

# **NP 369 CCNA Notes**

## 1. Subnet

### SUBNET

- Division of Large IP Networks in to multiple Small logical networks.
- Subnet mask is a 32 bit number used to identify the Network portion and the Host portion in the IP Address.
- 2 Types of Subnetting

*FLSM – Fixed Length Subnet Mask*

*VLSM – Variable Length Subnet Mask*

Advantages :

*Simplified Management*

*Minimizes Broadcast*

*Maximizes Network Performance*

*Secured*

### 1.1 Fixed-Length Subnet Mask - FLSM

#### FLSM

- Fixed Length Subnet mask.
- Dividing an IP Network with a Same or equal size.
- Formula  $2^n \geq N$  (Requirements)
- Binary to Decimals

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

If all the 8 bits in an Octet is 1 then its decimal value is 255

### Scenario 1:

Subnet a class A Network 10.0.0.0 as 4 Networks for 4 different Offices

Subnet mask for Class A : 255.0.0.0

Formula :  $2^n \geq N$  (Requirements)

$n = 0, 1, 2, 3 \dots$  i.e) the value of  $n = 2$

$$2^2 \geq 4$$

4 Possibilities are 00, 01, 10, 11

#### Network 1:

10.00000000.00000000.00000000

As the value of  $n = 2$  to satisfy its requirement, Move 2 bits from Host portion to Network Portion.

10.00 000000.00000000.00000000

Network Host

Subnet mask : 255.192.0.0

10.00 000000.00000000.00000000

Network Host

Keep All Host Bits as 0 to get the Network Address

10.00 000000.00000000.00000000

Convert to Decimals

10.0.0.0 Network Address

Keep all Host bits as 0 and last host bit as 1 to get First Host Address

10.00 000000.00000000.00000001

Convert to Decimals

10.0.0.1 First Host Address

Keep all Host bits as 1 and last host bit as 0 to get Last Host Address

10.00 111111.11111111.11111110

Convert to Decimals

10.63.255.254 Last Host Address

Keep all host bits as 1 to get Broadcast Address

10.00 111111.11111111.11111111

Convert to Decimals

10.63.255.255 Broadcast Address

### Network 2 : ( Second Possibility 0 1 )

**10.01** 000000.00000000.00000000  
Network Host

Subnet mask : 255.192.0.0

Keep All Host Bits as **0** to get the Network Address

**10.01** 000000.00000000.00000000 Convert to Decimals **10.64.0.0** Network Address

Keep all Host bits as **0** and last host bit as **1** to get First Host Address

**10.01** 000000.00000000.00000001 Convert to Decimals **10.64.0.1** First Host Address

Keep all Host bits as **1** and last host bit as **0** to get Last Host Address

**10.01** 111111.11111111.11111110 Convert to Decimals **10.127.255.254** Last Host Address

Keep all host bits as **1** to get Broadcast Address

**10.01** 111111.11111111.11111111 Convert to Decimals **10.127.255.255** Broadcast Address

### Network 3 : ( Third Possibility 1 0 )

**10.10** 000000.00000000.00000000  
Network Host

Subnet mask : 255.192.0.0

Keep All Host Bits as **0** to get the Network Address

**10.10** 000000.00000000.00000000 Convert to Decimals **10.128.0.0** Network Address

Keep all Host bits as **0** and last host bit as **1** to get First Host Address

**10.10** 000000.00000000.00000001 Convert to Decimals **10.128.0.1** First Host Address

Keep all Host bits as **1** and last host bit as **0** to get Last Host Address

**10.10** 111111.11111111.11111110 Convert to Decimals **10.191.255.254** Last Host Address

Keep all host bits as **1** to get Broadcast Address

**10.10** 111111.11111111.11111111 Convert to Decimals **10.191.255.255** Broadcast Address

#### Network 4 : ( Fourth Possibility 1 1 )

10.11 000000.00000000.00000000  
Network Host

Subnet mask : 255.192.0.0

Keep All Host Bits as 0 to get the Network Address

10.11 000000.00000000.00000000 → Convert to Decimals 10.192.0.0 Network Address

Keep all Host bits as 0 and last host bit as 1 to get First Host Address

10.11 000000.00000000.00000001 → Convert to Decimals 10.192.0.1 First Host Address

