

From
Basic Concepts
to
Advanced
Topics

Switching Fundamentals CCNA to CCIE

Complete Guide with Diagrams, Concepts and Real-World Examples

- MAC Address
- Switching
- VLAN
- Trunk & Access
- STP
- EtherChannel
- Inter-VLAN Routing



- Port Security
- DHCP Snooping
- Dynamic ARP Inspection
- STP Enhancements
- High Availability
- Troubleshooting
- Real-World Scenarios



PC 1
VLAN 10
192.168.10.10



PC 2
VLAN 10
192.168.10.11



PC 3
VLAN 20
192.168.20.10



PC 4
VLAN 20
192.168.20.11



Switching
Concepts



VLAN
and Trunking



Spanning Tree
Protocol (STP)



EtherChannel
(Link Aggregation)



Switch Security
Features



Troubleshooting
& Best Practices



Real-World Examples
and Interview Questions



Perfect for CCNA, CCNP, CCIE
and Network Engineers

1/10

Swipe Next



LEARN
ANYTIME



CLEAR
CONCEPTS



REAL
EXAMPLES



CCNA TO CCIE
LEVEL



BUILD
REAL SKILLS

Follow
@Technetworkk
For More



A switch is a Layer 2 device that forwards frames based on MAC address

A switch learns the MAC address of devices connected to its ports and forwards the data only to the destination port (unlike a hub which floods to all ports).

1 Key Points about Switch

- ✓ Operates at Layer 2 (Data Link Layer) by default.
- ✓ Forwards frames based on MAC address.
- ✓ Learns source MAC address automatically (MAC address table).
- ✓ Builds a MAC address table dynamically.
- ✓ Sends data only to the destination port (unicast).
- ✓ Floods frames for unknown destination (broadcast/unknown unicast).
- ✓ Each port is a separate collision domain.
- ✓ Supports multiple features like VLAN, STP, EtherChannel, Port Security etc.

3 Switch vs Hub (Difference)

Feature	Switch	Hub
OSI Layer	Layer 2	Layer 1
Forwarding	Based on MAC address	Floods to all ports
Intelligence	Learns MAC address	No learning
Collision Domain	Separate per port	Single (all ports)
Bandwidth Usage	Efficient	Less efficient
Performance	High	Low
Security	More secure	Less secure

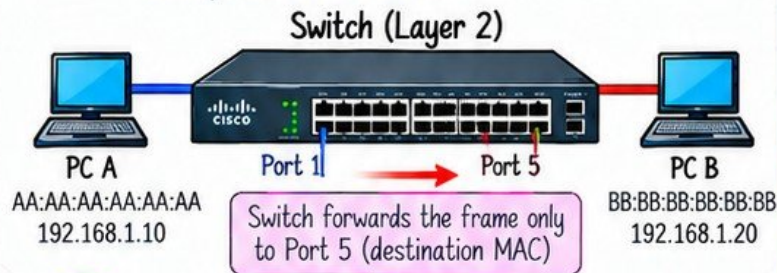
5 MAC Address Table Example

VLAN	MAC Address	Port	Type
1	AA:AA:AA:AA:AA:AA	Fa0/1	Dynamic
1	BB:BB:BB:BB:BB:BB	Fa0/2	Dynamic
1	CC:CC:CC:CC:CC:CC	Fa0/3	Dynamic

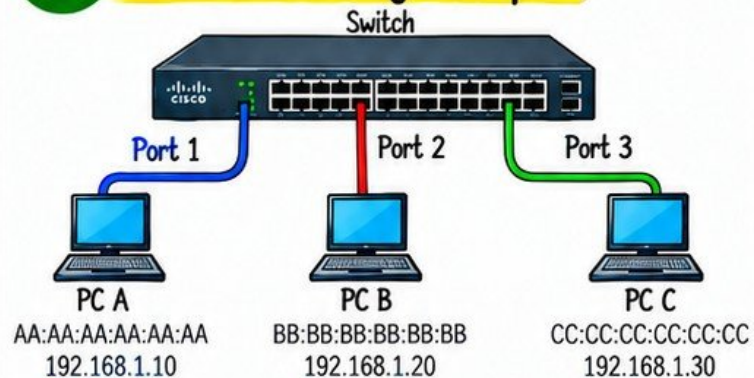
The switch automatically learns source MAC addresses and updates this table. Entries are removed after an aging time (default 300 seconds on Cisco).

