

MAC address

A **media access control address (MAC address)** is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment. This use is common in most IEEE 802 networking technologies, including Ethernet, Wi-Fi, and Bluetooth. Within the Open Systems Interconnection (OSI) network model, MAC addresses are used in the medium access control protocol sublayer of the data link layer. As typically represented, MAC addresses are recognizable as six groups of two hexadecimal digits, separated by hyphens, colons, or without a separator.



Label of a UMTS router with MAC addresses for LAN and WLAN modules

MAC addresses are primarily assigned by device manufacturers, and are therefore often referred to as the **burned-in address**, or as an **Ethernet hardware address**, **hardware address**, or **physical address**. Each address can be stored in hardware, such as the card's read-only memory, or by a firmware mechanism. Many network interfaces, however, support changing their MAC address. The address typically includes a manufacturer's organizationally unique identifier (OUI). MAC addresses are formed according to the principles of two numbering spaces based on Extended Unique Identifiers (EUI) managed by the Institute of Electrical and Electronics Engineers (IEEE): **EUI-48**, which replaces the obsolete term **MAC-48**,^[1] and **EUI-64**.^[2]

Network nodes with multiple network interfaces, such as routers and multilayer switches, must have a unique MAC address for each NIC in the same network. However, two NICs connected to two different networks can share the same MAC address.

Contents

Address details

Universal vs. local (U/L bit)

Universal addresses that are administered locally

Unicast vs. multicast (I/G bit)

Applications

Usage in hosts

Tracking

Randomization

Other information leakage

Anonymization

Notational conventions

Bit-reversed notation

See also

Notes

References

External links

Address details

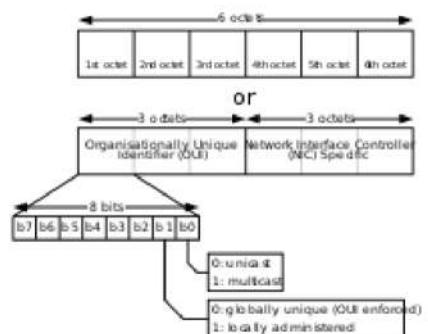
The original IEEE 802 MAC address comes from the original Xerox Network Systems Ethernet addressing scheme.^[3] This 48-bit address space contains potentially 2^{48} (over 281 trillion) possible MAC addresses. The IEEE manages allocation of MAC addresses, originally known as MAC-48 and which it now refers to as EUI-48 identifiers. The IEEE has a target lifetime of 100 years (until 2080) for applications using EUI-48 space and restricts applications accordingly. The IEEE encourages adoption of the more plentiful EUI-64 for non-Ethernet applications.

The distinction between EUI-48 and MAC-48 identifiers is in name and application only. MAC-48 was used to address hardware interfaces within existing 802-based networking applications; EUI-48 is now used for 802-based networking and is also used to identify other devices and software, for example Bluetooth.^{[2][4]} The IEEE now considers MAC-48 to be an obsolete term.^[1] EUI-48 is now used in all cases. In addition, the EUI-64 numbering system originally encompassed both MAC-48 and EUI-48 identifiers by a simple translation mechanism.^{[2][a]} These translations have since been deprecated.^[2]

An Individual Address Block (IAB) is an inactive registry activity which has been replaced by the MA-S (MA-S was previously named OUI-36 and have no overlaps in addresses with IAB^[5]) registry product as of January 1, 2014. The IAB uses an OUI from MA-L (MA-L (MAC address block large) registry was previously named OUI registry, the term OUI is still in use, but not for calling a registry^[5]) belonging to the IEEE Registration Authority, concatenated with 12 additional IEEE-provided bits (for a total of 36 bits), leaving only 12 bits for the IAB owner to assign to their (up to 4096) individual devices. An IAB is ideal for organizations requiring not more than 4096 unique 48-bit numbers (EUI-48). Unlike an OUI, which allows the assignee to assign values in various different number spaces (for example, EUI-48, EUI-64, and the various context-dependent identifier number spaces, like for SNAP or EDID (VSDB field)), the Individual Address Block could only be used to assign EUI-48 identifiers. All other potential uses based on the OUI from which the IABs are allocated are reserved, and remain the property of the IEEE Registration Authority. Between 2007 and September 2012, the OUI value 00:50:C2 was used for IAB assignments. After September 2012, the value 40:D8:55 was used. The owners of an already assigned IAB may continue to use the assignment.^[6]

MA-S (MAC address block small) registry activity includes both a 36-bit unique number used in some standards and the assignment of a block of EUI-48 and EUI-64 identifiers (while owner of IAB cannot assign EUI-64) by the IEEE Registration Authority. MA-S does not include assignment of an OUI.

