2024

DHCP SNOOPING CONFIGURATION

DCHP SNOOPING TRUSTED AND UNTRUSTED PORTS

INACIO ANDRE

- **DHCP Snooping** is a security technology on a Layer 2 network switch that can prevent unauthorized DHCP servers from accessing your network. It is a protection from the untrusted hosts that want to become DHCP servers. DHCP Snooping works as a protection from man-in-the-middle attacks. DHCP itself operates on Layer 3 of the OSI layer while DHCP snooping operates on Layer 2 devices to filter the traffic that is coming from DHCP clients.

- In Cisco switches, DHCP snooping is enabled manually. Trusted ports should be manually configured and the rest unconfigured ports are considered untrusted ports. Most devices connected to trusted ports are routers, switches, and servers. DHCP clients like PC and laptops are commonly connected to an untrusted port.

- How it works is that it will allow DHCP server messages like DHCPOFFER and DHCPACK that are coming from a trusted source. If the DHCP server messages are coming from untrusted ports, it will discard the DHCP traffic. The switch creates a table called the DHCP Snooping Binding Database. The DHCP snooping database registers the source MAC address and IP address of the hosts that are connected to an untrusted port.

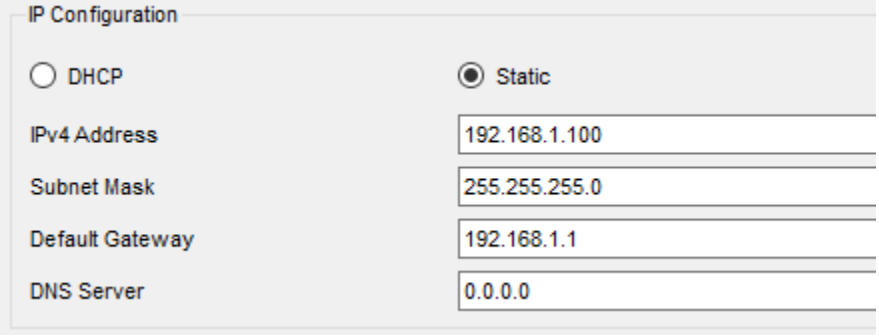
R1

```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#int g0/0
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#no shut
```