2 How a Switch Forwards a Frame?

- 1 Host A sends a frame to Host B.
- 2 Switch checks the destination MAC address in its MAC address table.
- 3 If MAC is known → forwards to the correct port.
- 4 If MAC is unknown → floods the frame to all ports (except the incoming port).
- 5 Switch also learns the source MAC address and updates its MAC table.



4 Switch Working Example



6 Important Terms

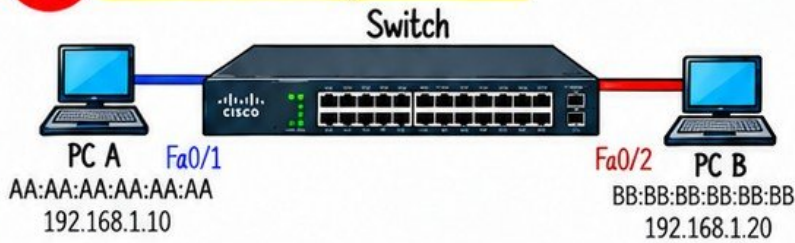
- ✓ Frame : Layer 2 data unit.
- ✓ MAC Address : Unique hardware address (48-bit).
- ✓ MAC Table : Stores MAC address to port mapping.
- ✓ Unicast : Frame to a single destination.
- ✓ Broadcast : Frame to all devices (FF:FF:FF:FF:FF:FF).
- ✓ Unknown Unicast : Destination MAC not in table (flooded).
- ✓ Collision Domain : Each port is a separate collision domain.
- ✓ VLAN : Logically separates a network into multiple broadcast domains.

3. MAC Address Table

How a Switch Learns and Maintains MAC Addresses

A switch builds a MAC address table by learning the source MAC address of incoming frames and mapping it to the port on which the frame was received.

1 MAC Learning Process



- 1 PC A sends a frame to PC B (destination MAC: BB:BB:BB:BB:BB:BB).
- 2 Switch learns the source MAC (AA:AA:AA:AA:AA:AA) on Fa0/1.
- 3 Since destination MAC is unknown, it floods the frame to all other ports.
- 4 PC B receives the frame and replies.
- 5 Switch learns the source MAC (BB:BB:BB:BB:BB:BB) on Fa0/2.
- 6 Now the switch forwards frames between PC A and PC B only on the correct ports.

2 MAC Address Table Example

VLAN	MAC Address	Port	Type	Age (sec)
1	AA:AA:AA:AA:AA:AA	Fa0/1	Dynamic	0
1	BB:BB:BB:BB:BB:BB	Fa0/2	Dynamic	0
1	CC:CC:CC:CC:CC:CC	Fa0/3	Dynamic	120
1	DD:DD:DD:DD:DD:DD	Fa0/4	Dynamic	250



- Entries are learned dynamically.
- Age timer is 300 seconds by default (Cisco).
- If no traffic is seen for 300 seconds, the entry is removed.
- MAC table is per VLAN.

3 Forwarding Decision Based on MAC Table

Known Destination

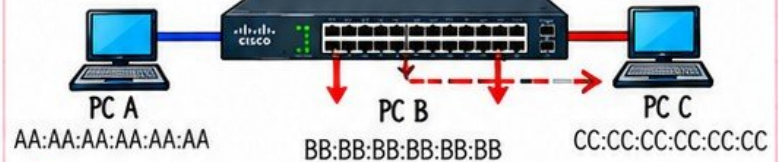
Switch



- ✓ If destination MAC is in table, frame is forwarded only to the specific port.
- ✓ Saves bandwidth and improves performance.

Unknown Destination

Switch



- ✓ If destination MAC is not in table, frame is flooded to all ports (except incoming port).
- ✓ Used for unknown unicast, broadcast and unknown traffic.

4 Viewing MAC Address Table (Cisco CLI)

```

SW1# show mac address-table
Vlan  Mac Address      Type      Ports
----  -
1      AA:AA:AA:AA:AA:AA    DYNAMIC   Fa0/1
1      BB:BB:BB:BB:BB:BB    DYNAMIC   Fa0/2
1      CC:CC:CC:CC:CC:CC    DYNAMIC   Fa0/3
1      DD:DD:DD:DD:DD:DD    DYNAMIC   Fa0/4
SW1#
    
```

5 Important Points

- ✓ Switch learns source MAC, not destination MAC.
- ✓ MAC table is built dynamically.
- ✓ Each entry is mapped to a specific VLAN.
- ✓ Default aging time is 300 seconds (can be changed).
- ✓ Known unicast → forwarded to single port.
- ✓ Unknown unicast, broadcast, multicast → flooded.
- ✓ MAC table helps in efficient forwarding and reduces collisions.
- ✓ You can configure static MAC entries for special cases (e.g., security).



