Table of Contents

[SWITCHING CONCEPTS 2](#_Toc206363109)

[Frame Forwarding 2](#_Toc206363110)

[Switching in Networking 2](#_Toc206363111)

[The Switch MAC Address Table 3](#_Toc206363112)

[The Switch Learn and Forward Method 4](#_Toc206363113)

[Video - MAC Address Tables on Connected Switches 4](#_Toc206363114)

[Switching Forwarding Methods 6](#_Toc206363115)

[Store-and-Forward Switching 6](#_Toc206363116)

[Cut-Through Switching 7](#_Toc206363117)

[Activity - Switch It! 8](#_Toc206363118)

[Collision and Broadcast Domains 13](#_Toc206363119)

[Collision Domains 13](#_Toc206363120)

[Broadcast Domains 14](#_Toc206363121)

[Alleviate Network Congestion 15](#_Toc206363122)

[Check Your Understanding - Switching Domains 16](#_Toc206363123)

[MODULE 3: VLANS 17](#_Toc206363124)

[Introduction 17](#_Toc206363125)

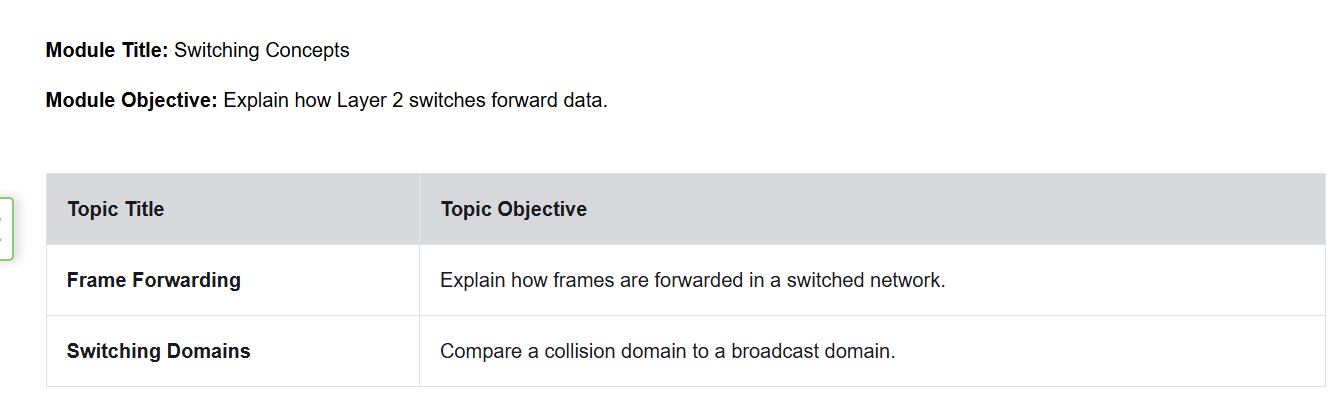
[Overview of VLANs 17](#_Toc206363126)

[VLAN Definitions 17](#_Toc206363127)

[Benefits of a VLAN Design 19](#_Toc206363128)

[Types of VLANs 20](#_Toc206363129)

# MODULE 2: SWITCHING CONCEPTS



## Frame Forwarding

### Switching in Networking

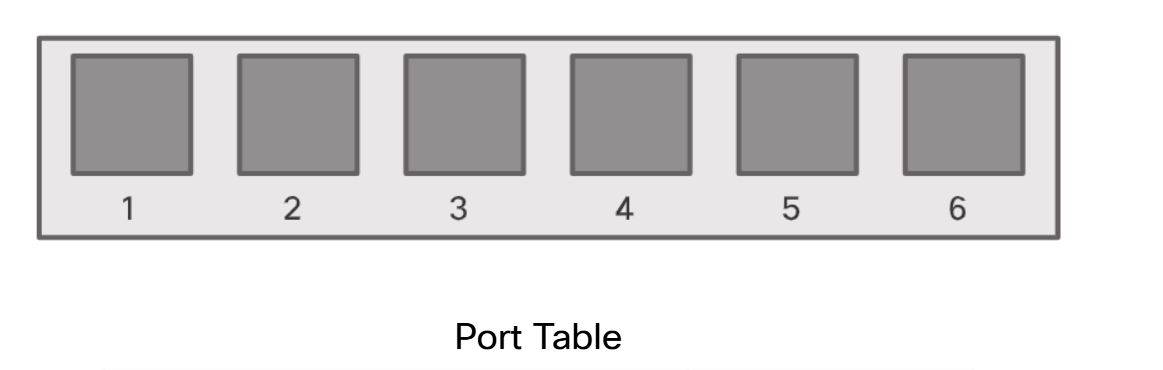
The concept of switching and forwarding frames is universal in networking and telecommunications. Various types of switches are used in LANs, WANs, and in the public switched telephone network (PSTN).

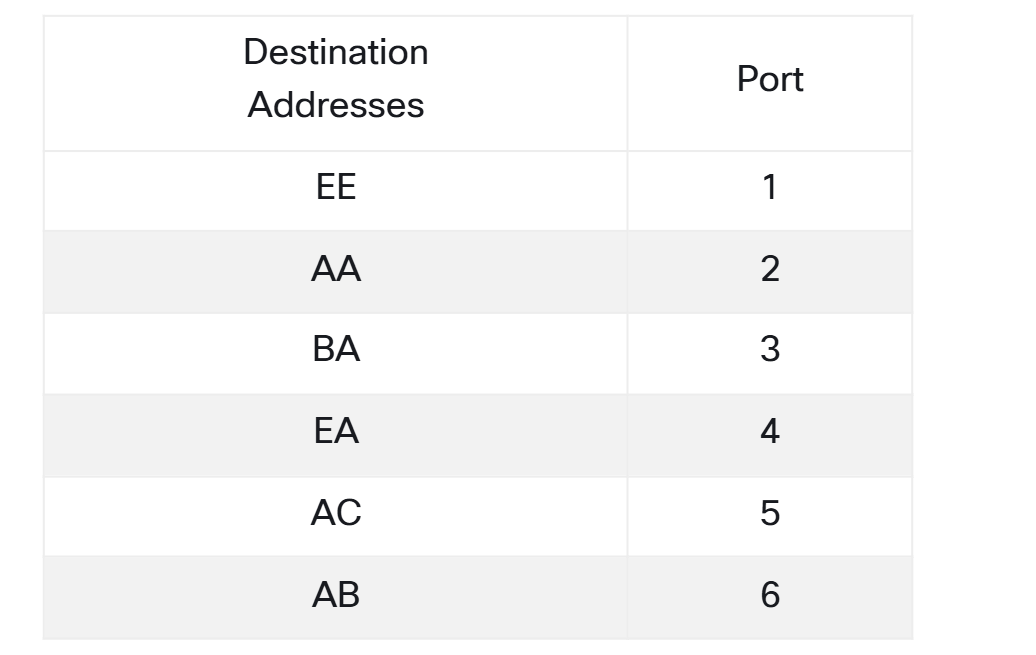
The decision on how a switch forwards traffic is made based on the flow of that traffic. There are two terms associated with frames entering and leaving an interface:

* **Ingress** - This is used to describe the port where a frame enters the device.
* **Egress** - This is used to describe the port that frames will use when leaving the device.

A LAN switch maintains a table that is referenced when forwarding traffic through the switch. The only intelligence of a LAN switch is its ability to use its table to forward traffic. A LAN switch forwards traffic based on the ingress port and the destination MAC address of an Ethernet frame. With a LAN switch, there is only one master switching table that describes a strict association between MAC addresses and ports; therefore, an Ethernet frame with a given destination address always exits the same egress port, regardless of the ingress port it enters.

**Note:** An Ethernet frame will never be forwarded out the same port it was on which it was received.

****

****

### The Switch MAC Address Table

A switch is made up of integrated circuits and the accompanying software that controls the data paths through the switch. Switches use destination MAC addresses to direct network communications through the switch, out the appropriate port, toward the destination.

For a switch to know which port to use to transmit a frame, it must first learn which devices exist on each port. As the switch learns the relationship of ports to devices, it builds a table called a MAC address table. This table is stored in content addressable memory (CAM) which is a special type of memory used in high-speed searching applications. For this reason, the MAC address table is sometimes also called the CAM table.

LAN switches determine how to handle incoming data frames by maintaining the MAC address table. A switch populates its MAC address table by recording the source MAC address of each device connected to each of its ports. The switch references the information in the MAC address table to send frames destined for a specific device out of the port which has been assigned to that device.

### The Switch Learn and Forward Method

The following two-step process is performed on every Ethernet frame that enters a switch.

**Step 1. Learn - Examining the Source MAC Address**

Every frame that enters a switch is checked for new information to learn. It does this by examining the source MAC address of the frame and port number where the frame entered the switch:

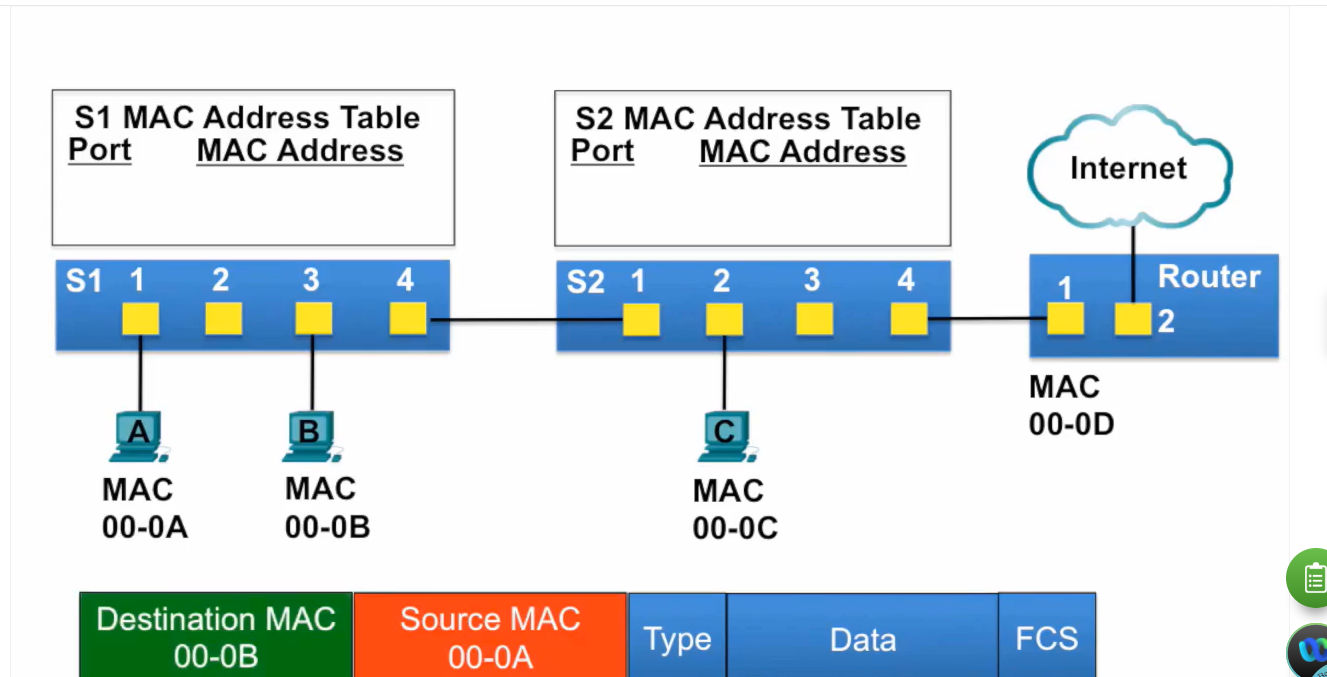
* If the source MAC address does not exist in the MAC address table, the MAC address and incoming port number are added to the table.
* If the source MAC address does exist, the switch updates the refresh timer for that entry. By default, most Ethernet switches keep an entry in the table for five minutes. If the source MAC address does exist in the table but on a different port, the switch treats this as a new entry. The entry is replaced using the same MAC address, but with the more current port number.

**Step 2. Forward - Examining the Destination MAC Address**

If the destination MAC address is a unicast address, the switch will look for a match between the destination MAC address of the frame and an entry in its MAC address table:

* If the destination MAC address is in the table, it will forward the frame out of the specified port.
* If the destination MAC address is not in the table, the switch will forward the frame out all ports except the incoming port. This is called an unknown unicast. If the destination MAC address is a broadcast or a multicast, the frame is also flooded out all ports except the incoming port.

