DevNet Associate v1.0

⌂ / Network Fundamentals / Internetwork Layer

Internetwork Layer

5.3.1

Understanding the Internetwork Layer

Interconnected networks have to have ways to communicate. Internetworking provides that "between" (inter) networks communication method. This topic describes addressing and routing.

5.3.2

IPv4 Addresses

Every device on a network has a unique IP address. An IP address and a MAC address are used for access and communication across all network devices. Without IP addresses there would be no internet.

Despite the introduction of IPv6, IPv4 continues to route most internet traffic today. During recent years, more traffic is being sent over IPv6 due to the exhaustion of IPv4 addresses and the proliferation of mobile and Internet of Things (IoT) devices.

An IPv4 address is 32 bits, with each octet (8 bits) represented as a decimal value separated by a dot. This representation is called dotted decimal notation. For example, 192.168.48.64 and 64.100.36.254 are IPv4 addresses represented in dotted decimal notation. The table shows the binary value for each octet.

Value	**192**	**168**	**48**	**64**
Binary	11000000	10101000	00110000	01000000
Value	**64**	**100**	**36**	**254**
Binary	01000000	01100100	00100100	11111110

The IPv4 subnet mask (or prefix length) is used to differentiate the network portion from the host portion of an IPv4 address. A subnet mask contains four bytes and can be written in the same format as an IP address. In a valid subnet mask, the most significant bits starting at the left most must be set to 1. These bits are the network portion of the subnet mask. The bits set to 0 are the host portion of the mask

For this example, look at 203.0.113.0/24. The network's IPv4 address is 203.0.113.0 with a subnet mask 255.255.255.0. The last octet of the subnet mask has all 8 bits available for host IPv4 addresses, which means that on the network 203.0.113.0/24, there can be up to 2^8 (256) available subnet addresses.

Two IPv4 addresses are in use by default and cannot be assigned to devices:

- 203.0.113.0 is the network address
- 203.0.113.255 is the broadcast address

Therefore, there are 254 (256 - 2) host IP addresses available, and the range of addresses available for hosts would be 203.0.113.1 to 203.0.113.254.

There are three types of IPv4 addresses:

- **Network address** - A network address is an address that represents a specific network and contains all 0 bits in the host portion of the address.
- **Host addresses** - Host addresses are addresses that can be assigned to a device such as a host computer, laptop, smart phone, web camera, printer, router, etc. Host addresses contain a least one 0 bit and one 1 bit in the host portion of the address.
- **Broadcast address** - A broadcast address is an address that is used when it is required to reach all devices on the IPv4 network. It contains all 1 bits in the host portion of the address.

A network can be divided into smaller networks called subnets. Subnets can be provided to individual organizational units, such as teams or business departments, to simplify the network and potentially make departmental data private. The subnet provides a specific range of IP addresses for a group of hosts to use. Every network is typically a subnet of a larger network.

For example, the network IPv4 network address is 192.168.2.0/24. The /24 (255.255.255.0) subnet mask means that the last octet has 8 bits available for host addresses. You can borrow from the host portion to create subnets. For example, you need to use three bits to create eight subnets (2^3 = 8). This leaves the remaining five bits for the hosts (2^5 = 32).

This can be more easily visualized when showing the subnet mask in binary format.

- /24 subnet mask: 11111111.11111111.11111111.00000000
- Modified /27 subnet mask: 11111111.11111111.11111111.11100000

Because you need to create eight subnets, you designate three bits in the last octet for subnet use. The remaining five bits are for the hosts, and provide each subnet with 32 IP addresses.

The following table lists the network address, broadcast address, and available host address range for each subnet.

Subnet	Network Address	Broadcast Address	Available Host Address Range
Subnet 1	192.168.2.0	192.168.2.31	192.168.2.1 to 192.168.2.30
Subnet 2	192.168.2.32	192.168.2.63	192.168.2.33 to 192.168.2.62
Subnet 3	192.168.2.64	192.168.2.95	192.168.2.65 to 192.168.2.94
Subnet 4	192.168.2.96	192.168.2.127	192.168.2.97 to 192.168.2.126
Subnet 5	192.168.2.128	192.168.2.159	192.168.2.129 to 192.168.2.158
Subnet 6	192.168.2.160	192.168.2.191	192.168.2.161 to 192.168.2.190
Subnet 7	192.168.2.192	192.168.2.223	192.168.2.193 to 192.168.2.222
Subnet 8	192.168.2.224	192.168.2.255	192.168.2.225 to 192.168.2.254

Notice the allocation for subnets and hosts specified for each row. You should now understand how designating bits to create subnets reduces the number of hosts available for each subnet. The number of hosts available per subnet takes into account that network and broadcast addresses each require an IP address. The more bits you use to create subnets, the fewer bits you have for hosts per subnet.