The MAC address table is the brain of a switch, which helps it forward frames efficiently.



Segment Networks and Improve Security

A VLAN (Virtual LAN) allows you to logically divide a physical network into multiple separate broadcast domains, independent of physical location.

1 What is VLAN?

- ✓ Logically divides a switch into multiple broadcast domains.
- ✓ Devices in the same VLAN can communicate with each other.
- ✓ Devices in different VLANs cannot communicate directly (Layer 2).
- ✓ Improves security, reduces broadcast traffic and better network management.

3 VLAN Key Points

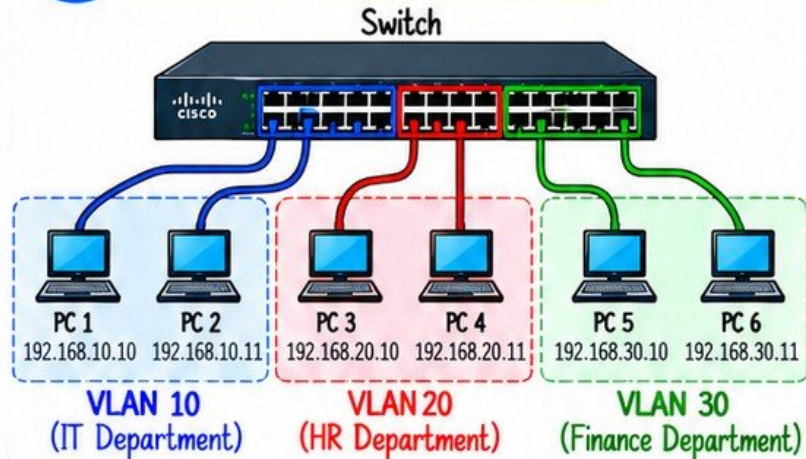
- ✓ Each VLAN is a separate broadcast domain.
- ✓ Devices in same VLAN can communicate (Layer 2).
- ✓ Devices in different VLANs need a router or Layer 3 switch for communication (Inter-VLAN routing).
- ✓ VLAN ID range: 1 - 4094 (1 and 1002-1005 are reserved).
- ✓ Port can be Access or Trunk.
- ✓ VLAN helps in security, segmentation and better network performance.

5 VLAN Configuration (Cisco CLI)

```
SW1(config)# vlan 10
SW1(config-vlan)# name IT
SW1(config-vlan)# exit
SW1(config)# vlan 20
SW1(config-vlan)# name HR
SW1(config-vlan)# exit
SW1(config)# vlan 30
SW1(config-vlan)# name FINANCE
SW1(config-vlan)# exit
```

- Creates VLAN 10, 20 and 30 with names.
- By default, VLAN is in active state.
- You can verify using: `show vlan brief`

2 VLAN Topology Example



4 Benefits of VLAN

- ✓ Reduces broadcast traffic.
- ✓ Improves network security.
- ✓ Logical separation of departments.
- ✓ Easy network management.
- ✓ Better performance and scalability.
- ✓ Flexibility (users can be in same VLAN even in different physical locations).

Same VLAN
= Can Communicate
Different VLAN
= Cannot Communicate
(Without Layer 3)

6 Access vs Trunk Port

Access Port (Single VLAN)

```
SW1(config)# interface fa0/1
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 10
SW1(config-if)# spanning-tree portfast
SW1(config-if)# end
```

Access Port
= Belongs to one VLAN only
(Used for End Devices)

Trunk Port (Multiple VLANs)

```
SW1(config)# interface fa0/24
SW1(config-if)# switchport mode trunk
SW1(config-if)# switchport trunk allowed vl
lan 10,20,30
```

Trunk Port
= Carries multiple VLANs
(Used between Switches or to a Router)

5. STP (Spanning Tree Protocol)

Prevent Loops and Ensure a Loop-Free Network

STP is a Layer 2 protocol that prevents switching loops in a network by blocking redundant paths and keeping only one active path.