There is also another registry which is called MA-M (MAC address block medium). The MA-M assignment block provides both 2^{20} EUI-48 identifiers and 2^{36} EUI-64 identifiers (that means first 28 bits are IEEE assigned bits). The first 24 bits of the assigned MA-M block are an OUI assigned to IEEE that will not be reassigned, so the MA-M does not include assignment of an OUI.



Structure of a 48-bit MAC address.
The group or I/G bit (b0)
distinguishes multicast and unicast
addressing and the local or U/L bit
(b1) distinguishes universal and
locally administered addressing.

Universal vs. local (U/L bit)

Addresses can either be *universally administered addresses* (UAA) or *locally administered addresses* (LAA). A universally administered address is uniquely assigned to a device by its manufacturer. The first three octets (in transmission order) identify the organization that issued the identifier and are known as the organizationally unique identifier (OUI).^[2] The remainder of the address (three octets for EUI-48 or five for EUI-64) are assigned by that organization in nearly any manner they please, subject to the constraint of uniqueness. A locally administered address is assigned to a device by a network administrator, overriding the burned-in address for physical devices.

Universally administered and locally administered addresses are distinguished by setting the second-least-significant bit of the first octet of the address. This bit is also referred to as the U/L bit, short for Universal/Local, which identifies how the address is administered.^{[7] [8]} If the bit is 0, the address is universally administered, which is why this bit is 0 in all OUIs. If it is 1, the address is locally administered. In the example address *06-00-00-00-00-00* the first octet is 06 (hex), the binary form of which is **00000110**, where the second-least-significant bit is **1**. Therefore, it is a locally administered address.^[9] Even though many hypervisors manage dynamic MAC addresses within their own OUI, often it is useful to create an entire unique MAC within the LAA range.^[10]

Local MAC ranges

x2 - xx - xx - xx - xx - xx
x6 - xx - xx - xx - xx - xx
xA - xx - xx - xx - xx - xx
xE - xx - xx - xx - xx - xx

Universal addresses that are administered locally

In virtualisation, hypervisors such as QEMU and Xen have their own OUIs. Each new virtual machine is started with a MAC address set by assigning the last three bytes to be unique on the local network. While this is local administration of MAC addresses, it is not an LAA in the IEEE sense.

An historical example of this hybrid situation is the DECnet protocol, where the universal MAC address (OUI AA-00-04, Digital Equipment Corporation) is administered locally. The DECnet software assigns the last three bytes of the MAC address to be *AA-00-04-00-XX-YY* where *XX-YY* reflects the DECnet network address *xx.yy* of the host. This eliminates the need for DECnet to have an address resolution protocol since the MAC address for any DECnet host can be determined from its DECnet address.

Unicast vs. multicast (I/G bit)

The least significant bit of an address's first octet is referred to as the I/G (Individual/Group) bit.^{[7][8]} When this bit is 0 (zero), the frame is meant to reach only one receiving NIC.^[11] This type of transmission is called unicast. A unicast frame is transmitted to all nodes within the collision domain. In a modern wired setting the collision domain usually is the length of the Ethernet cable between two network cards. In a wireless setting, the collision domain is all receivers that can detect a given wireless signal. If a switch does not know which port leads to a given MAC address, the switch will forward a unicast frame to all of its ports (except the originating port), an action known as unicast flood.^[12] Only the node with the matching hardware MAC address will accept the frame; network frames with non-matching MAC-addresses are ignored, unless the device is in promiscuous mode.

If the least significant bit of the first octet is set to 1, the frame will still be sent only once; however, NICs will choose to accept it based on criteria other than the matching of a MAC address: for example, based on a configurable list of accepted multicast MAC addresses. This is called multicast addressing.

