Chapter 5: Ethernet

**Ethernet Protocol:** Ethernet operates in the data link layer and the physical layer

**LLC and MAC Sublayers:**

**LLC:** The Ethernet LLC sublayer handles the communication between the upper layers and the lower layers. This is typically between the networking software and the device hardware. The LLC sublayer takes the network protocol data, which is typically an IPv4 packet, and adds control information to help deliver the packet to the destination node. The LLC is used to communicate with the upper layers of the application and transition the packet to the lower layers for delivery. The LLC can be considered the driver software for the NIC. The NIC driver is a program that interacts directly with the hardware on the NIC to pass the data between the MAC sublayer and the physical media.

**MAC:** MAC constitutes the lower sublayer of the data link layer. MAC is implemented by hardware, typically in the computer NIC.

the Ethernet MAC sublayer has two primary responsibilities:

* Data encapsulation- The data encapsulation process includes frame assembly before transmission, and frame disassembly upon reception of a frame.

Graphical user interface, application

Description automatically generated

Data encapsulation provides three primary functions:

* **Frame delimiting**: The framing process provides important delimiters that are used to identify a group of bits that make up a frame. This process provides synchronization between the transmitting and receiving nodes.
* **Addressing**: The encapsulation process also provides for data link layer addressing. Each Ethernet header added in the frame contains the physical address (MAC address) that enables a frame to be delivered to a destination node.
* **Error detection**: Each Ethernet frame contains a trailer with a cyclic redundancy check (CRC) of the frame contents. After reception of a frame, the receiving node creates a CRC to compare to the one in the frame. If these two CRC calculations match, the frame can be trusted to have been received without error.
* Media access control- Media access control is responsible for the placement of frames on the media and the removal of frames from the media. This sublayer communicates directly with the physical layer. Ethernet provides a method for controlling how the nodes share access through the use a Carrier Sense Multiple Access (CSMA) technology.

**MAC Address Structure:** A unique identifier called a MAC address was created to identify the actual source and destination nodes within an Ethernet network**.** All MAC addresses assigned to a NIC or other Ethernet device must use that vendor's assigned OUI as the first 3 bytes. (MAC address=burned-in address (BIA)). The address formats might be similar to 00-05-9A-3C-78-00

**Frame Processing:** When the computer starts up, the first thing the NIC does is copies the MAC address from ROM into RAM. When a device is forwarding a message to an Ethernet network, it attaches header information to the packet. The header information contains the source and destination MAC address. The source device sends the data through the network. Each NIC in the network views the information, at the MAC sublayer, to see if the destination MAC address in the frame matches the device’s physical MAC address stored in RAM. If there is no match, the device discards the frame. When the frame reaches the destination where the MAC of the NIC matches the destination MAC of the frame, the NIC passes the frame up the OSI layers, where the de-encapsulation process takes place.

**Ethernet Frame Attributes**

**Ethernet encapsulation:** At the data link layer, the frame structure is nearly identical for all speeds of Ethernet. The Ethernet frame structure adds headers and trailers around the Layer 3 PDU to encapsulate the message being sent.

**Ethernet Frame Size:** Both the Ethernet II and IEEE 802.3 standards define the minimum frame size as 64 bytes and the maximum as 1518 bytes. Any frame less than 64 bytes in length is considered a "collision fragment" or "runt frame" and is automatically discarded by receiving stations. If the size of a transmitted frame is less than the minimum or greater than the maximum, the receiving device drops the frame. Dropped frames are likely to be the result of collisions or other unwanted signals and are therefore considered invalid.

