At-a-Glance: Ethernet

Why Should I Care About Ethernet?

Ethernet was developed in 1972 as a way to connect newly invented computers to newly invented laser printers. It was recognized even at that time as a remarkable technology breakthrough. However, very few people would have wagered that the ability to connect computers and devices would change human communication on the same scale as the invention of the telephone and change business on the scale of the Industrial Revolution. Several competing protocols have emerged since 1972, but Ethernet remains the dominant standard for connecting computers into local-area networks (LAN). For many years Ethernet was dominant in home networks as well. Ethernet has been mostly replaced by wireless technologies in the home networking market. Wireless or Wi-Fi is covered in Part VIII, "Mobility."

What Problems Need to Be Solved?

Ethernet is a shared resource in which end stations (computers, servers, and so on) all have access to the transmission medium at the same time. The result is that only one device can send information at a time. Given this limitation, two viable solutions exist:

- **Use a sharing mechanism:** If all end stations are forced to share a common wire, rules must exist to ensure that each end station waits its turn before transmitting. In the event of simultaneous transmissions, rules must exist for retransmitting.
- **Divide the shared segments, and insulate them:** Another solution to the limitations of shared resources is to use devices that reduce the number of end stations sharing a resource at any given time.

Ethernet Collisions

In a traditional LAN, several users would all share the same port on a network device and would compete for resources (bandwidth). The main limitation of such a setup is that only one device can transmit at a time. Segments that share resources in this manner are called collision domains, because if two or more devices transmit at the same time, the information "collides," and both end points must resend their information (at different times). Typically the devices both wait a random amount of time before attempting to retransmit.

This method works well for a small number of users on a segment, each having relatively low bandwidth requirements. As the number of users increases, the efficiency of collision domains decreases sharply, to the point where overhead traffic (management and control) clogs the network.

Smaller Segments

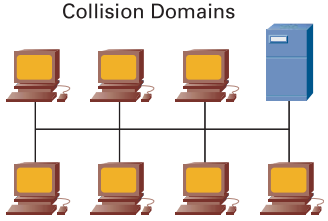
Segments can be divided to reduce the number of users and increase the bandwidth available to each user in the segment. Each new segment created results in a new collision domain. Traffic from one segment or collision domain does not interfere with other segments, thereby increasing the available bandwidth of each segment. In the following figure, each segment has greater bandwidth, but all segments are still on a common backbone and must share the available bandwidth. This approach works best when care is taken to make sure that the largest users of bandwidth are placed in separate segments.

There are a few basic methods for segmenting an Ethernet LAN into more collision domains:

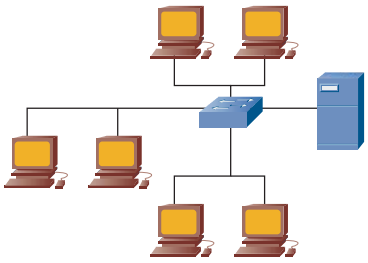
- Use bridges to split collision domains.
- Use switches to provide dedicated domains to each host.
- Use routers to route traffic between domains (and to not route traffic that does not matter to the other domain).

This sheet discusses segmenting using bridges and routers (switching is covered in the next chapter).

Single Segment, Multiple Collision Domains



Multiple Segments, Multiple Collision Domains



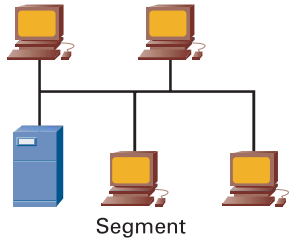
At-a-Glance: Ethernet

Increasing Bandwidth

In addition to creating additional segments to increase available bandwidth, you can use a faster medium such as optical fiber or Gigabit Ethernet. Although these technologies are faster, they are still shared media, so collision domains will still exist and will eventually experience the same problems as slower media.

Ethernet Segments

A segment is the simplest form of network, in which all devices are directly connected. In this type of arrangement, if any of the computers gets disconnected, or if one is added, the segment is disabled.

