IPv6 Basics

1 IPv6 Basics

1.1.1 Overview of IPv6

1.1.1.1 Need for IPv6

- Exhausted public IP addresses in IPv4 vs. nearly infinite address space in IPv6.

> The 128-bit address length creates an extremely large number of unique addresses, which is more than enough for the growing needs of things like the Internet of Things and allows for easy growth and development of new services.

- Improved packet header design.

Why ipv6 packet header better

1. **Simplified Header:** IPv6 has a fixed 40-byte header with fewer fields, making it quicker for routers to process.
2. **No Router Fragmentation:** IPv6 leaves packet fragmentation to the sender, simplifying router operations.
3. **Fixed Header Length:** The consistent length of the IPv6 header allows for predictable processing by network devices.
4. **Extension Headers:** IPv6 uses optional extension headers for special functions, which are skipped by routers if not needed, speeding up processing.
5. **Larger Address Space:** IPv6 has 128-bit addresses, vastly increasing the number of available IP addresses and solving exhaustion issues.

- In essence, IPv6 Simplifies packet processing and offers an expanded addressing scheme, leading to more efficient networking.

- Plug-and-play

> Plug-and-play networking allows devices to connect to a network with minimal setup by automatically obtaining an IP address. They can receive an IP address manually from an administrator, automatically from a DHCP server, or through self-configuration using SLAAC with IPv6. This simplifies device connection and network configuration.

- Hierarchical address allocation.

Note

- IPv4 can indeed use route aggregation to reduce the number of routing table entries, similar to IPv6. Both protocols allow networks to be summarized with a single prefix when announcing routes. For example, if an ISP owns the blocks 203.0.113.0/24 and 203.0.114.0/24, it can aggregate them and announce a single route to cover both blocks using the prefix 203.0.112.0/23.
- However, IPv6's larger address space (128-bit vs IPv4's 32-bit) allows for a much more detailed and hierarchical structure in address

allocation, which enhances the ability to aggregate routes even more efficiently than IPv4 due to its vast address space and flexible subnetting options.

- High scalability

> IPv6 extension headers, inserted between the basic header and payload as needed, enhance encryption, mobility, optimal path selection, and QoS without Overloading the main data packet, thus improving packet forwarding efficiency.

- Enhanced security features.

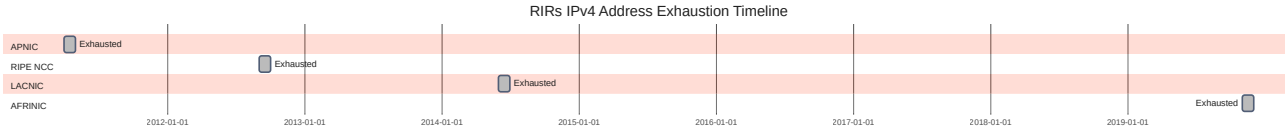
> IPsec, source address authentication, and other security features ensure E2E security, preventing NAT from damaging the integrity of E2E communication.

- Support for mobility and QoS.

> mobile devices can switch between network areas more efficiently without unnecessary extra paths, making the network faster and more reliable.

> A Flow Label field is additionally defined and can be used to allocate a specific resource for a special service and data flow.

1.1.1.2 Regional Internet Registries (RIRs) Status



> **Note**
>
> - **IANA (Internet Assigned Numbers Authority):** is an organization responsible for coordinating global IP address allocation and managing the DNS root zone.
> - **RIR (Regional Internet Registry):** is an entity that oversees the allocation and registration of Internet number resources within a specific region of the world.

1.1.1.3 IPv6 Header

Field	Description
Version	Indicates the IP protocol version, set to 6 for IPv6.
Traffic Class	Specifies packet priority for Quality of Service (QoS).
Flow Label (NEW)	Identifies data flows for special handling.
Payload Length	Length of data following the header, in bytes.
Next Header	Type of the next header or upper-layer protocol.
Hop Limit	Decrements by 1 at each hop; packet discarded if zero.
Source Address	The 128-bit address of the sender of the packet.
Destination Address	The 128-bit address where the packet is being sent to.

Extension Header Field	Description in Simple Terms
Hop-by-Hop Options Header	Provides instructions for each router the packet passes through on the network, such as how to process the packet.
Destination Options Header	Carries additional information for the final destination of the packet, and is checked after any Routing or Fragment headers have been processed.
Routing Header	Lists one or more routers the packet should visit before reaching its final destination.

