Introduction to Switched Networks

Objectives

After completing this course, students will be able to

- Explain how switched networks support small and medium-sized businesses.
- Understand the convergence of data, voice, and video affected switched networks.
- Describe the benefits of creating networks based on a structured hierarchical design model.
- Enumerate the two most commonly used Cisco hierarchical design models.
- Identify the layers found in the Cisco hierarchical design model.
- Identify what switch form factors are available.
- Explain how does Layer 2 switches build and uses MAC address table to forward data.
- Differentiate the collision domain to broadcast domain.

Introduction

Different devices must seamlessly work together to provide a fast, secure, and reliable connection between hosts. LAN switches provide the connection point for end users into the enterprise network and are also primarily responsible for the control of information within the LAN environment. Routers facilitate the movement of information between LANs and are generally unaware of individual hosts. All advanced services depend on the availability of a robust routing and switching infrastructure on which they can build. This infrastructure must be carefully designed, deployed, and managed to provide a necessary stable platform.

LAN Design

By knowing how to design a LAN, a network professional knows the network components and how those components interact with one another.

Converged Networks

- a single network designed to handle voice, video, and data
- an internal network where the Layer 3 devices, such as routers, have a complete routing table to be able to accurately and efficiently send data to a remote destination;
- a switch network that has completed calculations that result in a single path through the switch network.

Figure 1-1 Converged Network Components

Elements of a Converged Network

To support collaboration, business networks employ converged solutions using voice systems, IP phones, voice gateways, video support, and video conferencing (Figure 1-3). Including data services, a converged network with collaboration support may include features such as the following:

Call control -Telephone call processing, caller ID, call transfer, hold, and conference

Voice messaging – Voicemail

Mobility- Receive important calls wherever you are

Automated attendant - Serve customers faster by routing calls directly to the right department or individual

One of the primary benefits of transitioning to the converged network is that there is just one physical network to install and manage. This results in substantial savings over the installation and management of separate voice, video, and data networks. Such a converged network solution integrates IT management so that any moves, additions, and changes are completed with an intuitive management interface. A converged network solution also provides PC soft phone application support, as well as point-to-point video so that users can enjoy personal communications with the same ease of administration and use as a voice call.

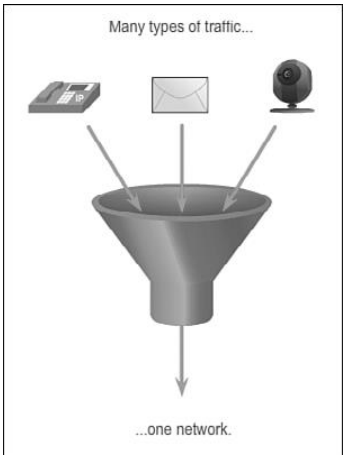

Figure 1-2 Network Traffic Convergence

The convergence of services onto the network has resulted in an evolution in networks from a traditional data transport role, to a super-highway for data, voice, and video communication. This one physical network must be properly designed and implemented to allow the reliable handling of the various types of information that it must carry. A structured design is required to allow management of this complex environment.

Borderless Switched Networks

The Cisco Borderless Network is a network architecture that combines several innovations and design considerations to allow organizations to connect anyone, anywhere, anytime, and on any device securely, reliably, and seamlessly. This architecture is designed to address IT and business challenges, such as supporting the converged network and changing work patterns.

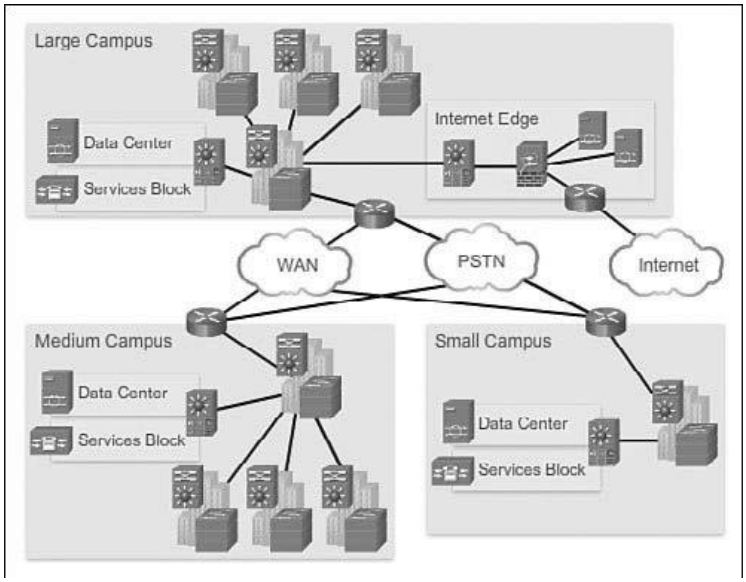

Figure 1-3 Borderless Switched Networks

The Cisco Borderless Network is built on an infrastructure of scalable and resilient hardware and software. It enables different elements, from access switches to wireless access points, to work together and allow users to access resources from any place at any time, providing optimization, scalability, and security to collaboration and virtualization.

Hierarchy in the Borderless Switched Network

Creating a borderless switched network requires that sound network design principles are used to ensure maximum availability, flexibility, security, and manageability. The borderless switched network must deliver on current requirements and future required services and technologies. Borderless switched network design guidelines are built upon the following principles:

Hierarchical: Facilitates understanding the role of each device at every tier, simplifies deployment, operation, and management, and reduces fault domains at every tier

Modularity: Allows seamless network expansion and integrated service enablement on an on-demand basis

Resiliency: Satisfies user expectations for keeping the network always on

Flexibility: Allows intelligent traffic load sharing by using all network resources. These are not independent principles. Understanding how each principle fits in the context of the others is critical. Designing a borderless switched network in a hierarchical fashion creates a foundation that allows network designers to overlay

security, mobility, and unified communication features. Two time-tested and proven hierarchical design frameworks for campus networks are the three-tier layer and the two tier layer models, as illustrated in Figure 1-4.

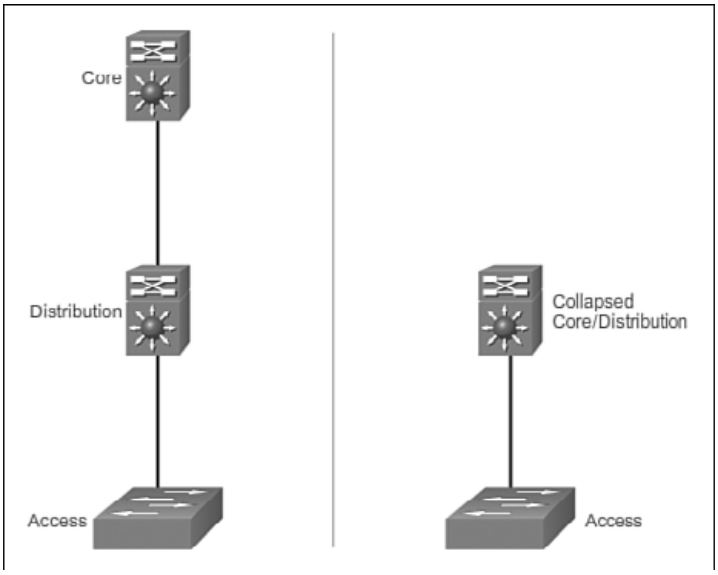

Figure 1-4 Switch Network Design Models

Core Distribution Access

Three layers of distribution access:

- Access layer
- Distribution layer
- Core layer

Access Layer

The ***access layer*** represents the network edge, where traffic enters or exits the campus network. Traditionally, the primary function of an access layer switch is to provide network access to the user. Access layer switches connect to distribution layer switches, which implement network foundation technologies such as routing, quality of service, and security.

