridge ID → 8 bytes (priority {2 bytes} + {6 bytes} MAC address)

Bits
1 System extended ID
2
4
8
16
32
64
128
256
512
1024
2048
4096
8192
16384
32768

Value will always be in multiple of 4096

- 0*4096
- 1*4096

- 2*4096

Change Priority

- Manually →(All Vlans, Per-vlan , Range of vlan)
- Primary & Secondary

#spanning-tree vlan 1-4094 root primary
#spanning-tree vlan 10 priority 0

PVST+

- Support both ISL and DOT1q

RSTP (Rapid spanning tree protocols) → CST algorithm (open standard)

RPVST+ (Rapid PVST+) → PVST + (no forward delay timer)

Timer =

  - hello 2 sec
  - Max age = 6 sec
- State =
  - Discard (disable , blocking , Listing)
  - Learning
  - Forwarding

BPDU Guard

- Only for access port
- Port fast must be enabled
- Portfast ports continue sends + receive BPDU's
- If BPDU guard is enabled , then it will stop receiving any BPDU (either inferior/Superior)
- If BPDU is still received then switch will put the port into error disabled mode.

- Error- disable mode →shut down state
- Error-disable state cannot be recover automatically
- Recovery →
    - shut / no shut(manually recovery)
    - error disable recovery (dynamic)
    - by default disable
    - Switch(config-if)#spanning-tree guard root
    - Switch(config-if)#spanning-tree bpduguard enable
- How to recover any port from error disable
    - Sw1(config-if)#error disable recovery cause all
    - Sw1(config-if)#error disable recovery interval 60
    -

Port fast → solution (insignificant topology change)

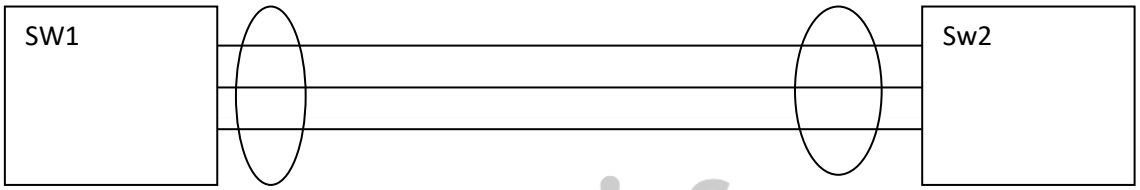
- Port fast only work on access port
- Port fast access port will become edge port " connected toward end devices"
- Port fast enabled access ports will not let switch to generate TCN BPDU
- Port fast enabled access port will move directly to forwarding state once protocols comes up
    - No listing and learning state
- But port role will remain DP
- If DTP is enabled received (DTP MSG) on portfast → port will become trunk→ portfast property will also removed
- Switch port mode access
- Configuration → per port and global
- spanning-tree portfast default
- -if)#spanning-tree portfast

STP

- Loop Free Topology
- Redundancy
- Cannot provide load balancing of balancing of physical links.

Ether channel

- It is a layer 2 technology which is used to bundle multiple physical links into logical link
- Not only provide redundancy but load balancing of physical links as well
- Load balancing for a single vlan



Port channel: - Bundle of multiple Physical links.

Group number: - To identify or differentiate multiple channels on same or different switches.

Adjacent channels can have same or different group number.

- One switch cannot have two port channels with same group number.
- When multiple physical links are bundled together, STP considers them as a single logical links.

Requirements:-

- Speed same (10 mbps , 100 mbps)
- Duplex same (half duplex , Full Duplex)

- Port type (Access , trunk)
- Access- same vlan
- Trunk – encapsulation same , all allowed vlan
- Native vlan same

How to configure Ether channel

1) Static :- on mode
2) Dynamic :- Protocols
    a. PAGP(Port Aggregation Protocols)
        i. Cisco Protocols
        ii. DMAC – 0100.0CCC.CCCC
        iii. Max ether channel 64
        iv. Per ether channel = Max 8 links can be bundled
        v. Mode
            1. Desirable (negotiate)
            2. Auto (wait)
                - Auto --- Auto (no etherchannel)
                - Auto ---Desirable (etherchannel)
                - Desirable ---Desirable(etherchannel)
    b. LACP(Link Aggregation control Protocols)
        - Open standard
        - Max etherchannel = 128
        - Per etherchannel = max 16 links can be bundled
        - Modes
            - Active (like desirable)
            - Passive (Like auto)
                - Passive --- Passive (no eth)
                - Active ---Passive(Formed)
                - Active---Active(Formed)
            - 16 links bundling
                - 8 link → Active
                - 8 link → Standby

Load balancing

- 9 algorithm
- SRC MAC
- DST MAC
- SRC DST MAC
- SRC IP
- DST IP
- SRC DST IP
- SRC PORT
- DST PORT
- SRC DST PORT

Configuration:-

Show etherchannel Summary

#channel- group 2 mode on

Show etherchannel

#sh etherchannel load-balance

#Port-channel load-balance DST –mac

Port Security

Switch Port Security

- To avoid unauthorized access

- To limit the number of mac address to be learned on a single port.
- Which mac address should be learned on that port
- Port security be only on access ports
- When enabled → max limit of mac add (1 default)
- During unauthorized access port security will take some action and that's called " violation"

1) Violation →
   a. Shutdown (Default)
      i. When any unauthorized takes place, then port will move into error disable state.
      ii. Also provide a log of mac address created the violation
      iii. After violation, authorized users will also not able to communicate.
   b. Protect
      i. It will only block the traffic of unauthorized users.
      ii. But the traffic of authorized user will continue to transmit
      iii. It will not give the log of unauthorized access
      iv. It will not show any violation.
   c. Restrict→
      i. Same as protect
      ii. Log msg to SNMP Server

