

# 1 IPv6 Basics Commands

Command	Function
<a href="#">clear ipv6 neighbors</a>	Clear dynamically learned neighbor discovery (ND) entries.
<a href="#">ipv6 address</a>	Configure an IPv6 address.
<a href="#">ipv6 address autoconfig</a>	Enable IPv6 stateless address auto-configuration on an interface.
<a href="#">ipv6 icmp error-interval</a>	Configure the transmission rate of other ICMPv6 error messages.
<a href="#">ipv6 enable</a>	Enable the IPv6 protocol on an interface.
<a href="#">ipv6 gateway</a>	Configure the IPv6 default gateway for a management interface.
<a href="#">ipv6 general-prefix</a>	Configure an IPv6 general prefix.
<a href="#">ipv6 hop-limit</a>	Configure the hop limit for unicast packets.
<a href="#">ipv6 icmp source</a>	Configure a specified source address for sending ICMPv6 packets.
<a href="#">ipv6 mtu</a>	Configure the MTU for IPv6 packets.
<a href="#">ipv6 nd cache interface-limit</a>	Configure the maximum number of neighbor cache entries that can be learned by an interface.
<a href="#">ipv6 nd dad attempts</a>	Configure the number of neighbor solicitation (NS) packets to be sent consecutively during duplicate address detection (DAD).
<a href="#">ipv6 nd dad learning enable</a>	Enable an interface to learn ND entries via DAD NS packets.
<a href="#">ipv6 nd dad retry</a>	Configure the DAD interval.
<a href="#">ipv6 nd log enable</a>	Enable ND logging.
<a href="#">ipv6 nd log rate</a>	Configure the ND logging rate.
<a href="#">ipv6 nd managed-config-flag</a>	Configure the Managed address configuration flag bit in the RA packets.
<a href="#">ipv6 nd max-opt</a>	Configure the number of ND options supported by

	the device.
<a href="#"><u>ipv6 nd ns-interval</u></a>	Configure the NS packet retransmission interval.
<a href="#"><u>ipv6 nd other-config-flag</u></a>	Configure the Other stateful configuration flag bit in the RA packets.
<a href="#"><u>ipv6 nd prefix</u></a>	Configure the address prefix to be contained in the RA packets.
<a href="#"><u>ipv6 nd packet rate-statistics interval</u></a>	Configure the interval for collecting ND packet rate statistics.
<a href="#"><u>ipv6 nd ra dns server suppress</u></a>	Configure RA packets not to carry the RDNSS option.
<a href="#"><u>ipv6 nd ra dns server sequence</u></a>	Configure the address of the DNS recursive query server in RA packets.
<a href="#"><u>ipv6 nd ra dns search-list suppress</u></a>	Configure RA packets not to carry the DNSSL option.
<a href="#"><u>ipv6 nd ra dns search-list sequence</u></a>	Configure the DNS suffix to be contained in an RA packet.
<a href="#"><u>ipv6 nd ra-hoplimit</u></a>	Configure the hop limit for RA packets to be sent by an interface.
<a href="#"><u>ipv6 nd ra-interval</u></a>	Configure the interval for sending RA packets on an interface.
<a href="#"><u>ipv6 nd ra-lifetime</u></a>	Configure the router lifetime in RA packets to be sent on an interface.
<a href="#"><u>ipv6 nd ra-mtu</u></a>	Configure the MTU for RA packets to be sent on an interface.
<a href="#"><u>ipv6 nd ra-url</u></a>	Configure the Uniform Resource Locator (URL) for RA packets to be sent on an interface.
<a href="#"><u>ipv6 nd ra-url</u></a>	Configure the URL option type value for RA packets to be sent.
<a href="#"><u>ipv6 nd reachable-time</u></a>	Configure the duration in which the device considers a neighbor reachable.
<a href="#"><u>ipv6 nd resolve vlan</u></a>	Configure the device to actively send NS packets to a specific sub VLAN in a super VLAN.
<a href="#"><u>ipv6 nd stale-time</u></a>	Configure the duration in which a neighbor keeps in stale state.
<a href="#"><u>ipv6 nd suppress-auth-vlan-ns</u></a>	Configure an interface not to send NS packets to an

	authenticated VLAN.
<a href="#"><u>ipv6 nd suppress-ra</u></a>	Configure an interface not to send RA packets.
<a href="#"><u>ipv6 nd unresolved</u></a>	Configure the maximum number of unresolved ND entries.
<a href="#"><u>ipv6 neighbor</u></a>	Configure a static neighbor entry.
<a href="#"><u>ipv6 ns-linklocal-src</u></a>	Configure the link-local address as the source address for sending NS packets.
<a href="#"><u>ipv6 redirects</u></a>	Enable the ICMPv6 redirection function.
<a href="#"><u>ipv6 source-route</u></a>	Configure the device to forward IPv6 packets carrying the routing header.
<a href="#"><u>local-proxy-nd enable</u></a>	Enable the local ND proxy function on an interface.
<a href="#"><u>show nd suppress table</u></a>	Display the ND suppression table, which gives the details about the ND suppression entries.
<a href="#"><u>show ipv6 address</u></a>	Display the information about an IPv6 address.
<a href="#"><u>show ipv6 general-prefix</u></a>	Display the prefix information in a general prefix.
<a href="#"><u>show ipv6 interface</u></a>	Display the information about an IPv6 interface.
<a href="#"><u>show ipv6 nd</u></a>	Display the statistics on IPv6 ND packets.
<a href="#"><u>show ipv6 neighbors</u></a>	Display IPv6 neighbor tables.
<a href="#"><u>show ipv6 neighbors statistics</u></a>	Display the statistics on IPv6 neighbor tables.
<a href="#"><u>show ipv6 packet statistics</u></a>	Display the statistics on IPv6 packets.
<a href="#"><u>show ipv6 raw-socket</u></a>	Displays all IPv6 raw sockets.
<a href="#"><u>show ipv6 routers</u></a>	Display neighbor router information and RA packets.
<a href="#"><u>show ipv6 sockets</u></a>	Display all IPv6 raw sockets.
<a href="#"><u>show ipv6 udp</u></a>	Display all IPv6 UDP sockets.
<a href="#"><u>show ipv6 udp statistics</u></a>	Display the statistics on IPv6 UDP sockets.

## 1.1 clear ipv6 neighbors

### Function

Run the **clear ipv6 neighbors** command to clear dynamically learned neighbor discovery (ND) entries.

### Syntax

```
clear ipv6 neighbors [ vrf vrf-name ] [ oob ] [ interface-type interface-number ]
```

### Parameter Description

**vrf vrf-name**: Specifies the name of a virtual routing and forwarding (VRF) instance. If this parameter is not specified, it indicates the public network instance.

**oob**: Clears all the ND entries dynamically learned via the Neighbor Discovery Protocol (NDP) on the management interface.

**interface-type interface-number**: Interface type and interface number. After this parameter is specified, the dynamic ND entries of a specified interface will be deleted.

### Command Modes

Privileged EXEC mode

### Default Level

14

### Usage Guidelines

Static ND entries will not be cleared.

When this command is run in gateway authentication mode, the device will not delete dynamic ND entries in authenticated VLANs.

### Examples

The following example clears all the dynamically learned ND entries.

```
Hostname> enable
Hostname# clear ipv6 neighbors
```

The following example clears all the dynamically learned ND entries on the management interface.

```
Hostname> enable
Hostname# clear ipv6 neighbors oob
```

The following example clears all the dynamically learned ND entries on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear ipv6 neighbors gigabitEthernet 0/1
```

### Notifications

N/A

### Platform Description

N/A

## Related Commands

N/A

## 1.2 ipv6 address

### Function

Run the **ipv6 address** command to configure an IPv6 address.

Run the **no** form of this command to remove this configuration.

No IPv6 address is configured by default.

### Syntax

**ipv6 address** *ipv6-address/prefix-length*

**no ipv6 address** *ipv6-address/prefix-length*

**ipv6 address** *ipv6-prefix/prefix-length eui-64*

**no ipv6 address** *ipv6-prefix/prefix-length eui-64*

**ipv6 address** *prefix-name sub-bits/prefix-length [ eui-64 ]*

**no ipv6 address** *prefix-name sub-bits/prefix-length [ eui-64 ]*

**no ipv6 address**

### Parameter Description

*ipv6-address*: IPv6 address, which must comply with the address format defined in RFC 4291. Separated by a colon (:), each address field consists of 16 bits and is represented by hexadecimal digits.

*ipv6-prefix*: IPv6 address prefix, which must comply with the address format defined in RFC 4291. Separated by a colon (:), each address field consists of 16 bits and is represented by hexadecimal digits.

*prefix-length*: Length of an IPv6 address prefix, that is, the network address part in an IPv6 address.

*prefix-name*: Name of a general prefix. This specified general prefix is used to generate an interface address.

*sub-bits*: Subprefix bits and host bits. This value is combined with the prefix in the general prefix to generate an interface address. This value must be represented in the form of colon hexadecimal notation as documented in RFC 4291.

**eui-64**: Indicates that the generated IPv6 address consists of the configured address prefix and 64-bit interface ID.

### Command Modes

Interface configuration mode

### Default Level

14

### Usage Guidelines

If an IPv6 interface is created and the link is in up state, the system automatically generates a link-local address for this interface.

The IPv6 address of an interface can also be generated using the general prefix mechanism. That is, IPv6 address = General prefix + Sub prefix + Host bits. The general prefix can be configured by running the **ipv6 general-prefix** command or learned by the prefix discovery (PD) function of the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) client. For details, see "Configuring DHCPv6" in the *IP Configuration Guide*. The sub prefix + host bits are specified by the *sub-bits/prefix-length* parameter in this command.

---

**⚠ Caution**

- If an interface is bound to a multiprotocol VRF instance configured with no IPv6 address family, no IPv6 address can be configured for this interface. You can configure an IPv6 address for this interface only after configuring an IPv6 address family for the multiprotocol VRF instance.
  - Anycast addresses (such as 1000:1::100/120 and 1000::/64) cannot be configured as interface IPv6 addresses. Exceptionally, anycast addresses with a subnet prefix of 127 or greater can be configured.
- 

## Examples

The following example sets the IPv6 address to 2001:1::1/64 for port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 address 2001:1::1/64
```

The following example configures an address for port GigabitEthernet 0/1 by using the general prefix my-prefix and setting the subprefix bits and host bits to 0:0:0:7272::72/64.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 address my-prefix 0:0:0:7272::72/64
```

---

**i Note**

Assume that the prefix configured by using the general prefix my-prefix is 2001:1111:2222::/48. The generated interface IPv6 address is 2001:1111:2222:7272::72/64.

---

## Notifications

N/A

## Common Errors

N/A

## Platform Description

N/A

## Related Commands

- [ipv6 general-prefix](#)
- [show ipv6 address](#)
- [show ipv6 interface](#)

## 1.3 ipv6 address autoconfig

### Function

Run the **ipv6 address autoconfig** command to enable IPv6 stateless address auto-configuration on an interface.

Run the **no** form of this command to disable this feature.

The IPv6 stateless address auto-configuration is disabled on an interface by default.

### Syntax

```
ipv6 address autoconfig [ default ]
```

```
no ipv6 address autoconfig
```

### Parameter Description

**default:** Generates a default route for the address that is automatically configured under stateless conditions. Only one L3 interface on a device can use the **default** keyword. No default route is generated by default.

### Command Modes

Interface configuration mode

### Default Level

14

### Usage Guidelines

---

**⚠ Caution**

If an interface is bound to a multiprotocol VRF instance not configured with the IPv6 address family, the IPv6 stateless address auto-configuration cannot be enabled on the interface. You can enable the IPv6 stateless address auto-configuration on this interface only after configuring an IPv6 address family for the multiprotocol VRF instance.

---

Stateless address auto-configuration means that, when a device receives a router advertisement (RA) packet, an interface address in EUI-64 format can be automatically generated using prefix information in the RA packet.

If the RA packet received contains **other-config-flag**, the interface will get other configuration parameters such as the IPv6 address of the domain name system (DNS) server and the IPv6 address of the Network Time Protocol (NTP) server through DHCPv6.

### Examples

The following example enables the IPv6 stateless address auto-configuration on port GigabitEthernet 0/1 and generates a default route.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 address autoconfig default
```

**Notifications**

N/A

**Common Errors**

N/A

**Platform Description**

N/A

**Related Commands**

- [show ipv6 address](#)
- [show ipv6 interface](#)

## 1.4 ipv6 icmp error-interval

**Function**

Run the **ipv6 icmp error-interval** command to configure the transmission rate of other ICMPv6 error messages.

