Ethernet

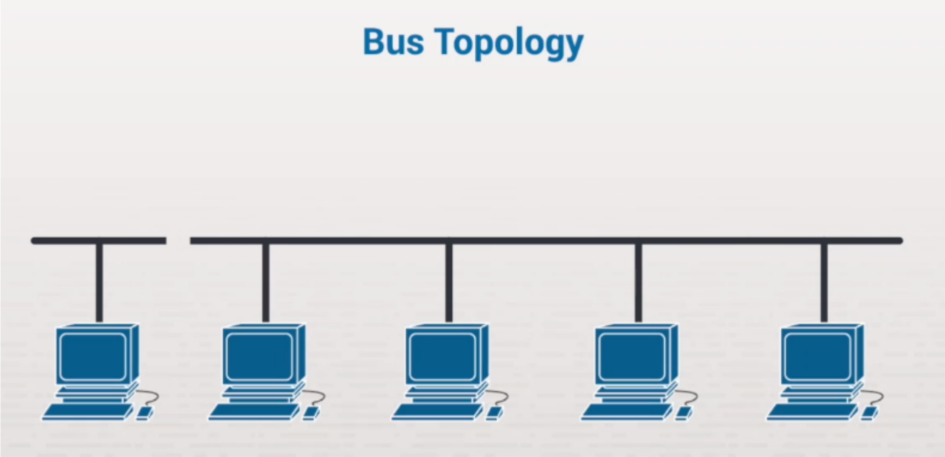
Network Topologies

Ethernet topologies determine a network's physical layout. The network topology determines how devices are connected, the cabling system's layout, and which device types are used to connect systems.

Bus Topology

The bus topology is made up of one long piece of cable, which is often called a trunk. Devices hang directly from it. Workstations and a trunk could be hundreds of meters long when they're connected together.

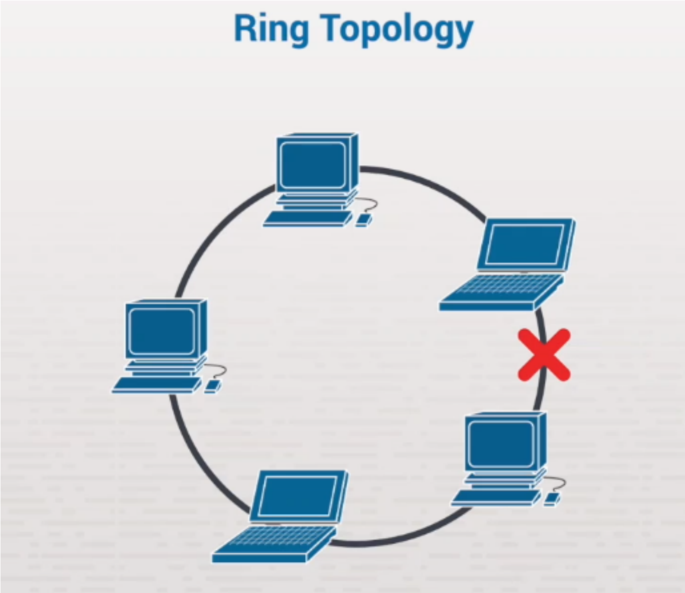
The problem with the linear topology is that there's a single point of failure. The entire trunk could fail if anything goes wrong from one end to the other. For example, if the cable breaks, then the entire trunk and all devices connected to it can no longer communicate.



Ring Topology

The next topology is called the ring topology. A ring means that you have different devices hooked together in a ring fashion. Data typically travels in a single direction around the ring, which indicates that you have a single point of failure.

You could see the ring topology in certain network environments. Certain local area network deployments, or LAN deployments, use it. But in the LAN switching environment, the star topology is still the most prevalent.

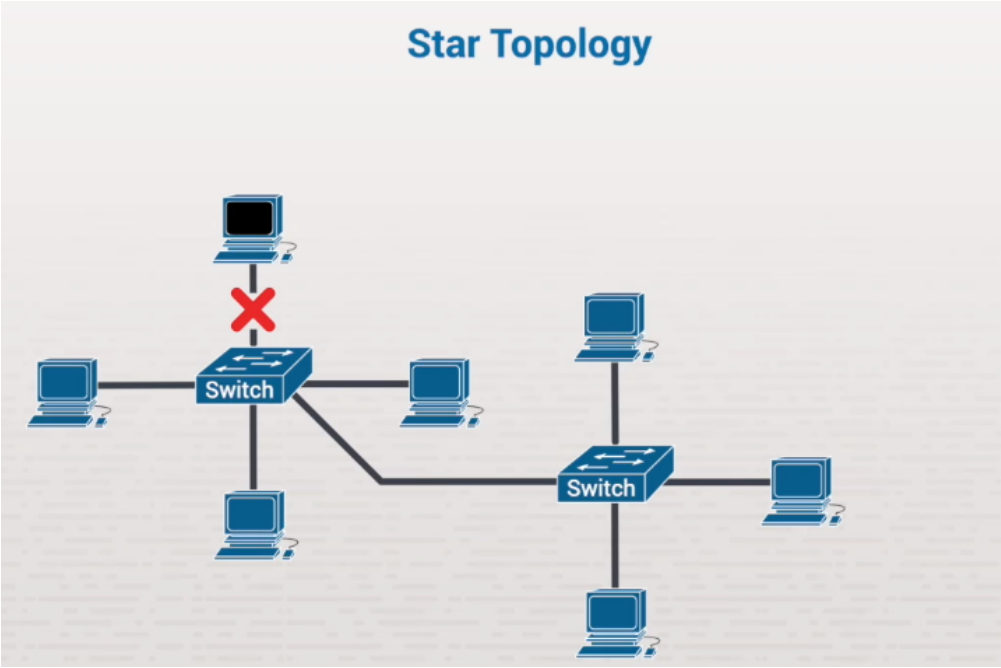


Star Topology

A star topology has a device in the middle, like a hub or a switch. Workstations are located off that device. You could daisy chain these devices to expand your network.

