IPv6 Basics



Huawei Technologies Co., Ltd.

|  |
| --- |
| **Copyright © Huawei Technologies Co., Ltd. 2020. All rights reserved.**  No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.  **Trademarks and Permissions**  HW_POS_RBG_Vertical-150ppi.png and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.  All other trademarks and trade names mentioned in this document are the property of their respective holders.  **Notice**  The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.  The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. |

|  |  |
| --- | --- |
| Huawei Technologies Co., Ltd. | |
| Address: | Huawei Industrial Base  Bantian, Longgang  Shenzhen 518129  People's Republic of China |
| Website: | <https://e.huawei.com/> |

**Huawei Certification System**

Huawei Certification follows the "platform + ecosystem" development strategy, which is a new collaborative architecture of ICT infrastructure based on "Cloud-Pipe-Terminal". Huawei has set up a complete certification system consisting of three categories: ICT infrastructure certification, platform and service certification, and ICT vertical certification. It is the only certification system that covers all ICT technical fields in the industry. Huawei offers three levels of certification: Huawei Certified ICT Associate (HCIA), Huawei Certified ICT Professional (HCIP), and Huawei Certified ICT Expert (HCIE). Huawei Certification covers all ICT fields and adapts to the industry trend of ICT convergence. With its leading talent development system and certification standards, it is committed to fostering new ICT talent in the digital era, and building a sound ICT talent ecosystem.

Huawei Certified ICT Associate-Datacom (HCIA-Datacom) is designed for Huawei's frontline engineers and anyone who want to understand Huawei's datacom products and technologies. The HCIA-Datacom certification covers routing and switching principles, basic WLAN principles, network security basics, network management and O&M basics, SDN and programmability and automation basics.

The Huawei certification system introduces the industry, fosters innovation, and imparts cutting-edge datacom knowledge.



Contents

[1 IPv6 Basics 1](#_Toc60149016)

[1.1 Foreword 1](#_Toc60149017)

[1.2 Objectives 1](#_Toc60149018)

[1.3 IPv6 Overview 1](#_Toc60149019)

[1.3.1 IPv4 Status 1](#_Toc60149020)

[1.3.2 Why IPv6? 2](#_Toc60149021)

[1.3.3 IPv6 Advantages 3](#_Toc60149022)

[1.3.4 Basic IPv6 Header 4](#_Toc60149023)

[1.3.5 IPv6 Extension Header 6](#_Toc60149024)

[1.3.6 IPv6 Packet Processing Mechanism 8](#_Toc60149025)

[1.3.7 IPv6 Address 8](#_Toc60149026)

[1.3.8 IPv6 Address Abbreviation Specifications 8](#_Toc60149027)

[1.3.9 IPv6 Address Classification 9](#_Toc60149028)

[1.3.10 IPv6 Unicast Address Format 10](#_Toc60149029)

[1.3.11 Interface ID of an IPv6 Unicast Address 10](#_Toc60149030)

[1.3.12 Common IPv6 Unicast Address - GUA 11](#_Toc60149031)

[1.3.13 Common IPv6 Unicast Address - ULA 12](#_Toc60149032)

[1.3.14 Common IPv6 Unicast Address - LLA 13](#_Toc60149033)

[1.3.15 IPv6 Multicast Address 14](#_Toc60149034)

[1.3.16 Solicited-Node Multicast Address 15](#_Toc60149035)

[1.3.17 IPv6 Anycast Address 16](#_Toc60149036)

[1.4 IPv6 Address Configuration 17](#_Toc60149037)

[1.4.1 IPv6 Addresses of Hosts and Routers 17](#_Toc60149038)

[1.4.2 Service Process of IPv6 Unicast Addresses 17](#_Toc60149039)

[1.4.3 NDP 18](#_Toc60149040)

[1.4.4 Dynamic IPv6 Address Configuration 18](#_Toc60149041)

[1.4.5 DAD 20](#_Toc60149042)

[1.4.6 Address Resolution 21](#_Toc60149043)

[1.5 Typical IPv6 Configuration Examples 21](#_Toc60149044)

[1.5.1 Basic IPv6 Configurations 21](#_Toc60149045)

[1.5.2 Example: Configuring a Small IPv6 Network 22](#_Toc60149046)

[1.6 Quiz 25](#_Toc60149047)

[1.7 Summary 25](#_Toc60149048)

# IPv6 Basics

## Foreword

In the 1980s, the Internet Engineering Task Force (IETF) released RFC 791 – Internet Protocol, which marks the standardization of IPv4. In the following decades, IPv4 has become one of the most popular protocols. Numerous people have developed various applications based on IPv4 and made various supplements and enhancements to IPv4, enabling the Internet to flourish.

However, with the expansion of the Internet and the development of new technologies such as 5G and Internet of Things (IoT), IPv4 faces more and more challenges. It is imperative to replace IPv4 with IPv6.

This course describes the reasons for IPv4-to-IPv6 transition and basic IPv6 knowledge.

## Objectives

On completion of this course, you will be able to:

Summarize the advantages of IPv6 over IPv4.

Describe the basic concepts of IPv6.

Describe the formats and functions of IPv6 packet headers.

Describe the IPv6 address format and address types.

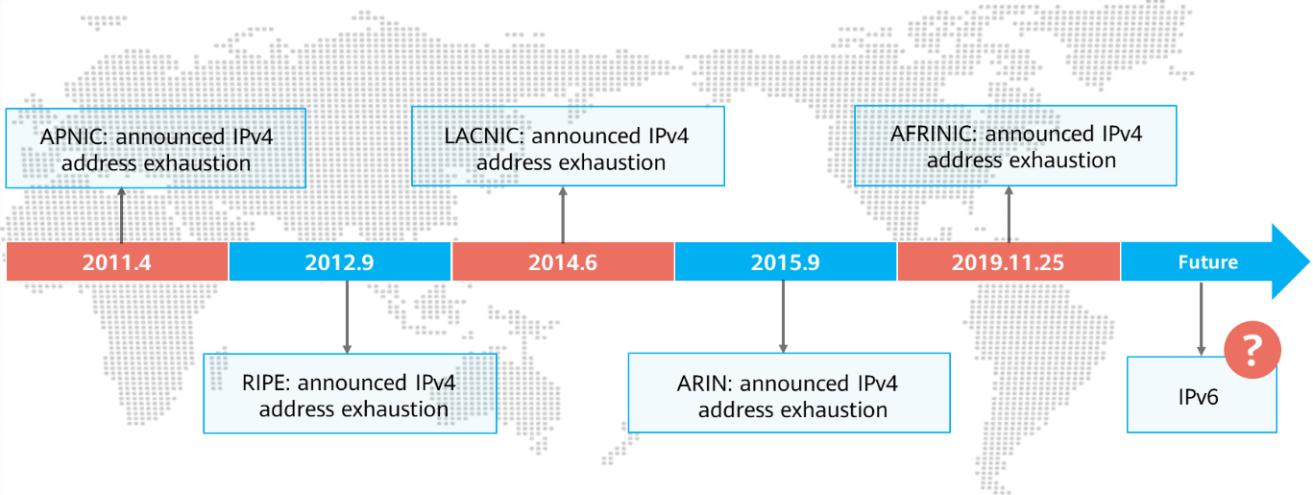
Describe the method and basic procedure for configuring IPv6 addresses.

Configure IPv6 addresses and IPv6 static routes.

## IPv6 Overview

### IPv4 Status

On February 3, 2011, the Internet Assigned Numbers Authority (IANA) announced even allocation of its last 4.68 million IPv4 addresses to five Regional Internet Registries (RIRs) around the world. The IANA thereafter had no available IPv4 address.



IPv4 Status

The IANA is responsible for assigning global Internet IP addresses. The IANA assigns some IPv4 addresses to continent-level RIRs, and then each RIR assigns addresses in its regions. The five RIRs are as follows:

1. RIPE: Reseaux IP Europeans, which serves Europe, Middle East, and Central Asia.
2. LACNIC: Latin American and Caribbean Internet Address Registry, which serves the Central America, South America, and the Caribbean.
3. ARIN: American Registry for Internet Numbers, which serves North America and some Caribbean regions.
4. AFRINIC: Africa Network Information Center, which serves Africa.
5. APNIC: Asia Pacific Network Information Centre, which serves Asia and the Pacific.

IPv4 has proven to be a very successful protocol. It has survived the development of the Internet from a small number of computers to hundreds of millions of computers. But the protocol was designed decades ago based on the size of the networks at that time. With the expansion of the Internet and the launch of new applications, IPv4 has shown more and more limitations.

The rapid expansion of the Internet scale was unforeseen at that time. Especially over the past decade, the Internet has experienced explosive growth and has been accessed by numerous households. It has become a necessity in people's daily life. Against the Internet's rapid development, IP address depletion becomes a pressing issue.

In the 1990s, the IETF launched technologies such as Network Address Translation (NAT) and Classless Inter-Domain Routing (CIDR) to delay IPv4 address exhaustion. However, these transition solutions can only slow down the speed of address exhaustion, but cannot fundamentally solve the problem.

### Why IPv6?

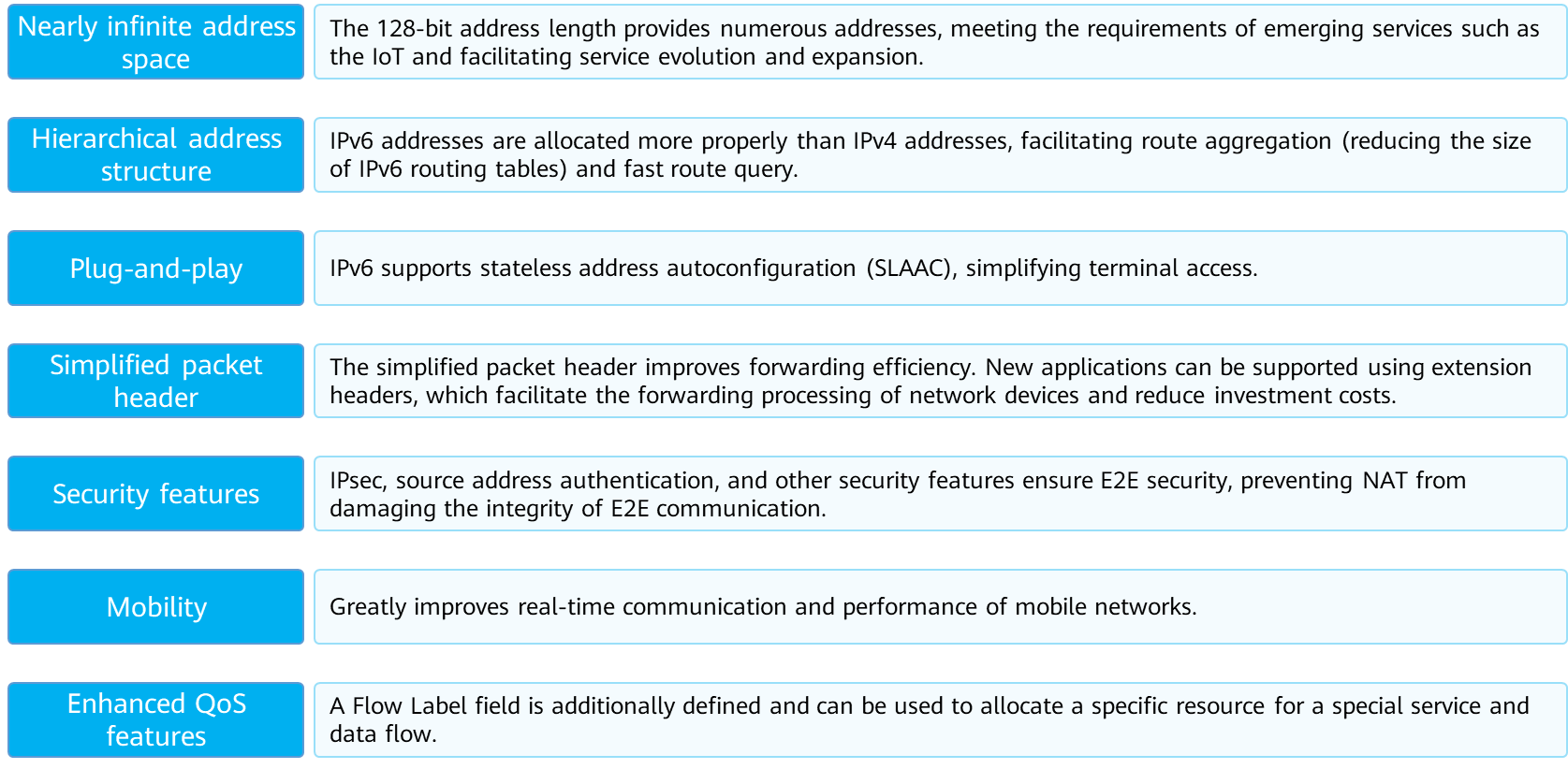
Characteristics of IPv4:

1. Exhausted public IP addresses
2. Improper packet header design
3. Large routing table, leading to inefficient table query
4. Dependency on ARP causes broadcast storms
5. ……

Characteristics of IPv6:

1. Nearly infinite address space
2. Hierarchical address allocation
3. Plug-and-play
4. Simplified packet header
5. IPv6 security features
6. Integrity of E2E communication
7. Support for mobility
8. Enhanced QoS features
9. ...

### IPv6 Advantages



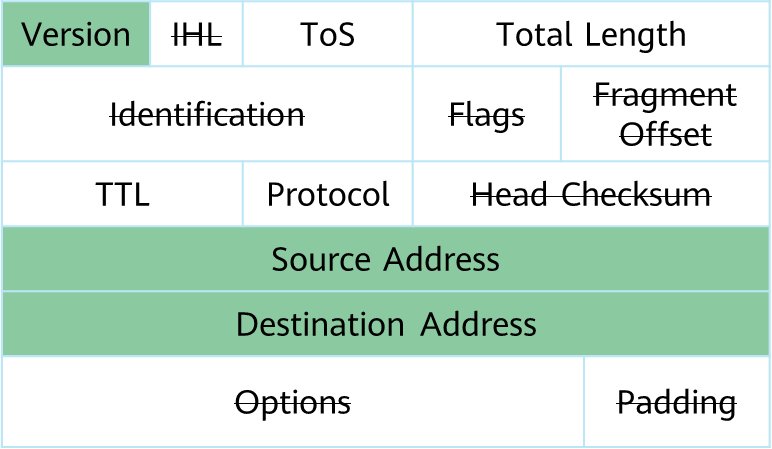
IPv6 Advantages

* Nearly infinite address space: This is the most obvious advantage over IPv4. An IPv6 address consists of 128 bits. The address space of IPv6 is about 8 x 1028 times that of IPv4. It is claimed that IPv6 can allocate a network address to each grain of sand in the world. This makes it possible for a large number of terminals to be online at the same time and unified addressing management, providing strong support for the interconnection of everything.
* Hierarchical address structure: IPv6 addresses are divided into different address segments based on application scenarios thanks to the nearly infinite address space. In addition, the continuity of unicast IPv6 address segments is strictly required to prevent "holes" in IPv6 address ranges, which facilitates IPv6 route aggregation to reduce the size of IPv6 address tables.
* Plug-and-play: Any host or terminal must have a specific IP address to obtain network resources and transmit data. Traditionally, IP addresses are assigned manually or automatically using DHCP. In addition to the preceding two methods, IPv6 supports SLAAC.
* E2E network integrity: NAT used on IPv4 networks damages the integrity of E2E connections. After IPv6 is used, NAT devices are no longer required, and online behavior management and network monitoring become simple. In addition, applications do not need complex NAT adaptation code.
* Enhanced security: IPsec was initially designed for IPv6. Therefore, IPv6-based protocol packets (such as routing protocol packets and neighbor discovery packets) can be encrypted in E2E mode, despite the fact that this function is not widely used currently. The security capability of IPv6 data plane packets is similar to that of IPv4+IPsec.
* High scalability: IPv6 extension headers are not a part of the main data packet. However, if necessary, the extension headers can be inserted between the basic IPv6 header and the valid payload to assist IPv6 in encryption, mobility, optimal path selection, and QoS, improving packet forwarding efficiency.
* Improved mobility: When a user moves from one network segment to another on a traditional network, a typical triangle route is generated. On an IPv6 network, the communication traffic of such mobile devices can be directly routed without the need of the original triangle route. This feature reduces traffic forwarding costs and improves network performance and reliability.
* Enhanced QoS: IPv6 reserves all QoS attributes of IPv4 and additionally defines a 20-byte Flow Label field for applications or terminals. This field can be used to allocate specific resources to special services and data flows. Currently, this mechanism has not been fully developed and applied yet.

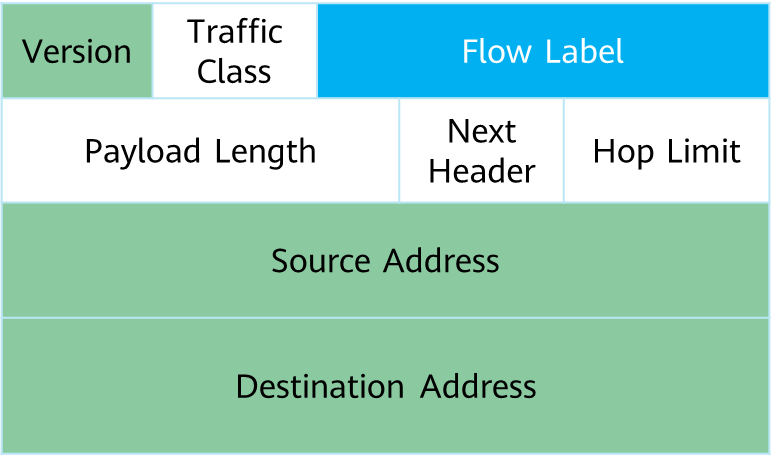
### Basic IPv6 Header

An IPv6 header consists of a mandatory basic IPv6 header and optional extension headers.

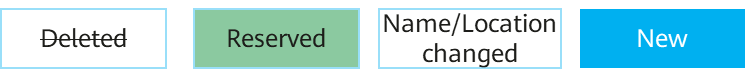
The basic header provides basic information for packet forwarding and is parsed by all devices on a forwarding path.



IPv4 packet header (20–60 bytes)



Basic IPv6 header

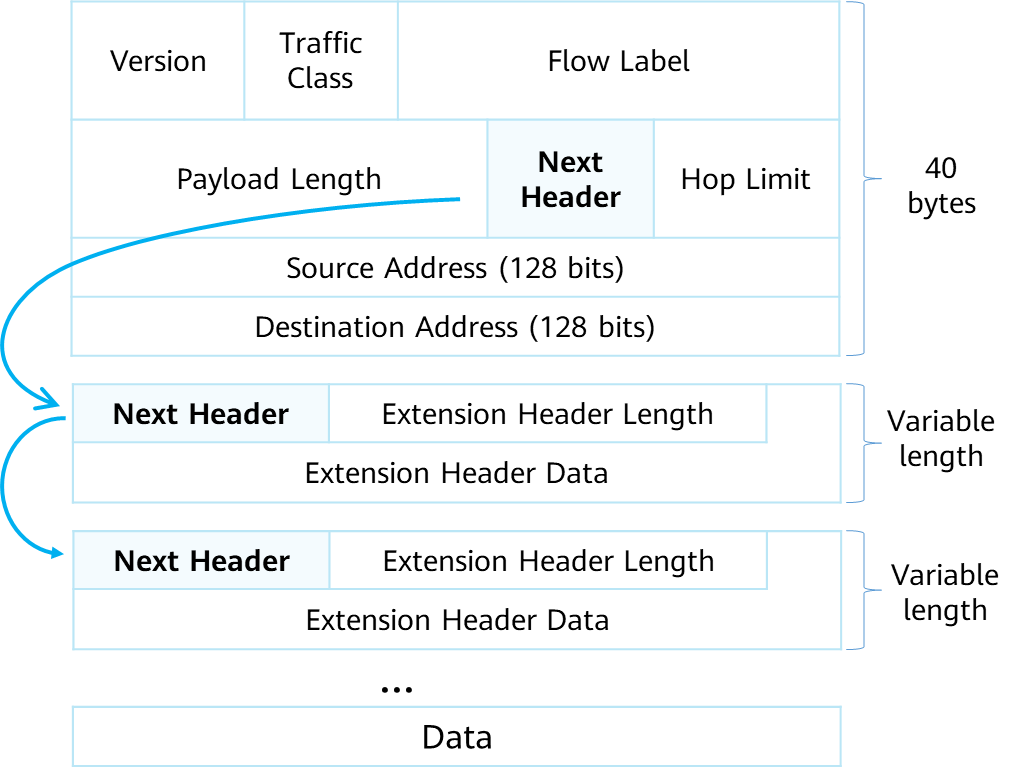


Label Styple Explain For IPv4 and IPv6 Packet Format

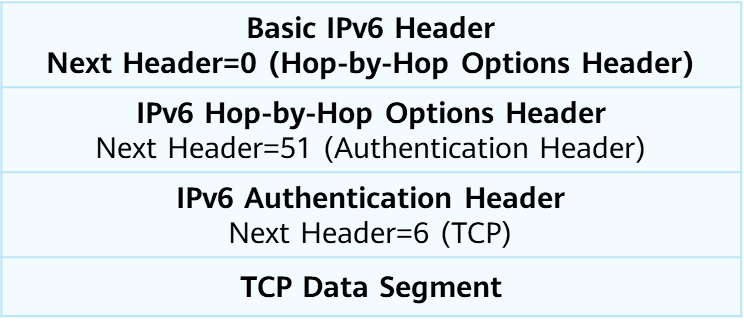
The fields in a basic IPv6 header are described as follows:

1. Version: 4 bits long. In IPv6, the value is 6.
2. Traffic Class: 8 bits long. This field indicates the class or priority of an IPv6 packet. It is similar to the TOS field in an IPv4 packet and is mainly used in QoS control.
3. Flow Label: 20 bits long. This field was added in IPv6 to differentiate real-time traffic. A flow label and a source IP address together can identify a unique data flow. Intermediate network devices can effectively differentiate data flows based on this field.
4. Payload Length: 16 bits long. This field indicates the length of the part (namely, extension headers and upper-layer PDU) in an IPv6 packet following the IPv6 basic header.
5. Next Header: 8 bits long. This field defines the type of the first extension header (if any) following a basic IPv6 header or the protocol type in an upper-layer PDU (similar to the Protocol field in IPv4).
6. Hop Limit: 8 bits long. This field is similar to the Time to Live field in an IPv4 packet. It defines the maximum number of hops that an IP packet can pass through. The value is decreased by 1 each time an IP packet passes through a node. The packet is discarded if Hop Limit is decreased to zero.
7. Source Address: 128 bits long. This field indicates the address of the packet sender.
8. Destination Address: 128 bits long. This field indicates the address of the packet receiver.

