Switching

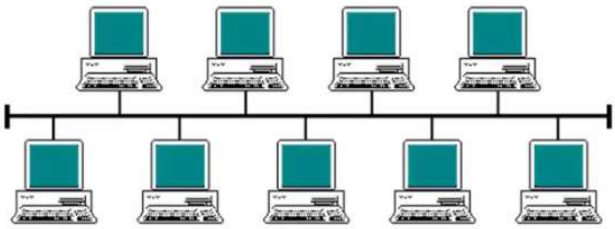
What is a Switch – A Centralized location where we can connect multiple devices .
Origin of this device .

Hub	Switch
1. It has no intelligence. 2. It always do broadcasts 3. It works with 0's and 1's (Bits) 4. It works with shared bandwidth 5. It has 1 Broadcast Domain 6. It has 1 Collision Domain.	1. Its is An Intelligent device & maintains a MAC address table. 2. It uses broadcast and Unicast 3. It works with Physical addresses (i.e. MAC addresses) 4. It works with fixed bandwidth 5. It has 1 Broadcast domain by default 6. Number of Collision domains depends upon the number of ports.

ASIC - (application-specific integrated circuit) .
[Lab : Mac address learning MAC table , ARP table] .
Broad cast domain and Collision domain .

CSMA/CD

- Carrier Sense Multiple Access /Collision Detection
- is the protocol for carrier transmission access in Ethernet networks.
- Collisions are identified using Access Methods called CSMA/CD and CSMA/CA
- CSMA/CD works in wired LAN & CSMA/CA works in wireless LAN



TEST with CD and BD examples .

Types of Switches

- **Unmanageable switches**
  - These switches are just plug and play
  - No configurations and verifications can be done
  - There is no console port.

- ***Manageable switches***
  - *These switches are also plug and play*
  - *It has console port and CLI access.*
  - *We can verify and modify configurations and can implement and test some advance switching technologies (VLAN, trunking , STP)*

Cisco's Hierarchical Design Model

Catalyst 2900

Catalyst 1900

Access Layer

1900 & 2900 (L2 switches)

Distribution Layer

3550, 3560, 3750 (L3 switches or multi-layer switches)

Cisco 3550

Core Layer

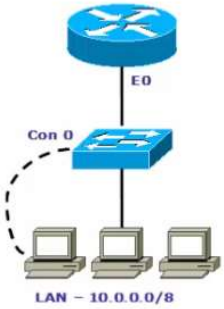
4500, 6500 (L3 switches or multi-layer switches)

4500 & 6500

Difference between Router and L3 switch .

Initial configuration of a switch:

- Console Connectivity
- Emulation Software (hyperterminal, putty, Secure CRT)



DB 9 connector or 9 Pin connector.

Basic Commands

switch>**enable**
switch# **Show running-config**
switch# **Show startup-config**
switch# **Show version**
switch# **Show flash**

switch# **Show mac-address-table**
switch# **Show interface status**

switch#**config terminal**
Switch(config)#

Passwords

TO assign telnet Password

switch(config) # **line vty 0 4**
switch(config-line) # **password <password>**
switch(config-line) # **login**

To assign Console Password

switch(config) # **line con 0**
switch(config-line) # password <password>
switch(config-line) # login

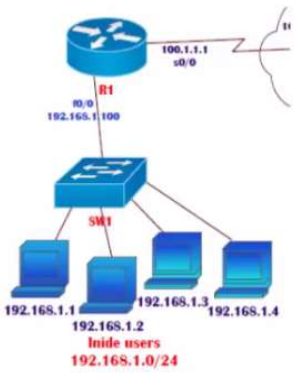
To assign Enable Password

switch(config) #**enable secret < password>**

OR

switch(config) #**enable password < password>**

Initial configuration of Switch for telnet Access



To assign IP to a Switch

```
switch(config)# Interface Vlan 1
switch(config-if)# ip address  <ip>  <mask>
switch(config-if)# no shutdown
```

To assign Default Gateway to a Switch

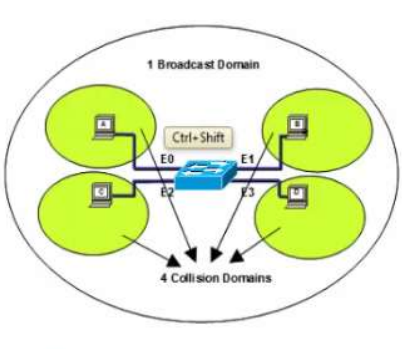
```
switch(config)# ip default-gateway 192.168.1.100
```

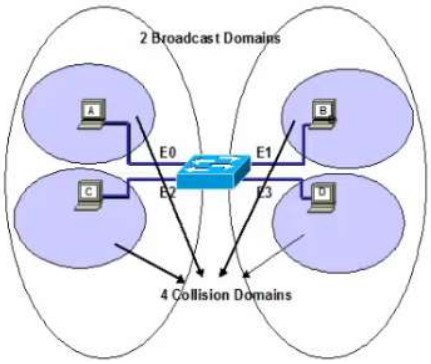
Only Reason we provide a IP address to a switch is to access that switch . Telnet access .
There are 3 conditions to access any device
1.Connectivity
2.IP address Configured on that device
3.There should be a VTY password configured .

Lab: Requirement here is , I need to access the switch from the computer 192.168.1.1

Virtual LAN

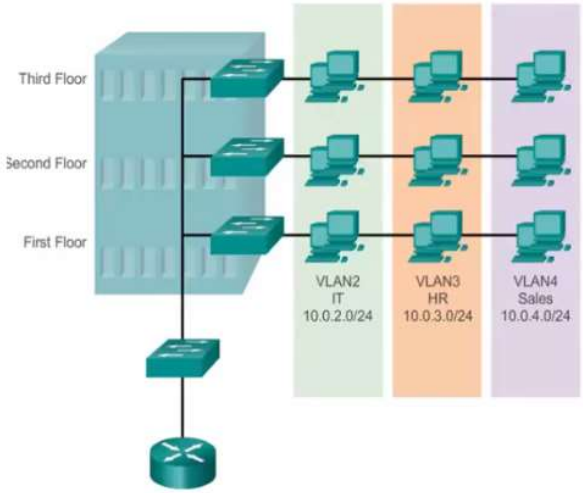
- Divides a Single Broadcast domain into Multiple Broadcast domains.
- A Layer 2 Security
- Vlan 1 is the default VLAN.
- We can create vlans from 2 – 1001
- Can be Configured on a Manageable switches only





Benefits of VLANs

- Limit the number of broadcast
- Better performance
- Security



Types of Vlans

1.Static Vlan - Based on port numbers

2.Dynamic Vlan – Based on Mac address .