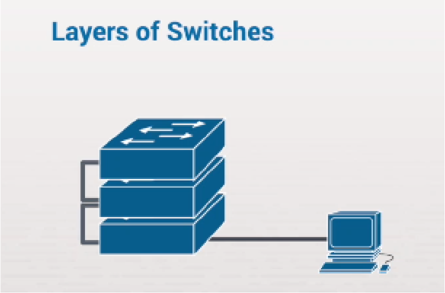
The primary benefit of the star topology is that if you lose one piece of cable, or segment, it only affects the device that's connected to that segment. But if you lose a switch, you'd lose all the devices connected to it. Even then, there's no single point of failure, like the bus topology.

The star topology is also easier to expand. You simply add another switch if you need more port density. You don't have to take the network down to do this; just add another device. Then you have as many extra ports as you need.

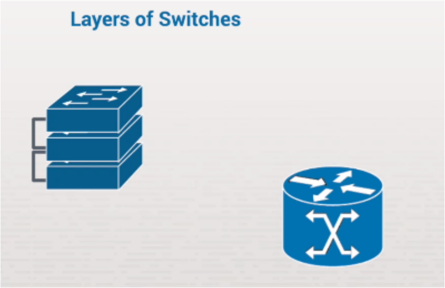


Layers of Switches

Today's Ethernet systems use a star topology. The device in the middle connects all workstations. There could be just a couple of ports, or as many as 48. It could have multiple switches stacked together. This way, they're all managed as a single switch, and the end stations connect to the network on these devices.



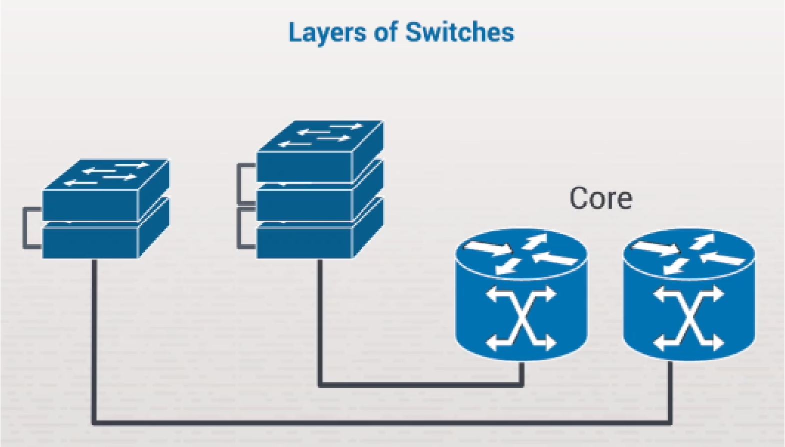
There are also chassis-based switches. A chassis-based switch is a box that has supervisors. This means they have redundant power supplies and CPUs. In the Cisco world, this is commonly how the box is maintained and managed.



You can put as many blades, or line cards, as needed to provide the port density required. Using chassis-based switches, you can create a switch that has several hundred network ports.

You also commonly see Ethernet networks with different layers of switching. In a secure data center, you may use one or more chassis-based switches as your core switches.

Then you have fiber connections coming out from those switches that go to different buildings or different floors. They'll connect to switches like these switch stacks, or even smaller ones. In this case, you don't need one massive switch that provides connectivity for every endpoint in your campus. Users can connect to access switches on individual buildings or floors.

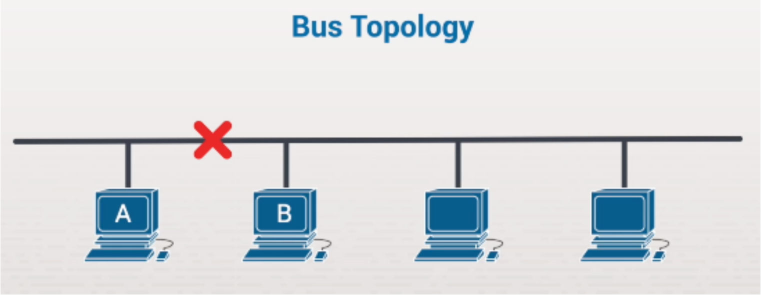


This is how Ethernet networks are typically built: with a dual-layer approach. The connectivity is divided between large chassis-based switches in a protective data center, and fiber distribution where users are.

Network Access (CSMA/Cx)

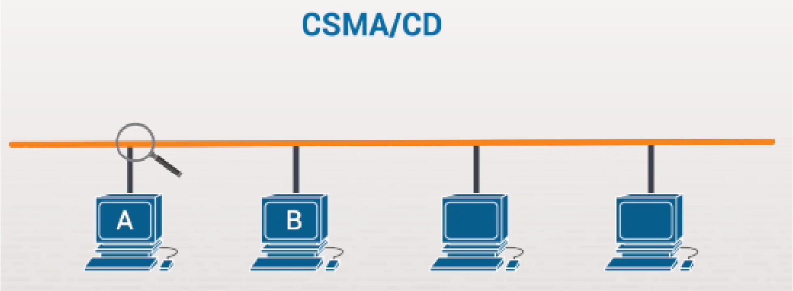
How Ethernet systems determine network access - bus topology example

In a bus topology, there's one long piece of cable called a trunk that all devices connect to. The main issue with this topology is that a single point of failure in this trunk, such as a break here, would take down the entire thing. No workstations could communicate. This is one of the reasons star topology became popular.



Network Access

Ethernet uses a technology called Carrier Sense Multiple Access/Collision Detection, or CSMA/CD. When a node on a network has something to send, it first senses the carrier. That means that it checks the trunk to see if there's any other transmission going on from another node. Even if the workstation has already packaged up the data and inserted it in a frame, it waits to send the bits out.



In this topology, when data is sent, it occupies the entire trunk for a period of time. If this workstation senses that no other signaling is present, then it assumes that the entire trunk is free of data and releases the bits.

The frame is sent out on this trunk in both directions as a series of bits. That's why it occupies the entire trunk length with its signaling. In this way, every workstation connected to that trunk receives the frame and sees if it was intended for itself. The node that the frame was intended for receives the frame, de-encapsulates the packet, and operates on the data.