### Video - MAC Address Tables on Connected Switches



* 00:02- In this video, PC-A is going to send
* 00:04an ethernet frame to PC-B, and
* 00:07PC-B is going to send an ethernet frame to PC-A.
* 00:10We're going to examine how switches S1 and S2
* 00:14build their MAC address tables,
* 00:16and also how they forward frames
* 00:18based on the information in those MAC address tables.
* 00:23PC-A has an ethernet frame to send to PC-B.
* 00:27The source MAC address of the frame is 00-0A
* 00:30and the destination MAC address is 00-0B.
* 00:34The ethernet frame is sent to switch S1.
* 00:38S1 receives the ethernet frame,
* 00:40examines the source MAC address
* 00:42and notices that this MAC address
* 00:43is not in its MAC address table,
* 00:46so it adds the MAC address and the incoming port number.
* 00:51Next, switch S1 examines the destination MAC address
* 00:55and notices that this MAC address is not in its table,
* 00:58so it floods it out all ports.
* 01:03PC-B receives the ethernet frame,
* 01:06examines the destination MAC address
* 01:08against its own MAC address and notices that
* 01:11that is a match and receives the rest of the frame.
* 01:16The ethernet frame continues to be
* 01:18forwarded to switch S2.
* 01:20Switch S2 examines the source MAC address
* 01:23to the frame and notices it is not in
* 01:25its MAC address table, so it adds the MAC address
* 01:29and the incoming port to its MAC address table.
* 01:33Next, switch S2 examines the destination MAC address,
* 01:36notices that is not in its MAC address table
* 01:39so it floods it out all ports.
* 01:43PC-C receives the ethernet frame
* 01:46and its MAC address does not match
* 01:49the destination MAC address of the ethernet frame,
* 01:52so it does not accept the rest of the frame.
* 01:55The router receives the ethernet frame,
* 01:58examines the destination MAC address
* 02:00against its own MAC address
* 02:02and notices it is not a match
* 02:04so it does not receive the rest of the frame.
* 02:08Now, let's have PC-B sending a frame back to PC-A.
* 02:16The source MAC address of the frame is 00-0B
* 02:20and the destination MAC address is 00-0A.
* 02:24PC-B sends it to switch S1.
* 02:27S1 notices that the source MAC address
* 02:31is not in its MAC address table
* 02:32so it adds the MAC address
* 02:34and the incoming port number.
* 02:37Next, switch S1 examines the destination MAC address
* 02:41and notices that MAC address is in its MAC address table.
* 02:46So it sends it out just port 1.
* 02:51PC-A receives the ethernet frame,
* 02:54examines the destination MAC address
* 02:56against its own MAC address and notices
* 02:59it is a match so it receives the rest of the frame.

### Switching Forwarding Methods

Switches make Layer 2 forwarding decisions very quickly. This is because of software on application-specific-integrated circuits (ASICs). ASICs reduce the frame-handling time within the device and allow the device to manage an increased number of frames without degrading performance.

Layer 2 switches use one of two methods to switch frames:

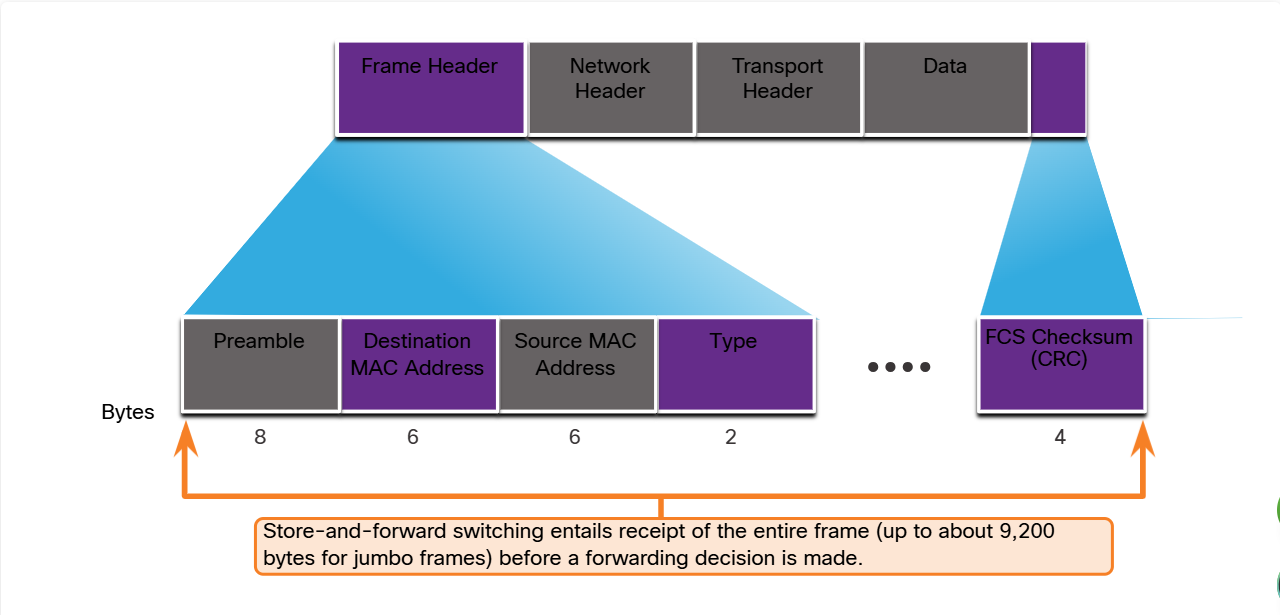
* **Store-and-forward switching** - This method makes a forwarding decision on a frame after it has received the entire frame and checked the frame for errors using a mathematical error-checking mechanism known as a cyclic redundancy check (CRC). Store-and-forward switching is Cisco’s primary LAN switching method.
* **Cut-through switching** - This method begins the forwarding process after the destination MAC address of an incoming frame and the egress port have been determined.

### Store-and-Forward Switching

Store-and-forward switching, as distinguished from cut-through switching, has the following two primary characteristics:

* **Error checking** - After receiving the entire frame on the ingress port, the switch compares the frame check sequence (FCS) value in the last field of the datagram against its own FCS calculations. The FCS is an error checking process that helps to ensure that the frame is free of physical and data-link errors. If the frame is error-free, the switch forwards the frame. Otherwise, the frame is dropped.
* **Automatic buffering** - The ingress port buffering process used by store-and-forward switches provides the flexibility to support any mix of Ethernet speeds. For example, handling an incoming frame traveling into a 100 Mbps Ethernet port that must be sent out a 1 Gbps interface would require using the store-and-forward method. With any mismatch in speeds between the ingress and egress ports, the switch stores the entire frame in a buffer, computes the FCS check, forwards it to the egress port buffer and then sends it.

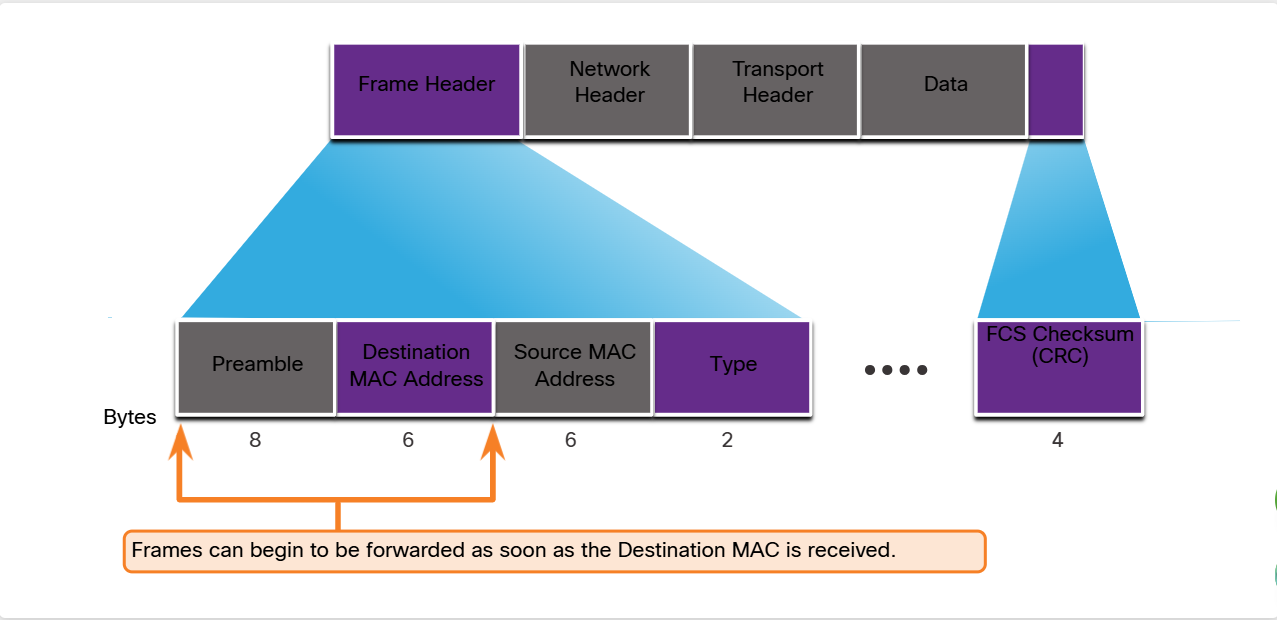
The figure illustrates how store-and-forward makes a decision based on the Ethernet frame.



### Cut-Through Switching

The store-and-forward switching method drops frames that do not pass the FCS check. Therefore, it does not forward invalid frames.

By contrast, the cut-through switching method may forward invalid frames because no FCS check is performed. However, cut-through switching has the ability to perform rapid frame switching. This means the switch can make a forwarding decision as soon as it has looked up the destination MAC address of the frame in its MAC address table, as shown in the figure.



The switch does not have to wait for the rest of the frame to enter the ingress port before making its forwarding decision.

Fragment free switching is a modified form of cut-through switching in which the switch only starts forwarding the frame. Fragment free switching provides better error checking than cut-through, with practically no increase in latency.

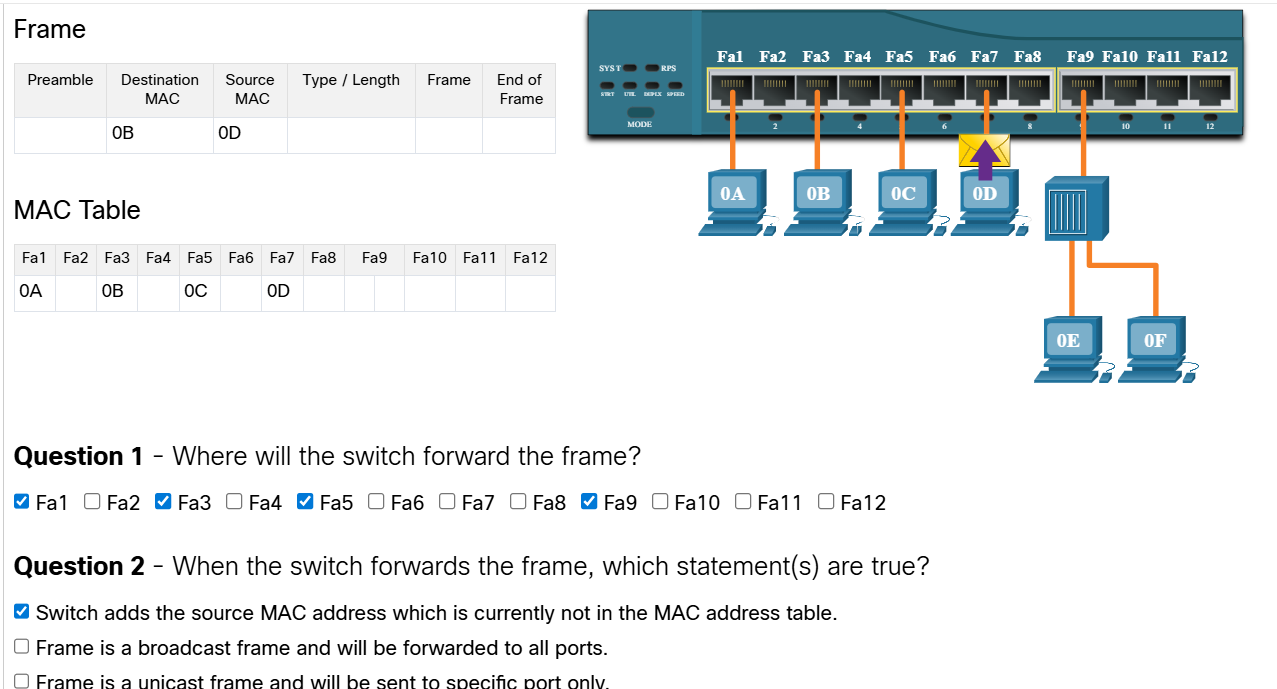
The lower latency speed of cut-through switching makes it more appropriate for extremely demanding, high-performance computing (HPC) applications that require process-to-process latencies of 10 microseconds or less.

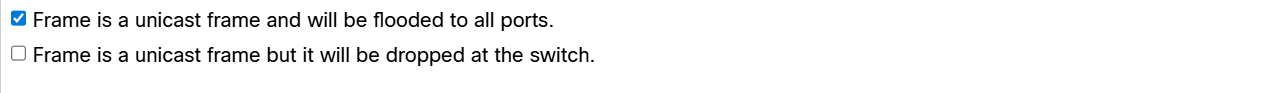
The cut-through switching method can forward frames with errors. If there is a high error rate (invalid frames) in the network, cut-through switching can have a negative impact on bandwidth, thereby clogging up bandwidth with damaged and invalid frames.