Extension Header Field	Description in Simple Terms
Fragment Header	Used for splitting large packets into smaller pieces that can travel across networks with smaller MTU limits.
Authentication Header (AH)	Provides a way to check if the packet is from a trusted sender and hasn't been tampered with (part of IPsec).
Encapsulating Security Payload	Helps keep data in the packet secret and secure from eavesdroppers, also part of IPsec (ESP header).

Extension headers are optional and variable in length. Only one `::` allowed per address to represent consecutive zeros.

1.1.1.4 Abbreviating IPv6 Addresses

Note

> An IPv6 address is 128 bits long, typically divided into eight 16-bit blocks in hexadecimal form separated by colons. For example, an IPv6 address can look like this: 2001:0DB8:0000:0000:0008:0800:200C:417A.

> IPv6 addresses can be shortened by removing leading zeroes within each block, and in a row blocks of zeroes can be replaced by a double colon (::), but only once in an address. For instance:

- **Full IPv6 Address:**
  - 2001:0DB8:0000:0000:0008:0800:200C:417A
- **Abbreviated:**
  - 2001:DB8::8:800:200C:417A

> **Tip**
>
> Also, the case of letters doesn't matter.

1.1.1.5 Classification of IPv6 Addresses

1.1.1.5.1 Unicast Addresses

- **Global Unicast Address** (`GUA`): `2000::/3`
- **Unique Local Address** (`ULA`): `FD00::/8`
- **Link-local Address** (`LLA`): `FE80::/10`
- **Special IPv6 address**
  - Unspecified address (::/128): Used as a source address for packets such as Neighbor Solicitation messages during Duplicate Address Detection (DAD) or DHCPv6 client requests.
  - Loopback address (::1/128): Functions like IPv4's 127.0.0.1 for local loopback, where packets sent to it are directed back to the sending host for testing.

1.1.1.5.2 Multicast Addresses

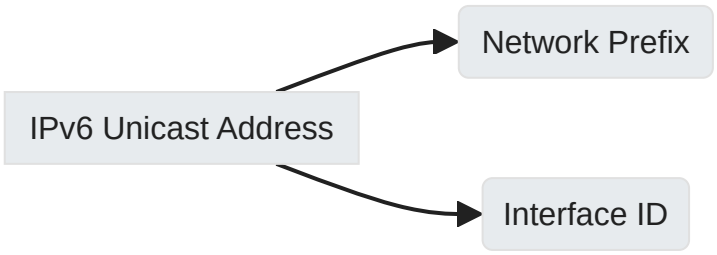
Identify multiple interfaces; packets sent to all group members.

1.1.1.5.3 Anycast Addresses

Identify a group of interfaces; packets sent to nearest member.

1. Anycast addresses offer service redundancy.
2. They enable efficient service delivery by selecting the optimal path.

1.1.1.6 Unicast Address Format



- **Network Prefix:** n bits (similar to IPv4's network ID)
- **Interface ID:** 128-n bits (similar to IPv4's host ID)

> Commonly, both the network prefix and interface ID are 64 bits long.

1.1.1.6.1 Interface ID Generation Methods

- Manual configuration
- Automatic system generation

> An automatic system generation for creating a unique identifier automatically assigns a distinct code to each user without human input.

- EUI-64 standard

> The EUI-64 standard extends a 48-bit MAC address to create a unique 64-bit interface identifier for IPv6 addresses by inserting 'FFFE' in the

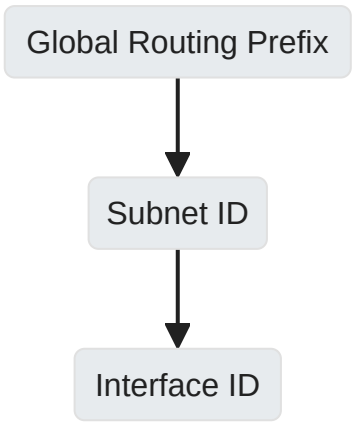
> middle and flipping the seventh bit. EUI Create unique identifier 64 bit is paired with a network prefix to form a complete IPv6 address.

