DHCP SNOOPING CONFIGURATION

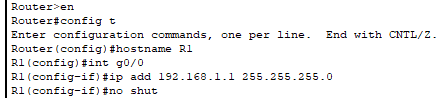
DCHP Snooping Trusted and Untrusted Ports

Inacio Andre

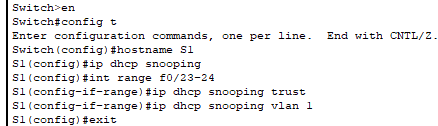
2024

* **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.

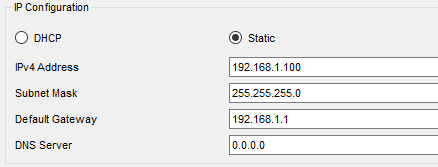
R1



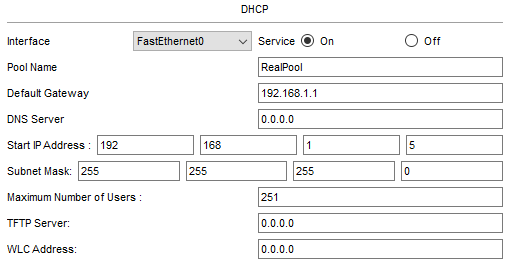
S1

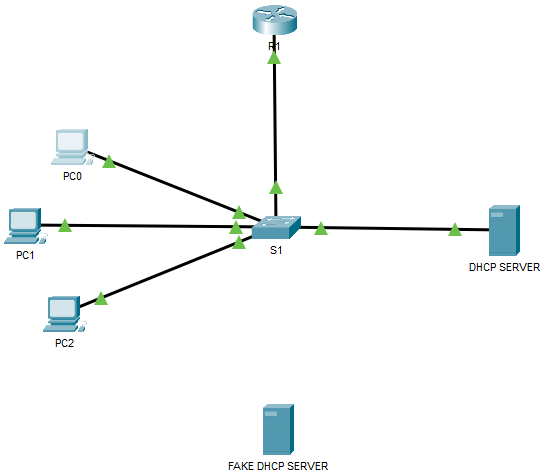


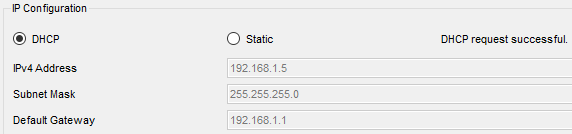
REAL DHCP SERVER



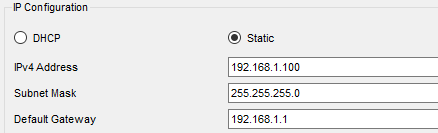
DHCP POOL







FAKE DHCP SERVER



DHCP POOL