Run the **no** form of this command to restore the default configuration.

Ten ICMPv6 error messages are transmitted in 100 ms by default.

**Syntax**

```
ipv6 icmp error-interval [ too-big ] interval [ bucket-size ]
```

```
no ipv6 icmp error-interval [ too-big ] interval [ bucket-size ]
```

**Parameter Description**

**too-big**: Specifies the transmission rate of ICMPv6 Packet Too Big messages.

*interval*: Refresh cycle of a token bucket, in ms. The value range is from 0 to 2147483647, and the default value is **100**. If the value is **0**, the transmission rate of ICMPv6 error messages is not restricted.

*bucket-size*: Number of tokens contained in a token bucket. The value range is from 1 to 200, and the default value is **10**.

**Command Modes**

Global configuration mode

**Default Level**

14

**Usage Guidelines**

To prevent denial of service (DoS) attacks, you can use the token bucket algorithm to restrict the transmission rate of ICMPv6 error messages.

If the length of an IPv6 packet to be forwarded exceeds the IPv6 maximum transmission unit (MTU) of the outbound interface, the router discards this IPv6 packet and sends an ICMPv6 Packet Too Big message to the source IPv6 address. This error message is mainly used for IPv6 PMTUD. When there are too many other



ICMPv6 error messages, the ICMPv6 Packet Too Big message cannot be sent, causing the failure of IPv6 PMTUD. Therefore, you are advised to restrict the transmission rate of ICMPv6 Packet Too Big messages and other ICMPv6 error packets separately.

---

**Note**

Although ICMPv6 Redirect packets are not a type of ICMPv6 error messages, the device limit the transmission rate of other ICMPv6 error messages, together with ICMPv6 Redirect packets.

---

Since the precision of the timer is 10 milliseconds, you are advised to set the refresh cycle of a token bucket to an integer multiple of 10 milliseconds. If the refresh cycle is set to a value greater than 0 and smaller than 10 milliseconds, the refresh cycle that actually takes effect is 10 milliseconds. For example, if the transmission rate is set to 1 packet per 5 milliseconds, two ICMP error packets are actually sent per 10 milliseconds. If the refresh cycle is not an integral multiple of 10 milliseconds, the refresh cycle that actually takes effect is automatically converted into an integral multiple of 10 milliseconds. For example, if the transmission rate is set to 3 packets per 15 milliseconds, two ICMP error packets are actually sent per 10 milliseconds.

## Examples

The following example sets the transmission rate of ICMPv6 Packet Too Big messages to 100 pps.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 icmp error-interval too-big 1000 100
```

The following example sets the transmission rate of other ICMPv6 error messages to 10 pps.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 icmp error-interval 1000 10
```

## Notifications

N/A

## Common Errors

N/A

## Platform Description

N/A

## Related Commands

N/A

## 1.5 ipv6 enable

### Function

Run the **ipv6 enable** command to enable the IPv6 protocol on an interface.

Run the **no** form of this command to disable this feature.

The IPv6 protocol is disabled on an interface by default.

## Syntax

**ipv6 enable**  
**no ipv6 enable**

## Parameter Description

N/A

## Command Modes

Interface configuration mode

## Default Level

14

## Usage Guidelines

There are two ways to enable the IPv6 function on an interface:

- Configure the **ipv6 enable** command on an interface;
- Directly configure an IPv6 address on an interface.

---

### ⚠ Caution

If an interface is bound to a multiprotocol VRF instance configured with no IPv6 address family, IPv6 cannot be enabled on this interface. You can enable IPv6 on this interface only after configuring an IPv6 address family for the multiprotocol VRF instance.

---

If an IPv6 address is configured on an interface, IPv6 is automatically enabled on this interface and cannot be disabled even when you run the **no ipv6 enable** command.

## Examples

The following example enables the IPv6 function on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 enable
```

## Notifications

N/A

## Common Errors

N/A

## Platform Description

N/A

## Related Commands

- [show ipv6 address](#)
- [show ipv6 interface](#)

## 1.6 ipv6 gateway

### Function

Run the **ipv6 gateway** command to configure the IPv6 default gateway for a management interface.

No IPv6 default gateway is configured for a management interface by default.

### Syntax

```
ipv6 gateway ipv6-address
```

### Parameter Description

*ipv6-address*: IPv6 default gateway address of a management interface.

### Command Modes

Interface configuration mode

### Default Level

14

### Usage Guidelines

The type of a management interface is MGMT and the interface number is fixed to 0.

### Examples

The following example sets the IPv6 default gateway of a management interface to 2001:1::1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface mgmt 0
Hostname(config-if-MGMT 0)# ipv6 gateway 2001:1::1
```

### Notifications

N/A

### Common Errors

N/A

### Platform Description

N/A

### Related Commands

- [show ipv6 interface](#)

## 1.7 ipv6 general-prefix

### Function

Run the **ipv6 general-prefix** command to configure an IPv6 general prefix.

Run the **no** form of this command to remove this configuration.

No IPv6 general prefix is configured by default.

### Syntax

```
ipv6 general-prefix prefix-name ipv6-prefix/prefix-length
```

```
no ipv6 general-prefix prefix-name ipv6-prefix/prefix-length
```

### Parameter Description

*prefix-name*: Name of a general prefix.

*ipv6-prefix/prefix-length*: Network prefix value and prefix length of the general prefix.

### Command Modes

Global configuration mode

### Default Level

14

### Usage Guidelines

A general prefix can facilitate network numbering. The prefix defined in a general prefix can be referenced by a longer specific prefix. When the general prefix changes, the specific prefixes that reference the general prefix will change accordingly. When a network ID changes, only the general prefix needs to be changed.

A general prefix can contain several prefixes.

### Examples

The following example configures a general prefix named my-prefixIPv6, with the network prefix value of 2001:1111:2222::/48.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 general-prefix my-prefix 2001:1111:2222::/48
```

### Notifications

N/A

### Common Errors

N/A

### Platform Description

N/A

### Related Commands

- [show ipv6 general-prefix](#)

## 1.8 ipv6 hop-limit

### Function

Run the **ipv6 hop-limit** command to configure the hop limit for unicast packets.

Run the **no** form of this command to restore the default configuration.

The default hop limit for unicast packets is 64.

### Syntax

```
ipv6 hop-limit hop
```

```
no ipv6 hop-limit
```

### Parameter Description

*hop*: Hop limit value. The value range is from 1 to 255.

### Command Modes

Global configuration mode

### Default Level

14

### Usage Guidelines

This command is effective to unicast packets only.

### Examples

The following example sets the hop limit for unicast packets to 100.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 hop-limit 100
```

### Notifications

N/A

### Common Errors

N/A

### Platform Description

N/A

### Related Commands

N/A

## 1.9 ipv6 icmp source

### Function

Run the **ipv6 icmp source** command to configure a specified source address for sending ICMPv6 packets.

Run the **no** form of this command to restore the default configuration.

No specified source address is configured for ICMPv6 packets by default.

### Syntax

```
ipv6 icmp source [ vrf vrf-name ] ipv6-address
```

## no ipv6 icmp source

### Parameter Description

**vrf** *vrf-name*: Specifies a VRF instance.

**ipv6-address**: IPv6 address used to send packets.

### Command Modes

Global configuration mode

### Default Level

14

### Usage Guidelines

In a network with a large number of IPv6 addresses configured, it is complex for receivers to recognize the device, from which an ICMPv6 packet is sent. To simplify the judgment, you can configure a specified source address for ICMPv6 packets. You can choose a specified address, like the address of the loopback interface, as the source address of ICMPv6 packets.

### Examples

The following example sets the source address of ICMPv6 reply packets to 1001::1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 icmp souce 1001::1
```

### Notifications

N/A

### Common Errors

N/A

### Platform Description

N/A

### Related Commands

N/A

## 1.10 ipv6 mtu

### Function

Run the **ipv6 mtu** command to configure the MTU for IPv6 packets.

Run the **no** form of this command to restore the default configuration.

The MTU value of IPv6 packets is the same as the value configured by running the **mtu** command on an interface by default.

### Syntax

**ipv6 mtu** *mtu*

## no ipv6 mtu

### Parameter Description

*mtu*: MTU of IPv6 packets. The value range is from 1280 to 1500.

### Command Modes

Interface configuration mode

### Default Level

14

### Usage Guidelines

If the size of an IPv6 packet exceeds the IPv6 MTU size, the packet will be fragmented.

For all devices in the same physical network segment, the IPv6 MTU of interconnected interfaces must be the same.

### Examples

The following example sets the IPv6 MTU of port gigabitEthernet 0/1 to 1400 bytes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 mtu 1400
```

### Notifications

N/A

### Common Errors

N/A

### Platform Description

N/A

### Related Commands

- [show ipv6 interface](#)

## 1.11 ipv6 nd cache interface-limit

### Function

Run the **ipv6 nd cache interface-limit** command to configure the maximum number of neighbor cache entries that can be learned by an interface.

Run the **no** form of this command to restore the default configuration.

The number of neighbor cache entries that can be learned by an interface is not limited by default.

### Syntax

**ipv6 nd cache interface-limit** *limit*

**no ipv6 nd cache interface-limit**

## Parameter Description

*limit*: Maximum number of neighbor cache entries that can be learned by an interface, including static and dynamic neighbor cache entries. The value range is from 1 to 8000.

## Command Modes

Interface configuration mode

## Default Level

14

## Usage Guidelines

Restricting the number of neighbor cache entries that can be learned by an interface can prevent malicious neighbor attacks. If this number is not restricted, a large number of neighbor cache entries will be generated on the device, occupying excessive memory space. The configured value must be equal to or greater than the number of the neighbor cache entries learned by the current interface. Otherwise, the configuration does not take effect. The configuration is subject to the ND entry capacity supported by the device.

