DHCP Snooping

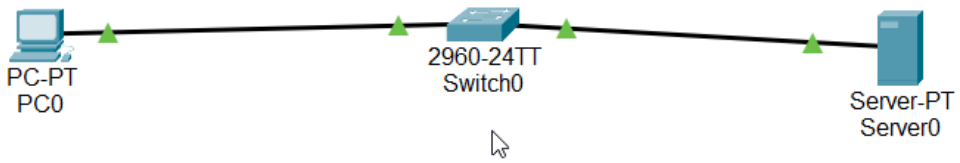
- **DHCP Snooping**: DHCP snooping acts as a network security measure by blocking rogue DHCP servers from issuing IP addresses to network devices. It specifically blocks DHCP offer and ACK packets from unauthorized servers during the DHCP transaction process (DORA), and builds an ARP to IP binding table to track legitimate host configurations.

Equipment and Software Needed

- Cisco Packet Tracer
- Cisco 2960 Switch
- A PC
- A Server

Step 1: Set Up the Environment

1. Place Devices:
    - Drag and drop a Cisco 2960 switch, a PC, and a server onto the Packet Tracer workspace.
2. Make Connections:
    - Connect the PC to the switch's port FastEthernet0/1.
    - Connect the server to the switch's port FastEthernet0/2.



Step 2: Configure DHCP Snooping

1. Access Switch Configuration:
    - Click on the switch to open its configuration interface.
    - Navigate to the CLI tab and enter the global configuration mode by typing

enable

configure terminal

```
Switch>enable
Switch#conf t
```

2. Enable DHCP Snooping Globally:

- In the configuration mode, enable DHCP snooping

ip dhcp snooping

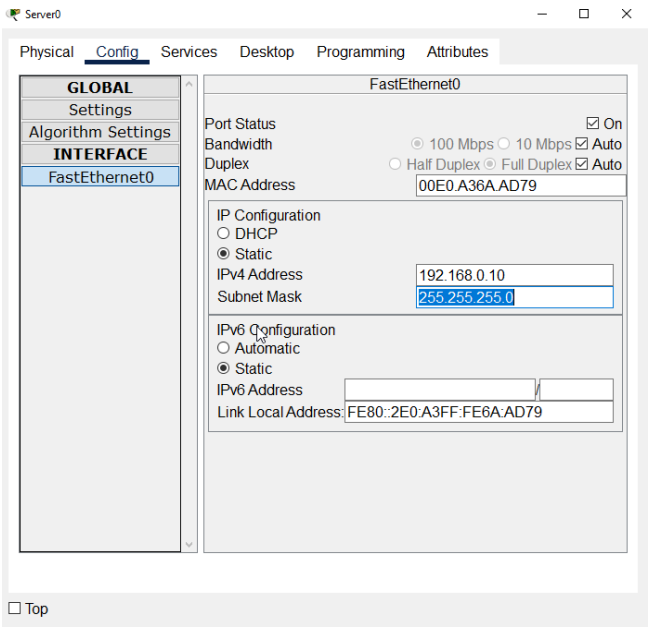
ip dhcp snooping vlan 1

```
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 1
```

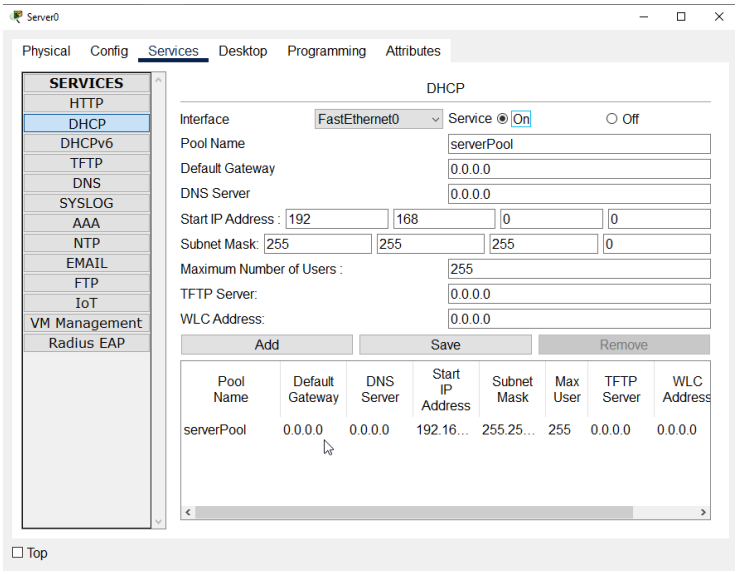
This step turns on DHCP snooping for the network, specifically for VLAN 1. By default, this will block all ports from accepting DHCP offer or ACK packets from DHCP servers unless specified otherwise.

