MAC Address and Hexadecimal

In networking, IPv4 addresses are represented using the decimal base ten number system and the binary base 2 number system. IPv6 addresses and Ethernet addresses are represented using the hexadecimal base sixteen number system. To understand hexadecimal, you must first be very familiar with binary and decimal.

The hexadecimal numbering system uses the numbers 0 to 9 and the letters A to F.

An Ethernet MAC address consists of a 48-bit binary value. Hexadecimal is used to identify an Ethernet address because a single hexadecimal digit represents four binary bits. Therefore, a 48-bit Ethernet MAC address can be expressed using only 12 hexadecimal values.

Hexadecimal

Given that 8 bits (one byte) is a common binary grouping, binary 00000000 to 11111111 can be represented in hexadecimal as the range 00 to FF, as shown in the next figure.

The figure is three columns showing the decimal and hexadecimal equivalents of select 8-bit binary numbers. From left to right, the column headings are: decimal, binary, and hexadecimal. Each column has 18 rows below the header.

Selected Decimal, Binary, and Hexadecimal Equivalents

When using hexadecimal, leading zeroes are always displayed to complete the 8-bit representation. For example, in the table, the binary value 0000 1010 is shown in hexadecimal as 0A.

Hexadecimal numbers are often represented by the value preceded by **0x** (e.g., 0x73) to distinguish between decimal and hexadecimal values in documentation.

Hexadecimal may also be represented by a subscript 16, or the hex number followed by an H (e.g., 73H).

You may have to convert between decimal and hexadecimal values. If such conversions are required, convert the decimal or hexadecimal value to binary, and then to convert the binary value to either decimal or hexadecimal as appropriate.

Ethernet MAC Address

In an Ethernet LAN, every network device is connected to the same, shared media. The MAC address is used to identify the physical source and destination devices (NICs) on the local network segment. MAC addressing provides a method for device identification at the data link layer of the OSI model.

An Ethernet MAC address is a 48-bit address expressed using 12 hexadecimal digits, as shown in the figure. Because a byte equals 8 bits, we can also say that a MAC address is 6 bytes in length.

The diagram shows that MAC address are composed of 48 bits total. These 48 bits can be divided into twelve 4-bit groupings, or 12 hex digits. Combining two hex digits together makes a byte, therefore the 48 bits is also equivalent to 6 bytes.

All MAC addresses must be unique to the Ethernet device or Ethernet interface. To ensure this, all vendors that sell Ethernet devices must register with the IEEE to obtain a unique 6 hexadecimal (i.e., 24-bit or 3-byte) code called the organizationally unique identifier (OUI).

When a vendor assigns a MAC address to a device or Ethernet interface, the vendor must do as follows: Use its assigned OUI as the first 6 hexadecimal digits and assign a unique value in the last 6 hexadecimal digits.

Therefore, an Ethernet MAC address consists of a 6 hexadecimal vendor OUI code followed by a 6 hexadecimal vendor-assigned value, as shown in the figure.

the first six hex digits of a MAC address (AKA first 6 hex digits or first 3 bytes) is the organizational unique identifier and the last six hex digits is vendor assigned

For example, assume that Cisco needs to assign a unique MAC address to a new device. The IEEE has assigned Cisco a OUI of **00-60-2F**. Cisco would then configure the device with a unique vendor code such as **3A-07-BC**. Therefore, the Ethernet MAC address of that device would be **00-60-2F-3A-07-BC.**

It is the responsibility of the vendor to ensure that none of its devices be assigned the same MAC address. However, it is possible for duplicate MAC addresses to exist because of mistakes made during manufacturing, mistakes made in some virtual machine implementation methods, or modifications made using one of several software tools. In any case, it will be necessary to modify the MAC address with a new NIC or make modifications via software.

Frame Processing

Sometimes the MAC address is referred to as a burned-in address (BIA) because the address is hard coded into read-only memory (ROM) on the NIC. This means that the address is encoded into the ROM chip permanently.

Note: On modern PC operating systems and NICs, it is possible to change the MAC address in software. This is useful when attempting to gain access to a network that filters based on BIA. Consequently, filtering or controlling traffic based on the MAC address is no longer as secure.

When the computer boots up, the NIC copies its MAC address from ROM into RAM. When a device is forwarding a message to an Ethernet network, the Ethernet header includes these:

- **Source MAC address** - This is the MAC address of the source device NIC.
- **Destination MAC address** - This is the MAC address of the destination device NIC.

When a NIC receives an Ethernet frame, it examines the destination MAC address to see if it matches the physical MAC address that is stored in RAM. If there is no match, the device discards the frame. If there is a match, it passes the frame up the OSI layers, where the de-encapsulation process takes place.

Note: Ethernet NICs will also accept frames if the destination MAC address is a broadcast or a multicast group of which the host is a member.

Any device that is the source or destination of an Ethernet frame, will have an Ethernet NIC and therefore, a MAC address. This includes workstations, servers, printers, mobile devices, and routers.

Unicast MAC Address

In Ethernet, different MAC addresses are used for Layer 2 unicast, broadcast, and multicast communications.

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

Click Play in the animation to view how a unicast frame is processed. In this example the destination MAC address and the destination IP address are both unicast.