Keep all Host bits as 1 and last host bit as 0 to get Last Host Address

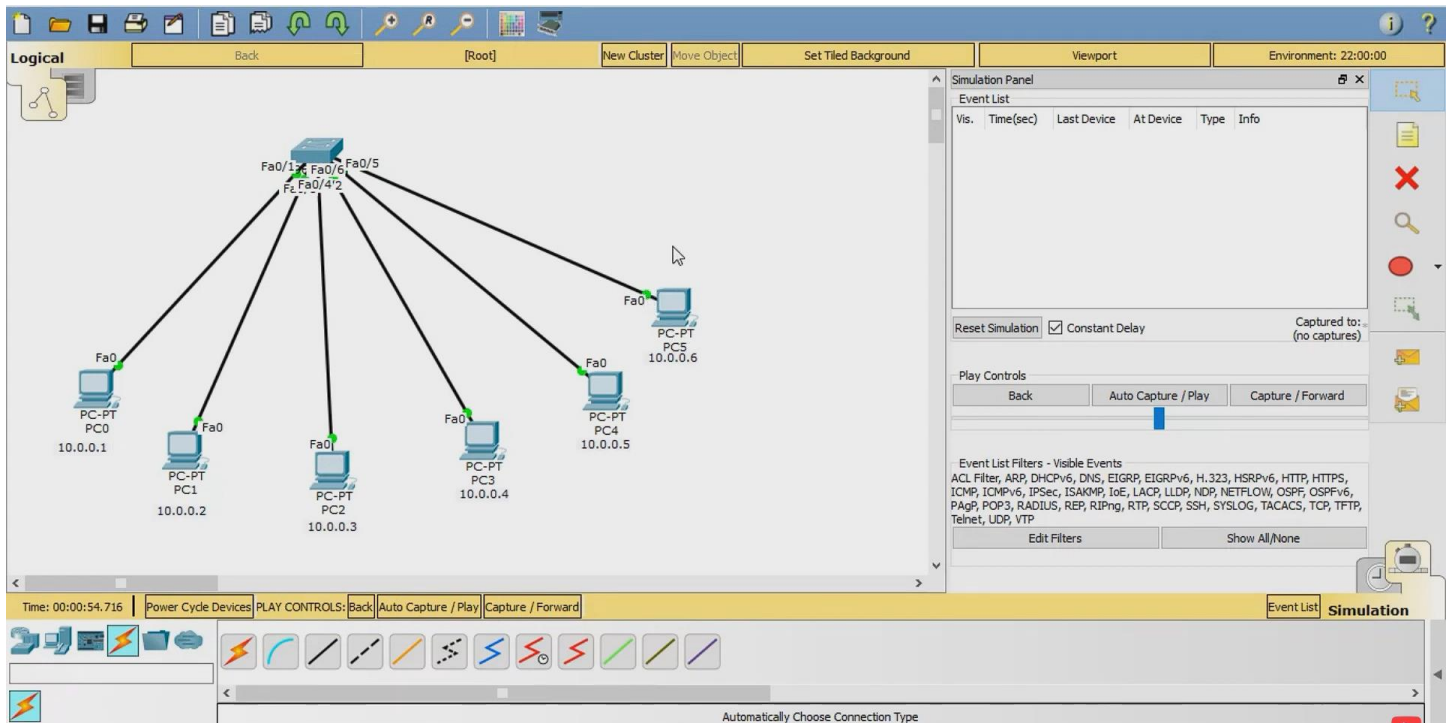
10.11 111111.11111111.11111110 → Convert to Decimals 10.255.255.254 Last Host Address

Keep all host bits as 1 to get Broadcast Address

10.10 111111.11111111.11111111 → Convert to Decimals 10.255.255.255 Broadcast Address



## Local Area Network – LAN



## 2. Virtual Local Area Network - VLAN

Vlan - Notepad

File Edit Format View Help

\* VLAN is Virtual Local Area Network.

\* VLAN is a logical group of devices that having same requirements are put in a single broadcast domain, that appears to be working on the same LAN, Even they are in different geographical locations.

\* It is not restricted to a physical boundaries in a switched Network.

\* It can be spread across multiple switches in a Network or even managed in a single switch.

\* Vlan ranges from 0 to 4095.

\* 2 Types of Ranges

- Normal Range Vlan (1 to 1005)
- Extended Range Vlan ( 1006 to 4095)