The table below shows the various options if you have a /24 subnet mask.

Subnet Mask	Binary	CIDR	Subnets	Hosts per Subnet
255.255.255.255	11111111.11111111.11111111.11111111	/32	None	N/A
255.255.255.254	11111111.11111111.11111111.11111110	/31	128	N/A
255.255.255.252	11111111.11111111.11111111.11111100	/30	64	2
255.255.255.248	11111111.11111111.11111111.11111000	/29	32	6
255.255.255.240	11111111.11111111.11111111.11110000	/28	16	14
255.255.255.224	11111111.11111111.11111111.11100000	/27	8	30
255.255.255.192	11111111.11111111.11111111.11000000	/26	4	62
255.255.255.128	11111111.11111111.11111111.10000000	/25	2	126
255.255.255.0	11111111.11111111.11111111.00000000	/24	1	254

Due to the depletion of IPv4 addresses, internally most addresses use private IPv4 addresses (RFC 1918). Use of variable-length subnet masks (VLSM) can also help support more efficient use of IPv4 address space. Originally used when IPv4 addresses were classful (Class A, B, C). VLSM is a method of dividing a single network (or subnet) using different subnet masks to provide subnets with different number of host addresses.

Network Address and Prefix RFC 1918 Private Address Range

- 10.0.0.0/8 10.0.0.0 - 10.255.255.255
- 172.16.0.0/12 172.16.0.0 - 172.31.255.255
- 192.168.0.0/16 192.168.0.0 - 192.168.255.255

Devices using private IPv4 addresses are able to access the internet via Network Address Translation (NAT) and Port Address Translation (PAT). Outgoing data from your device is sent through a router, which maps your device's private IPv4 address to a public IPv4 address. When the data returns to that router, it looks up your device's private IP address and routes it to its destination.

5.3.3

IPv6 Addresses

IPv6 is designed to be the successor to IPv4. IPv6 has a larger 128-bit address space, providing 340 undecillion (i.e., 340 followed by 36 zeroes) possible addresses. However, IPv6 is more than just larger addresses.

When the IETF began its development of a successor to IPv4, it used this opportunity to fix the limitations of IPv4 and included enhancements. One example is Internet Control Message Protocol version 6 (ICMPv6), which includes address resolution and address autoconfiguration features not found in ICMP for IPv4 (ICMPv4).

The depletion of IPv4 address space has been the motivating factor for moving to IPv6. As Africa, Asia, and other areas of the world become more connected to the internet, there are not enough IPv4 addresses to accommodate this growth.

IPv6 is described initially in RFC 2460. Further RFCs describe the architecture and services supported by IPv6.

The architecture of IPv6 has been designed to allow existing IPv4 users to transition easily to IPv6 while providing services such as end-to-end security, quality of service (QoS), and globally unique addresses. The larger IPv6 address space allows networks to scale and provide global reachability. The simplified IPv6 packet header format handles packets more efficiently. IPv6 prefix aggregation, simplified network renumbering, and IPv6 site multihoming capabilities provide an IPv6 addressing hierarchy that allows for more efficient routing. IPv6 supports widely deployed routing protocols such as Routing Information Protocol (RIP), Integrated Intermediate System-to-Intermediate System (IS-IS), OSPF, and multiprotocol

BGP (mBGP). Other available features include stateless autoconfiguration and an increased number of multicast addresses.

Private addresses in combination with Network Address Translation (NAT) have been instrumental in slowing the depletion of IPv4 address space. However, NAT is problematic for many applications, creates latency, and has limitations that severely impede peer-to-peer communications. IPv6 address space eliminates the need for private addresses; therefore, IPv6 enables new application protocols that do not require special processing by border devices at the edge of networks.

With the ever-increasing number of mobile devices, mobile providers have been leading the way with the transition to IPv6. The top two mobile providers in the United States report that over 90% of their traffic is over IPv6. Most top ISPs and content providers such as YouTube, Facebook, and NetFlix, have also made the transition. Many companies like Microsoft, Facebook, and LinkedIn are transitioning to IPv6-only internally. In 2018, broadband ISP Comcast reported a deployment of over 65% and British Sky Broadcasting over 86%.