### IPv6 Extension Header



IPv6 Extension Packet Format



IPv6 packet example

* Extension Header Length: 8 bits long. This field indicates the extension header length excluding the length of the Next Header field.
* Extension Header Data: variable length. This field indicates the payload of the extension headers and is a combination of a series of options and padding fields.

An IPv4 packet header carries the optional Options field, which can represent security, timestamp, or record route options. The Options field extends the IPv4 packet header from 20 bytes to 60 bytes. The Options field needs to be processed by all the intermediate devices, consuming a large number of resources. For this reason, this field is seldom used in practice.

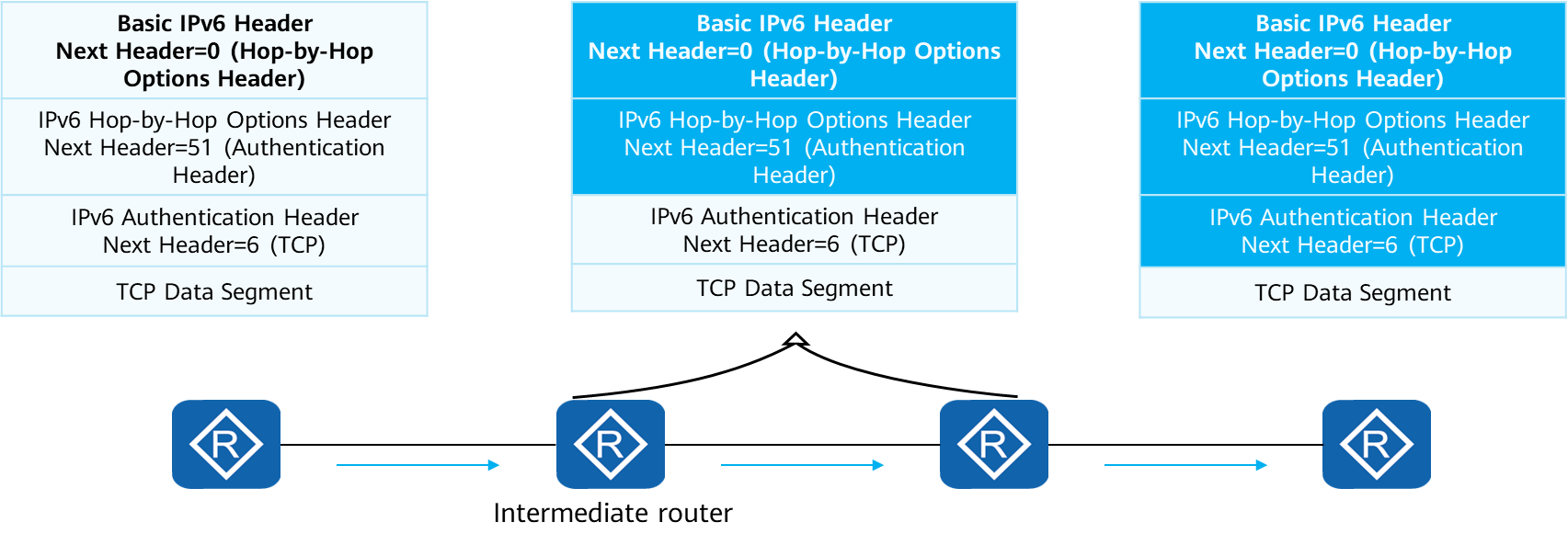
IPv6 removes the Options field from the basic header and puts it in the extension headers, which are placed between a basic IPv6 header and upper-layer PDU. An IPv6 packet may carry zero, one, or more extension headers. A sender adds one or more extension headers to a packet only when the sender requests the destination device or other devices to perform special handling. The length of IPv6 extension headers is not limited to 40 bytes so that new options can be added later. This feature together with the option processing modes enables the IPv6 options to be leveraged. To improve extension header processing efficiency and transport protocol performance, the extension header length, however, is always an integer multiple of 8 bytes.

When multiple extension headers are used, the Next Header field of the preceding header indicates the type of the current extension header. In this way, a chained packet header list is formed.

When more than one extension header is used in the same IPv6 packet, those headers must appear in the following order:

1. Hop-by-Hop Options header: carries optional information that must be examined by every node along a packet's delivery path.
2. Destination Options header: carries optional information that needs to be examined only by a packet's destination node.
3. Routing header: used by an IPv6 source to list one or more intermediate nodes to be "visited" on the way to a packet's destination.
4. Fragment header: used by an IPv6 source to send a packet longer than the path MTU to its destination.
5. Authentication header (AH): used by IPsec to provide authentication, data integrity, and replay protection.
6. Encapsulating Security Payload (ESP) header: used by IPsec to provide authentication, data integrity, replay protection, and confidentiality of IPv6 packets.

### IPv6 Packet Processing Mechanism



IPv6 Packet Processing Mechanism

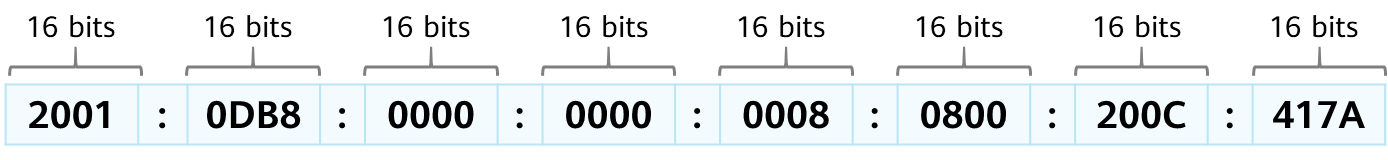
* Source router’s behavior：Constructs an IPv6 packet as required.
* Intermediate router’s behavior: Process the basic header and Hop-by-Hop Options header.
* Destination router’s behavior: Processes all packet headers.

The length of the basic packet header is fixed, improving the forwarding efficiency.

The extension headers meet special requirements.

### IPv6 Address

The length of an IPv6 address is 128 bits. Colons are generally used to divide the IPv6 address into eight segments. Each segment contains 16 bits and is expressed in hexadecimal notation.



Example for IPv6 Address

The letters in an IPv6 address are case insensitive. For example, A is equivalent to a.

Similar to an IPv4 address, an IPv6 address is expressed in the format of IPv6 address/mask length.，for example, 2001:0DB8:2345:CD30:1230:4567:89AB:CDEF/64,the IPv6 address is 2001:0DB8:2345:CD30:1230:4567:89AB:CDEF and subnet number is 2001:0DB8:2345:CD30::/64.

### IPv6 Address Abbreviation Specifications

For convenience, IPv6 can be abbreviated according to the following rules.

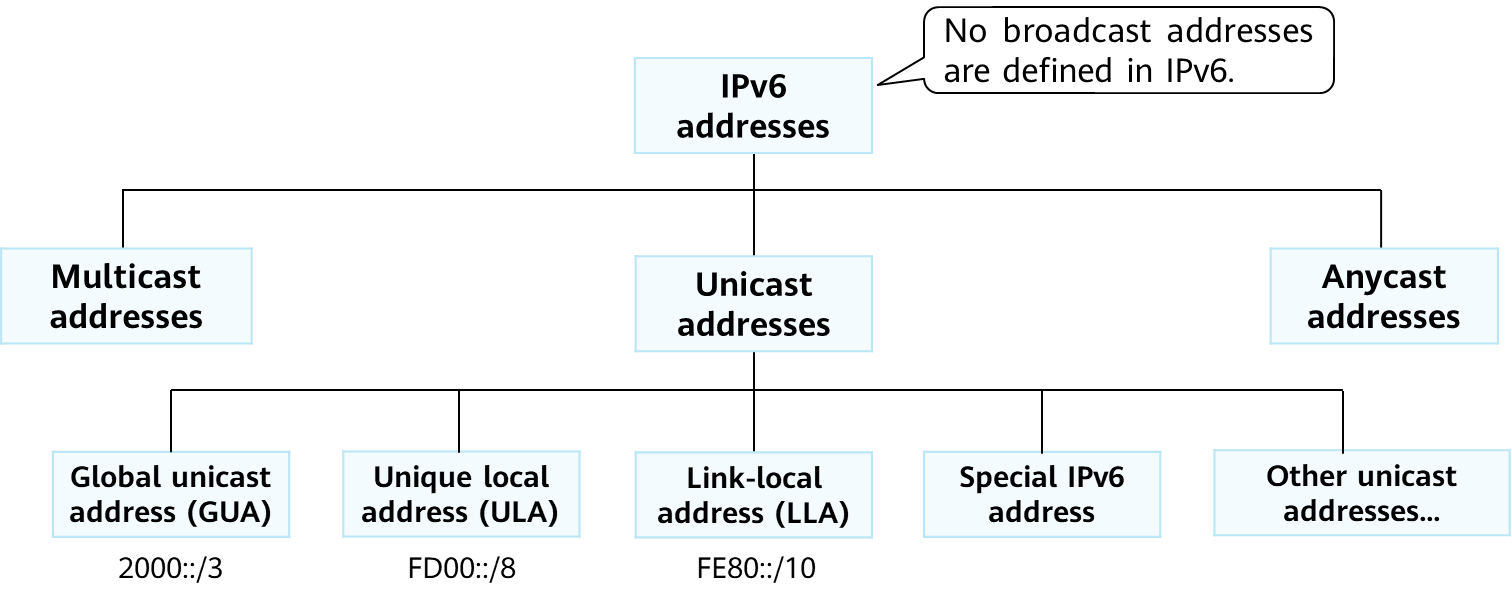
1. The leading 0s in each 16-bit segment can be omitted. However, if all bits in a 16-bit segment are 0s, at least one 0 must be reserved. The tailing 0s cannot be omitted.
2. If one or more consecutive 16-bit segments contain only 0s, a double colon (**::**) can be used to represent them, but only one **::** is allowed in an entire IPv6 address.
3. If an abbreviated IPv6 address contains two double colons (::), the IPv6 address cannot be restored to the original one.