1 Why STP is Needed?

- ✓ Prevent Layer 2 loops in a switched network.
- ✓ Avoid broadcast storms.
- ✓ Provide redundancy (backup path).
- ✓ Keep only one active path and block redundant links.
- ✓ Automatically reconverges if the active link fails.
- ✓ Improves network stability and availability.

3 STP Port States

Port State	Description
Blocking	Does not forward frames, listens for BPDUs.
Listening	Listens for BPDUs, preparing to forward.
Learning	Learns MAC addresses, not forwarding yet.
Forwarding	Forwards frames and learns MAC addresses.
Disabled	Administratively down.

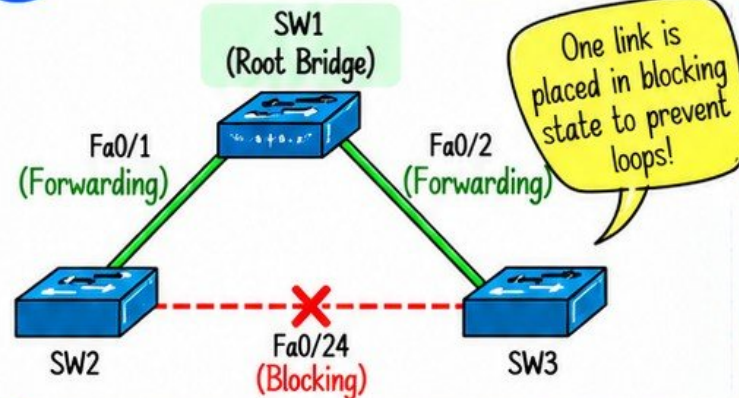
5 STP Example (show Commands)

```
SW1# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
            Address     0011.2233.4455
            This bridge is the root
  Interface  Role      Sts      Cost      Prio.Nbr
  Fa0/1      Desg     FWD      19        128.1
  Fa0/2      Desg     FWD      19        128.2
  Fa0/24     Desg     FWD      19        128.24
```

Key Takeaway

STP prevents loops, ensures a loop-free network, provides redundancy and keeps the network stable.

2 STP Topology Example



4 STP Election Process

- 1 Elects a Root Bridge (lowest Bridge ID).
- 2 Selects Root Ports on non-root switches (lowest path cost to root).
- 3 Selects Designated Ports on each segment (lowest path cost).
- 4 Places redundant ports in Blocking state.

Bridge ID
= Priority
+ MAC Address

6 Port Roles in STP

Port Role	Description
Root Port	Best path to the Root Bridge (only one per non-root switch).
Designated Port	Best path on a segment (forwards frames).
Non-Designated Port	Redundant port on a segment (placed in blocking state).

7 STP Versions (Quick Comparison)

Version	Standard	Convergence Time	Features
STP	802.1D	30-50 seconds	Basic (legacy)
RSTP	802.1w	1-6 seconds	Faster convergence
MSTP	802.1s	1-6 seconds	Multiple VLAN instances

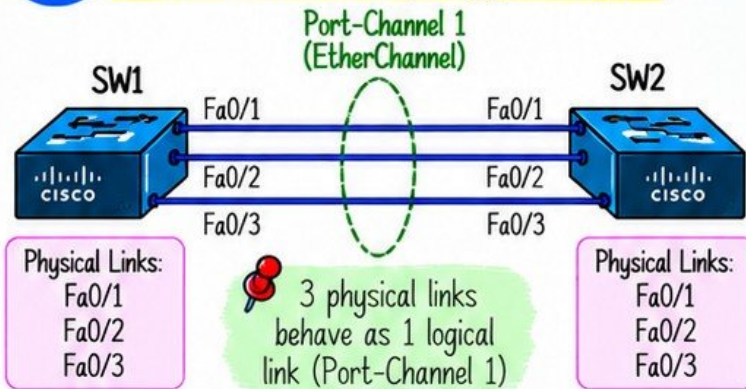
Combine Multiple Links for Higher Bandwidth and Redundancy

EtherChannel (Port-Channel) is a technology that bundles multiple physical links together to form one logical link, providing higher bandwidth, load balancing and redundancy.

1 Why EtherChannel?

- Increases bandwidth (link aggregation).
- Provides redundancy (if one link fails, traffic continues on remaining links).
- Load balances traffic across multiple links.
- Appears as a single logical link (Port-Channel).
- Simplifies network management.