\* Vlan 1 is known as Native or default vlan

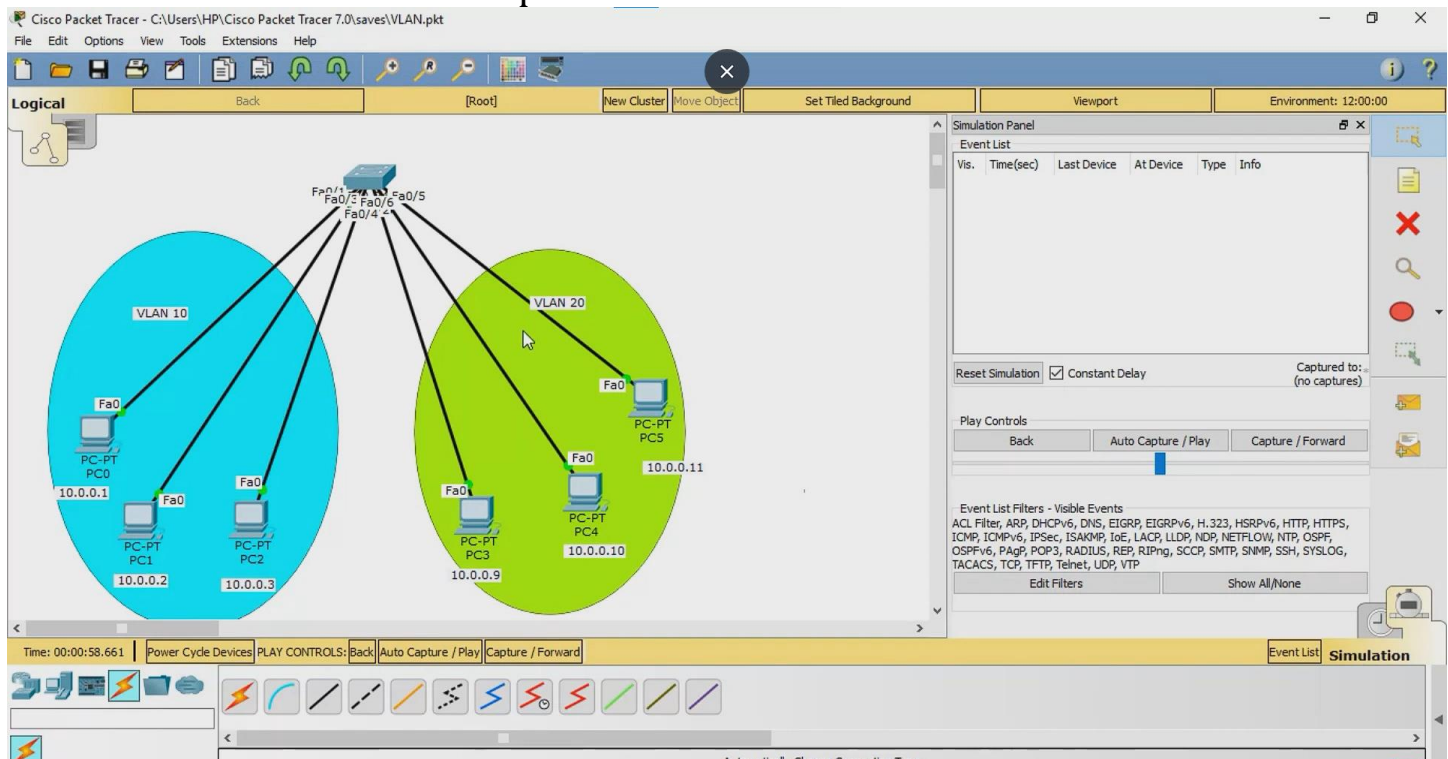
=====ADVANTAGES=====

- 1) Network Broadcast messages are minimized and hence Network Performance is better
- 2) Easy Administration.
- 3) Flexible and easy to Manage.
- 4) Reduced Cost.
- 5) Securied.

=====

### 2.1 VLAN Access Port

It allows declared vlan in that port.



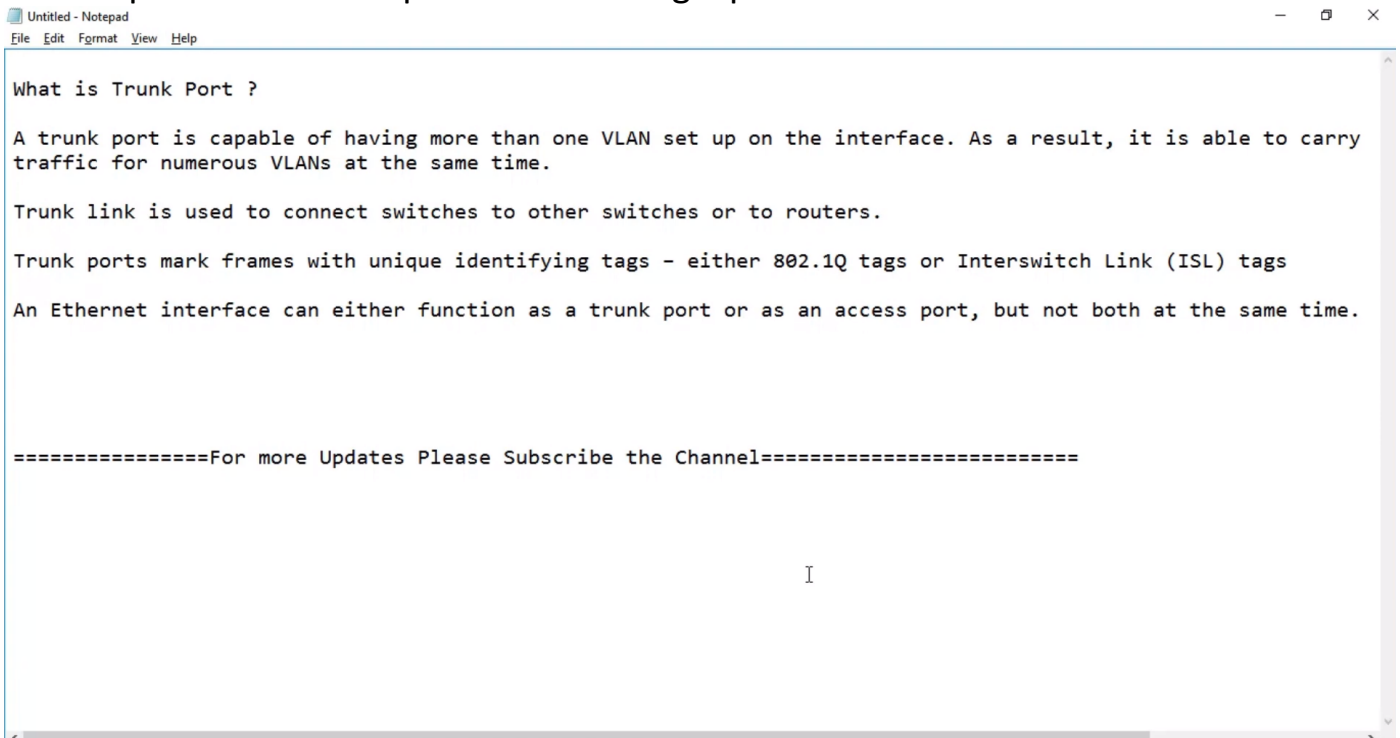


# Commands for creating VLAN in switch

1. Show running-config = it show the current running configuration of the switch.
2. Config terminal = to create vlan first get into the configuration mode.
3. Vlan 10 = this vlan 10 is the id of that vlan network. Only numbers are using to create id and that numbers are between 0 to 4095 range only.
4. Name Research and Development = any name can assign and this name is optional.
5. Exit = this exit form the config-vlan mode.
6. Int range fastEthernet 0/1-2 = assigning the already created vlan 10 to interface or port in switch.
7. Switchport mode access = converting the ports to access port for assigning the vlan.
8. Switchport access vlan 10 = passing the vlan 10 id for that port. That means the port allows only vlan 10 network communicate within the vlan 10 network.
9. Exit = exeting for the vlan config mode.
10. Show vlan brief = it shows the vlan details.