Abbreviation Examples:

1. Before 0000:0000:0000:0000:0000:0000:0000:0001   
   After ::1
2. Before 2001:0DB8:0000:0000:FB00:1400:5000:45FF   
   After 2001:DB8::FB00:1400:5000:45FF
3. Before 2001:0DB8:0000:0000:0000:2A2A:0000:0001   
   After 2001:DB8::2A2A:0:1
4. Before 2001:0DB8:0000:1234:FB00:0000:5000:45FF   
   After 2001:DB8::1234:FB00:0:5000:45FF  
   or 2001:DB8:0:1234:FB00::5000:45FF

### IPv6 Address Classification

IPv6 addresses are classified into unicast, multicast, and anycast addresses according to the IPv6 address prefix.



IPv6 Address Classification

* Unicast address: identifies an interface. A packet destined for a unicast address is sent to the interface having that unicast address. In IPv6, an interface may have multiple IPv6 addresses. In addition to GUAs, ULAs, and LLAs, IPv6 has the following special unicast addresses:

1. Unspecified address: 0:0:0:0:0:0:0:0/128, or ::/128. The address is used as the source address of some packets, for example, Neighbor Solicitation (NS) messages sent during DAD or request packets sent by a client during DHCPv6 initialization.
2. Loopback address: 0:0:0:0:0:0:0:1/128, or ::1/128, which is used for local loopback (same function as 127.0.0.1 in IPv4). The data packets sent to ::/1 are actually sent to the local end and can be used for loopback tests of local protocol stacks.

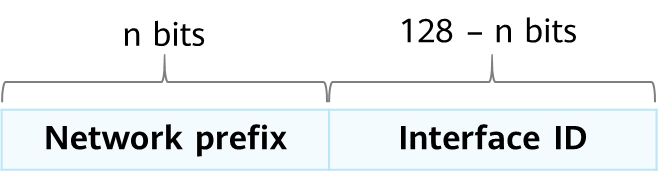
* Multicast address: identifies multiple interfaces. A packet destined for a multicast address is sent to all the interfaces joining in the corresponding multicast group. Only the interfaces that join a multicast group listen to the packets destined for the corresponding multicast address.
* Anycast address: identifies a group of network interfaces (usually on different nodes). A packet sent to an anycast address is routed to the nearest interface having that address, according to the router's routing table.
* IPv6 does not define any broadcast address. On an IPv6 network, all broadcast application scenarios are served by IPv6 multicast.

### IPv6 Unicast Address Format

An IPv6 unicast address is composed of two parts:

1. Network prefix: consists of n bits and is parallel to the network ID of an IPv4 address.
2. Interface ID: consists of (128 – n) bits and is parallel to the host ID of an IPv4 address.

Common IPv6 unicast addresses, such as GUAs and LLAs, require that the network prefix and interface ID be 64 bits.



IPv6 Unicast Address Format

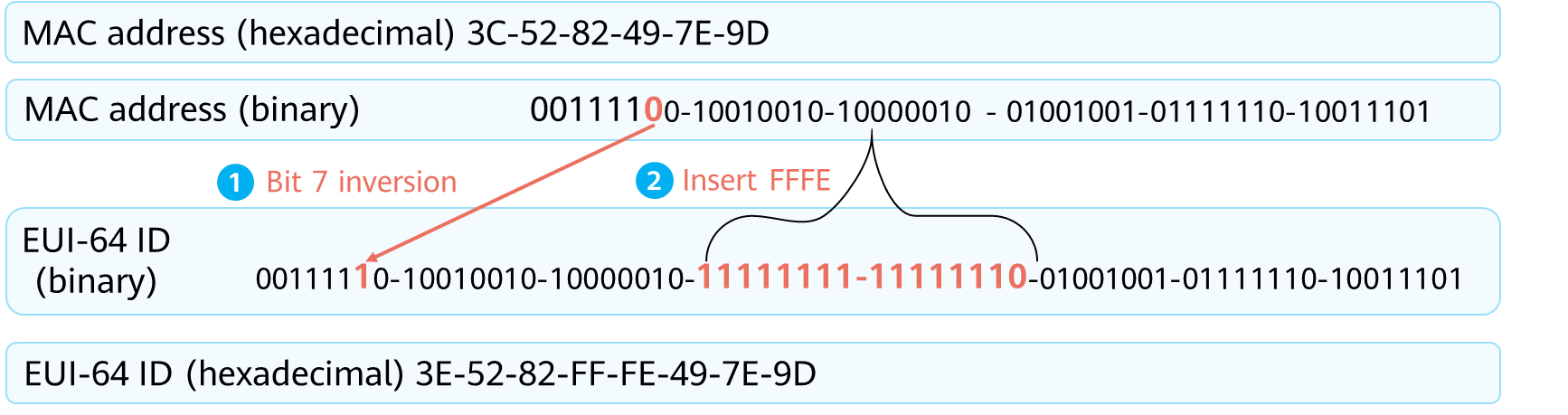
Global unicast addresses that start with binary value 000 can use a non-64-bit network prefix. Such addresses are not covered in this course.

### Interface ID of an IPv6 Unicast Address

3 methods to generate an interface ID:

1. Manual configuration
2. Automatic generation by the system
3. Using the IEEE 64-bit extended unique identifier (EUI-64) standard

EUI-64 is most commonly used. It converts the MAC address of an interface into an IPv6 interface ID.



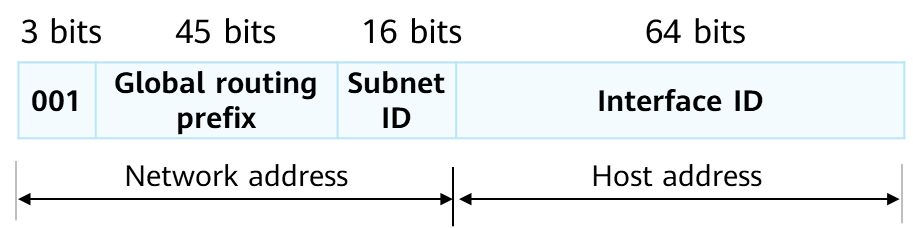
Generation of the EUI-64

* An interface ID is 64 bits long and is used to identify an interface on a link. The interface ID must be unique on each link. The interface ID is used for many purposes. Most commonly, an interface ID is attached to a link-local address prefix to form the link-local address of the interface. It can also be attached to an IPv6 global unicast address prefix in SLAAC to form the global unicast address of the interface.
* IEEE EUI-64 standard

1. Converting MAC addresses into IPv6 interface IDs reduces the configuration workload. Especially, you only need an IPv6 network prefix in SLAAC to form an IPv6 address.
2. The defect of this method is that IPv6 addresses can be deducted by attackers based on MAC addresses.

### Common IPv6 Unicast Address - GUA

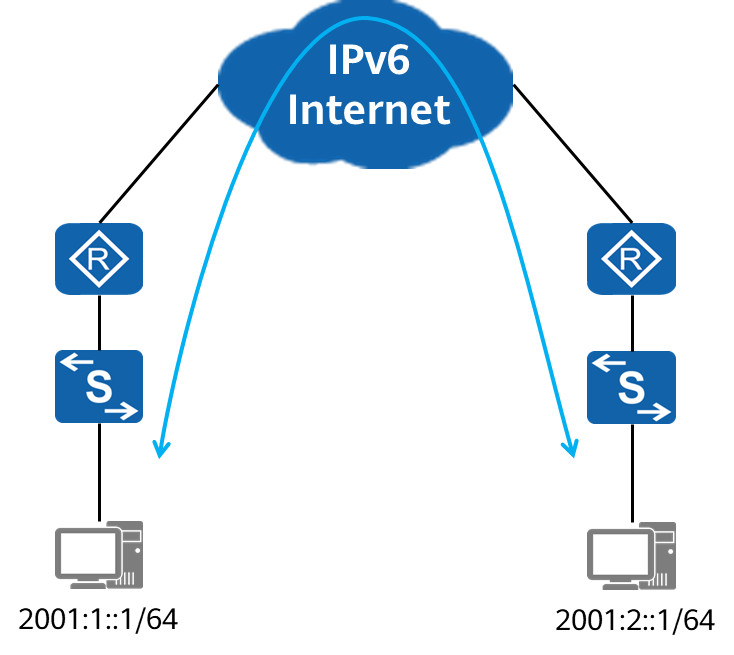
A GUA is also called an aggregatable GUA. This type of address is globally unique and is used by hosts that need to access the Internet. It is equivalent to a public IPv4 address.



Example of GUA

Illustration of GUA：

1. The network address and interface ID of a GUA are each generally 64 bits long.
2. Global routing prefix: is assigned by a provider to an organization and is generally at least 45 bits.
3. Subnet ID: An organization can divide subnets based on network requirements.
4. Interface ID: identifies a device's interface.

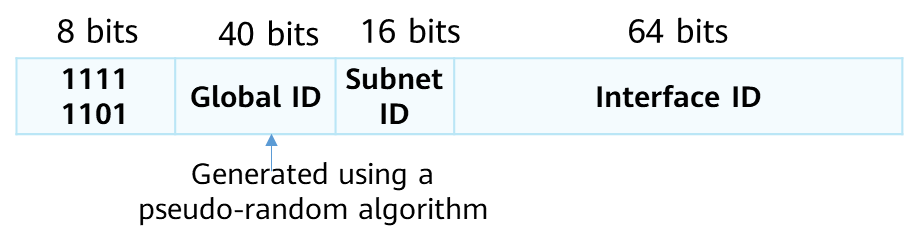


Scenario of GUA

You can apply for a GUA from a carrier or the local IPv6 address management organization.

### Common IPv6 Unicast Address - ULA

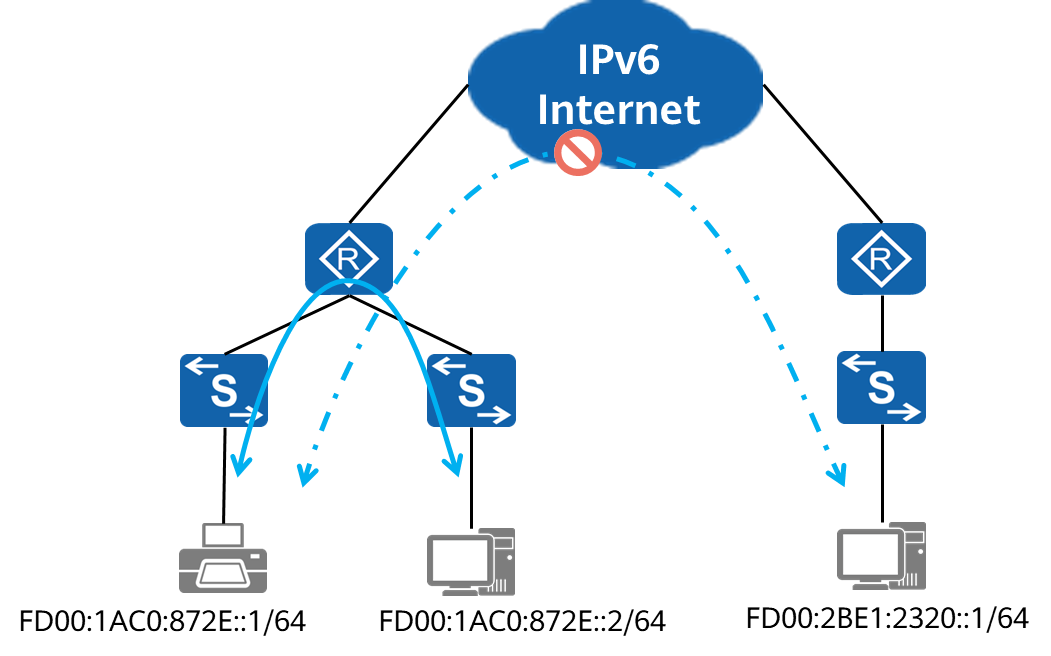
A ULA is a private IPv6 address that can be used only on an intranet. This type of address cannot be routed on an IPv6 public network and therefore cannot be used to directly access a public network.



