

Configure Dynamic Host Configuration Protocol (DHCP) Snooping on a Switch through the Command Line Interface (CLI)

Objective

Dynamic Host Configuration Protocol (DHCP) is a service that runs at the application layer of the TCP/IP protocol stack to dynamically assign IP addresses and to allocate TCP/IP configuration information to DHCP clients.

DHCP snooping is a security feature that acts as a firewall between untrusted hosts and trusted DHCP servers. Snooping prevents false DHCP responses and monitor clients. It can prevent man-in-the-middle attacks and authenticate host devices. DHCP Snooping classifies interfaces on the switch into two categories; trusted and untrusted. It also gives you a way to differentiate between untrusted interfaces connected to the end-user and trusted interfaces connected to the DHCP server or another switch.

Note: By default, the switch considers all interfaces as untrusted interfaces. Thus, it is important to configure the switch to specify trusted ports or interfaces as DHCP Snooping is enabled.

You can configure DHCP Snooping through the switch web-based utility or through the command line interface (CLI).

This article aims to show how to configure DHCP snooping on your switch through the CLI.

Applicable Devices

- Sx300 Series
- SG350X Series
- Sx500 Series
- SG500X

Software Version

- 1.4.7.06 — Sx300, Sx500, SG500X
- 2.2.8.04 — SG350X

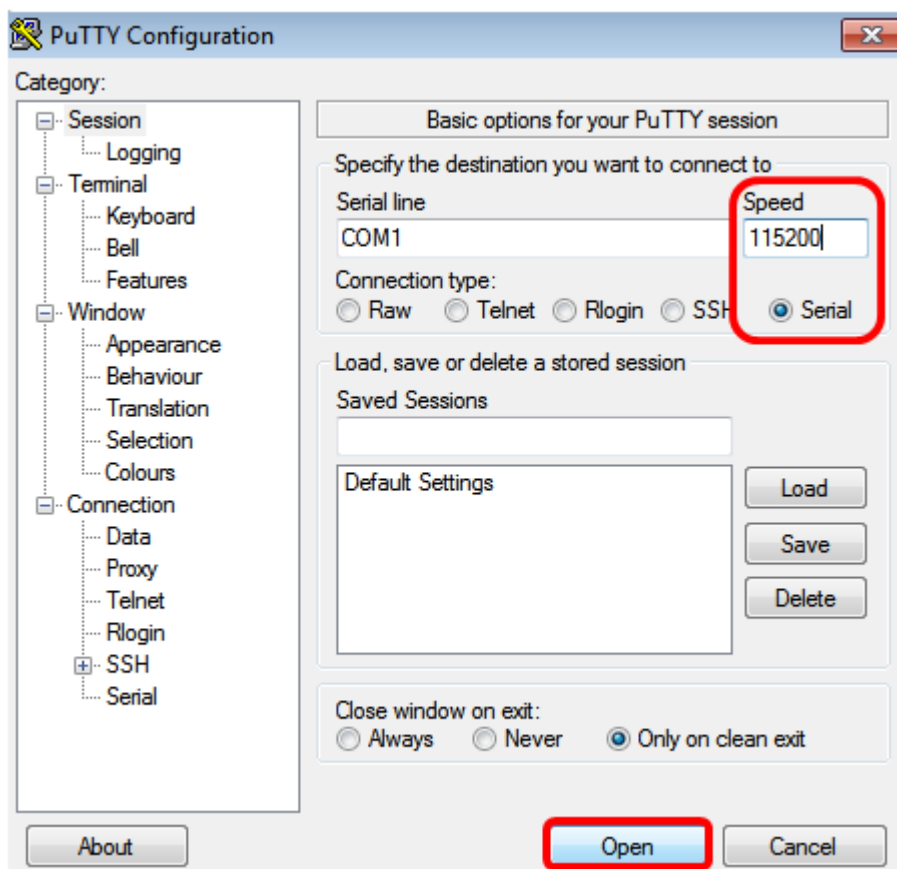
Configure DHCP Snooping through the CLI

Step 1. Connect your computer to the switch using a console cable and launch a terminal emulator application to access the switch CLI.



Note: In this example, PuTTY is used as the terminal emulator application.

Step 2. In the PuTTY Configuration window, choose **Serial** as the Connection type and enter the default speed for the serial line which is 115200. Then, click **Open**.



Step 3. In the CLI, enter the global configuration command mode by entering the following:

```
SG350X#configure terminal
```

```
SG350X#configure terminal  
SG350X(config)#
```

Note: In this example, the switch used is SG350X-48MP.