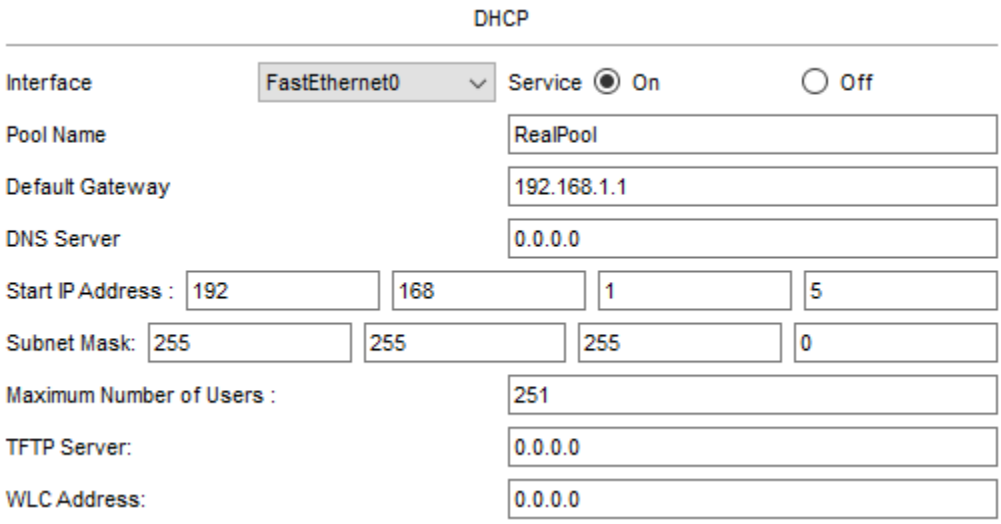
S1

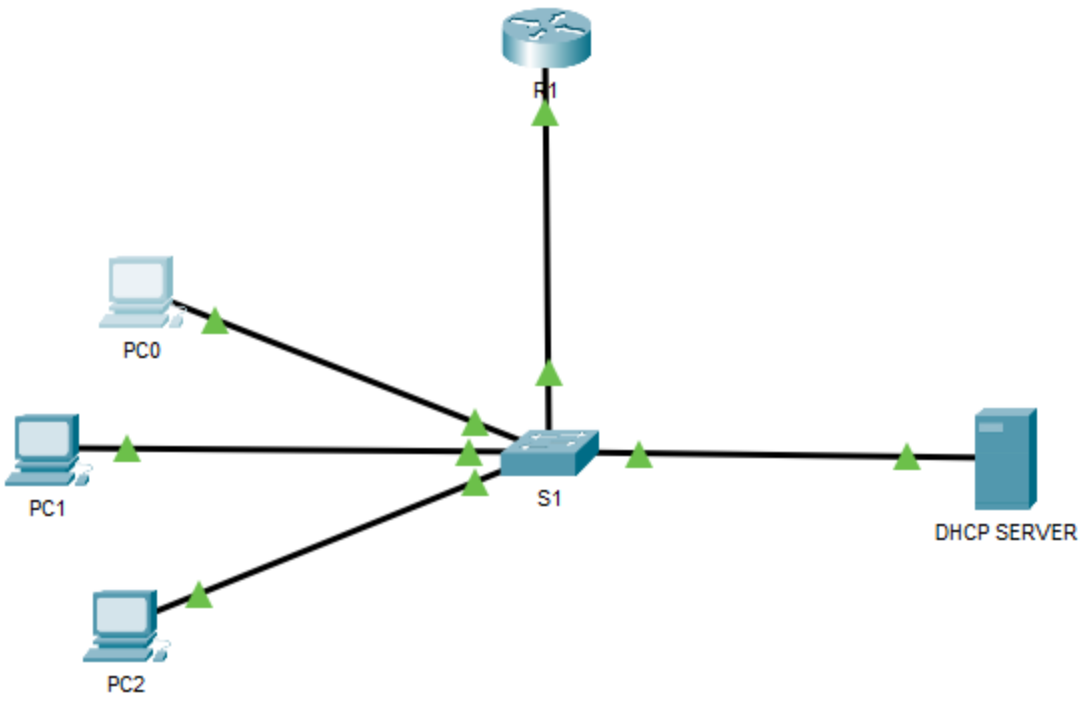
```
Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#ip dhcp snooping
S1(config)#int range f0/23-24
S1(config-if-range)#ip dhcp snooping trust
S1(config-if-range)#ip dhcp snooping vlan 1
S1(config)#exit
```