1.1.1.6.1.1 EUI-64 Example Conversion

---

1. Convert MAC `3C-52-82-49-7E-9D` to binary.
2. Invert bit 7.
3. Insert `FFFE` in the middle.
4. **Result:** `3E-52-82-FF-FE-49-7E-9D`

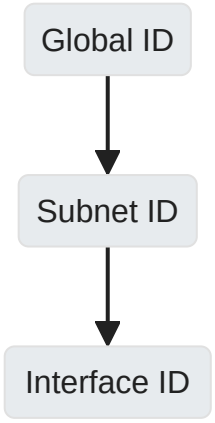
1.1.1.6.2 Global Unicast Addresses (GUAs)



> Network address is 64 bit and host address is 64 bit

> GUAs start with `2000::/3` . They are globally unique and used for Internet access.

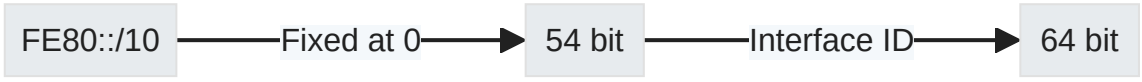
1.1.1.6.3 Unique Local Addresses (ULAs)



> It has 40 bit for random id(global id) Generated using a pseudo-random algorithm

> ULAs start with `FC00::/7` or more specifically `FD00::/8` for local communication.

1.1.1.6.4 Link-Local Addresses (LLAs)



> prefix of FE80::/10.

> LLAs are used within a single link and cannot be routed externally.

> Each IPv6 interface must have an LLA.

1.1.1.6.5 Multicast Address Format

---

8 bits	4 bits	4 bits	80 bits	32 bits
11111111	Flags	Scope	Reserved (must be 0)	Group ID

Field	Bits	Description
Flags	4	Indicates permanent/transient group
Scope	4	Specifies multicast group scope
GroupID	32	Multicast group identifier

Note

- **All nodes:** FF01::1, FF02::1
- **All routers:** FF01::2, FF02::2

1.1.1.6.5.1 Scopes:

---

1. Interface-local scope: span only a single interface.
2. Link-local scope: limited to the local network segment.
3. Site-local scope: confined to the local site.
4. Organization-local scope: spans across organizational boundaries.
5. Global scope: encompasses the entire IPv6 internet.

1.1.1.6.5.2 Solicited-Node Multicast Address

---

a solicited-node multicast address is a special type of address used in IPv6 networks to help devices find each other on the same local network. When a device has an IPv6 address, it automatically gets a corresponding solicited-node multicast address. This special address is used for two main purposes:

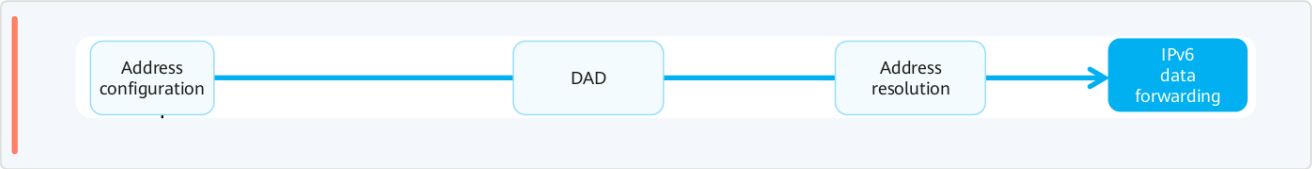
1. **Neighbor Discovery**: It helps devices on the same local network segment to identify who their neighbors are.

2. **Duplicate Address Detection (DAD)**: It ensures that no two devices try to use the same IP address on the network.

> **Note**
>
> This solicited-node multicast address is only relevant and used within the local network (it doesn't work over the internet). When one device wants to communicate with another, instead of sending a message to everyone, it sends a message just to this special multicast address. Only the intended recipient, which 'listens' for messages sent to this address, will receive and process the message. This makes things more efficient because it avoids bothering all other devices on the network with unnecessary traffic.

1.2 IPv6 Overview

1.2.1 Address Configuration Process



1.2.1.1 Global Unicast Address (GUA)

- Manual Configuration or SLAAC/DHCPv6.

1.2.2 Neighbor Discovery Protocol (NDP)

> NDP stands for Neighbor Discovery Protocol, and it's used by devices on an IPv6 network to discover each other and to determine each other's link-layer addresses, find routers, and maintain reachability information about the paths to other active neighbor nodes.

