Ethernet

Network Fundamentals – Chapter 9

Cisco Networking Academy®
Mind Wide Open™

Objectives

Identify the basic characteristics of network media used in Ethernet.

Describe the physical and data link features of Ethernet.

Describe the function and characteristics of the media access control method used by Ethernet protocol.

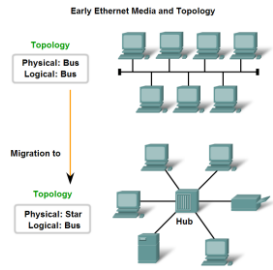
Explain the importance of Layer 2 addressing used for data transmission and determine how the different types of addressing impacts network operation and performance.

Compare and contrast the application and benefits of using Ethernet switches in a LAN as apposed to using hubs.

Explain the ARP process.

Characteristics of Network Media used in Ethernet

Identify several characteristics of Ethernet in its early years.



Earlier Ethernet

The first versions of Ethernet used coaxial cable to connect computers in a bus topology.

Each computer was directly connected to the backbone. These early versions of Ethernet were known as Thicknet, (10BASE5) and Thinnet (10BASE2).

10BASE5, or Thicknet, used a thick coaxial that allowed for cabling distances of up to 500 meters before the signal required a repeater.

10BASE2, or Thinnet, used a thin coaxial cable that was smaller in diameter and more flexible than Thicknet and allowed for cabling distances of 185 meters.

The early implementations of Ethernet were deployed in a low-bandwidth LAN environment where access to the shared media was managed by CSMA, and later CSMA/CD

Later Implementations

The physical topology was also changed to a star topology using hubs.

Hubs concentrate connections. In other words, they take a group of nodes and allow the network to see them as a single unit.

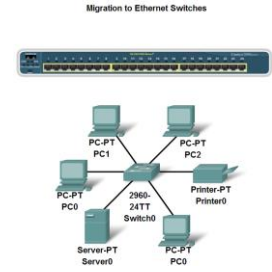
When a frame arrives at one port, it is copied to the other ports so that all the segments on the LAN receive the frame.

Using the hub in this bus topology increased network reliability by allowing any single cable to fail without disrupting the entire network.

However, repeating the frame to all other ports did not solve the issue of collisions.

Characteristics of Network Media used in Ethernet

Describe the emergence of the LAN switch as a key innovation for managing collisions on Ethernet-based networks



Legacy Ethernet

In 10BASE-T networks, typically the central point of the network segment was a hub.

This created a shared media. Because the media is shared, only one station could successfully transmit at a time.

This type of connection is described as a half-duplex communication.

During periods of low communications activity, the few collisions that occur are managed by CSMA/CD, with little or no impact on performance.

As the number of devices and subsequent data traffic increase, however, the rise in collisions can have a significant impact on the user's experience.

Current Ethernet

A significant development that enhanced LAN performance was the introduction of switches to replace hubs in Ethernet-based networks.

This development closely corresponded with the development of 100BASE-TX Ethernet.

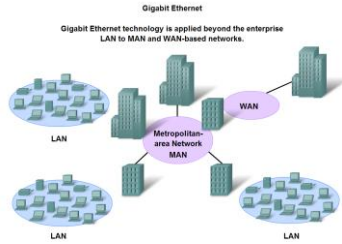
Switches can control the flow of data by isolating each port and sending a frame only to its proper destination (if the destination is known), rather than send every frame to every device.

The switch reduces the number of devices receiving each frame, which in turn reduces or minimizes the possibility of collisions.

This, and the later introduction of full-duplex communications (having a connection that can carry both transmitted and received signals at the same time), has enabled the development of 1Gbps Ethernet and beyond.

Characteristics of Network Media used in Ethernet

Identify the characteristics of state-of-the-art Ethernet and describe its utilization of cabling and point-to-point topography



Gigabit-Ethernet

Gigabit Ethernet is used to describe Ethernet implementations that provide bandwidth of 1000 Mbps (1 Gbps) or greater.