To meet network application and end-user demand, the next-generation switching platforms now provide more converged, integrated, and intelligent services tovarious types of endpoints at the network edge. Building intelligence into access layer switches allows applications to operate on the network more efficiently and securely.

Distribution Layer

The ***distribution layer*** interfaces between the access layer and the core layer toprovide many important functions, including:

- Aggregating large-scale wiring closet networks
- Aggregating Layer 2 broadcast domains and Layer 3 routing boundaries
- Providing intelligent switching, routing, and network access policy functions to access the rest of the network
- Providing high availability through redundant distribution layer switches to the end-user and equal cost paths to the core
- Providing differentiated services to various classes of service applications at the edge of the network

Core Layer

The ***core layer*** is the network backbone. It connects several layers of the campus network. The core layer serves as the aggregator for all of the other campus blocks and ties the campus together with the rest of the network. The primary purpose of the core layer is to provide fault isolation and high-speed backbone connectivity.

Figure 1-5 shows a ***three-tier campus network design*** for organizations where the access, distribution, and core are each separate layers. To build a simplified, scalable, cost-effective, and efficient physical cable layout design, the recommendation is to build an extended-star physical network topology from a centralized building location to all other buildings on the same campus.

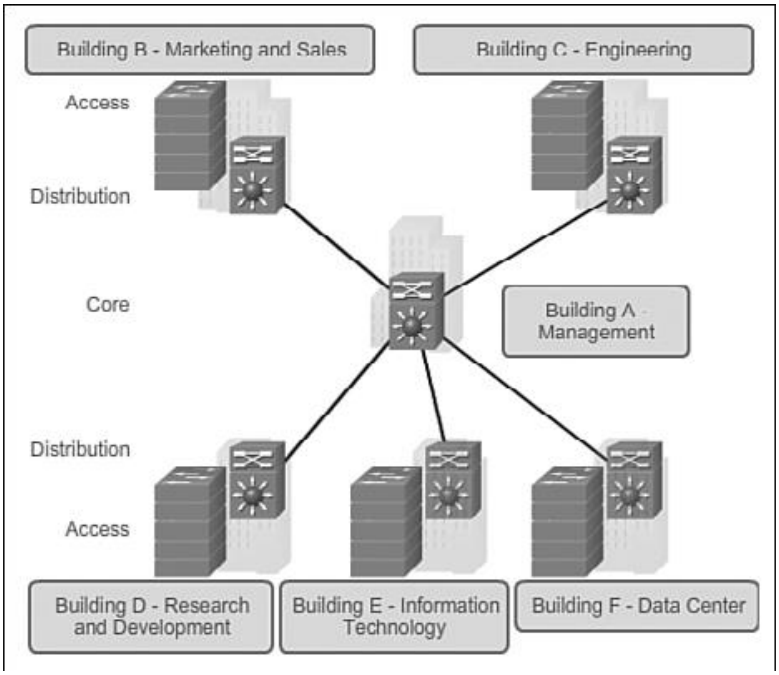

Figure 1-5 Three-Tier Campus Network Design

In some cases, because of a lack of physical or network scalability restrictions, maintaining a separate distribution and core layer is not required. In smaller campus locations where there are fewer users accessing the network or in campus sites consisting of a single building, separate core and distribution layers may not be needed. In this scenario, the recommendation is the alternate ***two-tier campus network design***, also known as the ***collapsed core network design.***

Figure 1-6 shows a two-tier campus network design example for an enterprise campus where the distribution and core layers are collapsed into a single layer .

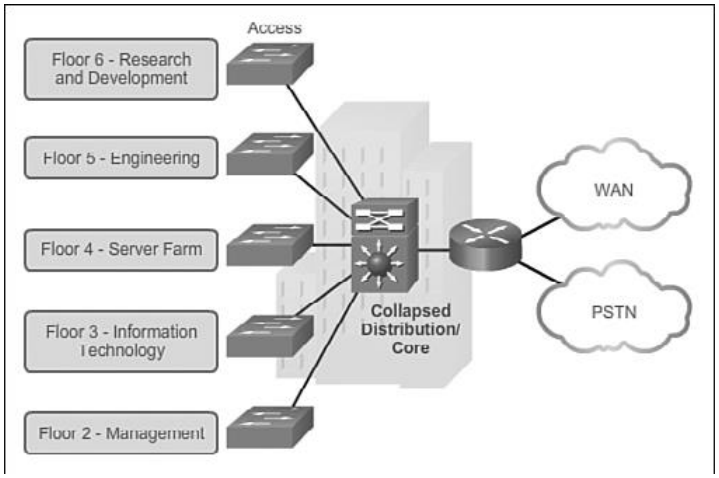

Figure 1-6 Two-Tier Campus Network Design

Switched Networks

Switched networks are important when deploying wired LANs. A network professional today must be well-versed in switches and LAN technology in order to add commonly deployed devices such as PCs, printers, video cameras, phones, copiers, and scanners. Sharing and accessing network devices is common in both the home and business network.

Role of Switched Networks

A switched LAN allows more flexibility, traffic management, and additional features, such as:

- Quality of service
- Additional security
- Support for wireless networking and connectivity
- Support for new technologies, such as IP telephony and mobility services

Figure 1-8 shows the hierarchical design used in the borderless switched network.

