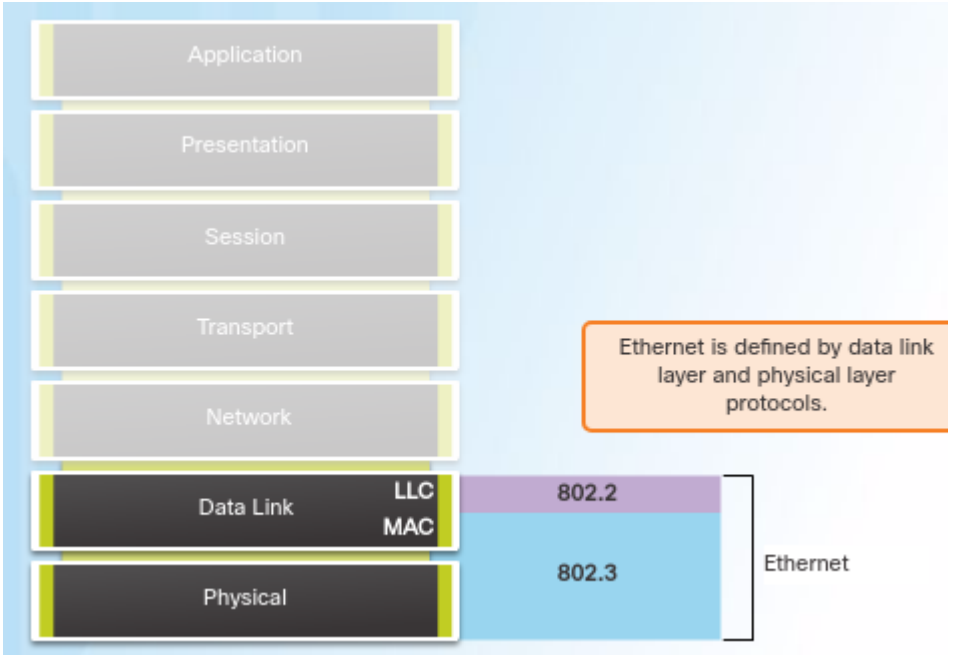
Ethernet

Ethernet

- The OSI physical layer provides the means to transport the bits that make up a data link layer frame across the network media.
- Ethernet is now the predominant LAN technology in the world
- Ethernet operates in the data link layer and the physical layer.
- Ethernet protocol standards define many aspects of network communication including frame format, frame size, timing, and encoding. When messages are sent between hosts on an Ethernet network, the hosts format the messages into the frame layout that is specified by the standards.
- The OSI model separates the data link layer functionalities of addressing, framing, and accessing the media from the physical layer standards of the media. Ethernet standards define both the Layer 2 protocols and the Layer 1 technologies.