## Examples

The following example sets the maximum number of neighbor cache entries that can be learned by port GigabitEthernet 0/1 to 100.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd cache interface-limit 100
```

## Notifications

N/A

## Common Errors

N/A

## Platform Description

N/A

## Related Commands

N/A

## 1.12 ipv6 nd dad attempts

### Function

Run the **ipv6 nd dad attempts** command to configure the number of neighbor solicitation (NS) packets to be sent consecutively during duplicate address detection (DAD).

Run the **no** form of this command to restore the default configuration.

The default number of NS packets to be sent consecutively during DAD is **1**.



## Syntax

```
ipv6 nd dad attempts attempts
```

```
no ipv6 nd dad attempts
```

## Parameter Description

*attempts*: Number of NS packets. The value range is from 0 to 600, and the default value is 1. When the parameter is set to 0, DAD is not enabled for the IPv6 address of this interface.

## Command Modes

Interface configuration mode

## Default Level

14

## Usage Guidelines

You need to enable DAD before configuring an IPv6 address for an interface. At this moment, the address is in tentative state. If no address conflict is detected by DAD, this address can be correctly used. If an address conflict is detected and the interface ID of this address is an EUI-64 ID, duplicate link-layer addresses exist on this link. In this case, the system automatically disables this interface to prevent IPv6-related operations on this interface. At the time, you must configure a new address for the interface and disable and then enable the interface to start DAD again.

When an interface changes from the down state to the up state, DAD is re-enabled on this interface.

## Examples

The following example configures three NS packets to be sent consecutively during DAD on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd dad attempts 3
```

## Notifications

N/A

## Common Errors

N/A

## Platform Description

N/A

## Related Commands

- [show ipv6 interface](#)

## 1.13 ipv6 nd dad learning enable

### Function

Run the **ipv6 nd dad learning enable** command to enable an interface to learn ND entries via DAD NS packets.

Run the **no** form of this command to restore the default configuration.

The function of learning ND entries via DAD NS packets by an interface is disabled by default.

### Syntax

**ipv6 nd dad learning enable**

**no ipv6 nd dad learning enable**

### Parameter Description

N/A

### Command Modes

Interface configuration mode

### Default Level

14

### Usage Guidelines

After this function is configured on an interface, the interface will create an ND entry in stale state when receiving a DAD NS packet.

By default, a general interface is disabled to learn ND entries via DAD NS packets but interfaces in a super VLAN are allowed to do so.

### Examples

The following example enables the function of learning ND entries via DAD NS packets on VLAN 1 interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface VLAN 1
Hostname(config-if-VLAN 1)# ipv6 nd dad learning enable
```

### Notifications

N/A

### Common Errors

N/A

### Platform Description

N/A

### Related Commands

N/A

## 1.14 ipv6 nd dad retry

### Function

Run the **ipv6 nd dad retry** command to configure the DAD interval.

Run the **no** form of this command to restore the default configuration.

The default DAD interval is 60s.

### Syntax

**ipv6 nd dad retry** *retry*

**no ipv6 nd dad retry**

### Parameter Description

*retry*: DAD interval after an address conflict is detected, in seconds. The value range is from 0 to 7200. If this value is set to **0**, the repeated DAD is disabled.

### Command Modes

Global configuration mode

### Default Level

14

### Usage Guidelines

You need to enable DAD before configuring an IPv6 address on an interface. If an address conflict is detected, the device will not receive IPv6 packets destined for this address.

With this command, the software will conduct DAD again on the conflicting address at the configured interval. If no address conflict is detected, this address can be normally used.

### Examples

The following example sets the DAD interval to 10s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd dad retry 10
```

### Notifications

N/A

### Common Errors

N/A

### Platform Description

N/A

### Related Commands

N/A

## 1.15 ipv6 nd log enable

### Function

Run the **ipv6 nd log enable** command to enable ND logging.

Run the **no** form of this command to disable this feature.

ND logging is disabled by default.

### Syntax

**ipv6 nd log enable**

**no ipv6 nd log enable**

### Parameter Description

N/A

### Command Modes

Global configuration mode

### Default Level

14

### Usage Guidelines

After this command is run, system logs will be printed for ND packets (including RS, RA, NS, and NA packets) received and sent by the device.

### Examples

The following example enables ND logging.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd log enable
```

### Notifications

N/A

### Common Errors

N/A

### Platform Description

N/A

### Related Commands

N/A

## 1.16 ipv6 nd log rate

### Function

Run the **ipv6 nd log rate** command to configure the ND logging rate.

Run the **no** form of this command to restore the default configuration.

Twenty ND logs are printed per minute by default.

### Syntax

**ipv6 nd log rate** *rate*

**no ipv6 nd log rate**

### Parameter Description

*rate*: ND logging rate, in entries/minute. The value range is from 0 to 65535. The default value is **20**, that is, 20 logs are printed per minute. The rate is not limited when *rate* is set to **0**.

### Command Modes

Global configuration mode

### Default Level

14

### Usage Guidelines

N/A

### Examples

The following example enables ND logging and sets the rate to 200 logs per minute.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd log enable
Hostname(config)# ipv6 nd log rate 200
```

### Notifications

N/A

### Common Errors

N/A

### Platform Description

N/A

### Related Commands

N/A

## 1.17 ipv6 nd managed-config-flag

### Function

Run the **ipv6 nd managed-config-flag** command to configure the **Managed address configuration** flag bit in the RA packets.

Run the **no** form of this command to remove this configuration.

The **Managed address configuration** flag bit in the RA packets is not configured by default.

### Syntax

```
ipv6 nd managed-config-flag
no ipv6 nd managed-config-flag
```

### Parameter Description

N/A

### Command Modes

Interface configuration mode

### Default Level

14

### Usage Guidelines

The settings of the **Managed address configuration** flag bit determine whether a host receiving this RA packet obtains an address through stateful address auto-configuration. If this flag bit is configured, an address will be obtained through stateful address auto-configuration. Otherwise, an address will not be obtained through stateful address auto-configuration.

### Examples

The following example configures the **Managed address configuration** flag bit in the RA packets on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd managed-config-flag
```

### Notifications

N/A

### Common Errors

N/A

### Platform Description

N/A

### Related Commands

- [show ipv6 interface](#)

## 1.18 ipv6 nd max-opt

### Function

Run the **ipv6 nd max-opt** command to configure the number of ND options supported by the device.

Run the **no** form of this command to restore the default configuration.

The device supports 10 ND options by default.

### Syntax

**ipv6 nd max-opt** *option*

**no ipv6 nd max-opt**

### Parameter Description

*option*: Number of supported options. The value range is from 1 to 100.

### Command Modes

Global configuration mode

### Default Level

14

### Usage Guidelines

This command is used to configure the maximum number of ND options that can be processed by the device, such as the source link-layer address option, MTU option, redirection option, and prefix option.

### Examples

The following example sets the maximum number of ND options supported by the device to 20.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd max-opt 20
```

### Notifications

N/A

### Common Errors

N/A

### Platform Description

N/A

### Related Commands

N/A

## 1.19 ipv6 nd ns-interval

### Function

Run the **ipv6 nd ns-interval** command to configure the NS packet retransmission interval.

Run the **no** form of this command to restore the default configuration.

The default NS packet retransmission interval of an interface is not specified when the interval is filled in the RA packets, and 1000 ms when it is used to control the interval for the device to transmit NS packets.

### Syntax

```
ipv6 nd ns-interval interval
```

```
no ipv6 nd ns-interval
```

### Parameter Description

*interval*: NS packet retransmission interval, in milliseconds. The value range is from 1000 to 4294967295, and the default value is **1000**.

### Command Modes

Interface configuration mode

### Default Level

14

### Usage Guidelines

The configured value is advertised in an RA packet and is also used on the device.

### Examples

The following example sets the NS packet retransmission interval to 2s on SVI 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)# ipv6 nd ns-interval 2000
```

### Notifications

N/A

### Common Errors

N/A

### Platform Description

N/A

### Related Commands

- [Ошибка: источник перекрёстной ссылки не найден](#)
- [show ipv6 interface](#)



## 1.20 ipv6 nd other-config-flag

### Function

Run the **ipv6 nd other-config-flag** command to configure the **Other stateful configuration** flag bit in the RA packets.

Run the **no** form of this command to remove this configuration.

No **Other stateful configuration** flag bit in the RA packets is configured by default.

### Syntax

```
ipv6 nd other-config-flag
```

```
no ipv6 nd other-config-flag
```

### Parameter Description

N/A

### Command Modes

Interface configuration mode

### Default Level

14

### Usage Guidelines

After the **Other stateful configuration** flag bit is set, the flag bit in the RA packets sent from the device is set to 1. After a host receives this flag bit, it obtains other information except the IPv6 address through DHCPv6 for auto-configuration. When **Managed address configuration** is set, **Other stateful configuration** is also set by default.

### Examples

The following example configures the **Other stateful configuration** flag bit in the RA packets on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd other-config-flag
```

### Notifications

N/A

### Common Errors

N/A

### Platform Description

N/A

### Related Commands

- [show ipv6 interface](#)

## 1.21 ipv6 nd prefix

### Function

Run the **ipv6 nd prefix** command to configure the address prefix to be contained in the RA packets.

Run the **no** form of this command to remove this configuration.

By default, the prefix in an RA packet on an interface is the prefix configured using the **ipv6 address** command on the interface.

### Syntax

```

ipv6 nd prefix { ipv6-prefix/prefix-length | default } [ valid-lifetime { infinite | preferred-lifetime } ] at valid-date
preferred-date | infinite { infinite | preferred-lifetime } ] [ no-advertise ] | [ [ off-link ] [ no-autoconfig ] ] | pool
pool-name | preference { high | medium | low } [ proxy ] ]
no ipv6 nd prefix { ipv6-prefix/prefix-length | default }

```

### Parameter Description

*ipv6-prefix/prefix-length*: IPv6 address prefix and prefix length, which must comply with the address representation format in RFC 4291.

*valid-lifetime*: Lifetime of a prefix considered valid by a host after the host receives the prefix in an RA packet, in seconds. The value range is from 0 to 4294967295. The default value is **2592000** seconds, that is, 30 days.

*preferred-lifetime*: Preferred lifetime of a prefix considered valid by a host after the host receives the prefix in an RA packet, in seconds. The value range is from 0 to 4294967295. The default value is **604800** seconds, that is, 7 days.

*valid-date preferred-date*: End time, before which the prefix in an RA packet is considered valid. The end time uses the format of dd+mm+yyyy+hh+mm.

*preferred-date*: Preferred end time, before which the prefix in an RA packet is considered valid. The end time uses the format of dd+mm+yyyy+hh+mm.

**infinite**: Indicates that it is permanently valid.

**default**: Configures the default parameter settings.

**no-advertise**: Indicates that the prefix is not advertised by a router.

**off-link**: If the prefix of the destination address in an IPv6 packet sent by a host matches the configured prefix, the destination address is considered on the same link (on-link) and directly reachable. This parameter indicates that this prefix is not used for on-link determination.

**no-autoconfig**: Indicates that the prefix in an RA packet received by a host cannot be used for address auto-configuration.

