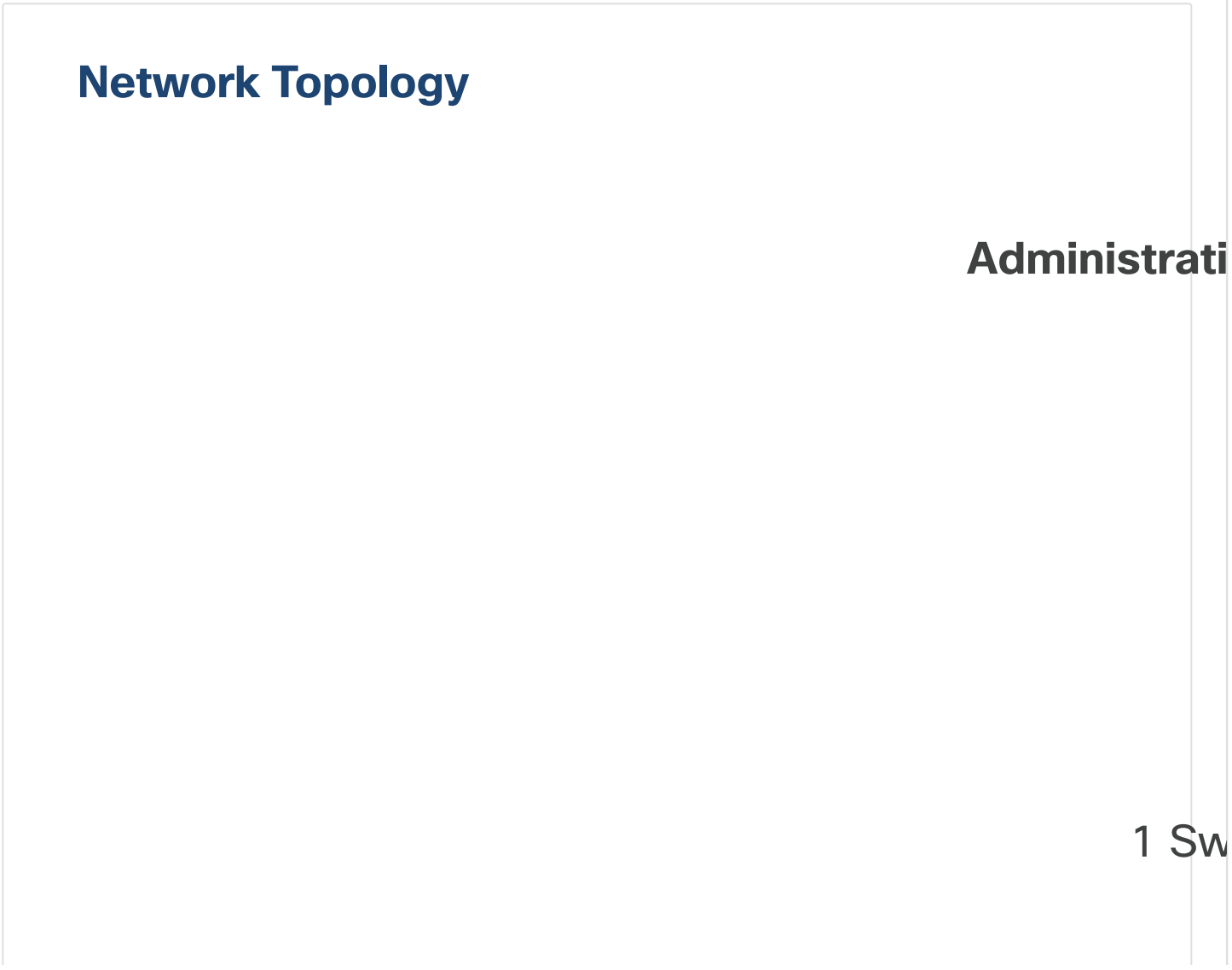
DevNet Associate v1.0

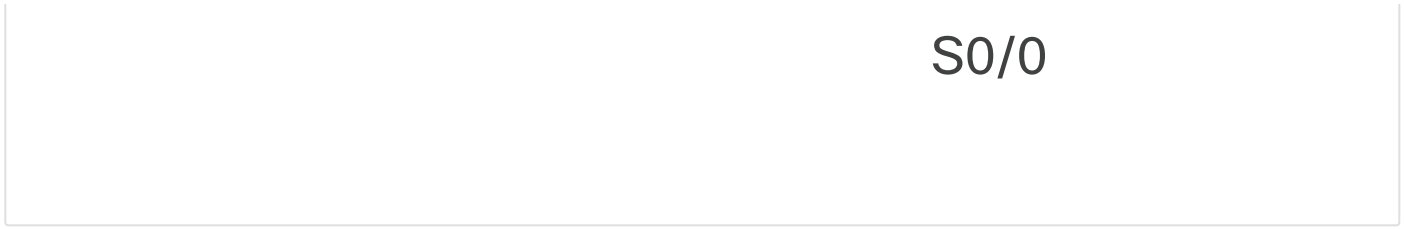
Network Interface Layer

5.2.1

Understanding the Network Interface Layer

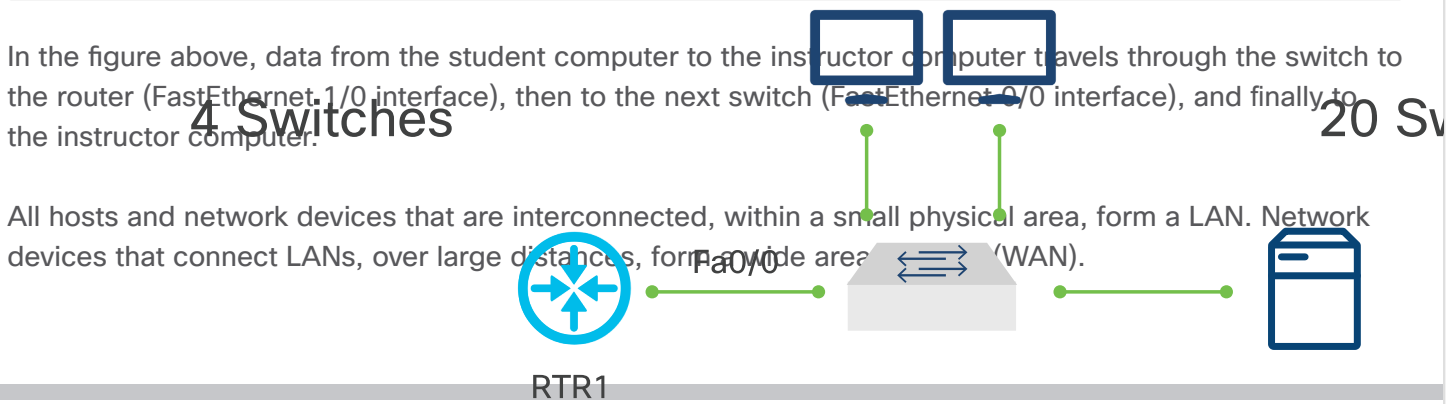
A network consists of end devices such as computers, mobile devices, and printers that are connected by networking devices such as switches and routers. The network enables the devices to communicate with one another and share data, as shown in the figure.





In the figure above, data from the student computer to the instructor computer travels through the switch to the router (FastEthernet 1/0 interface), then to the next switch (FastEthernet 0/0 interface), and finally to the instructor computer.

All hosts and network devices that are interconnected, within a small physical area, form a LAN. Network devices that connect LANs, over large distances, form a wide area network (WAN).



Connecting devices within a LAN requires a collection of technologies. The most common LAN technology is Ethernet. Ethernet is not just a type of cable or protocol. It is a network standard published by the IEEE. Ethernet is a set of guidelines and rules that enable various network components to work together. These guidelines specify cabling and signaling at the physical and data link layers of the OSI model. For example, Ethernet standards recommend different types of cable and specify maximum segment lengths for each type.

There are several types of media that the Ethernet protocol works with: coaxial cable, twisted copper pair cable, single mode and multimode fiber optics.

Bits that are transmitted over an Ethernet LAN are organized into frames. The Ethernet frame format is shown in the figure.

Ethernet Frame

In Ethernet terminology, the container into which data is placed for transmission is called a frame. The frame contains header information, trailer information, and the actual data that is being transmitted.

