CONFIG TOOLBOX

by real engineers

```
! DHCP Snooping is a security feature on switches that acts like a firewall between your users and
! devices and the DHCP Server.  Connected hosts are considered ‘untrusted’ and the DHCP Server
! is ‘trusted’.  This feature does the following when enabled on a switch:
!
!    - It will help prevent unauthorized DHCP Servers on your network
!    - Validates DHCP messages from untrusted sources and discards invalid messages
!    - Rate-limits DHCP traffic on trusted and untrusted sources
!    - Maintains a database of untrusted hosts with associated leased IP addresses
!    - The DHCP Server must be connected to the switch through trusted interfaces
!    - DHCP requests will only be forwarded from untrusted interfaces to trusted interfaces
!
! The DHCP Snooping database (aka binding) will be local on the switch and stored in memory, so
! it won’t survive a power loss or reboot.  This isn’t a concern if you are only running basic DHCP
! Snooping; however, if you are using Snooping with advanced features, such as dynamic ARP
! inspection or IP source guard, then you will run into problems if the database is down.  In
! this case, you will want a backup of the database.  The easiest way of doing this is configuring
! DHCP Snooping to store the database on a TFTP or FTP server.  However, it is unlikely that a
! small/mid network will be running these advanced features, so it should not be a concern and
! just something for you to be aware of.
!
!             - Email info@configtoolbox.com if you have any questions.
!
!
!
! DHCP Snooping operates on a per-VLAN basis by default, but has no active VLAN’s assigned.
! You will need to enable it on each VLAN connected to users, printers, copiers, etc.
ip dhcp snooping vlan 1-10,50 >>>>>>> This example enables snooping on VLAN’s 1-10 and 50
ip dhcp snooping
!
! All switch ports will be untrusted by default, so you only need to configure the trusted ports.
! These will generally be all uplink trunk ports to other switches and ports connecting to your
! individual servers or ports to your server farm, such as VMware or Hyper-V.  In this example, we
! will make switch port 49 trusted since a valid DHCP Server is downstream on that port.
interface GigabitEthernet1/0/49
 description UPLINK TRUNK TO NEIGHBOR SWITCH
 switchport mode trunk
 ip dhcp snooping trust
!
!
! Here are some commands to check operation and view the DHCP database (aka binding)
show ip dhcp snooping
show ip dhcp snooping binding
```

Let us know if you have any questions or need config guidance.
- Config Toolbox @ https://configtoolbox.com/contact-us

PRIVACY POLICY

Config Toolbox is mindful of your privacy. Please see our website for Disclaimer, Privacy Policy, and Terms and Conditions. (https://configtoolbox.com/config-toolbox-blog)