#Switchport port-security

#Switchport port-security maximum

#Switchport port-security mac-address

#Switchport port-security violation shutdown

#show port-security interface fa0/1

#Show port-security

#show port-security address

FHRP (First Hop Redundancy Protocols)

- This Technology is used when we have multiple gateways Router for LAN network.
- On the perspective of clients
- To provide redundancies for the gateways.
- Variants →
- HSRP (Hot standby Router Protocols)
- VRRP (Virtual Router Redundancy Protocols)
- GLBP (Gateway Load Balancing Protocols)

HSRP (Hot standby Router Protocols)

- It's is cisco Proprietary Protocols.
- Layer 7 Protocols use port number 1985 and UDP base Protocols
- Layer 3 multicast address 224.0.0.2 (version 1) , 224.0.0.102 (Version 2)
- Timer = hello 3 sec , Hold 10 sec
- Total Group 256 = 0-255
- Max 16 routers
- Active (primary gateway) , standby (secondary gateway), Listen
- Election Criteria for Active Router

    - Highest Priority → default (100) , (0-255)
    - Highest Physical Interface IP
- Virtual IP (100.0.0.10)
- Group Number → Is used to differentiate multiple gateways on the basis of VLANS in a single LAN Network.

- Packets
    - Hello
        - VIP
        - Group num
        - Priority
        - Hello
        - Hold
- Transport layer
    - UDP Port number 1985
    - SP 1985
    - DP 1985
- IP Header
    - SIP→Int IP
    - DIP →224.0.0.2
- Ethernet Header
    - SM→Int Mac
    - DM→Multicast
- Active router is responsible to give ARP reply to client
    - SM→OA (VM)
    - TM→PC1
    - SIP →10.100
    - TIP→10.10
- Ethernet Header
    - SM→OA(VM)
    - DM→PC1
- Virtual MAC →0000.0c07.acXX

- Once virtual mac is elected:
    - Arp reply will be given by active router using VM in ARP Header as well as ethernet header in source mac field
    - Hello sent by active router will be using virtual mac
    - Hello sent by stand by router will be physical mac
    - Now if active goes down
    - Hello → 3 sec
    - Hold → 10 sec
- When active goes down, then standby will hold for 10 sec and if still no hello is received then standby will become active and starts to send hello using virtual mac.
- If old active comes up again then new active will remain active and old active will become stand by.
- Preemption :-
    - Only works on the basis of priority.
    - Is used to reforce the election between the routers when old active come up again
    - By default disabled
    - Preemption delay = 0 sec (default) in how much time role will be shifted from new active to old active).
    - Standby 100 preempt delay minimum 30
- Do show stand brief
- Do show stand

ACL (Access Control List)

- Acl is used to filter traffic , it can filter layer 3 , layer 4 , layer 7
- Clauses
    1. Deny → Traffic is not allowed
    2. Permit→ Allow the traffic
- ACL two types
    1. Standard ACL
        - Number
            - Range (1-99)
            - We can only define source
            - It can configure next/near to destination network
        - Name
    2. Extended ACL
        - Number
            - (100-199)
            - Next to source
            - We can define Source , Destination , Protocols , Port number
        - Named
- Ingress→ Incoming
- Egress → Outgoing

➢ Step 1 → Create ACL, Match traffic and define action.

➢ Notes

1. If ACL is applied on incoming ports then acl will be checked first then routing table.
2. If ACL is applied on outgoing ports then routing table will be checked first then ACL.

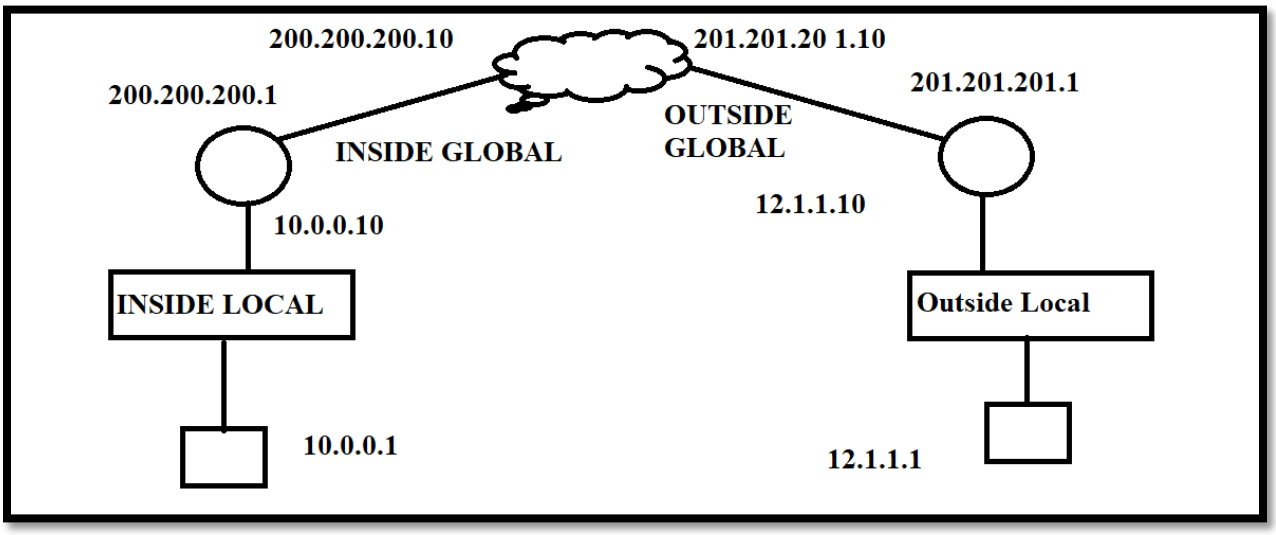
- IP access-list standard 10
- Deny 10.1.1.0 0.0.0.255
- Int f0/0
- IP access-group 10 in