Static VLAN

- Static VLAN's are based on port numbers
- Need to manually assign a port on a switch to a VLAN
- Also called Port-Based VLANs
- One port can be a member of only one VLAN

Vlan Creation :

```
Switch(config)# vlan <no>
Switch(config-Vlan)# name <name>
Switch(config-Vlan)# Exit
```

Assigning ports in Vlan

```
Switch(config)# interface <interface type> <interface no.>
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access Vlan <no>
```

Note : Can we assign multiple Vlans to same physical switch port-Access

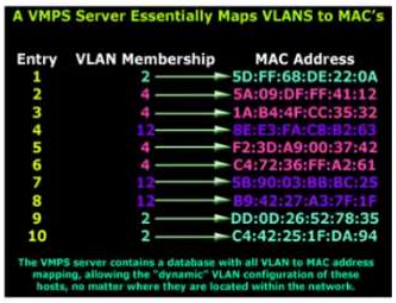
If your switch is POE then you can assign a single port to 2 VLAN

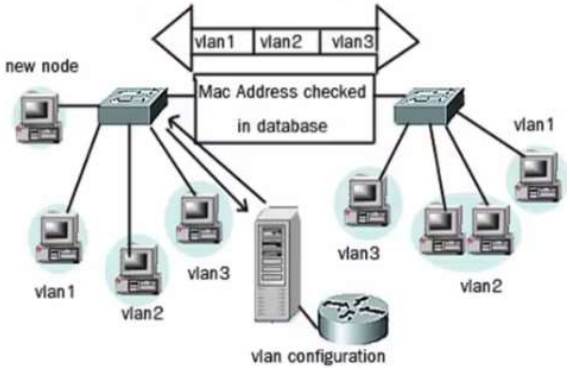
```
!
interface fa0/1
switchport mode access
switchport access vlan 2
switchport voice vlan 3
end
```

Lab Task : Create 4 vlans [Vlan 10 , 20 , 30 , 40]
Assign port 10 to Vlan 10 , Port 2 – 5 and port 8 to vlan 20

Dynamic VLAN

- Dynamic VLAN's are based on the MAC address of a PC
- Switch automatically assigns the port to a VLAN
- Each port can be a member of multiple VLAN's
- For Dynamic VLAN configuration, a software called VMPS(VLAN Membership Policy Server) is needed





.

Trunk

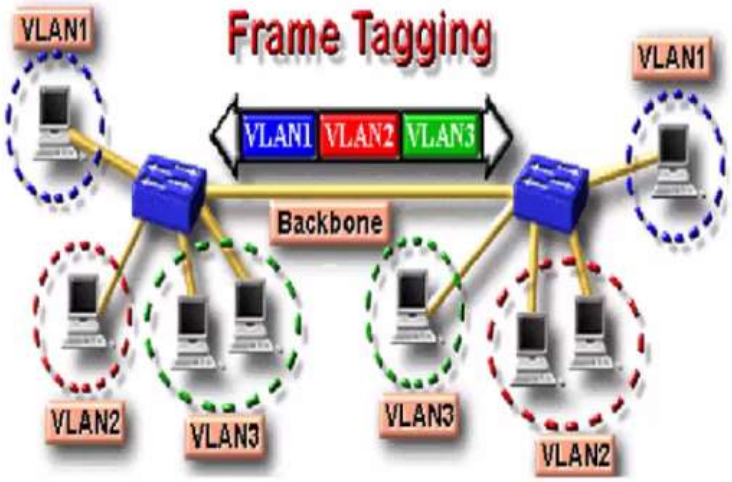
A **trunk port** is a **port** that is assigned to carry traffic for all the VLANs that are accessible by a specific switch, a process known as trunking.

Note : Show Real time Drawing

When multiple frames from different vlans are passing through the trunk how does the differentiation happens – Through Frame tagging . Who maes these tagging ?

Frame Tagging

- In oder to make sure that same vlan users on different switches communicate with each other there is a method of tagging happens on trunk links .
- Tag is added before a frame is send and removed once it is received on trunk link.
- Frame tagging happens only on the trunk links



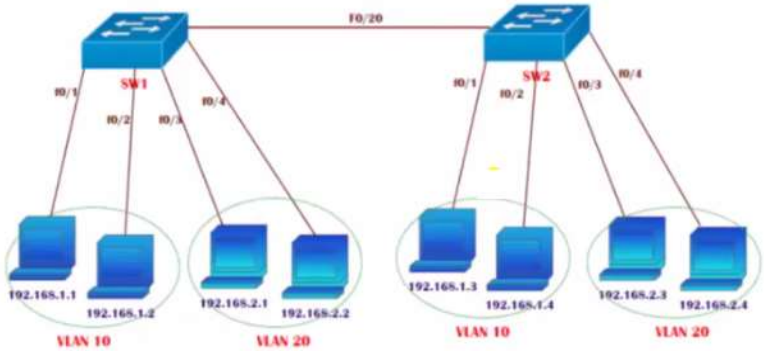
Adds tag and removes tag – at both ends of the trunk .
These tagging process is done by two protocols .