**Ethernet Frame:**

* **Preamble and Start Frame Delimiter Fields**: The Preamble (7 bytes) and Start Frame Delimiter (SFD), also called the Start of Frame (1 byte), fields are used for synchronization between the sending and receiving devices. These first eight bytes of the frame are used to get the attention of the receiving nodes. Essentially, the first few bytes tell the receivers to get ready to receive a new frame.
* **Destination MAC Address Field**: This 6-byte field is the identifier for the intended recipient. As you will recall, this address is used by Layer 2 to assist devices in determining if a frame is addressed to them. The address in the frame is compared to the MAC address in the device. If there is a match, the device accepts the frame.
* **Source MAC Address Field**: This 6-byte field identifies the frame's originating NIC or interface.
* **Length Field**: the Length field defines the exact length of the frame's data field. This is used later as part of the FCS to ensure that the message was received properly. Otherwise, the purpose of the field is to describe which higher-layer protocol is present. If the two-octet value is equal to or greater than 0x0600 hexadecimal or 1536 decimal, then the contents of the Data field are decoded according to the EtherType protocol indicated. Whereas if the value is equal to or less than 0x05DC hexadecimal or 1500 decimal then the Length field is being used to indicate the use of the IEEE 802.3 frame format. This is how Ethernet II and 802.3 frames are differentiated.
* **Data Field**: This field (46 - 1500 bytes) contains the encapsulated data from a higher layer, which is a generic Layer 3 PDU, or more commonly, an IPv4 packet. All frames must be at least 64 bytes long. If a small packet is encapsulated, additional bits called a pad are used to increase the size of the frame to this minimum size.
* **Frame Check Sequence Field**: The Frame Check Sequence (FCS) field (4 bytes) is used to detect errors in a frame. It uses a cyclic redundancy check (CRC). The sending device includes the results of a CRC in the FCS field of the frame. The receiving device receives the frame and generates a CRC to look for errors. If the calculations match, no error occurred. Calculations that do not match are an indication that the data has changed; therefore, the frame is dropped. A change in the data could be the result of a disruption of the electrical signals that represent the bits.

**Ethernet MAC:** The use of the MAC address is one of the most important aspects of the Ethernet LAN technology. MAC addresses use hexadecimal numbering. Example: 00-18-DE-C7-F3-FB.

**Unicast MAC address**: A unicast MAC address is the unique address used when a frame is sent from a single transmitting device to a single destination device.

**Broadcast MAC Address:** A broadcast packet contains a destination IP address that has all ones (1s) in the host portion. This numbering in the address means that all hosts on that local network (broadcast domain) will receive and process the packet. Many network protocols, such as DHCP and Address Resolution Protocol (ARP), use broadcasts

**Multicast MAC Address:** Multicast addresses allow a source device to send a packet to a group of devices. Multicast addresses would be used in remote gaming, where many players are connected remotely but playing the same game. Another use of multicast addresses is in distance learning through video conferencing, where many students are connected to the same class.

**MAC AND IP:**

There are two primary addresses assigned to a host device:

* Physical address (the MAC address)- However, along each link in a path, an IP packet is encapsulated in a frame specific to the data link technology associated with that link, such as Ethernet. End devices on an Ethernet network do not accept and process frames based on IP addresses, rather, a frame is accepted and processed based on MAC addresses. MAC addresses are used to identify, at a lower level, the source and destination hosts. When a host on an Ethernet network communicates, it sends frames containing its own MAC address as the source and the MAC address of the intended recipient as the destination. All hosts that receive the frame will read the destination MAC address. If the destination MAC address matches the MAC address configured on the host NIC, only then will the host process the message.
* Logical address (the IP address) - One of the most common ways a source device determines the IP address of a destination device is through Domain Name Service (DNS), in which an IP address is associated to a domain name. IP addressing determines the end-to-end behavior of an IP packet.

**Address Resolution Protocol (ARP):** While the IP address of the destination will be provided by a higher OSI layer, the sending node needs a way to find the MAC address of the destination for a given Ethernet link. This is the purpose of ARP.

The ARP protocol provides two basic functions:

* Resolving IPv4 addresses to MAC addresses
* Maintaining a table of mappings

**ARP functions:** For a frame to be placed on the LAN media, it must have a destination MAC address. When a packet is sent to the data link layer to be encapsulated into a frame, the node refers to a table in its memory to find the data link layer address that is mapped to the destination IPv4 address. This table is called the ARP table or the ARP cache. The ARP table is stored in the RAM of the device. The ARP table is maintained dynamically. **There are two ways that a device can gather MAC addresses**. **One** way is to monitor the traffic that occurs on the local network segment. As a node receives frames from the media, it can record the source IP and MAC address as a mapping in the ARP table. As frames are transmitted on the network, the device populates the ARP table with address pairs. **Another** way a device can get an address pair is to send an ARP request as shown in the figure. An ARP request is a Layer 2 broadcast to all devices on the Ethernet LAN. The ARP request contains the IP address of the destination host and the broadcast MAC address, FFFF.FFFF.FFFF. Since this is a broadcast, all nodes on the Ethernet LAN will receive it and look at the contents. The node with the IP address that matches the IP address in the ARP request will reply. The reply will be a unicast frame that includes the MAC address that corresponds to the IP address in the request. This response is then used to make a new entry in the ARP table of the sending node.