2 EtherChannel Topology Example



3 EtherChannel Modes (Cisco)

Mode	Keyword	Description
On	on	Forces EtherChannel (no negotiation).
PAgP (Desirable)	desirable	Actively tries to form EtherChannel (using PAgP).
PAgP (Auto)	auto	Passively waits for PAgP.
LACP (Active)	active	Actively tries to form EtherChannel (using LACP - IEEE 802.3ad).
LACP (Passive)	passive	Passively waits for LACP.

4 Load Balancing Methods

Method	Description
src-mac	Based on source MAC address
dst-mac	Based on destination MAC address
src-dst-mac	Based on source and destination MAC
src-ip	Based on source IP address
dst-ip	Based on destination IP address
src-dst-ip	Based on source and destination IP
src-dst-port	Based on source and destination port (L4)

Default load balancing method: **src-dst-mac**
You can change it per your network design.

5 EtherChannel Configuration Example (LACP)

SW1 Configuration

```
SW1(config)# interface range fa0/1 - 3
SW1(config-if-range)# channel-group 1 mode active
SW1(config-if-range)# exit
SW1(config)# interface port-channel 1
SW1(config-if)# switchport mode trunk
SW1(config-if)# exit
```

SW2 Configuration

```
SW2(config)# interface range fa0/1 - 3
SW2(config-if-range)# channel-group 1 mode active
SW2(config-if-range)# exit
SW2(config)# interface port-channel 1
SW2(config-if)# switchport mode trunk
SW2(config-if)# exit
```

6 Verification Commands

```
SW1# show etherchannel summary
Flags: D - down      P - bundled in port-channel
      I - stand-alone s - suspended
      Group Port-channel Protocol Ports
-----
1      Po1(SU)      LACP      Fa0/1(P) Fa0/2(P) Fa0/3(P)
SW1# show interfaces port-channel 1
SW1# show lacp neighbor
SW1# show etherchannel port-channel
```

7 Important Points

- All links in EtherChannel should have same speed and duplex.
- Switchport mode (access/trunk) should be same on all links.
- All links must be in the same VLAN (for access) or same trunk config.
- Max 8 links in one EtherChannel (on most Cisco switches).
- Use LACP (IEEE 802.3ad) for multi-vendor environments.

Prevent Unauthorized Devices from Accessing the Network

Port Security is a Layer 2 feature that limits the number of MAC addresses allowed on a switch port to prevent unauthorized access.

1 Why Port Security?

- ✓ Prevents unauthorized devices.
- ✓ Allows only specific MAC addresses.
- ✓ Improves network security.
- ✓ Helps to stop MAC address flooding attacks.
- ✓ Useful for access ports (end users).
- ✓ Easy to configure and monitor.

3 Port Security Parameters

Parameter	Description
Maximum MAC	Maximum number of MAC addresses allowed on the port (default 1).
Violation Mode	Action when unknown MAC is seen (protect, restrict, shutdown).
Sticky MAC	Dynamically learns and saves MAC address in running config.
Aging Time	Removes learned MAC after a specific time (optional).

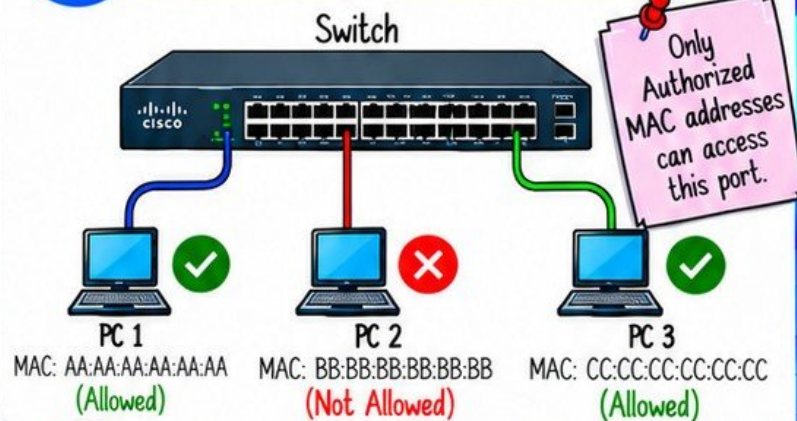
5 Port Security Configuration Example

```

SW1(config)# interface fa0/1
SW1(config-if)# switchport mode access
SW1(config-if)# switchport port-security
SW1(config-if)# switchport port-security maximum 2
SW1(config-if)# switchport port-security violation restrict
SW1(config-if)# switchport port-security mac-address sticky
SW1(config-if)# end
    
```

- maximum 2 → Allow 2 MAC addresses.
- violation restrict → Drop unknown MAC and log.
- mac-address sticky → Learn and save MAC automatically.