- ACL Guidelines
    1. ACL works sequentially
        - ACL will check list in sequential order

2 ACL has difference of 10 sequence number
3 After the complete ACL list there is an “implicit deny” at the bottom of ACL
4 If you add new ACL then it will always added by default at the bottom of pervious ACL
5 Once the ACL matched the clause present at any seq. Num then rest of the ACL’s will not checked.
6 Per int only one ACL can be applied per direction.

NAT (Network Address translation)

- What is NAT?
  - It is a protocol which is used to make communication possible between one IP address into another IP address.
    - Private to private
    - Private to public
    - Public to public
- What is need of NAT?
  - To save Ipv4
- Terminologies
  - Inside Local →Source IP before translation.(My private IP)
  - Inside Global→Source IP after translation.(My public IP)
  - Outside Local→Destination IP before translation.(Google Private IP)
  - Outside Global→Destination IP after translation.(Google Public IP)



- Types Of NAT

- Static NAT
  - One to One Mapping
  - For each private IP we need one Public IP
  - Security
  - To hide actual IPs
  - Entry is permanent
  - Bidirectional
  - If we have multiple users so we have to give multiple static statements
  - Disadvantage→to conservation of IPs
  - Max used in server forms(data center)
- Dynamic NAT
  - Define pool of public IPs
  - One to many Mapping
  - Unidirectional
  - Entry is not permanent
  - FIFO(First in First Out)
  - Conserve your IPs
- NAT overload {PAT (Port add. Translation)}
  - All private users are translated into single public IPs
  - One to all
  - Simultaneous.
  - Conserve your IPs

- Sh ip nat translation
- R1(config)#ip nat inside source static 10.0.0.1 200.200.200.1
- R1(config)#
- R1(config)#int fa0/0
- R1(config-if)#ip nat inside
- R1(config-if)#exit
- R1(config)#
- R1(config)#
- R1(config)#int s5/0
- R1(config-if)#ip nat outside
- R1(config-if)#exit
- clear ip nat translation *

IPV6

Rule 1:- It is 128 bits address in Hexadecimal from. Divided into 8 blocks and Separated by (:)

- No need of NAT
- No need of Subnetting
- DHCP Stateless (No need DHCP Server)
- DHCP State full (Need DHCP Pool)

16 bit: 16 bit: 16 bit: 16 bit: 16 bit: 16 bit: 16 bit: 16 bit

Starting 64 bits = Network Bits

Last 64 bits = Host bits

Rule 2:- Identify the network Id portion / Address type

- FF00 ::/8= Multicast address
- FC00 ::/7= Private Address(Unique local Unicast) these are used for Intra network communication
- 2000::/3 = Public Address(Global unicast address) these are used for communication in global (Internet)
- FE80::/10 = Link Local Address
    - Step 1 – FE80:: → 64 bits
        - FE80:0000:0000:0000:
    - Step 2—→Auto calculate by MAC Address of interface
        - → 1234.ABCD.0128 + FFFE

        - 1234.AB FF:FE CD.0128
    - Step 3—Change 7th bits of 1st octet
        - 1234.ABFF:FECD.0128
        - 1034.ABFF:FECD.0128
        - FE80:: 1034.ABFF:FECD.0128
- Manually IPV6 Address

Rule 3:- Identify the host ID portion.

→It is in 64 bits.

→10AA.01AO.190A

→10AA:01 FF: FEAO: 190A

→IF 7th bit is 0 then it converts into 1.

→IF 7th bit is 1 then it will convert into 0.

How to Write in Short form of IPV6:-

→If there is leading Zero in a field we can avoid them to write

➔ 2001:0014:0001:0002:3003:0008:7000:0080

➔ 2001:14:1:2:3003:8:7000: 80

→If multiple fields are zero then write ten with double colon [::] only once in a IPV6 address.

→ Ex- FC00:0000:0000:0001:0000:0000:0000:0001

- FC00::1:0:0:0:1
- FC00:0:0:1::1

→IPV6 Protocols

- ICMPV6
- OspfV3
- NDP → Neighbour Discovery Protocols
  - ICMPV6(Back)
  - Neighbour Solicitation (ARP REQUEST)(Multicast)
  - Neighbour Advertisement (ARP REPLY)(Unicast)

→How to assign IPV6

- R1(config-if)#ipv6 address 192:168:101:1::1/64
  - FE80::C801:9FF:FE20:8
  - ca01.0920.0008
- Router advertisement in every 60 sec (send if own prefix)
- Router Solicitation
- R1(config)# IPV6 unicast-routing
- R2(config-if)#ipv6 address autoconfig

→Create loopback IPV6

- R1(config)#int l0
- R1(config-if)#ipv6 address 1::1/128

→Configure Static Routing

- R1(config)#ipv6 route 2::2/128 fastethernet 0/0
- R1(config)#ipv6 route 2::2/128 fastethernet 0/0 FE80::C802:4FF:FE70:8
- R2(config)#ipv6 route 1::1/128 fastethernet 0/0 FE80::C801:9FF:FE20:8

