Application layer, Presentation layer, Sessin layer

Transport layer :

Working:

Transport layer breaks the data into managable segments comming from the upper layer. It adds its own header to create encapsulation.

Functionality:

It takes two critical decisions,

1. To decide whether the communicatin is reliable(TCP) or unreliable(UDP).

2. Assigning the port numbers.

What is unreliable and reliable communication:

Reliable - It needs an acknowledgement for every packet that needs to be sent.

Unreliable - There is no acknowledgement received for every segment transmission.

Transport layer creates the random source port number and adds the sourse port and destination port in the header. For example, if the destination is

webapplication then the destination port is 80, it adds this port number along with IP address.

(Note - This layer creates socket and sends it to network layer, socket is noting but an IP address and a port number)

Need for source port number:

for instance, if there are two applications running on the machine which sends information to the same IP address along with receiving acknowledgements. The

transport layer needs to identify, for which application it is receiving acknowledgement.

Network Layr:

when the network layer gets segments from the transport layer, it adds anetwork layer header, when the network header is added in the data, then it is

called a packet. In this layer IP address is added.

It also search for the best path in the routing to send the data.

Data Link Layer:

When the information coming from networklayer to the data-link layer, it adds data-link header to the information. This layer is responsible for MAC

Addressing

When a data is comming from physical layer to data-link layer, it checks for errors during the information partition or transmition.

Physical Layer:

It is the layer where actual data transfer happens

Internet Protocol(IP) Addressing:

Conversion of Binary Address to Decimal Address:

IP Address(decimal notation) – 192.168.100.225

IP Address(binary notation) – 11000000.10101000.01100100.11100001

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 132 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |

Here, 132 + 64 = 192.

This is how binary to decimal form of IP address are formed.

GateWay:

Gateway is a medium that can be any interface of a router, we need to configure which interface should be a gateway. Any data that need to be send from one network to another network is through gateway.

Subnetting:

When we go for subnetting then it should be class less, No Class A, B or C.

Class A – 1 – 126

Class B – 128 – 191

Class C – 192 – 223

Class D – 224 – 239 -- it is used for multicast

Class E – 240 – 255 -- It is used for experimental purposes

Any IP Address that starts with 127 is a loopback IP address.

For CCNA only Class A, B and C is enough.

Class C IP Address:

Subnet mask for Class C is 255.255.255.0

192.168.100.225/24 🡪 It means the subnet mask has 24 1s(One’s)

24 1s is nothing but Class C IP address – (11111111.11111111.11111111.00000000)

(Note : when the host is 0 then it is the first IP address – 192.168.100.0, it is the network ID(. Secondly, when the host turns to all 1s (last IP address – 192.168.100.255) then it is broadcast address.)

To find the number of IPs 🡪 2^n – 2

Here n 🡪 number of host bits(number of zeros in host), in this case it is 8. So, the result is 254

There are 254 hosts.

Class B IP Address:

Subnet mask for Class B is 255.255.0.0(11111111.11111111.00000000.00000000)

Example – 172.123.100.225/16 🡪 because 16 1s.

Network ID – 172.123.0.0

Broadcast ID – 172.123.255.255

To find number of host bits 🡪 2^n -2 , where n = 16( 16 bits are 0 in host), here total is 65,534 hosts.

Here hosts are high and difficult to manage. So the concept of subnetting was introduced.

Class A IP Address:

100.228.111.225/8 --- (11111111.00000000.00000000.00000000)

Subnet mask – 255.0.0.0

Total no of hosts – 2,097,150

First IP address – 100.0.0.0, Last IP address – 100.255.255.255

SUBNETTING:

It is breaking down the large networks

Subnetting is nothing but borrowing a bit from your host part and creating a network.

IP address - 192.168.100.0

Subnet - 11111111.11111111.11111111.00000000 – before borrowing

Subnet - 11111111.11111111.11111111.10000000 – after borrowing(here the host is 128, because 1 is only at 128th bit position.

So, it has subnet – 1 and subnet – 2

192.168.100.0 – Network ID – 1 (192.168.100.0/25) 🡪 here there are 25 1s after borrowing

192.168.100.127 – Broadcast Id – 1 (192.168.100.127/25)

192.168.100.128 – Network Id – 2 (192.168.100.128/25)

192.168.100.255 – Broadcast Id – 2 (192.168.100.255/25)

Another Example:

IP – 192.168.100.225

Subnet – 255.255.255.192 (11111111.11111111.11111111.11000000) 🡪 128 64 32 16 8 4 2 1

Here there are 4 subnets because 1s in host bit is at 64th bit position.