2 Port Security Topology Example



4 Violation Modes

Mode	Description
Protect	• Drops packets from unknown MAC. • No log and no SNMP trap.
Restrict	• Drops packets from unknown MAC. • Generates log and SNMP trap. • Port remains up.
Shutdown	• Puts the port in err-disable state. • Generates log and SNMP trap. • Port remains down until recovery.

6 Verify Port Security

```

SW1# show port-security interface fa0/1
Port Security           : Enabled
Port Status              : Secure-up
Violation Mode           : Restrict
Aging Time               : 0 mins
Maximum MAC Addresses    : 2
Total MAC Addresses      : 1
Configured MAC Addresses : 0
Sticky MAC Addresses      : 1
Last Source Address      : AA:AA:AA:AA:AA:AA
Security Violation Count : 0
    
```

7 Important Points

- ✓ Use Port Security on access ports only.
- ✓ Set maximum MAC based on requirement.
- ✓ Use sticky MAC for easy management.
- ✓ Choose violation mode as per your security policy.
- ✓ Monitor regularly using show port-security.

Recommended Violation Mode for Enterprise = **Restrict**

8. Inter-VLAN Routing

Enable Communication Between Different VLANs

Inter-VLAN Routing allows devices in different VLANs to communicate with each other. This can be achieved using a Layer 3 Switch or a Router (Router-on-a-Stick).

1 Why Inter-VLAN Routing?

- ✓ Allows communication between different VLANs.
- ✓ Used in enterprise networks.
- ✓ Better network segmentation and control.
- ✓ Improves security and traffic management.
- ✓ Can be implemented using Layer 3 Switch or Router.

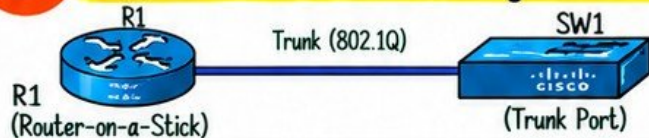
3 Layer 3 Switch Configuration

```
SW1(config)# ip routing          ! Enable L3 routing
SW1(config)# interface vlan 10
SW1(config-if)# ip address 192.168.10.1 255.255.255.0
SW1(config-if)# no shutdown
SW1(config-if)# exit

SW1(config)# interface vlan 20
SW1(config-if)# ip address 192.168.20.1 255.255.255.0
SW1(config-if)# no shutdown
SW1(config-if)# exit

SW1(config)# interface vlan 30
SW1(config-if)# ip address 192.168.30.1 255.255.255.0
SW1(config-if)# no shutdown
SW1(config-if)# exit
```

5 Router-on-a-Stick Configuration

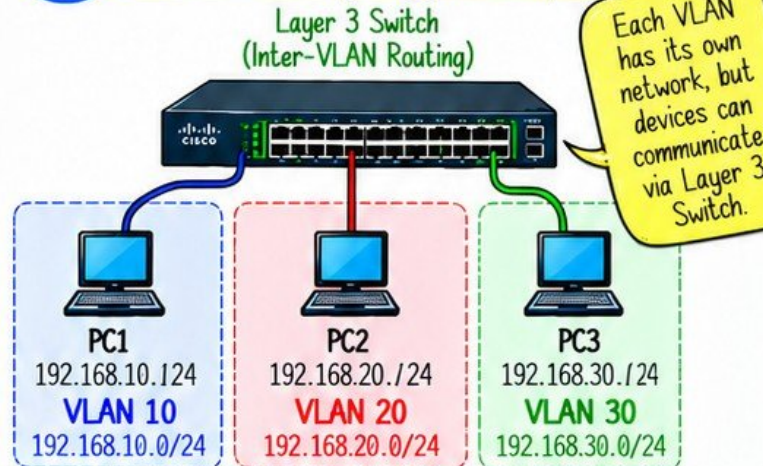


```
R1(config)# interface g0/0.10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip address 192.168.10.1 255.255.255.0
R1(config-subif)# exit

R1(config)# interface g0/0.20
R1(config-subif)# encapsulation dot1Q 20
R1(config-subif)# ip address 192.168.20.1 255.255.255.0
R1(config-subif)# exit

R1(config)# interface g0/0.30
R1(config-subif)# encapsulation dot1Q 30
R1(config-subif)# ip address 192.168.30.1 255.255.255.0
R1(config-subif)# exit
```