This capacity has been built on the full-duplex capability and the UTP and fiber-optic media technologies of earlier Ethernet.

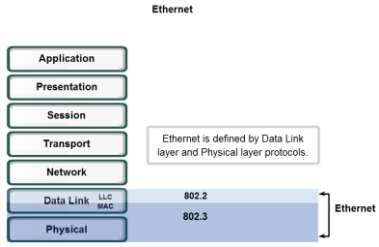
The increase in network performance is significant when potential throughput increases from 100 Mbps to 1 Gbps and above.

Upgrading to 1 Gbps Ethernet does not always mean that the existing network infrastructure of cables and switches has to be completely replaced.

Some of the equipment and cabling in modern, well-designed and installed networks may be capable of working at the higher speeds with only minimal upgrading.

Physical and Data Link Features of Ethernet

Standards and Implementation



IEEE Standards - History

The first LAN in the world was the original version of Ethernet. Robert Metcalfe and his coworkers at Xerox designed it more than thirty years ago.

The first Ethernet standard was published in 1980 by a consortium of Digital Equipment Corporation, Intel, and Xerox (DIX).

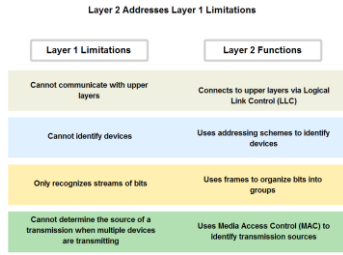
Metcalfe wanted Ethernet to be a shared standard from which everyone could benefit, and therefore it was released as an open standard. The first products that were developed from the Ethernet standard were sold in the early 1980s

The IEEE wanted to make sure that its standards were compatible with those of the International Standards Organization (ISO) and OSI model.

To ensure compatibility, the IEEE 802.3 standards had to address the needs of Layer 1 and the lower portion of Layer 2 of the OSI model. As a result, some small modifications to the original Ethernet standard were made in 802.3.

Physical and Data Link Features of Ethernet

Describe how the Ethernet operates across two layers of the OSI model



Layers 1 and 2

Ethernet at Layer 1 involves signals, bit streams that travel on the media, physical components that put signals on media, and various topologies.

Ethernet Layer 1 performs a key role in the communication that takes place between devices, but each of its functions has limitations.

As the figure shows, Ethernet at Layer 2 addresses these limitations.

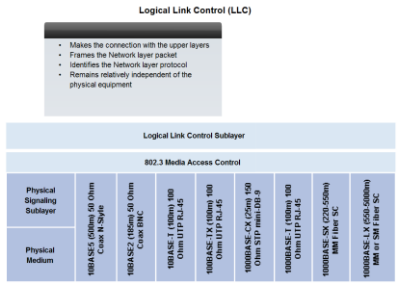
The Data Link sublayers contribute significantly to technological compatibility and computer communications.

The MAC sublayer is concerned with the physical components that will be used to communicate the information and prepares the data for transmission over the media.

The Logical Link Control (LLC) sublayer remains relatively independent of the physical equipment that will be used for the communication process.

Physical and Data Link Features of Ethernet

Logic Link Control – Connecting the Upper Layers



LLC – Logic Link Control

For Ethernet, the IEEE 802.2 standard describes the LLC sublayer functions, and the 802.3 standard describes the MAC sublayer and the Physical layer functions.

Logical Link Control handles the communication between the upper layers and the networking software, and the lower layers, typically the 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.

Layer 2 communicates with the upper layers through LLC.

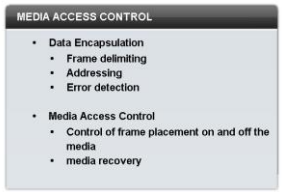
LLC is implemented in software, and its implementation is independent of the physical equipment.

In a computer, the LLC can be considered the driver software for the Network Interface Card (NIC).