Trunking protocols

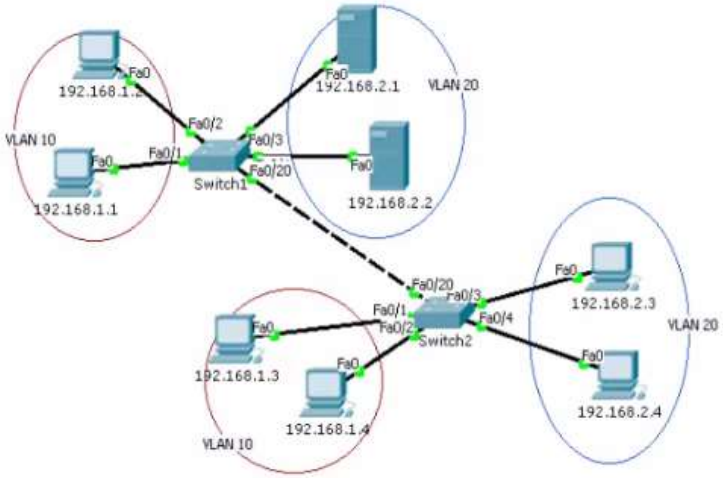
ISL	IEEE 802.1Q
• It's a Cisco proprietary	• Open standard
• It works with Ethernet, Token ring, FDDI	• It works only on Ethernet
• It adds 30 bytes of tag	• Only 4 Byte tag will be added to original frame.
• All VLAN traffic is tagged	

Trunk Configuration

Switch(config)# interface <interface type> <interface no.>
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk encapsulation dot1q/ISL



LAB : Perform Lab for Trunking . Also show it through simulator in Packet tracer .

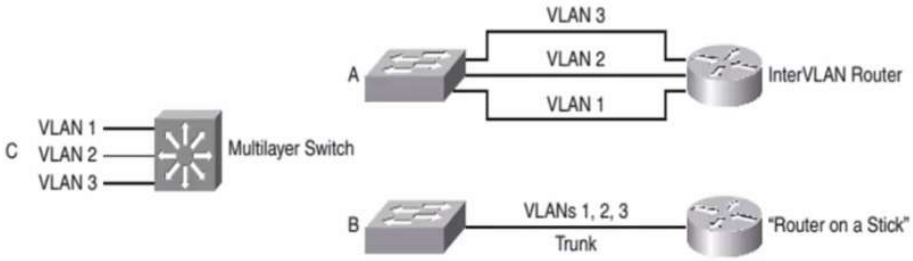


Inter Vlan Routing

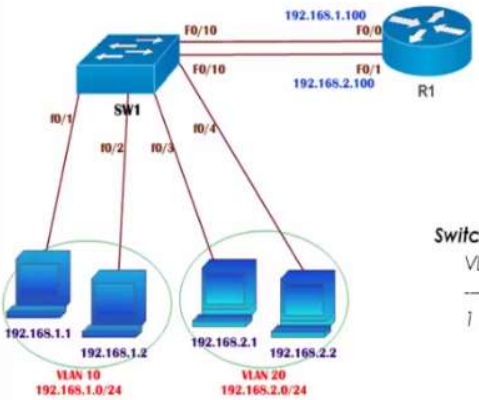
- packets in one VLAN cannot cross into another VLAN.
- To transport packets between VLANs, you must use a Layer 3 device.
- The router must have a physical or logical connection to each VLAN so that it can forward packets between them.
- This is known as inter-VLAN routing.
- Inter-VLAN routing can be performed by an external router that connects to each of the VLANs on a switch.

Inter-Vlan Routing Methods

A. Separate Physical Gateway on Router
B. Using Sub-interfaces
C. Using Layer 3 Switch



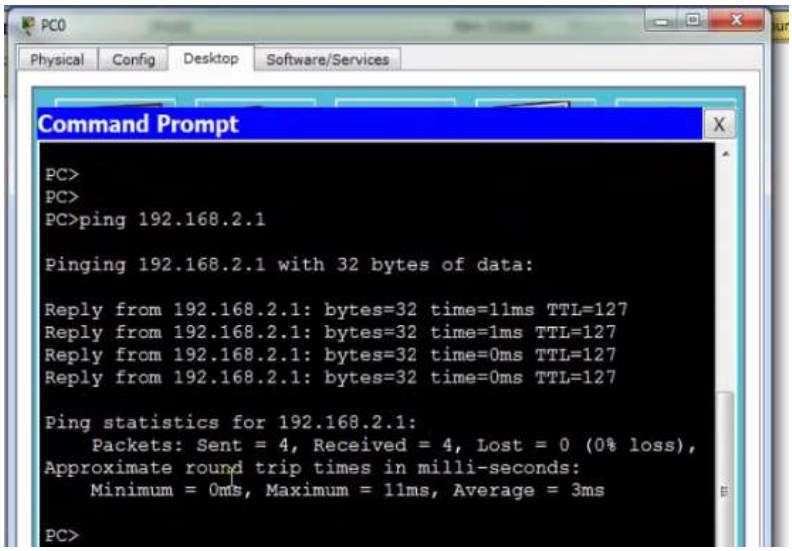
Inter-Vlan Routing using Separate Physical Gateway on Router




```
Router(config)#interface FastEthernet0/0
Router(config-if)# ip address 192.168.1.100 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit

Router(config)#interface FastEthernet0/1
Router(config-if)# ip address 192.168.2.100 255.255.255.0
Router(config-if)#no shutdown
```

```
Switch#sh vlan
VLAN Name                Status    Ports
---- ------------------- --------- -------------------------------
1    default             active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                   Fa0/9, Fa0/12, Fa0/13, Fa0/14
                                   Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                   Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                   Fa0/23, Fa0/24, Gig1/1, Gig1/2
10   sales               active    Fa0/1, Fa0/2, Fa0/10
20   marketing           active    Fa0/3, Fa0/4, Fa0/11
1002 fddi-default        act/unsup
```

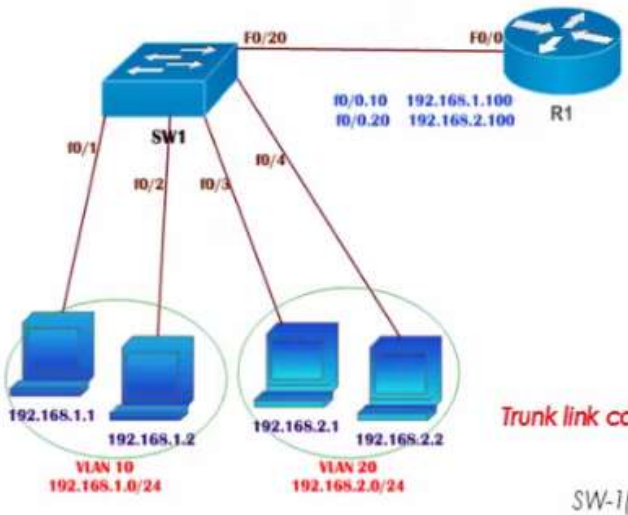


Minimum Maximum and average – Used to check Latency in real time

show tracert and traceroute .

