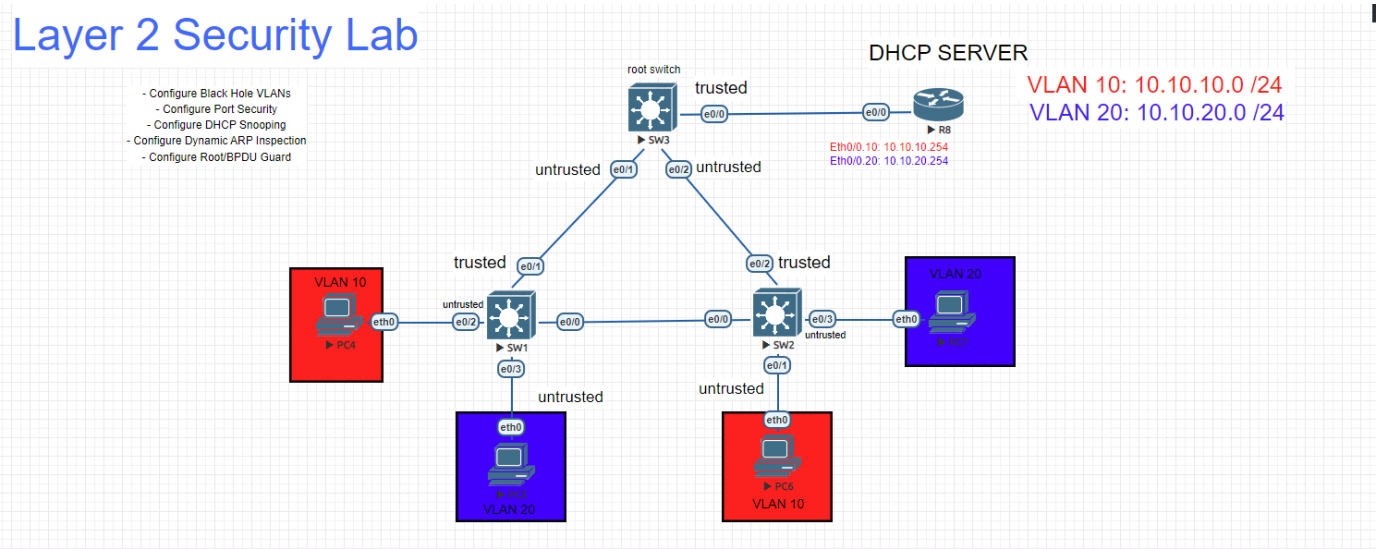
DHCP Snooping Configuration

In this How To we will cover how to configure DHCP Snooping with the L3 device in our network as the DHCP server. First thing we will have to do is configure the baselines for all devices. SW1, SW2, and SW3 will have VLANs 10,20 created, and all trunks links configured. The Router will have a DHCP pool configured and sub-interfaces.

This How To assumes you already know how to configure these technologies. If you do not know how to configure refer to the other How To's.



First we will have to determine the "trusted" and "untrusted" interfaces in the network. "trusted" ports will be the links that are receiving the DHCP server messages. [SW2--Eth0/2], [SW3--Eth0/0], [SW1--Eth0/1]. The "untrusted" ports will be all the ports that receive incoming DHCP client messages. Now let's start are basic configuration.

`SW1(config)#ip dhcp snooping` # This command will enable **"DHCP Snooping"** globally on our switch

`SW1(config)#ip dhcp snooping vlan 10,20` # This command will enable DHCP snooping to be enabled for the specified VLANs.

`SW1(config)#interface eth0/2` # This command will bring us into the sub-configuration mode for the interface we want to configure

`SW1(config-if)#ip dhcp snooping trusted` # This command will specify the interfaces that can receive incoming DHCP server messages. *** ***IMPORTANT NOTE*** *** The trusted interfaces will add DHCP option 82 to onto the DHCPDiscover message. This option will cause DHCP relay's to drop the DHCP packet.