The animation shows a host with IPv4 address 192.168.1.5 (source) requesting a web page from a server at IPv4 unicast address 192.168.1.200. The animation has a topology consisting of a host PC named H1 linked to a switch. The switch has connections to three other host PCs and two servers. At the bottom of the animation is an expanded view of an ethernet frame. The frame consists of the destination MAC 00-07-E9-42-AC-28, source MAC 00-07-E9-63-CE-53, Source IP 192.168.1.5, destination IP address 192.168.1.200, user data and trailer. The IP packet portion of the frame is the source IP, destination IP address, and user data. In the animation, H1 says I need to send this frame to Server. A frame is sent from H1 to the switch. The switch then forwards the frame to the server with the IP and MAC matching the destination IP and MAC address.

In the example shown in the animation, a host with IPv4 address 192.168.1.5 (source) requests a web page from the server at IPv4 unicast address 192.168.1.200. For a unicast packet to be sent and received, a destination IP address must be in the IP packet header. A corresponding destination MAC address must also be present in the Ethernet frame header. The IP address and MAC address combine to deliver data to one specific destination host.

The process that a source host uses to determine the destination MAC address associated with an IPv4 address is known as Address Resolution Protocol (ARP). The process that a source host uses to determine the destination MAC address associated with an IPv6 address is known as Neighbor Discovery (ND).

Note: The source MAC address must always be a unicast.

Broadcast MAC Address

An Ethernet broadcast frame is received and processed by every device on the Ethernet LAN. The features of an Ethernet broadcast are as follows:

- It has a destination MAC address of FF-FF-FF-FF-FF-FF in hexadecimal (48 ones in binary).
- It is flooded out all Ethernet switch ports except the incoming port.
- It is not forwarded by a router.

If the encapsulated data is an IPv4 broadcast packet, this means the packet contains a destination IPv4 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.

Click Play in the animation to view how a broadcast frame is processed. In this example the destination MAC address and destination IP address are both broadcasts.

The animation shows a source host sending an IPv4 broadcast packet to all devices on its network. The animation has a topology consisting of a host PC named H1 linked to a switch. The switch has connections to three other host PCs and two servers. At the bottom of the animation is an expanded view of an ethernet frame. The frame consists of the destination MAC FF-FF-FF-FF-FF-FF, source MAC 00-07-E9-63-CE-53, Source IP 192.168.1.5, destination IP address 192.168.1.255, user data and trailer. The IP packet portion of the frame is the source IP, destination IP address, and user data. In the animation, H1 says I need to send data to all hosts on the network. A frame is sent from H1 to the switch. The switch then forwards the frame out all its interfaces except the one connected to H1. The three other PC hosts and the two servers receive the frames.

As shown in the animation, the source host sends an IPv4 broadcast packet to all devices on its network. The IPv4 destination address is a broadcast address, 192.168.1.255. When the IPv4 broadcast packet is encapsulated in the Ethernet frame, the destination MAC address is the broadcast MAC address of FF-FF-FF-FF-FF-FF in hexadecimal (48 ones in binary).

DHCP for IPv4 is an example of a protocol that uses Ethernet and IPv4 broadcast addresses.

However, not all Ethernet broadcasts carry an IPv4 broadcast packet. For example, ARP Requests do not use IPv4, but the ARP message is sent as an Ethernet broadcast.

Multicast MAC Address

An Ethernet multicast frame is received and processed by a group of devices on the Ethernet LAN that belong to the same multicast group. The features of an Ethernet multicast are as follows:

- There is a destination MAC address of 01-00-5E when the encapsulated data is an IPv4 multicast packet and a destination MAC address of 33-33 when the encapsulated data is an IPv6 multicast packet.
- There are other reserved multicast destination MAC addresses for when the encapsulated data is not IP, such as Spanning Tree Protocol (STP) and Link Layer Discovery Protocol (LLDP).

- It is flooded out all Ethernet switch ports except the incoming port, unless the switch is configured for multicast snooping.
- It is not forwarded by a router, unless the router is configured to route multicast packets.

If the encapsulated data is an IP multicast packet, the devices that belong to a multicast group are assigned a multicast group IP address. The range of IPv4 multicast addresses is 224.0.0.0 to 239.255.255.255. The range of IPv6 multicast addresses begins with ff00::/8. Because multicast addresses represent a group of addresses (sometimes called a host group), they can only be used as the destination of a packet. The source will always be a unicast address.

As with the unicast and broadcast addresses, the multicast IP address requires a corresponding multicast MAC address to deliver frames on a local network. The multicast MAC address is associated with, and uses addressing information from, the IPv4 or IPv6 multicast address.

Click Play in the animation to view how a multicast frame is processed. In this example, the destination MAC address and destination IP address are both multicasts.

The animation shows a source host sending a multicast frame to devices that belong to the multicast group. The animation has a topology consisting of a host PC named H1 linked to a switch. The switch has connections to three other host PCs and two servers. At the bottom of the animation is an expanded view of an ethernet frame. The frame consists of the destination MAC 01-00-5E-00-00-C8, source MAC 00-07-E9-63-CE-53, Source IP 192.168.1.5, destination IP address 224.0.0.200, user data and trailer. The IP packet portion of the frame is the source IP, destination IP address, and user data. In the animation, H1 says I need to send to a group of hosts on the network. A frame is sent from H1 to the switch. The switch then forwards the frame out to only the devices in the multicast group. Two of the three PC hosts and one server receive the multicast frame.

Routing protocols and other network protocols use multicast addressing. Applications such as video and imaging software may also use multicast addressing, although multicast applications are not as common.