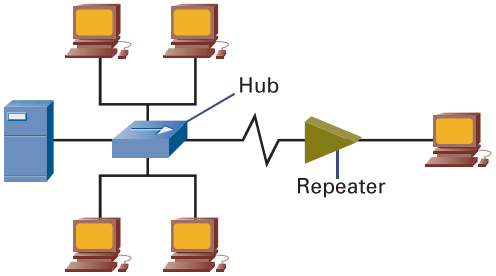


Hubs

Hubs enable you to add and remove computers without disabling the network, but they do not create additional collision domains.

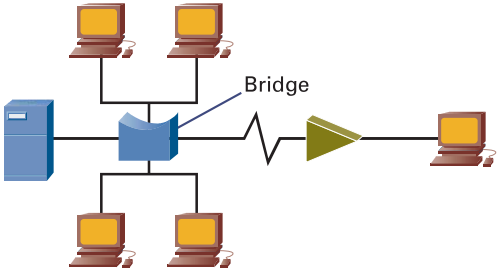
Repeaters

Repeaters simply extend the transmission distance of an Ethernet segment.



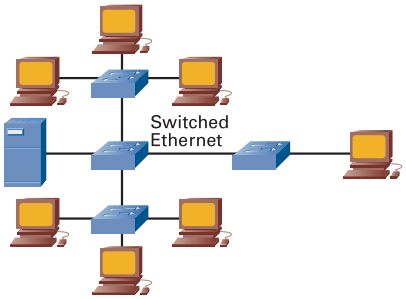
Bridges

Bridges are simple Layer 2 devices that create new segments, resulting in fewer collisions. Bridges must learn the addresses of the computers on each segment to avoid forwarding traffic to the wrong port. Unlike hubs, which are usually used for networks with a small number of end stations (4 to 8), bridges can handle much larger networks with dozens of end stations.



Switched Ethernet

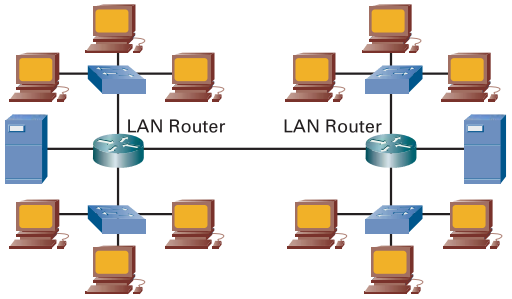
A LAN switch can be thought of as a high-speed, multiport bridge with a brain. Switches don't just allow each end station to have a dedicated port (meaning that no collisions occur). They also allow end stations to transmit and receive at the same time (using full duplex), greatly increasing the LAN's efficiency.



LAN Routers

LAN-based routers greatly extend the speed, distance, and intelligence of Ethernet LANs. Routers also allow traffic to be sent along multiple paths.

Routers, however, require a common protocol between the router and end stations.



At-a-Glance: Ethernet

What They Gave Away

In the 1970s Xerox Corporation assembled a group of talented researchers to investigate new technologies. The new group was located in the newly opened Palo Alto Research Center (PARC), well away from the corporate headquarters in Connecticut.

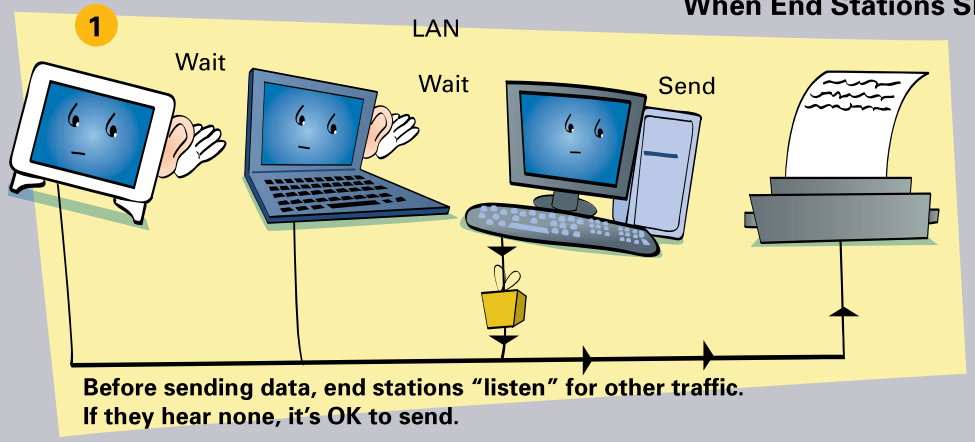
In addition to developing Ethernet, the brilliant folks at the PARC invented the technology for what eventually became the personal computer (PC), the graphical user interface (GUI), laser printing, and very-large-scale integration (VLSI).