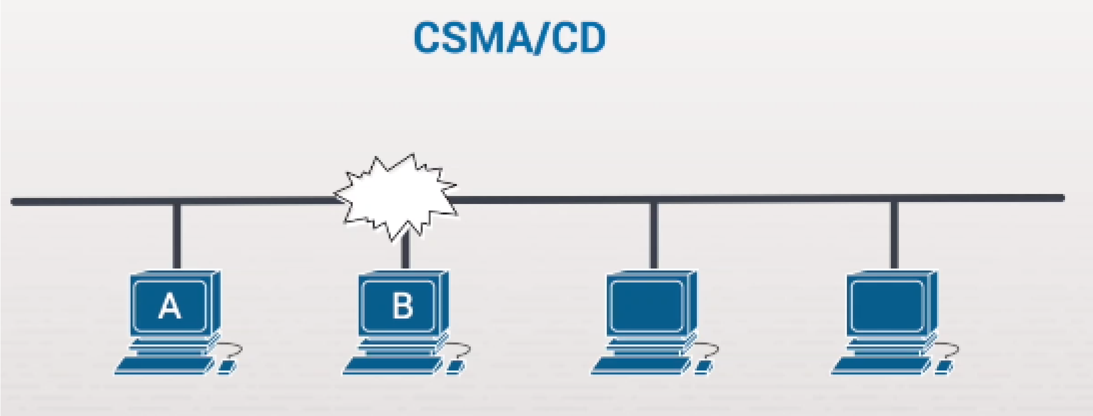
Critical Concept of CSMA/CD

This is the first critical concept of CSMA/CD: workstations can't send data whenever they want to. First, they have to check if the network's free. When it does send, other workstations can't transmit at the same time; that would cause a collision.

CSMA/CD is a multiple access technology, which means that A and B both sense the media to see if there's an existing transmission going on. If they sense the media at the same time, they'll both see it as free. So then both Workstations A and B send their signal out in the shared media, which makes the two signals collide. When you have more than one station trying to send data within a common collision domain, the two signals collide and are destroyed. None of the data gets to where it was supposed to go in this scenario.

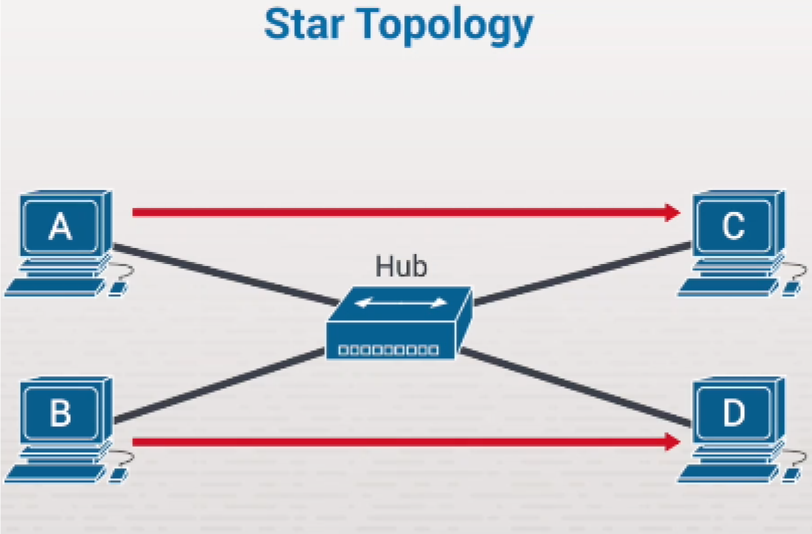
To prevent collisions, there's collision detection, or CD. This means that the Ethernet cards in both A and B have the power to realize that there was a collision that caused excess voltage on the wire. They know their signal didn't go through, so now they need to resend it. Both systems wait a random period of time and then attempt to retransmit. The waiting period is different lengths of time so that the same thing doesn't happen again.

After the waiting period is over, let's say Network A transmits earlier, and its signal gets through and is removed. Then Network B can transmit freely. It's important to understand this because in a shared linear trunk, all the workstations share a common collision domain. Two systems that try to talk at the same time will absolutely collide.



Star Topology

Now let's see how this process works on a star topology. Let's say there's a hub and several nodes connected to it. Node A is trying to talk to Node C, and Node B is trying to talk to Node D.

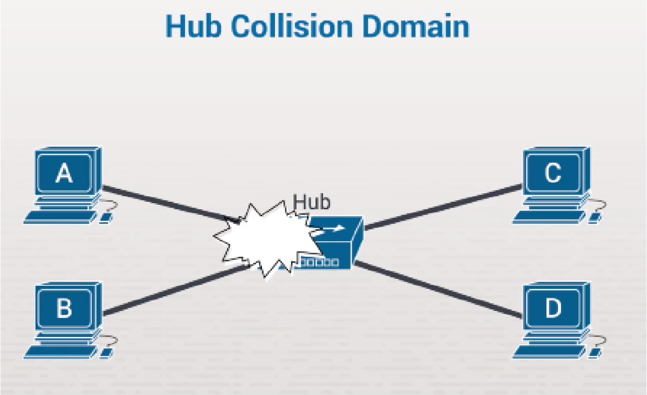


At first glance, it doesn't seem like these communications could affect each other because the path between A and C doesn't involve the ports that B and D require.

But that's not the case. In a hub-based environment, the hub is a physical layer device that repeats signaling. It sees electricity coming in and repeats those bits out to all ports. A hub is, essentially, a star topology version of the linear topology. Even though A's frame signaling is intended for C, the hub doesn't see it that way. It only sees a string of incoming bits. So the hub, being a dumb machine, repeats those bits to all connected ports.