The figure above shows the most important fields of the Ethernet frame:

- **Preamble** – This field consists of seven bytes of alternating 1s and 0s that are used to synchronize the signals of the communicating computers.
- **Start of frame delimiter (SFD)** – This is a 1-byte field that marks the end of the preamble and indicates the beginning of the Ethernet frame.
- **Destination MAC Address** – The destination address field is six bytes (48 bits) long and contains the address of the NIC on the local network to which the encapsulated data is being sent.
- **Source MAC Address** – The source address field is six bytes (48 bits) long and contains the address of the NIC of the sending device.
- **Type** – This field contains a code that identifies the network layer protocol. For example, if the network layer protocol is IPv4 then this field has a value of 0x0800 and for IPv6 it has a value of 0x086DD.
- **Data** – This field contains the data that is received from the network layer on the transmitting computer. This data is then sent to the same protocol on the destination computer. If the data is shorter than the minimum length of 46 bytes, a string of extraneous bits is used to pad the field.
- **Frame Check Sequence (FCS)** – The FCS field includes a checking mechanism to ensure that the packet of data has been transmitted without corruption.

MAC addresses are used in transporting a frame across a shared local media. These are NIC-to-NIC communications on the same network. If the data (encapsulated IP packet) is for a device on another network, the destination MAC address will be that of the local router (default gateway). The Ethernet header and trailer will be de-encapsulated by the router. The packet will be encapsulated in a new Ethernet header and trailer using the MAC address of the router's egress interface as the source MAC address. If the next hop is another router, then the destination MAC address will be that of the next hop router. If the router is on the same network as the destination of the packet, the destination MAC address will be that of the end device.

5.2.3

MAC Addresses

All network devices on the same network must have a unique MAC address. The MAC address is the means by which data is directed to the proper destination device. The MAC address of a device is an address that is burned into the NIC. Therefore, it is also referred to as the physical address or burned in address (BIA).

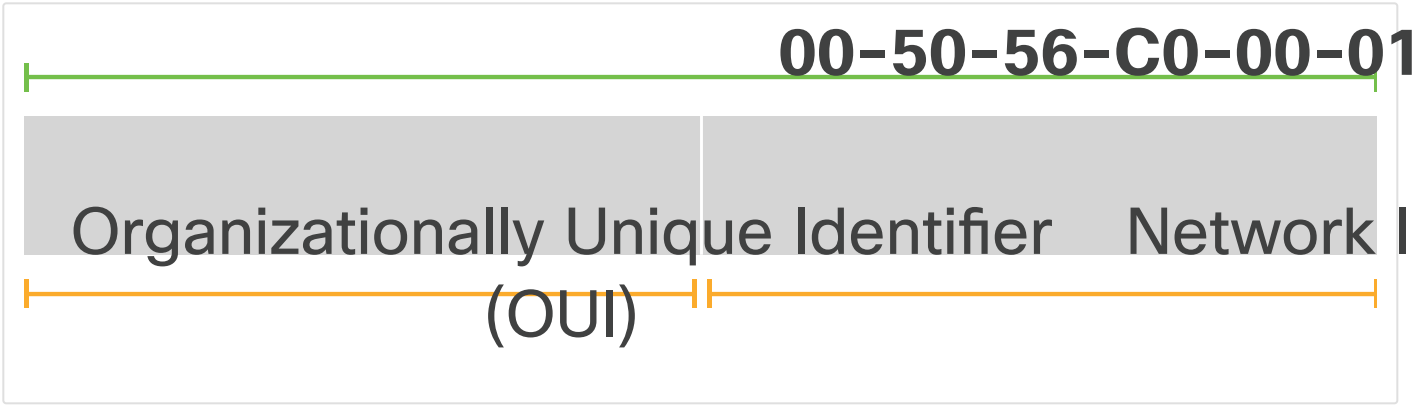
A MAC address is composed of 12 hexadecimal numbers, which means it has 48 bits. There are two main components of a MAC. The first 24 bits constitute the OUI. The last 24 bits constitute the vendor-assigned, end-station address, as shown in the figure.

- **24-bit OUI** – The OUI identifies the manufacturer of the NIC. The IEEE regulates the assignment of OUI numbers. Within the OUI, there are 2 bits that have meaning only when used in the destination address (DA) field of the Ethernet header:
- **24-bit, vendor-assigned, end-station address** – This portion uniquely identifies the Ethernet hardware.