Inexplicably, Xerox Corporation failed to recognize the brilliance (and commercial viability) of many of these homegrown innovations and let them walk out the door.

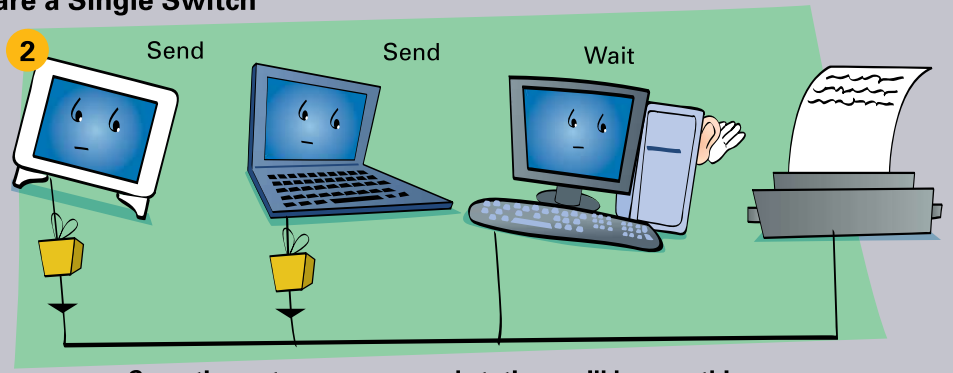
To give you an idea of what this cost Xerox in terms of opportunity, the worldwide budget for Ethernet equipment was more than $7 billion in 2006 and was expected to grow to more than $10 billion by 2009. Just imagine if a single company owned the assets of Apple, Intel, Cisco, HP, and Microsoft. There almost was such a company. Its name is Xerox.