## 3. Trunk Port

Trunk port allows multiple VLAN in a single port.



```
Untitled - Notepad
File Edit Format View Help

What is Trunk Port ?

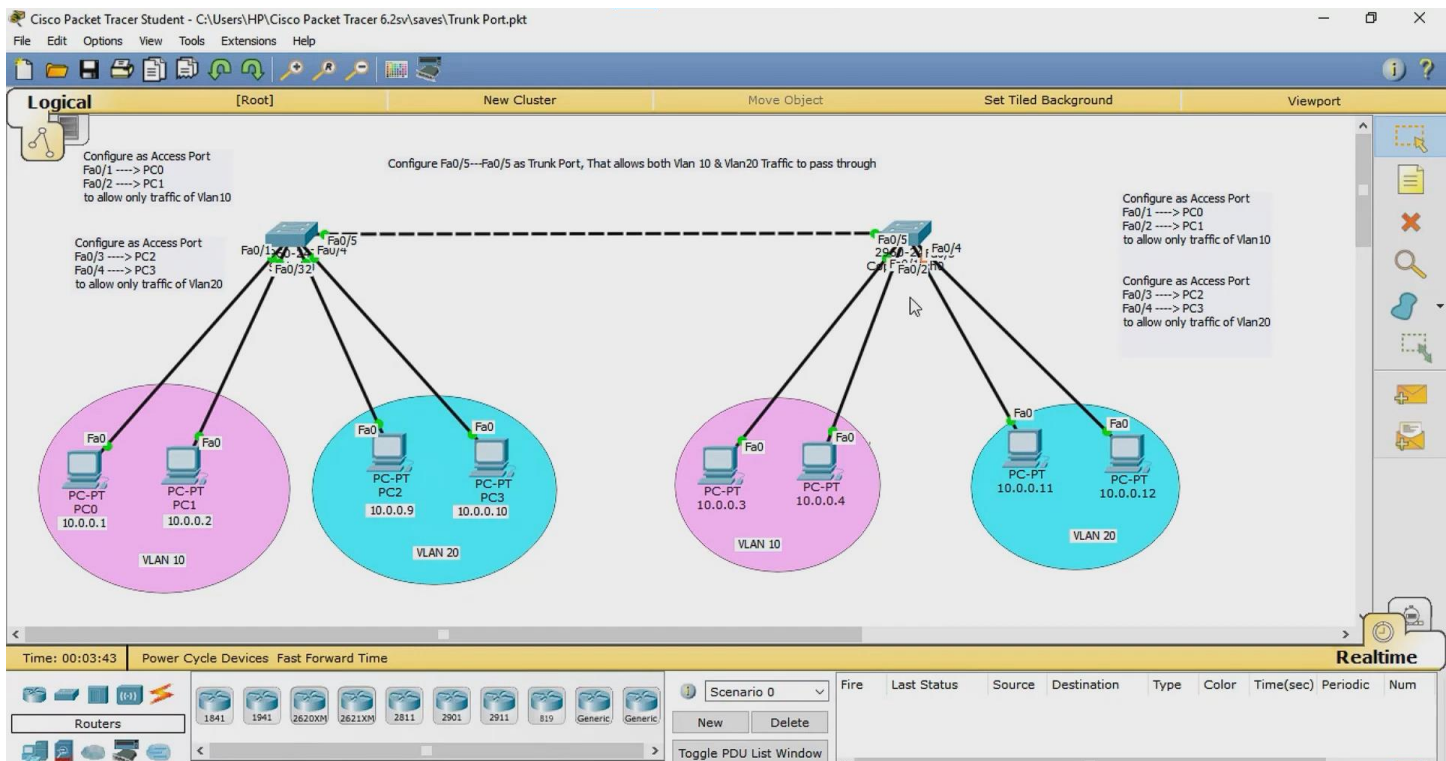
A trunk port is capable of having more than one VLAN set up on the interface. As a result, it is able to carry traffic for numerous VLANs at the same time.

Trunk link is used to connect switches to other switches or to routers.

Trunk ports mark frames with unique identifying tags - either 802.1Q tags or Interswitch Link (ISL) tags

An Ethernet interface can either function as a trunk port or as an access port, but not both at the same time.

=====For more Updates Please Subscribe the Channel=====
```



## Command to configure Trunk port

1. Config terminal = first want to create vlan so get into the configuration mode.
2. Vlan 10 = this vlan 10 is the id of that vlan network. Only numbers are using to create id and that numbers are between 0 to 4095 range only.
3. Exit = this exit form the config-vlan mode.
4. Interface range fastEthernet 0/1-2 = assigning the already created vlan 10 to interface or port in switch.
5. Switchport mode access = converting the ports to access port for assigning the vlan.
6. Switchport access vlan 10 = passing the vlan 10 id for that port. That means the port allows only vlan 10 network communicate within the vlan 10 network.
7. Exit = exiting for the vlan config mode.
8. Interface fastEthernet 0/5 = selecting the port for configuring that switch port as trunk port.
9. Switchport mode trunk = changing the switch port mode to trunk port mode.
10. Switchport trunk allowed vlan 10,20 = allowing the vlan 10 and vlan 20 in that trunk port.
11. Exit = exiting from the trunk port configuration.
12. Write = write cmd is for save the configuration.
13. Show vlan brief = it show to current running configuration.



# 1. Address Resolution Protocol – ARP

In local network communication is based on MAC address. So ARP protocol is used to get the MAC address using IP address it is like routing table but not exact routing table.

Example:

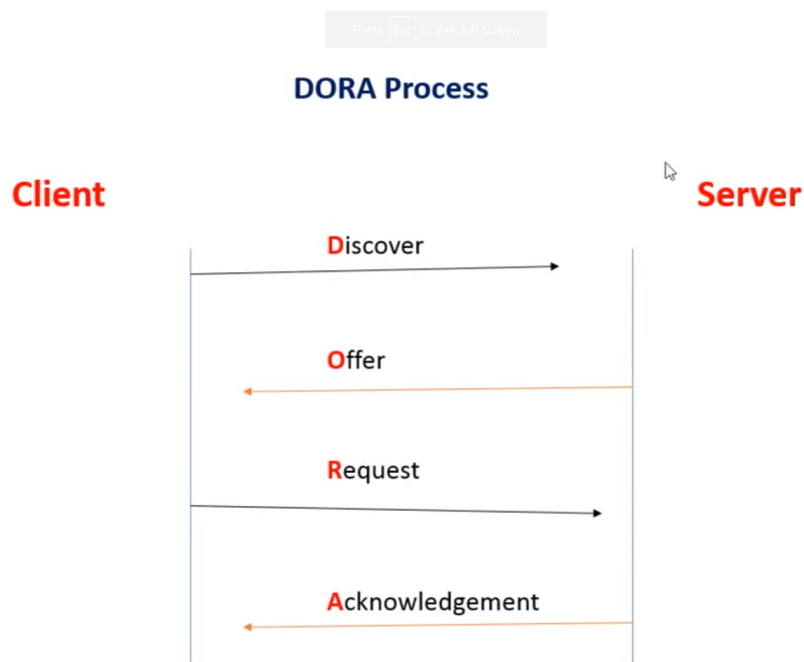
In a local network 5 computers are connected to switch. 1<sup>st</sup> computer want ping with 3<sup>rd</sup> computer. 1<sup>st</sup> computer know the 3<sup>rd</sup> computer ip address but in local network communication is based on the physical address(MAC address) so 1<sup>st</sup> computer check their arp table weather the destination MAC address is have or not. If not 1<sup>st</sup> computer want to get the MAC address of the destination computer. For that 1<sup>st</sup> computer sends the ARP message to switch in that ARP message contains source computer's IP address and MAC address and destination computer's IP address and for MAC address is don't know so source computer put FFFF:FFFF:FFFF:FFFF for broadcast. Now switch recives that ARP Message and broadcast that ARP packet to all computer in that local network. Every computer recives that broadcast packet without source. Then which computer have that exact destination IP address that computer give replay to source in that replay contains additionally add MAC address of that computer. Now source computer can get the destination computer's MAC address and save it in source computer's ( 1<sup>st</sup> computer's ARP table) then directly send that ping packet to destination computer (3<sup>rd</sup> computer) without broadcast.

Show mac address-table = switch shows the mac address-table in enable mode.

4.1 [ARP protocol working in other network](https://youtu.be/fsZBfloIEEI) = <https://youtu.be/fsZBfloIEEI>

## 5. DHCP & DORA Process

- Used to Provide Network Configuration Information's to the Clients.
  - Parameters include IP Address, Subnet mask, DNS IP, Gateway Information's.
  - Client Server Protocol.
  - Uses UDP ( User Datagram Protocol )
  - Port Number 67 for DHCP Server and 68 for DHCP Client.
  - Easy to Assign IP even for an Large Networks.
  - Reduces the load for Network Administrator
  - Uses **DORA** Process
- 



1<sup>st</sup> client broadcast the Discover. After DHCP server receives the discover message.

2<sup>nd</sup> DHCP server sent the available IP address to client before that DHCP server checks whether the IP address is being used by any other host in that network by sending the ARP message.

3<sup>rd</sup> Client receives Offer message. Client sends the Request message to DHCP server to assign the IP address to this device.

4<sup>th</sup> DHCP server getting the Request message from server. It assign the IP address to Client and DHCP server sent the Ack message to Client this IP address is assigned not only the IP address also Subnet mask address, Default gateway address and DNS address.

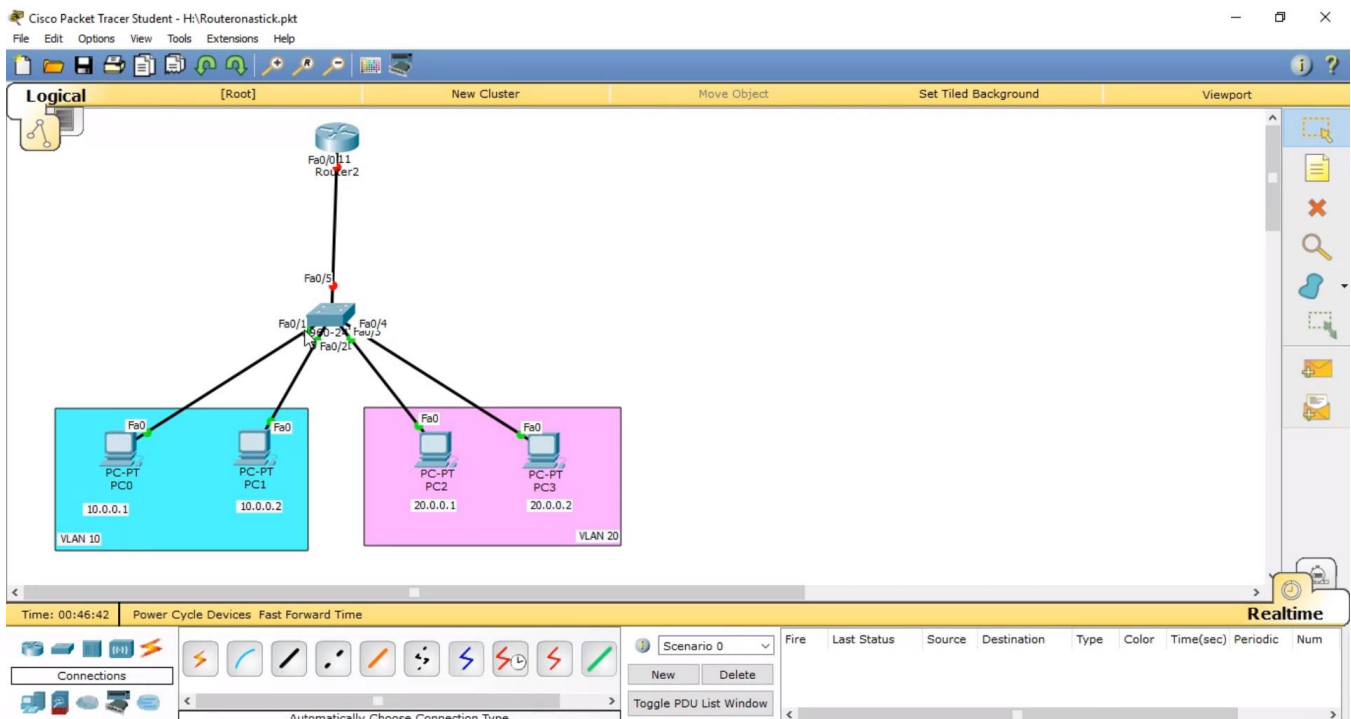
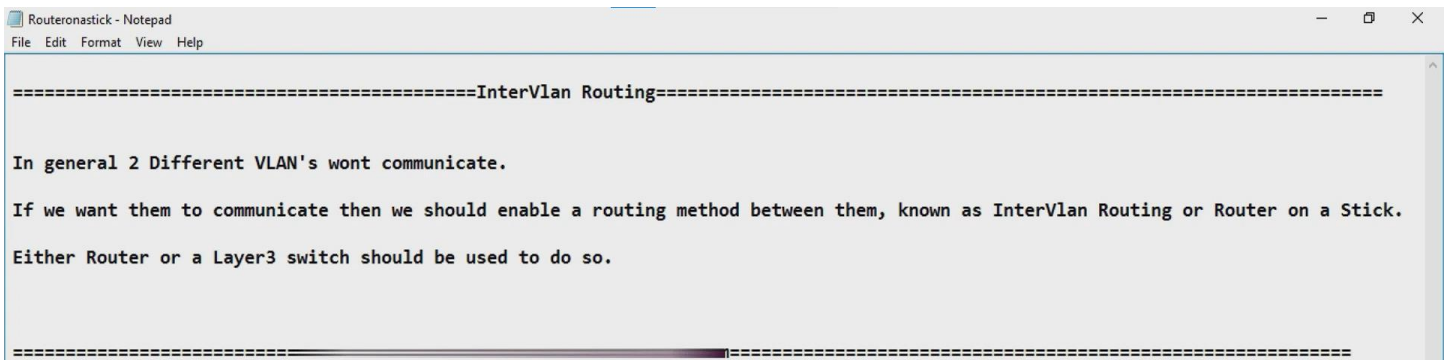
And after Client get IP address. Client also generate ARP message to check weather the recived IP address is using any other host in that network.