### Activity - Switch It!

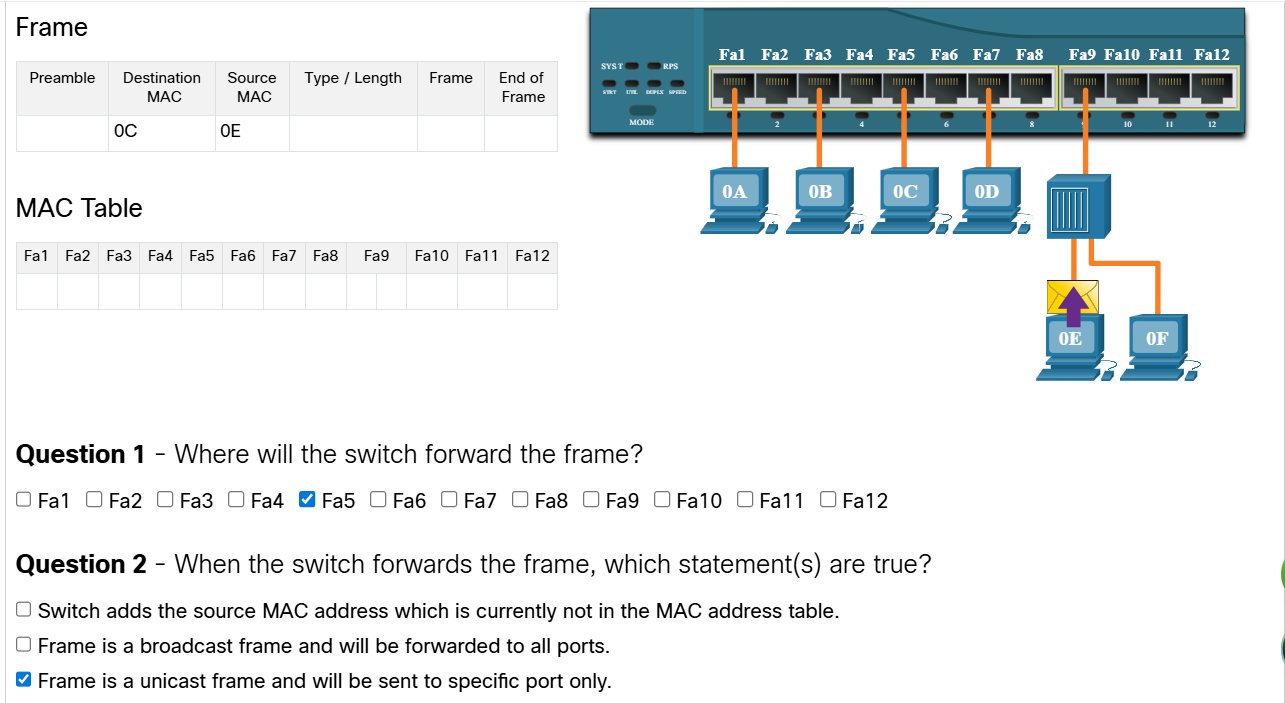
Use this activity to check your understanding of how a switch learns and forwards frames.