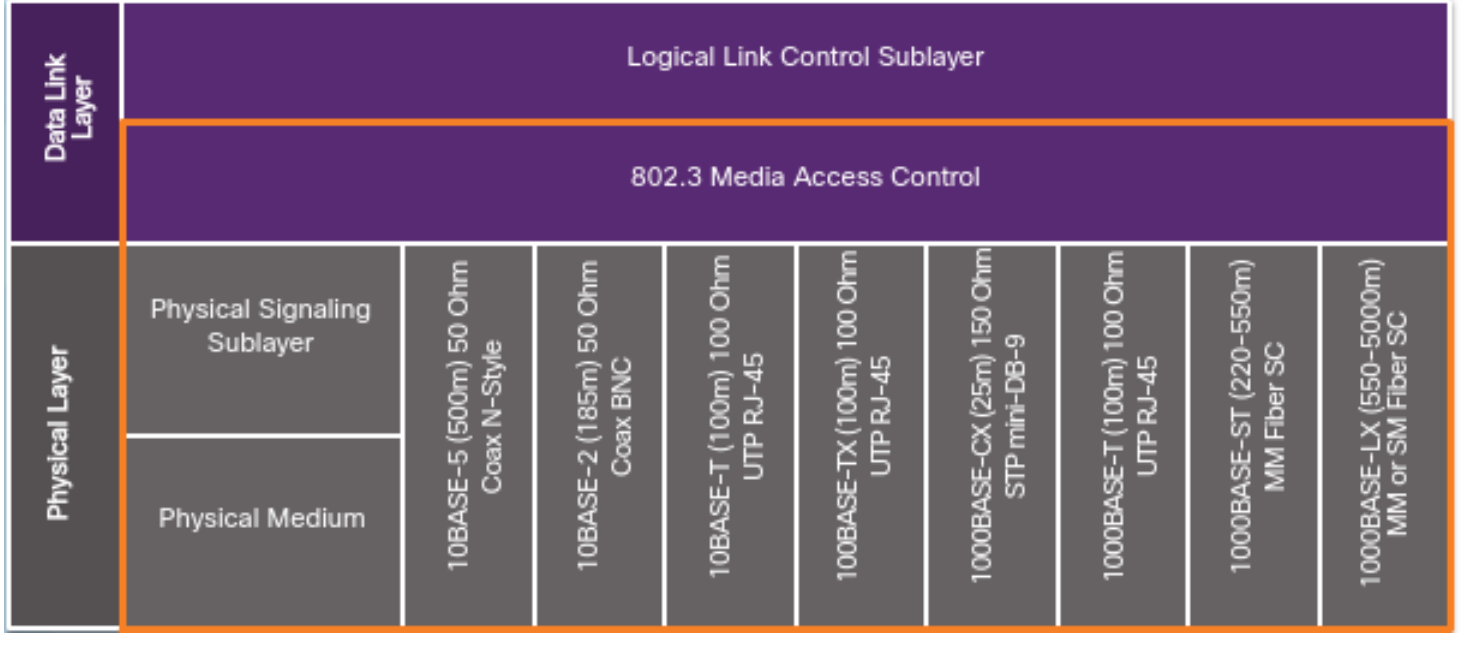
Ethernet Encapsulation



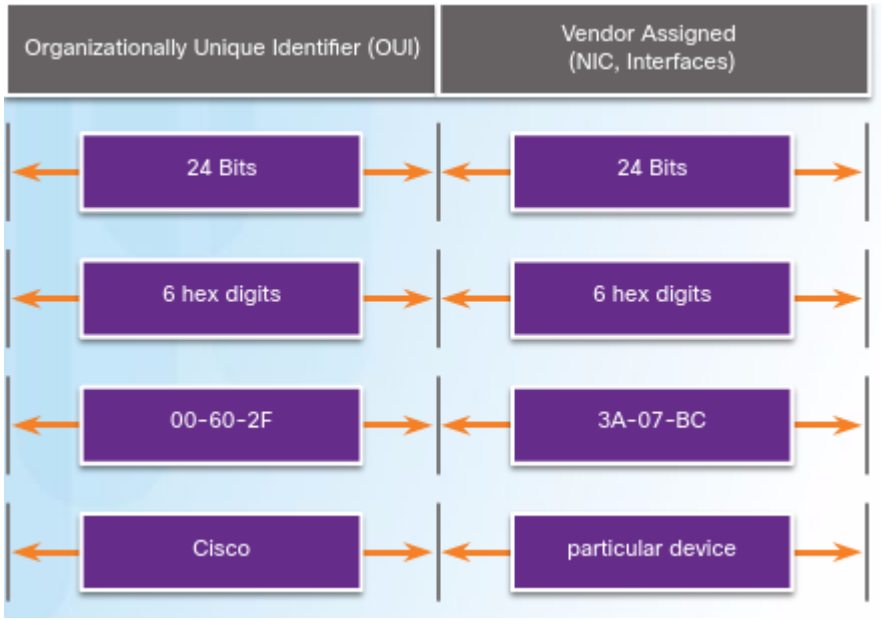
- Ethernet supports data bandwidths of:
- 10 Mb/s,100 Mb/s
- (1 Gb/s),10 Gb/s, 40 Gb/s,100 Gb/s
- It is a family of networking technologies that are defined in the IEEE 802.2 and 802.3 standards.
- Ethernet relies on the two separate sublayers of the data link layer to operate, the Logical Link Control (LLC) and the MAC sublayers.

MAC Sublayer

- The Ethernet MAC sublayer has two primary responsibilities:
- Data encapsulation
- Media access control
- The data encapsulation process includes frame assembly before transmission, and frame disassembly upon reception of a frame. The MAC layer adds a header and trailer to the network layer PDU.