IPv6 addresses are represented as a series of 16-bit hexadecimal fields (hextet) separated by colons (:) in the format: x:x:x:x:x:x:x:x. The preferred format includes all the hexadecimal values. There are two rules that can be used to reduce the representation of the IPv6 address:

1. Omit leading zeros in each hextet
2. Replace a single string of all-zero hextets with a double colon (::)

Leading zeros in each 16-bit hextet can be omitted. For example:

Preferred

2001:0db8:0000:1111:0000:0000:0000:0200

No leading 0s

2001:db8:0:1111:0:0:0:200

IPv6 addresses commonly contain successive hexadecimal fields of zeros. Two colons (::) may be used to compress successive hexadecimal fields of zeros at the beginning, middle, or end of an IPv6 address (the colons represent successive hexadecimal fields of zeros).

A double colon (::) can replace any single, contiguous string of one or more 16-bit hextets consisting of all zeros. For example, the following preferred IPv6 address can be formatted with no leading zeros.

Preferred

2001:0db8:0000:1111:0000:0000:0000:0200

No leading 0s

2001:db8:0:1111::200

Two colons (::) can be used only once in an IPv6 address to represent the longest successive hexadecimal fields of zeros. Hexadecimal letters in IPv6 addresses are not case-sensitive according to RFC 5952. The table below lists compressed IPv6 address formats:

IPv6 address type	Preferred format	Compressed format
Unicast	2001:0:0:0:db8:800:200c:417a	2001::db8:800:200c:417a
Multicast	ff01:0:0:0:0:0:0:101	ff01::101
Loopback	0:0:0:0:0:0:0:1	::1
Unspecified	0:0:0:0:0:0:0:0	::

The unspecified address listed in the table above indicates the absence of an IPv6 address or when the IPv6 address does not need to be known. For example, a newly initialized device on an IPv6 network may use the unspecified address as the source address in its packets until it receives or creates its own IPv6 address.

An IPv6 address prefix, in the format *ipv6-prefix/prefix-length*, can be used to represent bit-wise contiguous blocks of the entire address space. The prefix length is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). For example, 2001:db8:8086:6502::/32 is a valid IPv6 prefix.

5.3.4

IPv6 Unicast Addresses

An IPv6 unicast address is an identifier for a single interface, on a single device. A packet that is sent to a unicast address is delivered to the interface identified by that address. There are several types of IPv6 unicast addresses including:

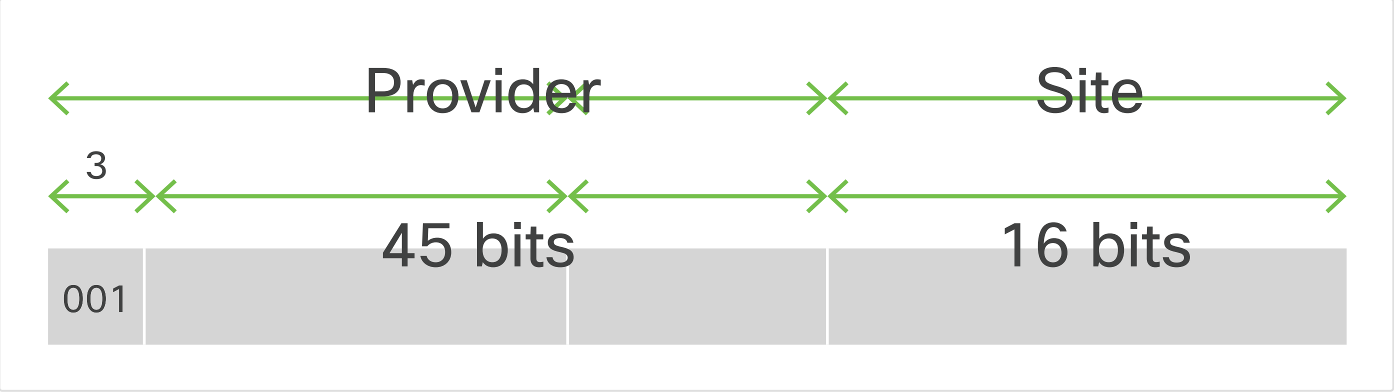
- Global unicast addresses
- Link-local addresses
- Unique local addresses
- Multicast addresses

Note: There are other types of IPv6 unicast addresses, but these four are the most significant to our discussion.

Global Unicast Addresses

A global unicast address (GUA) is an IPv6 similar to a public IPv4 address. IPv6 global unicast addresses are globally unique and routable on the IPv6 internet. The Internet Committee for Assigned Names and Numbers (ICANN), the operator for the Internet Assigned Numbers Authority (IANA), allocates IPv6 address blocks to the five Regional Internet Registries (RIRs). Currently, only GUAs with the first three bits (001), which converts to 2000::/3, are being assigned, as shown in the figure.