#### Challenge 1

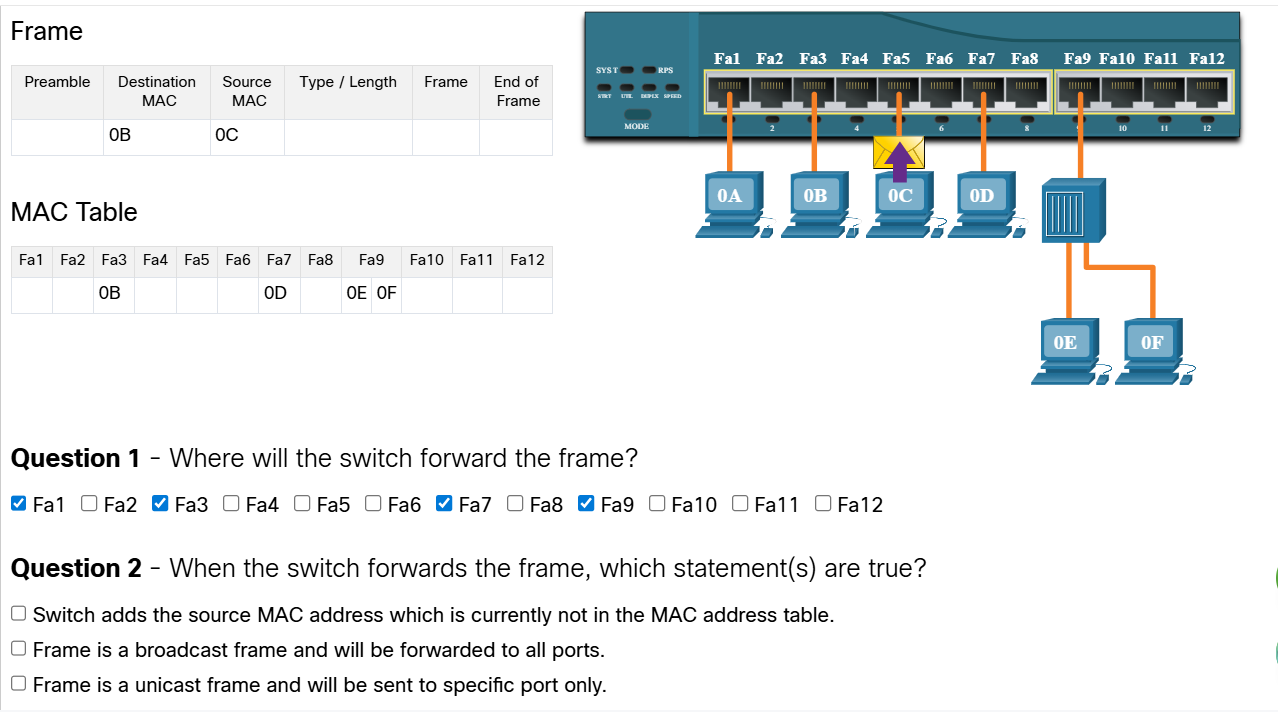




#### Challenge 2

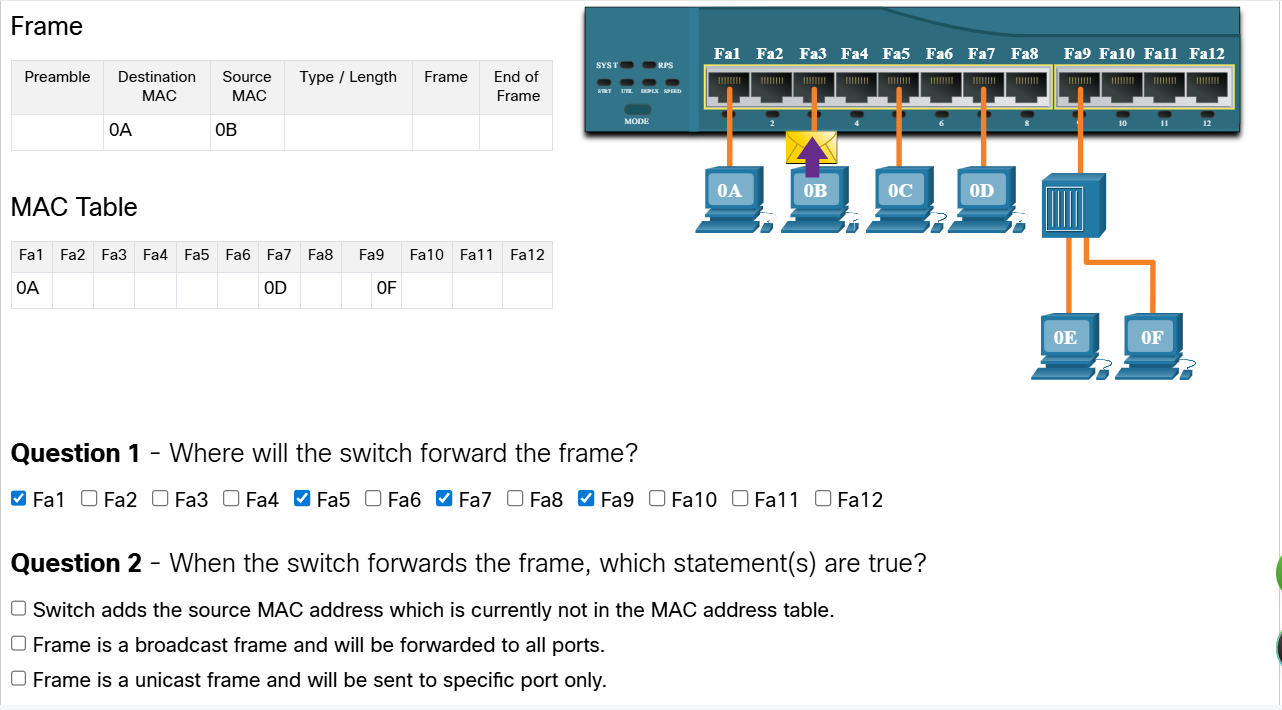


#### Challenge 3



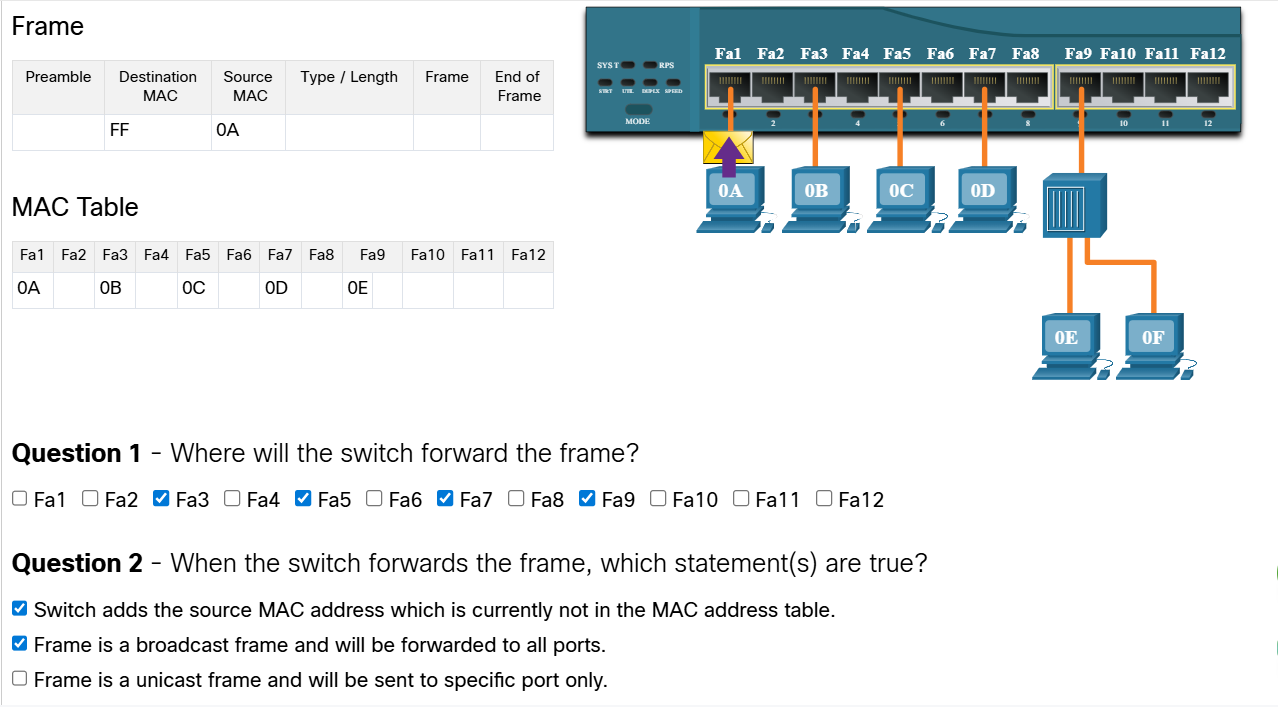


#### Challenge 4

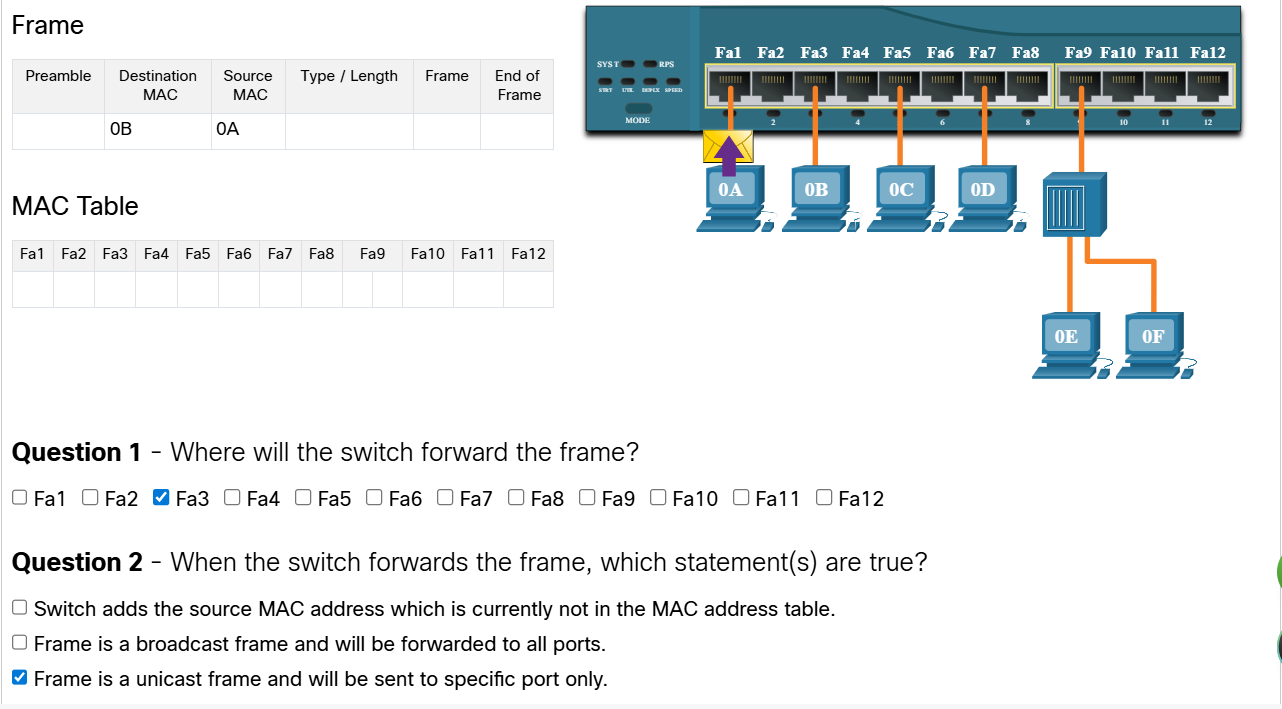




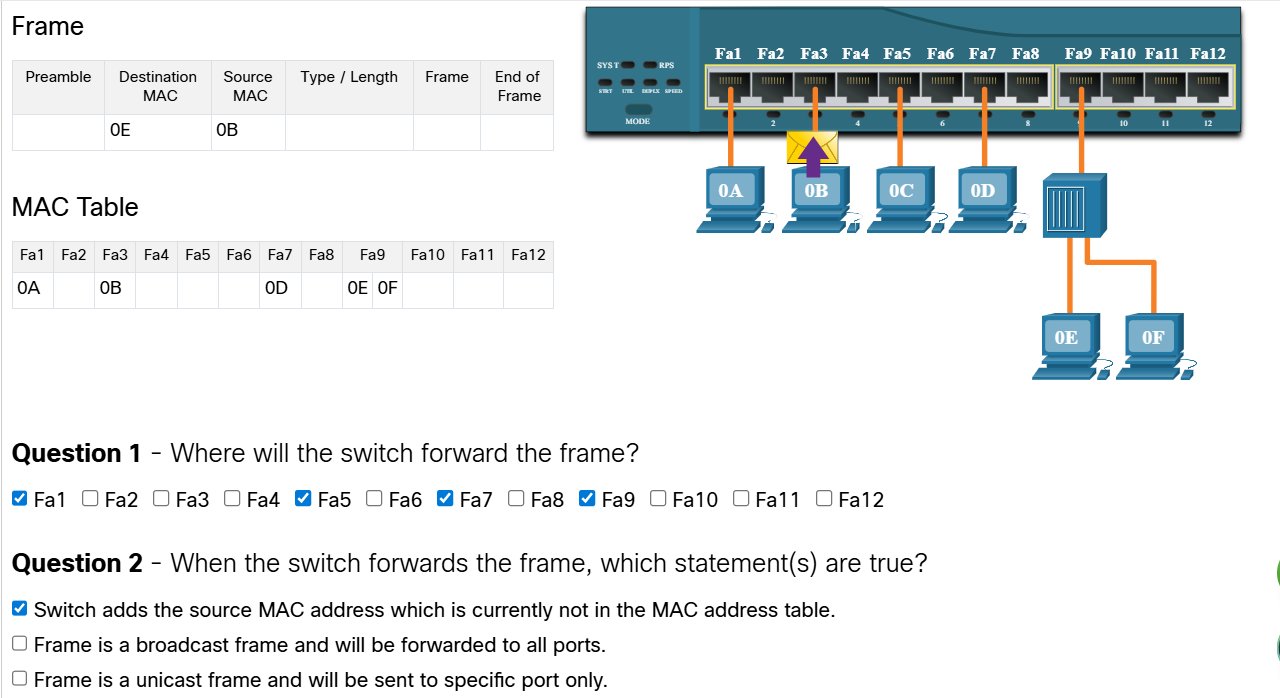
#### Challenge 5



#### Challenge 6

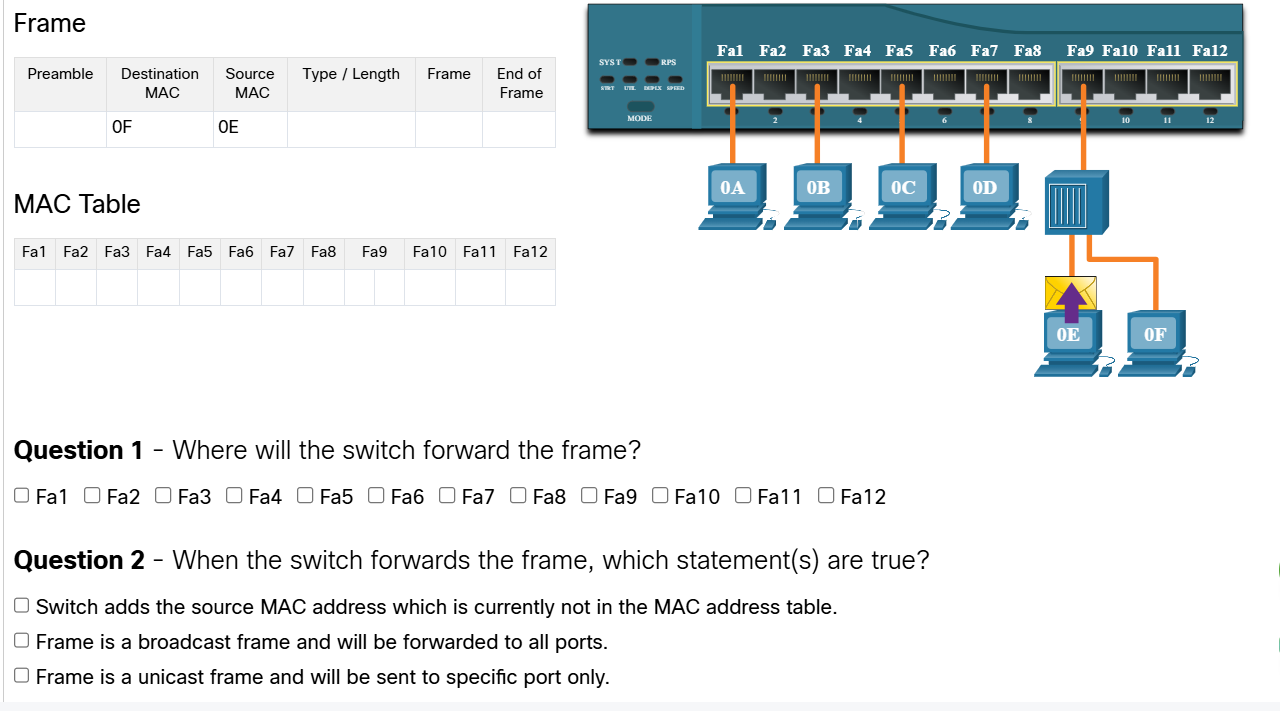


#### Challenge 7



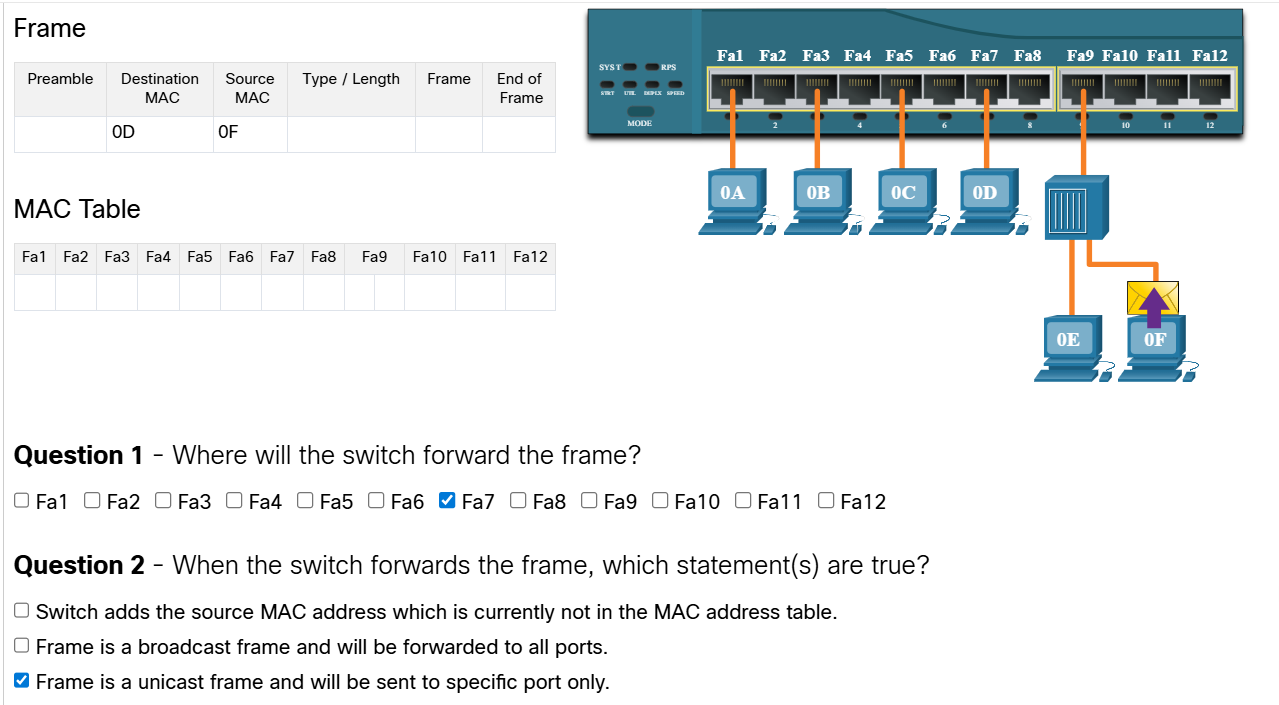


#### Challenge 8

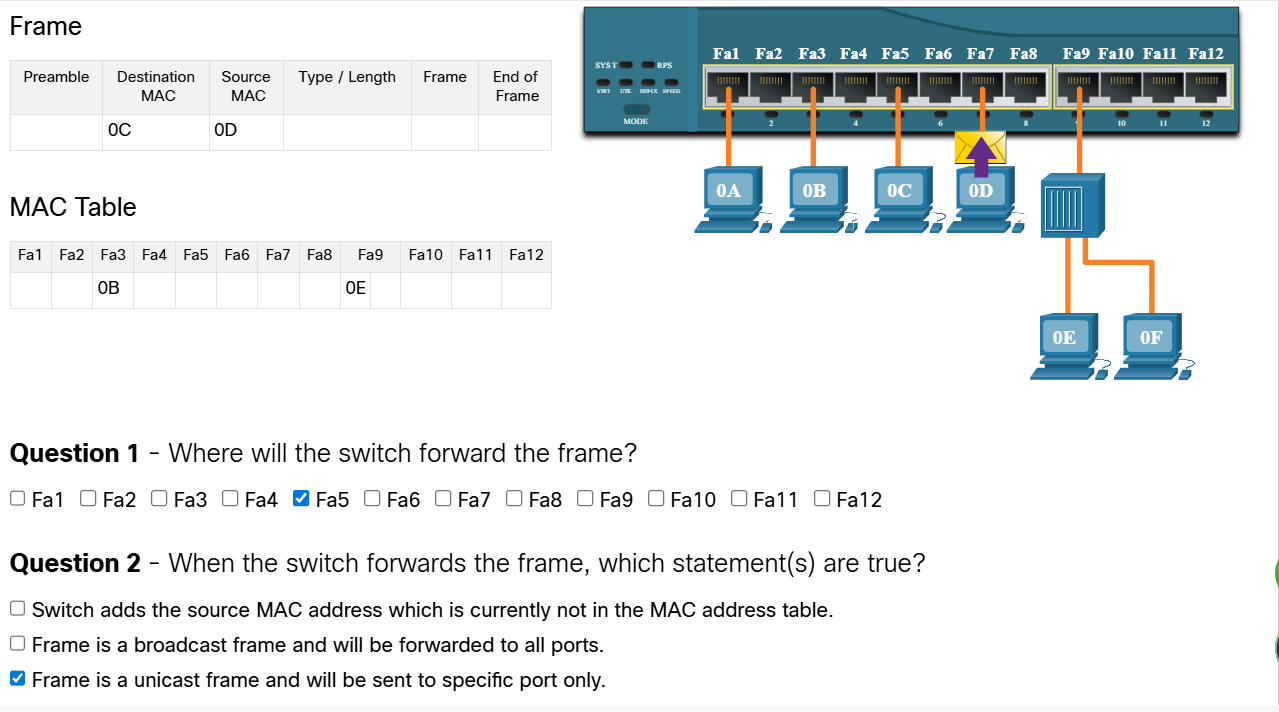




#### Challenge 9



#### Challenge 10



## Collision and Broadcast Domains

### Collision Domains

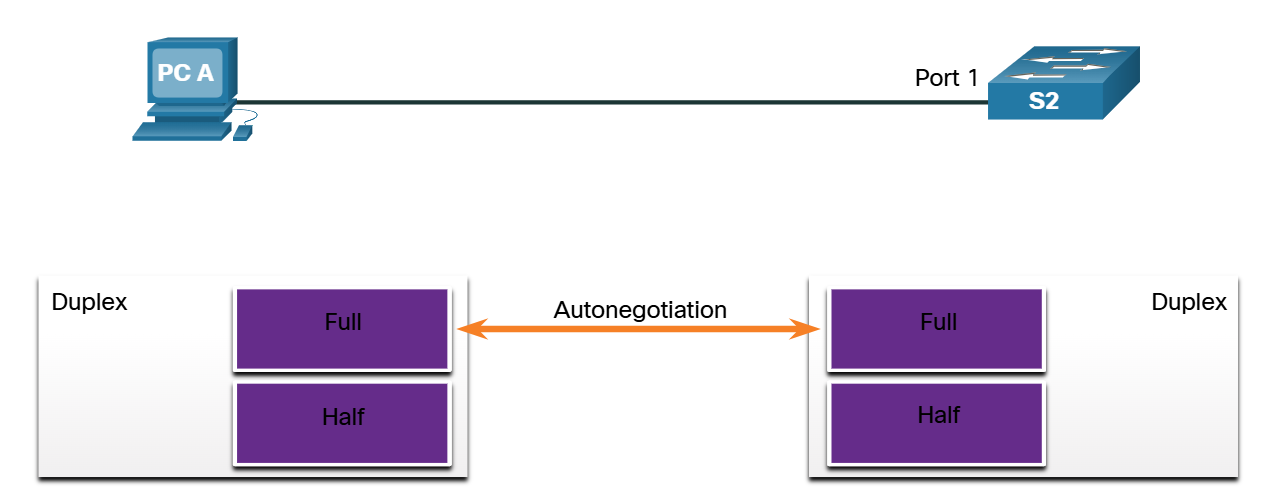
In the previous topic, you gained a better understanding of what a switch is and how it operates. This topic discusses how switches work with each other and with other devices to eliminate collisions and reduce network congestion. The terms collisions and congestion are used here in the same way that you use them in street traffic.