The IEEE has built in several special address types to allow more than one network interface card to be addressed at one time:

- Packets sent to the broadcast address, all one bits, are received by all stations on a local area network. In hexadecimal the broadcast address would be FF:FF:FF:FF:FF:FF. A broadcast frame is flooded and is forwarded to and accepted by all other nodes.
- Packets sent to a multicast address are received by all stations on a LAN that have been configured to receive packets sent to that address.
- **Functional addresses** identify one or more Token Ring NICs that provide a particular service, defined in IEEE 802.5.

These are all examples of *group addresses*, as opposed to *individual addresses*; the least significant bit of the first octet of a MAC address distinguishes individual addresses from group addresses. That bit is set to 0 in individual addresses and set to 1 in group addresses. Group addresses, like individual addresses, can be universally administered or locally administered.

Applications

The following network technologies use the EUI-48 identifier format:

- IEEE 802 networks
 - Ethernet
 - 802.11 wireless networks (Wi-Fi)
 - Bluetooth
 - IEEE 802.5 Token Ring
- Fiber Distributed Data Interface (FDDI)
- Asynchronous Transfer Mode (ATM), switched virtual connections only, as part of an NSAP address
- Fibre Channel and Serial Attached SCSI (as part of a World Wide Name)
- The ITU-T G.hn standard, which provides a way to create a high-speed (up to 1 gigabit/s) local area network using existing home wiring (power lines, phone lines and coaxial cables). The G.hn Application Protocol Convergence (APC) layer accepts Ethernet frames that use the EUI-48 format and encapsulates them into G.hn Medium Access Control Service Data Units (MSDUs).

Every device that connects to an IEEE 802 network (such as Ethernet and WiFi) has an EUI-48 address. Common networked consumer devices such as PCs, smartphones and tablet computers use EUI-48 addresses.

EUI-64 identifiers are used in:

- IEEE 1394 (FireWire)
- IPv6 (Modified EUI-64 as the least-significant 64 bits of a unicast network address or link-local address when stateless address autoconfiguration is used.)^[13] IPv6 uses a modified EUI-64,

treats MAC-48 as EUI-48 instead (as it is chosen from the same address pool) and inverts the local bit.^[b] This results in extending MAC addresses (such as IEEE 802 MAC address) to modified EUI-64 using only FF-FE (and never FF-FF) and with the local bit inverted.^[14]

- ZigBee / 802.15.4 / 6LoWPAN wireless personal-area networks

Usage in hosts

On broadcast networks, such as Ethernet, the MAC address is expected to uniquely identify each node on that segment and allows frames to be marked for specific hosts. It thus forms the basis of most of the link layer (OSI Layer 2) networking upon which upper layer protocols rely to produce complex, functioning networks.

Many network interfaces support changing their MAC address. On most Unix-like systems, the command utility ifconfig may be used to remove and add link address aliases. For instance, the *active* ifconfig directive may be used on NetBSD to specify which of the attached addresses to activate.^[15] Hence, various configuration scripts and utilities permit the randomization of the MAC address at the time of booting or before establishing a network connection.

Changing MAC addresses is necessary in network virtualization. In MAC spoofing, this is practiced in exploiting security vulnerabilities of a computer system. Some modern operating systems, such as Apple iOS and Android, especially in mobile devices, are designed to randomize the assignment of a MAC address to network interface when scanning for wireless access points to avert tracking systems.^{[16][17]}

In Internet Protocol (IP) networks, the MAC address of an interface corresponding to an IP address may be queried with the Address Resolution Protocol (ARP) for IPv4 and the Neighbor Discovery Protocol (NDP) for IPv6, relating OSI Layer 3 addresses to Layer 2 addresses.