IPv6 GUA Format



The parts of the GUA in the figure above are as follows:

- **Global Routing Prefix** - The global routing prefix is the prefix, or network, portion of the address that is assigned by the provider such as an ISP, to a customer or site. It is common for some ISPs to assign a /48 global routing prefix to its customers, which always includes the first 3 bit (001) shown in the figure. The global routing prefix will usually vary depending on the policies of the ISP.
  For example, the IPv6 address 2001:db8:acad::/48 has a global routing prefix that indicates that the first 48 bits (3 hextets or 2001:db8:acad) is how the ISP knows of this prefix (network). The double colon (::) following the /48 prefix length means the rest of the address contains all 0s. The size of the global routing prefix determines the size of the subnet ID.
- **Subnet ID** - The Subnet ID field is the area between the Global Routing Prefix and the Interface ID. Unlike IPv4, where you must borrow bits from the host portion to create subnets, IPv6 was designed with subnetting in mind. The Subnet ID is used by an organization to identify subnets within its site. The larger the Subnet ID, the more subnets available.
  For example, if the prefix has a /48 Global Routing Prefix, and using a typical /64 prefix length, the first four hextets are for the network portion of the address, with the fourth hextet indicating the Subnet ID. The remaining four hextets are for the Interface ID.
- **Interface ID** - The IPv6 Interface ID is equivalent to the host portion of an IPv4 address. The term Interface ID is used because a single device may have multiple interfaces, each having one or more IPv6 addresses. It is strongly recommended that in most cases /64 subnets should be used, which creates a 64-bit interface ID. A 64-bit interface ID allows for 18 quintillion devices or hosts per subnet. A /64 subnet or prefix (Global Routing Prefix + Subnet ID) leaves 64 bits for the interface ID. This is recommended to allow devices enabled with Stateless Address Autoconfiguration (SLAAC) to create their own 64-bit interface ID. It also makes developing an IPv6 addressing plan simple and effective.

The GUA is not a requirement; however every IPv6-enabled network interface must have an Link-local Address (LLA).

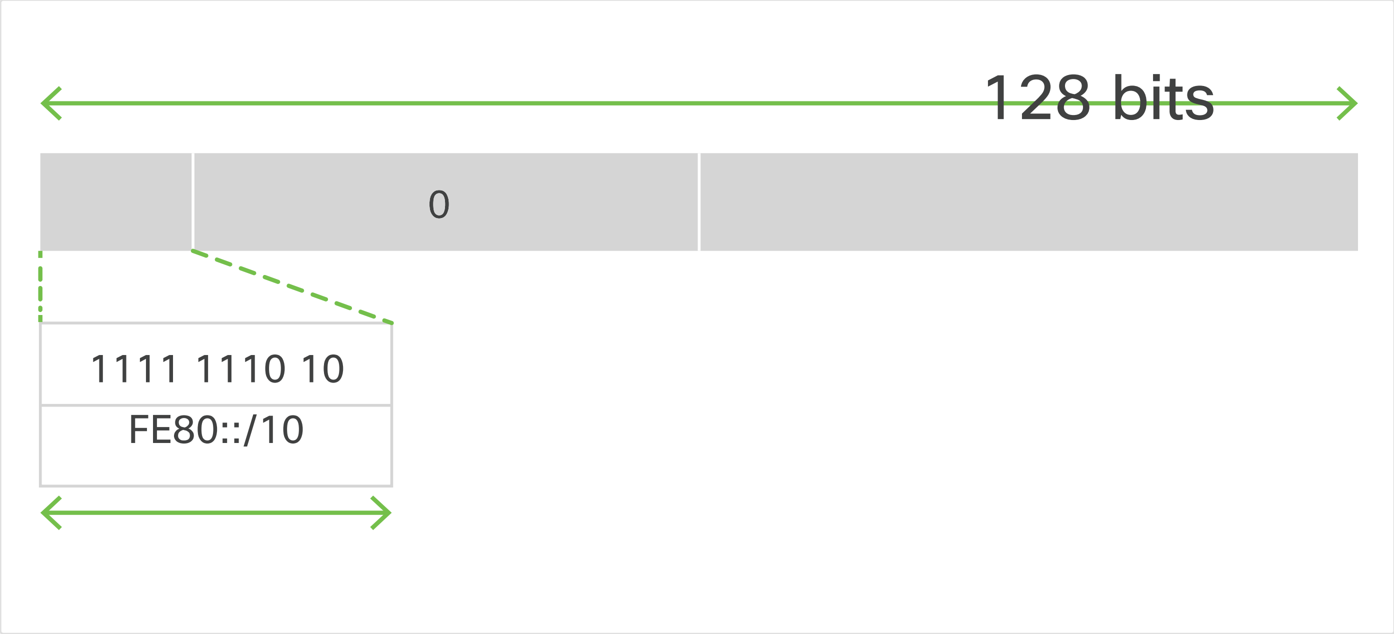
Link-Local Addresses

An IPv6 Link-local Address (LLA) enables a device to communicate with other IPv6-enabled devices on the same link and only on that link (subnet). Packets with a source or destination LLA cannot be routed beyond the link from which the packet originated.