Physical and Data Link Features of Ethernet

Media Access Control (MAC)

MAC—Getting Data to the Media



Data Encapsulation

Data encapsulation provides three primary functions:

1. Frame delimiting
2. Addressing
3. Error detection

The data encapsulation process includes frame assembly before transmission and frame parsing upon reception of a frame.

In forming the frame, the MAC layer adds a header and trailer to the Layer 3 PDU.

The use of frames aids in the transmission of bits as they are placed on the media and in the grouping of bits at the receiving node.

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.

Data Encapsulation – Addressing/Error Control

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.

An additional function of data encapsulation is 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

The MAC sublayer controls the placement of frames on the media and the removal of frames from the media. As its name implies, it manages the media access control.

This includes the initiation of frame transmission and recovery from transmission failure due to collisions.

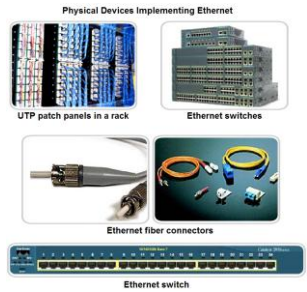
Logical Topology:

The underlying logical topology of Ethernet is a multi-access bus. This means that all the nodes (devices) in that network segment share the medium.

Ethernet provides a method for determining how the nodes share access to the media. The media access control method for classic Ethernet is Carrier Sense Multiple Access with Collision Detection (**CSMA/CD**).

Physical and Data Link Features of Ethernet

Physical Implementations of the Ethernet



Physical Aspects of Ethernet

The success of Ethernet is due to the following factors:

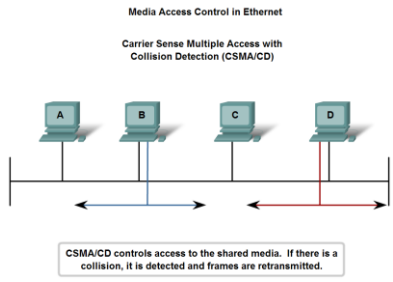
1. Simplicity and ease of maintenance
2. Ability to incorporate new technologies
3. Reliability
4. Low cost of installation and upgrade

As a technology associated with the Physical layer, Ethernet specifies and implements encoding and decoding schemes that enable frame bits to be carried as signals across the media.

Ethernet devices make use of a broad range of cable and connector specifications. In today's networks, Ethernet uses UTP copper cables and optical fiber to interconnect network devices via intermediary devices such as hubs and switches.

Function and Characteristics of the Media Access Control Method

MAC in Ethernet



CSMA/CD

In a shared media environment, all devices have guaranteed access to the medium, but they have no prioritized claim on it.

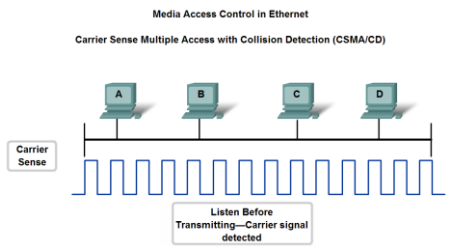
If more than one device transmits simultaneously, the physical signals collide and the network must recover in order for communication to continue.

Ethernet uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) to detect and handle collisions and manage the resumption of communications.

Because all computers using Ethernet send their messages on the same media, a distributed coordination scheme (CSMA) is used to detect the electrical activity on the cable. A device can then determine when it can transmit

Function and Characteristics of the Media Access Control Method

Carrier Sense Multiple Access with Collision Detection



CSMA/CD

1. **Carrier Sense**: In the CSMA/CD access method, all network devices that have messages to send must listen before transmitting. If a device detects a signal from another device, it will wait for a specified amount of time before attempting to transmit.
2. **Multiple-access**: If the distance between devices is such that the latency of one device's signals means that signals are not detected by a second device, the second device may start to transmit, too. The media now has two devices transmitting their signals at the same time. Their messages will propagate across the media until they encounter each other.