**pool** *pool-name*: Configures a specific prefix pool to be bound to an interface to ensure that different IPv6 prefixes are allocated to different users.

**preference**: Sets the routing priority. The value is **high**, **medium**, or **low**. The default value is **medium**.

**proxy**: Enables the ND proxy based on the prefix.

### Command Modes

Interface configuration mode

## Default Level

14

## Usage Guidelines

This command can be used to configure parameters for each prefix individually and determine whether to advertise a prefix.

By default, the prefix in an RA packet on an interface is the prefix configured using the **ipv6 address** command on the interface. To add other prefixes, run this command.

The **ipv6 nd prefix default** command is used to configure the default parameters on this interface. That is, if no parameter is specified when a prefix is added, the parameters configured using the **ipv6 nd prefix default** command will be used as the parameters of the new prefix. The default parameter configurations are abandoned once a parameter is specified for the prefix. That is, the use of the **ipv6 nd prefix default** command will not modify the configuration specified for a prefix, but only modify the configuration of a prefix that fully uses default parameter configurations.

The value of **at valid-date preferred-date** can be specified for a prefix in two ways: (1) specifying a fixed time length for each prefix in an RA packet; (2) specifying the end time. The valid lifetime of the prefix in each RA packet decreases till it becomes 0.

If no parameter is specified when a prefix is added, the default parameter configurations will apply. That is, this prefix is also not available for address auto-configuration.

## Examples

The following example configures the prefix of an address included in an RA packet to 2001::/64 and valid lifetime to 2,592000 seconds on VLAN 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)# ipv6 nd prefix 2001::/64 infinite 2592000
```

The following example configures the prefix of an address included in an RA packet not to be used for address auto-configuration on VLAN 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)# ipv6 nd default no-autoconfig
```

## Notifications

N/A

## Common Errors

N/A

## Platform Description

N/A

## Related Commands

- [show ipv6 interface](#)

## 1.22 ipv6 nd packet rate-statistics interval

### Function

Run the **ipv6 nd packet rate-statistics interval** command to configure the interval for collecting ND packet rate statistics.

Run the **no** form of this command to restore the default configuration.

The ND packet rate statistics collection is disabled by default.

### Syntax

**ipv6 nd packet rate-statistics interval** *interval*

**no ipv6 nd packet rate-statistics interval**

### Parameter Description

*interval*: Sampling interval, in seconds. The value range is from 60 to 86400.

### Command Modes

Global configuration mode

### Default Level

14

### Usage Guidelines

This configuration can modify the interval for collecting ND packet rate statistics. For example, if the interval is set to 60, the ND packet rate is calculated once every 60 seconds.

### Examples

The following example sets the interval for collecting ND packet rate statistics to 60 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd packet rate-statistics interval 60
```

### Notifications

N/A

### Common Errors

N/A

### Platform Description

N/A

### Related Commands

- [show ipv6 nd](#)

## 1.23 ipv6 nd ra dns server suppress

### Function

Run the **ipv6 nd ra dns server suppress** command to configure RA packets not to carry the RDNSS option.

Run the **no** form of this command to remove this configuration.

An RA packet does not carry the RDNSS option by default.

### Syntax

```
ipv6 nd ra dns server suppress
```

```
no ipv6 nd ra dns server suppress
```

### Parameter Description

N/A

### Command Modes

Interface configuration mode

### Default Level

14

### Usage Guidelines

The RDNSS option can provide IPv6 terminals with the address of the DNS recursive query server.

### Examples

The following example configures RA packets to carry the RDNSS option on SVI 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)# no ipv6 nd ra dns server suppress
```

### Notifications

N/A

### Common Errors

N/A

### Platform Description

N/A

### Related Commands

- [show ipv6 nd](#)

## 1.24 ipv6 nd ra dns server sequence

### Function

Run the **ipv6 nd ra dns server sequence** command to configure the address of the DNS recursive query server in RA packets.

Run the **no** form of this command to remove this configuration.

The address of the DNS recursive query server in RA packets is not configured by default.

### Syntax

```
ipv6 nd ra dns server ipv6-address { valid-lifetime | infinite } sequence number  
no ipv6 nd ra dns server ipv6-address { valid-lifetime | infinite } sequence number
```

### Parameter Description

*ipv6-address*: IPv6 address, which must comply with the address format defined in RFC 4291. Separated by a colon (:), each address field consists of 16 bits and is represented by hexadecimal digits.

*valid-lifetime*: Lifetime of the RDNSS option considered valid by a host after the host receives the RDNSS option in an RA packet, in seconds. The value range is from 0 to 4294967295. When the parameter is set to 0, the RDNSS option is no longer used.

**infinite**: Indicates that it is permanently valid.

**sequence number**: Indicates a sequence number, which represents the serial number of the same RDNSS option in an RA packet. The value range is from 0 to 7.

### Command Modes

Interface configuration mode

### Default Level

14

### Usage Guidelines

Only one option can be configured with the same sequence number under the same interface, and the same IPv6 address can only be used by one sequence number.

When configured, the RDNSS options are advertised through RA packet, and are organized in the descending order of sequence numbers.

### Examples

The following example configures RA packets to carry the RDNSS options, sets the address of the DNS recursive query server to 2018::1 and be permanently valid, and sets the sequence number to 0 on VLAN 1.

```
Hostname> enable  
Hostname# configure terminal  
Hostname(config)#interface vlan 1  
Hostname(config-if-VLAN 1)# no ipv6 nd ra dns server suppress  
Hostname(config-if-VLAN 1)# ipv6 nd ra dns server 2018::1 infinite sequence 0  
Hostname(config-if-VLAN 1)# ipv6 nd ra dns server 2020::1 1000 sequence 1
```

**Notifications**

N/A

**Common Errors**

N/A

**Platform Description**

N/A

**Related Commands**

- [show ipv6 nd](#)

## 1.25 ipv6 nd ra dns search-list suppress

**Function**

Run the **ipv6 nd ra dns search-list suppress** command to configure RA packets not to carry the DNSSSL option.

Run the **no** form of this command to remove this configuration.

RA packets do not carry the DNSSSL option by default.

**Syntax**

```
ipv6 nd ra dns search-list suppress
no ipv6 nd ra dns search-list suppress
```

**Parameter Description**

N/A

**Command Modes**

Interface configuration mode

**Default Level**

14

**Usage Guidelines**

The DNSSSL option can provide IPv6 terminals with a search list of DNS domain names.

**Examples**

The following example configures RA packets to carry the DNSSSL option on VLAN 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)#interface vlan 1
Hostname(config-if-VLAN 1)# no ipv6 nd ra dns search-list suppress
```

**Notifications**

N/A

**Common Errors**

N/A

**Platform Description**

N/A

**Related Commands**[show ipv6 nd](#)

## 1.26 ipv6 nd ra dns search-list sequence

### Function

Run the **ipv6 nd ra dns search-list sequence** command to configure the DNS suffix to be contained in an RA packet.

Run the **no** form of this command to remove this configuration.

The DNS suffix to be contained in an RA packet is not configured by default.

### Syntax

```
ipv6 nd ra dns search-list ipv6-domain-name { valid-lifetime | infinite } sequence number  
no ipv6 nd ra dns search-list ipv6-domain-name { valid-lifetime | infinite } sequence number
```

### Parameter Description

*ipv6-domain-name*: DNS suffix. It is a string of 1 to 64 characters.

*valid-lifetime*: Lifetime of the DNSSL option considered valid by a host after the host receives the DNSSL option in an RA packet, in seconds. The value range is from 0 to 4294967295. The default value is **1800**. When the value is set to **0**, it is no longer used.

**infinite**: Indicates that it is permanently valid.

**number**: Indicates a sequence number, which represents the serial number of the same DNSSL option in an RA packet.

### Command Modes

Interface configuration mode

### Default Level

14

### Usage Guidelines

Only one domain name option can be configured with the same sequence number under the same interface, and the same domain name can only be used by one sequence number.

When configured, the DNSSL option is advertised through RA packets, and are organized in the descending order of sequence numbers.

### Examples

The following example enables RA packets to carry the DNSSL option, sets the DNS suffix to text.com.cn, configures the suffix to be permanently valid, and sets the sequence number to 0 on SVI 1.

```
Hostname> enable  
Hostname# configure terminal  
Hostname(config)#interface vlan 1  
Hostname(config-if-VLAN 1)# no ipv6 nd ra dns search-list suppress  
Hostname(config-if-VLAN 1)# ipv6 nd ra dns search-list test.com.cn infinite  
sequence 0
```



**Notifications**

N/A

**Common Errors**

N/A

**Platform Description**

N/A

**Related Commands**

- [show ipv6 nd](#)

## 1.27 ipv6 nd ra-hoplimit

**Function**

Run the **ipv6 nd ra-hoplimit** command to configure the hop limit for RA packets to be sent by an interface.

Run the **no** form of this command to restore the default configuration.

The default hop limit of RA packets is 64.

**Syntax**

```
ipv6 nd ra-hoplimit hoplimit
```

```
no ipv6 nd ra-hoplimit
```

**Parameter Description**

*hoplimit*: Hop limit of RA packets. The value range is from 0 to 255.

**Command Modes**

Interface configuration mode

**Default Level**

14

**Usage Guidelines**

N/A

**Examples**

The following example sets the hop limit of RA packets to 110 on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd ra-hoplimit 110
```

**Notifications**

N/A

## Common Errors

N/A

## Platform Description

N/A

## Related Commands

- [show ipv6 interface](#)

## 1.28 ipv6 nd ra-interval

### Function

Run the **ipv6 nd ra-interval** command to configure the interval for sending RA packets on an interface.

Run the **no** form of this command to restore the default configuration.

The default interval for sending RA packets on an interface is 600s.

### Syntax

```
ipv6 nd ra-interval { interval | min-max min-interval max-interval }
```

```
no ipv6 nd ra-interval
```

### Parameter Description

*interval*: Interval for sending RA packets, in seconds. The value range is from 3 to 1800.

**min-max**: Sets the maximum and minimum intervals for sending RA packets.

*min-interval*: Minimum interval for sending RA packets, in seconds. The value range is from 3 to 1800.

*max-interval*: Maximum interval for sending RA packets, in seconds. The value range is from 4 to 1800.

### Command Modes

Interface configuration mode

### Default Level

14

### Usage Guidelines

When a device acts as a default routing device, the configured interval value cannot be greater than the lifetime of a router.

In addition, to prevent network bandwidth from being consumed by other devices sending RA packets at the same time on the link, the actual interval will fluctuate around this value by  $\pm 20\%$ .

If **min-max** is specified, then the actual interval will be randomly selected between the minimum and maximum values.

### Examples

The following example sets the interval for sending RA packets to 110 seconds on port GigabitEthernet 0/1.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd ra-interval 110
```

The following example sets the interval for sending RA packets to a value in the range of 110 seconds to 120 seconds on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd ra-interval min-max 110 120
```

### Notifications

N/A

### Common Errors

N/A

### Platform Description

N/A

### Related Commands

- [show ipv6 interface](#)

## 1.29 ipv6 nd ra-lifetime

### Function

Run the **ipv6 nd ra-lifetime** command to configure the router lifetime in RA packets to be sent on an interface.

Run the **no** form of this command to restore the default configuration.