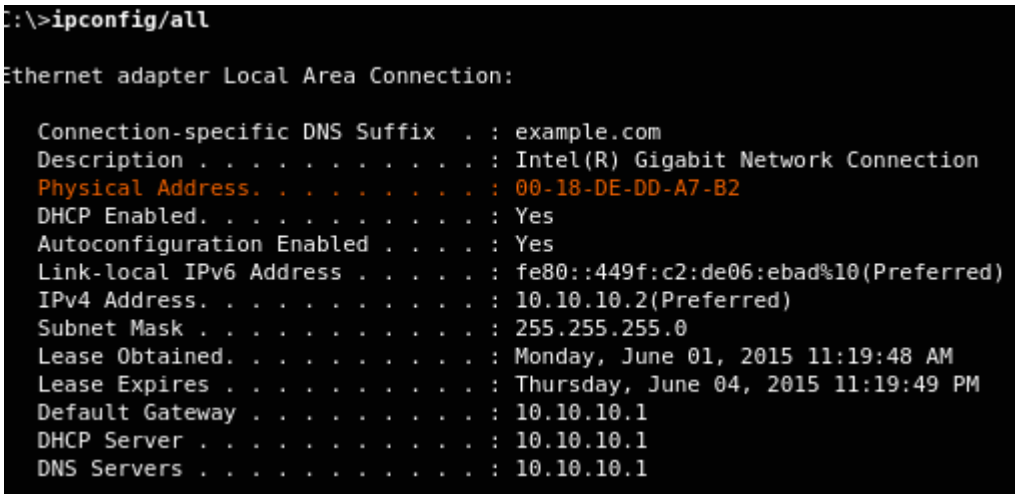
MAC Address: Ethernet Identity



- In Ethernet, every network device is connected to the same, shared media
- The rules established by IEEE require any vendor that sells Ethernet devices to register with IEEE.
- The IEEE assigns the vendor a 3-byte (24-bit) code, called the Organizationally Unique Identifier (OUI)
- All MAC addresses assigned to a NIC or other Ethernet device must use that vendor's assigned OUI as the first 3 bytes.
- All MAC addresses with the same OUI must be assigned a unique value in the last 3 bytes.