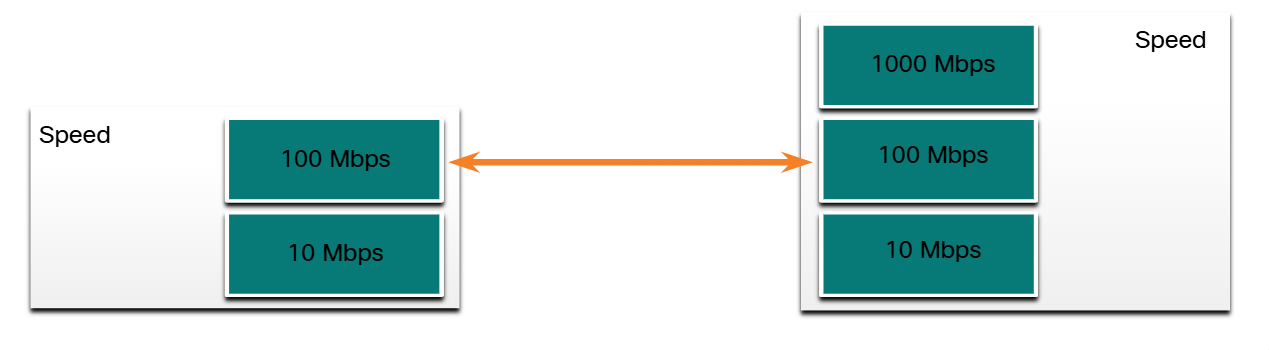
In legacy hub-based Ethernet segments, network devices competed for the shared medium. The network segments that share the same bandwidth between devices are known as collision domains. When two or more devices within the same collision domain try to communicate at the same time, a collision will occur.

If an Ethernet switch port is operating in half-duplex, each segment is in its own collision domain. There are no collisions when switch ports are operating in full-duplex. However, there could be a collision domain if a switch port is operating in half-duplex.

By default, Ethernet switch ports will autonegotiate full-duplex when the adjacent device can also operate in full-duplex. If the switch port is connected to a device operating in half-duplex, such as a legacy hub, then the switch port will operate in half-duplex. In the case of half-duplex, the switch port will be part of a collision domain.

As shown in the figure, full-duplex is chosen if both devices have the capability along with their highest common bandwidth.



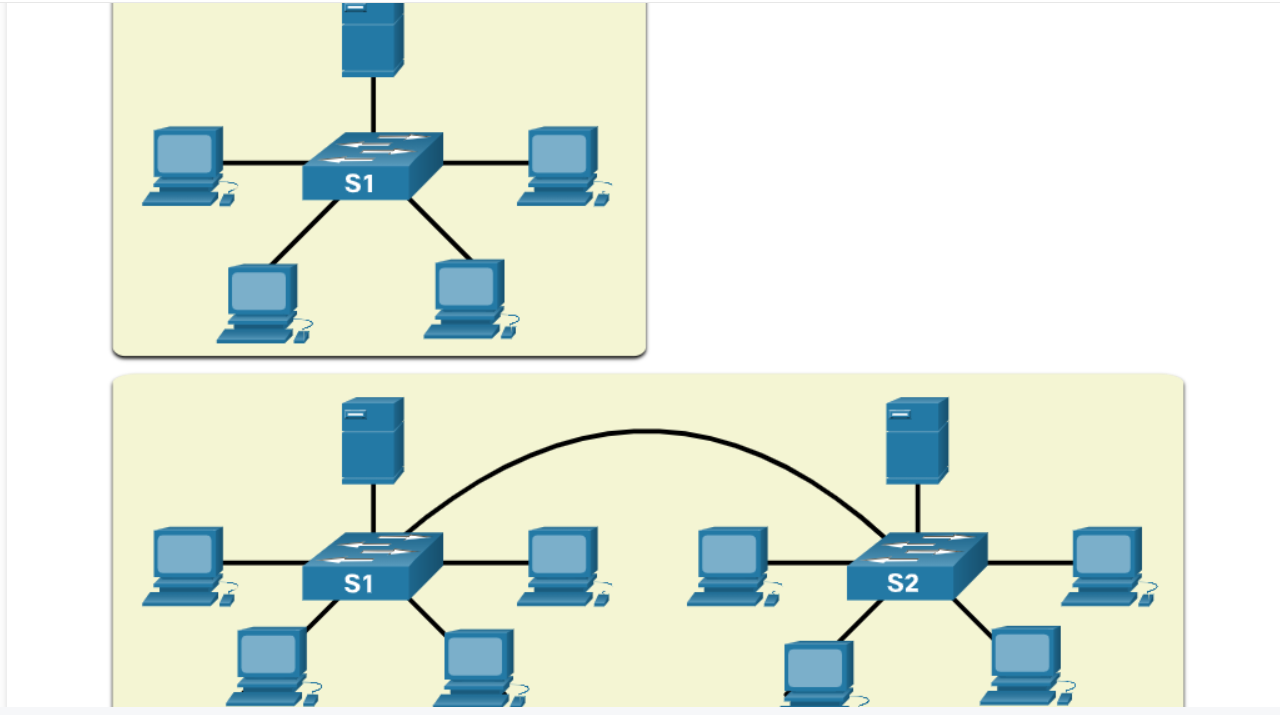


### Broadcast Domains

A collection of interconnected switches forms a single broadcast domain. Only a network layer device, such as a router, can divide a Layer 2 broadcast domain. Routers are used to segment broadcast domains, but will also segment a collision domain.

When a device sends a Layer 2 broadcast, the destination MAC address in the frame is set to all binary ones.

The Layer 2 broadcast domain is referred to as the MAC broadcast domain. The MAC broadcast domain consists of all devices on the LAN that receive broadcast frames from a host.



When a switch receives a broadcast frame, it forwards the frame out each of its ports, except the ingress port where the broadcast frame was received. Each device connected to the switch receives a copy of the broadcast frame and processes it.

Broadcasts are sometimes necessary for initially locating other devices and network services, but they also reduce network efficiency. Network bandwidth is used to propagate the broadcast traffic. Too many broadcasts and a heavy traffic load on a network can result in congestion, which slows down network performance.

When two switches are connected together, the broadcast domain is increased, as seen in the second half of the animation. In this case, a broadcast frame is forwarded to all connected ports on switch S1. Switch S1 is connected to switch S2. The frame is then also propagated to all devices connected to switch S2.

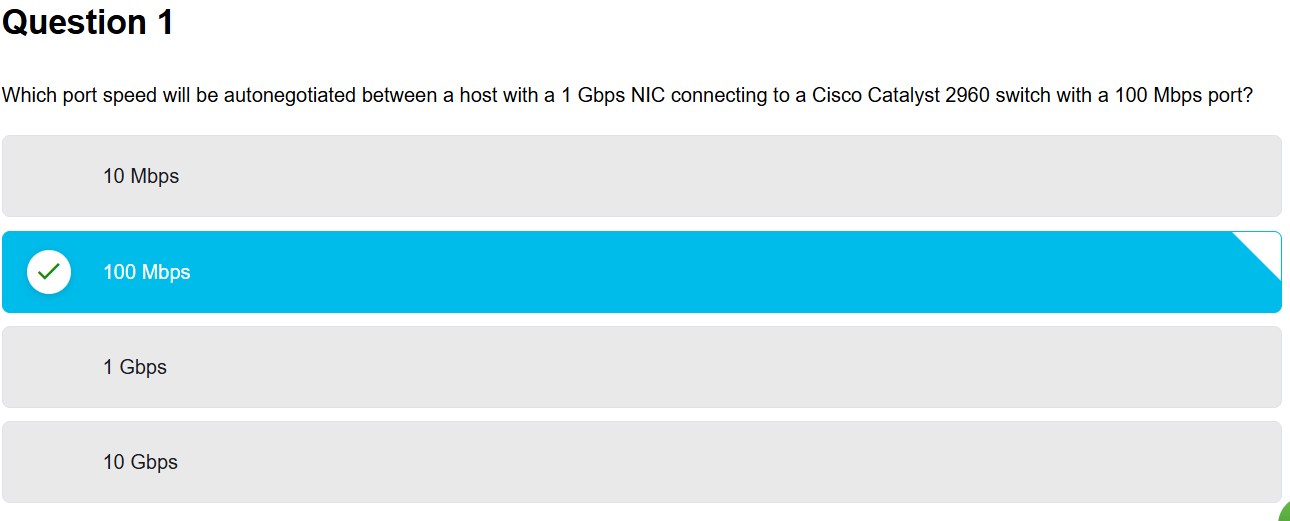
### Alleviate Network Congestion

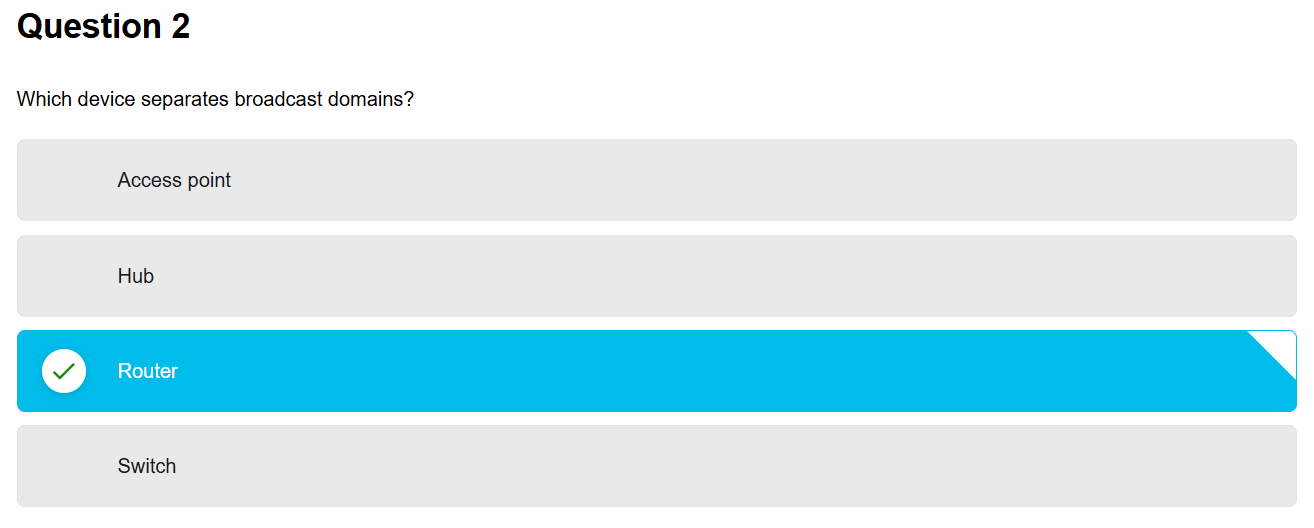
LAN switches have special characteristics that help them alleviate network congestion. By default, interconnected switch ports attempt to establish a link in full-duplex, therefore eliminating collision domains. Each full-duplex port of the switch provides the full bandwidth to the device or devices that are connected to that port. Full-duplex connections have dramatically increased LAN network performance, and are required for 1 Gbps Ethernet speeds and higher.

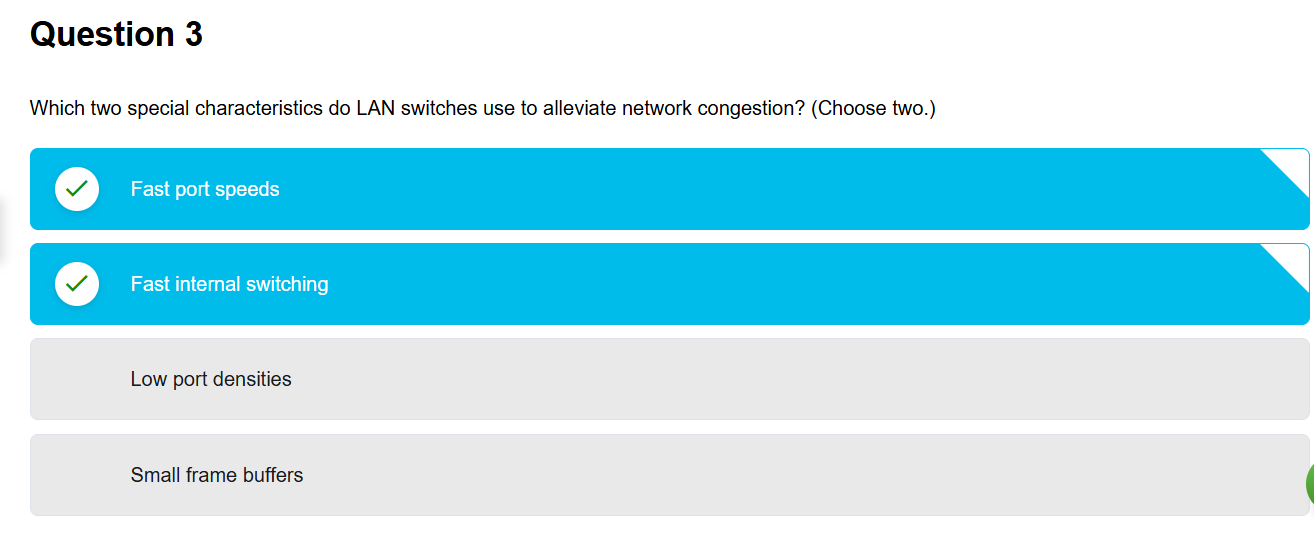
Switches interconnect LAN segments, use a MAC address table to determine egress ports, and can lessen or eliminate collisions entirely. Characteristics of switches that alleviate network congestion include the following:

* **Fast port speeds** - Ethernet switch port speeds vary by model and purpose. For instance, most access layer switches support 100 Mbps and 1 Gbps port speeds. Distribution layer switches support 100 Mbps, 1 Gbps, and 10 Gbps port speeds and core layer and data center switches may support 100 Gbps, 40 Gbps, and 10 Gbps port speeds. Switches with faster port speeds cost more but can reduce congestion.
* **Fast internal switching** - Switches use a fast internal bus or shared memory to provide high performance.
* **Large frame buffers** - Switches use large memory buffers to temporarily store more received frames before having to start dropping them. This enables ingress traffic from a faster port (e.g., 1 Gbps) to be forwarded to a slower (e.g., 100 Mbps) egress port without losing frames.
* **High port density** - A high port density switch lowers overall costs because it reduces the number of switches required. For instance, if 96 access ports were required, it would be less expensive to buy two 48-port switches instead of four 24-port switches. High port density switches also help keep traffic local, which helps alleviate congestion.

