

Filename: cisco-ccna200301-5-10-1-configuring dhcp_snooping_and_dai

ShowName: Cisco CCNA (200-301)

Topic: 5.0 Security Fundamentals

EpisodeName: Configuring DHCP Snooping & DAI

Description: In this episode, You will learn how to configure additional L2 security features: DHCP Snooping and Dynamic ARP Inspection (DAI). You will understand why both are used and how it is configured on switches. You will see a demonstration of how it also works effectively.

Configuring DHCP Snooping & DAI

- 5.7 Configure Layer 2 security features

- DHCP Snooping

- Inspect DHCP traffic at L2 and track IP addresses assigned to hosts at which port
- Helps for troubleshooting and setup for Dynamic ARP Inspection
- Mitigates against IP address spoofing

- Configure DHCP Snooping and Dynamic ARP Inspection

- Lab: Cisco Certified Network Associate (CCNA v3): Compare Static and Dynamic Routing
- Configure all interfaces we want to affect into same vlan

```
NYCORE1 (config)#int range fa1/0/1 - 2, fa1/0/22 - 23
NYCORE1 (config-if-range)#switchport mode access
NYCORE1 (config-if-range)#switchport access vlan 1
NYCORE1 (config-if-range)#spanning-tree portfast
```

- Configure DHCP Snooping on NYCORE1

```
NYCORE1#
NYCORE1#configure terminal
NYCORE1 (config)#ip dhcp snooping
NYCORE1 (config)#ip dhcp snooping vlan 1
NYCORE1 (config)#exit
NYCORE1#show ip dhcp snooping
```

- Configure which port DHCP packets are allowed to pass

```
NYCORE1 (config-if-range)# exit
NYCORE1 (config)#int fa1/0/1
NYCORE1 (config-if)#ip dhcp snooping trust
```

- Configure DHCP on NYEDGE1

```
NYEDGE1#
NYEDGE1#configure terminal
NYEDGE1 (config)#ip dhcp pool ITProTV
NYEDGE1 (dhcp-config)#network 192.168.16.0 255.255.255.0
NYEDGE1 (dhcp-config)#default-router 192.168.16.1
```

- Configure NYCORE2 as client

```
NYCORE2#
NYCORE2#configure terminal
NYCORE2 (config)#int vlan 1
NYCORE2 (config)#ip address dhcp
```

- Configure Dynamic ARP Inspection

```
NYCORE1#
NYCORE1#show ip dhcp snooping binding
NYCORE1#configure terminal
NYCORE1 (config)#ip arp inspection vlan 1
```

- Configure NYWAN1 as an attacker with NYCORE1's IP address

- NYWAN1#
NYWAN1#configure terminal
NYWAN1(config)#int g0/0
NYWAN1(config-if)#ip address 192.168.16.X 255.255.255.0
NYWAN1(config-if)#

- Verify NYCORE1

- NYCORE1#show ip arp inspection (note output)

- Ping from NYWAN1 to DHCP server (NYEDGE1)

- NYWAN1#ping 192.168.16.1

- Ping from NYCORE2 to DHCP server (NYEDGE1)

- NYCORE2#ping 192.168.16.1