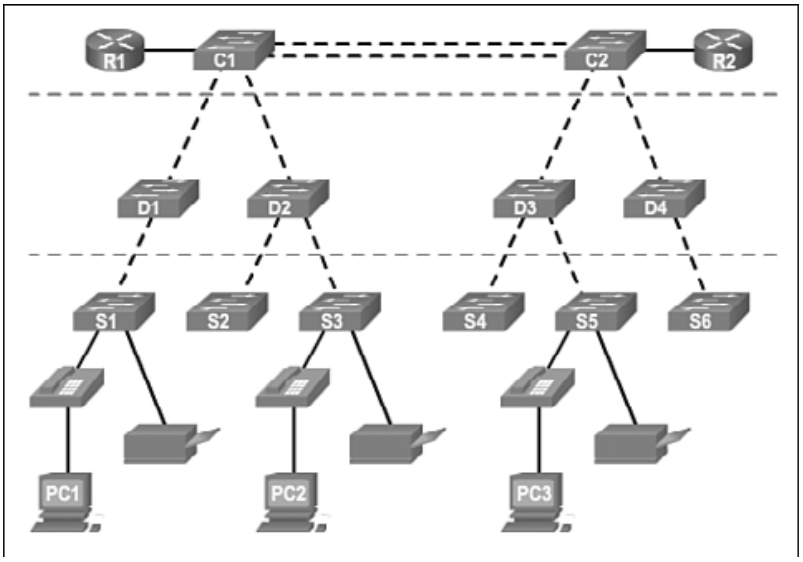

Figure 1-7 Hierarchical Networks

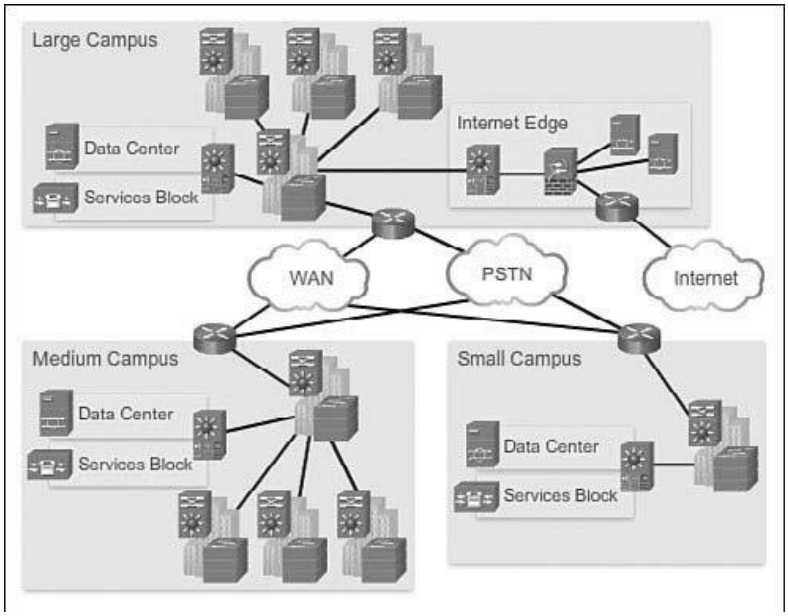

Figure 1-8 Three-Tier Design in Borderless Switched Networks

Form Factors

There are various types of switches used in business networks. It is important to deploy the appropriate types of switches based on network requirements. Table 1-1

Highlights some common business considerations when selecting switch equipment.

Table 1-1 Business Considerations for Switch Selection

Business Consideration

Switch Feature	**Business Consideration**
Cost	The cost of a switch will depend on the number and speed of the interfaces, supported features, and expansion capability.
Port density	Network switches must support the appropriate number of devices on the network.
Power	It is now common to power access points, IP phones, and even compact switches using Power over Ethernet (PoE). In addition to PoE considerations, some chassis-based switches support redundant power supplies.
Reliability	The switch should provide continuous access to the network.
Port speed	The speed of the network connection is of primary concern to the end users.
Frame buffers	The capability of the switch to store frames is important in a network where there may be congested ports to servers or other areas of the network.
Scalability	The number of users on a network typically grows over time; therefore, the switch should provide the opportunity for growth.

When selecting the type of switch, the network designer must choose between a fixed or a modular configuration, and stackable or non-stackable. Another consideration is the thickness of the switch, which is expressed in number of rack units. This is important for switches that are mounted in a rack. For example, the fixed configuration switches shown in Figure 1-9 are all 1 rack unit (1U). These options are sometimes referred to as switch form factors.

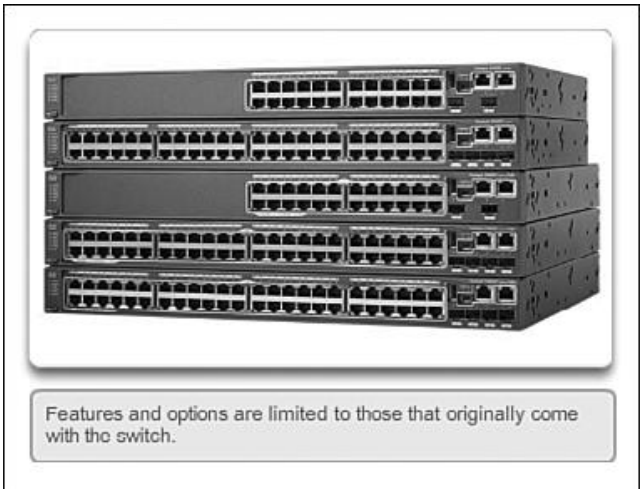

Figure 1-9 Fixed Configuration Switches

Fixed Configuration Switches

Fixed configuration switches do not support features or options beyond those that originally came with the switch (refer to Figure 1-9). The particular model determines the features and options available. For example, a 24-port gigabit fixed switch cannot support additional ports. There are typically different configuration choices that vary in how many and what types of ports are included with a fixed configuration switch.

Modular Configuration Switches

Modular configuration switches offer more flexibility in their configuration. Modular configuration switches typically come with different sized chassis that allow for the installation of different numbers of modular line cards (Figure 1-10). The line cards actually contain the ports. The line card fits into the switch chassis the way that expansion cards fit into a PC. The larger the chassis, the more modules it can support. There can be many different chassis sizes to choose from. A modular switch with a 24-port line card supports an additional 24-port line card, to bring the total number of ports up to 48.

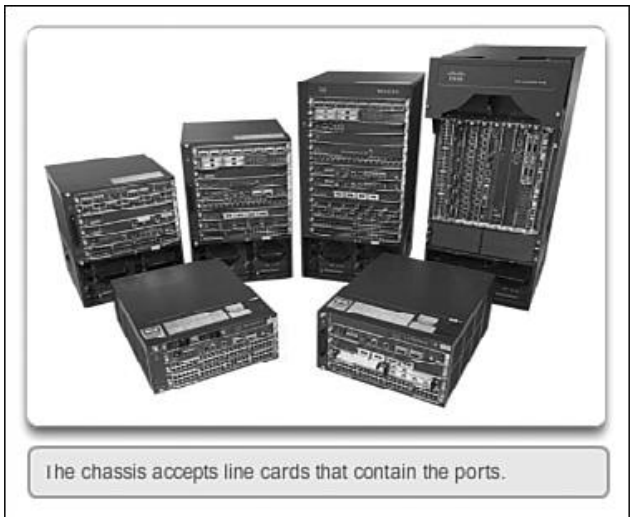

Figure 1-10 Modular Configuration Switches

Stackable Configuration Switches

Stackable configuration switches can be interconnected using a special cable that provides high-bandwidth throughput between the switches (Figure 1-11). Cisco StackWise technology allows the interconnection of up to nine switches. Switches can be stacked one on top of the other with cables connecting the switches in a daisy chain fashion. The stacked switches effectively operate as a single larger switch. Stackable switches are desirable where fault tolerance and bandwidth availability are critical and a modular switch is too costly to implement. Using cross-connected connections, the network can recover quickly if a single switch fails.