The default router lifetime in RA packets to be sent on an interface is 1800 seconds.

### Syntax

```
ipv6 nd ra-lifetime lifetime
```

```
no ipv6 nd ra-lifetime
```

### Parameter Description

*lifetime*: Lifetime of a device acting as a default device of this interface, in seconds. The value range is from 0 to 9000.

### Command Modes

Interface configuration mode

### Default Level

14

## Usage Guidelines

The router lifetime (**Ra-lifetime**) field exists in each RA packet. This value indicates the amount of time that a host in the link where the interface is located can use the device as the default device. If this parameter is set to **0**, the device is no longer used as the default device. If this parameter is set to a non-zero value, this value must be greater than or equal to the interval for sending RA packets (**Ra-interval**).

## Examples

The following example sets the lifetime in RA packets to 2000 seconds on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd ra-lifetime 2000
```

## Notifications

N/A

## Common Errors

N/A

## Platform Description

N/A

## Related Commands

- [show ipv6 interface](#)

## 1.30 ipv6 nd ra-mtu

### Function

Run the **ipv6 nd ra-mtu** command to configure the MTU for RA packets to be sent on an interface.

Run the **no** form of this command to restore the default configuration.

The default MTU of RA packets is the IPv6 MTU value of a network interface.

### Syntax

```
ipv6 nd ra-mtu ra-mtu
```

```
no ipv6 nd ra-mtu
```

### Parameter Description

*ra-mtu*: Value of the MTU field in an RA packet, in bytes. The value range is from 0 to 1500.

### Command Modes

Interface configuration mode

### Default Level

14

## Usage Guidelines

If this parameter is set to **0**, an RA packet does not carry the MTU option.

## Examples

The following example sets the MTU of RA packets to be sent to 1400 bytes on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd ra-mtu 1400
```

## Notifications

N/A

## Common Errors

N/A

## Platform Description

N/A

## Related Commands

- [show ipv6 interface](#)

## 1.31 ipv6 nd ra-url

### Function

Run the **ipv6 nd ra-url** command to configure the Uniform Resource Locator (URL) for RA packets to be sent on an interface.

Run the **no** form of this command to restore the default configuration.

No URL is configured for RA packets by default.

### Syntax

```
ipv6 nd ra-url [ra-url]
```

```
no ipv6 nd ra-url
```

### Parameter Description

*ra-url*: URL of an RA packet. It is a string of 1 to 255 characters in a standard URL format.

### Command Modes

Interface configuration mode

### Default Level

14

### Usage Guidelines

N/A

## Examples

The following example sets the URL address of RA packets to be sent to `www.test.com` on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1) # ipv6 nd ra-url www.test.com
```

## Notifications

N/A

## Common Errors

N/A

## Platform Description

N/A

## Related Commands

- [show ipv6 interface](#)

## 1.32 ipv6 nd ra-url

### Function

Run the **ipv6 nd ra-url** command to configure the URL option type value for RA packets to be sent.

Run the **no** form of this command to restore the default configuration.

No URL option type value is configured for RA packets to be sent by default.

### Syntax

**ipv6 nd ra-url** *type*

**no ipv6 nd ra-url**

### Parameter Description

*type*: URL option type value of an RA packet. The value range is from 140 to 254, and should not be duplicate with a known type definition.

### Command Modes

Global configuration mode

### Default Level

14

### Usage Guidelines

N/A

## Examples

The following example sets the URL option type value of RA packets to be sent to 234.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd ra-url 234
```

## Notifications

N/A

## Common Errors

N/A

## Platform Description

N/A

## Related Commands

N/A

## 1.33 ipv6 nd reachable-time

### Function

Run the **ipv6 nd reachable-time** command to configure the duration in which the device considers a neighbor reachable.

Run the **no** form of this command to restore the default configuration.

The default duration in which the device considers a neighbor reachable is 30000 ms (30s).

### Syntax

**ipv6 nd reachable-time** *time*

**no ipv6 nd reachable-time**

### Parameter Description

*time*: Duration in which the device considers a neighbor reachable, in milliseconds. The value range is from 0 to 3600000.

### Command Modes

Interface configuration mode

### Default Level

14

### Usage Guidelines

A device detects unreachable neighbors based on the configuration. A shorter duration indicates that the device detects unreachable neighbors more quickly but more network bandwidth and device resources will be consumed. Therefore, you are not advised to set the duration to a very small value.

The configured value is advertised in an RA packet and is also used on the device. If the value is **0**, the duration is not specified on the device and the default value is used.

### Examples

The following example sets the duration in which a neighbor is considered reachable to 1000 seconds on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd reachable-time 1000000
```

### Notifications

N/A

### Common Errors

N/A

### Platform Description

N/A

### Related Commands

- [show ipv6 interface](#)

## 1.34 ipv6 nd resolve vlan

### Function

Run the **ipv6 nd resolve vlan** command to configure the device to actively send NS packets to a specific sub VLAN in a super VLAN.

Run the **no** form of this command to disable this feature.

Run **default** form of this command to restore the default configuration.

The device is not configured to actively send NS packets to a specific sub VLAN in a super VLAN by default.

### Syntax

```
ipv6 nd resolve vlan { vlan-list | none }
```

```
no ipv6 nd resolve vlan { vlan-list | none }
```

```
default ipv6 nd resolve vlan
```

### Parameter Description

*vlan-list*: Sub VLAN segment, to which the device actively sends NS packets in the Super VLAN. After this parameter is configured, NS requests are sent to these VLAN lists only. The start and end VLANs in a sub VLAN segment are connected by a hyphen (-), and multiple sub VLAN segments are separated by commas (,), for example, 1, 3-5.

**none**: Indicates that no NS packet will be sent to any sub VLAN in a super VLAN.



## Command Modes

Global configuration mode

## Default Level

2

## Usage Guidelines

If there are many sub VLANs in a super VLAN, when actively broadcasting and resolving ND requests, the device will send NS packets to the entire super VLAN by default, and the packets will be replicated in large quantities, which will affect the performance of the device.

Most terminals (such as PCs or servers) request the ND tables of the gateway before accessing the network. Therefore, there is no need to actively send NS packets to the sub VLANs where these terminals reside. For dumb terminals (that do not actively send NA packets), this command can be deployed in the VLAN segment specified in *vlan-list*, to enable the device to actively send NS packets to these VLANs in an effort to generate ND entries with reachable state.

---

### ⚠ Caution

If an authentication-exempt VLAN is configured and the authentication-exempt VLAN is not in the VLAN list configured by running the **ipv6 nd resolve vlan** command, NS packets will not be actively broadcast to the authentication-exempt VLAN.

---

## Examples

The following example configures the device to actively send NS packets to specific sub VLANs 10-20 and 25-30 in a super VLAN.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd resolve vlan 10-20, 25-30
```

The following example configures the device not to send NS packets to any sub VLAN in a super VLAN.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd resolve vlan none
```

## Notifications

N/A

## Common Errors

N/A

## Platform Description

N/A

## Related Commands

N/A

## 1.35 ipv6 nd stale-time

### Function

Run the **ipv6 nd stale-time** command to configure the duration in which a neighbor keeps in stale state.

Run the **no** form of this command to restore the default configuration.

The default duration in which a neighbor keeps in stale state is 3600s.

### Syntax

```
ipv6 nd stale-time time
```

```
no ipv6 nd stale-time
```

### Parameter Description

*time*: Duration in which a neighbor keeps in stale state, in seconds. The value range is from 0 to 86400.

### Command Modes

Global configuration mode

Interface configuration mode

### Default Level

14

### Usage Guidelines

This command can be used to modify the duration of the stale state. After the duration expires, neighbor unreachability detection (NUD) is performed. A shorter duration indicates that the device detects unreachable neighbors more quickly but more network bandwidth and device resources will be consumed. Therefore, you are not advised to set the duration to a very small value.

This command can be configured on an interface or in global configuration mode. The configuration configured on an interface takes priority over that configured in global configuration mode. That is, if the duration is configured on an interface, the duration configured on the interface applies. Otherwise, the global configuration will apply.

### Examples

The following example sets the duration in which a neighbor keeps in stale state to 600s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd stale-time 600
```

The following example sets the duration in which a neighbor keeps in stale state to 600s on SVI 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface VLAN 1
Hostname(config-if-VLAN 1)# ipv6 nd stale-time 600
```

### Notifications

N/A

**Common Errors**

N/A

**Platform Description**

N/A

**Related Commands**

N/A

## 1.36 ipv6 nd suppress-auth-vlan-ns

**Function**

Run the **ipv6 nd suppress-auth-vlan-ns** command to configure an interface not to send NS packets to an authenticated VLAN.

Run the **no** form of this command to remove this configuration.

Interfaces in an IPv6-enabled super VLAN will not send NS packets to an authenticated sub VLANs by default.

**Syntax**

```
ipv6 nd suppress-auth-vlan-ns  
no ipv6 nd suppress-auth-vlan-ns
```

**Parameter Description**

N/A

**Command Modes**

Interface configuration mode

**Default Level**

14

**Usage Guidelines**

The command is supported only on SVIs and takes effect in gateway authentication mode.

**Examples**

The following example configures SVI 2 to send NS packets to an authenticated VLAN.

```
Hostname> enable  
Hostname# configure terminal  
Hostname(config)# interface VLAN 2  
Hostname(config-if-VLAN 2)# no ipv6 nd suppress-auth-vlan-ns
```

**Notifications**

N/A

**Common Errors**

N/A

**Platform Description**

N/A

**Related Commands**

N/A

## 1.37 ipv6 nd suppress-ra

**Function**

Run the **ipv6 nd suppress-ra** command to configure an interface not to send RA packets.

Run the **no** form of this command to remove this configuration.

IPv6 interfaces do not send RA packets by default.

**Syntax**

```
ipv6 nd suppress-ra
```

```
no ipv6 nd suppress-ra
```

**Parameter Description**

N/A

**Command Modes**

Interface configuration mode

**Default Level**

14

**Usage Guidelines**

N/A

**Examples**

The following example configures port GigabitEthernet 0/1 not to send RA packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd suppress-ra
```

**Notifications**

N/A

**Common Errors**

N/A

**Platform Description**

N/A

**Related Commands**

- [show ipv6 interface](#)

## 1.38 ipv6 nd unresolved

**Function**

Run the **ipv6 nd unresolved** command to configure the maximum number of unresolved ND entries.

Run the **no** form of this command to restore the default configuration.

The maximum number of unresolved ND entries is 0 by default, indicating no restriction. That is, the number of unresolved ND entries is subject to the ND entry capacity supported by the device.

**Syntax**

**ipv6 nd unresolved** *number*

**no ipv6 nd unresolved**

**Parameter Description**

*number*: Maximum number of unresolved ND entries. The value range is from 1 to 8000.

**Command Modes**

Global configuration mode

**Default Level**

14

**Usage Guidelines**

To prevent malicious scanning attacks from causing the generation of a large number of unresolved ND entries and occupying entry resources, you can restrict the number of unresolved ND entries.