**ARP Operation/ARP Role in Remote communication.**

**Removing Entries from an ARP Table:** For each device, an ARP cache timer removes ARP entries that have not been used for a specified period. The times differ depending on the device and its operating system. For example, some Windows operating systems store ARP cache entries for 2 minutes. If the entry is used again during that time, the ARP timer for that entry is extended to 10 minutes. Each device has an operating system-specific command to delete the contents of the ARP cache. These commands do not invoke the execution of ARP in any way.

**Issues with ARP:**

**Overhead on the Media**

As a broadcast frame, an ARP request is received and processed by every device on the local network. On a typical business network, these broadcasts would probably have minimal impact on network performance. However, if a large number of devices were to be powered up and all start accessing network services at the same time, there could be some reduction in performance for a short period of time. For example, if all students in a lab logged into classroom computers and attempted to access the Internet at the same time, there could be delays. However, after the devices send out the initial ARP broadcasts and have learned the necessary MAC addresses, any impact on the network will be minimized.

**Security**

In some cases, the use of ARP can lead to a potential security risk. ARP spoofing, or ARP poisoning, is a technique used by an attacker to inject the wrong MAC address association into a network by issuing fake ARP replies. An attacker forges the MAC address of a device and then frames can be sent to the wrong destination.

Manually configuring static ARP associations is one way to prevent ARP spoofing. Authorized MAC addresses can be configured on some network devices to restrict network access to only those devices listed.

**Solutions:** Broadcast and security issues related to ARP can be mitigated with modern switches. Switches provide segmentation of a LAN, dividing the LAN into independent collision domains. Each port on a switch represents a separate collision domain and provides the full media bandwidth to the node or nodes connected on that port. While switches do not by default prevent broadcasts from propagating to connected devices, they do isolate unicast Ethernet communications so that they are only "heard" by the source and destination devices. So if there are a large number of ARP requests, each ARP reply will only be between two devices.

* **LAN Switches**

Switches use MAC addresses to direct network communications through their switch fabric to the appropriate port toward the destination node. The switch fabric is the integrated circuits and the accompanying machine programming that allows the data paths through the switch to be controlled. A switch determines how to handle incoming data frames by using its MAC address table. A switch builds its MAC address table by recording the MAC addresses of the nodes connected to each of its ports. Once a MAC address for a specific node on a specific port is recorded in the address table, the switch then knows to send traffic destined for that specific node out the port mapped to that node for subsequent transmissions.

The following describes this process:

**Step 1.** The switch receives a broadcast frame from PC1 on Port 1.

**Step 2.** The switch enters the source MAC address and the switch port that received the frame into the address table.

**Step 3.** Because the destination address is a broadcast, the switch floods the frame to all ports, except the port on which it received the frame.

**Step 4.** The destination device replies to the broadcast with a unicast frame addressed to PC1.

**Step 5.** The switch enters the source MAC address of PC3 and the port number of the switch port that received the frame into the address table. The destination address of the frame and its associated port is found in the MAC address table.

**Step 6.** The switch can now forward frames between source and destination devices without flooding because it has entries in the address table that identify the associated ports.

Timeline

Description automatically generated

**Auto-MDIX**

In addition to having the correct duplex setting, it is also necessary to have the correct cable type defined for each port. Connections between specific devices, such as switch-to-switch, switch-to-router, switch-to-host, and router-to-host device, once required the use of a specific cable types (crossover or straight-through). Instead, most switch devices now support the **mdix auto** interface configuration command in the CLI to enable the automatic medium-dependent interface crossover (auto-MDIX) feature.