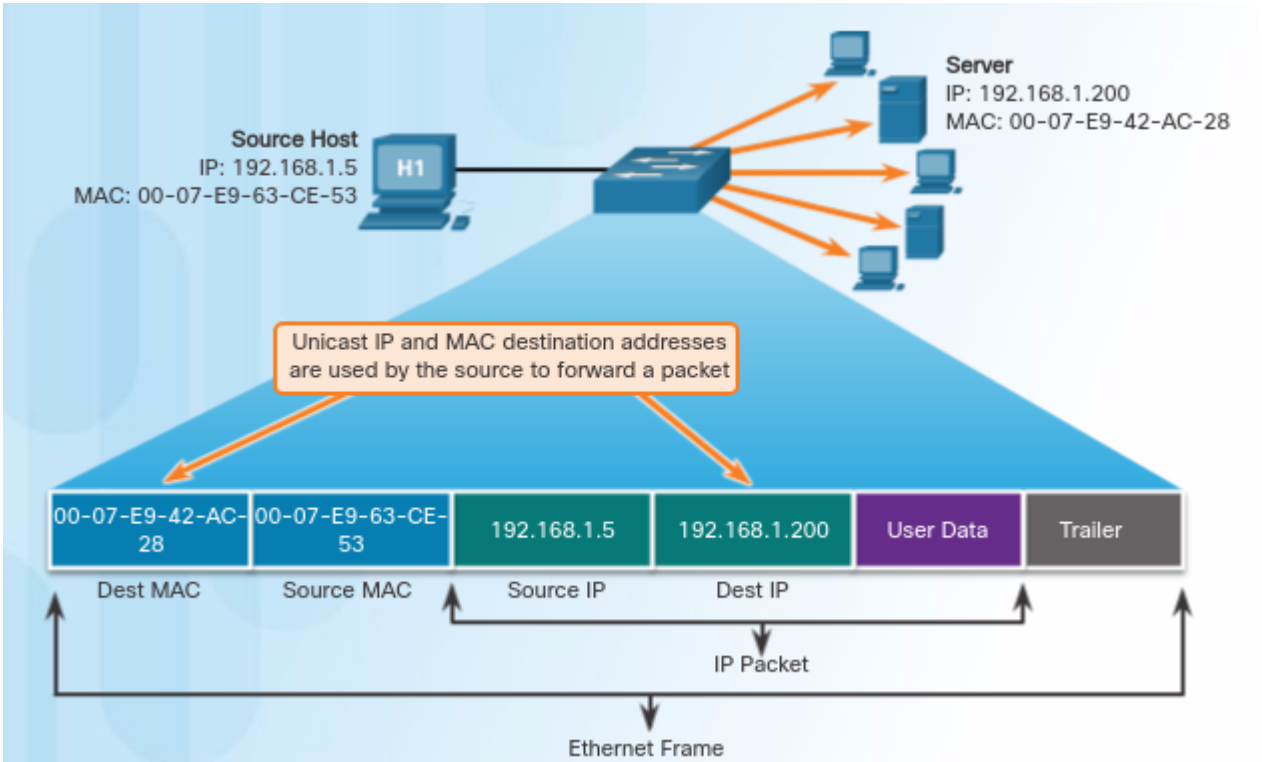
MAC Address Representations

- On a linux host, the ifconfig -a command can be used to identify the MAC address of an Ethernet adapter
- Notice the display indicates the Physical Address (MAC) of the computer to be 00-18-DE-DD-A7-B2



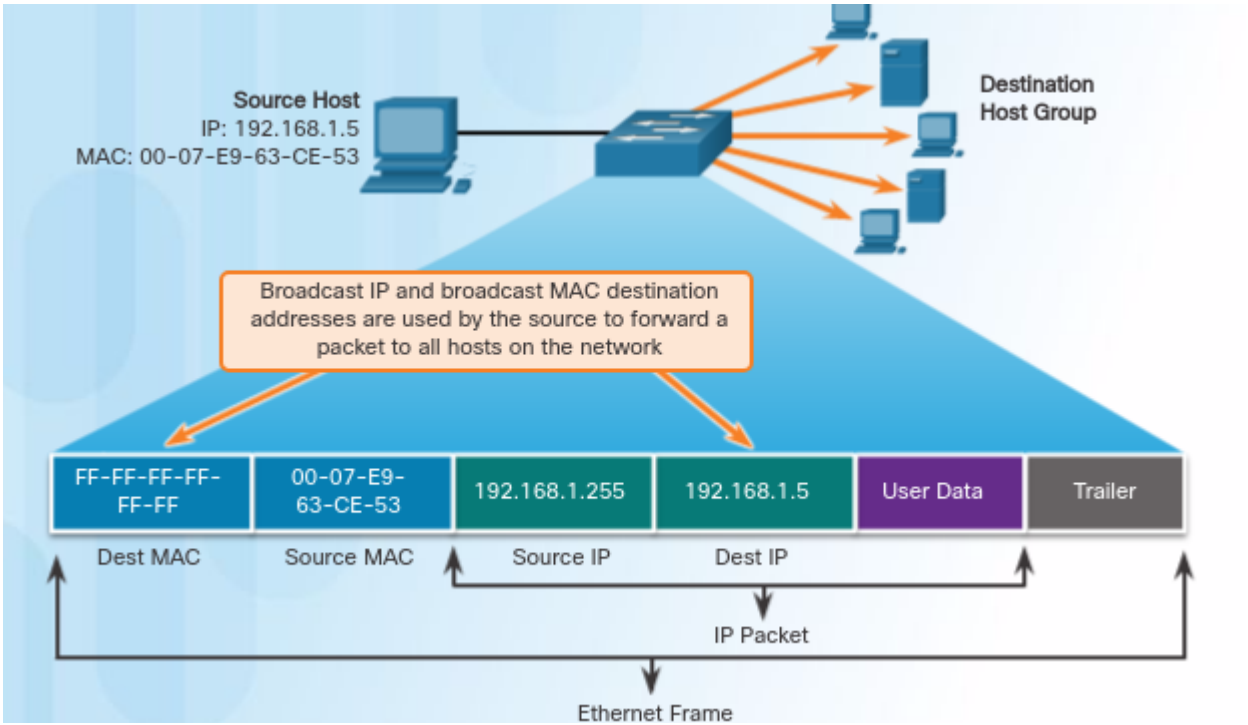
Unicast MAC Address

- A unicast MAC address is the unique address used when a frame is sent from a single transmitting device to a single destination device.
- For a unicast packet to be sent and received, a destination IP address must be in the IP packet header. A corresponding destination MAC address must also be present in the Ethernet frame header.
- The IP address and MAC address combine to deliver data to one specific destination host.The process that a source host uses to determine the destination MAC address is known as Address Resolution Protocol (ARP).