Stackable switches use a special port for interconnections. Many Cisco stackable switches also support StackPower technology, which enables power sharing among stack members.

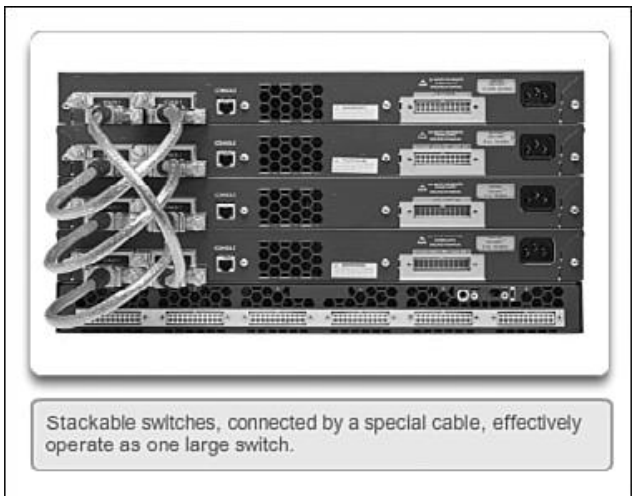

Figure 1-11 Stackable Configuration Switches

The Switched Environment

One of the most exciting functions of networking is the switched environment because businesses are always adding devices to the wired network, and they will do so through a switch. Learning how switches operate is important to someone entering the networking profession.

Frame Forwarding

On Ethernet networks, frames contain a source MAC address and a destination MAC address. Switches receive a frame from the source device and quickly forward it toward the destination device.

Switching as a General Concept in Networking and Telecommunications

The concept of switching and forwarding frames is universal in networking and telecommunications.

Various types of switches are used in LANs, WANs, and the public switched telephone network (PSTN). The fundamental concept of switching refers to a device making a decision based on two criteria:

- Ingress port
- Destination address

The decision on how a switch forwards traffic is made in relation to the flow of thattraffic. The term ***ingress*** is used to describe a frame entering a device on a specific port. The term ***egress*** is used to describe frames leaving the device through a particular port.

When a switch makes a decision, it is based on the ingress port and the destinationaddress of the message.

A LAN switch maintains a table that it uses to determine how to forward traffic through the switch.

The only intelligence of the LAN switch is its capability to use its table to forward traffic based on the ingress port and the destination address of a message. With a LAN switch, there is only one master switching table that describes a strict association between addresses and ports; therefore, a message with a given destination address always exits the same egress port, regardless of the ingress port it enters. Cisco LAN switches forward Ethernet frames based on the destination MAC address of the frames.

Dynamically Populating a Switch MAC Address Table

Switches use MAC addresses to direct network communications through the switch to the appropriate outbound port toward the destination. A switch is made up of integrated circuits and accompanying software that controls the data paths through the switch. 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,*** or content addressable memory (CAM) table. CAM is a special type of memory used in high-speed searching applications.

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

An easy way to remember how a switch operates is the following saying: A switch learns on “source” and forwards based on “destination.” This means that a switch populates the MAC address table based on source MAC addresses. As frames enter the switch, the switch “learns” the source MAC address of the received frame and adds the MAC address to the MAC address table or refreshes the age timer of an existing MAC address table entry.

To forward the frame, the switch examines the destination MAC address and compares it to addresses found in the MAC address table. If the address is in the table, the frame is forwarded out the port associated with the MAC address in the table.

When the destination MAC address is not found in the MAC address table, the switch forwards the frame out of all ports (flooding) except for the ingress port of the frame. In networks with multiple interconnected switches, the MAC address table contains multiple MAC addresses for a single port connected to the other switches.

The following steps describe the process of building the MAC address table:

Step 1. The switch receives a frame from PC 1 on Port 1 (Figure 1-12).

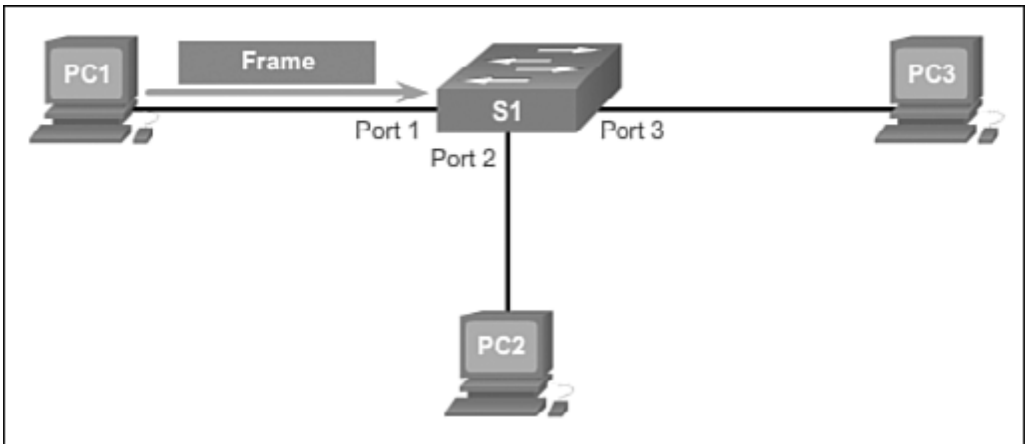

Figure 1-12 Building a MAC Address Table: PC1 Sends Frame to Port 1

Step 2. The switch examines the source MAC address and compares it to the MAC address table.

How To

If the address is not in the MAC address table, it associates the source MAC address of PC 1 with the ingress port (Port 1) in the MAC address table (Figure 1-13).

If the MAC address table already has an entry for that source address, it resets the aging timer. An entry for a MAC address is typically kept for five minutes.

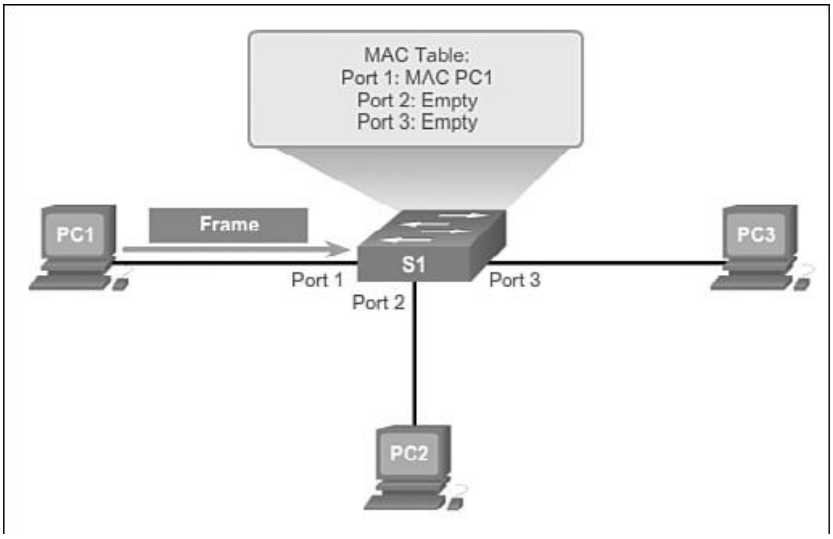

Figure 1-13 Building a MAC Address Table: S1 Adds MAC Address Heard Through Port 1

Step 3. After the switch has recorded the source address information, the switch examines the destination MAC address.