> - Defined in RFC 4861.

ICMPv6 Messages:

- **RS (Router Solicitation):** A device sends this message asking for routing information.
- **RA (Router Advertisement):** A router sends this message in response, providing routing information.
- **NS (Neighbor Solicitation):** A device sends this message either looking for another device's physical address or doing DAD.
- **NA (Neighbor Advertisement):** A device replies with this message, providing its physical address or responding to DAD.

1. **SLAAC (Stateless Address Autoconfiguration):** Devices automatically configure their IP addresses using Router Advertisements from NDP to obtain network prefixes.

> Routers send Router Advertisements (RA) with prefix information, and devices use this information to generate an IP address.

2. **DAD (Duplicate Address Detection):** Devices use NDP to send a Neighbor Solicitation message for their proposed IP to ensure its uniqueness on the network.

> sending a Neighbor Solicitation (NS) message with its proposed IP address as the target address. If another device is already using that

> address, it will respond with a Neighbor Advertisement (NA), indicating there's a conflict.

3. **Address Resolution:** NDP facilitates discovery of a device's link-layer address by exchanging Neighbor Solicitation and Advertisement messages.

> A device sends an NS message asking "Who has this IPv6 address?" and the owner of that IP sends back an NA message with its link-layer address.

4. **Prefix Advertisement:** Routers broadcast IPv6 prefix information via NDP in Router Advertisements for address configuration on the local network.

> This is done through Router Advertisement messages which include prefix information options.

1.2.3 Dynamic IPv6 Address Configuration

1.2.3.1 Stateless Address Autoconfiguration (SLAAC)

- Uses ICMPv6 RA and RS messages.
- Host generates an address using the prefix from RA and its own interface ID.

> Only IPv6 addresses can be obtained

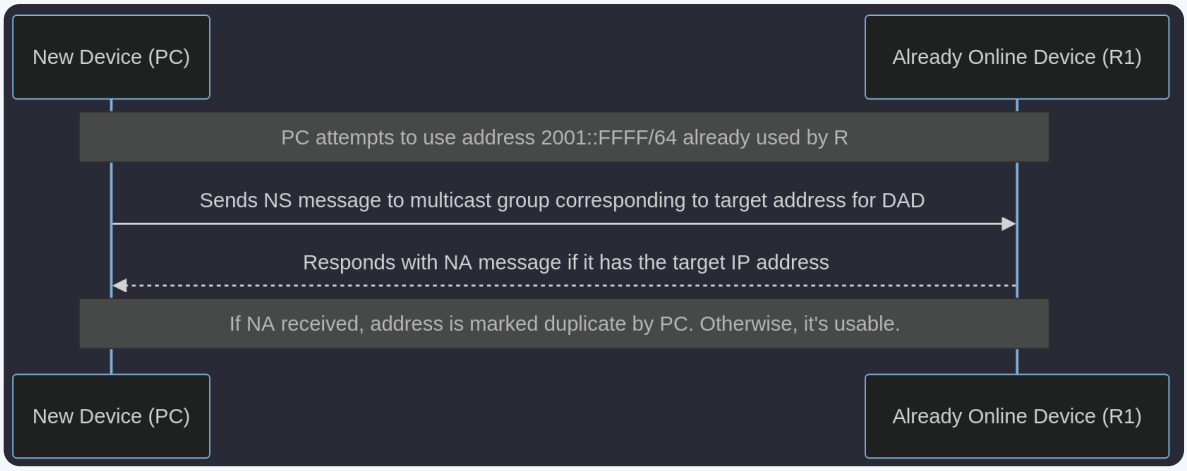
1.2.3.2 Stateful Address Autoconfiguration (DHCPv6)

- Managed by DHCPv6 server.
- Provides full IPv6 addresses and other network parameters.