### Check Your Understanding - Switching Domains



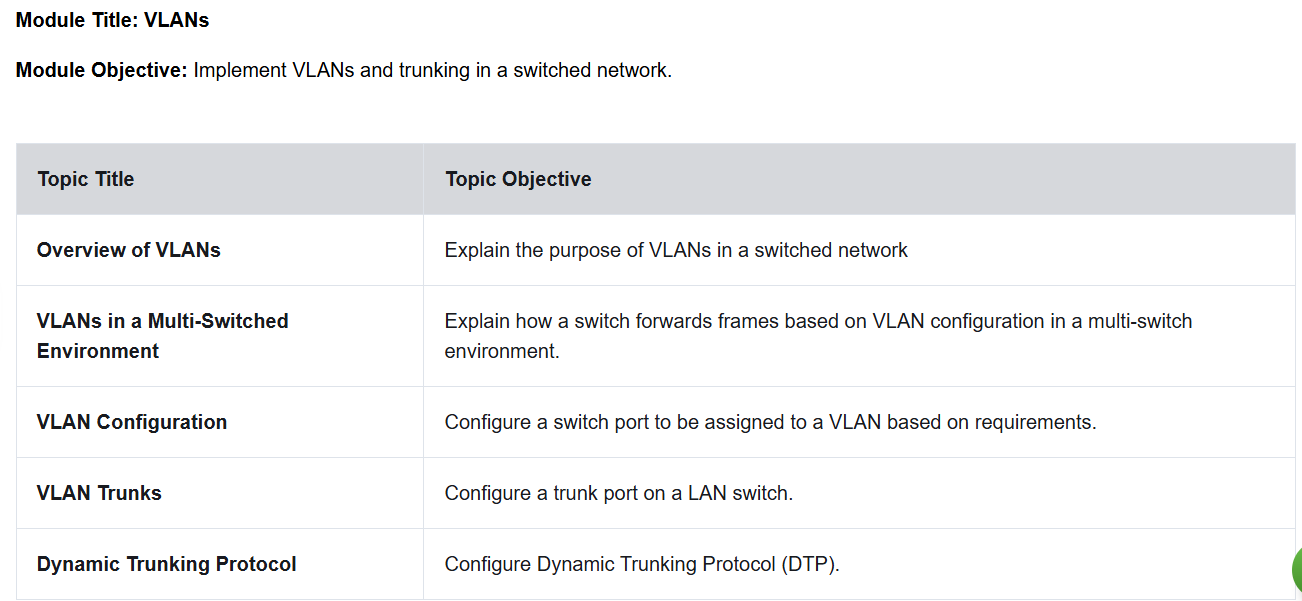




# MODULE 3: VLANS

## Introduction

VLANs are created at Layer 2 to reducing or eliminate broadcast traffic. **VLANs** are how you break up your network into smaller networks, so that the devices and people within a single VLAN are communicating with each other and not having to manage traffic from other networks. The network administrator can organize VLANs by location, who is using them, the type of device, or whatever category is needed.

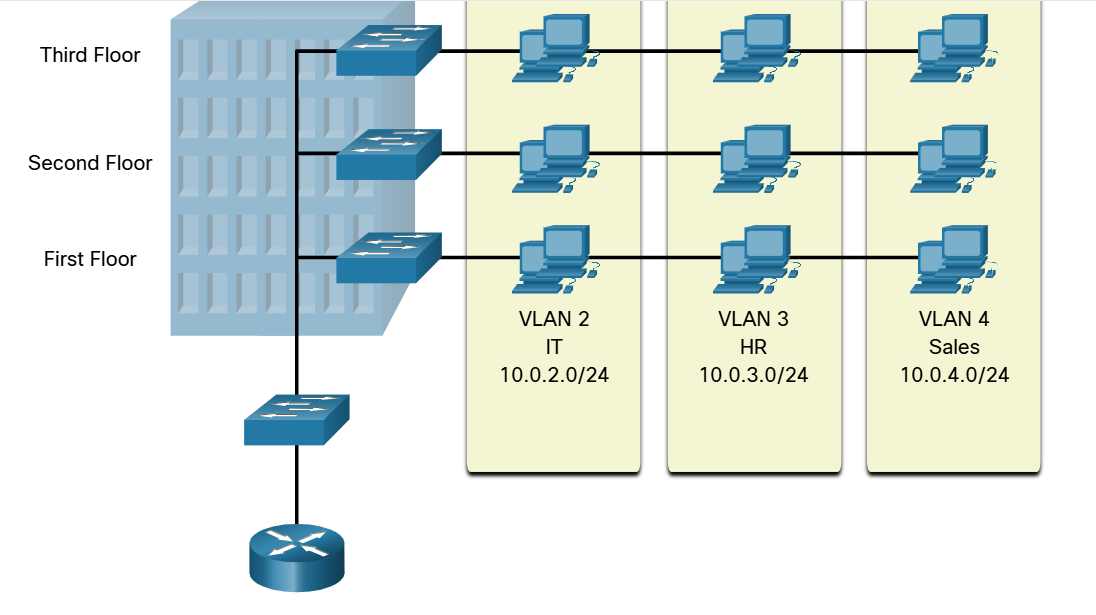


## Overview of VLANs

### VLAN Definitions

Virtual LANs (VLANs) provide segmentation and organizational flexibility in a switched network. A group of devices within a VLAN communicate as if each device was attached to the same cable. VLANs are based on logical connections, instead of physical connections.

As shown in the figure, VLANs in a switched network enable users in various departments (i.e., IT, HR, and Sales) to connect to the same network regardless of the physical switch being used or location in a campus LAN.



VLANs allow an administrator to segment networks based on factors such as function, team, or application, without regard for the physical location of the users or devices. Each VLAN is considered a separate logical network. Devices within a VLAN act as if they are in their own independent network, even if they share a common infrastructure with other VLANs. Any switch port can belong to a VLAN.

Unicast, broadcast, and multicast packets are forwarded and flooded only to end devices within the VLAN where the packets are sourced. Packets destined for devices that do not belong to the VLAN must be forwarded through a device that supports routing.

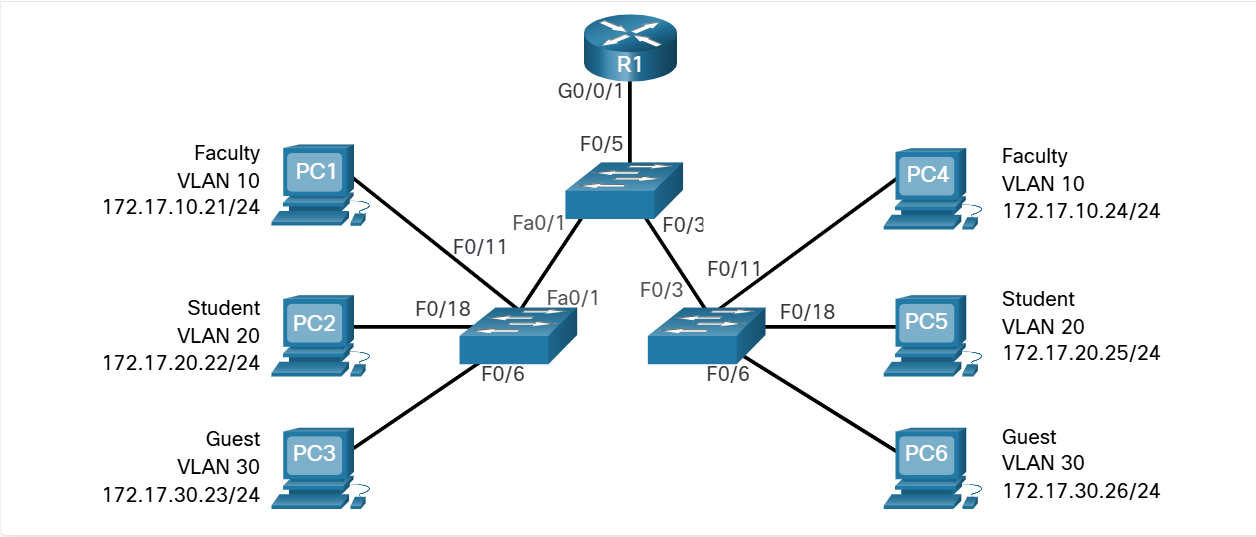
Multiple IP subnets can exist on a switched network, without the use of multiple VLANs. However, the devices will be in the same Layer 2 broadcast domain. This means that any Layer 2 broadcasts, such as an ARP request, will be received by all devices on the switched network, even by those not intended to receive the broadcast.

A VLAN creates a logical broadcast domain that can span multiple physical LAN segments. VLANs improve network performance by separating large broadcast domains into smaller ones. If a device in one VLAN sends a broadcast Ethernet frame, all devices in the VLAN receive the frame, but devices in other VLANs do not.

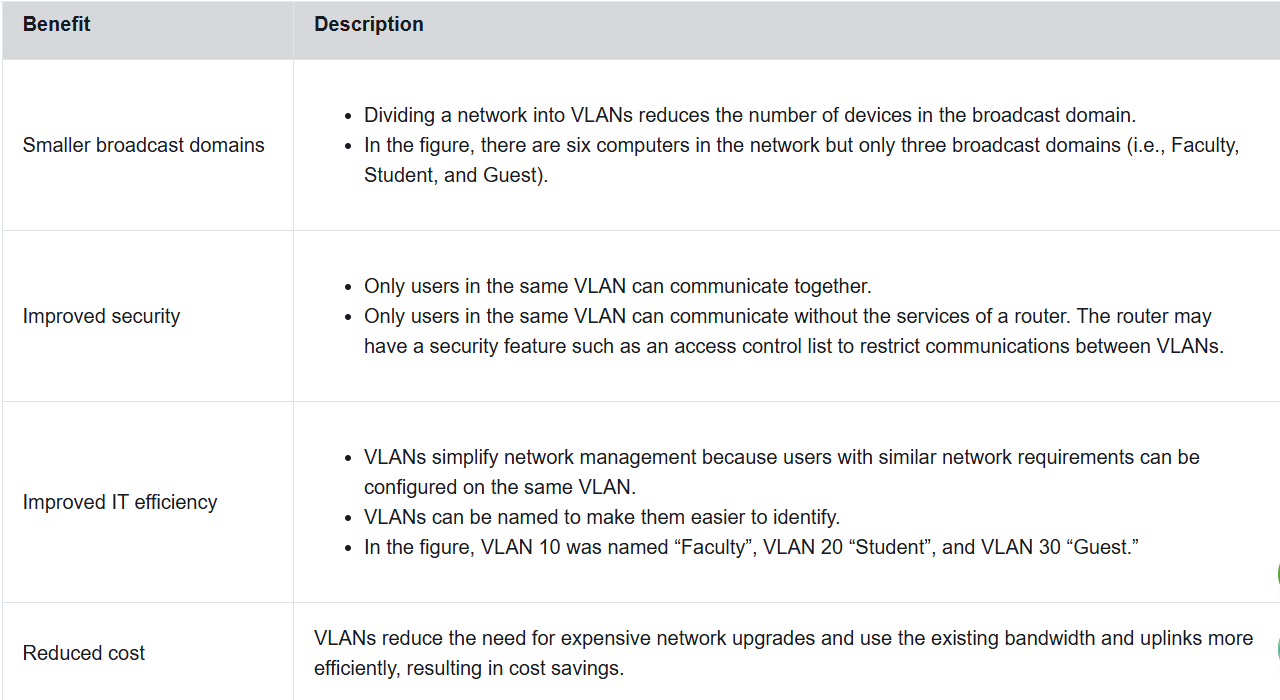
Using VLANs, network administrators can implement access and security policies according to specific groupings of users. Each switch port can be assigned to only one VLAN (except for a port connected to an IP phone or to another switch).

### Benefits of a VLAN Design

Each VLAN in a switched network corresponds to an IP network. Therefore, VLAN design must take into consideration the implementation of a hierarchical network-addressing scheme. Hierarchical network addressing means that IP network numbers are applied to network segments or VLANs in a way that takes the network as a whole into consideration. Blocks of contiguous network addresses are reserved for and configured on devices in a specific area of the network, as shown in the figure.