If the destination address is not in the MAC table or if it's a broadcast MAC address, as indicated by all Fs, the switch floods the frame to all ports, except the ingress port (Figure 1-14).

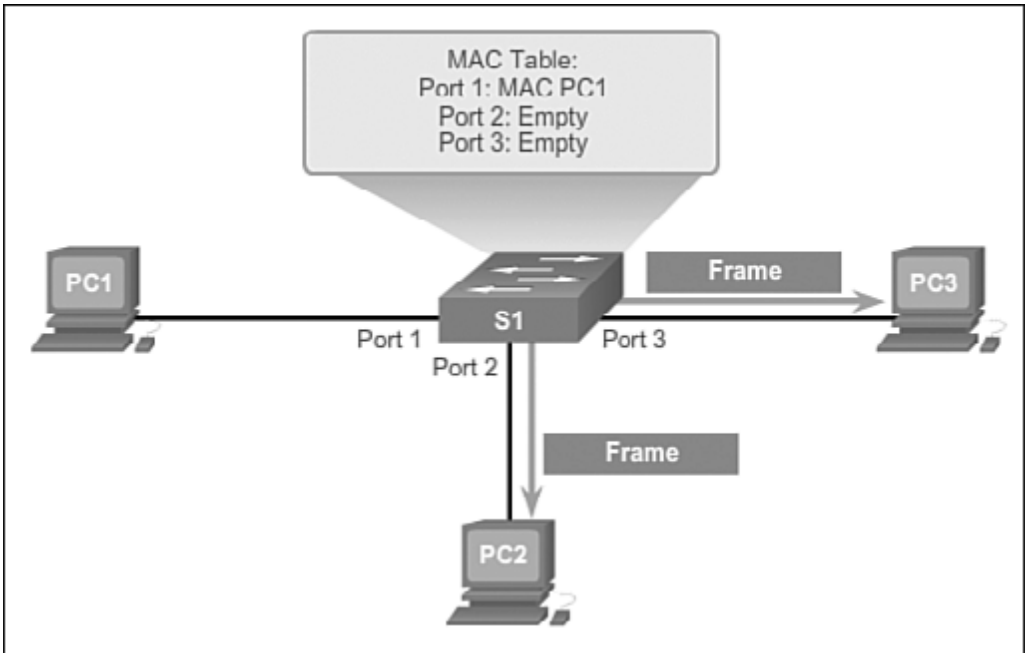

Figure 1-14 Building a MAC Address Table: S1 Broadcasts the Frame

Step 4. The destination device (PC 3) replies to the frame with a unicast frame addressed to PC 1 (Figure 1-15).

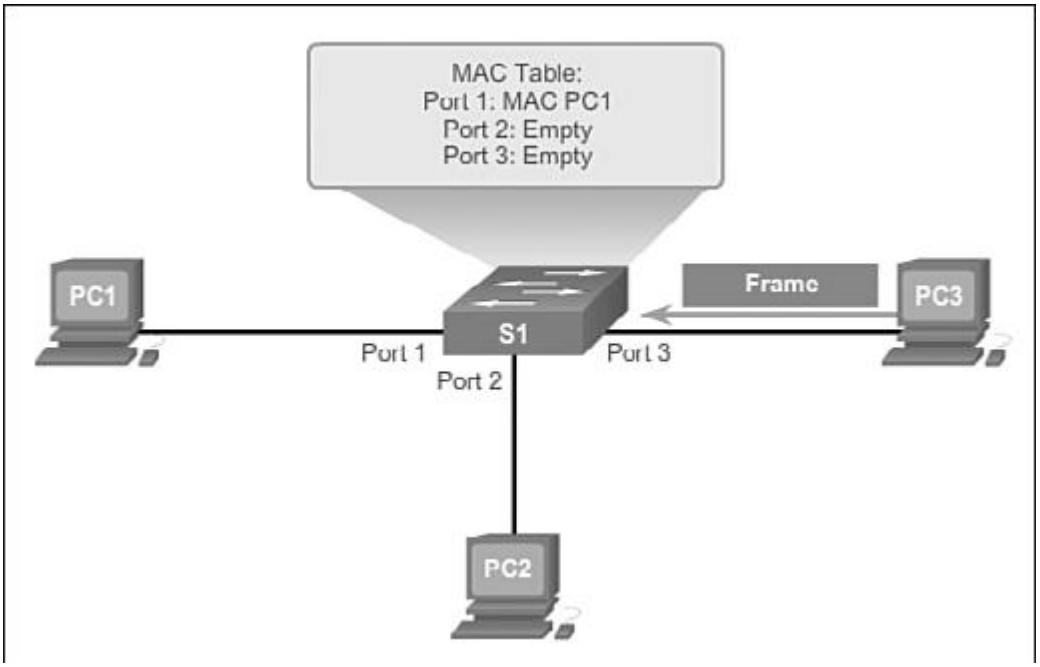

Figure 1-15 Building a MAC Address Table: PC3 Sends a Reply Frame

Step 5. The switch enters the source MAC address of PC 3 and the port number of the ingress port into the address table. The destination address of the frame and its associated egress port is found in the MAC address table

(Figure 1-16).

