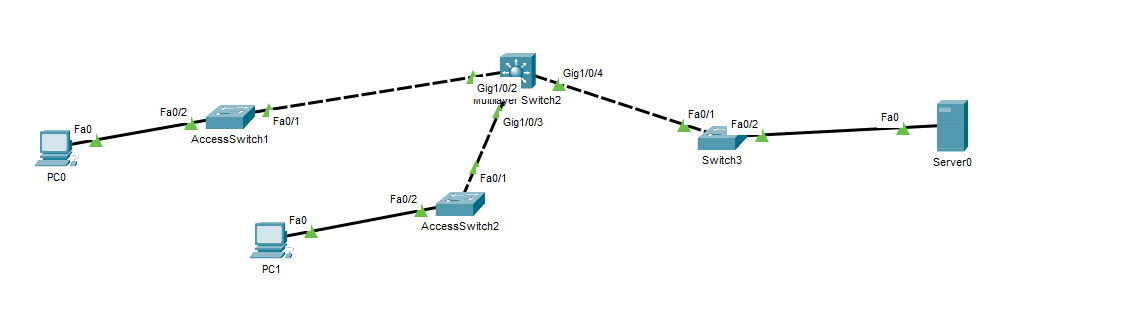
**A Functional Discussion of IP DHCP Snooping**

# **Topology**



This topology employs SVIs and 2 VLANs with multiple access switches and an L3 switch and will be used to practice and test out ip DHCP snooping.

# **Connections**

L3 Switch g1/0/2 is connected to AccessSwitch1 Fa0/1

L3 Switch g1/0/3 is connected to AccessSwitch2 Fa0/1

L3 Switch g1/0/4 is connected to AccessSwitch3 Fa0/1

AccessSwitch1 Fa0/2 is connected to a PC for VLAN 10

AccessSwitch2 Fa0/2 is connected to a PC for VLAN 20

AccessSwitch3 Fa0/2 is connected to a DHCP Server for VLAN 100

# **L3 Switch Configurations**

no ip domain lookup

hostname Distribution\_MLS1

int vlan 10

description "Corporate Banking VLAN for Corporate & Relationship Managers"

ip add 10.1.10.1 255.255.255.0

no sh

int vlan 20

description "Retail Banking VLAN for tellers, account clerks, etc."

ip add 10.1.20.1 255.255.255.0

no sh

int vlan 100

description "Servers VLAN"

ip add 10.1.100.1 255.255.255.0

no sh

vlan 10

name "Corporate Banking"

vlan 20

name "Retail Banking"

vlan 100

name "Servers"

int r g1/0/2-4

switchport mode trunk

switchport trunk allowed vlan 10,20,100

int vlan 10

ip helper-address 10.1.100.2

int vlan 20

ip helper-address 10.1.100.2

# **AccessSwitch1-3 Configurations**

vlan 10

name "Corporate Banking"

vlan 20

name "Retail Banking"

vlan 100

name "Servers"

int fa0/1

switchport mode trunk

switchport trunk allowed vlan 10,20,100

int fa0/2

switchport mode access

switchport access vlan # !10/20/100

# **Server Configuration**

CorporateBanking\_Pool | VLAN 10

Address Block: 10.1.10.0/24

Default gateway: 10.1.10.1

RetailBanking\_Pool | VLAN 20

Address Block: 10.1.20.0/24

Default gateway: 10.1.20.1

# **What is DHCP Snooping**

* **Definition**: DHCP snooping is a Layer 2 security feaature on switches that classifies switch ports as either **trusted** or **untrusted**.
* **Goal**: Prevent **rogue DHCP servers** from handing out IP addresses in your network.
* **How It Works**:
* **Trusted Ports**: Usually uplinks towards the legitimate DHCP server or distribution/core switches. DHCP replies are allowed.
* **Untrusted Ports**: Default for access ports connected to end devices. DHCP replies from here are blocked.

# **Why it matters in you topology**

Here’s where DHCP snooping comes in:

* PCs on VLAN 10 and VLAN 20 must get their IP addresses only from the DHCP server in VLAN 100.
* Without snooping, a malicious user could connect their laptop, enable DHCP services, and hand out fake IPs → breaking client connectivity or enabling attacks like MITM.
* With snooping, only the **ports leading to the real DHCP server** (on AccessSwitch3 Fa0/2) and **the trunks to the MLS** are trusted.

# **Implementation in Cisco Packet Tracer**

Although Packet Tracer doesn’t support every advanced DHCP snooping feature (like option-82 insertion), it does support the basics.

## **Distribution MLS Configurations**

|  |
| --- |
| **! Enable DHCP snooping globally**  **Ip dhcp snooping**  **! Enable DHCP snooping for the VLANs**  **Ip dhcp snooping vlan 10,20,100**  **! Trust all trunk ports**  **Int range g1/0/2-4**  **Ip dhcp snooping trust** |

## **AccessSwitch1-2 Configurations**

|  |
| --- |
| **! Enable DHCP snooping globally**  **Ip dhcp snooping**  **! Enable DHCP snooping for the VLANs**  **Ip dhcp snooping vlan 10,20,100**  **! Trust only the uplink trunk ports to the Distribution MLS**  **Int fa0/1**  **Ip dhcp snooping trust**  **! Limit DHCP request rate on access ports to prevent DoS**  **Int fa0/2**  **Ip dhcp snooping limit rate 10** |

## AccessSwitch3 Configurations

|  |
| --- |
| **! Enable DHCP snooping globally**  **Ip dhcp snooping**  **! Enable DHCP snooping for the VLANs**  **Ip dhcp snooping vlan 10,20,100**  **! Trust only the uplink trunk ports to the Distribution MLS**  **Int fa0/1**  **Ip dhcp snooping trust**  **! Trust the port where the real DHCP server connects**  **Int fa0/2**  **Ip dhcp snooping trust** |

**Notes:**

* **AccessSwitch1/2**: Only trunk uplinks to the MLS are trusted. PC-facing Fa0/2 stays untrusted.
* **AccessSwitch3**: Both the trunk to MLS (Fa0/1) and the DHCP server-facing Fa0/2 are trusted.

# **Operational Behavior**

* When a PC in VLAN 10 or 20 sends DHCPDISCOVER:
  + The request goes through the access switch (untrusted port).
  + Forwarded to Distribution MLS (trusted trunk).
  + MLS relays it (via ip helper-address) to the DHCP server in VLAN 100.
* If a rogue DHCP server is connected to an untrusted port:
  + Its DHCPOFFER or DHCPACK is blocked at the switch.
  + Only the legitimate DHCP server’s offers reach clients.

# **Verification Commands**

In Packet Tracer (and real IOS):

show ip dhcp snooping

show ip dhcp snooping binding

* **show ip dhcp snooping** → Confirms VLANs and trusted ports.
* **show ip dhcp snooping binding** → Lists legitimate DHCP bindings (IP–MAC–VLAN).

✅ **In summary:**  
In your Packet Tracer file, DHCP snooping ensures that **VLAN 10 and 20 clients** get their IP addresses securely from the **server in VLAN 100** via the MLS. Rogue DHCP servers connected to client-facing access ports are automatically blocked.