Tracking

Randomization

According to Edward Snowden, the US National Security Agency has a system that tracks the movements of mobile devices in a city by monitoring MAC addresses.^[18] To avert this practice, Apple has started using random MAC addresses in iOS devices while scanning for networks.^[16] Other vendors followed quickly. MAC address randomization during scanning was added in Android starting from version 6.0,^[17] Windows 10,^[19] and Linux kernel 3.18.^[20] The actual implementations of the MAC address randomization technique vary largely in different devices.^[21] Moreover, various flaws and shortcomings in these implementations may allow an attacker to track a device even if its MAC address is changed, for instance its probe requests' other elements,^{[22][23]} or their timing.^{[24][21]} If random MAC addresses are not used, researchers have confirmed that it is possible to link a real identity to a particular wireless MAC address.^{[25][26]}

Other information leakage

Using wireless access points in SSID-hidden mode (network cloaking), a mobile wireless device may not only disclose its own MAC address when traveling, but even the MAC addresses associated to SSIDs the device has already connected to, if they are configured to send these as part of probe request packets. Alternative modes to prevent this include configuring access points to be either in

beacon-broadcasting mode, or probe-response with SSID mode. In these modes, probe requests may be unnecessary, or sent in broadcast mode without disclosing the identity of previously-known networks.^[27]

Anonymization

Notational conventions

The standard (IEEE 802) format for printing EUI-48 addresses in human-friendly form is six groups of two hexadecimal digits, separated by hyphens (-) in transmission order (e.g. *01-23-45-67-89-AB*). This form is also commonly used for EUI-64 (e.g. *01-23-45-67-89-AB-CD-EF*).^[2] Other conventions include six groups of two hexadecimal digits separated by colons (:) (e.g. *01:23:45:67:89:AB*), and three groups of four hexadecimal digits separated by dots (.) (e.g. *0123.4567.89AB*); again in transmission order.^[28]

Bit-reversed notation

The standard notation, also called canonical format, for MAC addresses is written in transmission order with the least significant bit of each byte transmitted first, and is used in the output of the ifconfig, ip address, and ipconfig commands, for example.

However, since IEEE 802.3 (Ethernet) and IEEE 802.4 (Token Bus) send the bytes (octets) over the wire, left-to-right, with least significant bit in each byte first, while IEEE 802.5 (Token Ring) and IEEE 802.6 (FDDI) send the bytes over the wire with the most significant bit first, confusion may arise when an address in the latter scenario is represented with bits reversed from the canonical representation. For example, an address in canonical form *12-34-56-78-9A-BC* would be transmitted over the wire as bits 01001000 00101100 01101010 00011110 01011001 00111101 in the standard transmission order (least significant bit first). But for Token Ring networks, it would be transmitted as bits 00010010 00110100 01010110 01111000 10011010 10111100 in most-significant-bit first order. The latter might be incorrectly displayed as *48-2C-6A-1E-59-3D*. This is referred to as *bit-reversed order*, *non-canonical form*, *MSB format*, *IBM format*, or *Token Ring format*, as explained in RFC 2469 (<https://tools.ietf.org/html/rfc2469>).

See also

- Hot Standby Router Protocol
- MAC filtering
- Network management
- Sleep Proxy Service, which may spoof another device's MAC address during certain periods
- Transparent bridging
- Virtual Router Redundancy Protocol

Notes

- a. To convert a MAC-48 into an EUI-64, copy the OUI, append the two octets FF-FF and then copy the organization-specified extension identifier. To convert an EUI-48 into an EUI-64, the same process is used, but the sequence inserted is FF-FE.^[2] In both cases, the process could be trivially reversed when necessary. Organizations issuing EUI-64s were cautioned against issuing identifiers that could be confused with these forms.

- b. With local identifiers indicated with a zero bit, locally assigned EUI-64 begin with leading zeroes and it is easier for administrators to type locally assigned IPv6 addresses based on the modified EUI-64