If an LLA is not configured manually on an interface, the device will automatically create its own without communicating with a DHCP server. IPv6-enabled hosts create an IPv6 LLA even if the device has not been assigned a global unicast IPv6 address. This allows IPv6-enabled devices to communicate with other IPv6-enabled devices on the same subnet. This includes communication with the default gateway (router).

The format for an IPv6 LLA is shown in the figure.

IPv6 LLA Format



IPv6 LLAs are in the fe80::/10 range. The /10 indicates that the first 10 bits are **1111 1110 10.** The first hextet has the following range:

1111 1110 1000 0000 (fe80) to

1111 1110 1011 1111 (febf)

IPv6 devices must not forward packets that have source or destination LLAs to other links.

Unique Local Addresses

Unique local addresses (range fc00::/7 to fdff::/7) are not yet commonly implemented. However, unique local addresses may eventually be used to address devices that should not be accessible from the outside, such as internal servers and printers.

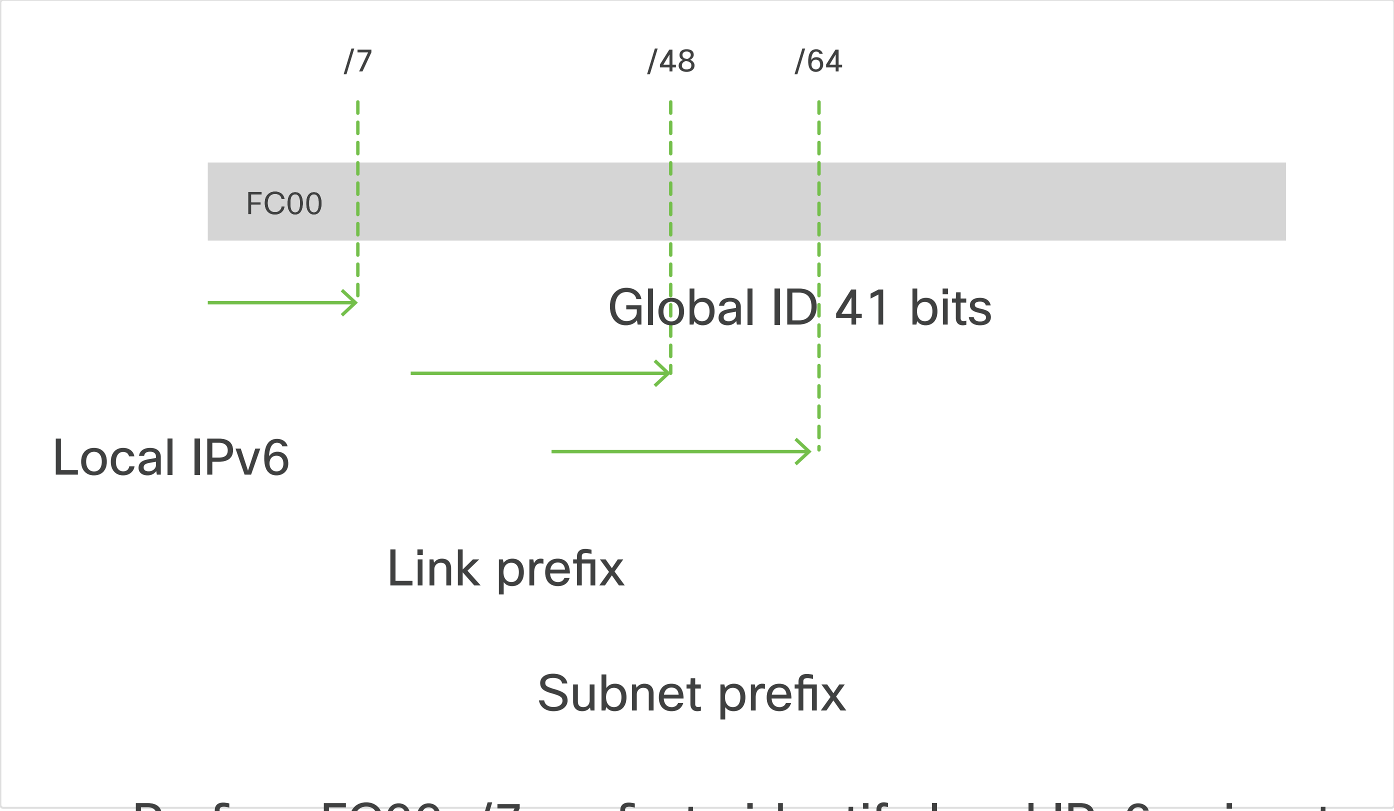
The IPv6 unique local addresses have some similarity to RFC 1918 private addresses for IPv4, but there are significant differences:

- Unique local addresses are used for local addressing within a site or between a limited number of sites.
- Unique local addresses can be used for devices that will never need to access another network.
- Unique local addresses are not globally routed or translated to a global IPv6 address.