Disadvantages in 1 st method is , for communication we need 2 separate cables as DG for 10 Vlans 10 cables cannot be used , Hence Router on a stick was found .

INTER VLAN-ROUTING USING ROUTER
(Router On Stick)



SW-1#sh vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gig1/1, Gig1/2
10	VLAN0010	active	Fa0/1, Fa0/2
20	VLAN0020	active	Fa0/3, Fa0/4

Trunk link configuration

SW-1(config) #**interface fastEthernet 0/20**

(interface facing Router)

SW-1(config-if) #**switchport mode trunk**

SW-1(config-if) #**switchport trunk encapsulation dot1q**

Router configuration .

Creating sub interfaces on router interface f0/0

R-1(config) #**int fa0/0**
R-1(config-if) # **no shutdown**
R-1(config-if) # **exit**

R-1(config) #**int fa0/0.10**
R-1(config-sub-if) # **encapsulation dot1Q 10**

It should be the exact vlan no (vlan 10)

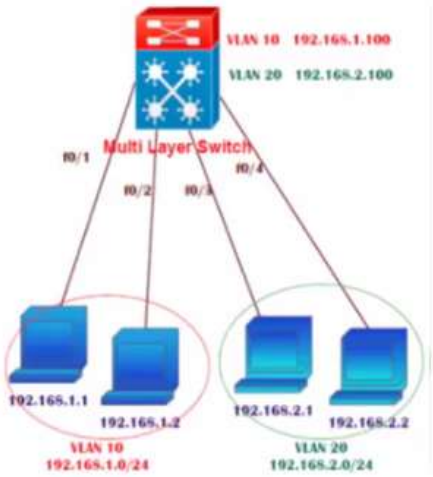
R-1(config-sub-if) # **ip add 192.168.1.100 255.255.255.0**
R-1(config-sub-if) # **exit**

R-1(config) #**int fa0/0.20**
R-1(config-sub-if) # **encapsulation dot1Q 20**

It should be the exact vlan no (vlan 20)

R-1(config-sub-if) # ip add 192.168.2.100 255.255.255.0

Inter Vlan-Routing Using MLS



SW-1#sh vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gig1/1, Gig1/2
10	VLAN0010	active	Fa0/1, Fa0/2
20	VLAN0020	active	Fa0/3, Fa0/4

```
Switch(config)#int vlan 10
Switch(config-if)#ip address 192.168.1.100 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit

Switch(config)#int vlan 20
Switch(config-if)#ip address 192.168.2.100 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
```

Switch # sh ip int brief

"IP ROUTING" – Important .
So here we using something called SVI Switch Virtual Interface similar to DG for each Vlan .

Extended Vlan
Voice Vlan

Normal VLAN:

Normal VLANs range are VLANs **1-1005**. Normal range VLANS can be configured in both database configuration mode and global configuration mode and are stored in **vlan.dat** file in Flash memory. VTP versions 1 and 2 can advertise normal range VLANs only.

Extended VLANs:

Extended VLANs are VLANs that fall in the range **1006 to 4094**. They are mainly used in service provider networks to allow for the provisioning of large numbers of customers. Extended VLAN differ from normal VLANs because they have higher numbers. Extended VLANs must be configured in VTP transparent mode. Extended VLANs are saved to the running-config.

Voice VLAN:

A voice VLAN enables the access port to carry IP voice traffic from an IP phone. By default, the voice VLAN is disabled. When enabled, all untagged traffic is sent according to the default CoS priority of the port.

NOTE: Extended Vlan are store in Running configuration but normal Vlan is stored in Flash .

Description	Commands
Verify VLAN database vlan.dat	SW# show flash OR dir flash
Verify VLAN creation	SW# show vlan brief OR show vlan
Check VTP mode and status	SW# show vtp status
Configure a Voice VLAN	SW(config)#vlan 5 SW(config-vlan) # name VOICE SW(config)#interface f0/4 SW(config-if)#switchport voice vlan 5
Verify switchport Configuration	SW# show interface f0/4 switchport

Extended VLAN

- Historically, Cisco Catalyst switches have supported only up to 1024 VLANs
- ISL uses 10-bit VLAN ID (upto 1024 Vlan)
- 802.1Q includes a 12-bit VLAN ID field (upto 4096 vlan)
- Cisco refers to the VLANs between 1025 and 4096 as extended-range VLANs.

We can create Vlan from 2- 1001 which is called as Ethernet vlans.
1002 – 4096 We call it as Extended Vlan

NOTE : For using Extended the Hardware feature should support it first , Then to enable we should use this command "Switch(config)#**spanning-tree extend system-id**" , Meaning we should enable the extend system-id feature only then we can create Extended Vlan

NOTE : Catalyst was a company which produced switches and which was bought by Cisco. Cisco has sold that series of switches formerly sold by that company named catalyst as catalyst switches. Nowadays, Cisco has also some switches, that are develoed by Cisco itself, for example Nexus switches. Calalyst switches are switches belonging to that old series of switches and switches developed on the base of those switches (for example catalyst 2960 series, catalyst 4500 series, catalyst 6500 series). For catalyst switches, CatOS and IOS are available (for newer models like 2960 only IOS). Nexus switches have a different architecture. The operating system of Nexus switches is not IOS anymore, it's NXOS.

Basic pre-requsite for Extended vlans .

1.

Cisco Catalyst switches support extended-range VLANs under the following restrictions:

VTP cannot be used for VLAN management. (VTP must be configured in transparent mode or off

```
SW7(config)#vtp mode server
Setting device to VTP Server mode for VLANS.

SW7(config)#vlan 4000
SW7(config-vlan)#name sales
SW7(config-vlan)#exit
% Failed to create VLANs 4000
Extended VLAN(s) not allowed in current VTP mode.
%Failed to commit extended VLAN(s) changes.
```

```
SW1(config)#vtp mode ?
 client      Set the device to client mode.
 off         Set the device to off mode.
 server      Set the device to server mode.
 transparent Set the device to transparent mode.
```

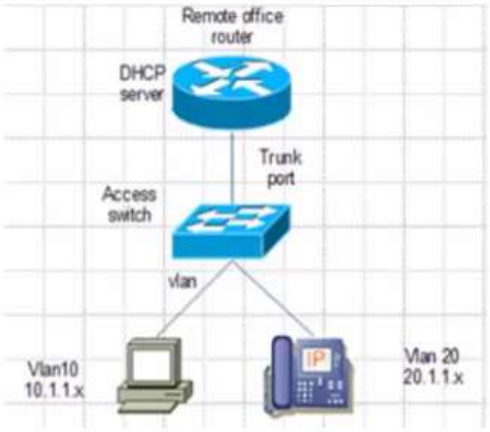
2.