**Examples**

The following example sets the maximum number of unresolved ND entries to 200.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd unresolved 200
```

**Notifications**

N/A

**Common Errors**

N/A

**Platform Description**

N/A

**Related Commands**

N/A

## 1.39 ipv6 neighbor

### Function

Run the **ipv6 neighbor** command to configure a static neighbor entry.

Run the **no** form of this command to remove this configuration.

No static neighbor entry is configured by default.

### Syntax

**ipv6 neighbor** *ipv6-address interface-type interface-number mac-address*

**no ipv6 neighbor** *ipv6-address interface-type interface-number*

### Parameter Description

*ipv6-address*: IPv6 address of a neighbor, which must comply with the address representation format in RFC 4291.

*interface-type interface-number*: Type and number of the interface to which the neighbor resides.

*mac-address*: Link address of a neighbor, that is, 48-bit MAC address.

### Command Modes

Global configuration mode

### Default Level

14

### Usage Guidelines

This command is similar to the **arp** command. A static neighbor entry can be configured on IPv6-enabled interfaces only. If the neighbor entry to be configured has been learned through NDP and stored in the neighbor table, the dynamic neighbor entry will be automatically converted into a static one. An effective static neighbor entry will be always reachable.

An invalid static neighbor entry refers to a static neighbor entry with the configured IPv6 address not matching the address configured on the interface (not within any IPv6 network segment of this interface, or in conflict with the address of this interface). In this case, packets will not be forwarded through the MAC address specified in the static neighbor entry. An invalid static neighbor entry is inactive. You can run the **show ipv6 neighbor static** to display the validity status of this static neighbor entry.

### Examples

The following example configures a static neighbor entry on VLAN 1, with the IP address of 2001::1 and MAC address of 00d0.f811.1111.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 neighbor 2001::1 vlan 1 00d0.f811.1111
```

### Notifications

N/A

## Common Errors

N/A

## Platform Description

N/A

## Related Commands

- [clear ipv6 neighbors](#)
- [show ipv6 neighbors](#)

## 1.40 ipv6 ns-linklocal-src

### Function

Run the **ipv6 ns-linklocal-src** command to configure the link-local address as the source address for sending NS packets.

Run the **no** form of this command to remove this configuration.

The link-local address is always used as the source address for sending NS packets by default.

### Syntax

**ipv6 ns-linklocal-src**

**no ipv6 ns-linklocal-src**

### Parameter Description

N/A

### Command Modes

Global configuration mode

### Default Level

14

### Usage Guidelines

The **no ipv6 ns-linklocal-src** command is used to cancel configuring the link-local address as the source address for sending NS packets. Instead, a link-local address or global unicast address is used based on the destination IPv6 address according to RFC 3484.

### Examples

The following example configures not to use the link-local address as the source address for sending NS packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ipv6 ns-linklocal-src
```

### Notifications

N/A

**Common Errors**

N/A

**Platform Description**

N/A

**Related Commands**

N/A

- 

## 1.41 ipv6 redirects

**Function**

Run the **ipv6 redirects** command to enable the ICMPv6 redirection function.

Run the **no** form of this command to disable this feature.

The ICMPv6 redirection function is enabled by default.

**Syntax****ipv6 redirects****no ipv6 redirects****Parameter Description**

N/A

**Command Modes**

Interface configuration mode

**Default Level**

14

**Usage Guidelines**

N/A

**Examples**

The following example enables the ICMPv6 redirection function on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 redirects
```

**Notifications**

N/A

**Common Errors**

N/A



**Platform Description**

N/A

**Related Commands**

- [show ipv6 interface](#)

## 1.42 ipv6 source-route

**Function**

Run the **ipv6 source-route** command to configure the device to forward IPv6 packets carrying the routing header.

Run the **no** command to forbid the device from forwarding IPv6 packets carrying the routing header.

IPv6 packets carrying the routing header are not forwarded by default.

**Syntax****ipv6 source-route****no ipv6 source-route****Parameter Description**

N/A

**Command Modes**

Global configuration mode

**Default Level**

14

**Usage Guidelines**

Since the Type 0 routing header may cause the device vulnerable to DoS attacks, the device is forbidden from forwarding IPv6 packets carrying the routing header by default. However, the device still processes IPv6 packets that carry the Type 0 routing header and are finally destined for the device itself.

**Examples**

The following example configures the device to forward IPv6 packets carrying the routing header.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 source-route
```

**Notifications**

N/A

**Common Errors**

N/A

**Platform Description**

N/A

**Related Commands**

N/A

## 1.43 local-proxy-nd enable

**Function**

Run the **local-proxy-nd enable** command to enable the local ND proxy function on an interface.

Run the **no** form of this command to disable this feature

Local ND proxy is disabled on an interface by default.

**Syntax**

```
local-proxy-nd enable [ force ]
```

```
no local-proxy-nd enable
```

**Parameter Description**

**force**: Forcibly enables local ND proxy. That is, an interface always serves as a proxy to respond to NS packets regardless of whether the destination device exists.

**Command Modes**

Interface configuration mode

**Default Level**

14

**Usage Guidelines**

If L2 access isolation or inter-subnet isolation (such as sub VLANs) is configured, after local ND proxy is enabled on the gateway, the gateway serves as a proxy to process NS packets from downlink users and replies with NA packets containing the gateway's MAC address. Thus, the traffic of communication among these users is forwarded by the gateway at L3.

**Examples**

The following example enables local ND proxy on SVI 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface VLAN 1
Hostname(config-if-VLAN 1)# local-proxy-nd enable
```

The following example enables forcible local ND proxy on SVI 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface VLAN 1
Hostname(config-if-VLAN 1)# local-proxy-nd enable force
```

**Notifications**

N/A

**Common Errors**

N/A

**Platform Description**

N/A

**Related Commands**

N/A

## 1.44 show nd suppress table

**Function**

Run the **show nd suppress table** command to display the ND suppression table, which gives the details about the ND suppression entries.

**Syntax**

```
show nd suppress table [ ipv6 ipv6-address ]
```

**Parameter Description**

**ipv6 ipv6-address**: Specifies the IPv6 address in a suppression entry.

**Command Modes**

All modes except the user EXEC mode

**Default Level**

2

**Usage Guidelines**

N/A

**Examples**

The following example displays all ND suppression entries.

```
Hostname> enable
Hostname# show nd suppress table
ipv6 address      vrf    vni    vid    port    interface  hardware addr  host mac
location
30::2             1      30     30     0t6166  Or30       0001.0001.0001
0001.0002.0003   remote
30::3             1      30     30     ag1     Or30       0001.0001.0002
0001.0001.0002   local
```

The following example displays an individual ND suppression entry with the IPv6 address of 30::2.

```
Hostname> enable
```

```

Hostname# show nd suppress table ipv6 30::2
ipv6 address      vrf      vni      vid      port      interface  hardware addr  host mac
location
30::2             1        30       30       0t6166    Or30       0001.0001.0001
0001.0002.0003   remote

```

**Table 1-1** Output Fields of the show nd suppress table Command

Field	Description
ipv6 address	IPv6 address corresponding to an ND entry.
vrf	Index of a VRF instance to which an ND entry belongs.
vni	ID of a VXLAN where an ND entry resides.
vid	ID of a VLAN where an ND entry resides.
port	L2 outbound interface corresponding to an ND entry.
hardware addr	MAC address corresponding to an ARP entry.
host mac	Virtual MAC address of a remote host in a VXLAN network.
location	Location attribute of an ND entry. <b>Remote</b> indicates that the entry is synchronized by Ethernet virtual private network (EVPN) and <b>Local</b> indicates that the entry is locally learned.

**Notifications**

N/A

**Platform Description**

N/A

**Related Commands**

N/A

## 1.45 show ipv6 address

**Function**

Run the **show ipv6 address** command to display the information about an IPv6 address.

**Syntax**

```
show ipv6 address [ interface-type interface-number ]
```

**Parameter Description**

*interface-type interface-number*: Interface type and interface number. All IPv6 addresses are displayed by default.

## Command Modes

All modes except the user EXEC mode

## Default Level

14

## Usage Guidelines

N/A

## Examples

The following example displays all configured IPv6 addresses.

```

Hostname> enable
Hostname# show ipv6 addr
Global unicast address limit: 1024, Global unicast address count: 2
Tentative address count: 3,Duplicate address count: 0
Preferred address count: 0,Deprecated address count: 0
GigabitEthernet 0/5
  2003:1::23/64                               Tentative
  Preferred lifetime: INFINITE, Valid lifetime: INFINITE
  fe80::2d0:f8ff:fe8b:deb2/64                 Tentative
  Preferred lifetime: INFINITE, Valid lifetime: INFINITE
  2005:1::1111/64                             Tentative
  Preferred lifetime: INFINITE, Valid lifetime: INFINITE

```

The following example displays the IPv6 address configured on port GigabitEthernet 0/1.

```

Hostname> enable
Hostname# show ipv6 addr gi 0/1
Global unicast address count: 2
Tentative address count: 3,Duplicate address count: 0
Preferred address count: 0,Deprecated address count: 0
  2003:1::23/64                               Tentative
  Preferred lifetime: INFINITE, Valid lifetime: INFINITE
  fe80::2d0:f8ff:fe8b:deb2/64                 Tentative
  Preferred lifetime: INFINITE, Valid lifetime: INFINITE
  2005:1::1111/64                             Tentative
  Preferred lifetime: INFINITE, Valid lifetime: INFINITE

```

**Table 1-1** Output Fields of the show ipv6 address Command

Field	Description
Global unicast address count	Number of global unicast IPv6 address configured on this interface.
Tentative address count	Number of tentative addresses.
Duplicate address count	Number of duplicate addresses.
Preferred address count	Number of preferred addresses.

Deprecated address count	Number of expired addresses.
Preferred lifetime	Preferred lifetime.
Valid lifetime	Valid lifetime.

### Notifications

N/A

### Platform Description

N/A

### Related Commands

N/A

## 1.46 show ipv6 general-prefix

### Function

Run the **show ipv6 general-prefix** command to display the prefix information in a general prefix.

### Syntax

```
show ipv6 general-prefix
```

### Parameter Description

N/A

### Command Modes

All modes except the user EXEC mode

### Default Level

14

### Usage Guidelines

After this command is ran, general prefixes that are manually configured and learned by the DHCPV6 client are displayed.

### Examples

The following example displays the prefix information in a general prefix.

```
Hostname> enable
Hostname# show ipv6 general-prefix
There is 1 general prefix.
Ipv6 general prefix my-prefix, acquired via Manual configuration
    2001:1111:2222::/48
    2001:1111:3333::/48
```

**Table 1-1 Output Fields of the show ipv6 general-prefix Command**

Field	Description
There is	Number of current general prefixes.
IPv6 general prefix	Name of a general prefix.
acquired via	Prefix acquisition method.
Prefix/len	Prefix list.

**Notifications**

N/A

**Platform Description**

N/A

## 1.47 show ipv6 interface

**Function**

Run the **show ipv6 interface** command to display the information about an IPv6 interface.

**Syntax**

```
show ipv6 interface [ [ interface-type interface-number ] [ ra-info ] | brief [ interface-type interface-number ] ]
```

**Parameter Description**

*interface-type interface-number*: Interface type and interface number. If this parameter is not specified, the information about all IPv6 interfaces is displayed.

**ra-info**: Displays the parameter information of RA packets on this interface.

**brief**: Displays the brief information of an interface, including status and address information.

**Command Modes**

All modes except the user EXEC mode

**Default Level**

14

**Usage Guidelines**

This command can be used to display address configuration, ND configuration, and statistics of an IPv6 interface.

**Examples**

The following example displays the information about an IPv6 interface.