Note: Many sites also use the private nature of RFC 1918 addresses to attempt to secure or hide their network from potential security risks. However, this was never the intended use of these technologies, and the IETF has always recommended that sites take the proper security precautions on their internet-facing router.

The figure shows the structure of a unique local address.

IPv6 Unique Local Address Format



Prefix - FC00::/7 prefix to identify local IPv6 unicast add
Global ID - 41-bit global identifier used to created a glol
Subnet ID - 16-bit subnet ID is an identifier of a subnet v
Interface ID - 64-bit ID

Multicast Addresses

There are no broadcast addresses in IPv6. IPv6 multicast addresses are used instead of broadcast addresses. IPv6 multicast addresses are similar to IPv4 multicast addresses. Recall that a multicast address is used to send a single packet to one or more destinations (multicast group). IPv6 multicast addresses have the prefix ff00::/8.

Note: Multicast addresses can only be destination addresses and not source addresses.

There are two types of IPv6 multicast addresses:

- Well-known multicast addresses
- Solicited node multicast addresses

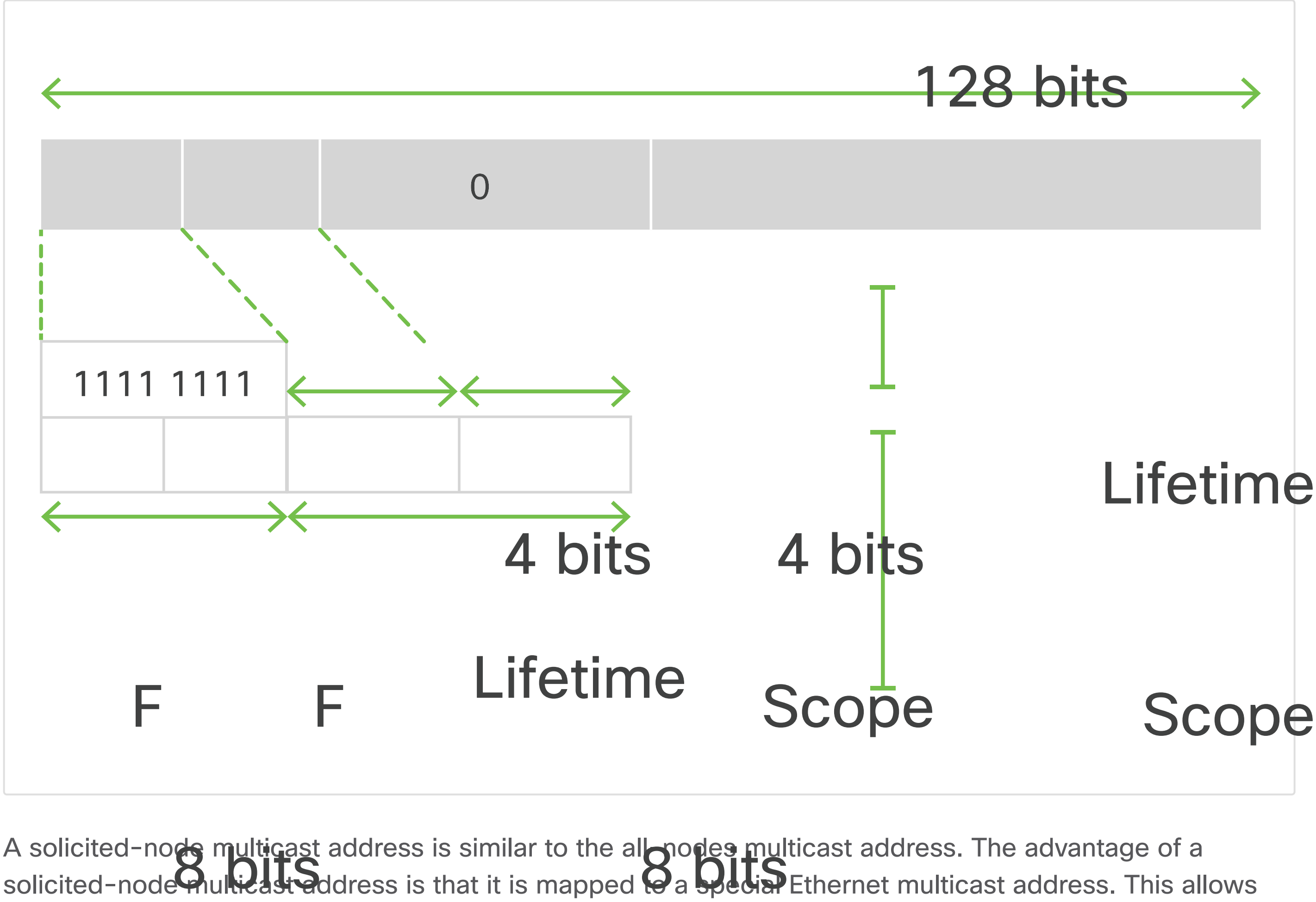
Well-known IPv6 multicast addresses are assigned. Assigned multicast addresses are reserved multicast addresses for predefined groups of devices. An assigned multicast address is a single address used to reach a group of devices running a common protocol or service. Assigned multicast addresses are used in context with specific protocols such as DHCPv6.