Spanning tree extended ID feature must be enabled , However by default in most of the switches this feature is enabled by default .

“Show spanning ree summary” .

Voice VLAN

- voice VLAN feature enables access ports to carry IP voice traffic from an IP phone.
- switch can connect to IP Phone to carry IP voice traffic
- The Cisco IP Phone contains an integrated three-port 10/100 switch



NOTE: Two ports can be a part of two vlans only when it is a Voice vlan ,

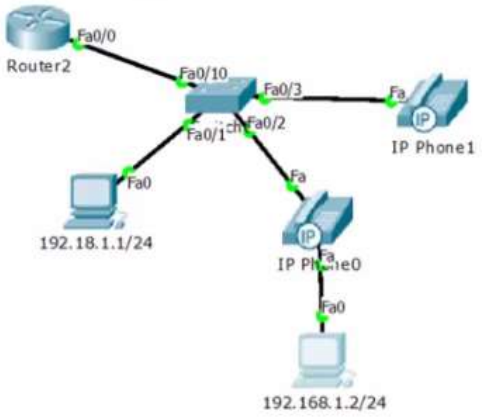
Configuring Voice VLAN (contd)

Assign Ports connecting to PC to Datav lan and IP phones to Voice VLAN

```
Switch(config)#int f0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit

Switch(config)# int f0/3
Switch(config-if)#  switchport mode access
Switch(config-if)#switchport voice vlan 50
Switch(config-if)#exit
```

```
Switch(config)#int f0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#switchport voice vlan 50
Switch(config-if)#end
```

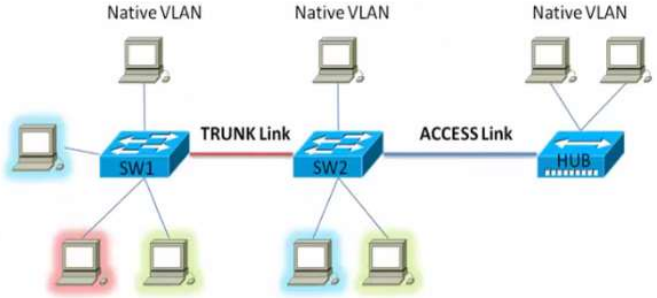


Default VLAN configuration :

- The voice VLAN feature is disabled by default.
- You should configure voice VLAN on switch access ports.
- The voice VLAN should be present and active on the switch for the IP phone to correctly communicate on the voice VLAN.
- Use the show vlan privileged EXEC command to see if the VLAN is present
- The Port Fast feature is automatically enabled when voice VLAN is configured.

Native VLAN

- If a packet is received on a dot1q link, that does not have VLAN tagged, it is assumed that it belongs to native VLAN.
- Default native vlan is VLAN 1

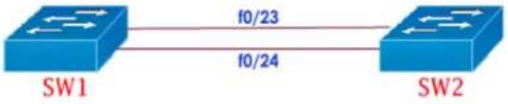


Native VLAN best Practices

- Best Practice is to configure the Native VLAN ID to VLAN 666 and to ensure that this VLAN is not used anywhere in the network.
- No ports should be assigned to the native vlan
- An attacker who attempts to use the VLAN hopping attack will end up in a dead VLAN that has no hosts to leverage.

Native VLAN Configuration

SWx(config)#**vlan 999**
SWx(config-vlan)#**end**



SWx(config)#**int f0/20**
SWx(config-if)#**switchport mode trunk**
SWx(config-if)#**switchport trunk native vlan 999**

For Cisco switches the Native VLAN ID must match on both end of the trunk.

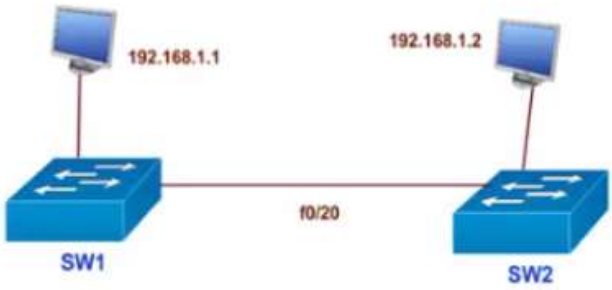
This message appears when the native VLAN is mismatched on the two Cisco switches:

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/20 (1), with SW1 FastEthernet0/20 (999).

SW-1#sh interfaces trunk

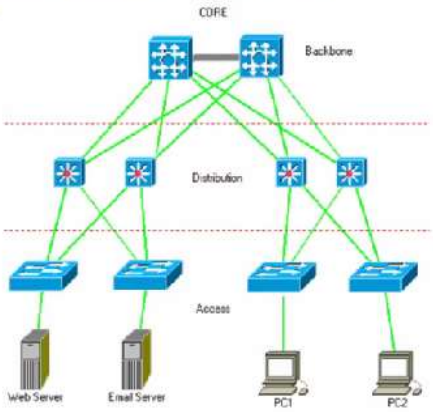
Port	Mode	Encapsulation	Status	Native vlan
Fa0/20	on	802.1q	trunking	999

SW1#sh interfaces f0/20 switchport
Name: Fa0/20
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 999 (VLAN0999)
Voice VLAN: none



VLAN TRUNKING PROTOCOL

- VTP is a CISCO proprietary protocol
- used to share the VLAN configurations with multiple switches and to maintain consistency throughout that network.