References

1. "MAC Address Block Small (MA-S)" (<https://standards.ieee.org/products-services/regauth/oui36/index.html>). Retrieved 2019-02-24.
2. "Guidelines for Use of Extended Unique Identifier (EUI), Organizationally Unique Identifier (OUI), and Company ID (CID)" (<https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/tutorials/eui.pdf>) (PDF). IEEE Standards Association. IEEE. Retrieved 5 August 2018.
3. IEEE Std 802-2001 (<http://standards.ieee.org/getieee802/download/802-2001.pdf>) (PDF). The Institute of Electrical and Electronics Engineers, Inc. (IEEE). 2002-02-07. p. 19. ISBN 978-0-7381-2941-9. Retrieved 2011-09-08. "The universal administration of LAN MAC addresses began with the Xerox Corporation administering Block Identifiers (Block IDs) for Ethernet addresses."
4. "IEEE-SA - IEEE Registration Authority" (<https://standards.ieee.org/faqs/regauth.html#11>). standards.ieee.org. Retrieved 2018-09-20.
5. "IEEE-SA - IEEE Registration Authority" (<https://standards.ieee.org/faqs/regauth.html#13>). standards.ieee.org. Retrieved 2018-11-27.
6. "IEEE-SA - IEEE Registration Authority" (<https://standards.ieee.org/faqs/regauth.html#20>). standards.ieee.org. Retrieved 2018-09-20.
7. "Ethernet frame IG/LG bit explanation - Wireshark" (<https://networkengineering.stackexchange.com/a/69847>). networkengineering.stackexchange.com. Retrieved 2021-01-05.
8. "RFC 4291 IP Version 6 Addressing Architecture Appendix A" (<https://tools.ietf.org/html/rfc4291#page-20>). tools.ietf.org. Retrieved 2021-01-05.
9. "Standard Group MAC Addresses: A Tutorial Guide" (<https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/tutorials/macgrp.pdf>) (PDF). IEEE-SA. Retrieved 2018-09-20.
10. "Generating a New Unique MAC Address" (https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/virtualization_administration_guide/sect-virtualization-tips_and_tricks-generating_a_new_unique_mac_address). RedHat. Retrieved 2020-06-15.
11. "Guidelines for Fibre Channel Use of the Organizationally Unique Identifier (OUI)" (<https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/tutorials/fibre.pdf>) (PDF). IEEE-SA. Retrieved 2018-10-11.
12. "Overview of Layer 2 Switched Networks and Communication | Getting Started with LANs | Cisco Support Community | 5896 | 68421" (<https://supportforums.cisco.com/document/68421/overview-layer-2-switched-networks-and-communication>). supportforums.cisco.com. 2011-07-23. Retrieved 2016-05-17.
13. S. Thomson; T. Narten; T. Jinmei (September 2007). IPv6 Stateless Address Autoconfiguration (<https://tools.ietf.org/html/rfc4862>). Network Working Group, IETF. doi:10.17487/RFC4862 (<https://doi.org/10.17487%2FRFC4862>). RFC 4862 (<https://tools.ietf.org/html/rfc4862>).
14. IANA Considerations and IETF Protocol Usage for IEEE 802 Parameters (<https://tools.ietf.org/html/rfc7042#section-2.2.1>). IETF. September 2008. sec. 2.2.1. doi:10.17487/RFC7042 (<https://doi.org/10.17487%2FRFC7042>). RFC 7042 (<https://tools.ietf.org/html/rfc7042>).
15. "ifconfig(8) manual page" (<https://netbsd.gw.com/cgi-bin/man-cgi?ifconfig++NetBSD-current>). Retrieved 16 October 2016.
16. Mamiit, Aaron (2014-06-12). "Apple Implements Random MAC Address on iOS 8. Goodbye, Marketers" (<https://www.techtimes.com/articles/8233/20140612/apple-implements-random-mac-address-on-ios-8-goodbye-marketers.htm>). Tech Times. Retrieved 2014-12-01.
17. "Android 6.0 Changes" (<https://developer.android.com/about/versions/marshmallow/android-6.0-changes>). Android developers. Retrieved 2018-08-22.