→Ospf V3

- R1 (config)#ipv6 router ospf 10
- R1(config-rtr)#router-id 1.1.1.1
- R1(config-if)#int r fa0/0,l0
- R1(config-if-range)#ipv6 ospf 10 area 1

- R3(config)#router ospfv3 10
- R3(config-router)#router-id 3.3.3.3
- R3(config)#int r fa0/0,l0
- R3(config-if-range)#ospfv3 10 ipv6 area 1

NETWORK BULLS WHERE CAREERS FLY infoogy

Security

- Something you want to secure

Security Terminology

- Vulnerability: - Weakness of network.
  - In terms of security, vulnerability is anything that can be considered to be a weakness that can compromise the security of something else, such as the integrity of data or how a system performs.
  - Example :- Port security
  - Exploit: - Use something by which you can misuse the device.
    - The key that is used for vulnerability (weak).
- Threat:- Misuse of network using exploit

Layer 2 security

- Port Security --- For Secure Port
- DHCP Snooping
- Man in the middle attack
- DOS(Denial of Service)Attack -→ Arp Inspection

Layer 3 Security

- ACL
  - Standard
  - Extended
- Router
  - Routing
  - Filtering
- Firewall:- It is a security device which is used to filter layer 3 and layer 4 & layer 7 traffic
  - ACL
  - Object Group
  - Cisco Firewall – ASA (Adaptive Security appliance)
    - Every Interface is a part of Zone
    - Zone represent some security level(0-100)
    - Inside Zone (by default 100)
    - Outside Zone (by default 0)
    - Demilitarized Zone (DMZ)
    - Traffic travel higher to lower then data will be permit
    - Traffic travel lower to higher then data will be drop
    - Firewall will make entry in Connection table

Traditional Firewall → Old Firewall

- Like router IP ACLs, match the source and destination IP addresses.
- Like router IP ACLs, identify applications by matching their static well-known TCP and UDP ports.
- Watch application-layer flows to know what additional TCP and UDP ports are used by a particular flow, and filter based on those ports.
- Match the text in the URI of an HTTP request—that is, look at and compare the contents of what is often called the web address—and match patterns to decide whether to allow or deny the download of the web page identified by that URI.
- Keep state information by storing information about each packet, and make decisions about filtering future packets based on the historical state information (called *stateful inspection*, or being a stateful firewall).

Intrusion Detection System (IDS)

- This device is used to detect virus and any malicious data in packet and inform this to administrator.
- Example :- fake Mail

Intrusion Prevention System (IPS)

- It will detect infected data and drop it.

AAA

- Authentication → Who are you?
- Authorization→ what can you do?
- Accounting→ what you did?
- The user who are coming that are authenticate user or not
- How much access you have Privilege level
- We will use cisco device ISE (Identity service Engine)
  - Username
  - Password
  - Privilege level
- **TACACS+:** A Cisco proprietary protocol that separates each of the AAA functions. Communication is secure and encrypted over TCP port 49.
- **For device access**
- **RADIUS:** A standards-based protocol that combines authentication and authorization into a single resource. Communication uses UDP ports 1812 and 1813 (accounting) but is not completely encrypted
- **Network access**

Wireless

- When a connection between source and destination is established through radio frequency signal is termed as Wireless Network. In wireless communication data travels in air.
- Communication without any physical connectivity.
    - Wired –IEEE- 802.3
    - Wireless- 802.11

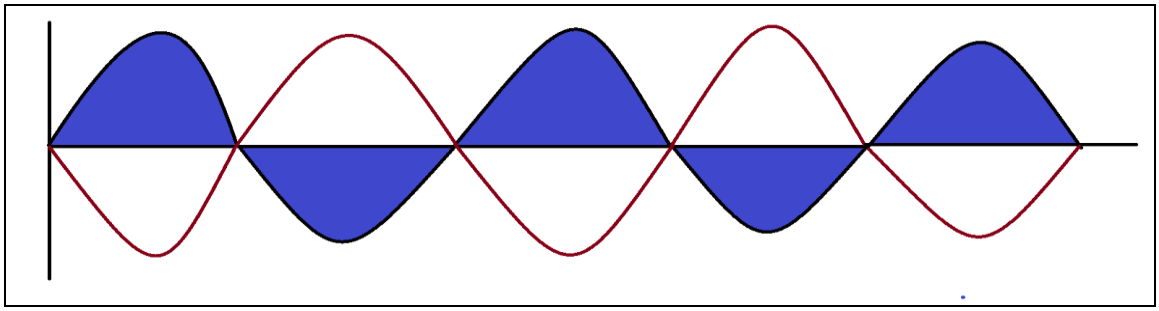
Requirement of wireless media:-

1) Mini Devices:- Smart Phone , Remote Controller
2) Mobility :- Those can carry any where
    a. Example :- laptop

- Wireless data is travel in form of Frequency

    - **Radio Frequency**: The RF (Radio Frequency) is the combination of Electromagnetic waves (electric and magnetic signals). Electromagnetic waves don't travel in straight direction. Waves are expanded and travel in all directions.