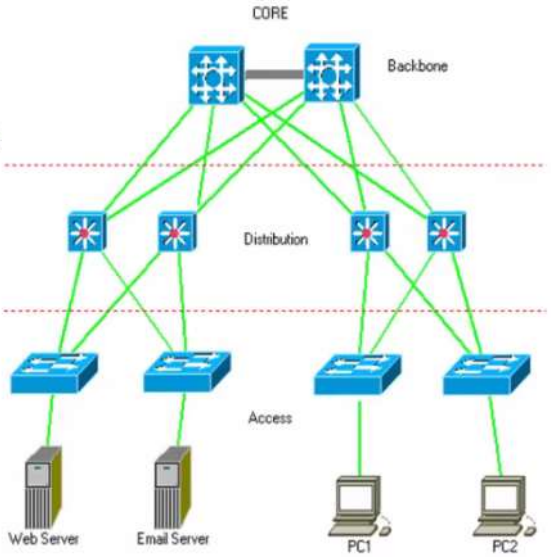
Create , Modify and delete – If we have to do these three things can be done from server switch itself that's the feature of VTP

VTP

- VTP manages the addition, deletion, and renaming of VLANs across the network from a central point of control.
- Information will be passed only if switches connected with Fast Ethernet or higher ports.
- Also must be trunk links

Note:

- Switches Should be configure with same Domain.
- Domain are not Case sensitive.

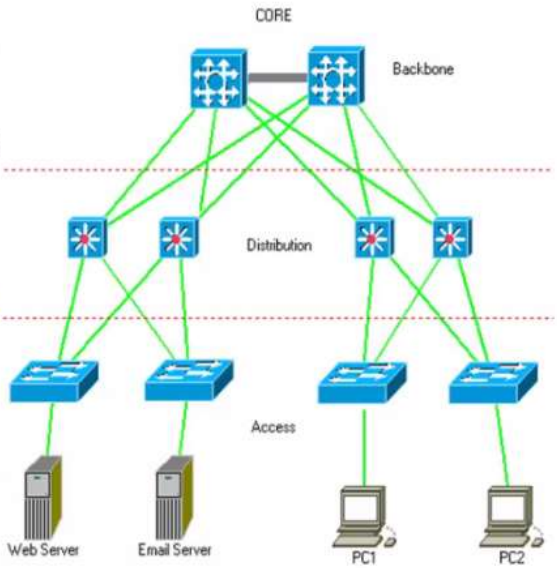


VTP

- VTP manages the addition, deletion, and renaming of VLANs across the network from a central point of control.
- Information will be passed only if switches connected with Fast Ethernet or higher ports.
- Also must be trunk links

Note:

- Switches Should be configure with same Domain.
- Domain are not Case sensitive.



Server Mode

- Default mode
- Creates, modifies, and deletes VLANs
- Synchronizes VLAN configurations
- Sends and forwards advertisements
- Saves configuration in NVRAM

Client Mode

- cannot Add , Modify and Delete its VLAN configurations
- Doesn't store its VLAN configuration information in the NVRAM. Instead , learns it from the server every time it boots up
- Forwards advertisements
- Synchronizes VLAN configurations
- Do not save in NVRAM

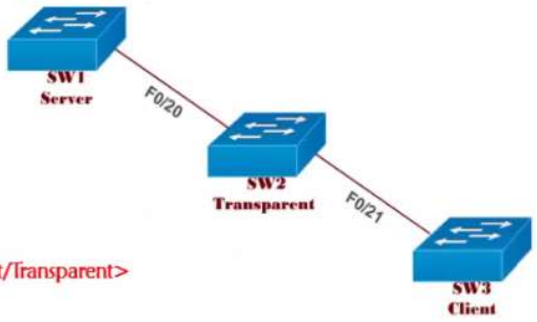
Transparent Mode

- can Add , Modify and Delete VLAN configurations.
- Does not synchronize VLAN configurations
- Forwards advertisements
- Saves configuration in NVRAM

Transparent will not send any information but it will forward the information.

In this lab the pre-requisite is Trunking . Password is Optional ,"VTP domain CCIE" – Will enable VTP , difference between Version 1 and 2 – 2 is much secure than 1 and Token will be added in 2 .

Configuring VTP



Switch(Config)# VTP domain CCIE
Switch(Config)# Vtp password cisco123
Switch(Config)# Vtp version 2
Switch(Config)# Vtp mode <server/Client/Transparent>

SW1#sh vtp status
SW1#sh vtp password

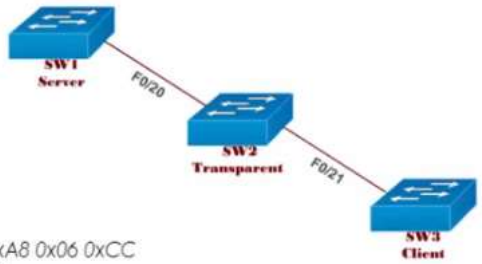
- VTP is off by default
- VTP once enabled uses version 1 only

If a switch with a highest revision number is added to the above topology the vlan database will be changed . Question here is what will happen if a new switch with same revision number is added to the above topology .

Configuration Revision Number

- VTP switches use an index called the VTP configuration revision number to keep track of the most recent information.
- The VTP advertisement process always starts with configuration revision number 0 (zero).
- When subsequent changes are made on a VTP server, the revision number is incremented before the advertisements are sent.

```
SW-3#sh vtp status
        VTP Version                     : 2
        Configuration Revision          : 2
        Maximum VLANs supported locally : 255
        Number of existing VLANs        : 5
        VTP Operating Mode              : Client
        VTP Domain Name                 : CCNP
        VTP Pruning Mode                : Disabled
        VTP V2 Mode                     : Enabled
        VTP Traps Generation            : Disabled
        MD5 digest                      : 0x86 0x22 0x83 0x8E 0x23 0xA8 0x06 0xCC
        Configuration last modified by 0.0.0.0 at 3-1-93 00:07
```



Before Adding a Switch to an Existing VTP Domain , Ensure a new switch has VTP revision is 0 before adding it to a network.

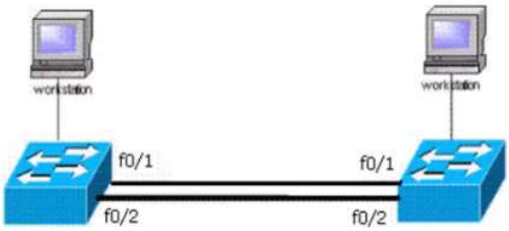
- Change the switch's **VTP mode to transparent** and then change the mode **back to server.**
- Change the **switch's VTP domain** to a bogus name (a nonexistentVTP domain), and then change the VTP domain back to the original name.
- **Delete Vlan.dat file** inside the Flash and reload

Spanning tree protocol

Bridging loops

Redundant link between switches provides redundancy.
Also possibility to create loops when switches do broadcasts.