When the auto-MDIX feature is enabled, the switch detects the required cable type for copper Ethernet connections and configures the interfaces accordingly. Therefore, you can use either a crossover or a straight-through cable for connections to a copper 10/100/1000 port on the switch, regardless of the type of device on the other end of the connection.

switches used one of the following forwarding methods for switching data between network ports:

* Store-and-forward switching- when the switch receives the frame, it stores the data in buffers until the complete frame has been received. During the storage process, the switch analyzes the frame for information about its destination. In this process, the switch also performs an error check using the Cyclic Redundancy Check (CRC) trailer portion of the Ethernet frame.
* Cut-through switching- the switch acts upon the data as soon as it is received, even if the transmission is not complete. The switch buffers just enough of the frame to read the destination MAC address so that it can determine to which port to forward the data. The switch looks up the destination MAC address in its switching table, determines the outgoing interface port, and forwards the frame onto its destination through the designated switch port. The switch does not perform any error checking on the frame. Because the switch does not have to wait for the entire frame to be completely buffered, and because the switch does not perform any error checking, cut-through switching is faster than store-and-forward switching. However, because the switch does not perform any error checking, it forwards corrupt frames throughout the network. The corrupt frames consume bandwidth while they are being forwarded. The destination NIC eventually discards the corrupt frames.

There are two variants of cut-through switching:

* **Fast-forward switching**: Fast-forward switching offers the lowest level of latency. Fast-forward switching immediately forwards a packet after reading the destination address. Because fast-forward switching starts forwarding before the entire packet has been received, there may be times when packets are relayed with errors. This occurs infrequently, and the destination network adapter discards the faulty packet upon receipt. In fast-forward mode, latency is measured from the first bit received to the first bit transmitted. Fast-forward switching is the typical cut-through method of switching.
* **Fragment-free switching**: In fragment-free switching, the switch stores the first 64 bytes of the frame before forwarding. Fragment-free switching can be viewed as a compromise between store-and-forward switching and fast-forward switching. The reason fragment-free switching stores only the first 64 bytes of the frame is that most network errors and collisions occur during the first 64 bytes. Fragment-free switching tries to enhance fast-forward switching by performing a small error check on the first 64 bytes of the frame to ensure that a collision has not occurred before forwarding the frame. Fragment-free switching is a compromise between the high latency and high integrity of store-and-forward switching, and the low latency and reduced integrity of fast-forward switching.

Table

Description automatically generated

**Half Duplex**

Half-duplex communication relies on unidirectional data flow where sending and receiving data are not performed at the same time. This is similar to how walkie-talkies or two-way radios function in that only one person can talk at any one time. If someone talks while someone else is already speaking, a collision occurs. As a result, half-duplex communication implements CSMA/CD to help reduce the potential for collisions and detect them when they do happen. Half-duplex communications have performance issues due to the constant waiting, because data can only flow in one direction at a time. Half-duplex connections are typically seen in older hardware, such as hubs. Nodes that are attached to hubs that share their connection to a switch port must operate in half-duplex mode because the end computers must be able to detect collisions. Nodes can operate in a half-duplex mode if the NIC card cannot be configured for full duplex operations. In this case the port on the switch defaults to a half-duplex mode as well. Because of these limitations, full-duplex communication has replaced half duplex in more current hardware.

**Full Duplex**

In full-duplex communication, data flow is bidirectional, so data can be sent and received at the same time. The bidirectional support enhances performance by reducing the wait time between transmissions. Most Ethernet, Fast Ethernet, and Gigabit Ethernet NICs sold today offer full-duplex capability. In full-duplex mode, the collision detect circuit is disabled. Frames sent by the two connected end nodes cannot collide because the end nodes use two separate circuits in the network cable. Each full-duplex connection uses only one port. Full-duplex connections require a switch that supports full duplex or a direct connection between two nodes that each support full duplex. Nodes that are directly attached to a dedicated switch port with NICs that support full duplex should be connected to switch ports that are configured to operate in full-duplex mode.

The figure shows the two duplex settings available on modern network equipment.

A Cisco Catalyst switch supports three duplex settings:

* The full option sets full-duplex mode.
* The half option sets half-duplex mode.
* The auto option sets autonegotiation of duplex mode. With autonegotiation enabled, the two ports communicate to decide the best mode of operation.

Power over Ethernet (PoE) allows a switch to deliver power to a device, such as IP phones and some wireless access points, over the existing Ethernet cabling. This allows more flexibility for installation.

The forwarding rate defines the processing capabilities of a switch by rating how much data the switch can process per second.

The port density of a device can vary depending on whether the device is a fixed configuration device or a modular device.