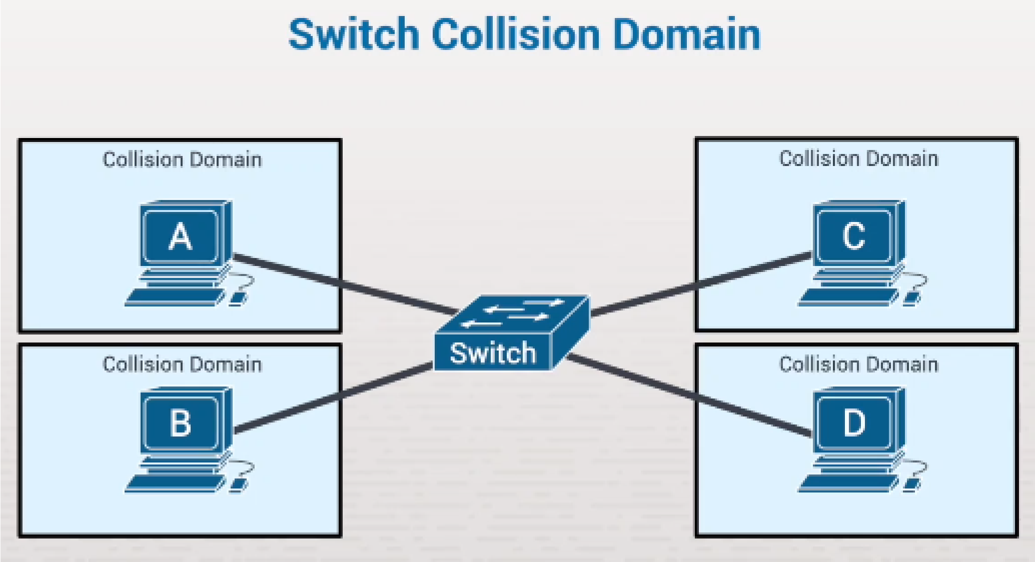
Hub Collision Domain

Even though a hub can be used for a star topology, it replicates all data to all ports, so there will be collisions. While a hub star topology is better than a linear topology (in that there isn't a single point of failure for the cabling), it still has the problem of a single shared-collision domain. **This is one of the primary advantages switches have over hubs.**



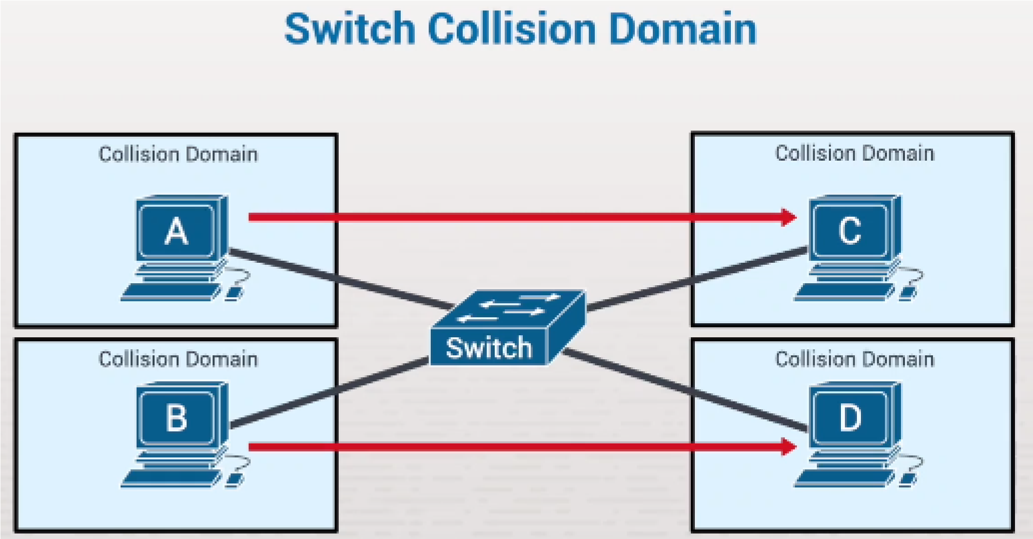
Switch Collision Domains

If I replace that hub with a switch, every connection into the switch is a separate collision domain.



This is good because when A tries to reach C, the switch not only receives the data, it knows that this data is intended only for C. It won't send the data down here, to B or D; only out the port leading to C.

This allows A to talk to C at the same time as B is talking to D, all through the same switch and without collisions. Because the switch defines every connected port as a separate collision domain, each switch knows exactly where an incoming frame is addressed to.



Unicast Traffic: What I just described is unicast traffic. Workstation A puts Workstation C's Media Access Control address, or MAC address, directly in the frame header. Workstation B does the same with Workstation D. Again, the switch knows exactly what to do.

There are different types of transmissions. A broadcast frame is addressed to all nodes, and the switch sends the broadcast frame to every active port on the switch (like a hub would). The difference is that the hub copies bits to all ports. A switch, in contrast, replicates frames that have the broadcast and, by default, multicast addresses in the frame header to all ports. So, this ability to send concurrent traffic streams—A to C, B to D—is only valid when sending unicast frames. It doesn't apply to either broadcast or multicast frames.

The CSMA process works the same way in wireless Ethernet networks, although in wireless, we use collision avoidance technology instead of collision detection.

How CSMA/CD is used to access Ethernet Systems

The primary characteristics of CSMA/CD allow nodes to determine if it's safe to transmit. Two nodes can send data at the same time, but if it's a single collision domain, both signals are destroyed. If a collision happens, the collision detection circuitry on the Ethernet cards recognizes it and waits a random period of time before retransmitting the data.

When a collision occurs on an Ethernet network:

1. The device that detected the collision transmits a jam signal.
2. All devices wait a random period of time before attempting to retransmit.
3. After the time interval has expired, a device will listen to the transmission medium, then transmit if it is free.

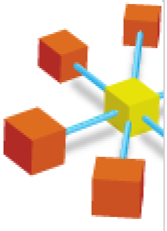
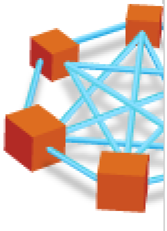
Collision avoidance uses Request to send/clear to send (RTS/CTS) messages to determine when to use the transmission medium.