Example of ULA

Illustration of ULA：

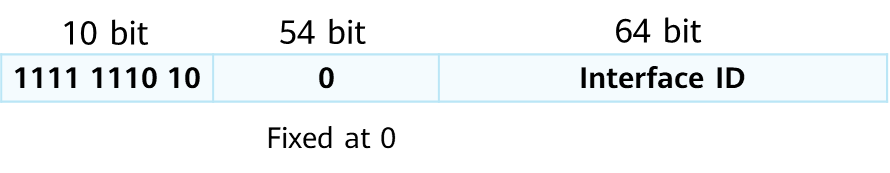
1. ULAs use the FC00::/7 address segment, among which, only the FD00::/8 address segment is currently used. FC00::/8 is reserved for future expansion.
2. Although a ULA is valid only in a limited range, it also has a globally unique prefix (generated using a pseudo-random algorithm, low conflict probability).



Scenario of ULA

### Common IPv6 Unicast Address - LLA

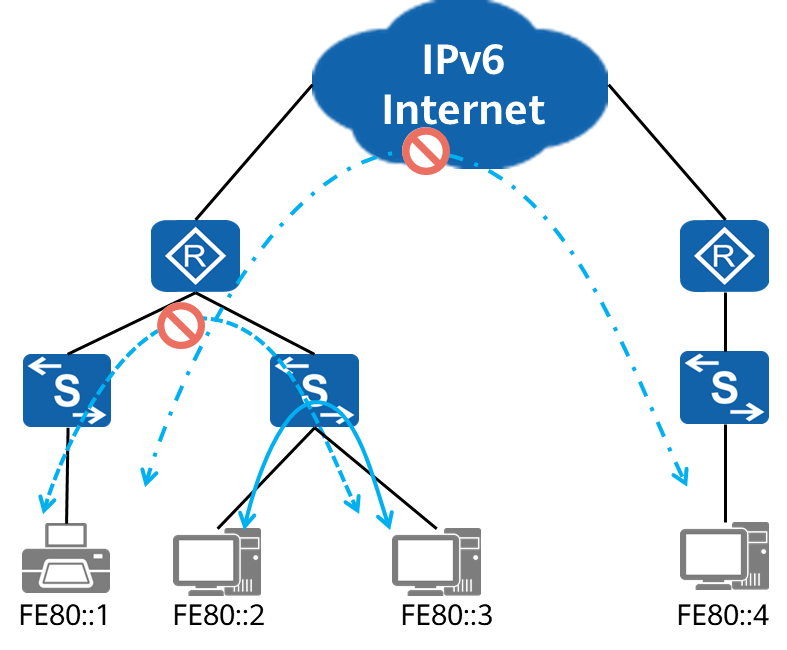
An LLA is another type of IPv6 address with limited application scope. The valid range of the LLA is the local link, with the prefix of FE80::/10.



Example of LLA

Illustration of LLA:

1. An LLA is used for communication on a single link, such as during IPv6 SLAAC and IPv6 neighbor discovery.
2. Data packets with the source or destination IPv6 address being an LLA are not forwarded out of the originating link. In other words, the valid scope of an LLA is the local link.
3. Each IPv6 interface must have an LLA. Huawei devices support automatic generation and manual configuration of LLAs.

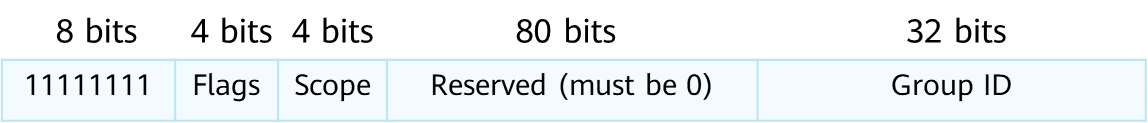


Scenario of LLA

### IPv6 Multicast Address

An IPv6 multicast address identifies multiple interfaces and is generally used in one-to-many communication scenarios.

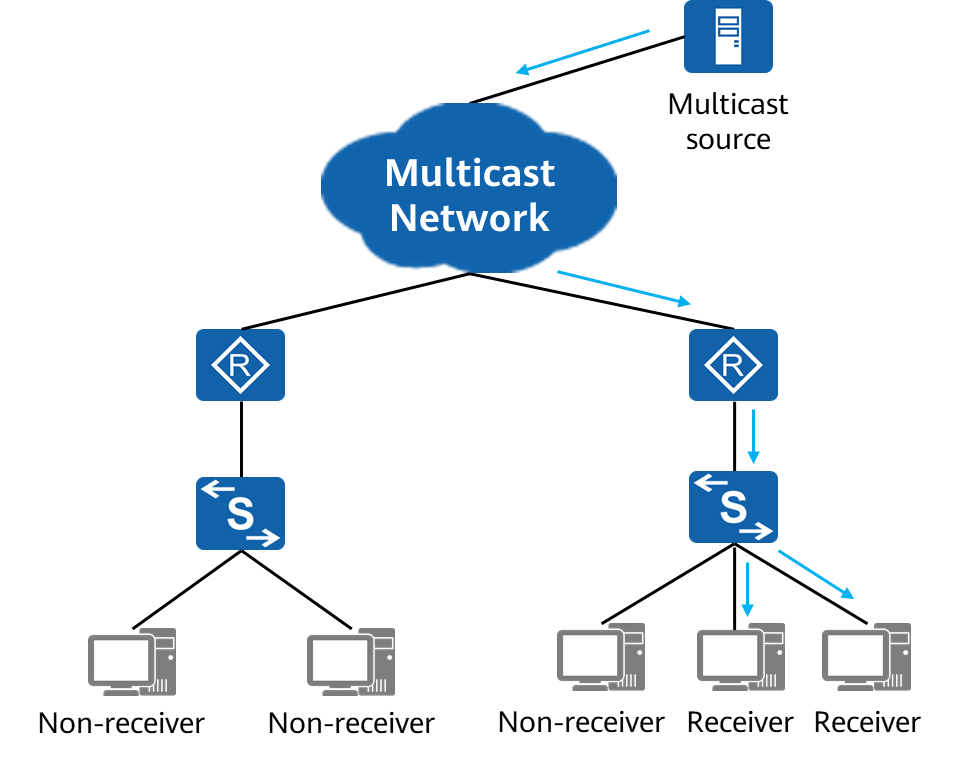
An IPv6 multicast address can be used only as the destination address of IPv6 packets.



IPv6 Multicast Address

Illustration of IPv6 multicast address:

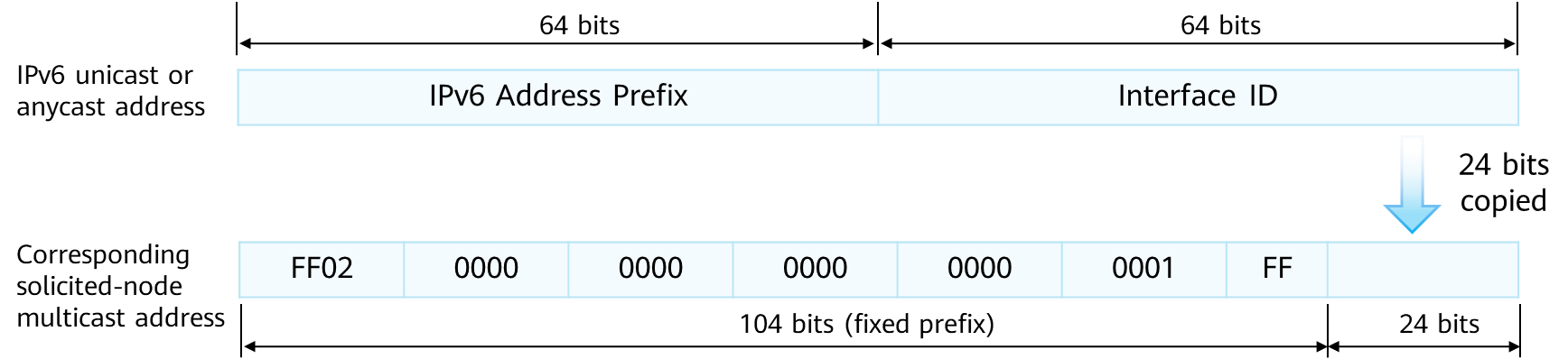
1. Flags: indicates a permanent or transient multicast group.
   1. 0000: permanent or well-known multicast group
   2. 0001: transient multicast group
2. Scope: indicates the multicast group scope.
   1. 0: reserved
   2. 1: interface-local scope, which spans only a single interface on a node and is useful only for loopback transmission of multicast
   3. 2: link-local scope (for example, FF02::1)
   4. 5: site-local scope
   5. 8: organization-local scope
   6. E: global scope
   7. F: reserved
3. Group ID: indicates a multicast group ID.



Scenario of IPv6 Multicast Group

### Solicited-Node Multicast Address

If a node has an IPv6 unicast or anycast address, a solicited-node multicast address is generated for the address, and the node joins the corresponding multicast group. This address is used for neighbor discovery and duplicate address detection (DAD). A solicited-node multicast address is valid only on the local link.