The table lists the benefits of designing a network with VLANs





### Types of VLANs

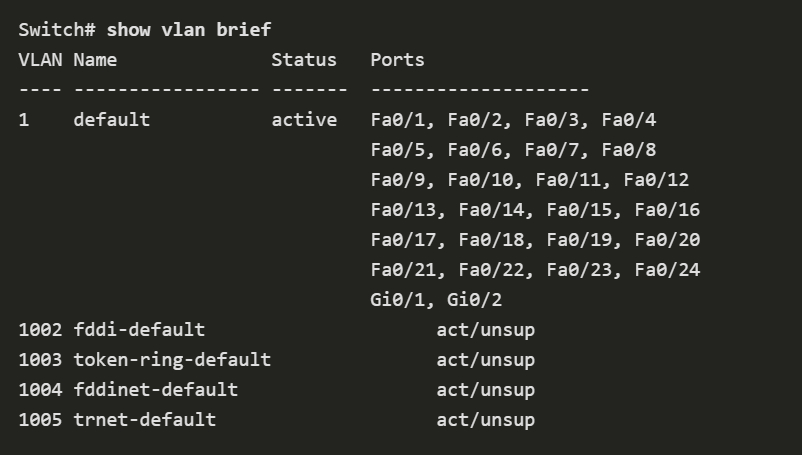
#### Default VLAN

The default VLAN on a Cisco switch is VLAN 1. Therefore, all switch ports are on VLAN 1 unless it is explicitly configured to be on another VLAN. By default, all Layer 2 control traffic is associated with VLAN 1.

Important facts to remember about VLAN 1 include the following:

* All ports are assigned to VLAN 1 by default.
* The native VLAN is VLAN 1 by default.
* The management VLAN is VLAN 1 by default.
* VLAN 1 cannot be renamed or deleted.

For instance, in the **show vlan brief** output, all ports are currently assigned to the default VLAN 1. No native VLAN is explicitly assigned and no other VLANs are active; therefore, the network is designed with the native VLAN the same as the management VLAN. This is considered a security risk.



#### Data VLAN

Data VLANs are VLANs configured to separate user-generated traffic. They are referred to as user VLANs because they separate the network into groups of users or devices. A modern network would have many data VLANs depending on organizational requirements. Note that voice and network management traffic should not be permitted on data VLANs.

#### Native VLAN

User traffic from a VLAN must be tagged with its VLAN ID when it is sent to another switch. Trunk ports are used between switches to support the transmission of tagged traffic. Specifically, an 802.1Q trunk port inserts a 4-byte tag in the Ethernet frame header to identify the VLAN to which the frame belongs.

A switch may also have to send untagged traffic across a trunk link. Untagged traffic is generated by a switch and may also come from legacy devices. The 802.1Q trunk port places untagged traffic on the native VLAN. The native VLAN on a Cisco switch is VLAN 1 (i.e., default VLAN).

It is a best practice to configure the native VLAN as an unused VLAN, distinct from VLAN 1 and other VLANs. In fact, it is not unusual to dedicate a fixed VLAN to serve the role of the native VLAN for all trunk ports in the switched domain.

#### Management VLAN

A management VLAN is a data VLAN configured specifically for network management traffic including SSH, Telnet, HTTPS, HTTP, and SNMP. By default, VLAN 1 is configured as the management VLAN on a Layer 2 switch.

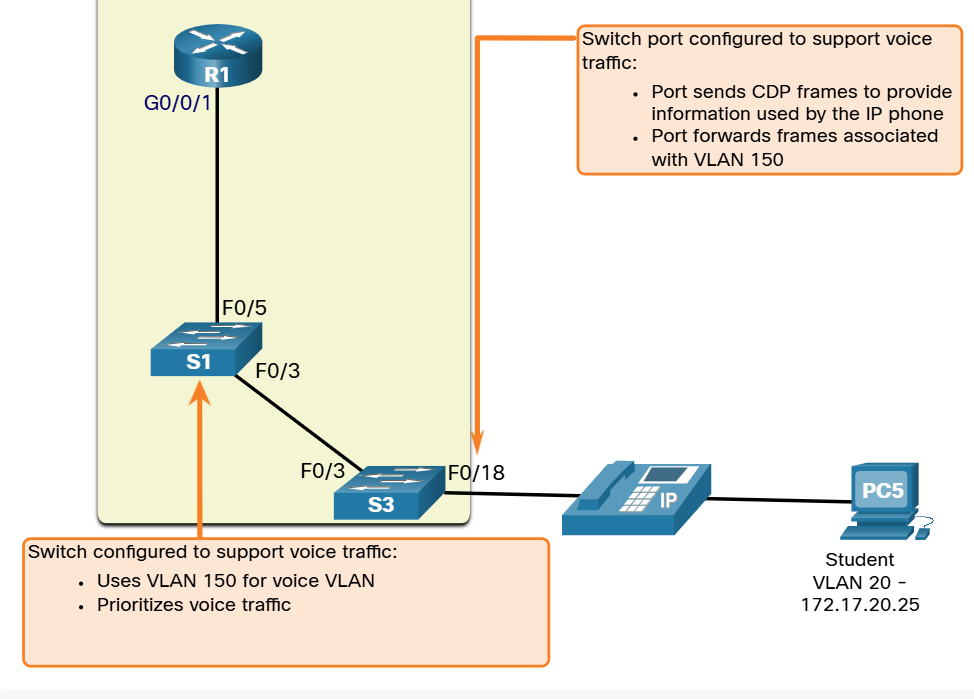
#### Voice VLAN

A separate VLAN is needed to support Voice over IP (VoIP). VoIP traffic requires the following:

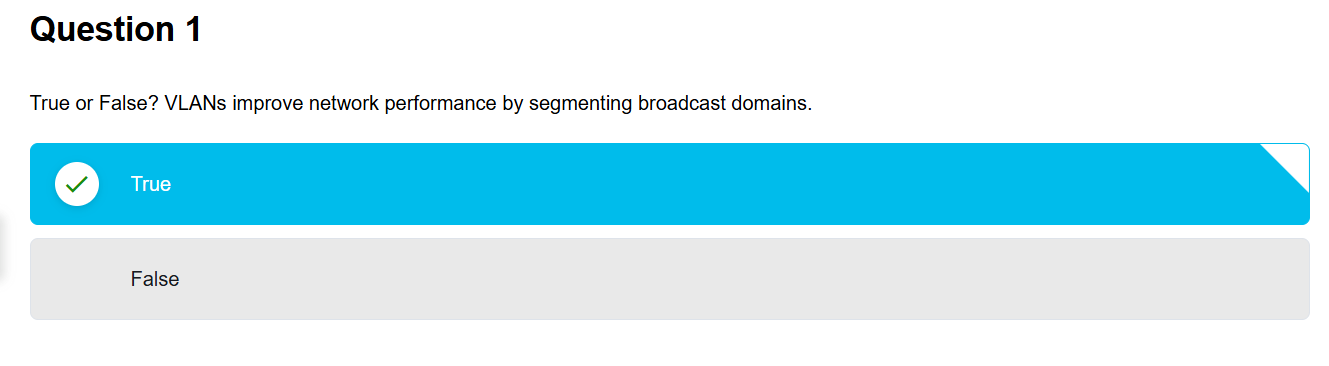
* Assured bandwidth to ensure voice quality
* Transmission priority over other types of network traffic
* Ability to be routed around congested areas on the network
* Delay of less than 150 ms across the network

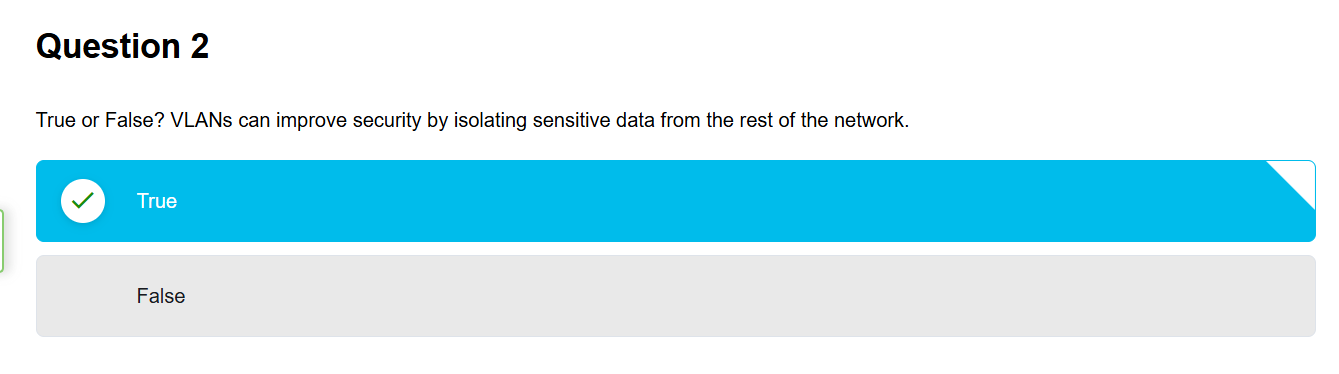
To meet these requirements, the entire network has to be designed to support VoIP.

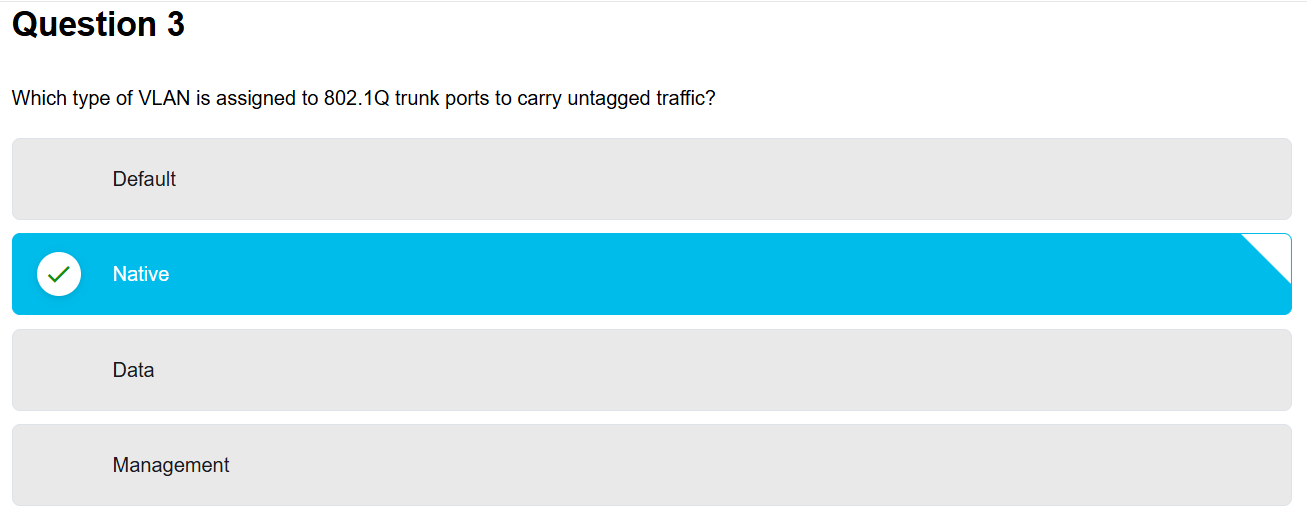
In the figure, VLAN 150 is designed to carry voice traffic. The student computer PC5 is attached to the Cisco IP phone, and the phone is attached to switch S3. PC5 is in VLAN 20, which is used for student data.

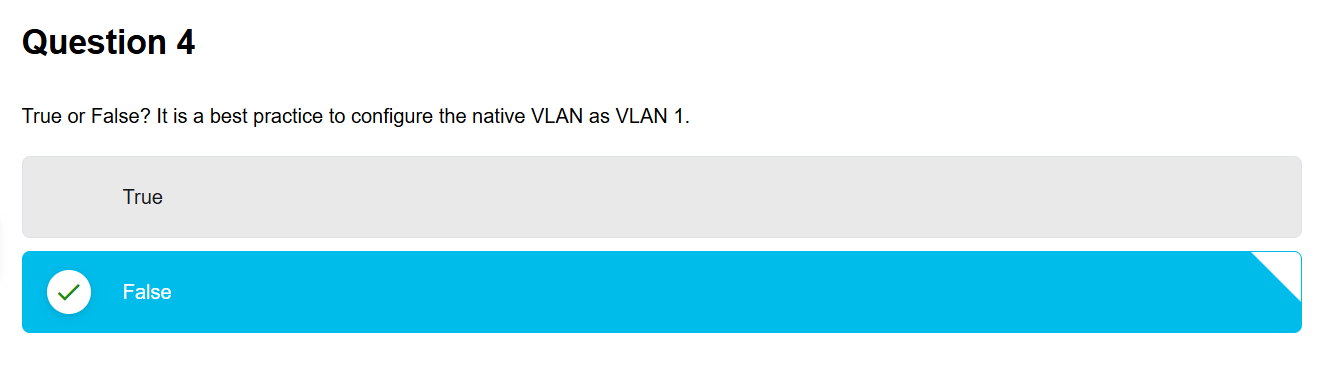


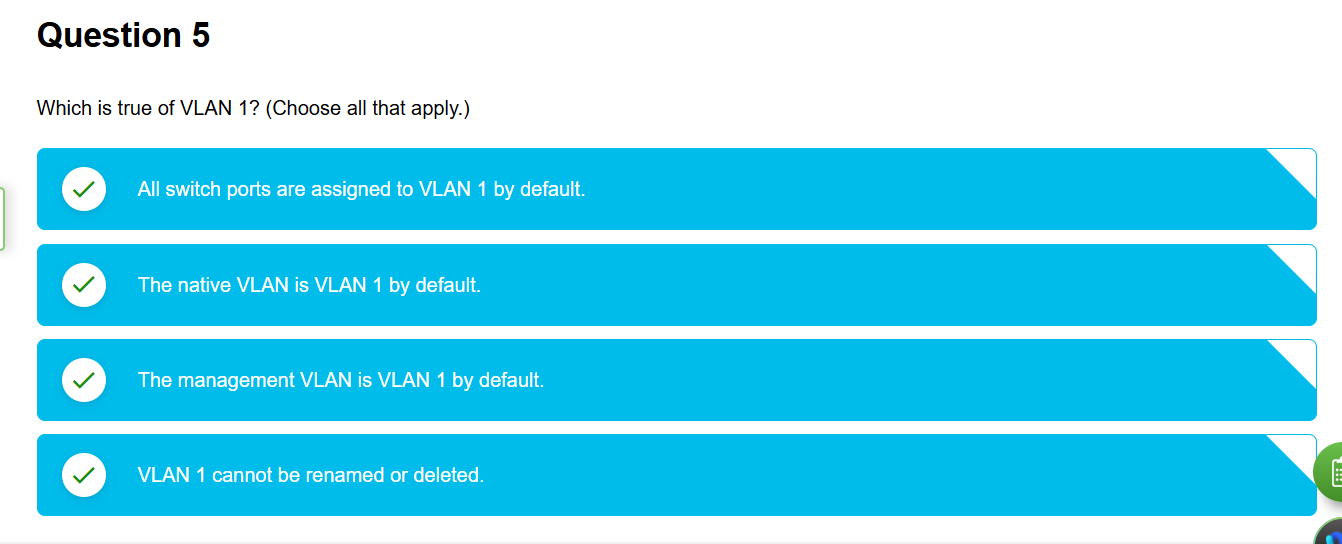
### Check Your Understanding - Overview of VLANs











