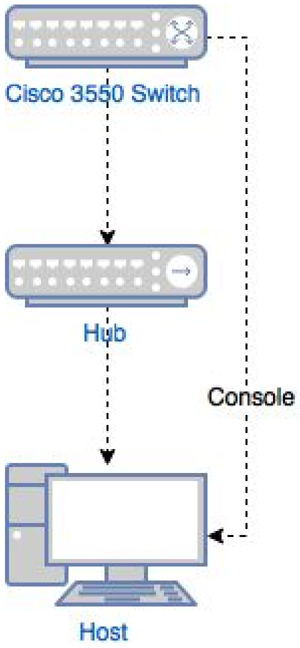
Securing your Network

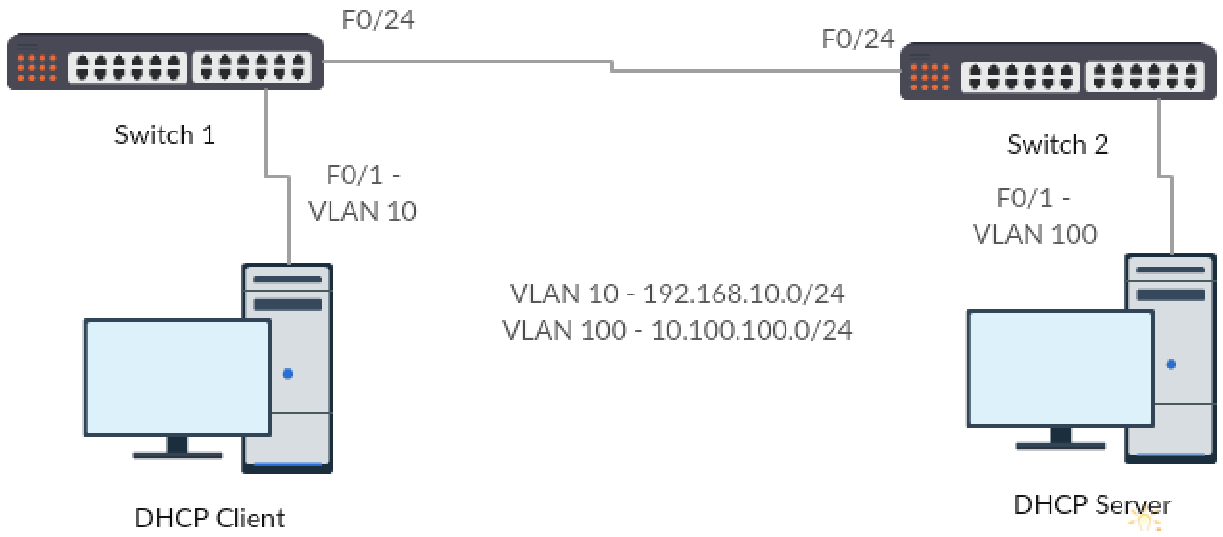
Port Security: Defining how many and/or what MAC addresses are allowed on a port.



1. Set up the simple topology shown above. Connect a single host to the hub and connect the hub to the switch. Establish a console connection between the host and the switch. No IP address configuration is necessary as port security operates at layer 2.
2. Under the interface configuration mode for the port your hub is connected to, issue the following commands:
   a. `switchport mode access`
   b. `switchport port-security`
   c. `switchport port-security maximum 1`
3. Now that we have defined a maximum of 1 host (mac address) allowed on the port, add a second host by connecting it to the hub. What happened on your switch? Hint: take a look at the console window.

4. Experiment with the command `switchport port-security violation ?`. Can you guess what the default violation mode is based on what happened above?
5. Now, remove the maximum 1 configuration line. Add a configuration line to only allow 1 of your host's mac addresses. Do not use the maximum command. Hint: `switchport port-security mac-address XXXX.XXXX.XXXX`.
6. With the default mode, every time a port enters the disabled state, an administrator must manually issues the `shutdown` and `no shutdown` commands to bring an interface back up.

<u>DHCP Snooping</u>: Preventing rogue DHCP servers by defining what port DHCP offers can be received on.



1. On the DHCP server, download the server program from http://www.dhcpserver.de/cms/download. Disconnect from the lab network and connect to your topology. Assign the DHCP server a static IP address in the 10.100.100.0/24 network. Configure the server using the wizard. Create a pool for the 192.168.10.0 network, specifying 192.168.10.254 as the gateway address. Start the DHCP server on the interface connected to your topology.
2. Finish connecting your topology as shown above. Switch 1 should NOT have ip routing enabled, but Switch 2 MUST have ip routing enabled. Both switches should have VLANs 10 and 100.

3. Switch 2 should have VLAN interfaces for VLANs 10 and 100, both ending in .254/24. Configure the VLAN 10 interface to have an IP helper address of the IP address of your DHCP server. This enables DHCP relaying.
4. Next, we need to enable DHCP snooping on switch 1, the client switch. In global configuration mode, enter the commands `ip dhcp snooping`, `ip dhcp snooping vlan 10`, and `no ip dhcp snooping information option`.
5. Ensure your ports are configured in the correct VLANs, as designated by the diagram above. Connect your client PC to switch 1 and see if it is able to obtain an IP address. Why doesn't it work?
6. To allow DHCP offers to enter the trunk port on switch 1, we must enter interface configuration mode and use the command `ip dhcp snooping trust`.
7. Try obtaining an IP address on the client, again. Does it work this time?
8. Once you have an address, use the command `show ip dhcp snooping binding` on the switch. What type of information is in the DHCP snooping binding table? This information is critical for the next part of the lab.

IP Source Guard (IPSG): Prevents a host from spoofing the IP address of another host.

1. Enabling IP source guard is very easy. It should be enabled on all ports that are untrusted, such as ports that clients are connected to.
2. Enter into interface configuration mode for the client PC and type `ip verify source`.
3. Change the client's IP address manually to a different address than the one provided by DHCP. Can the client still ping its gateway? Why not?

The DHCP snooping binding table plays a critical role with IP source guard functionality. If IPSG is enabled on an interface, the switch makes sure that the MAC address and IP address of packets received match the information in the DHCP snooping binding table. If not, the traffic does not get forwarded, hence preventing IP address spoofing.

Dynamic ARP Inspection (DAI): Prevents MAC address spoofing and ARP poisoning by ensuring ARP replies contain the correct MAC address based on the IP address.

1. Enabling DAI is even easier than IPSG. In global configuration mode, enter the command `ip arp inspection vlan 10`.

Once again, the DHCP snooping binding table plays a crucial role in assisting DAI. When an ARP reply is seen, the switch verifies the MAC and IP addresses based on the information contained in the DHCP snooping binding table.

*Be aware that any host using static addressing in a DHCP snooping enabled VLAN will need to have its MAC address and IP address manually added to the DHCP snooping binding table. This is done using the command `ip dhcp snooping binding [MACADDR] vlan [vlan] [IPADDR] interface [INTERFACE] expiry [EXP IN SEC]` command in privileged EXEC mode.