Reducing Collisions on Ethernet

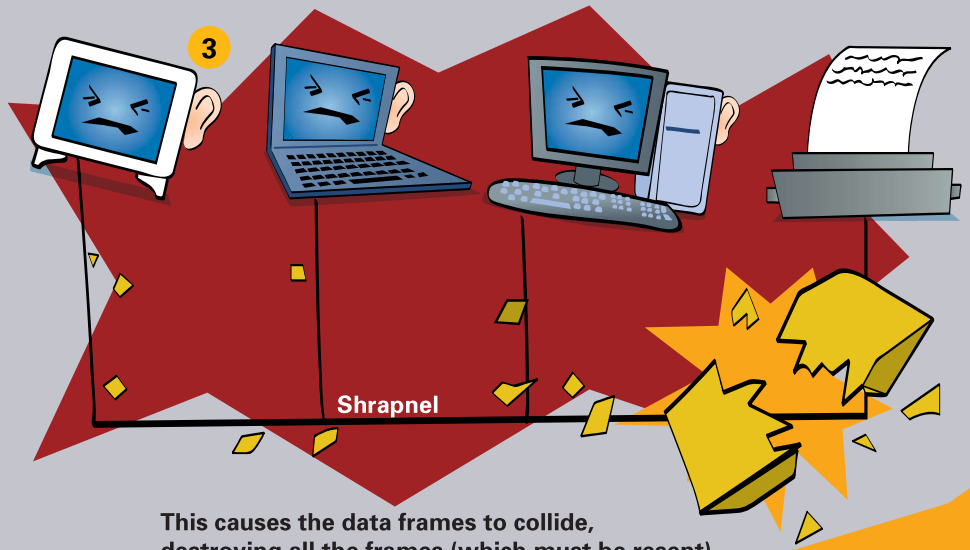
When End Stations Share a Single Switch



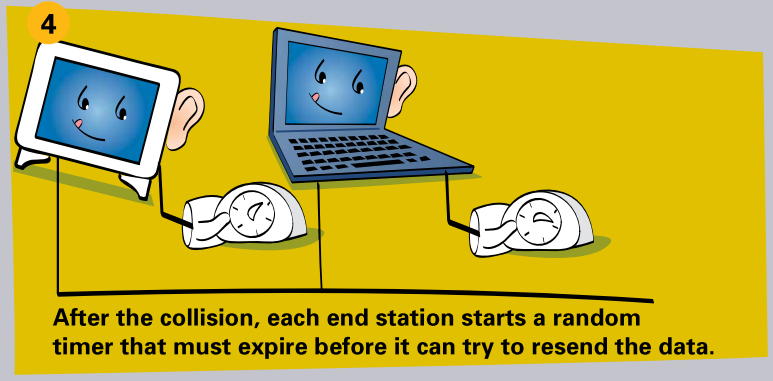
Before sending data, end stations "listen" for other traffic. If they hear none, it's OK to send.



Sometimes, two or more end stations will hear nothing and send data simultaneously.



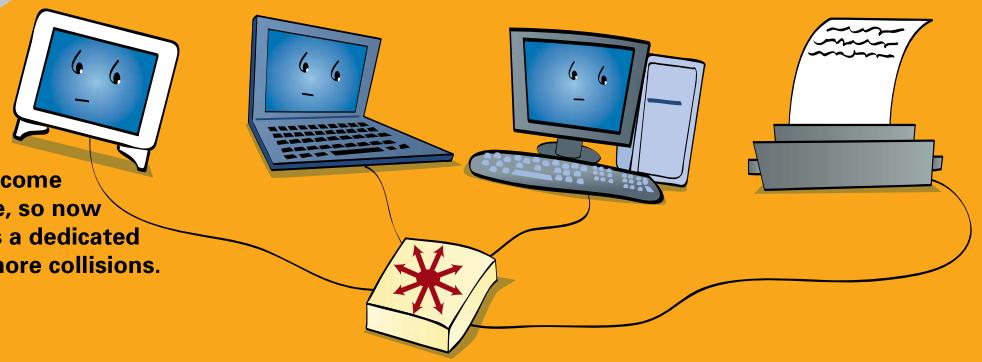
This causes the data frames to collide, destroying all the frames (which must be resent).



After the collision, each end station starts a random timer that must expire before it can try to resend the data.

The Switch Port Option

Switch ports have become relatively inexpensive, so now each end station gets a dedicated port. The result: no more collisions.



Fast Computers Need Faster Networks

The PC emerged as the most common desktop computer in the 1980s. LANs emerged as a way to network PCs in a common location. Networking technologies such as Token Ring and Ethernet allowed users to share resources such as printers and exchange files with each other. As originally defined, Ethernet and Token Ring provided network access to multiple devices on the same network segment or ring. These LAN technologies have inherent limitations as to how many devices can connect to a single segment, as well as the physical distance between computers. Desktop computers got faster, the number of computers grew, operating systems began *multitasking* (allowing multiple tasks to operate at the same time), and applications became more network-centric. All these advancements resulted in congestion on LANs.

To address these issues, two device types emerged: repeaters and bridges. *Repeaters* are simple Open Systems Interconnection (OSI) Layer 1 devices that allow networks to extend beyond their defined physical distances (which were limited to about 150 feet without the use of a repeater).

Bridges are OSI Layer 2 devices that physically split a segment into two and reduce the amount of traffic on either side of the bridge. This setup allows more devices to connect to the LAN and reduces congestion. LAN switches emerged as a natural extension of bridging, revolutionizing the concept of local-area networking.