Network Id 1 - 192.168.100.0 / 26

Broadcast Id 1- 192.168.100.63 / 26

Network Id 2 – 192.168.100.64 / 26

Broadcast Id 2- 192.168.100.127 / 26

Network Id 3 – 192.168.100.128 / 26

Broadcast Id 3 - 192.168.100.191 / 26

Network Id 4 – 192.168.100.192 / 26

Broadcast Id 4 - 192.168.100.255 / 26

Task with Requirements:

1. Create 3 sub-networks
2. Use a Class C IP address : 192.168.1.0
3. Determine the network id and broadcast id of all the subnets

Solution:

We can able to break the network into multiples of 2.

For this scenario we can break the network into 4 parts because the need is 3 here.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 132 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |

Each subnets get 64 masks, out of which 2 are network id and broadcast id, so (64 - 2 = 62)

General Notes:

When n = number of 1s in host, then (2^n) gives number of subnets

When n = number of 0s in host, then (2^n – 2) gives number of hosts

Hub:

It is not intelligent,

The collision domain is 1. Because if we connect a two device in the two ports of a hub and they are transmitting a data, if we connect a 3rd device then the data transmission is interrupted. So the data should be re-transmitted. So the collision domain for Hub is 1.

Broadcast domain is 1. Because it broadcasts the information to all the devices which are connected to it. It does not have any intelligence to hold the traffic.

Bridge:

A bridge is slightly intelligent than Hub, but not as intelligent as switch.

Switch:

It has (Application Specific Integrate Circuit). This has the capability of storing MAC address information. If the devices are connected in the switch, after the switch is going up(power supply given) with in 10 seconds, it has the ability to read the MAC address of the devices which are connected to it.

If wont broadcast the information to all the devices, if the information have destination MAC address.

So switch has more collision domain, if the new devices are connected to it, it won’t affect the other device communication. For example if a switch have 24 ports, then the collision domain is 24.

If the VLAN is not configured in switch, then it has 1 broadcast domain.

Router:

It is a intelligent device. It has many collision domain as many as number of ports. Also it has many broadcast domains. For instance, if a router receives a broadcast domain from one of its ports, it just drop it. It does not forward it to other ports.

DHCP (Dynamic Host Configuration Protocol):

When a device is connected in a network, it shouts around (broadcast) like is there any DHCP around. All the devices I the same network hears the broadcast. If there is a DHCP server, dhcp sends a dhcp offer packet. It offers an IP address to the device along with that dhcp gives its own IP address to the device in the packet.

In another case, but rare case, there are two dhcp servers connected in the same network. If the device connected to the network asks the dhcp server for IP address. Then the client receives two IP address from two different dhcp servers. Then it’s upto the client to decide which IP address to choose.

Steps:

1. DHCP discovery
2. DHCP offer
3. DHCP request
4. DHCP Ack
5. DHCP Information 🡪 it is about additional information sharing
6. DHCP Release 🡪 it’s abt release IP req when the device wants to disconnect from the network.

TCP Transmission:

Before information is shared through TCP, there should a connection needs to be established.

Three way handshake will be happened during the establishment of TCP connection.

First device A sends SYN packet to device B, B receives it. Then B sends SYN/ACK (both the information in the same packet) message to A.

Then again A sends ACK to B about receiving the packet.

TCP Transmission (Windowing Technique):

It is the process of transmitting the data to devices to find the transmission capacity for receiving devices. At first the sender will send one packet and receiver sends acknowledgement. Then sender gradually increases the packets to check the receivers capability of sending acknowledgement. At final stage sender will find receiver capability.

Common Port Numbers:

Switch Configuration in GNS3 S/W:

Things that can be configurable,

1. Hostname – name of the host, we can configure it
2. Logon Banner – after the successful log in, we can give some description about the switch, that will be displayed, same like putty.
3. Console Password – there are 16 terminals starting from console-0 to console-15, we can configure the password in console-0
4. Telnet Password – this password should be configured in virtual line, and the command is “line vty”, also we can configure upto (0 t0 15) virtual lines, totally 16 virtual lines.

Virtual Line:

It is about how many remote virtual instances can be taken through Telnet starting from 0 to 15. If a first person login the switch through telnet then line -0 is assigned when the 2nd person logins it’s now line -2 and so on.

1. Enable Password

To go to privilege configuration mode, we need to configure the “enable password”.

1. Management IP

Switch is a layer 2 device and doesn’t require an IP address for every port. But if we want to access the switch from other device we need an IP. So we need to assign management IP to the switch.

Note: Sh ip int brief (show ip interface brief) will show all the interface belong to the switch.

How to go to the interface:

1. Go to the global configuration mode
2. Give the command (int <name of the interface>) 🡪 eg. Int vlan 1
3. Default Gateway
4. Shutdown

It is about shutdown the interface by giving the command (<interface name> shutdown)

1. Negating Command
2. Saving Configuration

It is about saving all the above configuration by giving the command (write)