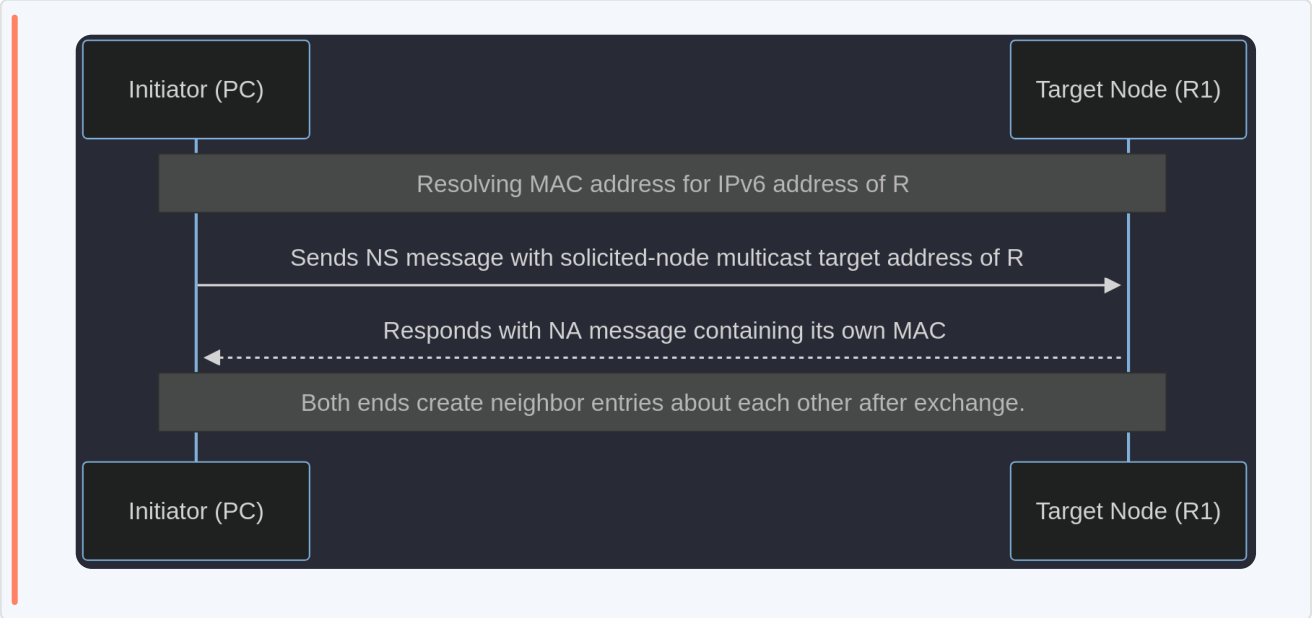
Flag	Purpose
M Flag	Managed address configuration
O Flag	Other stateful configurations

> M flag = 1 and O flag = 1 indicates stateful configuration via DHCPv6.

1.2.4 DAD Mechanism Example



1.2.4.1 Address Resolution with NDP Example



1.3 Typical IPv6 Configuration Examples

1.3.1 General Commands

1.3.1.1 Enabling IPv6 Globally

```Markdown
[Huawei] ipv6
```

> Enable IPv6 on the device globally.

1.3.1.2 Enabling IPv6 on an Interface

```Markdown
[Huawei-GigabitEthernet0/0/0] ipv6 enable
```

> Activate IPv6 on a specific interface.

1.3.1.3 Link Local Address (LLA)

1.3.1.3.1 Configuring LLA Manually/Automatically

```Markdown
[Huawei-GigabitEthernet0/0/0] ipv6 address <ipv6-address> link-local
```

> Set LLA manually

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

> Configure LLA automatically.

1.3.1.4 Global Unicast Address (GUA)

1.3.1.4.1 Configuring GUA Manually/Automatically

```Markdown
[Huawei-GigabitEthernet0/0/0] ipv6 address {<ipv6-address> prefix-length | <ipv6-address>/prefix-length}
```

Assign GUA manually.

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

Obtain GUA via DHCPv6/stateless autoconfig.

1.3.1.5 Static Routing

1.3.1.6 Adding a Static Route

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

Define static routes.

1.3.1.7 Display Commands

Command	Description
`display ipv6 interface [<interface-type> <interface-number> | brief]`	Show IPv6 details of interfaces.
`display ipv6 neighbors`	List neighbor entries (similar to ARP in IPv4).

1.3.1.8 Router Advertisement (RA) Messages

1.3.1.8.1 Enabling RA Messages on an Interface

> **Note**
>
> By default, Huawei routers do not send ICMPv6 RA messages necessary for SLAAC. To enable this function:
>
> - `[Huawei-GigabitEthernet0/0/0] undo ipv6 nd ra halt` : Allow the interface to send RA messages.