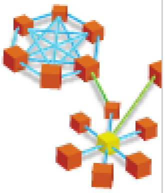
Ethernet Architecture Facts

The *physical topology* is the mapping of the nodes of a network and the physical connections between them. These physical connections include the layout of wiring, cables, node locations, and the interconnections between the nodes and the cabling or wiring system.

Network Topologies

The logical network topology is the way messages are sent through network connections. Ethernet supports the following topologies:

Topology	Description
 Star	A star topology uses a hub or switch to connect all network connections to a single physical location. Today it is the most popular type of topology for a LAN. With a star: • All network connections are located in a single place. This makes it easy to troubleshoot and reconfigure. • Nodes can be added to or removed from the network easily. • Cabling problems usually affect only one node.
 Mesh	A mesh topology exists when there are multiple paths between any two nodes on a network. Mesh topologies are created using point-to-point connections. This increases the network's fault tolerance because an alternate path can be used when one path fails. Two variations of mesh topologies exist: • Partial Mesh: some redundant paths exist. • Full Mesh: every node has a point-to-point connection with every other node. Full mesh topologies are usually impractical in a standard LAN, because the number of connections increases dramatically with every new node added to the network. A separate network interface and cable for each host on the network is required. However, a full mesh topology is commonly used to interconnect routers. It provides alternate paths should one path go down or become overloaded. Mesh networks are also commonly used to create redundant paths between access points in a wireless network. They provide alternate paths back to the wireless controller should one access point go down or become overloaded. With this topology, every access point can communicate directly with every other access point on the wireless network.

 Hybrid	A hybrid topology exists when two or more types of network topologies are connected with each other. For example, a network of wireless access points (mesh topology) connected to a network switch (star topology) would be considered a hybrid topology.

Ethernet Network Architecture

Ethernet networks use the following architecture components:

<table>
<tr><th>Specification</th><th>Description</th></tr>
<tr><td>Media access</td><td>Ethernet uses Carrier Sense Multiple Access/Collision Detection (CSMA/CD) to control access to the transmission medium. Devices use the following process to send data:
<ol>
<li>Because all devices have equal access to the transmission media (multiple access), a device with data to send, first listens to the transmission medium to determine if it is free (carrier sense).</li>
<li>If it is not free, the device waits a random time and listens again to the transmission medium. When it is free, the device transmits its message.</li>
<li>If two devices transmit at the same time, a collision occurs. The sending devices detect the collision (collision detection) and send a jam signal.</li>
<li>Both devices wait a random length of time before attempting to resend the original message. The process of waiting before attempting to resend is called a <i>backoff</i>.</li>
</ol></td></tr>
<tr><td>Transmission media</td><td>Ethernet supports the following cable types:
● Unshielded twisted-pair cables (UTP) with RJ-45 connectors. This is the most common transmission medium used for Ethernet. Each cable consists of eight wires twisted into four pairs. UTP cables are classified by the following types (called categories):
<table>
<tr><th>Type</th><th>Speed</th></tr>
<tr><td>Cat5</td><td>100 Mbps</td></tr>
</table></td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td>Cat5e</td><td>1000 Mbps</td></tr>
<tr><td>Cat6</td><td>10 Gbps</td></tr>
</table>
<ul>
<li>Fiber optic is most commonly used in high-speed applications, e.g., servers or streaming media. Fiber optic cables have ST, SC, LC, and MT-RJ connectors.</li>
</ul>
</td></tr>
<tr><td>Frame type</td><td>
The Ethernet frame size is 64 to 1518 bytes This is the same for all Ethernet standards. The most common frame types are:
<ul>
<li>Ethernet 802.3 is the original Ethernet frame type.</li>
<li>Ethernet 802.2 is the frame type that accommodates standards set by the IEEE 802.2 committee related to the logical link control (LLC) sublayer. It is a more current frame type than 802.3.</li>
<li>Ethernet II is a frame type that provides the ability to use TCP/IP as a transport/network layer protocol.</li>
</ul>
</td></tr>
<tr><td>Physical address</td><td>
The MAC address (also called the burned-in address) is the Data Link layer physical device address. The MAC address is:
<ul>
<li>A 12-digit hexadecimal number (each number ranges from 0-9 or A-F).</li>
<li>Often written using hyphens (e.g., 00-B0-D0-06-BC-AC), periods, (e.g., 00B0.D006.BCAC), or colons (e.g., 00:B0:D0:06:BC:AC) to separate the address parts.</li>
<li>Guaranteed unique through design. The first six digits of the MAC address is assigned to each manufacturer. The manufacturer determines the rest of the address, assigning a unique value that identifies the host address. A manufacturer that uses all the addresses in the original assignment can apply for a new MAC address assignment.</li>
</ul>
Even though it is possible to temporarily change the MAC address of a network interface card, there is little practical reason for doing so.
</td></tr>
</table>

Half and Full Duplex Facts

In the original Ethernet standards, all devices shared the same cable. This caused issues with data transmission.

The two problems caused by cabling sharing were:

- Collisions would occur when two devices transmitted at the same time. This meant that devices had to be able to detect and recover from collisions.
- Each device could either transmit data or receive data at any given time. The device was either receiving data or listening for incoming data. Devices were not able to both send and receive at the same time. This was much like using a one-lane road for traffic in two directions.

These two problems were solved as follows:

- Twisted pair cables are used to allow simultaneous transmission, Twisted pair cables combine multiple strands of wires into a single cable. It allows devices to use different wires to send and receive data simultaneously.
- Switches are used to eliminate collisions. Switches use dedicated switch ports (a single device per port) to give devices a dedicated communication path, making collisions impossible.