2 Network Topology Example



4 Verify Inter-VLAN Routing

```
SW1# show ip interface brief
```

Interface	IP Address	Status	Protocol
Vlan10	192.168.10.1	up	up
Vlan20	192.168.20.1	up	up
Vlan30	192.168.30.1	up	up

```
SW1# show ip route
```

Route	Description	VLAN
C 192.168.10.0/24	is directly connected,	Vlan10
C 192.168.20.0/24	is directly connected,	Vlan20
C 192.168.30.0/24	is directly connected,	Vlan30

6 Trunk Port Configuration (Switch Side)

```
SW1(config)# interface g0/1
SW1(config-if)# switchport mode trunk
SW1(config-if)# switchport trunk allowed vlan 10,20,30
SW1(config-if)# exit
```

7 Important Points

- ✓ Inter-VLAN routing is required for communication between different VLANs.
- ✓ Can be done using Layer 3 Switch or Router.
- ✓ Use trunk link (802.1Q) for Router-on-a-Stick.
- ✓ Configure SVI (interface vlan) on Layer 3 Switch.
- ✓ Ensure proper IP addressing and routing.
- ✓ Used for better network segmentation and security.

Use Layer 3 Switch for better performance in large networks.

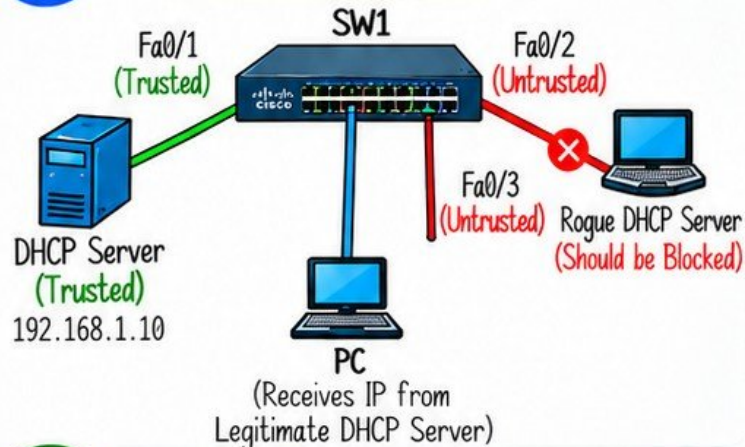
Prevent Rogue DHCP Servers and Improve Network Security

DHCP Snooping is a Layer 2 security feature that allows the switch to trust only specific ports for DHCP server messages and block rogue DHCP servers.

1 Why DHCP Snooping?

- ✓ Prevents rogue DHCP servers.
- ✓ Allows only trusted ports to send DHCP server messages.
- ✓ Blocks unauthorized DHCP responses.
- ✓ Protects users from getting wrong IP configuration.
- ✓ Improves network security and control.

2 Network Topology Example



3 DHCP Snooping Configuration

```

SW1(config)# ip dhcp snooping
SW1(config)# ip dhcp snooping vlan 10,20,30
SW1(config)# interface fa0/1
SW1(config-if)# ip dhcp snooping trust
SW1(config-if)# exit
SW1(config)# interface range fa0/2 - 24
SW1(config-if-range)# ip dhcp snooping limit rate 10
SW1(config-if-range)# ip dhcp snooping
SW1(config-if-range)# exit
    
```

5 Verification Commands

```

SW1# show ip dhcp snooping
DHCP Snooping is enabled
DHCP Snooping is configured on following VLANs:
10,20,30
Insertion of Option 82 is disabled
DHCP Snooping trust/rate is configured on the following
interfaces:

SW1# show ip dhcp snooping binding
    
```

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
0011.2233.4455	192.168.10.10	86400	dhcp	10	Fa0/10
0022.3344.5566	192.168.20.20	86400	dhcp	20	Fa0/11

```

SW1# show ip dhcp snooping interface
    
```

Interface	Trusted	Rate limit (pps)
Fa0/1	yes	unlimited
Fa0/2	no	10
Fa0/3	no	10

4 Trusted vs Untrusted Ports

Port Type	Description	Example
Trusted Port	- Allowed to send DHCP server messages (Offers, Acks, etc.) - Connected to legitimate DHCP Server	Fa0/1 (to DHCP Server)
Untrusted Port	- Not allowed to send DHCP server messages - Only allows DHCP client messages (Discover, Request) - Blocks rogue DHCP servers	Fa0/2, Fa0/3 (to End Users)

6 How DHCP Snooping Works?

- 1 Switch trust only specific ports.
 - 2 Allows DHCP client messages from untrusted ports.
 - 3 Blocks DHCP server messages from untrusted ports.
 - 5 Builds DHCP Snooping Binding Table (IP, MAC, VLAN, Port).
- Can be used with other features like Dynamic ARP Inspection (DAI) and IP Source Guard.

