Basic Switched Network (Layer 2)

How a Switch Works

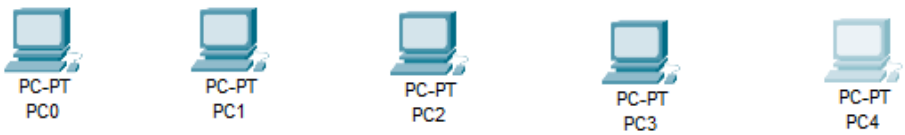
- ➔ Switches are network devices that are used to interconnect links to form a larger network
- ➔ They operate on the data link layer (layer 2) by forwarding information based on the destination MAC address (this function is referred to as switching/forwarding)
- ➔ Out of the box, Cisco switches are fully operational and do not require any configuration for basic functionality.
- ➔ More advanced configuration will be covered in the next lab.

MAC Address Table

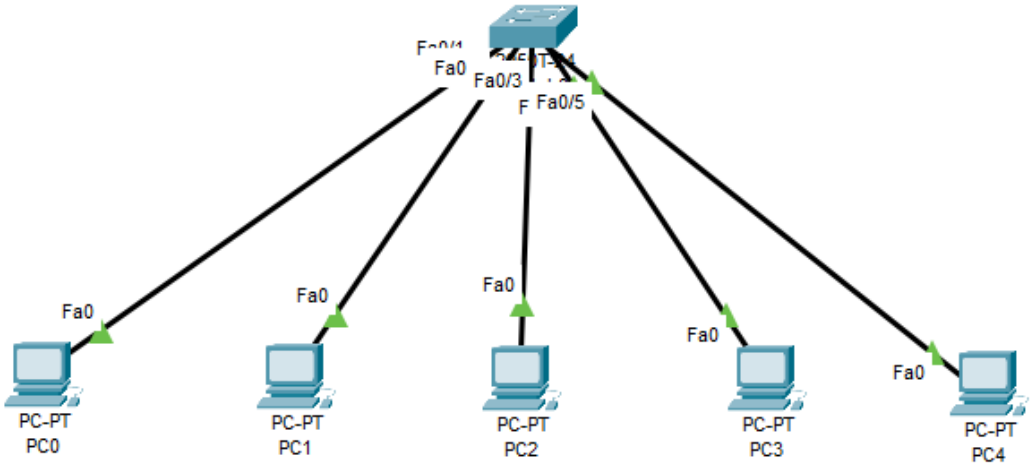
- ➔ Layer 2 network switches keep a table in their memory that matches MAC addresses to the switch's Ethernet ports
- ➔ Referred to as a Content Addressable Memory (CAM) table
- ➔ Once a switch receives an ethernet frame, it adds its MAC address and the port it was sourced from to the CAM table. Then, it looks in the CAM table for an exact match for the destination address. If one is not found, the switch floods that packet out of all ports.
- ➔ The current CAM table is can be viewed on a Cisco switch by using the following command in user-exec mode
  - ◆ **Switch#** show mac address-table

Creating the Basic Switched Network

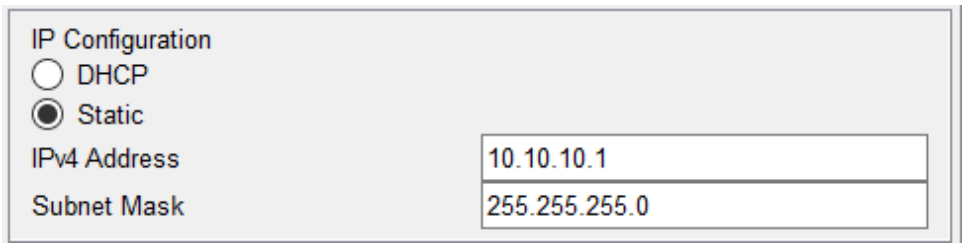
1. Drag and drop 1 switch and 5 PCs.