DHCP sever use port 67

Client use the port 68

DHCP DORA process all message are send in broadcast only.

## 6. Inter VLAN Routing or Router on Stick



# Inter VLAN routing configuration commands:

VLAN configuration and Trunk port configuration commands on page 6.

1. Enable = entering into terminal mode.
2. Configure terminal = (config)#  
[Linkup the port](#)
3. Int fastEthernet 0/0 = do configuration in fastEthernet 0/0 port so entering into that port(config-if)#.
4. No shutdown = no shutdown will linkup the connection state in logically.
5. Exit = exiting for the port configuration mode.  
[Creating the sub-interface](#)
6. Int fastEthernet 0/0.10 = physically one interface was connected, router to switch but in that switch have two VLAN (id: vlan 10, vlan 20) so creating the sub interface in router. 0/0 is the physical port number of the router, in that port creating the sub interface. .10 is the identify of the sub interface, we can give any number to identity but give the VLAN id is the best identity to easily identify the sub interface.
7. Encapsulation dot1Q 10 = to specifying that traffic is vlan 10.
8. IP address 10.0.0.50 255.255.255.0 = assigning IP address for the 0/0.10 sub interface. 10.0.0.50 is default gateway for VLAN 10. 255.255.255.0 is subnet mask of VLAN 10. Do same for VLAN 20.
9. No shutdown = to linkup the sub-interface.
10. Exit = exiting from the sub-interface of 0/0.10. Do same for VLAN 20 sub-interface.  
[checking](#)
11. Show IP route = indicates the IP address of a router that is the next hop to the remote network and the router interface on which the last update arrived.

## 7. Spanning Tree Protocol - STP

### STP : Spanning Tree Protocol

- Introduction
- Advantages
  - Broadcast Storm
  - Layer2 Loop
  - Duplicate Frames
- Components of STP
- How does STP Works ?
  - Root Bridge Election Process.
  - Root Ports selection Process.
  - Designated & Non-Designated Port selection Process.
- STP States

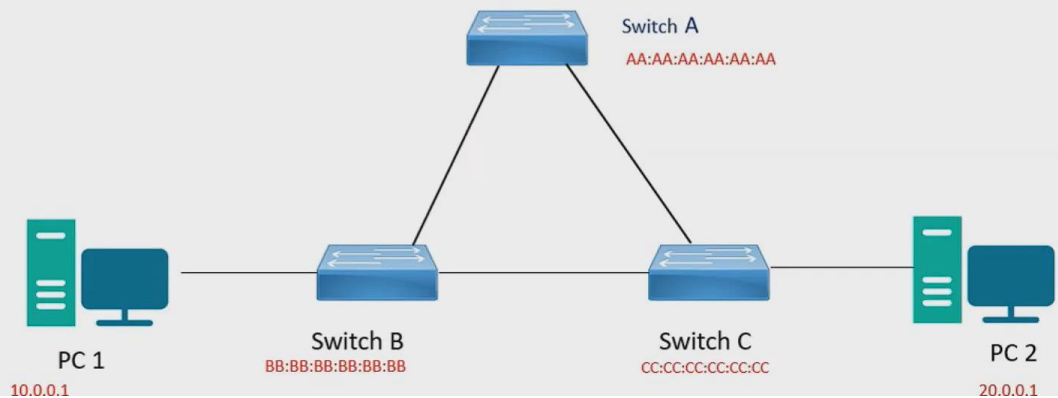
#### Introduction:

- STP – Spanning Tree Protocol
- IEEE Standard – **802.1d**
- There can be only one active link between two devices in the Layer 2 network.
- STP force the redundant link in to blocked state.
- In case of Active link goes down, It allows to use redundant link in the network to prevent network failure.
- It is designed to prevent the **Layer 2 loop** and to stop the **broadcast storm** in the network.
- It is enabled by default in all cisco catalyst switches.
- It is **slow convergence**.