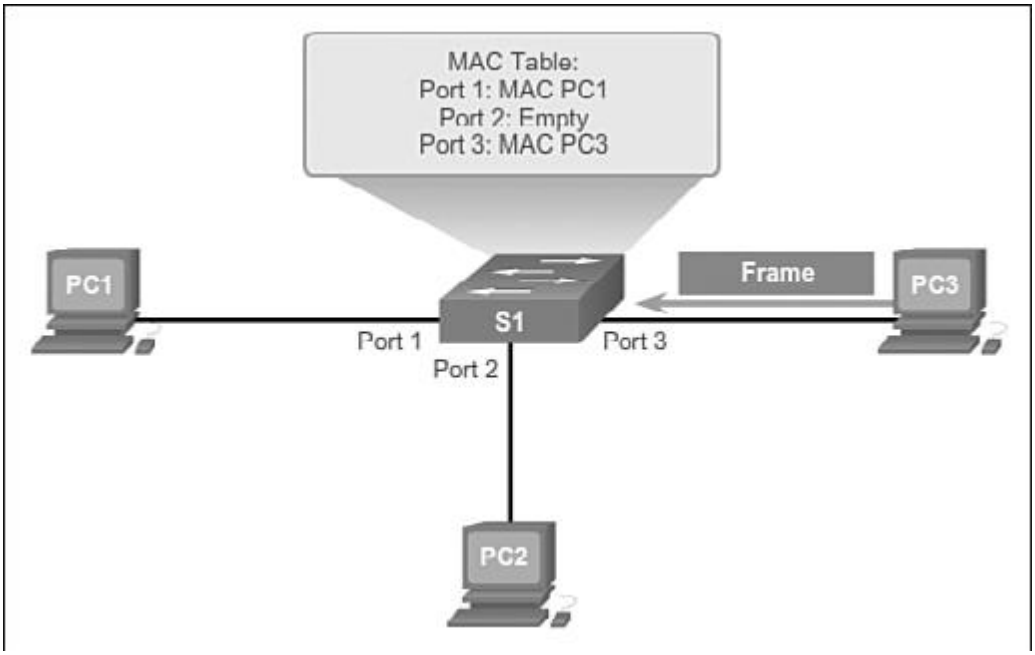

Figure 1-16 Building a MAC Address Table: S1 Adds the MAC Address for PC3

Step 6. The switch can now forward frames between these source and destination devices without flooding because it has entries in the address table that identify the associated ports (Figure 1-17).

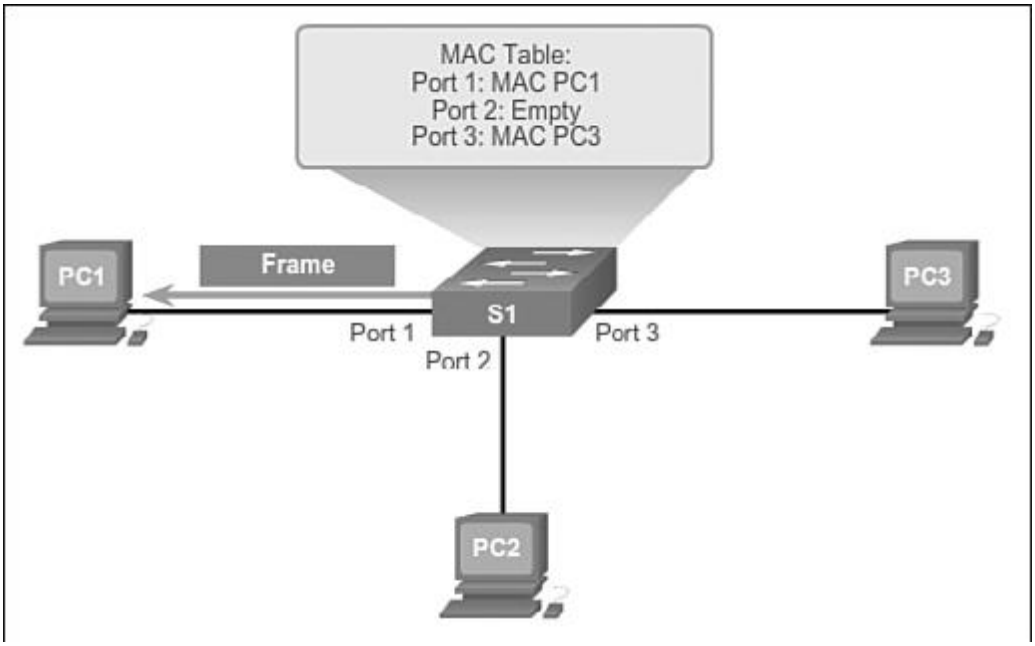

Figure 1-17 Building a MAC Address Table: S1 Sends the Frame to Port 1

Switch Forwarding Methods

Commonly, in earlier networks, as they grew, enterprises began to experience slowernetwork performance. Ethernet bridges (an early version of a switch) were added to networks to limit the size of the collision domains. In the 1990s, advancements in integrated circuit technologies allowed for LAN switches to replace Ethernet bridges. These LAN switches were able to move the Layer 2 forwarding decisions from software to ***application-specific-integrated circuits (ASICs).*** ASICs reduce the packet-handling time within the device, and allow the device to handle an increased number of ports without degrading performance. This method of forwarding data frames at Layer 2 was referred to as ***store-and-forward switching.*** This term distinguished it from cut-through switching. As shown in the online video, the store-and-forward method makes a forwarding decision on a frame after it has received the entire frame and then checked the frame for errors.

By contrast, the ***cut-through switching method,*** as shown in the online video, begins the forwarding process after the destination MAC address of an incoming frame and the egress port has been determined.

Store-and-Forward Switching

Store-and-forward switching has two primary characteristics that distinguish it from cut-through: error checking and automatic buffering.

Error Checking

A switch using store-and-forward switching performs an error check on an incoming frame. After receiving the entire frame on the ingress port, as shown in Figure 1-18, 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.

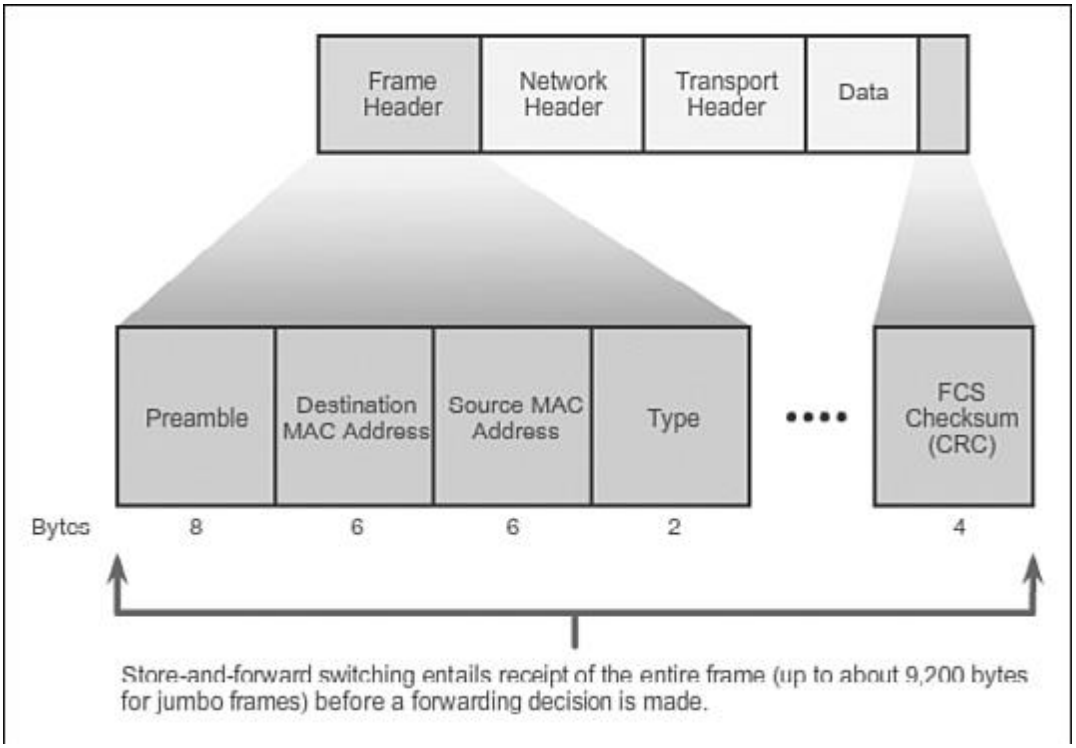

Figure 1-18 Store-and-Forward Switching

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 Mb/s Ethernet port that must be sent out a 1 Gb/s interface would require using the store-and-forward method. With any mismatch in speeds between the ingress and egress ports, the witch stores the entire frame in a buffer, computes the FCS check, forwards the frame to the egress port buffer and then sends the frame.

