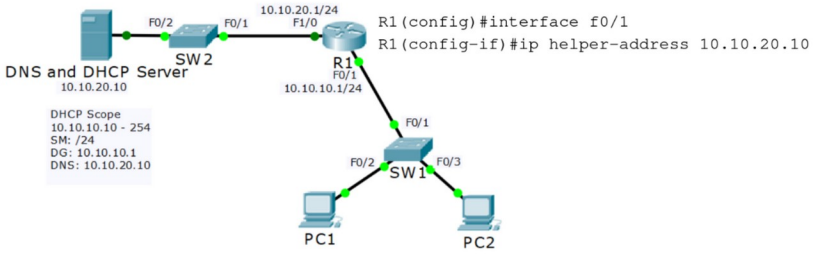
ARP Inspection and DHCP Snooping

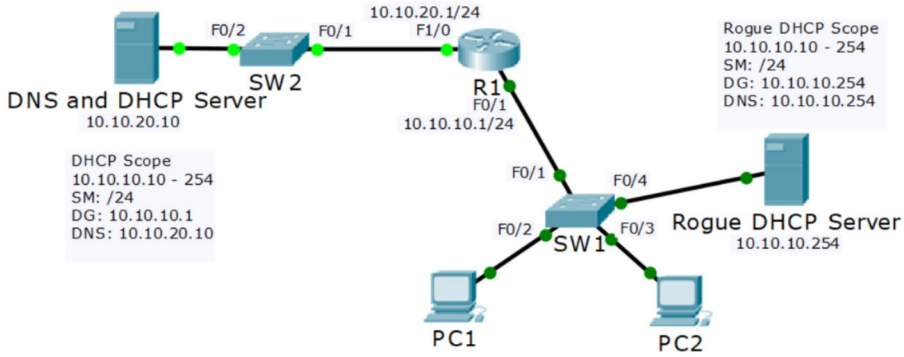
These a port security features for a Switch
When DHCP Snooping is enabled (for a VLAN), DHCP Server responses are dropped if they don't come from a trusted port.
DHCP Snooping is enabled for an entire VLAN
SW1(config)#ip dhcp snooping vlan 10
And on the interface you would like to trust
SW1(config)#interface fa0/0
SW1(config-if)#ip dhcp snooping trust

DHCP Snooping

External DHCP Server Configuration
R1(config)#interface f0/1
R1(config-if)#ip helper-address 10.10.20.10



Rogue DHCP Server



Dynamic ARP Inspection (DAI)

- a security feature that rejects invalid and malicious ARP packets
- DAI prevents a class of man-in-the-middle attacks, where an unfriendly station intercepts traffic for other stations by poisoning the ARP caches of its unsuspecting neighbors.
- The miscreant sends ARP requests or responses mapping another station's IP address to its own MAC address. known as ARP poisoning or ARP cache poisoning
- DAI relies on DHCP snooping
- DHCP snooping listens to DHCP message exchanges and builds a bindings database of valid tuples (MAC address, IP address, VLAN interface).
- When enabled, the switch drops ARP packet if the sender MAC address and sender IP address do not match an entry in the "DHCP snooping bindings database"
- DAI is not performed on trusted ports

- Enable this for non DHCP clients

802.1x Identity Based Networking

When 802.1x is enabled, only authentication traffic is allowed on switch ports, until the host and user are authenticated

When the user has entered a valid user name and password, the switch port transitions to a normal access port in the relevant VLAN

Port Security

Enables an admin to specify which MAC address(es) can send traffic into an individual switch port

This can be used to lock a port down to a particular host ot hosts

It is easy to spoof a MAC address, so locking ports down to a specific host is not usually Port Secuirty's main rol in production netwroks

Port Secuirty can also configure individual switch ports to allow only a specified number of source MAC addresses to send traffic into that port

It can learn connected mac address (statically or dynamically)

This is useful to prevent users from adding Wireless Access Points or other shared devices

Three Options when an unauthorized MAC address sends traffic into the port

Shutdown - (Default) the interface is placed into the error-disabled state, blocking all traffic

Protect – Traffic from unauth add is dropped, traffic from auth add is forwarded

Restrict – Traffic from unauth add is dropped, logged, and the violation counter is incremented

To bring an error-disabled port back into service

Physically remove ht host with the offending MAC address

Manually shutdown then no shut the interface

Auto-Recovery

You can bring disabled ports back into service automatically after thy have been disabled for a configurable period of time (in seconds0

Sw1(config)#errdisable recovery cause psecure-violation

Sw1(config)#errdisable recovery interval 600 (seconds)