        - When one wave completes one up and one down circle so it is known as Cycle. It can also be represented in from where one wave starts from one peak and finishes at next peak so, one complete circle or one sequence is called cyclic pattern.
            - Frequency = 4 cycle / second
                - Frequency = 4 hertz



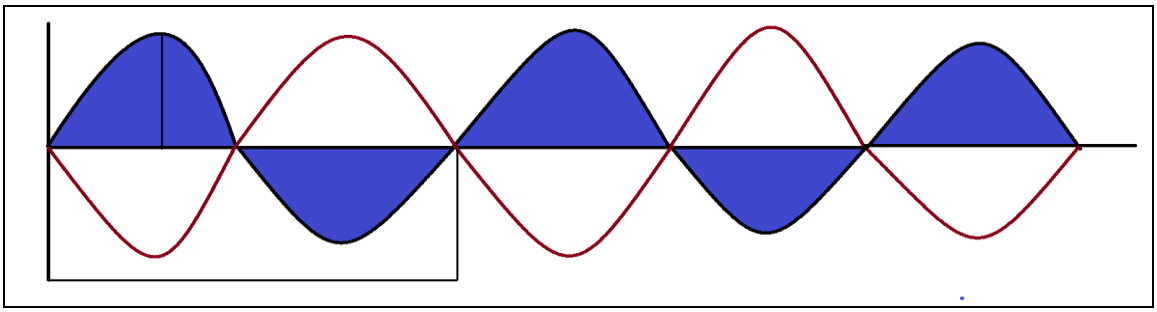
- Its means that when a wave complete for 4 cyclic circle per second it complete one Frequency.

- As distance increase limit of wireless network also increase and range of numbers is also depends on increasing distance. To memories unit with large numbers is hard for user, so we modified unit name to keep it simple way.

- Table – **Frequency Unit Name**

Unit	Meaning	Abbreviation
Hertz	Cycles per Second	Hz
Kilohertz	1000 Hz	kHz
Megahertz	1,000,000 Hz	MHz
Gigahertz	1,000,000,000 Hz	GHz

  - The Frequency range between 3 kHz to 300 GHz is terms called Micro wave and Radder .The micro wave category also contains the two main frequency ranges that are used for wireless LAN communication: 2.4 and 5GHz.
  - Wave length = Length of wave
    - It is directly proportional to distance
    - 2.4 GHz = 2.4 * 10^9 cycle/sec (wavelength more means number of cycles is more)
    - 5GHz= 5*10^9 cycle/sec



- Amplitude: - It is use to increase power of Frequency.

Wireless Bands and channels

A range of IP address is representing by Network ID. Just like "A group of frequency is known a Wireless Band".

There are two types of bands commonly LAN wireless Network use that are:

a) **2.4 –GHz Band**: The range of this band lies between 2.400 and 2.4835 GHz is represent by 2.4-GHz. Example: 2.412, 2.417, 2.442, 2.452, 2.484 all frequency are part of one band that represent is 2.4–GHz Band. Total 14 frequencies in 2.4 GHz.

b) **5-GHz :** The range of this band lies between 5.150 and 5.825 GHz. In this band contain four separate bands:

   i) 5.150 to 5.250 GHz
   ii) 5.250 to 5.350 GHz
   iii) 5.470 to 5.725 GHz
   iv) 5.725 to 5.825 GHz

Note: - You do not need to learn the name of particular frequency. You just aware with name of bands name 2.4-GHz and 5-GHz.

- Non over lapping
- Over lapping

- **AP(Access-Point)**

It is a wireless network device which is used to connect different devices like Computer, Laptop, Switch, etc. to make communication possible and Share data.

There are some parameters by which we identify an Access point

a) **SSID**: It is a short form for Service Set Identifier. Every AP (Access point) uses a unique name or logical name as an identity, so that the devices can find it and connect to it. One AP can have Multiple SSIDs. It is locally unique ID but could be same in different network.

- Example: NB Network

b) **BSSID**: It is a sort form for Basic Service Set Identifier. The term which is used to represent Access point Mac Address is called BSSID.

- Example: a2:e4:r5:8u:9r:50

c) **BSS**: It stands for Basic Service Set. Every access point have range or radius called Basic Service Set. Any device that wants to connect to the AP must fall in the BSS. The Access Point is like the heart of BSS. In a BSS devices are directly connected to AP with help of SSID (NB Network) and BSSID (a2:e4:45:76:d6:r6).

NETWORK BUILDS infoogy

- Let's suppose host A wants to connect with host B so it must first connect with Access Point

1) Host A cannot directly get connected with host B. They both can communicate via AP.

2) It not possible to Host A directly connect with host B. Why? Because then the whole idea to create and maintain the BSS is debatable.

IBSS (Independent Basic Service Set)

- As the name suggests this basic services set is independent of the AP, that is, two wireless clients can communicate with each other directly without getting connect to AP. This is also known as Ad-HOC Wireless Network.
- One of the wireless clients behave like an AP as it advertises the network name and the required radio parameters. The other devices can then join as required.

a) Unidirectional Communication

- When a sender and a receiver communicate only in one direction through radio frequency (or channel) then this type of communication is called unidirectional Communication. A device can only be either a sender or a receiver.
    - Example: Simplex Mode

b) Bidirectional Communication

- When a two device communicate in both the ways but one at a time through frequency (or channel) is called Bidirectional Communication. A device cannot be a sender as well as a receiver simultaneously.
    - Example: half Duplex

DSS(Distribution System):-

In BSS multiple devices are directly connected to AP with the help of radio frequency, AP also manages BSS, but this is not the sole work of AP. The devices which are connected to AP also need Internet connectivity. AP has both wireless and wired capabilities. With the help of wired (Ethernet Media) AP connect with uplink networks and that uplink network is called Distribution System (DS) .This standard is refers by 802.11 to connect with upstream with wireless BSS.