A MAC address can be displayed in any of the following ways:

- 0050.56c0.0001
- 00:50:56:c0:00:01
- 00-50-56-c0-00-01

MAC Address Format



Destination MAC addresses include the three major types of network communications:

- **Unicast** – Communication in which a frame is sent from one host and is addressed to one specific destination. In a unicast transmission, there is only one sender and one receiver. Unicast transmission is the predominant form of transmission on LANs and within the internet.
- **Broadcast** – Communication in which a frame is sent from one address to all other addresses. In this case, there is only one sender, but the information is sent to all of the connected receivers. Broadcast transmission is essential for sending the same message to all devices on the LAN. Broadcasts are typically used one a device is looking for MAC address of the destination.
- **Multicast** – Communication in which information is sent to a specific group of devices or clients. Unlike broadcast transmission, in multicast transmission, clients must be members of a multicast group to receive the information.

5.2.4

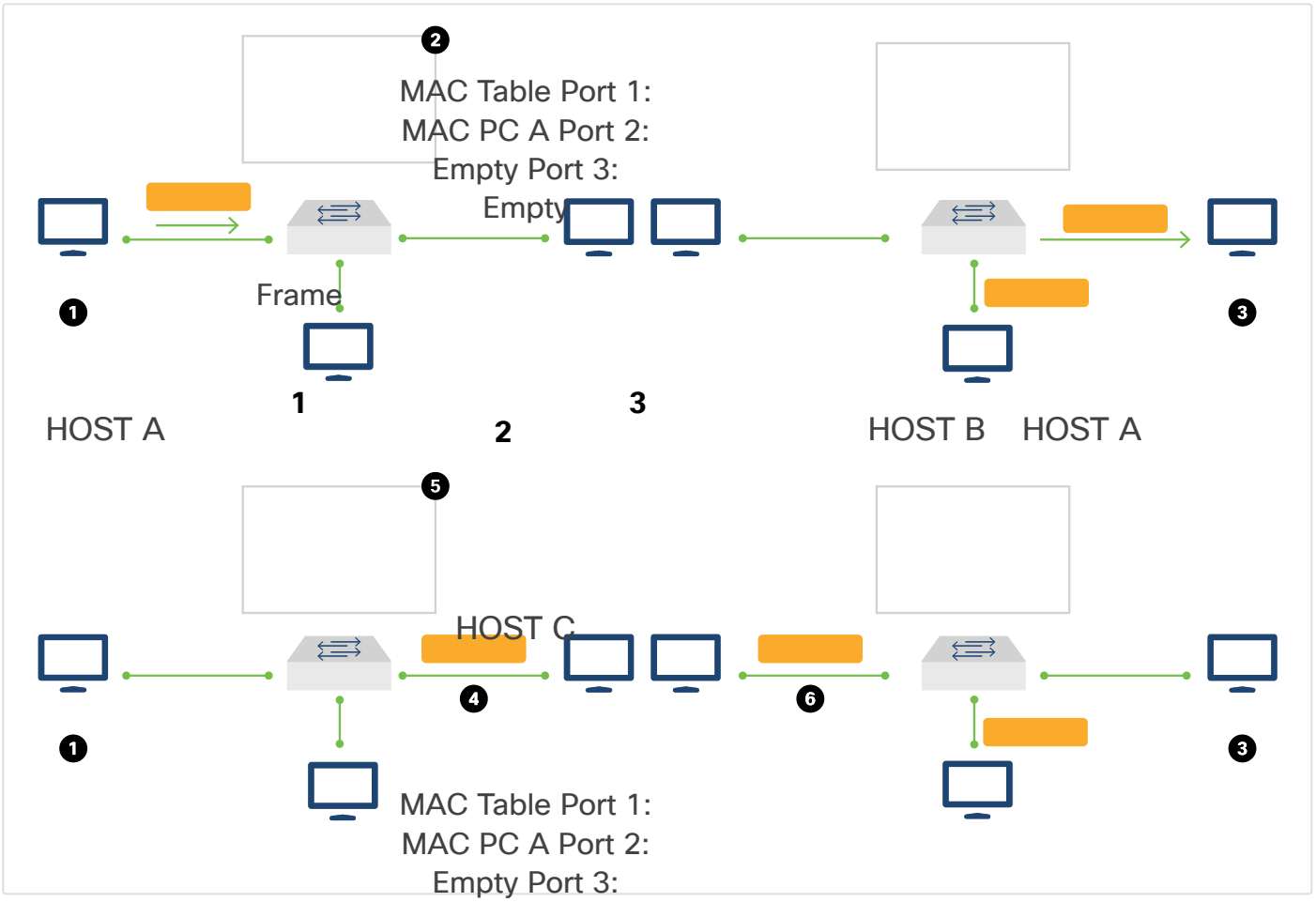
Switching

The switch builds and maintains a table (called the MAC address table) that matches the destination MAC address with the port that is used to connect to a node. The MAC address table is stored in the Content Addressable Memory (CAM), which enables very fast lookups.

The switch dynamically builds the MAC address table by examining the source MAC address of 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. Depending on the result, the switch will

decide whether to filter or flood the frame. If the destination MAC address is in the MAC address table, it will send it out the specified port. Otherwise, it will flood it out all ports except the incoming port.

Switching Process



In the figure, four topologies are shown. Each topology has a switch and three hosts (HOST A, HOST B, and HOST C). The following describes the switching process illustrated in the figure as Host A sends a frame to Host B:

1. In the first topology, top left, the switch receives a frame from Host A on port 1.
2. The switch enters the source MAC address and the switch port that received the frame into the MAC address table.
3. The switch checks the table for the destination MAC address. Because the destination address is not known, the switch floods the frame to all of the ports except the port on which it received the frame. In the second topology, top right, Host B, the destination MAC address, receives the Ethernet frame.
4. In the third topology, bottom left, Host C replies to the Host A with the destination MAC address of Host A.
5. The switch enters the source MAC address of Host B and the port number of the switch port that received the frame into the MAC table. The destination address of the frame and its associated port is known in the MAC address table.
6. In the fourth topology, bottom right, the switch can now directly forward this frame to Host A out port 1. Frames between the source and destination devices are sent without flooding because the switch has entries in the MAC address table that identify the associated ports.