REAL DHCP SERVER



DHCP POOL

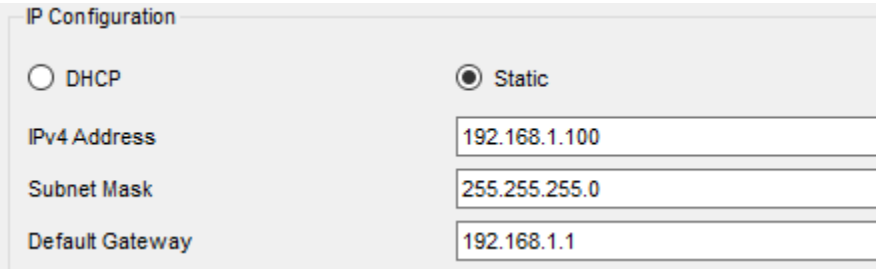




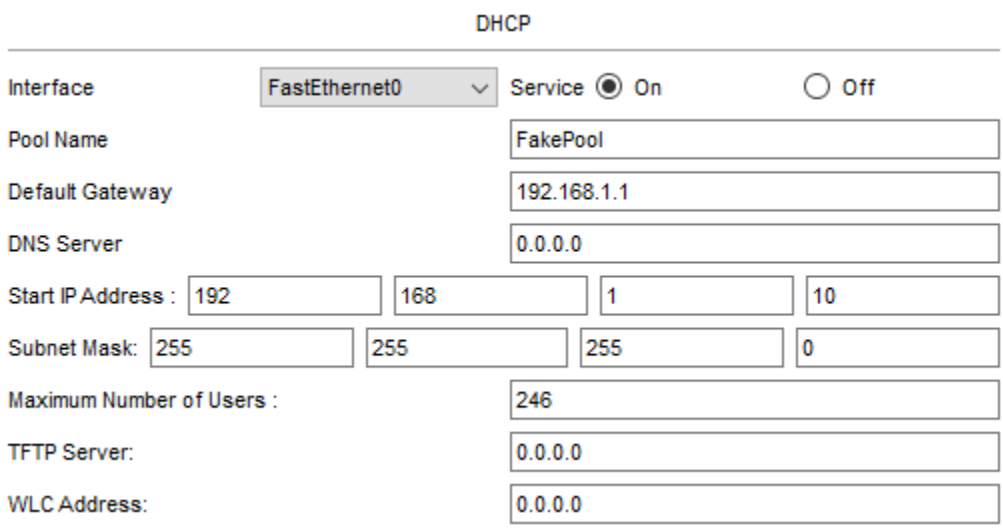
IP Configuration

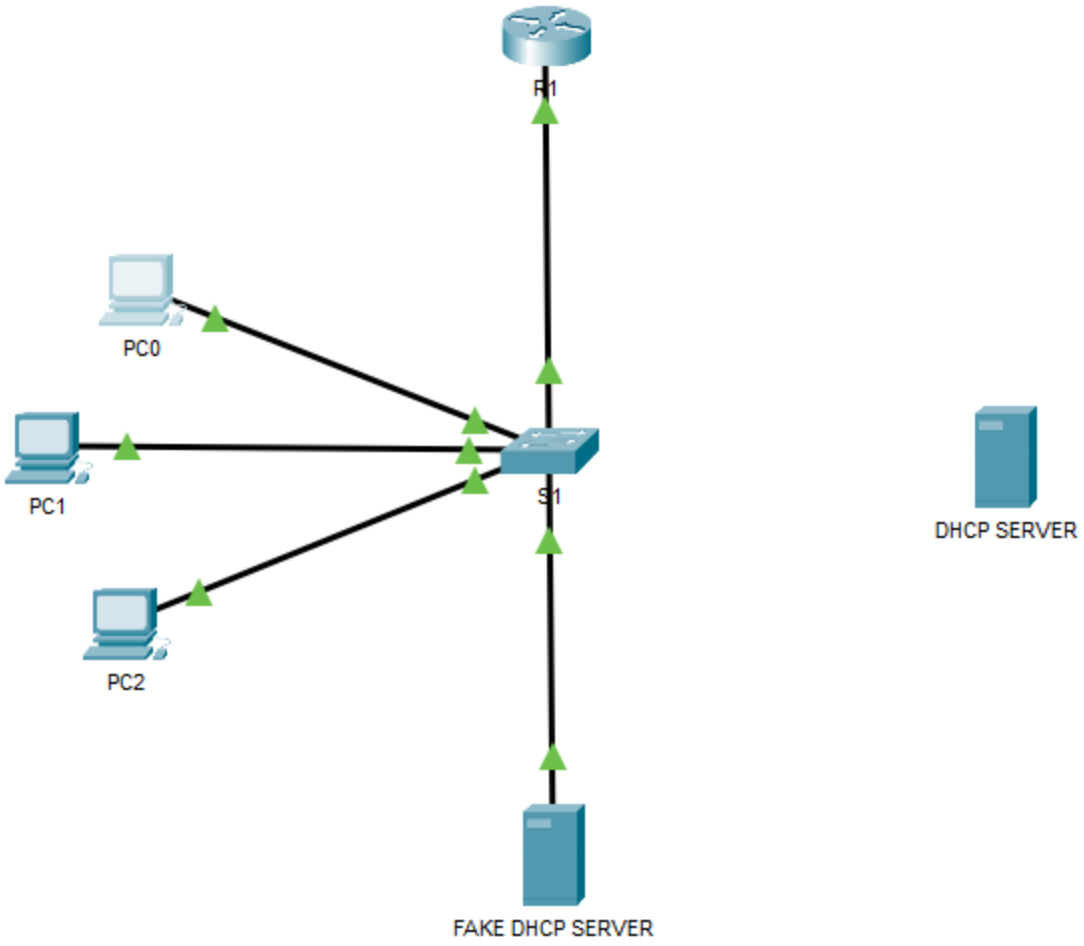
(•) DHCP	( ) Static	DHCP request successful.
IPv4 Address	192.168.1.5	
Subnet Mask	255.255.255.0	
Default Gateway	192.168.1.1	

FAKE DHCP SERVER



DHCP POOL





IP Configuration

(•) DHCP	( ) Static	DHCP failed. APIPA is being used.
IPv4 Address	169.254.188.170	
Subnet Mask	255.255.0.0	
Default Gateway	0.0.0.0	

```
S1#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
-----------------------    -------    ----------------
FastEthernet0/24           yes        unlimited
FastEthernet0/22           no         unlimited
FastEthernet0/23           yes        unlimited
FastEthernet0/1            no         unlimited
FastEthernet0/3            no         unlimited
FastEthernet0/2            no         unlimited
```

```
S1#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:30:F2:DB:9A:4E   192.168.1.6      86400       dhcp-snooping  1     FastEthernet0/2
00:01:C7:C6:E2:E1   192.168.1.7      86400       dhcp-snooping  1     FastEthernet0/3
00:0A:F3:08:BC:AA   192.168.1.8      86400       dhcp-snooping  1     FastEthernet0/1
Total number of bindings: 3
```