Switching Basics: It's a Bridge

Network devices have one primary purpose: to pass network traffic from one segment to another. (There are exceptions, of course, such as network analyzers, which inspect traffic as it goes by.) With devices that independently make forwarding decisions, traffic can travel from its source to the destination. The higher up the OSI model a device operates, the deeper it looks into a packet to make a forwarding decision. Railroad-switching stations provide a similar example. The switches enable a train to enter the appropriate tracks (path) that take it to its final destination. If the switches are set wrong, a train can end up traveling to the wrong destination or traveling in a circle.

Switching technology emerged as the replacement for bridging. Switches provide all the features of traditional bridging and more. Compared to bridges, switches provide superior throughput performance, higher port density, and lower per-port cost.

The different types of bridging include the following:

- Transparent bridging primarily occurs in Ethernet networks.
- Source-route bridging occurs in Token Ring networks.
- Translational bridging occurs between different media. For example, a translational bridge might connect a Token Ring network to an Ethernet network.

Bridging and switching occur at the data link layer (Layer 2 in the OSI model), which means that bridges control data flow, provide transmission error handling, and enable access to physical media. Basic bridging is not complicated: A bridge or switch analyzes an incoming frame, determines where to forward the frame based on the packet's header information (which contains information on the source and destination addresses), and forwards the frame toward its destination. With transparent bridging, forwarding decisions happen one hop (or network segment) at a time. With source-route bridging, the frame contains a predetermined path to the destination.

Bridges and switches divide networks into smaller, self-contained units. Because only a portion of the traffic is forwarded, bridging reduces the overall traffic that devices see on each connected network. The bridge acts as a kind of firewall in that it prevents frame-level errors from propagating from one segment to another. Bridges also accommodate communication among more devices than are supported on a single segment or ring.

Bridges and switches essentially extend the effective length of a LAN, permitting more workstations to communicate with each other within a single broadcast domain. The primary difference between switches and bridges is that bridges segment a LAN into a few smaller segments. Switches, through their increased port density and speed, permit segmentation on a much larger scale. Modern-day switches used in corporate networks have hundreds of ports per chassis (unlike the four-port box connected to your cable modem).

Additionally, modern-day switches interconnect LAN segments operating at different speeds.

Switching describes technologies that are an extension of traditional bridges. Switches connect two or more LAN segments and make forwarding decisions about whether to transmit packets from one segment to another. When a frame arrives, the switch inspects the destination and source Media Access Control (MAC) addresses in the packet. (This is an example of *store-and-forward switching*.) The switch places an entry in a table indicating that the source MAC address is located off the switch interface on which the packet arrived. The bridge then consults the same table for an entry for the destination MAC address. If it has an entry for the destination MAC address, and the entry indicates that the MAC address is located on a different port from which the packet was received, the switch forwards the frame to the specified port.

If the switch table indicates that the destination MAC address is located on the same interface on which the frame was just received, the bridge does not forward the frame. Why send it back onto the network segment from which it came? This decision is where a switch reduces network congestion. Finally, if the destination MAC address is not in the switch's table, this indicates that the switch has not yet seen a frame destined for this MAC address. In this case, the switch then forwards the frames out all other ports (called *flooding*) except the one on which the packet was received.

At their core, switches are multiport bridges. However, switches have radically matured into intelligent devices, replacing both bridges and hubs. Switches not only reduce traffic through the use of bridge tables, but also offer new functionality that supports high-speed connections, virtual LANs, and even traditional routing.

Switching Ethernets

As switch Ethernet ports became less expensive, switches replaced hubs in the wiring closet. Initially, when switches were introduced, network administrators plugged hubs (containing multiple hosts) into switch ports. But eventually, it became cost-effective to plug the hosts directly into a switch port. This arrangement gives each host its own dedicated Ethernet and removes the possibility of collisions. Because a dedicated switch connection has only two devices (the switch and the host), you can configure an Ethernet switch port as *full duplex*. This means that a device can receive incoming traffic and transmit traffic simultaneously. End stations have considerably more bandwidth when they use switches. Ethernet can run at multiple speeds: 10 Mbps, 100 Mbps, 1 Gbps, and 10 Gbps. Therefore, switches can provide connectivity at these speeds. However, network applications and the web create considerably more network traffic, reintroducing new congestion problems. Switches can use quality of service (QoS) and other mechanisms to help solve the congestion issue.