Main Disadvantage is it takes 30sec. early it was over come by RSTP.

### Advantages:

- Avoid Broadcast Storm in the Layer2 network.
- Avoid Database Inconsistency.
- Avoid Duplicate and Multiple copy of data transmission.



### Broadcast Storm:

- PC 1 sends ARP packet to Switch B. Then Switch B Broadcast to all other port in Switch B except PC 1 port.
- Next that Broadcast was received to Switch A and Switch C. Now Switch A Broadcast the message again to Switch B and Switch C. Like that Switch C Broadcast the message again to Switch B and Switch A. This was done again and again like looping, this makes the Layer 2 Broadcast Storm.
- This makes network down and device reboot.

### Database Inconsistency:

- Actually PC 1 wants to reach PC 2 so that PC 1 sends the Broadcast message.
- Now this Broadcast Storm is happening so now Switch C sends the MAC address to Switch B, to reach PC 2 via Switch C and Switch A sends MAC address to Switch B, to reach PC 2 via Switch A. For this Switch B gets confuse to reach PC 2. It makes DATA Base Inconsistency.

### Duplicate and Multiple copy of data Transmission:

- Single Frame was generated in Multiple copy of data Transmission. So it makes slow down the network.



# How STP Works ?

**Step 1 → Root Bridge election.**

**Step 2 → Root Port selection.**

**Step 3 → Selecting the Designated and Non-Designated port.**

## Components of STP:

STP uses a tree like structure with a Root bridge and form a loop-free path from the Root Bridge to all the devices in the network.

### Root Bridge (RB) :

- One among the switches in the network will be selected as Root Bridge and that provides the interconnection to all other switches.
- All the other switch in the network should have a path to the Root Bridge.
- Root Bridge can be selected automatically by the STP; However, if the Network Administrator wants he can manually make any switch in the network as the Root Bridge.

### Non-Root Bridge (NRB) :

- All the other switches in the network except Root Bridge is known as Non-Root Bridge.

### Root Port:

- It is a port at the Non-Root Bridge that leads towards the Root Bridge.
- The root port will have low cost to the Root bridge.
- RB does not have any Root port.
- Every NRB will have one Root Port.

### Designated Port (DP):

- Each LAN segment will have one DP.
- Every NRB will receive the frames from the DP and forward the same through its Root Port towards the Root Bridge.
- DP is responsible for every LAN segment to be connected to the STP Tree Topology.

### BPDU:

- Bridge Protocol Data Unit.
- BPDU is a message that is exchanged between the Network devices using Spanning Tree Protocol to form a loop-free Topology.
- ❖ Configuration BPDU
- ❖ Topology change Notification (TCN) BPDU

### Path Cost:

All the Non Root Switch will reach the Root Bridge through its Root Port. The Root Port is calculated in every switch with its path cost. The port which has the lowest accumulated Path cost value to reach the Root bridge is selected as the Root Port.

Link Speed	Cost
10Gbps	2
1Gbps	4
155Mbps	14
100Mbps	19
45Mbps	39
16Mbps	62
10Mbps	100
4Mbps	250

### Step 1: Root Bridge Election:

- STP uses the **64bit Bridge ID** for the selection of Root Bridge.
- Bridge ID = **Switch Priority + MAC address**.
- Default Bridge Priority for all cisco switches is **32768** .
- Bridge Priority of a switch can be manually changed; however, it should be in the incremented or decremented of **4096** .
- The Bridge (Switch) with the **lowest Bridge ID** will be selected as Root Bridge.
- If more than one switch has same bridge ID then the device with **lowest MAC address** will be selected as Root Bridge.
- All the ports at the Root Bridge will be in **Forwarding state**.

## Step 2 : Selecting Root Port

Every Non Root switches should have at least one Root Port to reach the Root Bridge.

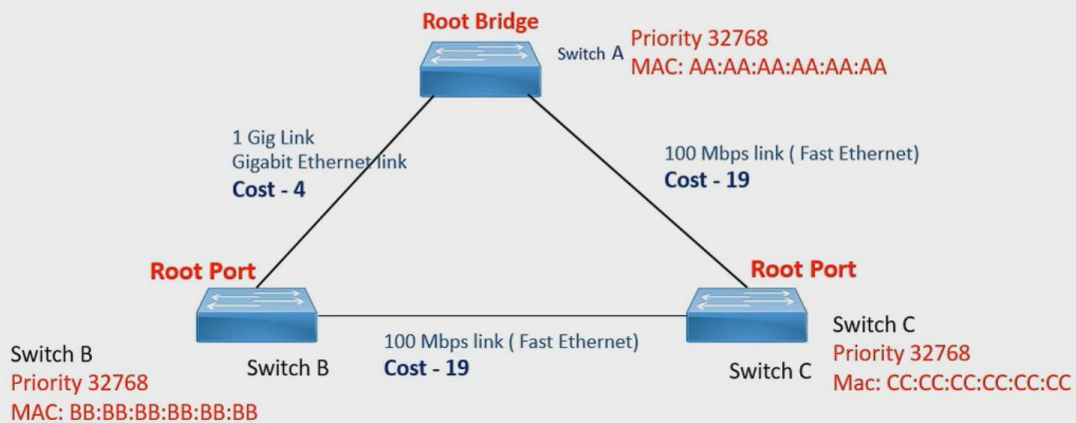
Root ports are selected based on the below for 3 different setup :

- Port that has **the lowest path cost** to reach Root Bridge.
- If **Path cost are same**, **Lowest switch ID** (Priority + MAC) of the forwarding device is preferred.
- If **Path cost and Switch ID is same**, **Lowest physical port** of the forwarding device is preferred.