The full configuration is shown below.

```
SW2(config)#ip dhcp snooping
SW2(config)#ip dhcp snooping vlan 10,20
SW2(config)#interface eth0/2
SW2(config-if)#ip dhcp snooping trust
SW2(config-if)#exit
SW2(config)#
```

Now let's try to pull a DHCP address. We will show a wireshark capture and a debug message from SW2 that shows the packet being dropped because of the DHCP option 82 being inserted.

`SW2#debug ip dhcp snooping packets` # This debug command will show us the steps of the DHCP snooping process.


```
SW2#
*Dec  5 01:21:38.487: 0xBB
*Dec  5 01:21:38.487: 0xCC
*Dec  5 01:21:38.487: 0x0
*Dec  5 01:21:38.487: 0x20
*Dec  5 01:21:38.487: 0x0
*Dec  5 01:21:38.487: DHCP_SNOOPING_SW: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (10)
*Dec  5 01:21:38.487: DHCP_SNOOPING_SW: bridge packet send packet to port: Ethernet0/2, vlan 10.
SW2#
*Dec  5 01:21:41.189: DHCP_SNOOPING: checking expired snoop binding entries
SW2#
```

Although output is limited essentially what is happening here is the DHCP packet is getting dropped before it even makes it to the DHCP server. Because at the next hop at SW3 that 82 option will make the switch believe it is a relay message, which it is not. It is a DHCP broadcast message. To fix we must a command to both our switches and a command for our router.

`SW2(config)#no ip dhcp snooping information option` # This command will stop the DHCP option 82 from being inserted onto the DHCP packet.

`R1(config)#ip dhcp relay information trust-all` # By default, if the gateway address is set to all zeros in the DHCP packet and the relay agent information option is already present in the packet, the DHCP relay agent will discard the packet. Use the ip dhcp relay information trust-all command to override this behavior and accept the packets.

with these two commands configured we will now be able to receive an IP address via DHCP.

Below we have our PC completing the DORA process, and then a packet capture of the link between SW3 and the DHCP server. And also our DHCP snooping verification command.

```
VPCS> ip dhcp
DDORA IP 10.10.20.1/24 GW 10.10.20.254

VPCS>
```

29	9.376712	0.0.0.0	255.255.255.255	DHCP	410	DHCP Discover - Transaction ID 0xe93e1731
30	9.377845	10.10.20.254	10.10.20.1	DHCP	346	DHCP Offer - Transaction ID 0xe93e1731
31	10.044082	aa:bb:cc:00:30:00	PVST+	STP	68	RST. Root = 32768/1/aa:bb:cc:00:10:00 Cost = 100 Port = 0x8001
32	10.044295	aa:bb:cc:00:30:00	Spanning-tree-(for-bridges)_00	STP	60	RST. Root = 32768/1/aa:bb:cc:00:10:00 Cost = 100 Port = 0x8001
33	10.091789	aa:bb:cc:00:30:00	PVST+	STP	68	RST. Root = 0/10/aa:bb:cc:00:30:00 Cost = 0 Port = 0x8001
34	10.092142	aa:bb:cc:00:30:00	PVST+	STP	68	RST. Root = 0/20/aa:bb:cc:00:30:00 Cost = 0 Port = 0x8001
35	10.092240	aa:bb:cc:00:30:00	PVST+	STP	68	RST. Root = 32768/902/aa:bb:cc:00:30:00 Cost = 0 Port = 0x8001
36	10.377889	0.0.0.0	255.255.255.255	DHCP	410	DHCP Request - Transaction ID 0xe93e1731
37	10.378718	10.10.20.254	10.10.20.1	DHCP	346	DHCP ACK - Transaction ID 0xe93e1731

```
SW2#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------
-----
00:50:79:66:68:07   10.10.20.1       86029       dhcp-snooping   20    Ethernet0/3
Total number of bindings: 1

SW2#
```