These are two common IPv6 assigned multicast groups:

- **ff02::1 All-nodes multicast group** – This is a multicast group that all IPv6-enabled devices join. A packet sent to this group is received and processed by all IPv6 interfaces on the link or network. This has the same effect as a broadcast address in IPv4.
- **ff02::2 All-routers multicast group** – This is a multicast group that all IPv6 routers join. A router becomes a member of this group when it is enabled as an IPv6 router with the **ipv6 unicast-routing** global configuration command. A packet sent to this group is received and processed by all IPv6 routers on the link or network.

The format for an IPv6 multicast address is shown in the figure.

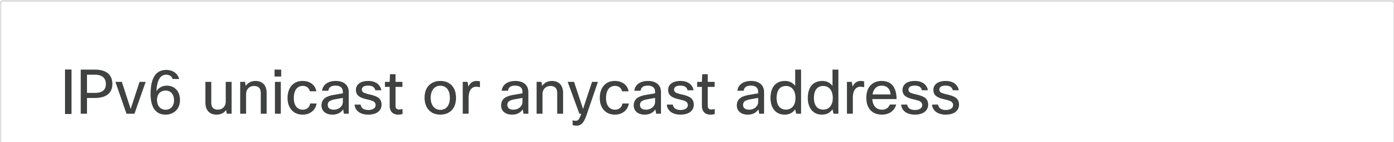
IPv6 Multicast Address Format

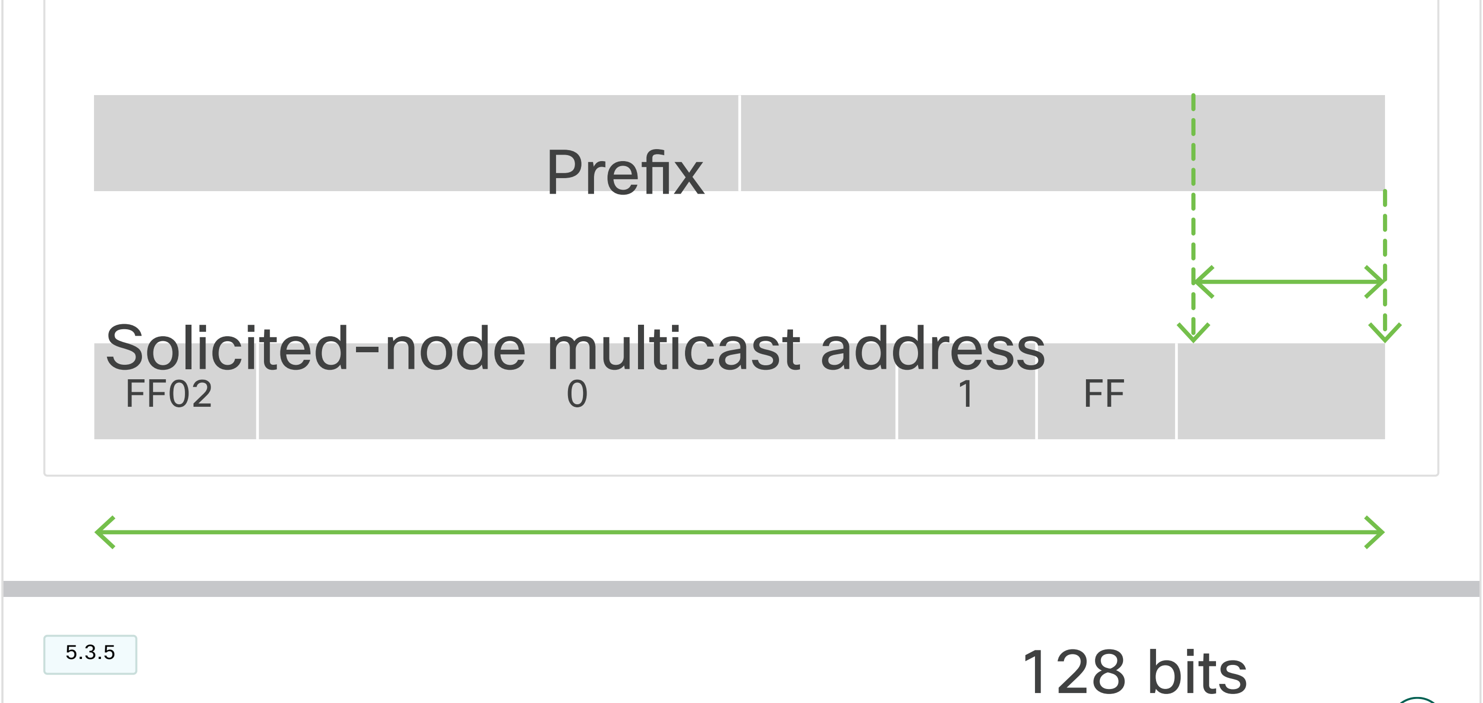


A solicited-node multicast address is similar to the all-nodes multicast address. The advantage of a solicited-node multicast address is that it is mapped to a special Ethernet multicast address. This allows the Ethernet NIC to filter the frame by examining the destination MAC address without sending it to the IPv6 process to see if the device is the intended target of the IPv6 packet.

The format for an IPv6 solicited-node multicast address is shown in the figure.

IPv6 Solicited-Node Address Format





5.3.5

Routers and Routing

Recall that a router is a networking device that functions at the internet layer of the TCP/IP model or Layer 3 network layer of the OSI model. Routing involves the forwarding packets between different networks. Routers use a routing table to route between networks. A router generally has two main functions: Path determination, and Packet routing or forwarding.

Path Determination

Path determination is the process through which a router uses its routing table to determine where to forward packets. Each router maintains its own local routing table, which contains a list of all the destinations that are known to the router and how to reach those destinations. When a router receives an incoming packet on one of its interfaces, it checks the destination IP address in the packet and looks up the best match between the destination address and the network addresses in its routing table. A matching entry indicates that the destination is directly connected to the router or that it can be reached by forwarding the packet to another router. That router becomes the next-hop router towards the final destination of the packet. If there is no matching entry, the router sends the packet to the default route. If there is no default route, the router drops the packet.

Packet Forwarding