Waterfall chart

Description automatically generated

**Fixed Configuration Switches**

Fixed configuration switches are just as you might expect, fixed in their configuration. What that means is that you cannot add features or options to the switch beyond those that originally came with the switch. The model you purchase determines the features and options available. For example, if you purchase a 24-port gigabit fixed switch, you cannot add additional ports when you need them. There are typically different configuration choices that vary in how many and what types of ports are included.

**Modular Switches**

Modular switches offer more flexibility in their configuration. Modular switches typically come with different sized chassis that allow for the installation of different numbers of modular line cards. The line cards contain the ports. The line card fits into the switch chassis like expansion cards fit into a PC. The larger the chassis, the more modules it can support. As you can see in the figure, there can be many different chassis sizes to choose from. If you bought a modular switch with a 24-port line card, you could easily add an additional 24 port line card, to bring the total number of ports up to 48.

**Layer 2 vs Layer 3 switching**

Recall that a Layer 2 LAN switch performs switching and filtering based only on the OSI data link layer (Layer 2) MAC address and depends upon routers to pass data between independent IP subnetworks (see Figure 1).

As shown in Figure 2, a Layer 3 switch, such as the Catalyst 3560, functions similarly to a Layer 2 switch, such as the Catalyst 2960, but instead of using only the Layer 2 MAC address information for forwarding decisions, a Layer 3 switch can also use IP address information. Instead of only learning which MAC addresses are associated with each of its ports, a Layer 3 switch can also learn which IP addresses are associated with its interfaces. This allows the Layer 3 switch to direct traffic throughout the network based on IP address information as well.

Layer 3 switches are also capable of performing Layer 3 routing functions, reducing the need for dedicated routers on a LAN. Because Layer 3 switches have specialized switching hardware, they can typically route data as quickly as they can switch.

**Cisco Express Forwarding:**

Cisco devices which support Layer 3 switching utilize Cisco Express Forwarding (CEF). This forwarding method is quite complex, but fortunately, like any good technology, is carried out in large part "behind the scenes".

The two main components of CEF operation are the:

* Forwarding Information Base (FIB)
* Adjacency tables

The FIB is conceptually like a routing table. A router uses the routing table to determine best path to a destination network based on the network portion of the destination IP address. With CEF, information previously stored in the route cache is, instead, stored in several data structures for CEF switching. The data structures provide optimized lookup for efficient packet forwarding. A networking device uses the FIB lookup table to make destination-based switching decisions without having to access the route cache.

The FIB is updated when changes occur in the network and contains all routes known at the time.

Adjacency tables maintain Layer 2 next-hop addresses for all FIB entries.

The separation of the reachability information (in the FIB table) and the forwarding information (in the adjacency table), provides several benefits:

* The adjacency table can be built separately from the FIB table, allowing both to be built without any packets being process switched.
* The MAC header rewrite used to forward a packet is not stored in cache entries, so changes in a MAC header rewrite string do

The major types of Layer 3 interfaces are:

* **Switch Virtual Interface (SVI)** - Logical interface on a switch associated with a virtual local area network (VLAN).
* **Routed Port** - Physical port on a Layer 3 switch configured to act as a router port.
* **Layer 3 EtherChannel** - Logical interface on a Cisco device associated with a bundle of routed ports.
* an SVI for the default VLAN (VLAN1) must be enabled to provide IP host connectivity to the switch and permit remote switch administration. SVIs must also be configured to allow routing between VLANs. As stated, SVIs are logical interfaces configured for specific VLANs; to route between two or more VLANs, each VLAN must have a separate SVI enabled.
* Routed ports enable (Layer 3) Cisco switches to effectively serve as routers. Each port on such a switch can be configured as a port on an independent IP network.
* Layer 3 EtherChannels are used to bundle Layer 3 Ethernet links between Cisco devices in order to aggregate bandwidth, typically on uplinks.

A switch port can be configured to be a Layer 3 routed port and behave like a regular router interface. Specifically, a routed port:

* Is not associated with a particular VLAN.
* Can be configured with a Layer 3 routing protocol.
* Is a Layer 3 interface only and does not support Layer 2 protocol.

Configure routed ports by putting the interface into Layer 3 mode with the **no switchport** interface configuration command. Then assign an IP address to the port. That's it!

Graphical user interface

Description automatically generated