The AP holds the responsibility of mapping a VLAN to a SSID. The AP map the VLAN 10 to the wireless LAN which is using SSID- NB NETWORK

Clients who are associated with the SSID (NB NETWORK) will be connected to VLAN 10.

Also, multiple vlan can be mapped to multiple SSID. TO achieve this AP must be connected to the switch with the trunk link that will be caring the VLAN. The AP looks like multiple logical AP, one per BSS having a unique BSS ID for each.

In the case of cisco AP it is done by incrementing the last digit of the mac address for each SSID.

ESS (Extended Service Set)

One AP cannot cover the entire geographical area where the wireless clients are located. So, in order to cover the entire geographical area we need to add more AP's so that the entire

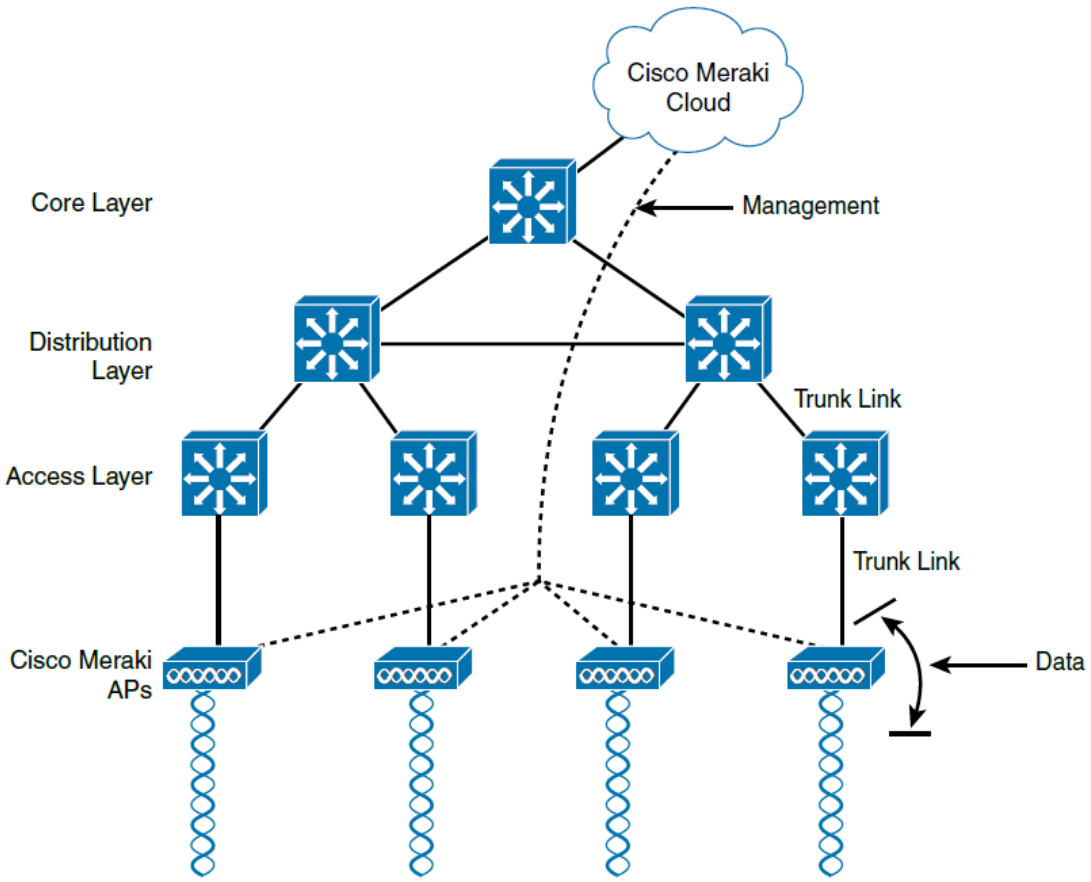
wireless client could join the available BSS. In this way we are extending the services set for the client.

Types of AP (Access-Point)

1) Autonomous Access Point :-
    a. This are stand alone AP
    b. Everything is configured on AP
    c. Acl , DHCP , MAC-Filtering

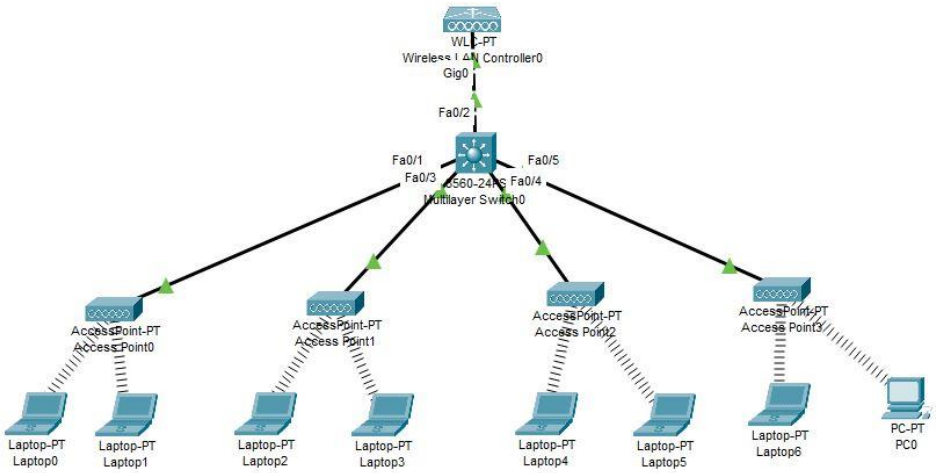
- There are three different layers in Architecture.
    1) Core layer
        a. Multilayer Switch→ (4500,6500)
        b. ASA, Router
    2) Distribution Layer → Provide connectivity between Core layer and Access layer
        a. Switches L3 → (3850 , 3750)
        b. Routing , L2 switches , etherchannel
        c. Server connectivity
    3) Access layer
        a. Normal layer 2 switches
        b. 2450 , 3550 , 3560 , 2460
        c. Host connectivity