CSMA/CD

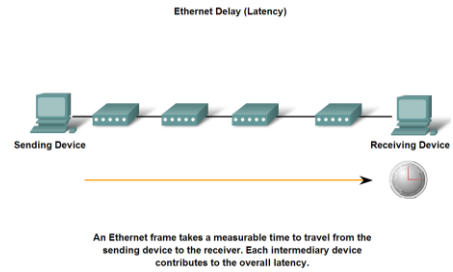
3. Collision Detection: When a device is in listening mode, it can detect when a collision occurs on the shared media. The detection of a collision is made possible because all devices can detect an increase in the amplitude of the signal above the normal level.

4. Jam Signal: Once the collision is detected by the transmitting devices, they send out a jamming signal. This jamming signal is used to notify the other devices of a collision, so that they will invoke a backoff algorithm.

This backoff algorithm causes all devices to stop transmitting for a random amount of time, which allows the collision signals to subside.

Function and Characteristics of the Media Access Control Method

Ethernet Timing



Ethernet Timing

As discussed, each device that wants to transmit must first "listen" to the media to check for traffic.

If no traffic exists, the station will begin to transmit immediately.

The electrical signal that is transmitted takes a certain amount of time (latency) to propagate (travel) down the cable. Each hub or repeater in the signal's path adds latency as it forwards the bits from one port to the next.

This accumulated delay increases the likelihood that collisions will occur because a listening node may transition into transmitting signals while the hub or repeater is processing the message.

Because the signal had not reached this node while it was listening, it thought that the media was available. This condition often results in collisions.

Preamble

Frame Synchronization for Asynchronous Communications

Field Names				
A	B	C	D	E
Start Frame Field	Address Field	Type/Length Field	Data Field	FCS Field

10 Mbps and slower Ethernet use the first 64 bits of the frame Preamble to synchronize the receiver.

Layer 2 addressing and its Impact on Network Operation and Performance

The Frame – Encapsulating the Packet

Comparison of 802.3 and Ethernet Frame Structures and Field Size

Field size in bytes

IEEE 802.3						
7	1	6	6	2	46 to 1500	4
Preamble	Start of Frame delimiter	Destination Address	Source Address	Length/ Type	802.2 Header and Data	Frame Check Sequence

Ethernet					
8	6	6	2	46 to 1500	4
Preamble	Destination Address	Source Address	Type	Data	Frame Check Sequence

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.

This includes all bytes from the Destination MAC Address field through the Frame Check Sequence (FCS) field.

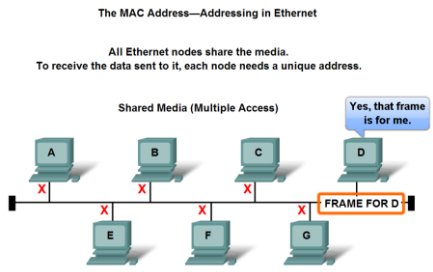
The Preamble and Start Frame Delimiter fields are not included when describing the size of a frame. The IEEE 802.3ac standard, released in 1998, extended the maximum allowable frame size to 1522 bytes.

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.

Layer 2 addressing and its Impact on Network Operation and Performance

The Ethernet MAC Address



MAC Addressing

A unique identifier called a Media Access Control (MAC) address was created to assist in determining the source and destination address within an Ethernet network.

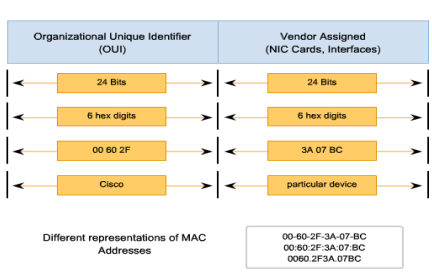
Regardless of which variety of Ethernet was used, the naming convention provided a method for device identification at a lower level of the OSI model.

The MAC address value is a direct result of IEEE-enforced rules for vendors to ensure globally unique addresses for each Ethernet device.