```
Hostname> enable
Hostname# show ipv6 interface vlan 1
```

```

Interface vlan 1 is Up, ifindex: 2001
address(es):
Mac Address: 00:00:00:00:00:01
INET6: fe80::200:ff:fe00:1 , subnet is fe80::/64
INET6: 2001::1 , subnet is 2001::/64 [TENTATIVE]
Joined group address(es):
ff01:1::1
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
MTU is 1500 bytes
ICMP error messages limited to one every 10 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds<240--160>
ND router advertisements live for 1800 seconds

```

The command output displays the following line: INET6: 2001::1, subnet is 2001::/64 [TENTATIVE]. The flag bits in [ ] after the IPv6 address are defined as follows.

**Table 1-1** Output Fields of the show ipv6 interface vlan 1 Command

Field	Description
ANYCAST	Anycast address.
TENTATIVE	DAD is being performed on the address. This address is tentative before the detection ends.
DUPLICATED	A duplicate address has been detected for this address.
DEPRECATED	This address reaches the preferred lifetime, and the address becomes deprecated.
NODAD	No DAD will be performed on this address.
AUTOIFID	The interface identifier for this address is automatically generated by the system, usually, an EUI-64 identifier.
PRE	Automatically configured stateless address.
GEN	Address generated by general prefix.

The following example displays the parameter information of RA packets on the IPv6 interface.

```

Hostname> enable
Hostname# show ipv6 interface vlan 1 ra-info

```



```

vlan 1: DOWN
RA timer is stopped
waits: 0, initcount: 3
statistics: RA(out/in/inconsistent): 4/0/0, RS(input): 0
Link-layer address: 00:00:00:00:00:01
Physical MTU: 1500
ND router advertisements live for 1800 seconds
ND router advertisements are sent every 200 seconds<240--160>
Flags: !M!O, Adv MTU: 1500
ND advertised reachable time is 0 milliseconds
ND advertised retransmit time is 0 milliseconds
ND advertised CurHopLimit is 64
Prefixes: (total: 1)
fec0:1:1:1::/64(Def,Auto,vltime:2592000,pltime:604800, flags: LA)

```

**Table 1-2**Output Fields of the show ipv6 interface vlan 1 ra-info Command

Field	Description
RA timer is stopped (on)	Whether the RA packet sending timer is started.
waits	Number of RS packets that have been received but not responded to.
initcount	Number of RA packets initially sent when the RA timer restarts.
RA (out/in/inconsistent)	RA packets. <ul style="list-style-type: none"> <li>● <b>Out</b>: Indicates the number of RA packets sent.</li> <li>● <b>In</b>: Indicates the number of RA packets received.</li> <li>● <b>Inconsistent</b>: Indicates the number of received RA packets with parameters inconsistent with those advertised by the router itself.</li> </ul>
RS (input)	Number of RS packets received.
Link-layer address	Link layer address of this interface.
Physical MTU	Link MTU of this interface.
!M   M	<ul style="list-style-type: none"> <li>● <b>!M</b> indicates that the <b>Managed-config-flag</b> option is not carried in an RA packet.</li> <li>● <b>M</b> indicates that the <b>Managed-config-flag</b> option is carried in an RA packet.</li> </ul>
!O   O	<ul style="list-style-type: none"> <li>● <b>!O</b> indicates that the <b>Other-config-flag</b> option is not carried in an RA packet.</li> <li>● <b>O</b> indicates that the <b>Other-config-flag</b> option is carried in an RA packet.</li> </ul>
total	Number of prefixes on this interface.
fec0:1:1:1::/64	Specific prefix.
Def	Default prefix configuration is used for this prefix.

Field	Description
Auto   CFG	<ul style="list-style-type: none"> <li>● <b>Auto</b> indicates that this prefix is automatically generated since the corresponding IPv6 address is configured on an interface.</li> <li>● <b>CFG</b> indicates that this prefix is manually configured.</li> </ul>
!Adv	This prefix will not be advertised.
vltime	Valid lifetime of this prefix, in seconds.
pltime	Preferred lifetime of this prefix, in seconds.
L   !L	<ul style="list-style-type: none"> <li>● <b>L</b> indicates that the prefix is On-link.</li> <li>● <b>!L</b> indicates that the prefix is Off-link.</li> </ul>
A   !A	<ul style="list-style-type: none"> <li>● <b>A</b> indicates that the prefix can be automatically configured.</li> <li>● <b>!A</b> indicates that the prefix cannot be automatically configured.</li> </ul>

The following example displays the brief information of an IPv6 interface.

```

Hostname> enable
Hostname# show ipv6 interface brief
GigabitEthernet 0/1          [down/down]
    2222::2
    FE80::1614:4BFF:FE5C:ED3A

```

**Table 1-3** Output Fields of the show ipv6 interface brief Command

Field	Description
GigabitEthernet 0/1	Interface name.
down/down	Link status or IPv6 protocol status of an interface.
2222::2	Primary IPv6 address of an interface.
FE80::1614:4BFF:FE5C:ED3A	Secondary IPv6 address of an interface.

#### Notifications

N/A

#### Platform Description

N/A

#### Related Commands

N/A

## 1.48 show ipv6 nd

#### Function

Run the **show ipv6 nd** command to display the statistics on IPv6 ND packets.

## Syntax

```
show ipv6 nd [ interface interface-type interface-number ] statistics
```

## Parameter Description

**interface** *interface-type interface-number*: Specifies the type and number of an IPv6 interface. After this parameter is configured, ND packet statistics of this interface will be displayed.

**statistics**: Displays the statistics on ND packets.

## Command Modes

All modes except the user EXEC mode

## Default Level

14

## Usage Guidelines

N/A

## Examples

The following example displays the statistics on IPv6 ND packets of SVI 1.

```

Hostname> enable
Hostname# show ipv6 nd interface vlan 1 statistics
interface VLAN 1 is Up, ifindex: 4097, vrf_id 0
  ipv6 interface packet statics:
  stat-type                Router Solicitations                Router advertisements
Neighbor solicitations    Neighbor advertisements
  Received                 0                                0
0
  Send                     0                                0
1
  Rate(receive, pps)      0                                0
0
  Rate(send, pps)         0                                0
0
  Interval time: 60s

```

**Table 1-1** Output Fields of the show ipv6 nd Command

Field	Description
stat-type	Statistics type: RS/RA/NS/NA packets.
Received	Statistics on received packets.
Send	Statistics on sent packets.
Rate	Packet transmission/receiving rate, in PPS.
Interval time	Sampling interval of ND packets.

**Notifications**

N/A

**Platform Description**

N/A

**Related Commands**

N/A

## 1.49 show ipv6 neighbors

**Function**

Run the **show ipv6 neighbors** command to display IPv6 neighbor tables.

**Syntax**

```
show ipv6 neighbors [ vrf vrf-name ] [ verbose ] [ interface-type interface-number ] [ ipv6-address ] [ static ] [ oob ]
```

**Parameter Description**

**vrf** *vrf-name*: Specifies a VRF instance.

**verbose**: Displays detailed neighbor information.

*interface-type interface-number*: Interface type and interface number. After this parameter is configured, the neighbor table of an interface will be displayed. The neighbor tables of all interfaces are displayed by default.

*ipv6-address*: IPv6 address. After this parameter is configured, information about a specified neighbor will be displayed.

**static**: Displays the status of a static neighbor entry.

**oob**: Displays the IPv6 neighbors of the management interface.

**Command Modes**

All modes except the user EXEC mode

**Default Level**

14

**Usage Guidelines**

N/A

**Examples**

The following example displays the neighbor table on SVI 1.

```
Hostname> enable
Hostname# show ipv6 neighbors vlan 1
Ipv6 Address Linklayer Addr  Interface
fa::1          00d0.0000.0002  vlan 1
```

```
fe80::200:ff:fe00:2 00d0.0000.0002 vlan 1
```

The following example displays details about a neighbor

```

Hostname> enable
Hostname# show ipv6 neighbors verbose
Ipv6 Address  Linklayer Addr Interface
2001::1       00d0.f800.0001 vlan 1
                State: Reach/H Age: - asked: 0
fe80::200:ff:fe00:1 00d0.f800.0001 vlan 1
                State: Reach/H Age: - asked: 0

```

**Table 1-1** Output Fields of the show ipv6 neighbors Command

Field	Description
IPv6 Address	IPv6 address of a neighbor.
Linklayer Addr	Link address, that is, MAC address. If this address is not obtained, "incomplete" is displayed.
Interface	Interface where the neighbor resides.
State	<p>Status of the neighbor.</p> <ul style="list-style-type: none"> <li>● <b>INCOMP</b> (Incomplete) indicates that the address resolution of the neighbor is underway, the NS packet has been sent, but no reply packet is received from the neighbor.</li> <li>● <b>REACH</b> (Reachable) indicates that the device is reachable to the neighbor and no additional action is required to send packets to the neighbor.</li> <li>● <b>STALE</b> indicates that the time that the neighbor considered reachable has elapsed. In this state, no additional action is required on the device until a packet is sent to the neighbor. Then, the device performs NUD.</li> <li>● <b>DELAY</b> indicates that a packet is sent to the neighbor in stale state. The neighbor changes from STALE state to DELAY state. If no notification indicating that the neighbor is reachable is received within DELAY_FIRST_PROBE_TIME seconds (5 seconds), then the neighbor will change from DELAY state to PROBE state, and an NS packet will be sent to the neighbor to officially start NUD.</li> <li>● <b>PROBE</b> indicates that NUD has been started to detect the neighbor reachability. NS packets are sent to the neighbor every RetransTimer milliseconds until reply packets are received or the number of NS packets sent reaches the limit MAX_UNICAST_SOLICIT (three NS packets).</li> <li>● <b>?</b> indicates unknown state.</li> <li>● <b>/R</b> indicates that the neighbor is deemed as a device.</li> <li>● <b>/H</b> indicates that the neighbor is deemed as a host.</li> </ul>
Age	<p>Amount of time that a neighbor is considered reachable.</p> <ul style="list-style-type: none"> <li>● <b>-</b> indicates that a neighbor is always reachable. Static neighbor entries will rely on whether they are actually reachable.</li> <li>● <b>expired</b> indicates the amount of time that a neighbor is considered reachable has elapsed and NUD is to be triggered.</li> </ul>
Asked	Number of NS packets sent to a neighbor during the resolution of the neighbor's link address.

The following example displays the status of static neighbor entries.