Store-and-forward switching is Cisco's primary LAN switching method.

A store-and-forward switch drops frames that do not pass the FCS check, therefore it does not forward invalid frames. By contrast, a cut-through switch may forward invalid frames because no FCS check is performed.

Cut-Through Switching

An advantage to cut-through switching is the capability of the switch to start forwarding a frame earlier than store-and-forward switching. There are two primary characteristics of cut-through switching: rapid frame forwarding and invalid frame processing.

Rapid Frame Forwarding

As indicated in Figure 1-19, a switch using the cut-through method can make a forwarding decision as soon as it has looked up the destination MAC address of the frame in its MAC address table. The switch does not have to wait for the rest of the frame to enter the ingress port before making its forwarding decision.

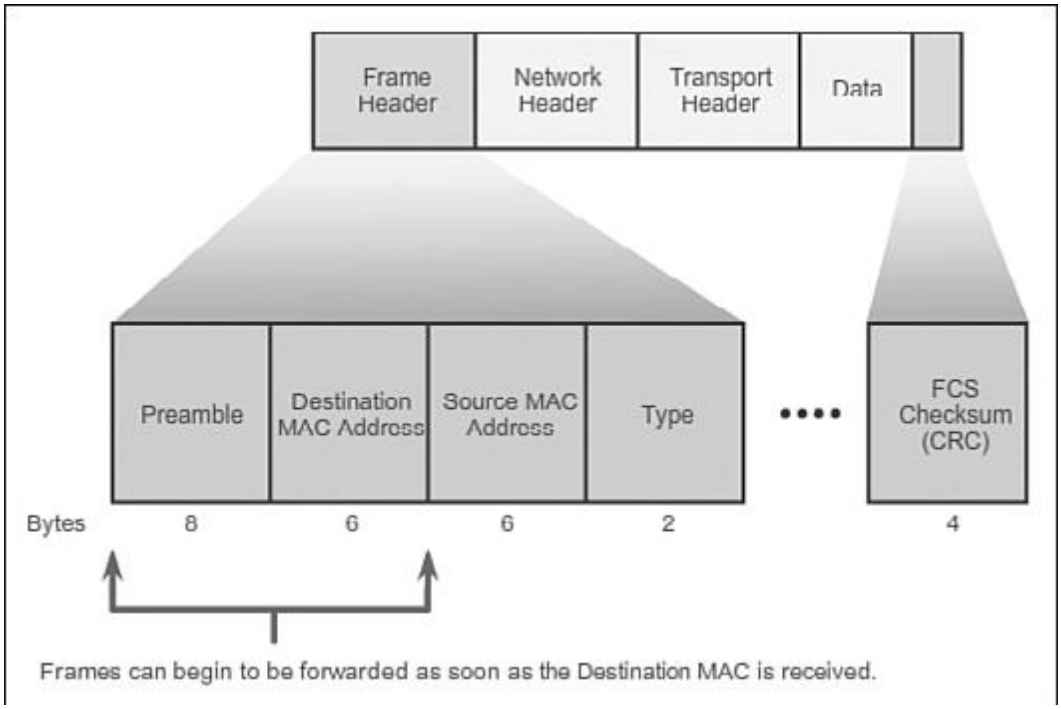

Figure 1-19 Cut-Through Switching

With today's MAC controllers and ASICs, a switch using the cut-through method can quickly decide whether it needs to examine a larger portion of a frame's headers for additional filtering purposes. For example, the switch can analyze past the first 14 bytes (the source MAC address, destination MAC, and the EtherType fields), and examine an additional 40 bytes in order to perform more sophisticated functions relative to IPv4 Layers 3 and 4.

The cut-through switching method does not drop most invalid frames. Frames with errors are forwarded to other segments of the network. If there is a high error rate (invalid frames) in the network, cut-through switching can have a negative impact on bandwidth; thus, clogging up bandwidth with damaged and invalid frames.

Fragment Free

Fragment free switching is a modified form of cut-through switching in which the switch waits for the collision window (64 bytes) to pass before forwarding the frame. This means each frame will be checked into the data

field to make sure no fragmentation has occurred. Fragment free mode provides better error checking than cut-through, with practically no increase in latency.

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

Switching Domains

Two commonly misunderstood terms used with switching are collision domains and broadcast domains. This section tries to explain these two important concepts that affect LAN performance.

Collision Domains

In hub-based Ethernet segments, network devices compete for the medium, because devices must take turns when transmitting. The network segments that share the same bandwidth between devices are known as ***collision domains,*** because when two or more devices within that segment try to communicate at the same time, collisions may occur active.

It is possible, however, to use networking devices such as switches, which operate at the data link layer of the OSI model to divide a network into segments and reduce the number of devices that compete for bandwidth. Each port on a switch is a new segment because the devices plugged into the ports do not compete with each other for bandwidth. The result is that each port represents a new collision domain. More bandwidth is available to the devices on a segment, and collisions in one collision domain do not interfere with the other segments. This is also known as ***microsegmentation***.

As shown in the Figure 1-20, each switch port connects to a single PC or server, and each switch port represents a separate collision domain.