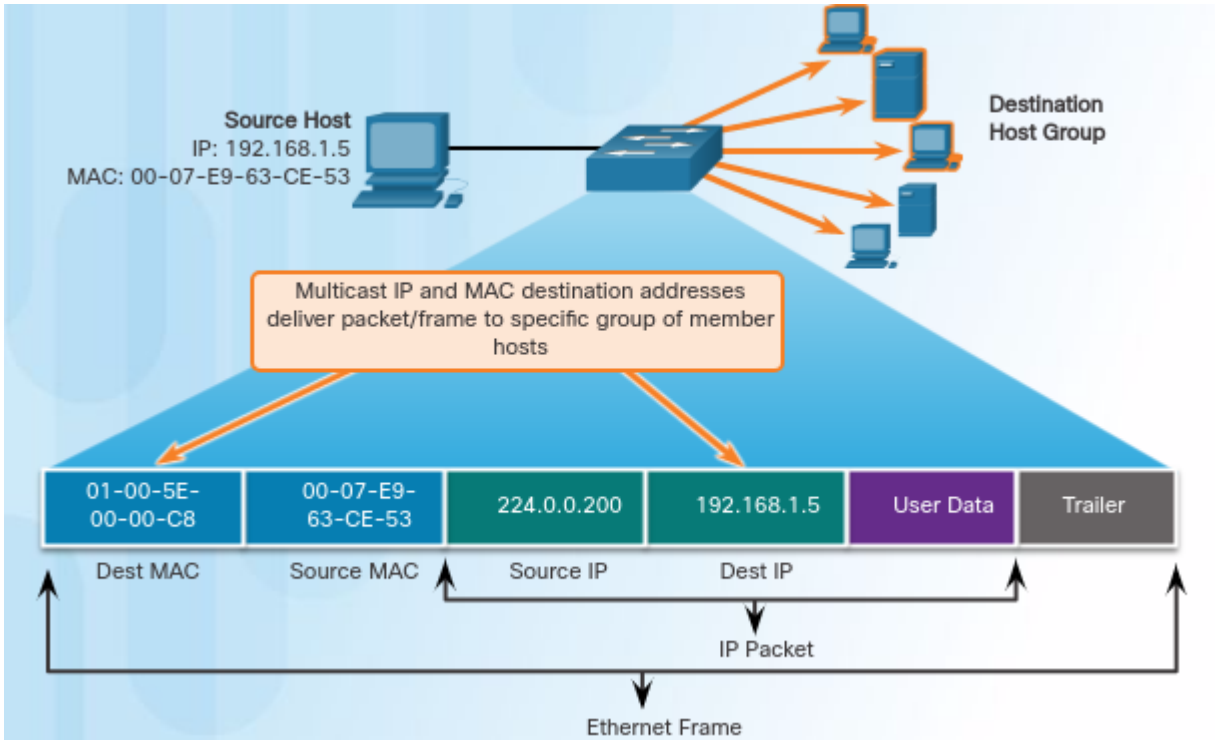
Broadcast MAC Address

- A broadcast packet contains a destination IPv4 address that has all ones (1s) in the host portion. Many network protocols, such as DHCP and ARP, use broadcasts.The source host sends an IPv4 broadcast packet to all devices on its network.
- The IPv4 destination address is a broadcast address, 192.168.1.255. When the IPv4 broadcast packet is encapsulated in the Ethernet frame, the destination MAC address is the broadcast MAC address of FF-FF-FF-FF-FF-FF



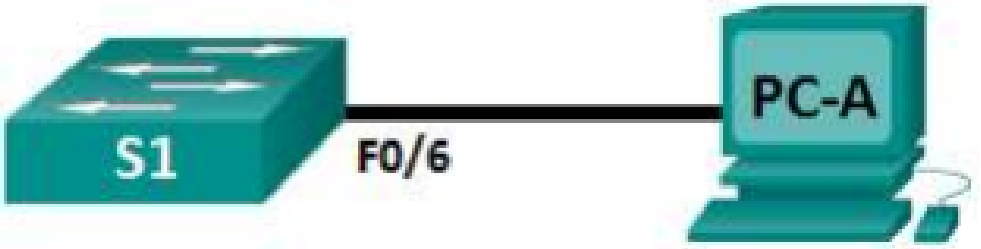
Multicast MAC Address

- Multicast addresses allow a source device to send a packet to a group of devices. Devices that belong to a multicast group are assigned a multicast group IP address.
- The range of IPv4 multicast addresses is 224.0.0.0 to 239.255.255.255.As with the unicast and broadcast addresses, the multicast IP address requires a corresponding multicast MAC address to actually deliver frames on a local network.
- The multicast MAC address associated with an IPv4 multicast address is a special value that begins with 01-00-5E in hexadecimal.