Step 3: Test and Verify DHCP Snooping Block

1. Configure the Server:
    - Click on the server, go to the Config tab, and set a static IP:
        - IP Address: 192.168.0.10
        - Subnet Mask: 255.255.255.0

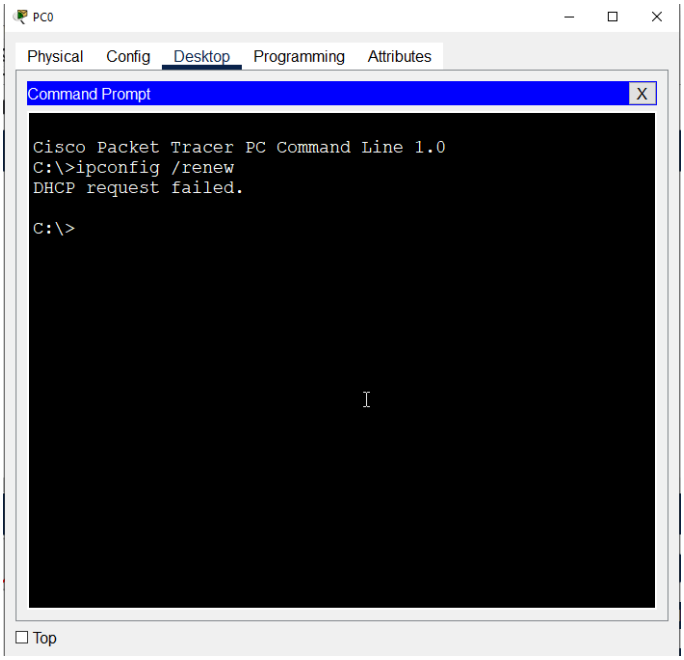


- Enable the DHCP service and check the default DHCP pool settings.



2. Test from PC:
   - On the PC, open Command Prompt from the Desktop tab and type

ipconfig /renew



This command attempts to renew the DHCP lease. Observe that the PC fails to obtain an IP address because DHCP snooping is blocking the replies from the server.

Step 4: Allow DHCP Replies on the Server Port

1. Configure Trusted Port on the Switch:
    - Go back to the switch's CLI and specify the server's port as a trusted port to allow DHCP replies:

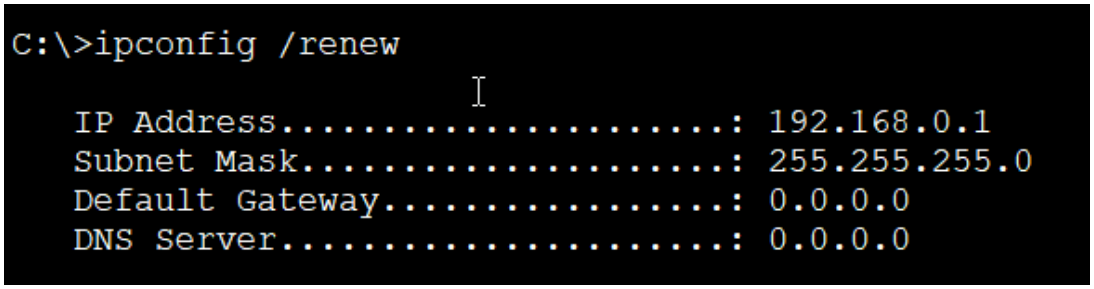
interface FastEthernet0/2
ip dhcp snooping trust

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 1
Switch(config)#interface FastEthernet0/2
Switch(config-if)#dhcp snooping trust
                 ^
% Invalid input detected at '^' marker.

Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#
```

This command sets the switch port connected to the server as trusted, permitting DHCP offer and ACK packets to be accepted from this port.

Step 5: Verify Successful DHCP Configuration

1. Re-test DHCP on PC:
    - Return to the PC and run the `ipconfig /renew` command again.
    - This time, the PC should successfully receive an IP address from the DHCP server, demonstrating that DHCP snooping is configured correctly and selectively allowing DHCP traffic through the designated trusted port.



Conclusion

This guide demonstrates setting up and configuring DHCP snooping in Cisco Packet Tracer, ensuring that only designated ports can respond to DHCP requests, enhancing the security of the network against rogue DHCP servers.