The rules established by IEEE require any vendor that sells Ethernet devices to register with IEEE. The IEEE assigns the vendor a 3-byte code, called the Organizationally Unique Identifier (OUI).

MAC Address Structure

The Ethernet MAC Address Structure



Layer 2 addressing and its Impact on Network Operation and Performance

Hexadecimal Numbering and Addressing

Hexadecimal Numbering

Decimal and Binary equivalents of 0 to F Hexadecimal

Decimal	Binary	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Selected Decimal, Binary and Hexadecimal equivalents

Decimal	Binary	Hexadecimal
0	0000 0000	00
1	0000 0001	01
2	0000 0010	02
3	0000 0011	03
4	0000 0100	04
5	0000 0101	05
6	0000 0110	06
7	0000 0111	07
8	0000 1000	08
10	0000 1010	0A
15	0000 1111	0F
16	0001 0000	10
32	0010 0000	20
64	0100 0000	40
128	1000 0000	80
192	1100 0000	C0
202	1100 1010	CA
240	1111 0000	F0
255	1111 1111	FF

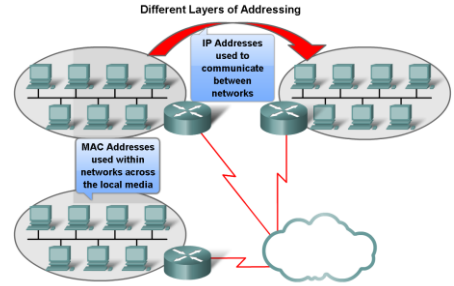
IPCONFIG /all

Viewing the MAC Address

```
C:\>ipconfig /all
Ethernet adapter Network Connection:
        Connection-specific DNS Suffix: exsmple.com
        Description . . . . . . . . . . . : Intel(R) PRO/Wireless 3945ABG Network
Connection
        Physical Address. . . . . . . . . : 00-18-DE-C7-F3-FB
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 10.2.3.4
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.2.3.254
        DHCP Server . . . . . . . . . . . : 10.2.3.69
        DNS Servers . . . . . . . . . . . : 192.168.226.120
        Lease Obtained. . . . . . . . . . : Thursday, May 03, 2007 3:47:51 PM
        Lease Expires . . . . . . . . . . : Friday, May 04, 2007 6:57:11 AM
C:\>
```

Layer 2 addressing and its Impact on Network Operation and Performance

Another Layer of Addressing



Different Addressing

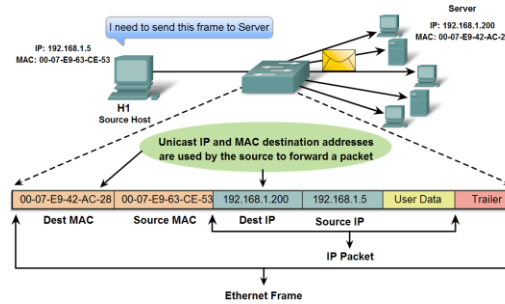
In a nutshell:

The Network layer address enables the packet to be forwarded toward its destination.

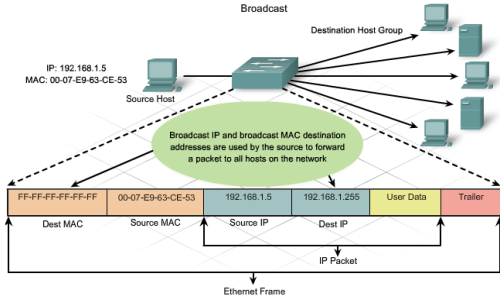
The Data Link layer address enables the packet to be carried by the local media across each segment.