## VLANs in a Multi-Switched Environment

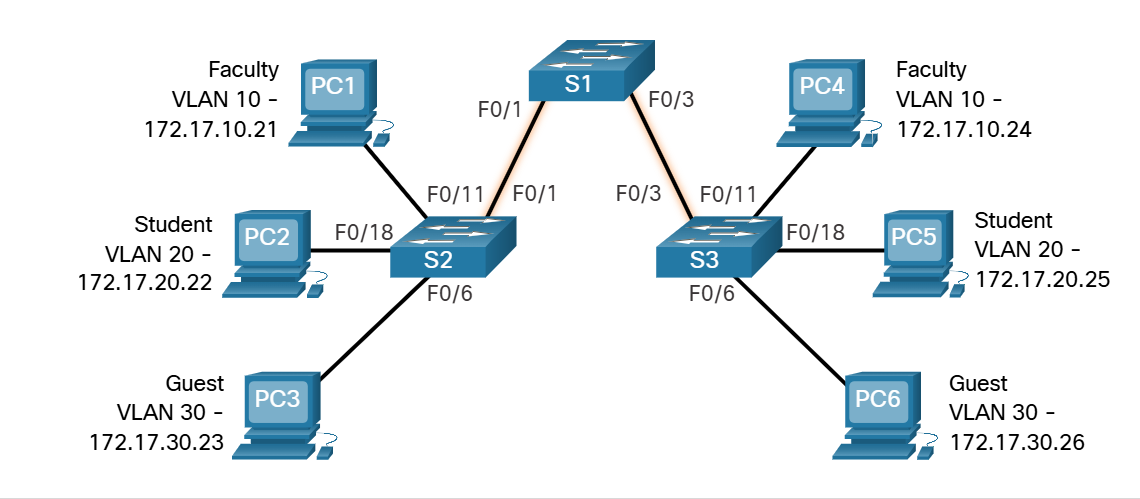
### Defining VLAN Trunks

VLANs would not be very useful without VLAN trunks. VLAN trunks allow all VLAN traffic to propagate between switches. This enables devices connected to different switches but in the same VLAN to communicate without going through a router.

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. Cisco supports IEEE 802.1Q for coordinating trunks on Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces.

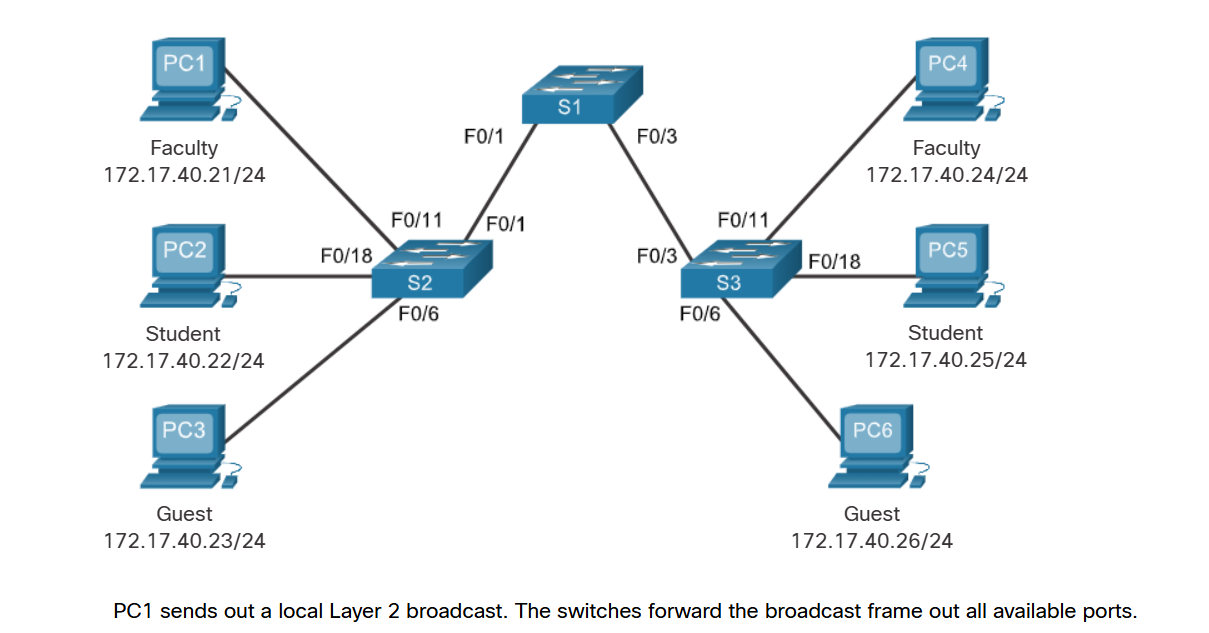
A VLAN trunk does not belong to a specific VLAN. Instead, it is a conduit for multiple VLANs between switches and routers. A trunk could also be used between a network device and server or another device that is equipped with an appropriate 802.1Q-capable NIC. By default, on a Cisco Catalyst switch, all VLANs are supported on a trunk port.

In the figure, the highlighted links between switches S1 and S2, and S1 and S3 are configured to transmit traffic coming from VLANs 10, 20, 30, and 99 (i.e., native VLAN) across the network. This network could not function without VLAN trunks.



### Network without VLANs

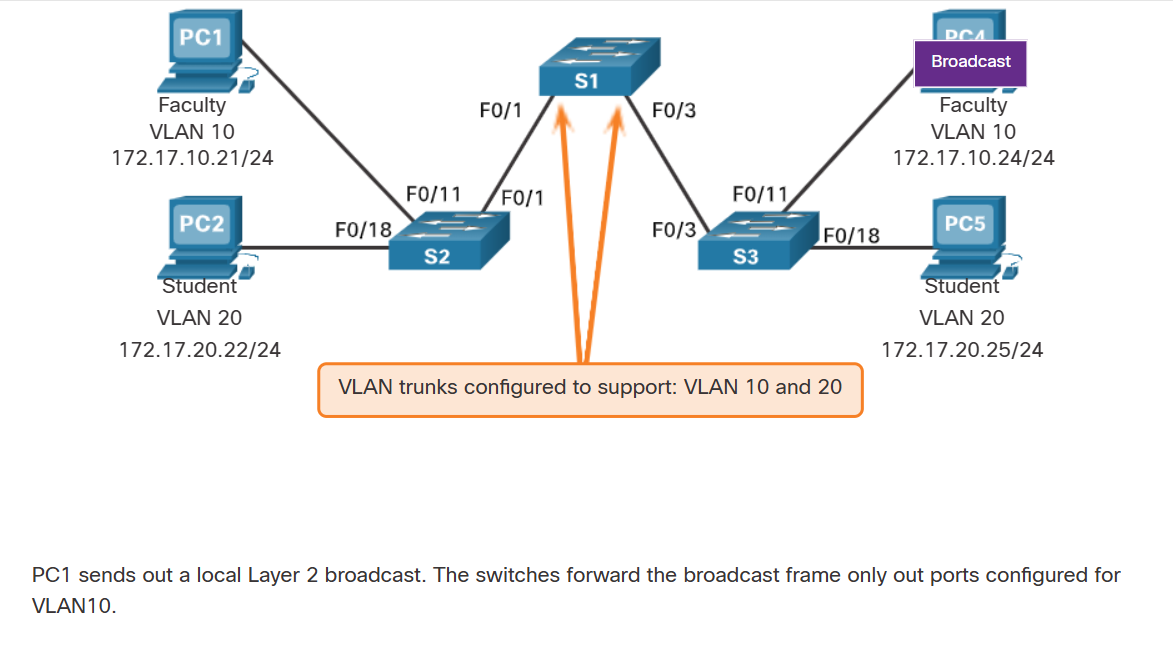
When a switch receives a broadcast frame on one of its ports, it forwards the frame out all other ports except the port where the broadcast was received. In the animation, the entire network is configured in the same subnet (172.17.40.0/24) and no VLANs are configured. As a result, when the faculty computer (PC1) sends out a broadcast frame, switch S2 sends that broadcast frame out all of its ports. Eventually the entire network receives the broadcast because the network is one broadcast domain.



### Network with VLANs

VLANs are associated with and configured on individual switch ports. Devices attached to those ports have no concept of VLANs. However, these devices are configured with IP addressing and are members of a specific IP network. This is where the connection between VLAN and IP network is apparent. A VLAN is the equivalent to an IP network (or subnet). VLANs are configured on the switch, whereas IP addressing is configured on the device.

Click Play in the animation to see that the same network has now been segmented using two VLANs. Faculty devices are assigned to VLAN 10 and student devices are assigned to VLAN 20. When a broadcast frame is sent from the faculty computer, PC1, to switch S2, the switch forwards that broadcast frame only to those switch ports configured to support VLAN 10.



The ports that comprise the connection between switches S2 and S1 (ports F0/1), and between S1 and S3 (ports F0/3) are trunks and have been configured to support all the VLANs in the network.

When S1 receives the broadcast frame on port F0/1, S1 forwards that broadcast frame out of the only other port configured to support VLAN 10, which is port F0/3. When S3 receives the broadcast frame on port F0/3, it forwards that broadcast frame out the only other port configured to support VLAN 10, which is port F0/11. The broadcast frame arrives at the only other computer in the network configured in VLAN 10, which is faculty computer PC4.

When VLANs are implemented on a switch, the transmission of unicast, multicast, and broadcast traffic from a host in a particular VLAN are restricted to the devices that are in that VLAN.

### VLAN Identification with a Tag

The standard Ethernet frame header does not contain information about the VLAN to which the frame belongs. Therefore, when Ethernet frames are placed on a trunk, information about the VLANs to which they belong must be added. This process, called tagging, is accomplished by using the IEEE 802.1Q header, specified in the IEEE 802.1Q standard. The 802.1Q header includes a 4-byte tag inserted within the original Ethernet frame header, specifying the VLAN to which the frame belongs.

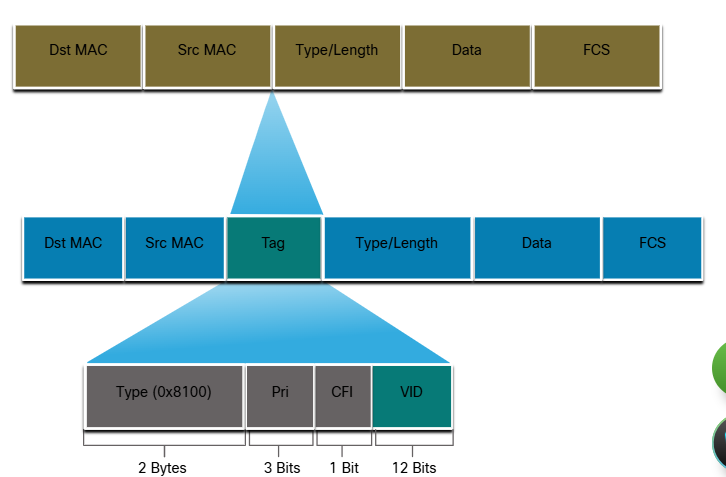
When the switch receives a frame on a port configured in access mode and assigned a VLAN, the switch inserts a VLAN tag in the frame header, recalculates the Frame Check Sequence (FCS), and sends the tagged frame out of a trunk port.

**VLAN Tag Field Details**

As shown in the figure, the VLAN tag control information field consists of a Type field, a Priority field, a Canonical Format Identifier field, and VLAN ID field:

* **Type** - A 2-byte value called the tag protocol ID (TPID) value. For Ethernet, it is set to hexadecimal 0x8100.
* **User priority** - A 3-bit value that supports level or service implementation.
* **Canonical Format Identifier (CFI)** - A 1-bit identifier that enables Token Ring frames to be carried across Ethernet links.
* **VLAN ID (VID)** - A 12-bit VLAN identification number that supports up to 4096 VLAN IDs.

After the switch inserts the tag control information fields, it recalculates the FCS values and inserts the new FCS into the frame.



### Native VLANs and 802.1Q Tagging