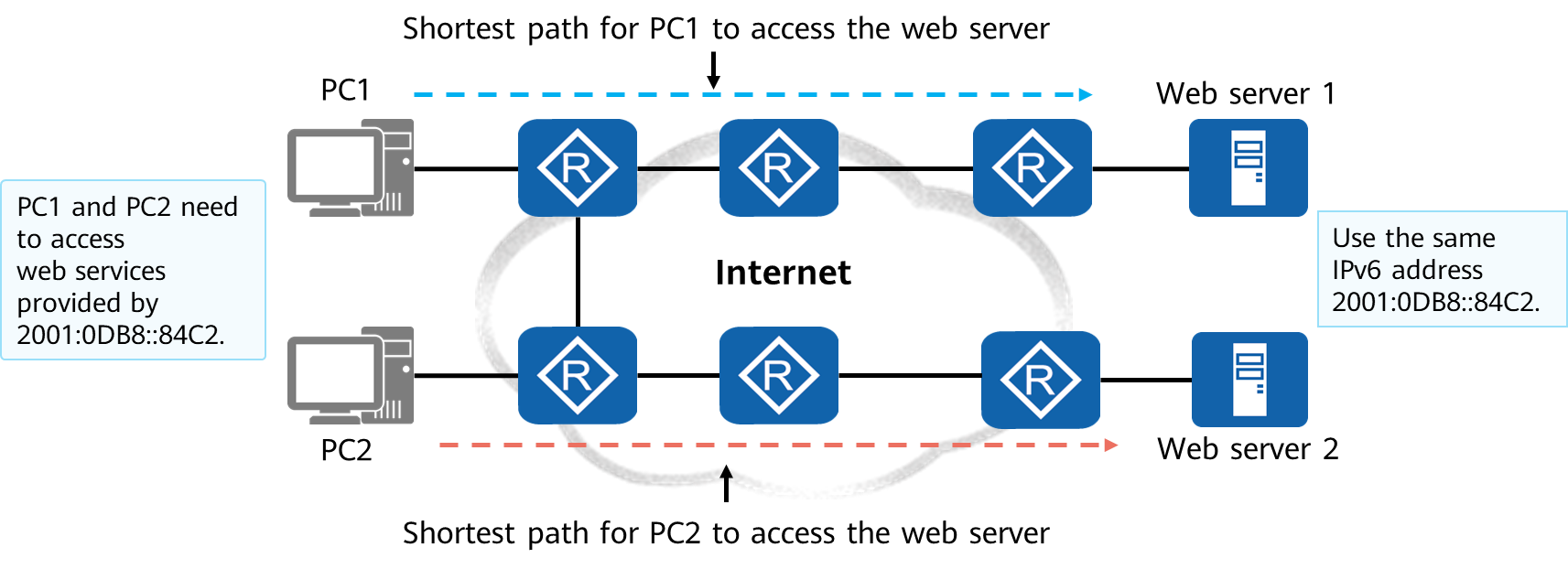


Generation of Solicited-node Multicast Address

An application scenario example of a solicited-node multicast group address is as follows: In IPv6, ARP and broadcast addresses are canceled. When a device needs to request the MAC address corresponding to an IPv6 address, the device still needs to send a request packet, which is a multicast packet. The destination IPv6 address of the packet is the solicited-node multicast address corresponding to the target IPv6 unicast address. Because only the target node listens to the solicited-node multicast address, the multicast packet is received only by the target node, without affecting the network performance of other non-target nodes.

### IPv6 Anycast Address

An anycast address identifies a group of network interfaces, which usually belong to different nodes. An anycast address can be used as the source or destination address of IPv6 packets.



Scenario of IPv6 Anycast Address

The anycast process involves an anycast packet initiator and one or more responders.

1. An initiator of an anycast packet is usually a host requesting a service (for example, a web service).
2. The format of an anycast address is the same as that of a unicast address. A device, however, can send packets to multiple devices with the same anycast address.

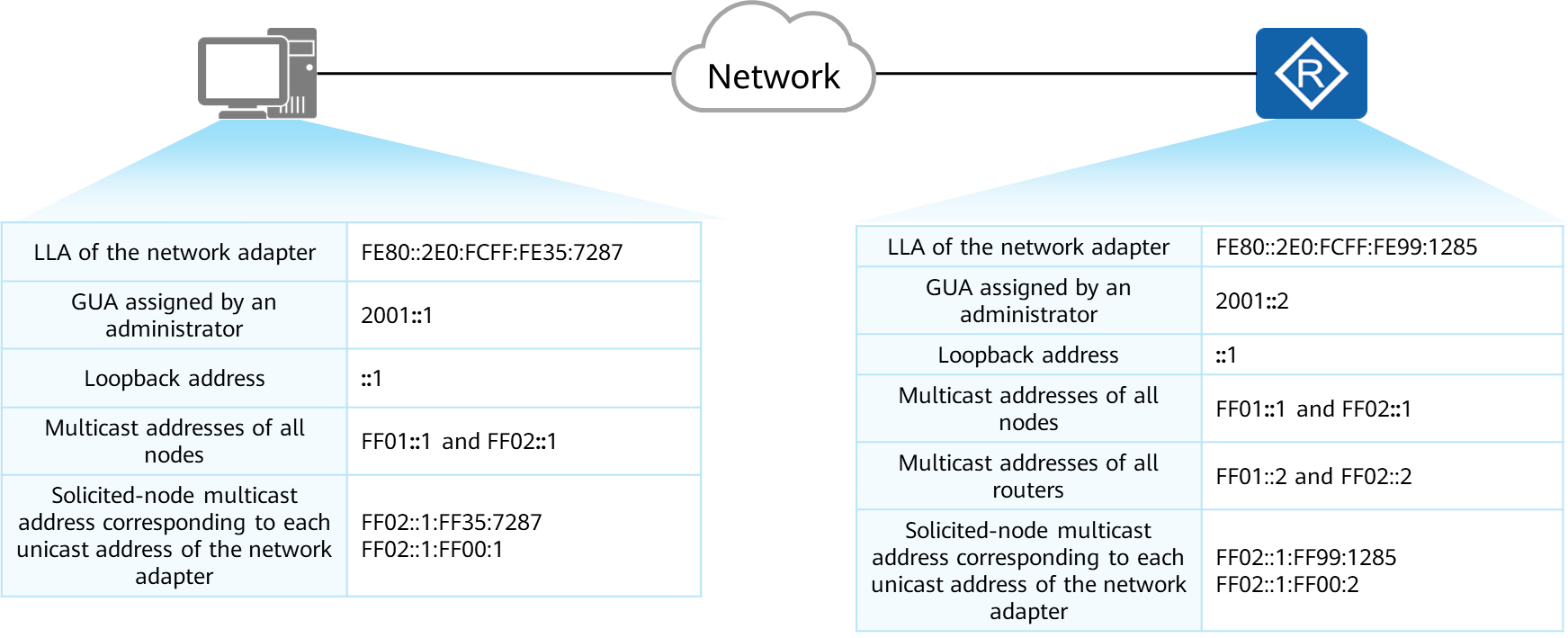
Anycast addresses have the following advantages:

1. Provide service redundancy. For example, a user can obtain the same service (for example, a web service) from multiple servers that use the same anycast address. These servers are all responders of anycast packets. If no anycast address is used and one server fails, the user needs to obtain the address of another server to establish communication again. If an anycast address is used and one server fails, the user can automatically communicate with another server that uses the same address, implementing service redundancy.
2. Provide better services. For example, a company deploys two servers – one in province A and the other in province B – to provide the same web service. Based on the optimal route selection rule, users in province A preferentially access the server deployed in province A when accessing the web service provided by the company. This improves the access speed, reduces the access delay, and greatly improves user experience.

## IPv6 Address Configuration

### IPv6 Addresses of Hosts and Routers

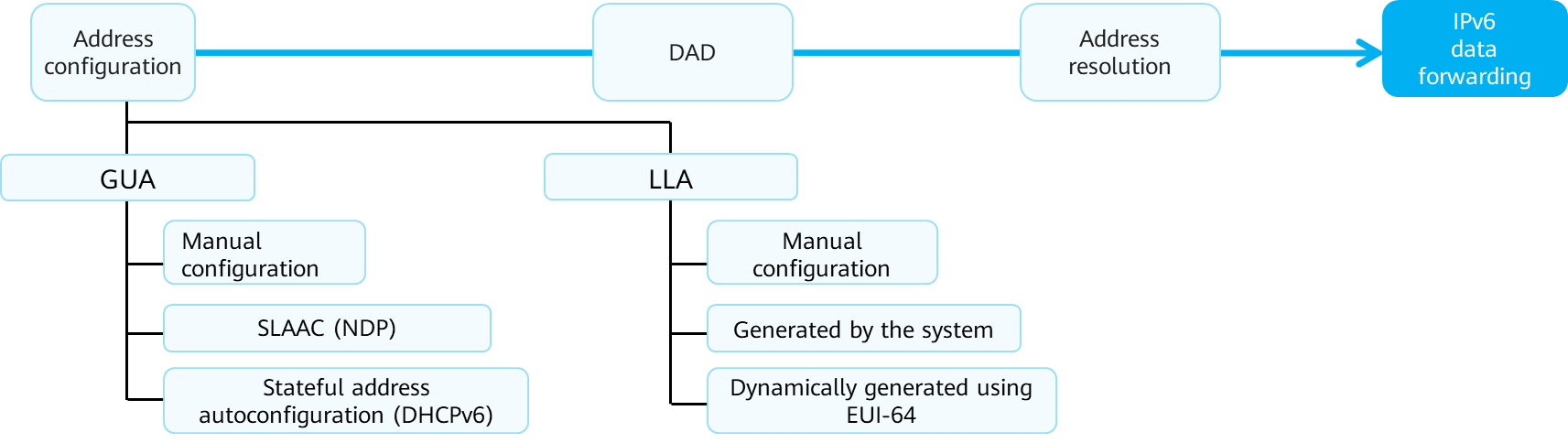
The unicast IPv6 addresses and multicast addresses of hosts and routers are typically as follows:



Unicast IPv6 Addresses and Multicast Addresses of Hosts

### Service Process of IPv6 Unicast Addresses

Before sending IPv6 packets, an interface undergoes address configuration, DAD, and address resolution. During this process, the Neighbor Discovery Protocol (NDP) plays an important role.



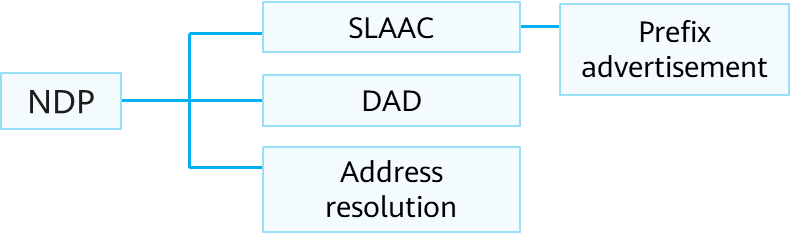
Service Process of IPv6 Unicast Addresses

* Address configuration：  
  GUAs and LLAs are the most common IPv6 unicast addresses on an interface. Multiple IPv6 addresses can be configured on one interface.
* DAD：  
  DAD is similar to gratuitous ARP in IPv4 and is used to detect address conflicts.
* Address resolution：  
  Similar to ARP requests in IPv4, ICMPv6 messages are used to generate the mappings between IPv6 addresses and data link layer addresses (usually MAC addresses).

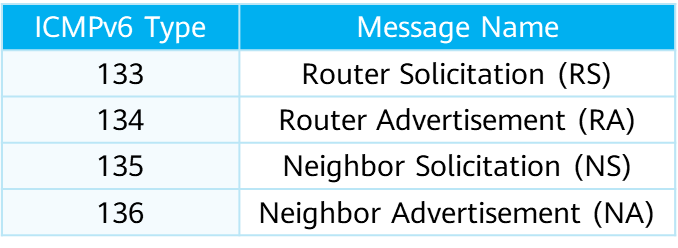
### NDP

NDP is defined in RFC 2461, which was replaced by RFC 4861.