Layer 2 addressing and its Impact on Network Operation and Performance

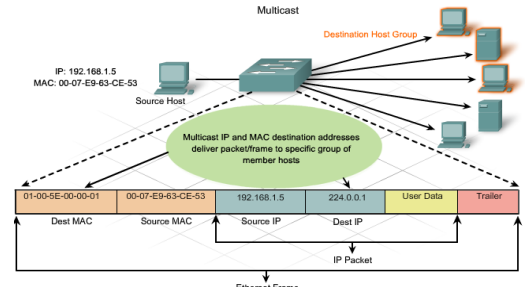
Ethernet Unicast, Multicast and Broadcast



Broadcast

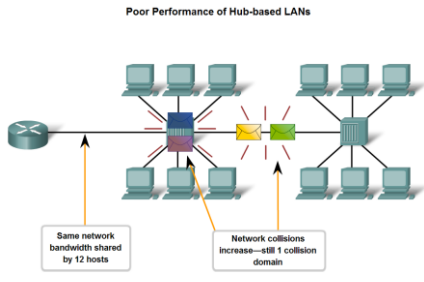


Multicast



Compare and Contrast the Use of Ethernet Switches versus Hubs in a LAN.

Legacy Ethernet – Using Hubs



Legacy Ethernet – Performance Issues

Scalability - With each device added to the shared media, the average bandwidth available to each device decreases. With each increase in the number of devices on the media, performance is degraded.

Latency - Latency can increase significantly as the distance between nodes is extended.

Latency is also affected by a delay of the signal across the media as well as the delay added by the processing of the signals through hubs and repeaters.

Increasing the length of media or the number of hubs and repeaters connected to a segment results in increased latency. With greater latency, it is more likely that nodes will not receive initial signals, thereby increasing the collisions present in the network.

Legacy Ethernet

Network Failure - Because classic Ethernet shares the media, any device in the network could potentially cause problems for other devices.

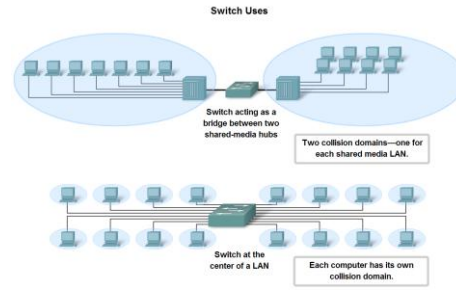
If any device connected to the hub generates detrimental traffic, the communication for all devices on the media could be impeded. This harmful traffic could be due to incorrect speed or full-duplex settings on a NIC.

Collisions - If two nodes send packets at the same time, a collision occurs and the packets are lost. Then both nodes send a jam signal, wait for a random amount of time, and retransmit their packets.

Any part of the network where packets from two or more nodes can interfere with each other is considered a collision domain. A network with a larger number of nodes on the same segment has a larger collision domain and typically has more traffic.

Compare and Contrast the Use of Ethernet Switches versus Hubs in a LAN.

Ethernet – Using Switches



Switch Uses

Switches allow the segmentation of the LAN into separate collision domains.

Each port of the switch represents a separate collision domain and provides the full media bandwidth to the node or nodes connected on that port.

With fewer nodes in each collision domain, there is an increase in the average bandwidth available to each node, and collisions are reduced.

A LAN may have a centralized switch connecting to hubs that still provide the connectivity to nodes. Or, a LAN may have all nodes connected directly to a switch. Theses topologies are shown in the figure.

Switch V Hubs

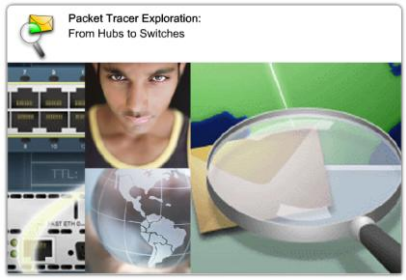
In a LAN where all nodes are connected directly to the switch, the throughput of the network increases dramatically. The three primary reasons for this increase are:

1. Dedicated bandwidth to each port
2. Collision-free environment
3. Full-duplex operation

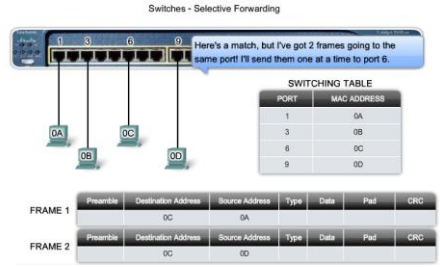
There are three reasons why hubs are still being used:

1. Availability – not developed until the 90's
2. Economics – rather expensive
3. Requirements – LANs have simple design and hubs accommodate this

Packet Tracer Labs



Selective Forwarding



Selective Switching – Store and Forward

Ethernet switches selectively forward individual frames from a receiving port to the port where the destination node is connected.

This selective forwarding process can be thought of as establishing a momentary point-to-point connection between the transmitting and receiving nodes.

The connection is made only long enough to forward a single frame.

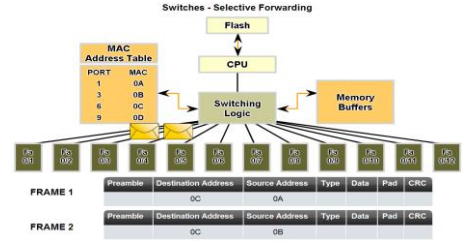
During this instant, the two nodes have a full bandwidth connection between them and represent a logical point-to-point connection.

With store and forward switching, the switch receives the entire frame, checks the FSC for errors, and forwards the frame to the appropriate port for the destination node.

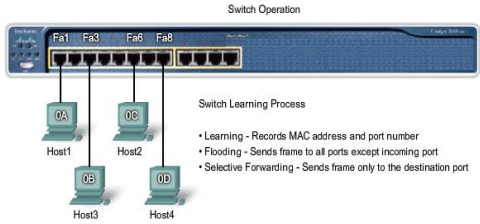
Because the nodes do not have to wait for the media to be idle, the nodes can send and receive at full media speed without losses due to collisions or the overhead associated with managing collisions.

Compare and Contrast the Use of Ethernet Switches versus Hubs in a LAN.

Describe how a switch can eliminate collisions, backoffs and re- transmissions, the leading factors in reduced throughput on a hub-based Ethernet network



Switch Learning Process



Switch Operation

Learning - As each frame enters the switch, the switch examines the source MAC address. Using a lookup procedure, the switch determines if the table already contains an entry for that MAC address.

Aging - The entries in the MAC table acquired by the Learning process are time stamped. This timestamp is used as a means for removing old entries in the MAC table

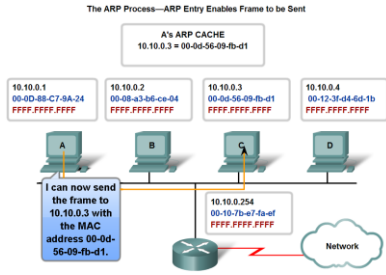
Flooding - If the switch does not know to which port to send a frame because the destination MAC address is not in the MAC table, the switch sends the frame to all ports except the port on which the frame arrived.

Selective forwarding - is the process of examining a frame's destination MAC address and forwarding it out the appropriate port. This is the central function of the switch.

Filtering - In some cases, a frame is not forwarded. This process is called frame filtering. One use of filtering has already been described: a switch does not forward a frame to the same port on which it arrived. A switch will also drop a corrupt frame. If a frame fails a CRC check, the frame is dropped.

Explain the Address Resolution Protocol (ARP) process.

Mapping IP to MAC Addresses



Purpose of ARP

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.

To begin the process, a transmitting node attempts to locate in the ARP table the MAC address mapped to an IPv4 destination.

If this map is cached in the table, the node uses the MAC address as the destination MAC in the frame that encapsulates the IPv4 packet. The frame is then encoded onto the networking media.

Maintaining ARP

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.