18. Bamford, James (2014-08-13). "The Most Wanted Man in the World" (<https://www.wired.com/2014/08/edward-snowden/>). Wired: 4. Retrieved 2014-12-01.
19. Winkey Wang. "Wireless networking in Windows 10" (<https://channel9.msdn.com/Events/WinHEC/2015/WHT201>).
20. Emmanuel Grumbach. "iwifi: mvm: support random MAC address for scanning" (<https://github.com/torvalds/linux/commit/effd05ac479b80641835f9126bbe93146686c2b8>). Linux commit effd05ac479b. Retrieved 2018-08-22.
21. Célestin Matte (December 2017). Wi-Fi Tracking: Fingerprinting Attacks and Counter-Measures (<https://hal.archives-ouvertes.fr/tel-01659783/>). 2017 (Theses). Université de Lyon. Retrieved 2018-08-22.
22. Vanhoef Mathy and Matte Célestin and Cunche Mathieu and Cardoso Leonardo and Piessens Frank (2016-05-30). "Why MAC address randomization is not enough: An analysis of Wi-Fi network discovery mechanisms" (<https://hal.inria.fr/hal-01282900>). Retrieved 2018-08-22.
23. Martin Jeremy and Mayberry Travis and Donahue Collin and Foppe Lucas and Brown Lamont and Riggins Chadwick and Rye Erik C and Brown Dane. "A study of MAC address randomization in mobile devices and when it fails" (<https://www.degruyter.com/downloadpdf/j-popets.2017.2017.issue-4/popets-2017-0054/popets-2017-0054.pdf>) (PDF). 2017. Retrieved 2018-08-22.
24. Matte Célestin and Cunche Mathieu and Rousseau Franck and Vanhoef Mathy (2016-07-18). "Defeating MAC address randomization through timing attacks" (<https://hal.inria.fr/hal-01330476>). Retrieved 2018-08-22.
25. Cunche, Mathieu. "I know your MAC Address: Targeted tracking of individual using Wi-Fi" (https://hal.archives-ouvertes.fr/file/index/docid/858324/filename/Wi-Fi_Stalking.pdf) (PDF). 2013. Retrieved 19 December 2014.
26. Muhammad Hassan. "How to Find iPhone MAC Address" (<https://itechbeast.com/iphone-mac-address/>).
27. "Hidden network no beacons" (<https://security.stackexchange.com/questions/61576/hidden-network-no-beacons>). security.stackexchange.com. Retrieved 16 October 2016.
28. "Agentless Host Configuration Scenario" (https://web.archive.org/web/20160802102024/http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4-2/configuration/guide/acs42_config_guide/noagent.html#wp1010965). Configuration Guide for Cisco Secure ACS 4.2. Cisco. February 2008. Archived from the original (http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/configuration/guide/noagent.html#wp1017547) on 2016-08-02. Retrieved 2015-09-19. "You can enter the MAC address in the following formats for representing MAC-48 addresses in human-readable form: six groups of two hexadecimal digits, separated by hyphens (-) in transmission order,[...]six groups of two separated by colons (:),[...]three groups of four hexadecimal digits separated by dots (...)"

External links

- IEEE Registration Authority Tutorials (<https://standards.ieee.org/products-services/regauth/tut/index.html>)
- IEEE Registration Authority - Frequently Asked Questions (<https://standards.ieee.org/faqs/regauth.html>)
- IEEE Public OUI and Company ID, etc. Assignment lookup (<https://regauth.standards.ieee.org/standards-ra-web/pub/view.html#registries>)
- IEEE Public OUI/MA-L list (<http://standards-oui.ieee.org/oui/oui.txt>)
- IEEE Public OUI-28/MA-M list (<http://standards-oui.ieee.org/oui28/mam.txt>)
- IEEE Public OUI-36/MA-S list (<http://standards-oui.ieee.org/oui36/oui36.txt>)
- IEEE Public IAB list (<http://standards-oui.ieee.org/iab/iab.txt>)

- IEEE IAB and OUI MAC Address Lookup Database and API (<https://www.macvendorlookup.com/>)
 - RFC 7042. IANA Considerations and IETF Protocol and Documentation Usage for IEEE 802 Parameters (<https://tools.ietf.org/html/rfc7042>)
 - IANA list of Ethernet Numbers (<https://www.iana.org/assignments/ethernet-numbers/ethernet-numbers.xhtml>)
 - Wireshark's OUI Lookup Tool (<https://www.wireshark.org/tools/oui-lookup.html>) and MAC address list (https://code.wireshark.org/review/gitweb?p=wireshark.git;a=blob_plain;f=manuf)
-

Retrieved from "https://en.wikipedia.org/w/index.php?title=MAC_address&oldid=1001054538"

This page was last edited on 18 January 2021, at 01:26 (UTC).

Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.