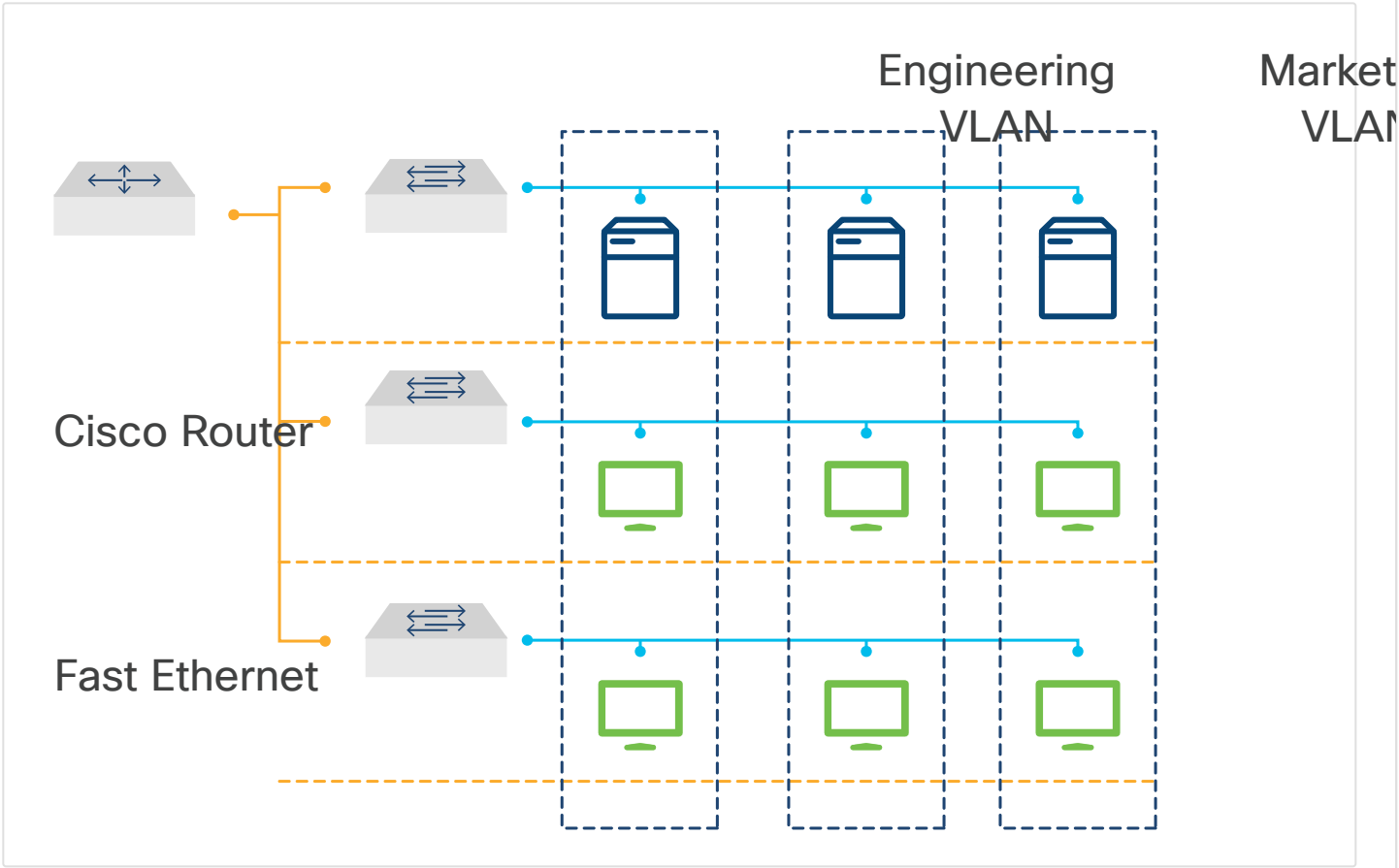
5.2.5

Virtual LANs (VLANs)

A virtual LAN (VLAN) is used to segment different Layer 2 broadcast domains on one or more switches. A VLAN groups devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

For example, in the figure, the network administrator created three VLANs based on the function of its users: engineering, marketing, and accounting. Notice that the devices do not need to be on the same floor.

VLANs



VLANs define Layer 2 broadcast domains. Broadcast domains are typically bounded by routers because routers do not forward broadcast frames. VLANs on Layer 2 switches create broadcast domains based on the configuration of the switch. Switch ports are assigned to a VLAN. A Layer 2 broadcast received on a switch port is only flooded out onto other ports belonging to the same VLAN.

You can define one or many VLANs within a switch. Each VLAN you create in the switch defines a new broadcast domain. Traffic cannot pass directly to another VLAN (between broadcast domains) within the

switch or between two switches. To interconnect two different VLANs, you must use a router or Layer 3 switch.

VLANs are often associated with IP networks or subnets. For example, all of the end stations in a particular IP subnet belong to the same VLAN. Traffic between VLANs must be routed. You must assign a VLAN membership (VLAN ID) to a switch port on an port-by-port basis (this is known as interface-based or static VLAN membership). You can set various parameters when you create a VLAN on a switch, including VLAN number (VLAN ID) and VLAN name.

Switches support 4096 VLANs in compliance with the IEEE 802.1Q standard which specifies 12 bits (2^12=4096) for the VLAN ID.

A trunk is a point-to-point link between two network devices that carries more than one VLAN. A VLAN trunk extends VLANs across an entire network. IEEE 802.1Q defines a "tag" that is inserted in the frame containing the VLAN ID. This tag is inserted when the frame is forwarded by the switch on its egress interface. The tag is removed by the switch that receives the frame. This is how switches know of which VLAN the frame is a member.

These VLANs are organized into three ranges: reserved, normal, and extended. Some of these VLANs are propagated to other switches in the network when you use the VLAN Trunking Protocol (VTP).

VLANs	Range	Usage
0, 4095	Reserved	For system use only. You cannot see or use these VLANs.
1	Normal	Cisco default. You can use this VLAN, but you cannot delete it.
2 - 1001	Normal	Used for Ethernet VLANs; you can create, use, and delete these VLANs.
1002 - 1005	Normal	Cisco defaults for FDDI and Token Ring. You cannot delete VLANs 1002-1005.
1006 - 4094	Extended	For Ethernet VLANs only.

5.1
Introduction to Network Fundamentals

5.3
Internetwork Layer