7 Key Takeaways

- ✓ Enable DHCP Snooping on required VLANs.
- ✓ Trust only the port connected to legitimate DHCP Server.
- ✓ Set rate limit on untrusted ports.
- ✓ Use with DAI and IP Source Guard for better security.
- ✓ Verify bindings and monitor regularly.

DHCP Snooping
= Simple but
Powerful
Layer 2
Security Feature!

10. Key Takeaways & Useful Commands

Switching is the foundation of every network. Understanding these concepts and commands will help you design, manage and troubleshoot enterprise networks from CCNA to CCIE level.

1 Key Takeaways from This Series

- ✓ Understood how a switch works.
- ✓ Learned MAC address table and frame forwarding.
- ✓ Studied VLAN and Inter-VLAN routing.
- ✓ Learned STP to prevent loops.
- ✓ Understood EtherChannel for higher bandwidth.
- ✓ Secured the network using Port Security, DHCP Snooping.
- ✓ These concepts are essential from CCNA to CCIE level.

2 Most Useful Show Commands

Command	Purpose
show mac address-table	View MAC address table
show interfaces status	Check port status
show vlan brief	Display VLAN information
show spanning-tree	Check STP status
show etherchannel summary	View EtherChannel details
show ip interface brief	Check SVI status
show ip route	View routing table
show port-security interface fa0/1	Check port-security
show ip dhcp snooping binding	View DHCP snooping bindings
show running-config	View current configuration

3 Most Useful Configuration Commands

```

SW1(config)# vlan 10
SW1(config-vlan)# name Users
SW1(config)# interface fa0/1
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 10
SW1(config)# interface g0/1
SW1(config-if)# switchport mode trunk
SW1(config-if)# switchport trunk allowed vlan 10,20,30
SW1(config)# interface range fa0/2 - 24
SW1(config-if-range)# switchport port-security
SW1(config-if-range)# switchport port-security maximum 2
SW1(config-if-range)# switchport port-security violation restrict
SW1(config)# interface vlan 10
SW1(config-if)# ip address 192.168.10.1 255.255.255.0
SW1(config-if)# no shutdown
SW1(config)# ip dhcp snooping
SW1(config)# ip dhcp snooping vlan 10,20,30
SW1(config)# interface fa0/1
SW1(config-if)# ip dhcp snooping trust
    
```

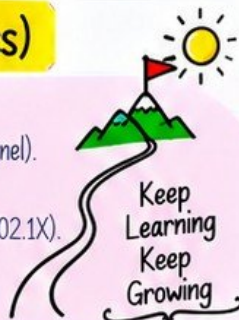
4 Troubleshooting Commands

```

SW1# show mac address-table | include fa0/1
SW1# show spanning-tree detail
SW1# show etherchannel summary
SW1# show interfaces fa0/1
SW1# show vlan brief
SW1# show port-security interface fa0/1
SW1# show ip dhcp snooping binding
SW1# show logging | include DHCP_SNOOPING
SW1# show cdp neighbors
SW1# show lldp neighbors
SW1# show ip interface brief
SW1# show standby brief (HSRP/VRRP)
SW1# show storm-control interface fa0/1
SW1# debug dhcp snooping events (if needed)
    
```

5 Next Steps (CCIE Level Topics)

- ✓ Advanced STP (PVST+, Rapid-PVST, MST).
- ✓ Campus network design (VLANs, Trunks, EtherChannel).
- ✓ First Hop Redundancy (HSRP, VRRP, GLBP).
- ✓ Advanced security features (DAI, IP Source Guard, 802.1X).
- ✓ Large scale Layer 2 and Layer 3 design.
- ✓ Troubleshooting and real-world scenarios.



6 Final Thoughts

“Switching is not just about connecting devices, it’s about building a **secure, reliable and scalable network.**”

– Urvish Patel