Lab – Viewing Network Device MAC Addresses

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 1	192.168.1.1	255.255.255.0	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objectives

Part 1: Configure Devices and Verify Connectivity

Part 2: Display, Describe, and Analyze Ethernet MAC Addresses

Continue

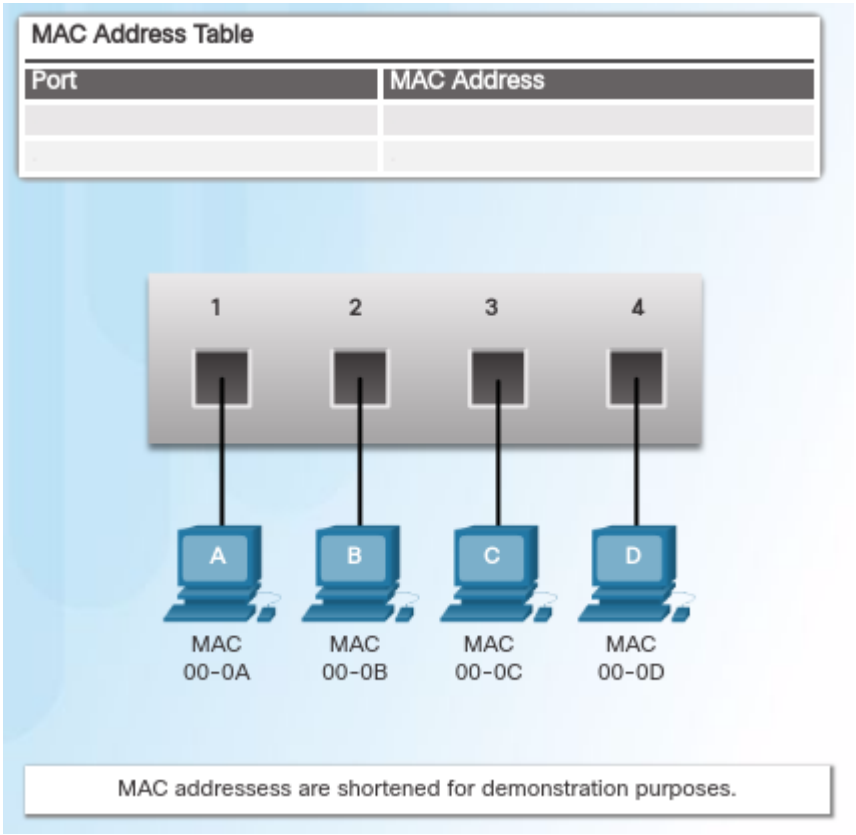
- Configure the IPv4 address, subnet mask, and default gateway address for PC-A.
- From the command prompt on PC-A, ping the switch address.
- In this step, you will configure the device name and the IP address, and disable DNS lookup on the switch.