Once the Root Port is selected it will be always in forwarding state.

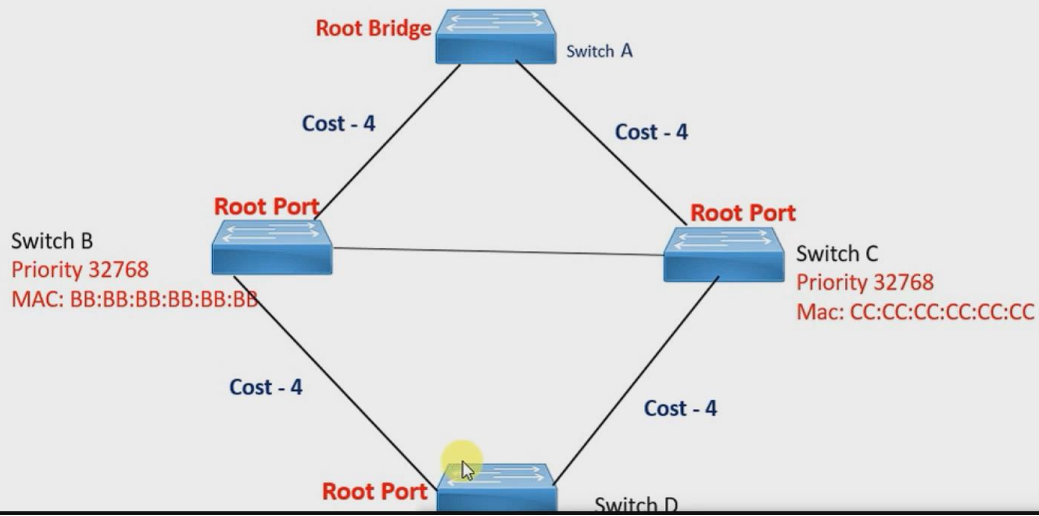
## Step 2 : Selecting Root Port

**Rule- 1 : Port that has the lowest path cost to reach Root Bridge.**



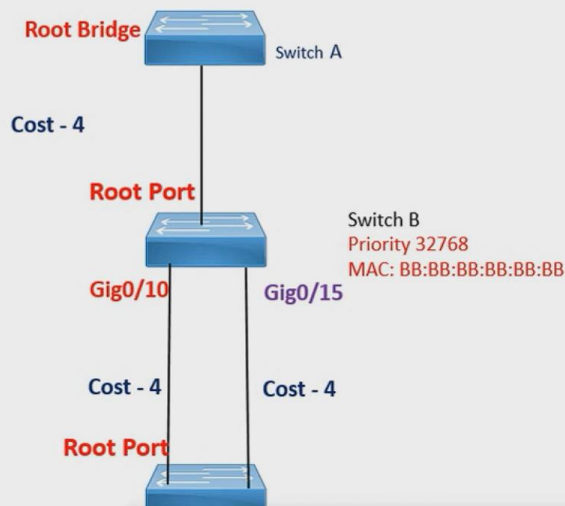
## Step 2 : Selecting Root Port

**Rule- 2 :** If Path cost are same, Lowest switch ID (Priority + MAC) of the forwarding device is preferred.



## Step 2 : Selecting Root Port

**Rule- 3 :** If Path cost and Switch ID is same, Lowest physical port of the forwarding device is preferred.

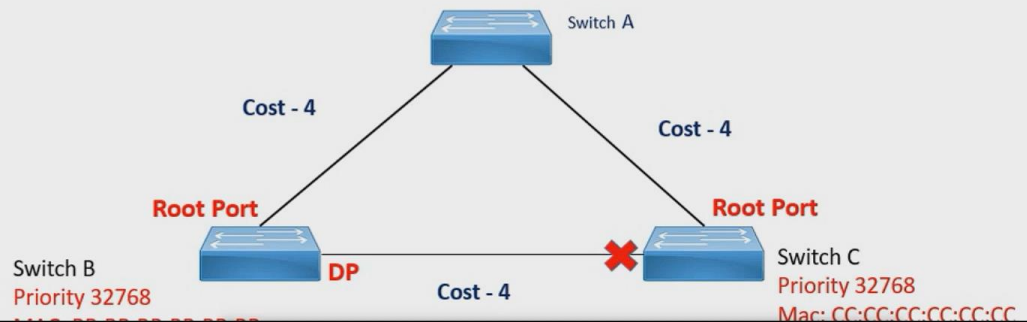


### Step 3: Selecting Designated and Non Designated Port

Designated port will be in forwarding state; however, it go through Blocking > Listening > Learning > Forwarding state step by step and Non designated ports will be in Blocking state.

Below are the selection criteria for Designated:

- Port with the **least cost**.
- Device with Least **local** switch ID (Switch priority + MAC Address) is preferred.
- If both the device has same switch ID, device that **has least port number** connected is preferred.



### States:

#### Blocking State:

- This port does not forward Ethernet frames and does not learn the MAC Address.
- Receives and process the BPDU only.
- Port will remain in Blocking state for 20 seconds before transition to Listen state.

#### Listening State:

- At this state the port listens to STP messages in the form of BPDU's and determine how the network topology is configured.
- In the listening state, the port is not forwarding frames.
- The port is in listening state for 15 seconds before transitioning to the learning state.

#### Learning State:

- The port begins to process the user frames and starts to updating the MAC address table; however, it will never forward the frames.
- Port will be in learning state for 15 seconds before transitioning to Forward port.

#### Forward State:

- Port will do the normal operations of sending and receiving the frames.

#### Disable state:

- The port will not participate in the STP operations.