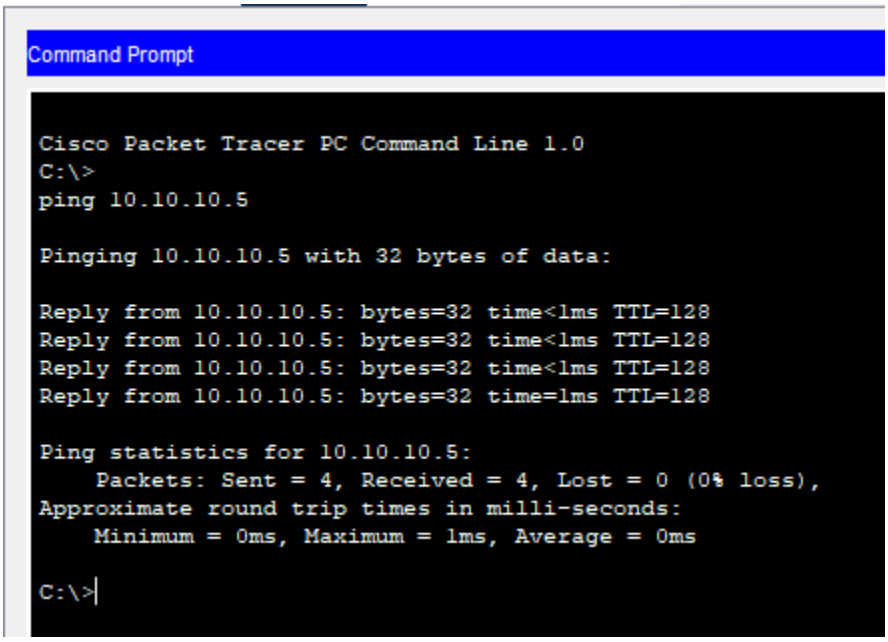
2. Connect the fastEthernet interfaces on the PCs to the switch. Because we are treating the switch as an unmanaged ‘dumb’ switch for this lab, it does not matter what ports you use.



3. We now need to assign an IP address to each of our PCs so that they can communicate with one another.
    a. Start with 10.10.10.1 255.255.255.0 and increment the last octet until you assign 10.10.10.5 255.255.255.0

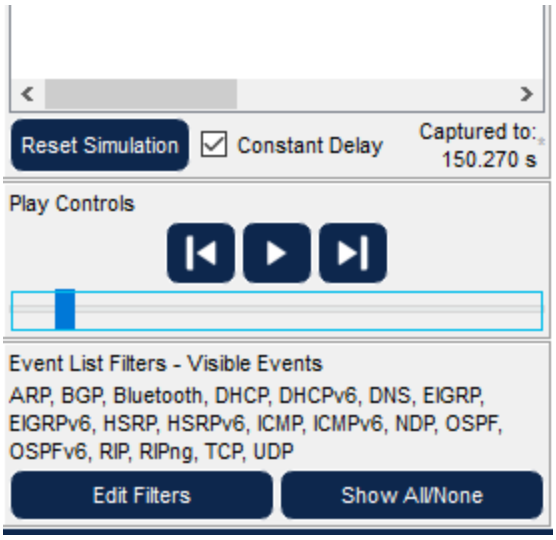


4. Send a packet from PC0 to PC5 using the PING command using the command prompt on PC0

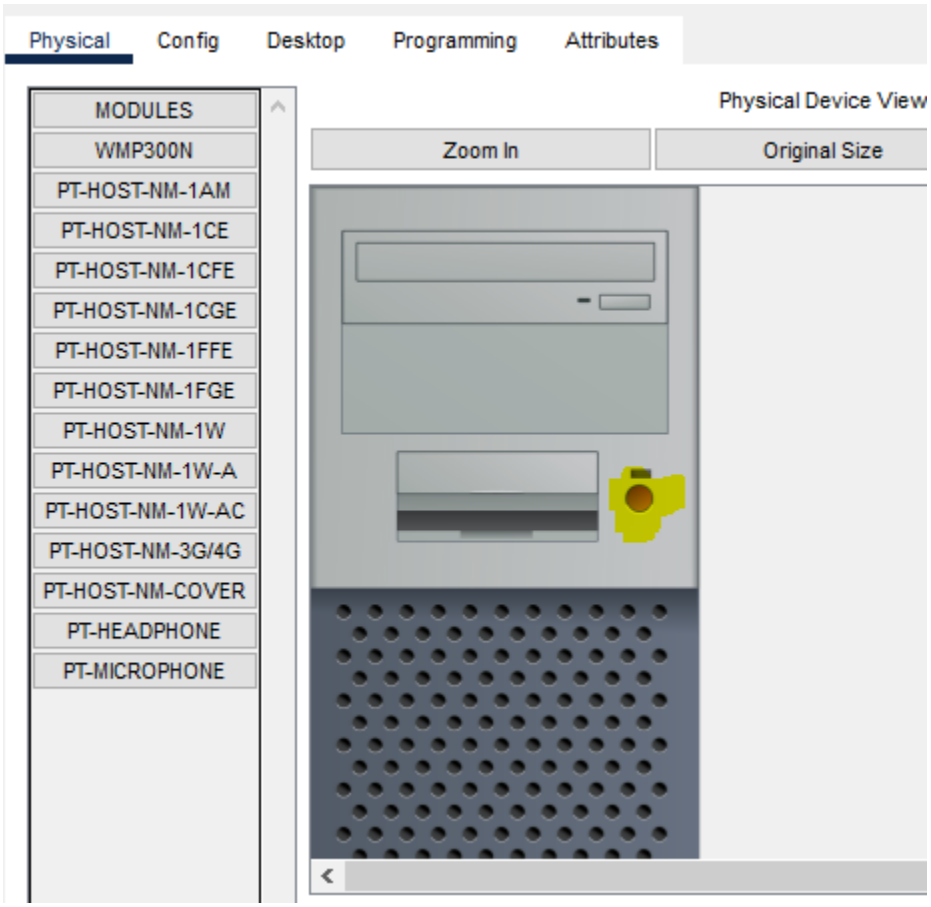


Now, we are going to view this traffic in detail using the simulation tool in the bottom-right of the screen.