Switches Take Over the World

As switches established themselves in networks, vendors added increasing functionality. Modern switches can perform forwarding decisions based on Layer 3 routing, as well as on Layer 4 and above. Even though switches can perform the functions of other higher-layer devices such as routers and content switches, you still must separate these functionalities to avoid single points of failure. Switches are the workhorse of networks, providing functionality across almost all layers of the OSI model reliably and quickly. Switches can also provide power to devices such as IP-based phones using the same Ethernet connection. Again, this applies to very large switches serving corporate networks rather than the switches in a small office or home.

At-a-Glance: Switching

Why Should I Care About Switching?

Advances in switching technology combined with a decrease in switch prices have made computer networks a common and increasingly important aspect of business today.

What Problems Need to Be Solved?

- **MAC address learning:** Switches must learn about the network to make intelligent decisions. Because of the size and changing nature of networks, switches have learned how to discover network addresses and keep track of network changes. Switches do this by finding the address information contained in the frames flowing through the network, and they maintain private tables with that information.
- **Forwarding and filtering:** Switches must decide what to do with traffic. These decisions are based on the switch's knowledge of the network.
- **Segmenting end stations:** Switches must also have mechanisms for segregating users into logical groupings (virtual LANs [VLAN] or broadcast domains) to allow efficient provisioning of service.

Broadcast and Collision Domains

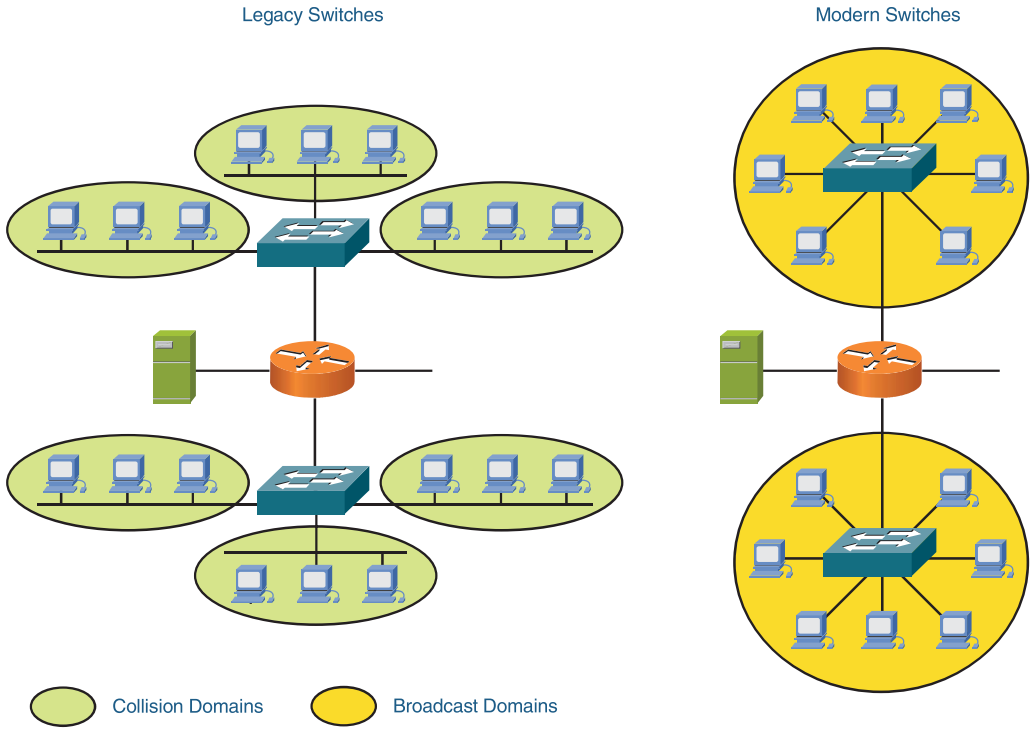
From time to time, a device on the network will want to communicate with all other "local" devices at the same time. Typically, this occurs when a device wants to query the network for an IP address, when a device is newly added to a network, or when a change occurs in the network.