NETWORK BULLS WHERE CAREERS FLY
infoogy



- Lightweight AP
  - Those are managed by Wireless LAN Controller.
  - Split Mac Architecture

- WLC (Wireless LAN Controller)
  - It is a device that is use to control and manage the APs. All the management function like specifying Channel, maintaining the association tables, creating SSID etc. is performs by the WLC. The remaining data plane work is carried out by the AP itself. The messages between the WLC and the AP is exchanged through a tunnel named CAPWAP (**Control and Provisioning of Wireless Access Points)**



- Summary of WLC Deployment Models

Deployment Model	WLC Location(DC,Access,Central,AP)	APs Supported	Clients	Typical Use
Unified	Central	6000	64,000	Large enterprise
Cloud	DC	3000	32,000	Private Cloud
Embedded	Access	200	4000	Small campus
Mobility Express	Other	100	2000	Branch location

- CAPWAP Control plane tunnel→ UDP 5246
- CAPWAP Data Plan Tunnel → UDP 5247

Wireless Security

- Security Provide some parameters
  - Authentication: - To authenticate the user (who are you).
  - Message Integrity: - Calculate a Hash value over data to check data is real or not. (Like checksum).
  - Encryption: - To convert plain text into Cipher Text.
- To Authenticate User
  - Open Authentication
  - Wired Equivalent Privacy (WEP)
  - 802.1x/EAP:- Username / password
  - MAB:- Mac address
  - LEAP
  - EAP-FAST
- To encrypt the data
  - WPA
  - WPA2
  - WPA3
    - TKIP
      - MIC → Hashing Algorithm

Virtualization

- When device is Deploy on server on need a hardware device for that.
  - Physical hardware Server
    - Ram – 256 GB
    - HD- 4TB
    - VCPU – 28 VCPU

- Virtual Machine
  - Router , Switch , Window 7 , cisco firewall (ASA)
  - Configuration – RAM, CPU , HD
- Hyper- visor
  - VMware
  - Vsphere
  - Microsoft
- Port-group
  - Vlan
- Virtual Switch

Automation and Programmability

  - Do something with less effort.

- Traditional Network
  - Configure all devices manually.
    - Human Error (Misconfiguration)
    - Costly
      - Need a good team for implementation.
      - Need Firewall , NGIPS
- Control Plane :- The Traffic is send between Device to Device
  - Example :- OSPF , CDP , VTP etc
  - Create a best path for user traffic.
  - Routing Table
- Data Plane :- The Traffic which is send between host to host or host to server
- Management Plane :-The traffic which is need to manage a network
  - Example :- Telnet , SSH , tftp , SNMP
  - Host to device

Control Plane(OPSF , EIGRP)
Management Plane(Telnet , SNMP)
DATA PLANE(USER DATA)

CPU(Control Plane) ➔ RIB(Routing Information Base)
Fabric
I/O Module (FIB) CEF(Data Plane) →Forwarding Information Base

- FIB→ Duplicate Copy of RIB
- Fabric → Make communication between software and Hardware
- Control plane and management plane is manage by Controller.
    - Configuration
    - Implement
    - T-shoot
    - Monitor
    - Manage

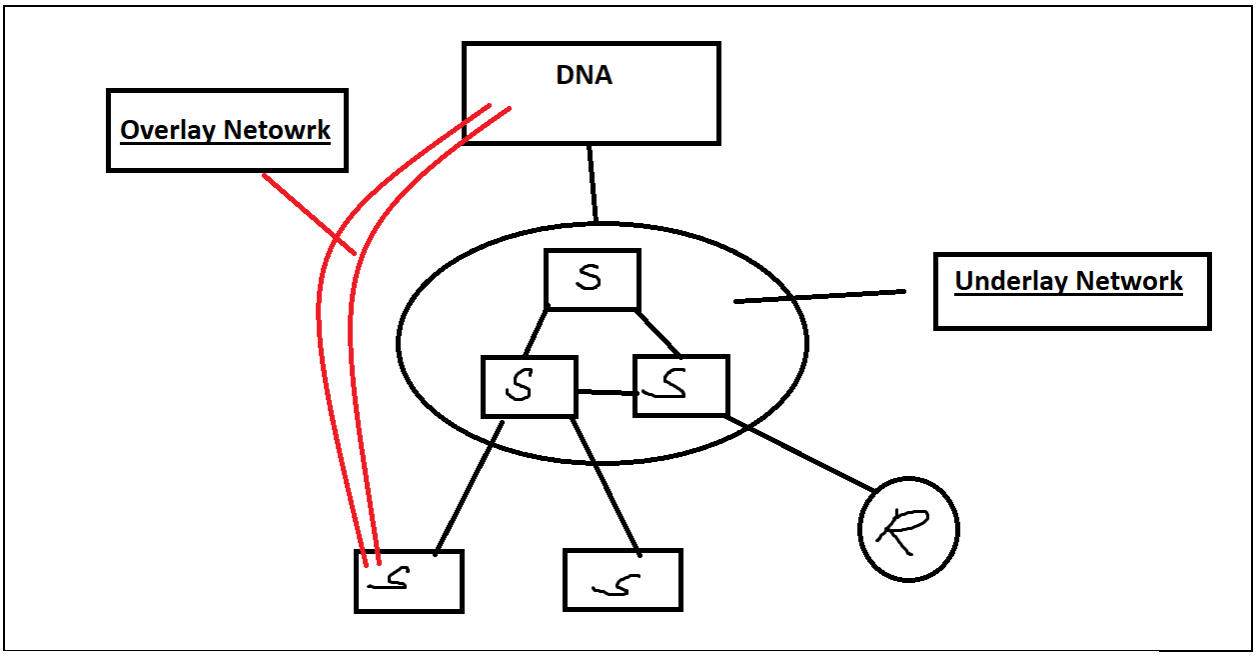
And this technology is called SDN (Software defined Network)