1. Broadcast storms
2. Mac-table instability
3. Multiple frame transmissions



Solution

1. Only one link between switches (no redundancy)
2. Shutdown extra link temporarily
   1. Manually (shutdown command)
   2. Automatically block extra links (done by STP)

- STP stop the loops which occurs when you have multiple links between switches
- STP stops avoiding Broadcast Storms, Multiple Frame Copies & Database instability.
- STP is a open standard (IEEE 802.1D)
- STP is enabled by default on all Cisco Catalyst switches

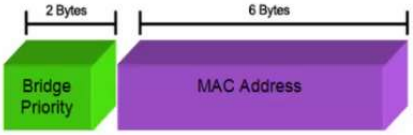
STP was initially found by “digital equipment co-operation” later made as a standard.

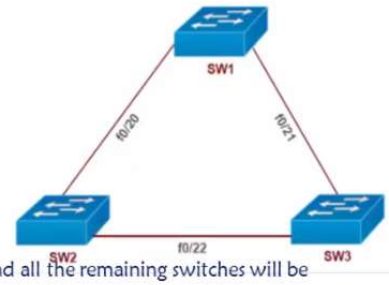
How STP works

1. Selecting the Root Bridge
2. Selecting the Root Port
3. Selecting Designated port & Non Designated port

1) Selecting the Root Bridge

- The bridge with the Best (Lowest) Bridge ID.
- Bridge ID = Priority + MAC address of the switch
- Out of all the switches in the network, one is elected as a root bridge that becomes the focal point in the network.





- Every LAN will have only one Root Bridge and all the remaining switches will be considered as Non-root Bridges.

Default Priority – 32786 . If priority is same then the tie breaker will be Mac Address .
Show version – Base mac address . Only One root bridge , remaining non root bridges , BPDU will pass bridge ID information with all .

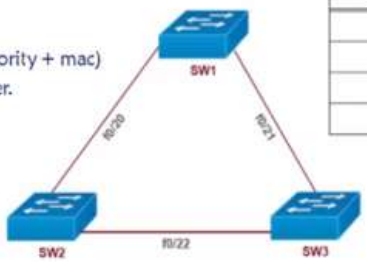
Note:Least is always preferred in Spanning tree .
****
SW1(config)#spanning-tree vlan 1 priority 1
% Bridge Priority must be in increments of 4096.
% Allowed values are:
0 4096 8192 12288 16384 20480 24576 28672
32768 36864 40960 45056 49152 53248 57344 61440
SW1(config)#
****

2) Selecting the Root Port:

- Shortest path to the Root bridge
- Every Non-root Bridge looks the best way to go Root-bridge

1. least cost (Speed)
2. The Lowest forwarding Switch ID (priority + mac)
3. Lowest forwarding Physical Port Number.

- For every non-root bridge there is only one root port.

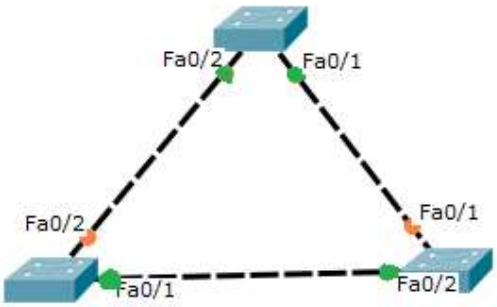


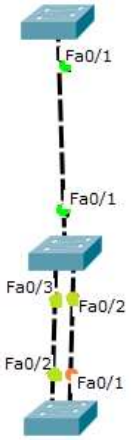
STP Port Cost

Link Speed(Bandwidth)	Port Cost
10 mbps	100
100 bmps	19
1 gbps	4
10 gbps	2

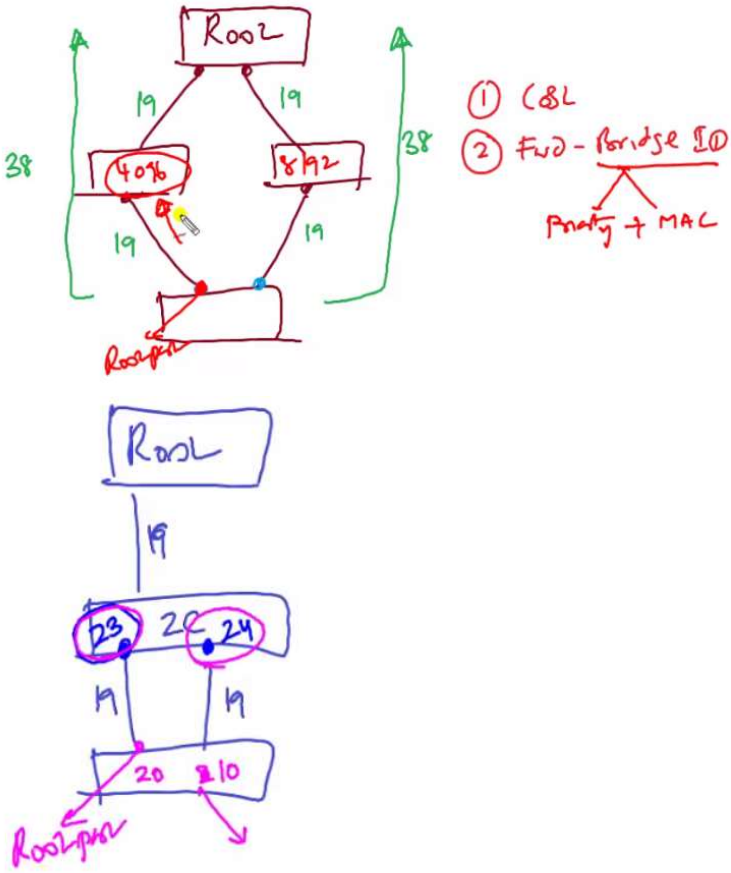
Lowest cost – Highest Bandwidth .