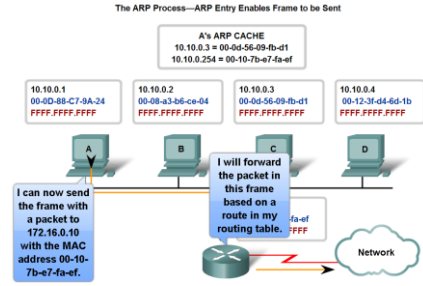
As frames are transmitted on the network, the device populates the ARP table with address pairs.

Another way a device can get an address pair is to broadcast an ARP request. ARP sends a Layer 2 broadcast to all devices on the Ethernet LAN.

The frame contains an ARP request packet with the IP address of the destination host.

Explain the Address Resolution Protocol (ARP) process.

ARP – Destinations Outside the Local Network



ARP and Outside Networks

If the destination IPv4 host is not on the local network, the source node needs to deliver the frame to the router interface that is the gateway or next hop used to reach that destination.

The source node will use the MAC address of the gateway as the destination address for frames containing an IPv4 packet addressed to hosts on other networks.

The gateway address of the router interface is stored in the IPv4 configuration of the hosts.

When a host creates a packet for a destination, it compares the destination IP address and its own IP address to determine if the two IP addresses are located on the same Layer 3 network.

If the receiving host is not on the same network, the source uses the ARP process to determine a MAC address for the router interface serving as the gateway.

Proxy ARP

Outside Network Problem - To provide a MAC address for these hosts, a router interface may use a proxy ARP to respond on behalf of these remote hosts.

This means that the ARP cache of the requesting device will contain the MAC address of the gateway mapped to any IP addresses not on the local network.

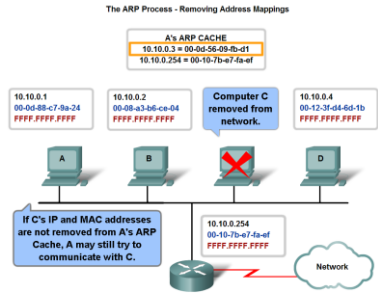
Using proxy ARP, a router interface acts as if it is the host with the IPv4 address requested by the ARP request.

By "faking" its identity, the router accepts responsibility for routing packets to the "real" destination.

Yet another use for a proxy ARP is when a host is not configured with a default gateway. Proxy ARP can help devices on a network reach remote subnets without the need to configure routing or a default gateway.

Explain the Address Resolution Protocol (ARP) process.

ARP – Removing Address Mappings



ARP Removal

For each device, an ARP cache timer removes ARP entries that have not been used for a specified period of time.

The times differ depending on the device and its operating system. For example, some Windows operating systems store ARP cache entries for 2 minutes.

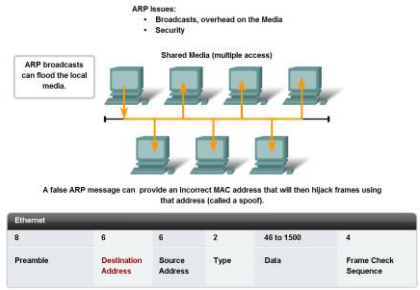
If the entry is used again during that time, the ARP timer for that entry is extended to 10 minutes.

Commands may also be used to manually remove all or some of the entries in the ARP table.

After an entry has been removed, the process for sending an ARP request and receiving an ARP reply must occur again to enter the map in the ARP table.

Explain the Address Resolution Protocol (ARP) process.

ARP Broadcasts - Issues

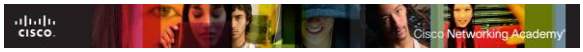


ARP Issues

Overhead - 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.

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 requests. 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.



Summary

In this chapter, you learned to:

- Identify the basic characteristics of network media used in Ethernet.
- Describe the Physical and Data Link layer features of Ethernet.
- Describe the function and characteristics of the media access control method used by Ethernet protocol.
- Explain the importance of Layer 2 addressing used for data transmission and determine how the different types of addressing impacts network operation and performance.
- Compare and contrast the application and benefits of using Ethernet switches in a LAN as opposed to using hubs.
- Explain the ARP process.