- Type of network
    - Enterprise Network(LAN, CAN)
    - WAN
    - DATA Center

NETWORK BULLS WHERE CAREERS FLY
infoogy

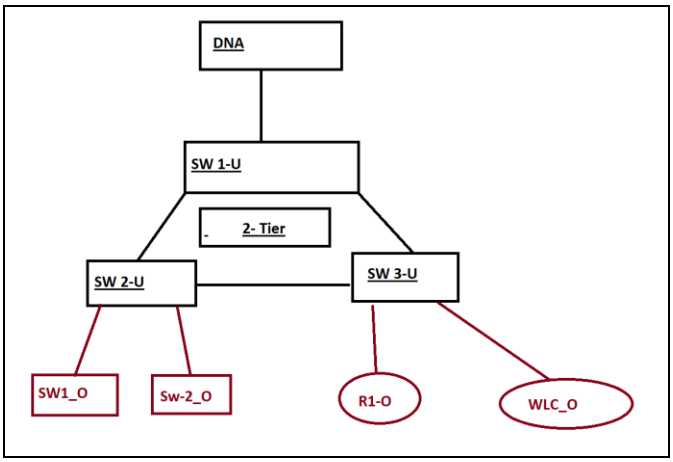
- SDN is divided in three Part
    - SDA(Software Defined Access) it is use in Enterprise Network
    - SD-WAN(Software Defined WAN) it is use in WAN
    - ACI(Application Centric Infrastructure) it is use in DATA Center
- SDA
    - Controller use →DNA(Digital Network Architecture)
- SD-WAN
    - VMANAGE →Configuration , Manage , T-shoot
    - VBOND → Authentication
    - VMSART→Control Plane

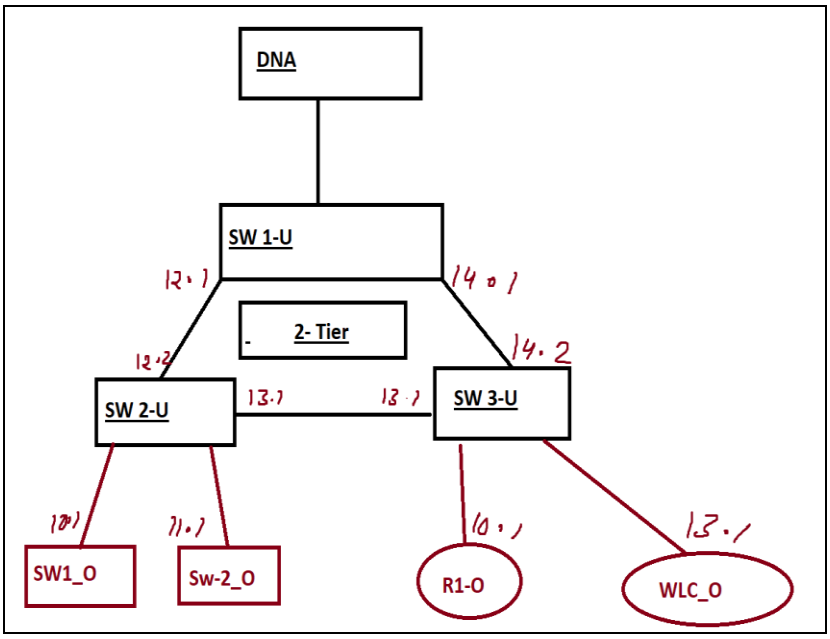
- ACI
    - APIC (Application Policy Infrastructure Controller)
- DNA



- There are 3 type of layer
  - Core
  - Distribution
  - Access

- 2-tier architecture
  - Distribution
  - Access





- 3-tier architecture
  - Core
  - Distribution
  - Access
- Non cisco → Open day light controller→Prime ->APIC-EM →DNA
- API (Application Programmability Interface)
  - API is used to exchange data between applications.
- South bound Interface API → when DNA give information to device
  - OPFlex (Cisco)
  - Open flow (Open standard)
- North bound Interface API→ When DNA gets information with Application.
  - REST API (Representational State Transfer Application Programming Interface)
  - GET
  - Information
  - Variable
  - XML , JSON
  - Application (POST MAN)
- DNA →GUI , APPLICATION use (JAVA, SCRIPT{python})
- Fabric = Overlay + Under lay
- Control Plane use some Protocols in SDA
  - LISP(Locator and Identity Separation Protocol)
    - It use to encapsulate L2 header

- VXLAN(Virtual Extensible LAN)
- It use to encapsulate L2 and L3 header

NETWORK BULLS WHERE CAREERS FLY
infoogy

Thank You ☺

Visit us at nb.infoogy.com

Will help you to build a great networking career