Click ‘simulation’ and then the ‘play’ button.

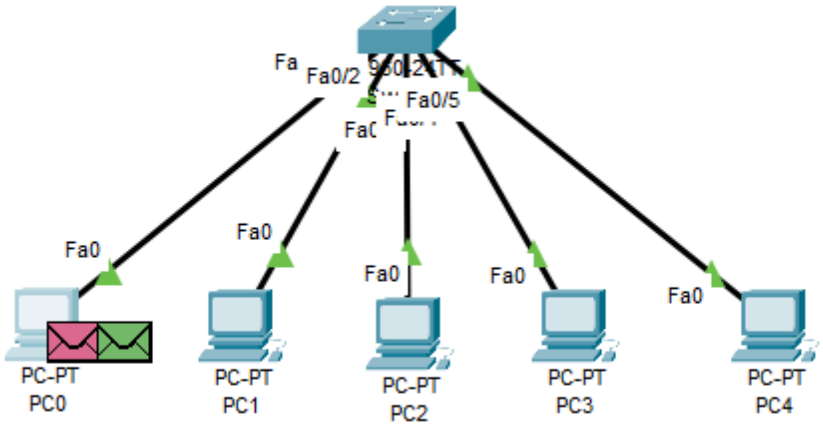


Go back to PC0 and power cycle it in the ‘physical’ tab by clicking the power button on the simulated PC twice.

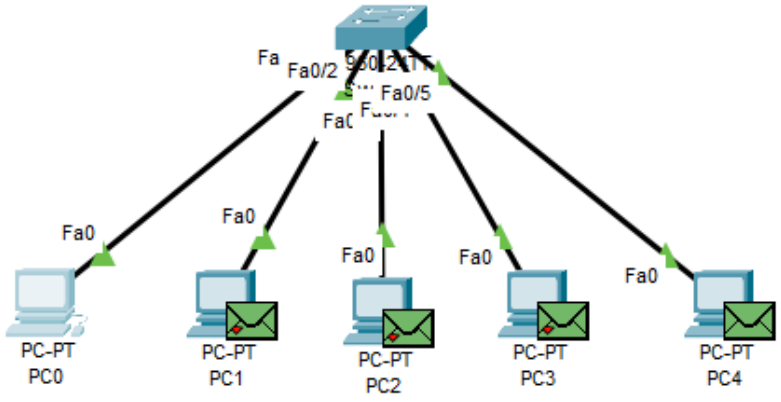


This will clear out the ARP cache of the PC.

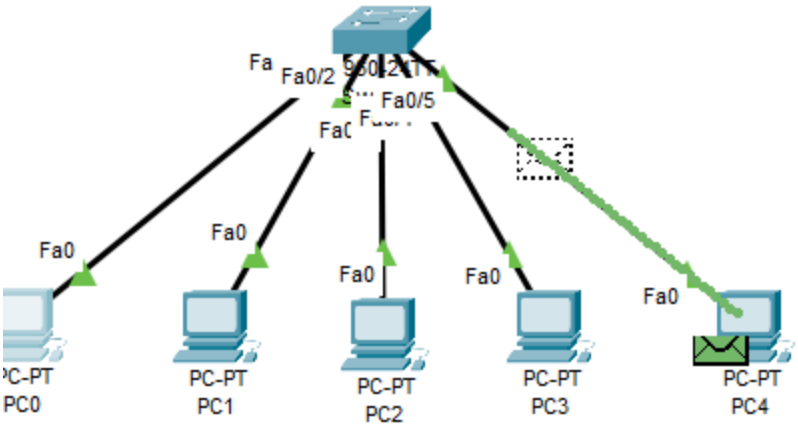
Now Ping PC 4 again.



As you can see, the green ARP packet originates at PC0. This is because PC0 does not know the MAC address that is corresponds to the IP address that was pinged, so It must use ARP to find this address before it can send the ICMP Echo packet.



Because the destination MAC address was a broadcast address, the switch forwarded it out to all active ports.



PC 4 responds to the ARP request with its MAC information

PC 0 is now able to send the ICMP ECHO request directly to PC4

5. Click on the switch and go into the CLI. Enter these commands and you can see the MAC address table filled with the MAC addresses of PC1 and PC5. If you were to create network traffic with the other PCs, then they would also show up as well.

```
Switch>enable
Switch#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    00d0.bc04.b69e    DYNAMIC     Fa0/5
   1    00e0.8f63.dcd8    DYNAMIC     Fa0/1
Switch#
```