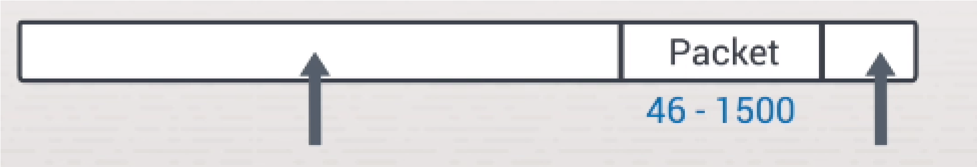
With these problems solved, collision detection can be turned off. Devices can transmit and receive data simultaneously and can begin transmitting data as soon as they have data to send. Devices with collision detection turned on operate in *half-duplex* mode; devices with collision detection turned off operate in *full-duplex* mode. The following table describes half-duplex and full-duplex modes:

Mode	Description	Bandwidth
Half-duplex	In half-duplex mode: ● Collision detection is turned on. ● The device can only send or receive at any given time. ● Devices connected to a hub must use half-duplex communication.	Up to the rated bandwidth (100 Mbps for 100BaseT, 1000 Mbps for 1000BaseT, etc.)
Full-duplex	In full-duplex mode: ● Collision detection is turned off. ● The device can send and receive at the same time. ● NICs need to be full-duplex capable. ● A switch with dedicated switch ports is required.	Double the rated bandwidth (200 Mbps for 100BaseT, 2000 Mbps for 1000BaseT, etc.)

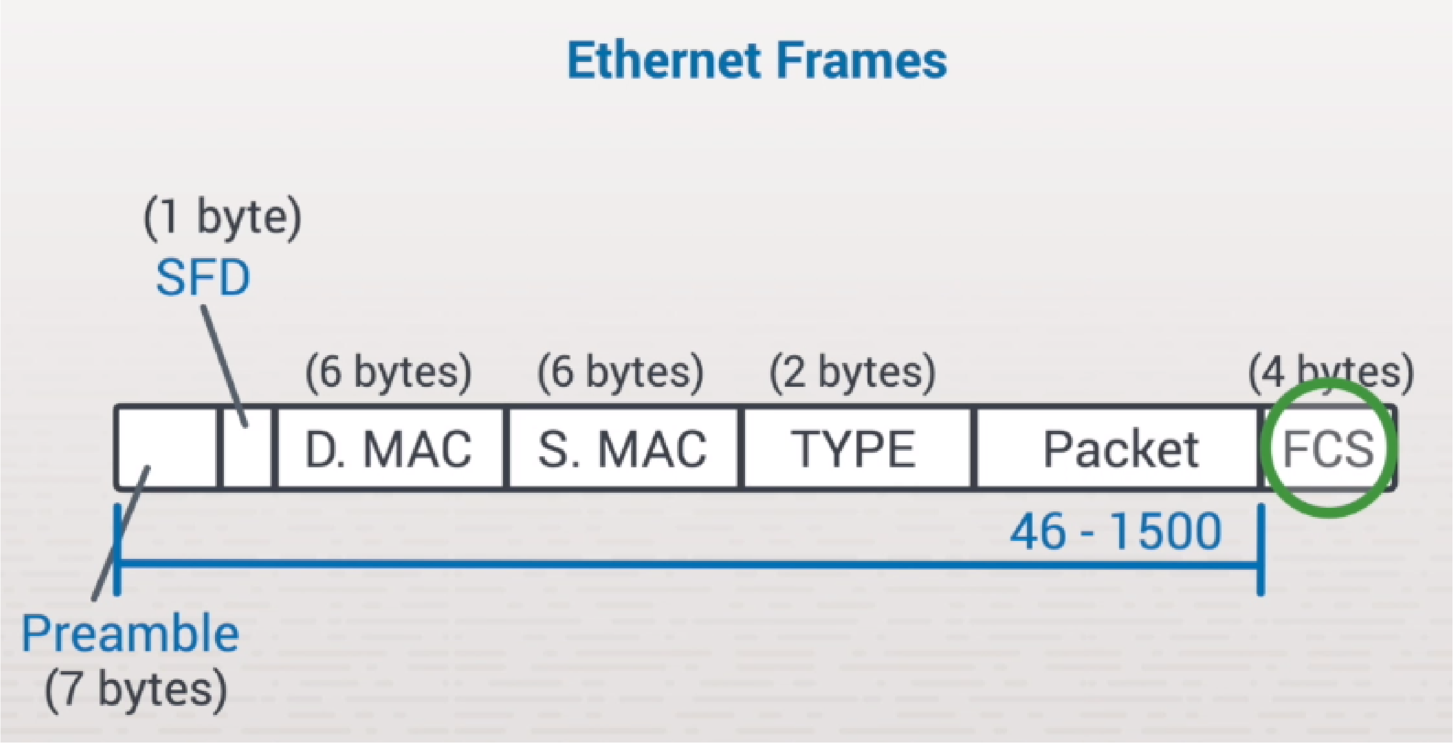
Frame Format

Frame Format
We need frames to properly envelop a packet before sending it across a network.

Packets are created at the network layer, and frames are created at the data link layer. Packets contain data sent down from the layers above it. Ethernet Frames are read from left to right. This is the packet. The purpose of the frame is to then envelop the packet and provide enough information to successfully navigate the media.



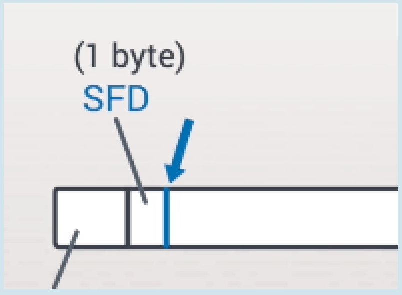
The data can be anywhere from 46 to 1,500 bytes in length, depending on what you're doing. If you're just making a web request, that might be a very small packet. The web response, or the data sent back to you, might be a full-size packet, about 1,500 bytes. Before this packet can make it onto the wire, fields are placed both in front of and behind the packet to form the frame. These fields are referred to as prepend and append.



The first field in the frame is called the preamble. The preamble is 7 bytes in length, and its purpose is to handshake. When a receiving system sees a series of bits coming in, specifically the length of 7 bytes, it detects this as an incoming frame. So, the preamble gives the receiving system a handshake that signals something like, "Get ready, here comes a data message."