After the router determines the correct path for a packet, it forwards the packet through a network interface towards the destination network.

A routing table might look like the following:

Network	Interface or Next Hop
10.9.2.0/24	directly connected: Gi0/0

Network	Interface or Next Hop
10.9.1.0/24	directly connected: Gi0/1
10.5.3.0/24	directly connected: Se0/0/1
10.8.3.0/24	via 10.9.2.2 (next-hop router)

As you can see, each row in the routing table lists a destination network and the corresponding interface or next-hop address. For directly connected networks, it means the router has an interface that is part of that network. For example, assume that the router receives a packet on its Serial 0/0/1 interface with a destination address of 10.9.1.5. The router looks up the destination address in its routing table and decides to forward the packet out its interface GigabitEthernet 0/1 towards its destination. Following the same logic, assume the router receives a packet with a destination address in the 10.8.3.0 network on its GigabitEthernet0/1 interface. Doing a routing table lookup, the router decides to forward this packet out its GigabitEthernet0/0 interface that connects it to the next-hop router towards the final destination in the 10.8.3.0 network.

A routing table may contain the following types of entries:

- **Directly connected networks** - These network route entries are active router interfaces. Routers add a directly connected route when an interface is configured with an IP address and is activated. Each router interface is connected to a different network segment.
- **Static routes** - These are routes that are manually configured by the network administrator. Static routes work relatively well for small networks that do not change in time, but in large dynamic networks they have many shortcomings.
- **Dynamic routes** - These are routes learned automatically when a dynamic routing protocol is configured and a neighbor relationship to other routers is established. The reachability information in this case is dynamically updated when a change in the network occurs. Several routing protocols with different advantages and shortcomings have been developed through the years. Routing protocols are extensively used throughout networks deployed all over the world. Examples of routing protocols include OSPF, EIGRP, IS-IS, and BGP.
- **Default routes** - Default routes are either manually entered, or learned through a dynamic routing protocol. Default routes are used when no explicit path to a destination is found in the routing table. They are a gateway of last resort option instead of just dropping the packet.

‹ 5.2 Network Interface Layer

5.4 Network Devices ›