NDP uses ICMPv6 messages to implement its functions.



NDP framework



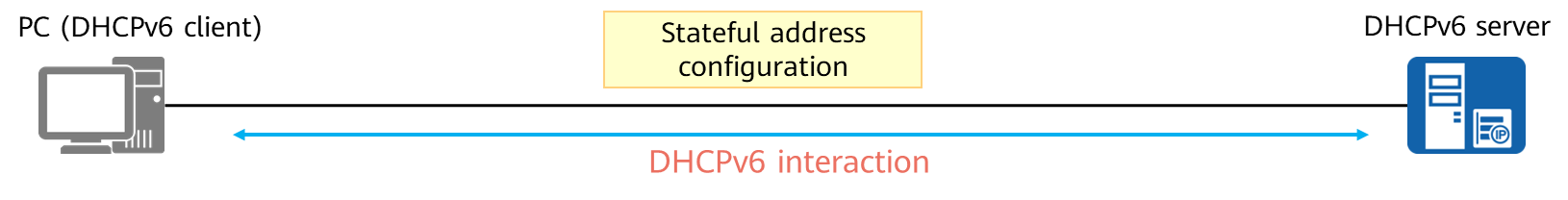
ICMPv6 messages used by NDP

SLAAC is a highlight of IPv6. It enables IPv6 hosts to be easily connected to IPv6 networks, without the need to manually configure IPv6 addresses and to deploy application servers (such as DHCP servers) to assign addresses to hosts. SLAAC uses ICMPv6 RS and RA messages.

Address resolution uses ICMPv6 NS and NA messages.

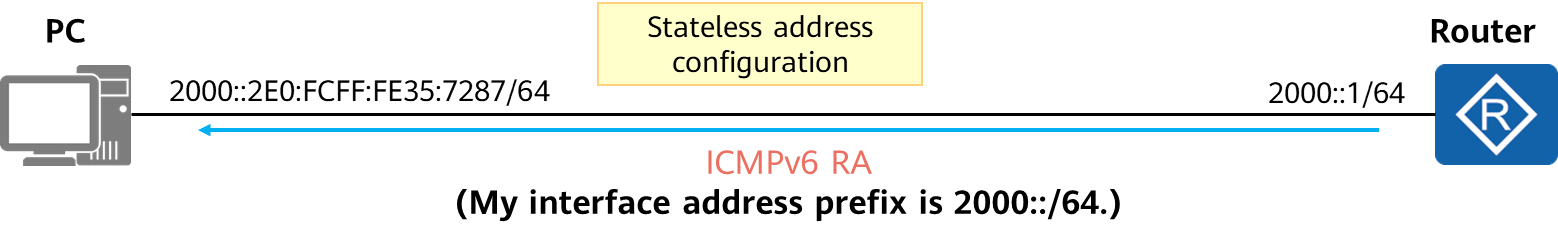
DAD uses ICMPv6 NS and NA messages to ensure that no two identical unicast addresses exist on the network. DAD must be performed on all interfaces before they use unicast addresses.

### Dynamic IPv6 Address Configuration



Statefull address configuration(DHCPv6)

* Through DHCPv6 message exchange, the DHCPv6 server automatically configures IPv6 addresses/prefixes and other network configuration parameters (such as DNS, NIS, and SNTP server addresses).



Stateless address configuration(ICMPv6)

* The PC generates a unicast address based on the address prefix in the RA and the locally generated 64-bit interface ID (for example, using EUI-64).
* Only IPv6 addresses can be obtained. Parameters such as NIS and SNTP server parameters cannot be obtained. DHCPv6 or manual configuration is required to obtain other configuration information.

IPv6 supports stateful and stateless address autoconfiguration. The managed address configuration flag (M flag) and other stateful configuration flag (O flag) in ICMPv6 RA messages are used to control the mode in which terminals automatically obtain addresses.

For stateful address configuration (DHCPv6), M = 1, O = 1:

* DHCPv6 is used. An IPv6 client obtains a complete 128-bit IPv6 address, as well as other address parameters, such as DNS and SNTP server address parameter, from a DHCPv6 server.
* The DHCPv6 server records the allocation of the IPv6 address (this is where stateful comes).
* This method is complex and requires high performance of the DHCPv6 server.
* Stateful address configuration is mainly used to assign IP addresses to wired terminals in an enterprise, facilitating address management.

For SLAAC, M = 0, O = 0:

* ICMPv6 is used.

1. The router enabled with ICMPv6 RA periodically advertises the IPv6 address prefix of the link connected to a host.
2. Alternatively, the host sends an ICMPv6 RS message, and the router replies with an RA message to notify the link's IPv6 address prefix.
3. The host obtains the IPv6 address prefix from the RA message returned by the router and combines the prefix with the local interface ID to form a unicast IPv6 address.
4. If the host wants to obtain other configuration information, it can use DHCPv6. When DHCPv6 is used, M = 0, and O = 1.
5. In SLAAC, routers do not care about the status of hosts or whether hosts are online.
6. SLAAC applies to scenarios where there are a large number of terminals that do not need other parameters except addresses. IoT is such a scenario.

Domain name system (DNS): a mechanism that maps easy-to-remember domain names to IPv6 addresses that can be identified by network devices

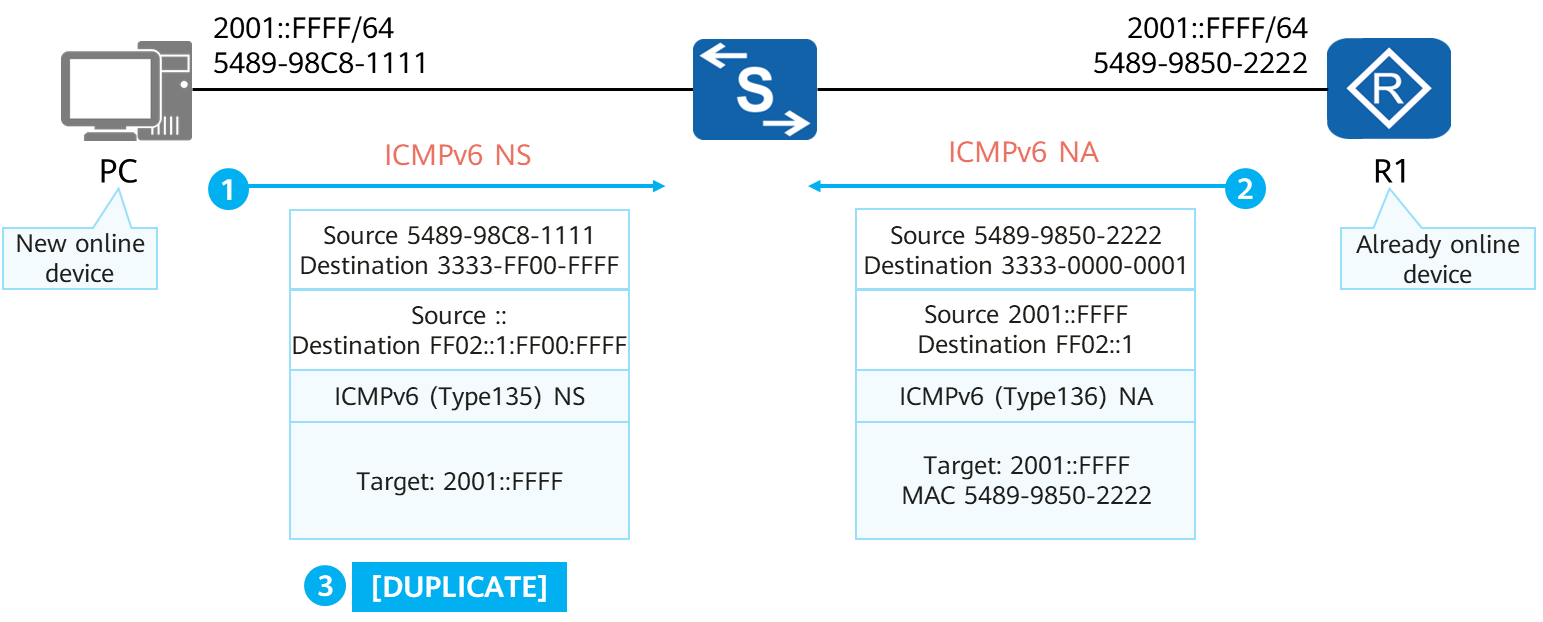
Network information system (NIS): a system manages all configuration files related to computer system management on computer networks

Simple Network Time Protocol (SNTP): adapted from NTP and is used to synchronize the clocks of computers on the Internet

### DAD

Regardless of how an IPv6 unicast address is configured, a host or router:

1. Performs DAD through ICMPv6 messages.
2. Uses a unicast address only after passing the DAD procedure.



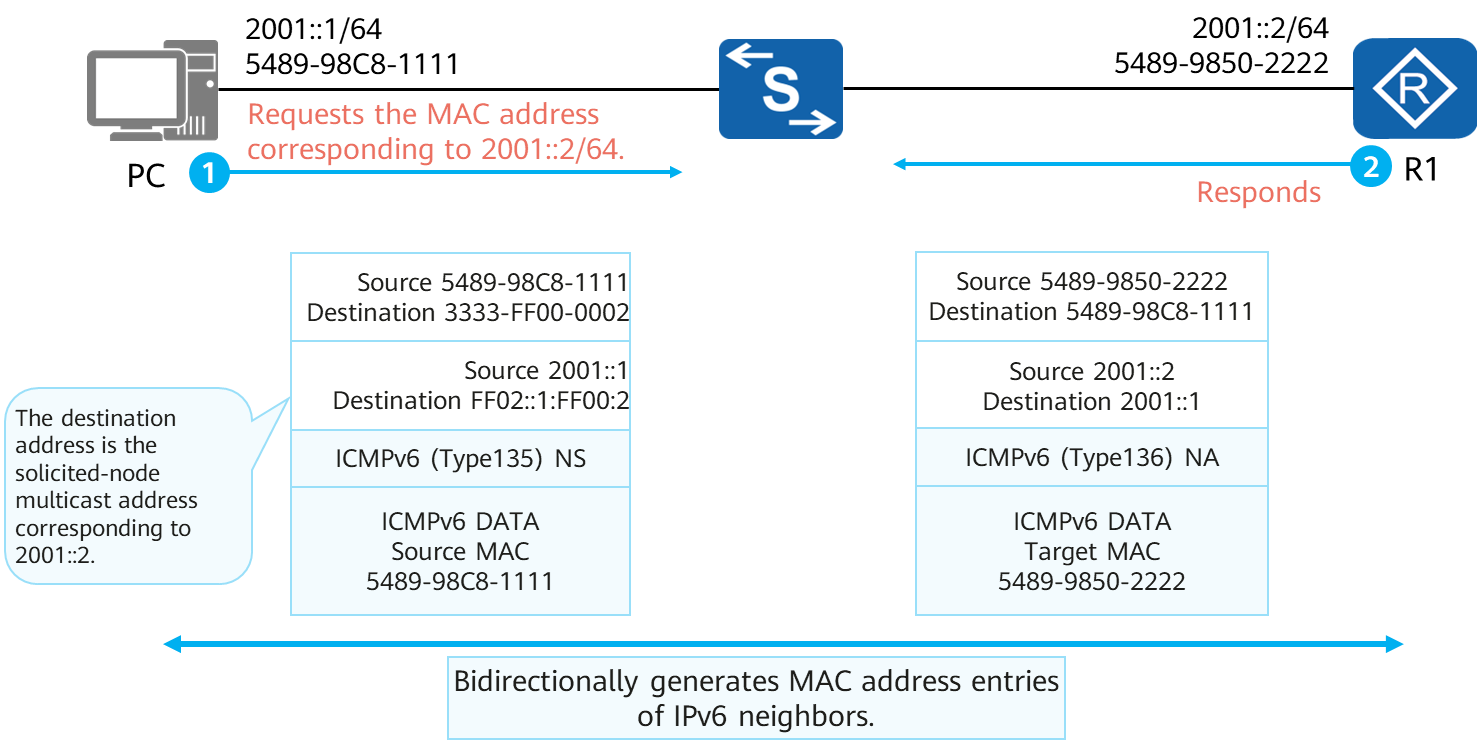
DAD

Assume that R1 is an online device with an IPv6 address 2001::FFFF/64. After the PC goes online, it is configured with the same IPv6 address. Before the IPv6 address is used, the PC performs DAD for the IPv6 address. The process is as follows:

1. The PC sends an NS message to the link in multicast mode. The source IPv6 address of the NS message is ::, and the destination IPv6 address is the solicited-node multicast address corresponding to 2001::FFFF for DAD, that is, FF02::1:FF00:FFFF. The NS message contains the destination address 2001::FFFF for DAD.
2. All nodes on the link receive the multicast NS message. The node interfaces that are not configured with 2001::FFFF are not added to the solicited-node multicast group corresponding to 2001::FFFF. Therefore, these node interfaces discard the received NS message. R1's interface is configured with 2001::FFFF and joins the multicast group FF02::1:FF00:FFFF. After receiving the NS message with 2001::FFFF as the destination IP address, R1 parses the message and finds that the destination address of DAD is the same as its local interface address. R1 then immediately returns an NA message. The destination address of the NA message is FF02::1, that is, the multicast address of all nodes. In addition, the destination address 2001::FFFF and the MAC address of the interface are filled in the NA message.
3. After the PC receives the NA message, it knows that 2001::FFFF is already in use on the link. The PC then marks the address as duplicate. This IP address cannot be used for communication. If no NA message is received, the PC determines that the IPv6 address can be used. The DAD mechanism is similar to gratuitous ARP in IPv4.

### Address Resolution

IPv6 uses ICMPv6 NS and NA messages to replace the address resolution function of ARP in IPv4.



Address Resolution

IPv6 address resolution does not use ARP or broadcast. Instead, IPv6 uses the same NS and NA messages as those in DAD to resolve data link layer addresses.

Assume that a PC needs to parse the MAC address corresponding to 2001::2 of R1. The detailed process is as follows:

1. The PC sends an NS message to 2001::2. The source address of the NS message is 2001::1, and the destination address is the solicited-node multicast address corresponding to 2001::2.
2. After receiving the NS message, R1 records the source IPv6 address and source MAC address of the PC, and replies with a unicast NA message that contains its own IPv6 address and MAC address.
3. After receiving the NA message, the PC obtains the source IPv6 address and source MAC address from the message. In this way, both ends create a neighbor entry about each other.

## Typical IPv6 Configuration Examples

### Basic IPv6 Configurations

* Enable IPv6.

[Huawei] **ipv6**

Enable the device to send and receive IPv6 unicast packets, including local IPv6 packets.

[Huawei-GigabitEthernet0/0/0] **ipv6 enable**

Enable IPv6 on the interface in the interface view.

* Configure an LLA for the interface.

[Huawei-GigabitEthernet0/0/0] **ipv6 address***ipv6-address*  **link-local**

[Huawei-GigabitEthernet0/0/0] **ipv6 address auto link-local**

Configure an LLA for the interface manually or automatically in the interface view.

* Configure a GUA for the interface.

[Huawei-GigabitEthernet0/0/0] **ipv6 address** { ipv6-address prefix-length | ipv6-address/prefix-length }

[Huawei-GigabitEthernet0/0/0] ipv6 address auto { global | dhcp }

Configure a GUA for the interface manually or automatically (stateful or stateless) in the interface view.

* Configure an IPv6 static route.

[Huawei] **ipv6 route-static** dest-ipv6-address prefix-length { interface-type interface-number [ nexthop-ipv6-address ] | nexthop-ipv6-address } [ **preference** preference ]

* Display IPv6 information on an interface.

[Huawei] **display ipv6 interface** [ *interface-type interface-number* | **brief** ]

* Display neighbor entry information.

[Huawei] display ipv6 neighbors

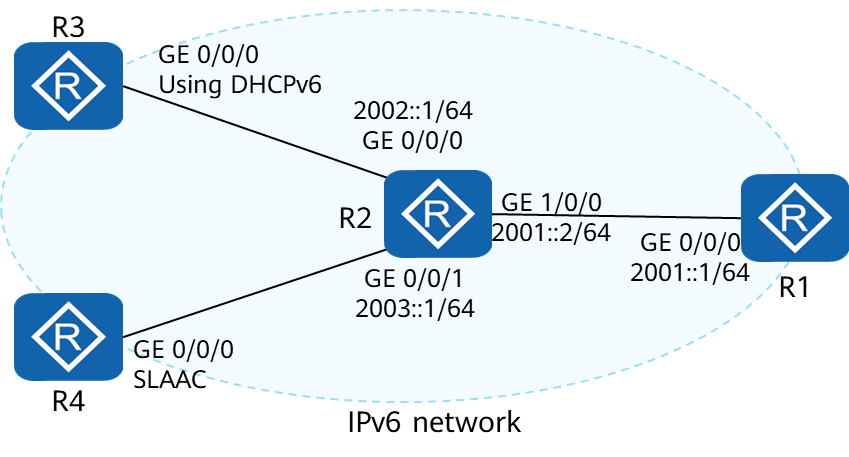
* Enable an interface to send RA messages.

[Huawei-GigabitEthernet0/0/0] **undo ipv6 nd ra halt**

By default, a Huawei router's interfaces do not send ICMPv6 RA messages. In this situation, other devices on the links connected to the interfaces cannot perform SLAAC.

To perform SLAAC, you need to manually enable the function of sending RA messages.

### Example: Configuring a Small IPv6 Network



Example Figure

Configuration Requirements

1. Connect R1 and R2 through interfaces with static IPv6 addresses.
2. Configure R2 as a DHCPv6 server to assign a GUA to GE 0/0/0 of R3.
3. Enable R2 to send RA messages, and configure GE 0/0/0 of R4 to automatically perform SLAAC based on the RA messages sent by R2.
4. Configure static routes to implement mutual access between the devices.

Configuration Step：

1. Enable IPv6 globally and on related interfaces of R1, R2, R3, and R4, and enable the interfaces to automatically generate LLAs. The following uses R1 configurations as an example.

[R1]ipv6

[R1]interface GigabitEthernet 0/0/0

[R1-GigabitEthernet0/0/0]ipv6 enable

[R1-GigabitEthernet0/0/0]ipv6 address auto link-local

1. Configure static IPv6 GUAs on the related interfaces of R1 and R2.

[R1]interface GigabitEthernet 0/0/0

[R1-GigabitEthernet0/0/0]ipv6 address 2001::1 64

[R2]interface GigabitEthernet 1/0/0

[R2-GigabitEthernet1/0/0]ipv6 address 2001::2 64

[R2-GigabitEthernet1/0/0]interface GigabitEthernet 0/0/0

[R2-GigabitEthernet0/0/0]ipv6 address 2002::1 64

[R2-GigabitEthernet0/0/0]interface GigabitEthernet 0/0/1

[R2-GigabitEthernet0/0/1]ipv6 address 2003::1 64

1. Configure R2 as a DHCPv6 server. Configure the related interface of R3 to obtain a GUA using DHCPv6.

[R2]dhcp enable

[R2]dhcpv6 pool pool1

[R2-dhcpv6-pool-pool1]address prefix 2002::/64

[R2]interface GigabitEthernet 0/0/0

[R2-GigabitEthernet0/0/0]dhcpv6 server pool1

[R3]dhcp enable

[R3]interface GigabitEthernet 0/0/0

[R3-GigabitEthernet0/0/0]ipv6 address auto dhcp

1. Enable R2 to advertise RA messages. Enable R4 to obtain an address through SLAAC based on the RA messages sent by R2.

[R2]interface GigabitEthernet 0/0/1

[R2-GigabitEthernet0/0/1]undo ipv6 nd ra halt

[R4]interface GigabitEthernet 0/0/0

[R4-GigabitEthernet0/0/0]ipv6 address auto global

1. Configure static routes on R4.

[R4]ipv6 route-static 2001:: 64 2003::1

[R4]ipv6 route-static 2002:: 64 2003::1

1. Configure an aggregated static route on R1.

[R1]ipv6 route-static 2002:: 15 2001::2

1. Configure a default route on R3.

[R3]ipv6 route-static :: 0 2002::1

## Quiz

1. (Single) Which of the following packet types does not exist in IPv6? ( )
2. Unicast
3. Broadcasting
4. Multicast
5. Anycast
6. (Single) Which of the following address types does an IPv6 link-local address belong to? ( )
7. Unicast
8. Broadcast
9. Multicast
10. Anycast
11. (Single) Which of the following statements about the compression expression of IPv6 address 2001:0410:0000:0001:0000:0000:0000:45FF is correct? ( )
12. 2001:410:0:1:0:0:0:45FF
13. 2001:41:0:1:0:0:0:45FF
14. 2001:410:0:1::45FF
15. 2001:410::1::45FF
16. (True or False) No matter how an IPv6 unicast address is configured, the host or router performs DAD. ( )
17. True
18. False
19. (True or False) The global unicast address and link-local address in IPv6 can be manually set. ( )
20. True
21. False
22. What is the most abbreviated form of the IPv6 address 2001:0DB8:0000:0000:032A:0000:0000:2D70?
23. What is the process of SLAAC for IPv6 hosts?

## Summary

|  |  |  |
| --- | --- | --- |
| **Comparison** | **IPv6** | **IPv4** |
| Address length | 128 bits | 32 bits |
| Packet format | A fixed 40-byte basic packet header+variable-length extension headers | A basic header containing the Options field to  support extended features |
| Address type | Unicast, multicast, and anycast | Unicast, multicast, and broadcast |
| Address configuration | Static, DHCP, and SLAAC | Static and DHCP |
| DAD | ICMPv6 | Gratuitous ARP |
| Address resolution | ICMPv6 | ARP |