SFD

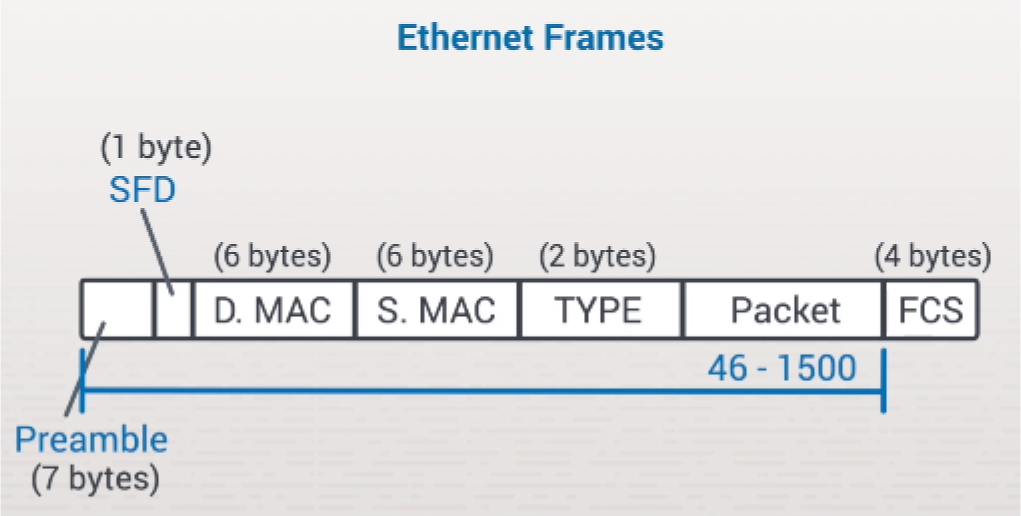
The second field is called the Start Frame Delimiter, or SFD, and it's only 1 byte. After the alternating 1s and 0s for 7 different bytes, the Start Frame Delimiter ends on two consecutive 1s.after all these alternating ones and zeros, when the system sees an 11 occur, it knows that the data begins at that point. It knows to interpret the very next bit, which is right here, as the first important field of the frame.



The next field is the destination MAC address, and this is critical. It's 6 bytes in length, and it's the MAC address of the next device the data will stop at on the network, but not necessarily the final destination.

After that, there's the source MAC address. This is the address where the frame is coming from. So, in this case, your system.

The next field is a standard Ethernet frame is the type field. This field is 2 bytes, and it simply dictates the Layer 3, or Network/Internet Layer Protocol, being used. So, the type field will have a value indicating that this is an IP packet.



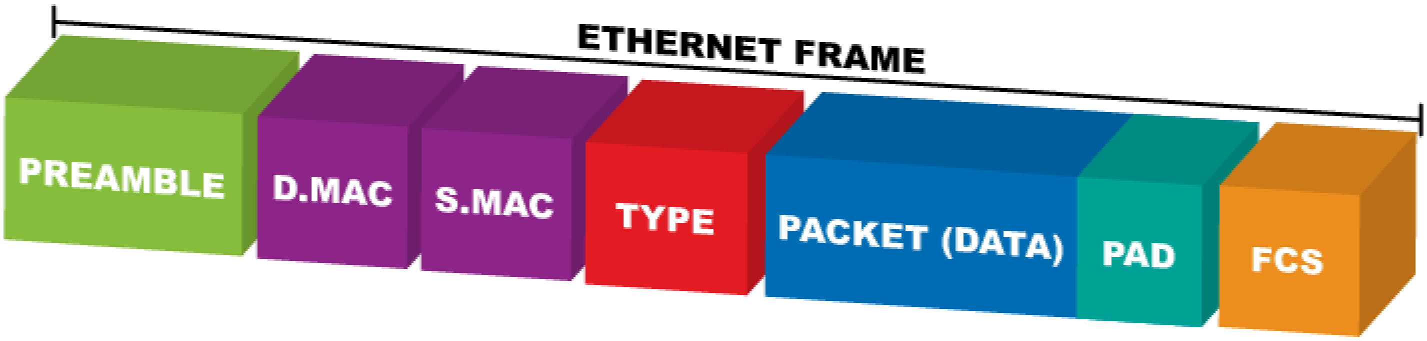
You can see that five fields are prepended to the packet, but there's one field on the end. This one's called the frame check sequence, or FCS, and it's 4 bytes long. The FCS, sometimes called a CRC, or checksum, is used for error detection. Once the entire frame has been built from the left all the way to here, a calculation is performed on all that data. Then the result is stored in this FCS field.

Its purpose is to give the receiving system a number to compare it to and confirm that all the data sent was successfully received. When the receiving system gets this frame, it receives all these fields. It performs the same calculation on all these bits, and it should come up with the exact same value as the FCS that was sent. If not, then there was an issue in the transmission of that frame.

If there is a discrepancy like this, that means the data is corrupt, and the sender will reproduce and resend the frame.

Ethernet Frame Format Facts

A frame is a unit of data that is ready to be sent on the network medium. Ethernet frames contain the following components:



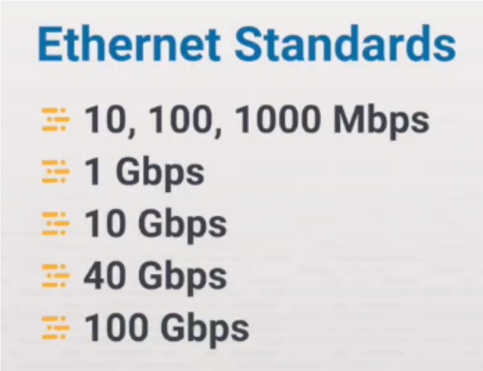
Component	Description
Preamble	The preamble is a set of alternating ones and zeros terminated by two ones (11), which mark it as a frame.
Destination address	The destination address identifies the receiving host's MAC address.
Source address	The source address identifies the sending host's MAC address.
Type	The type field is two bytes and specifies the network/internet layer protocol being used.
Packet (data)	The packet or data contains the information that needs to be transmitted from one host to the other.
Pad	Ethernet frames are sized between 64 and 1518 bytes. If the frame is smaller than 64 bytes, the sending NIC places junk data in the pad to make it the required 64 bytes.
Frame Check Sequence (FCS)	The FCS helps verify that the frame contents have arrived uncorrupted. It uses a cyclic redundancy check (CRC), which is a mathematical calculation performed on the frame.