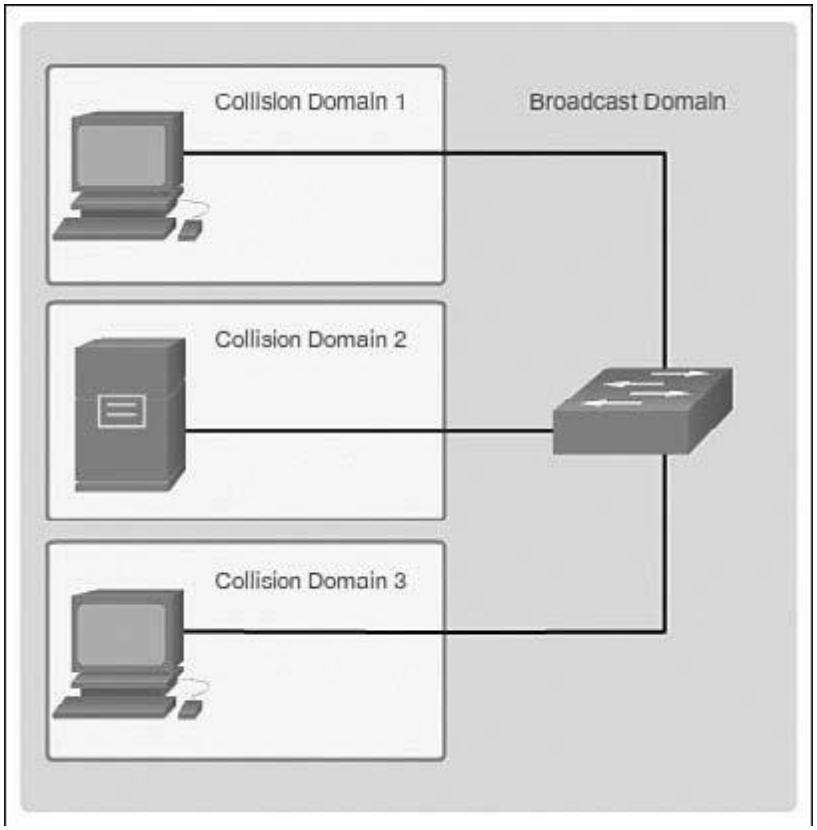

Figure 1-20 Collision Domains

Broadcast Domains

Although switches filter most frames based on MAC addresses, they do not filter broadcast frames. For other switches on the LAN to receive broadcast frames, switches must flood these frames out all ports. A collection of interconnected switches forms a single ***broadcast domain***. A network layer device, such as a router, can divide a Layer 2 broadcast domain. Routers are used to segment both collision and broadcast domains.

When a device sends a Layer 2 broadcast, the destination MAC address in the frame is set to all binary ones. A frame with a destination MAC address of all binary ones is received by all devices in the broadcast domain.

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, the switch forwards the frame out each of the switch 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, as shown in the top broadcast domain in Figure 1-21. 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: a slowdown in the network performance.

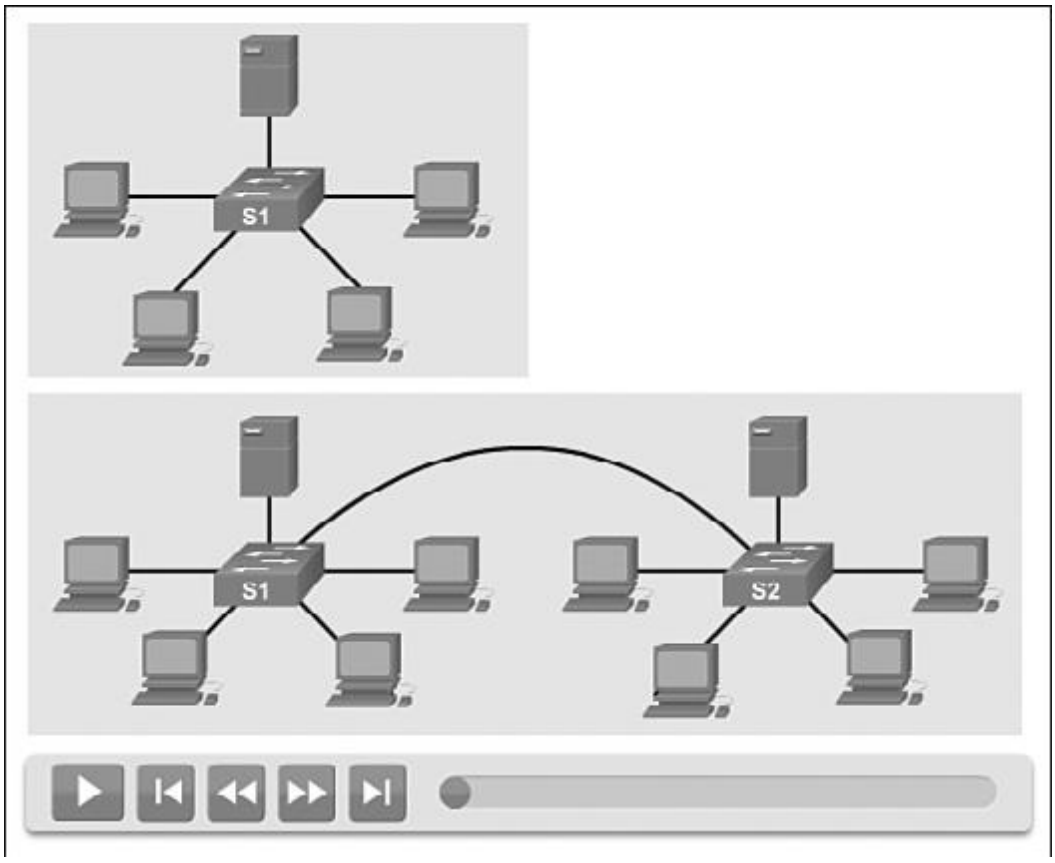

Figure 1-21 Broadcast Domains

When two switches are connected together, the broadcast domain is increased, as seen in the second (bottom) broadcast domain shown in Figure 1-22. 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.

Alleviating Network Congestion

LAN switches have special characteristics that make them effective at alleviating network congestion. First, they allow the segmentation of a LAN into separate collision domains. Each port of the switch represents a separate collision domain and provides the full bandwidth to the device or devices that are connected to that port. Second, they provide full-duplex communication between devices. A full-duplex connection can carry transmitted and received signals at the same time. Full-duplex connections have dramatically increased LAN network performance and are required for 1 Gb/s Ethernet speeds and higher.

Switches interconnect LAN segments (collision domains), use a table of MAC addresses to determine the segment to which the frame is to be sent, and can lessen or eliminate collisions entirely. Table 1-2 shows some important characteristics of switches that contribute to alleviating network congestion.

Table 1-2 Switch Characteristics That Help with Congestion

Characteristic	**Explanation**
High port density	Switches have high-port densities: 24- and 48-port switches are often just 1 rack unit (1.75 inches) in height and operate at speeds of 100 Mb/s, 1 Gb/s, and 10 Gb/s. Large enterprise switches may support hundreds of ports.
Large frame buffers	The ability to store more received frames before having to start dropping them is useful, particularly when there may be congested ports to servers or other parts of the network.
Port speed	Depending on the cost of a switch, it may be possible to support a mixture of speeds. Ports of 100 Mb/s and 1 or 10 Gb/s are common. (100 Gb/s is also possible.)
Fast internal switching	Having fast internal forwarding capabilities allows high performance. The method that is used may be a fast internal bus or shared memory, which affects the overall performance of the switch.
Low per-port cost	Switches provide high-port density at a lower cost. For this reason, LAN switches can accommodate network designs featuring fewer users per segment, therefore, increasing the average available bandwidth per user.

Reference:

- http://www.ciscopress.com/articles/article.asp?p=2180208
- http://www.cisco.com/c/en/us/td/docs/ios/12_2/configfun/command/reference/ffun_r/frf004.html