1. Lowest Cost
   If tie in the cost





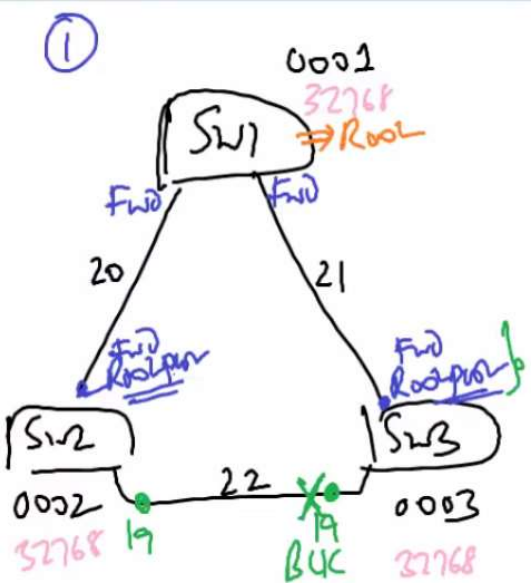
Root port = fa 0/1
Bcoz f0/2 is lowest than Fa 03



2. Lowest Forwarding Bridge ID = Priority + Mac address .
   When Priority is same then Lowest Mac address .

3. IF there is Tie in the mac address then it will see the “forwarding uplink Port number” . Note: It will not see the Local Port numbers .

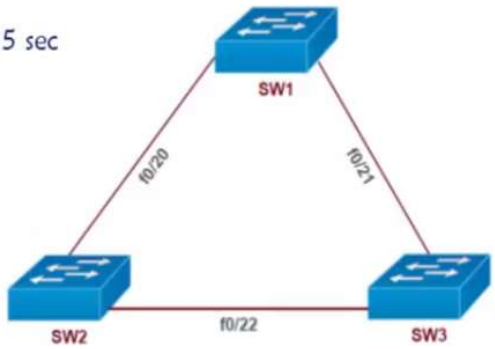
Now to Find out the blocking ports and Forwarding ports , All ports connecting to Root bridge will be forwarding , and all root ports will be in forwarding , the left over ports will decide the BLK port[non designated port] and designated Port .



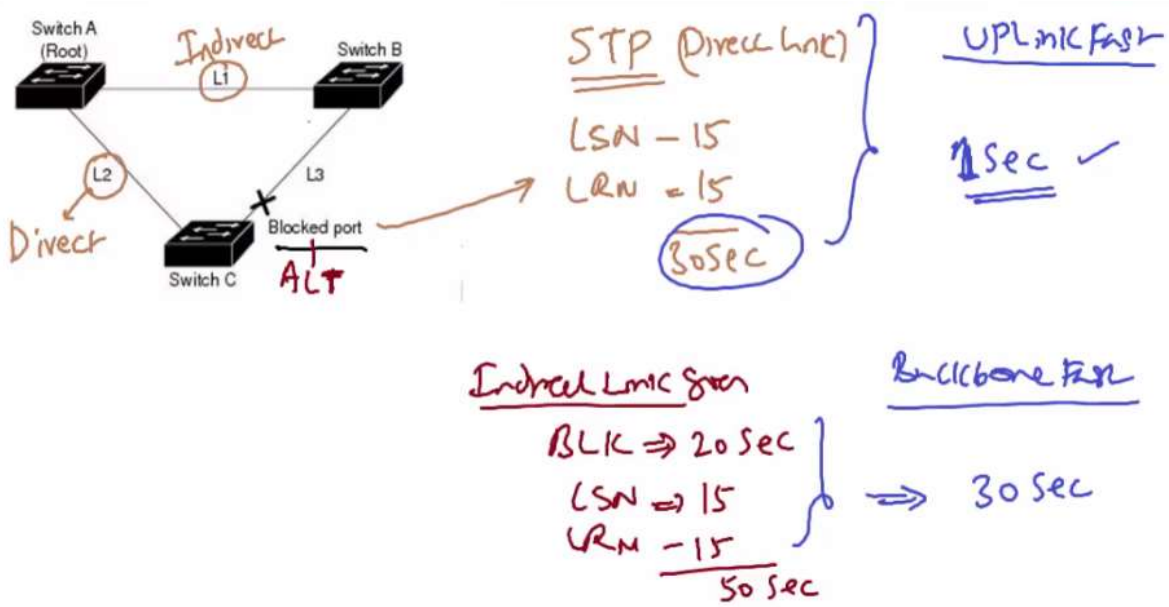
1. Lowest cost
2. Local – Bridge ID = Priority + Mac address
3. Local Port Numbers .

BPDU

- All switches exchange information through what is called as Bridge Protocol Data Units (BPDUs)
- Hello = BPDUs are sent every 2 sec
- Max age(dead)= 20 sec
- Forward Delay (listening/learning time) = 15 sec



RSTP – Combination of Port fast , Uplink fast and Backbone fast .
Port fast –Any device connected to switch it takes 30 seconds , As it goes to LSN and LRN state – Once portfast enabled it will take 1 sec time .
Uplink fast – If any direct link goes down , The BLK takes 30 sec time to come up but when Uplink fast is enabled it will take only 1 – 5 second
Backbone fast – If any Indirect link goes down– 50 sec --→ 1 sec



When RSTP is enabled if any indirect link / Direct Link goes down it will send TCN [Topology change notification] and 1 sec it will come up .

TOPIC 10 - Securing a switch

10.1 Configuring Port Security

Port security is a layer two traffic control feature on **Cisco** Catalyst switches. It enables an administrator configure individual switch **ports** to allow only a specified number of source MAC addresses ingressing the **port –** Mac flooding .

NOTE:

1. Port security is disabled by default. **switchport port-security** command is used to enables it.
2. Port security feature does not work on three types of ports.
   Trunk ports
   Ether channel ports
   Switch port analyzer ports
3. Port security work on host port. In order to configure port security we need to set it as host port. It could be done easily by *switchport mode access* command.

Switchport port-security Voilation modes

1.
2.
3.

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security ?
mac-address          Secure mac address
maximum     Max secure addresses
violation       Security violation mode

Switch(config-if)#switchport port-security mac-address ?
H.H.H                48 bit mac address
sticky               Configure dynamic secure addresses as sticky
Switch(config-if)#switchport port-security maximum ?
<1-132>       Maximum addresses

Switch(config-if)#switchport port-security violation ?
protect         Security violation protect mode
restrict        Security violation restrict mode
shutdown     Security violation shutdown mode
```