- The preamble is a set of alternating ones and zeros terminated by two ones (11), which mark it as a frame.
- The destination address identifies the receiving host's MAC address.

- The source address identifies the sending host's MAC address.
- The type field is two bytes and specifies the Network/Internet layer protocol being used.
- The packet or data contains the information that needs to be transmitted from one host to the other.
- Ethernet frames are 64 to 1518 bytes in size. If the frame is smaller than 64 bytes, the sending NIC places junk data in the pad to make it the required 64 bytes.
- The FCS helps verify that the frame contents have arrived uncorrupted using a cyclic redundancy check (CRC), which is a mathematical calculation performed on the frame.

Ethernet Standards

In this lesson, we'll look at some of the different speeds currently available with Ethernet technologies.



Ethernet Standards

- 10, 100, 1000 Mbps
- 1 Gbps
- 10 Gbps
- 40 Gbps
- 100 Gbps

Current Segment Indicator10/100/1000 Mbps
Most switches are capable of handling 10, 100, or 1,000 megabits per second data rates. This means that the switch port can handle these speeds, depending on the device that's connected to it.

If the device you're connected to can only speak 10BASE-T, or 10 megabits per second, then the switch will obviously have to run at that speed. But, if the device can handle 100 megabits per second, then it'll automatically shift the port into operation for that speed. Most switches can auto-detect that. But if the switch doesn't support auto-negotiation, you'll have to manually set the speed to what the endpoint can support.

1 Gbps
For switching, there are ports that can offer all three speeds, and this can be done on a per port basis. I can have endpoints with different speeds that connect to different ports, all on the same switch. One thousand megabit per second Ethernet is also called 1 gigabit Ethernet, or just 1G.

10 Gbps
Some years ago, Ethernet introduced 10 gigabit, or 10G standards. You won't see this for switch ports connected to workstations because there's no 10G requirement for them. They're mostly used on ports for backbone connections, such as core switches between different floors or campuses or between different buildings.

In data centers, you often connect to servers or server farms. These could be very powerful blade server environments. In these cases, 10G connectivity or higher is very common.

40 Gbps and 100 Gbps

In the last several years, even faster standards of Ethernet have come to the market, including 40 Gig and even 100 Gig options. You typically see these technologies and the need for this type of extreme bandwidth in data center environments.

Ethernet Standards Facts

Ethernet standards are defined by the IEEE 802.3 committee. These standards define the networking characteristics for each Ethernet category. The following table compares the characteristics of the various Ethernet standards:

Category	Standard	Bandwidth	Cable Type	Maximum Segment Length
Ethernet	10BaseT	10 Mbps (half-duplex); 20 Mbps (full-duplex)	Twisted pair (Cat3, 4, or 5)	100 meters
Ethernet	10BaseFL	10 Mbps (multimode cable)	Fiber optic	1,000 to 2,000 meters
Fast Ethernet	100BaseTX	100 Mbps (half-duplex); 200 Mbps (full-duplex)	Twisted pair (Cat5 or higher), uses 2 pairs of wires	100 meters
Fast Ethernet	100BaseFX	100 Mbps	Fiber optic (multimode cable)	412 meters
Fast Ethernet	100BaseFX	100 Mbps	Fiber optic (single-mode cable)	2,000 meters
Gigabit Ethernet	1000BaseT	1,000 Mbps (half-duplex); 2,000 Mbps (full-duplex)	Twisted pair (Cat5 or higher)	100 meters

Gigabit Ethernet	1000BaseT	1000BaseCX (short copper)	Special copper (150 ohm)	25 meters, used within wiring closets
Gigabit Ethernet	1000BaseT	1000BaseSX (short)	Fiber optic	220 to 550 meters depending on cable quality
Gigabit Ethernet	1000BaseT	1000BaseLX (long)	Fiber optic	550 meters (multimode); 10 kilometers (single-mode)
10 Gigabit Ethernet	10GBaseT	10 Gbps (full-duplex only)	Twisted pair (Cat6 or 7)	100 meters
10 Gigabit Ethernet	10GBaseSR/10GBaseSW	10 Gbps (full-duplex only)	Multimode fiber optic	300 meters
10 Gigabit Ethernet	10GBaseLR/10GBaseLW	10 Gbps (full-duplex only)	Single-mode fiber optic	10 kilometers
10 Gigabit Ethernet	10GBaseER/10GBaseEW	10 Gbps (full-duplex only)	Single-mode fiber optic	40 kilometers

You should also know the following facts about Ethernet:

- The maximum cable length for UTP Ethernet T implementations is 100 meters for all standards.
- Ethernet standards support a maximum of 1024 hosts on a single subnet.

Power over Ethernet (PoE) is a networking feature defined by the IEEE 802.3af and 802.3at standards. It describes any of several standard or ad-hoc systems which pass electric power along with data on twisted pair Ethernet cabling. PoE technology is used to distribute electrical power along with network data on twisted-pair Ethernet cabling (CAT 5 or higher). Power is usually supplied by a PoE-enabled Ethernet switch.

PoE is commonly used to power network devices that are located where physical access to a power outlet may not be available. For example, a PoE-enabled surveillance camera mounted on a tall pole can be powered via its Ethernet cabling. You can use a PoE injector to add PoE capability to regular non-PoE network links. PoE injectors can be used to upgrade existing LAN installations to PoE and provide a solution where fewer PoE ports are required. To upgrade a network connection to PoE, patch it through the PoE injector. Power injection is controlled and automatic.

Gigabit Ethernet is very similar to Fast Ethernet. It uses Carrier Sense, Multiple Access/Collision Detection as the media access method. It can use both copper and fiber optic cables.