A group of devices that receive all broadcast messages from members of that group is called a broadcast domain. Network broadcast domains typically are segmented with Layer 3 devices (routers).

Think of a broadcast domain as like standing in your yard and yelling as loudly as you can. The neighbors who hear you are within your broadcast domain.

Forwarding and Filtering

From a network efficiency standpoint, it is easy to see that it is much better for the network when the switch knows all the addresses on every port. However, it is not always practical to enter this information manually. As the network grows and changes are made, it becomes almost impossible to keep up.



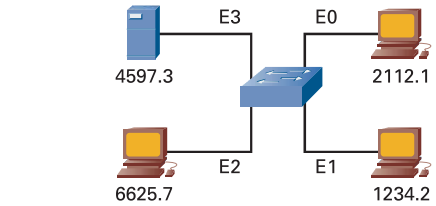
At-a-Glance: Switching

A switch always does something when it receives traffic. The preference is to send the traffic out a specific port (called filtering), but this works only when the location of the intended destination is known. When the destination address is unknown, the switch forwards the traffic out every port, except the one on which the traffic was received. This process is called flooding. Think of this as a guy calling every number in the phone book because he lost a woman's number from the night before.

Address Learning

A switch must learn the addresses of the devices attached to it. First it inspects the source address of all the traffic sent through it. Then it associates the port the traffic was received on with the MAC address listed. The following example illustrates this concept. The MAC addresses are not in the correct format and are shown for clarity only:

- **Time 0:** The switch shown has an empty MAC address table.
- **Time 1:** The device attached to port 2 sends a message intended for the device on port 0. This kicks off two actions within the switch. First, the switch now knows the address associated with the device on port 2, so it enters the information into its table. Second, because it does not have an association for the device the traffic is intended for (the computer on port 0), the switch floods the message out all ports except the one on which it was received.



Time 0

Port	Address

Time 1

Port	Address
E2	6625.7

Time 2

Port	Address
E2	6625.7
E0	2112.1

- **Time 2:** The device on port 0 replies to the message. The switch associates the source address of the message with port 0.

Any future communications involving either of these end stations will not require these steps, because the switch now knows which ports they are associated with.

This process happens all the time in every switch. For most switches, when a table entry has reached a certain "age" and has not been referenced in a while, it can be removed. This process is called *aging out*.

Frame Transmission Modes

Switches typically are Layer 2 devices (some switches now perform Layer 3 and higher functions). According to the OSI model, the data unit processed by a switch is called a frame. Switches must balance speed and accuracy (no errors) when processing frames, because typically they are measured on both attributes.

The three primary frame switching modes are as follows:

- **Cut-through:** Also known as fast-forward. The switch checks only the destination address and immediately begins forwarding the frame. This can decrease latency but also can transmit frames containing errors.
- **Store-and-forward:** The switch waits to receive the entire frame before forwarding. The entire frame is read, and a cyclic redundancy check (CRC) is performed. If the CRC is bad, the frame is discarded. Although this method increases latency (processing time), it also tends to minimize errors.
- **Fragment-free (modified cut-through):** The switch reads the first 64 bytes before forwarding the frame. 64 bytes is the minimum number of bytes necessary to detect and filter out collision frames.

At-a-Glance: Switching

Virtual LANs (VLAN)

VLANs provide the means to logically group several end stations with common sets of requirements. VLANs are independent of physical locations, meaning that two end stations connected to different switches on different floors can belong to the same VLAN. Typically the logical grouping follows workgroup functions such as engineering or finance, but this can be customized.

With VLANS it is much easier to assign access rules and provision services to groups of users regardless of their physical location. For example, using VLANs you can give all members of a project team access to project files by virtue of their VLAN membership. This ability also makes it easier to add or delete users without rerunning cables or changing network addresses.

VLANs also create their own broadcast domains without the addition of Layer 3 devices.