Step 4. Once you are on the global configuration mode, enable global DHCP snooping by entering the following:

```
SG350X (config)#ip dhcp snooping
```

```
SG350X#  
SG350X#configure terminal  
SG350X(config)#ip dhcp snooping
```

Step 5. Specify on which Virtual Local Area Network (VLAN) you want to enable DHCP snooping by entering the following:

```
SG350X (config)#ip dhcp snooping vlan 1
```

```
SG350X#  
SG350X#configure terminal  
SG350X(config)#ip dhcp snooping  
SG350X(config)#ip dhcp snooping vlan 1
```

Note: In this example, VLAN 1 is used.

Step 6. Specify the port or interface where you want to enable DHCP snooping by entering the following:

```
SG350X (config)#int ge1/0/1
```

```
SG350X#  
SG350X#configure terminal  
SG350X(config)#ip dhcp snooping  
SG350X(config)#ip dhcp snooping vlan 1  
SG350X(config)#interface ge1/0/1
```

Note: In this example, interface ge1/0/1 is used. This stands for Gigabit Ethernet port number/stack number (if your switch belongs to a stack/switch number).

Step 7. Specify that the port is a trusted port or interface by entering the following:

```
SG350X (config-if)#ip dhcp snooping trust
```

```
SG350X#  
SG350X#configure terminal  
SG350X(config)#ip dhcp snooping  
SG350X(config)#ip dhcp snooping vlan 1  
SG350X(config)#interface ge1/0/1  
SG350X(config-if)#ip dhcp snooping trust  
SG350X(config-if)#
```

Note: The prompt has now changed from (*config*) to (*config-if*) indicating that the configuration is for the specific port mentioned in the previous command.

Step 8. Exit the specific interface and the global configuration command mode to go back to the privileged EXEC mode by entering the following:

```
SG350X (config-if)#exit
```

```
SG350X (config)#exit
```

```
SG350X#  
SG350X#configure terminal  
SG350X(config)#ip dhcp snooping  
SG350X(config)#ip dhcp snooping vlan 1  
SG350X(config)#interface gel/0/1  
SG350X(config-if)#ip dhcp snooping trust  
SG350X(config-if)#exit  
SG350X(config)#exit  
SG350X#
```

Step 9. (Optional) Once on the privileged EXEC mode, check if your new settings have been saved in the running configuration file by entering the following:

```
SG350X #show ip dhcp snooping
```

```
SG350X#  
SG350X#configure terminal  
SG350X(config)#ip dhcp snooping  
SG350X(config)#ip dhcp snooping vlan 1  
SG350X(config)#interface gel/0/1  
SG350X(config-if)#ip dhcp snooping trust  
SG350X(config-if)#exit  
SG350X(config)#exit  
SG350X#show ip dhcp snooping
```

The newly-configured settings should now appear:

```
SG350X#  
SG350X#configure terminal  
SG350X(config)#ip dhcp snooping  
SG350X(config)#ip dhcp snooping vlan 1  
SG350X(config)#interface gel/0/1  
SG350X(config-if)#ip dhcp snooping trust  
SG350X(config-if)#exit  
SG350X(config)#exit  
SG350X#show ip dhcp snooping  
DHCP snooping is Enabled  
DHCP snooping is configured on following VLANs: 1  
DHCP snooping database is Disabled  
Relay agent Information option 82 is Enabled  
Option 82 on untrusted port is allowed  
Verification of hwaddr field is Enabled  
  
Interface    Trusted  
-----  
gi1/0/1     Yes
```

Step 10. (Optional) To permanently save the settings, enter the following:

SG350X# copy running-config startup-config

```
DHCP snooping is Enabled
DHCP snooping is configured on following VLANs: 1
DHCP snooping database is Disabled
Relay agent Information option 82 is Enabled
Option 82 on untrusted port is allowed
Verification of hwaddr field is Enabled

Interface      Trusted
-----
gi1/0/1       Yes

SG350X#copy running-config startup-config
```

Step 11. Enter Y in the Overwrite file prompt to indicate Yes and to save the settings to the startup configuration file.

Overwrite file [startup-config].... (Y/N) [N] ? Y

```
SG350X#copy running-config startup-config
Overwrite file [startup-config].... (Y/N) [N] ?Y
02-Mar-2017 07:57:17 %COPY-1-FILECOPY: Files Copy - source URL running-config destination
URL flash://system/configuration/startup-config
02-Mar-2017 07:57:17 %COPY-N-TRAP: The copy operation was completed successfully
```

You should now have successfully configured DHCP snooping on your switch through the command line interface.