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname S1
// Disable DNS lookup.
S1(config)# no ip domain-lookup
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.1 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# end// Ping the switch from PC-A.
```

Analyze the MAC address for PC-A

- To find the manufacturer, you can use a tool like www.macvendorlookup.com or go to the IEEE web site to find the registered OUI vendor codes.
- From the command prompt on PC-A, issue the ipconfig /all command and identify the OUI portion of the MAC address for the NIC of PC-A.
- You can use a variety of commands to display MAC addresses on the switch.
- use the **show interfaces vlan 1** command to find the MAC address information.
- Another way to display the MAC address on the switch is to use the **show arp** command.
- This command maps the Layer 2 address to its corresponding Layer 3 address.
- View the MAC addresses on the switch- Issue the **show mac address-table** command on S1

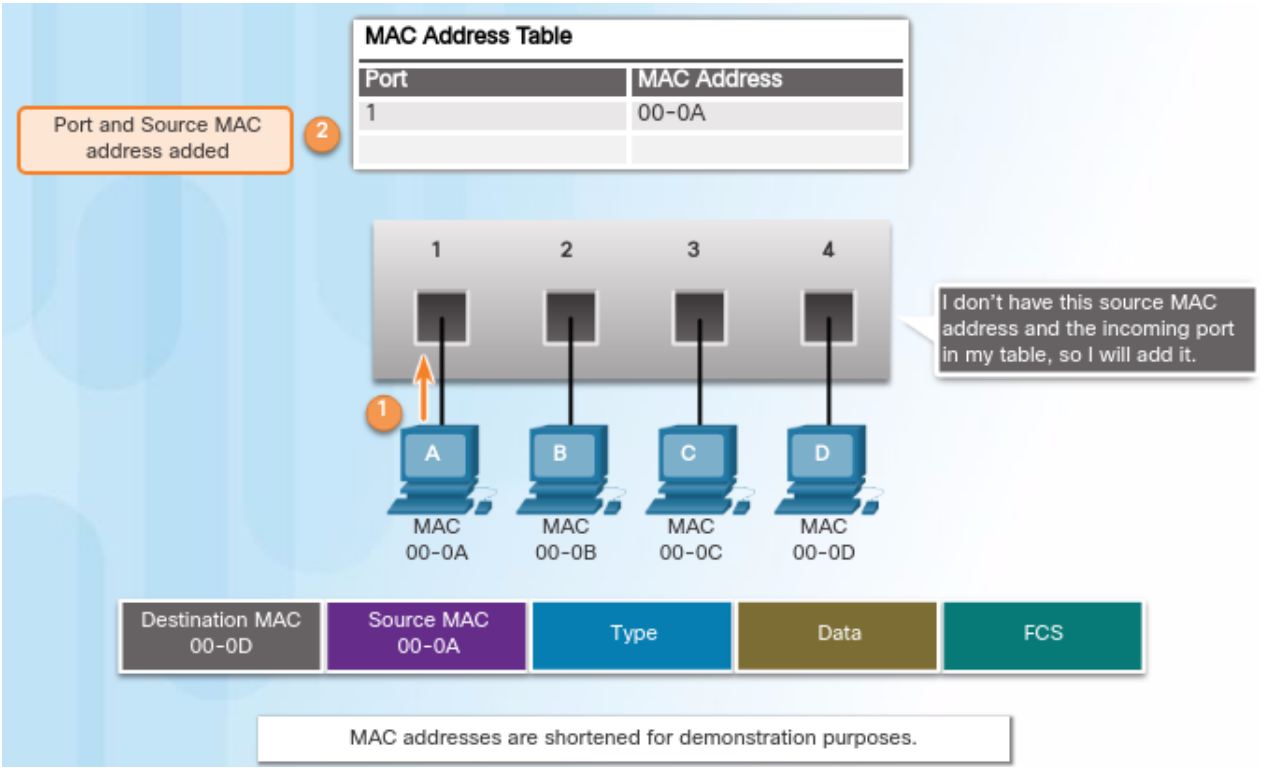
Switch Fundamentals



- A Layer 2 Ethernet switch uses MAC addresses to make forwarding decisions.
- It is completely unaware of the protocol being carried in the data portion of the frame, such as an IPv4 packet.
- The switch makes its forwarding decisions based only on the Layer 2 Ethernet MAC addresses.
- Unlike legacy Ethernet hubs that repeat bits out all ports except the incoming port, an Ethernet switch consults a MAC address table to make a forwarding decision for each frame
- The MAC address table is sometimes referred to as a content addressable memory (CAM) table

Learning MAC Addresses

- The switch dynamically builds the MAC address table by examining the source MAC address of the frames received on a port
- The switch forwards frames by searching for a match between the destination MAC address in the frame and an entry in the MAC address table.
- Every frame that enters a switch is checked for new information to learn.



Filtering Frames

- As a switch receives frames from different devices, it is able to populate its MAC address table by examining the source MAC address of every frame.
- When the switch's MAC address table contains the destination MAC address, it is able to filter the frame and forward out a single port.
- Figures show PC-D sending a frame back to PC-A. The switch will first learn PC-D's MAC address. Next, because the switch has PC-A's MAC address in its table, it will send the frame only out port 1.