```

Hostname> enable
Hostname# show ipv6 neighbors static
IPv6 Address      Linklayer Addr  Interface                State
2001:1::1         00d0.f822.33ab  GigabitEthernet 0/14    ACTIVE
2001:2::2         00d0.f822.33ac  VLAN 1                    INACTIVE

```

**Table 1-2**Output Fields of the show ipv6 neighbors static Command

Field	Description
IPv6 Address	IPv6 address of a static neighbor entry.
Linklayer Addr	Link address, that is, MAC address.
Interface	Interface where the neighbor resides.
State	Status of a static neighbor entry. The value of <b>State</b> includes: <ul style="list-style-type: none"> <li>● <b>ACTIVE</b>, indicating that a static neighbor entry is active.</li> <li>● <b>INACTIVE</b>, indicating that a static neighbor entry is inactive. When the IPv6 address configured for a static neighbor entry does not match that on the interface (not within any address segment of this interface, or in conflict with the address of this interface), the static neighbor entry is inactive, that is, packets will not be forwarded through the MAC address specified in the static neighbor entry.</li> </ul>

### Notifications

N/A

### Platform Description

N/A

### Related Commands

N/A

## 1.50 show ipv6 neighbors statistics

### Function

Run the **show ipv6 neighbors statistics** command to display the statistics on IPv6 neighbor tables.

### Syntax

```
show ipv6 neighbors [ vrf vrf-name ] statistics [ all ]
```

### Parameter Description

**vrf** *vrf-name*: Specifies the name of a VRF instance.

**all**: Displays the statistics on all IPv6 neighbor tables.

## Command Modes

All modes except the user EXEC mode

## Default Level

14

## Usage Guidelines

N/A

## Examples

The following example displays the statistics on global IPv6 neighbor tables.

```

Hostname> enable
Hostname# show ipv6 neighbor statistics
Memory: 0 bytes
Entries: 0
  Static: 0,Dynamic: 0,Local: 0
  Incomplete:0, Reachable:0, Stale:0, Delay:0, Probe:0

```

The following example displays the statistics on all IPv6 neighbor tables.

```

Hostname> enable
Hostname# show ipv6 neighbor statistics all
Ipv6 neighbor table count: 1
Static neighbor count: 0(0 active, 0 inactive)
Total
Memory: 0 bytes
Entries: 0
  Static: 0,Dynamic: 0,Local: 0
  Incomplete:0, Reachable:0, Stale:0, Delay:0, Probe:0;
Global
Memory: 0 bytes
Entries: 0
  Static: 0,Dynamic: 0,Local: 0
  Incomplete:0, Reachable:0, Stale:0, Delay:0, Probe:0;

```

**Table 1-1**Output Fields of the show ipv6 neighbors statistics Command

Field	Description
IPv6 neighbor table count	Number of neighbor tables
Static neighbor count	Number of static neighbor entries.
active	Number of active neighbor entries.
inactive	Number of inactive neighbor entries.
Memory	Memory usage.
Entries	Number of neighbor entries.

Field	Description
Static	Number of static entries.
Dynamic	Number of dynamic entries.
Local	Number of entries corresponding to the local IPv6 address.
Incomplete	Number of unresolved entries.
Reachable	Number of reachable neighbor entries.
Stale	Number of entries in stale state.
Delay	Number of entries in the delay state.
Probe	Number of entries in the probe state.

**Notifications**

N/A

**Platform Description**

N/A

**Related Commands**

N/A

## 1.51 show ipv6 packet statistics

**Function**

Run the **show ipv6 packet statistics** command to display the statistics on IPv6 packets.

**Syntax**

```
show ipv6 packet statistics [ total | interface-type interface-number ]
```

**Parameter Description**

**total**: Specifies the sum of the statistics on all interfaces. If this parameter is not specified, the sum of the statistics of all interfaces as well as the statistics of each interface are displayed.

*interface-type interface-number*: Interface type and interface number.

**Command Modes**

All modes except the user EXEC mode

**Default Level**

14

**Usage Guidelines**

N/A



## Examples

The following example displays the sum of the statistics on IPv6 packets and the statistics of each interface.

```

Hostname> enable
Hostname# show ipv6 pack statistics
Total
  Received 0 packets, 0 bytes
    Unicast:0,Multicast:0
  Discards:0
    HdrErrors:0 (HoplimitExceeded:0,Others:0)
    NoRoutes:0
    Others:0
  Sent 0 packets, 0 bytes
    Unicast:0,Multicast:0
GigabitEthernet 0/5
  Received 0 packets, 0 bytes
    Unicast:0,Multicast:0
  Discards:0
    HdrErrors:0 (HoplimitExceeded:0,Others:0)
    NoRoutes:0
    Others:0
  Sent 0 packets, 0 bytes
    Unicast:0,Multicast:0

```

The following example displays the sum of the statistics on IPv6 packets.

```

Hostname> enable
Hostname# show ipv6 pack statistics total
Total
  Received 0 packets, 0 bytes
    Unicast:0,Multicast:0
  Discards:0
    HdrErrors:0 (HoplimitExceeded:0,Others:0)
    NoRoutes:0
    Others:0
  Sent 0 packets, 0 bytes
    Unicast:0,Multicast:0

```

**Table 1-1** Output Fields of the show ipv6 pack statistics Command

Field	Description
Total	Sum of the statistics on IPv6 packets of all interfaces.
Received	Number of received IPv6 packets, in bytes.
Unicast	Number of IPv6 unicast packets.
Multicast	Number of IPv6 multicast packets.
Discards	Number of discarded IPv6 packets.

Field	Description
HdrErrors	Number of IPv6 packets discarded due to header error.
HoplimitExceeded	Number of packets discarded due to hop limit overrange during forwarding.
Others	Number of other IPv6 packets discarded due to header error.
NoRoutes	Number of IPv6 packets discarded due to no routing.
Others	Number of IPv6 packets discarded due to other reasons.
Sent	Number of sent IPv6 packets, in bytes.
Unicast	Number of unicast packets.
Multicast	Number of multicast packets.

**Notifications**

N/A

**Platform Description**

N/A

**Related Commands**

N/A

## 1.52 show ipv6 raw-socket

**Function**

Run the **show ipv6 raw-socket** command to displays all IPv6 raw sockets.

**Syntax**

```
show ipv6 raw-socket [ protocol ]
```

**Parameter Description**

*protocol*: Protocol number. The value range is from 1 to 255.

**Command Modes**

All modes except the user EXEC mode

**Default Level**

14

**Usage Guidelines**

N/A

**Examples**

The following example displays all IPv6 raw sockets.

```

Hostname> enable
Hostname# show ipv6 raw-socket
Number Protocol Process name
1      ICMPv6   vrrp.elf
2      ICMPv6   tcpip.elf
3      VRRP     vrrp.elf
Total: 3

```

**Table 1-1** Output Fields of the show ipv6 raw-socket Command

Field	Description
Number	Serial number.
Protocol	Protocol number.
Process name	Process name.
Total	Total number of IPv6 raw sockets.

**Notifications**

N/A

**Platform Description**

N/A

**Related Commands**

N/A

## 1.53 show ipv6 routers

**Function**

Run the **show ipv6 routers** command to display neighbor router information and RA packets.

**Syntax**

```
show ipv6 routers [ interface-type interface-number ]
```

**Parameter Description**

*interface-type interface-number*: Interface type and interface number. After this parameter is specified, RA packets received by a specified interface will be displayed.

**Command Modes**

All modes except the user EXEC mode

**Default Level**

14

## Usage Guidelines

If no interface is specified, then the information about RA packets received by this device is displayed.

## Examples

The following example displays neighbor router information and RA packets.

```

Hostname> enable
Hostname# show ipv6 routers
Router FE80::2D0:F8FF:FEC1:C6E1 on VLAN 2, last update 62 sec
  Hops 64, Lifetime 1800 sec, ManagedFlag=0, OtherFlag=0, MTU=1500
  Preference=MEDIUM
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 6001:3::/64 onlink autoconfig
    Valid lifetime 2592000 sec, preferred lifetime 604800 sec
  Prefix 6001:2::/64 onlink autoconfig
    Valid lifetime 2592000 sec, preferred lifetime 604800 sec

```

**Table 1-1** Output Fields of the show ipv6 routers Command

Field	Description
Router	Neighbor router, which is described using the IPv6 address and the network interface receiving RA packets.
last update	Time that has elapsed since the last RA packet is received.
Hops	Hop count of RA packets.
Lifetime	Lifetime of the router.
ManagedFlag	Managed flag of the router.
OtherFlag	Other flag of the router.
MTU	MTU of the interface sending RA packets on the router.
Reachable time	Amount of time that the router is considered reachable.
Retransmit time	RA packet retransmission time of the router.
Prefix	Prefix of RA packets.
Valid lifetime	Lifetime of a prefix.
preferred lifetime	Preferred lifetime of a prefix.

## Notifications

N/A

## Platform Description

N/A

**Related Commands**

N/A

**1.54 show ipv6 sockets****Function**

Run the **show ipv6 sockets** command to display all IPv6 raw sockets.

**Syntax**

```
show ipv6 sockets
```

**Parameter Description**

N/A

**Command Modes**

All modes except the user EXEC mode

**Default Level**

14

**Usage Guidelines**

This command is used to display all IPv6 sockets and thus obtain the UDP port and TCP port that provide services for external devices.

**Examples**

The following example displays all IPv6 sockets.

```

Hostname> enable
Hostname# show ipv6 sockets
Number Process name      Type   Protocol  LocalIP:Port  ForeignIP:Port  State
1      vrrp.elf              RAW    ICMPv6    :::58         :::0            *
2      tcpip.elf             RAW    ICMPv6    :::58         :::0            *
3      vrrp.elf              RAW    VRRP      :::112        :::0            *
4      orion-snmpd           DGRAM  UDP       :::161        :::0            *
5      orion-snmpd           DGRAM  UDP       :::162        :::0            *
6      dhcp6.elf             DGRAM  UDP       :::547        :::0            *
7      orion-sshd            STREAM TCP     :::22         :::0            LISTEN
8      orion-telnetd         STREAM TCP     :::23         :::0            LISTEN
Total: 8

```

**Table 1-1 Output Fields of the show ipv6 sockets Command**

Field	Description
Number	Serial number.
Process name	Process name.

Field	Description
Type	Socket type. <ul style="list-style-type: none"> <li>● <b>RAW</b> indicates a raw socket.</li> <li>● <b>DGRAM</b> indicates the packet type.</li> <li>● <b>STREAM</b> indicates the stream type.</li> </ul>
Protocol	Protocol number.
LocalIP:Port	Local IPv6 address and port.
ForeignIP:Port	Peer IPv6 address and port.
State	Status (only for IPv6 TCP sockets).
Total	Total number of sockets.

**Notifications**

N/A

**Platform Description**

N/A

**Related Commands**

N/A

## 1.55 show ipv6 udp

**Function**

Run the **show ipv6 udp** command to display all IPv6 UDP sockets.

**Syntax**

```
show ipv6 udp [ local-port port-number ] [ peer-port port-number ]
```

**Parameter Description**

**local-port** *port-number*: Specifies a local port number.

**peer-port** *port-number*: Specifies a peer port number.

**Command Modes**

All modes except the user EXEC mode

**Default Level**

14

**Usage Guidelines**

This command is used to display all IPv6 UDP sockets and thus learn the UDP port that provides services for external devices.

## Examples

The following example displays all IPv6 UDP sockets.

```

Hostname> enable
Hostname# show ipv6 udp
Number Local Address    Peer Address    Process name
1      :::161                :::0            orion-snmpd
2      :::162                :::0            orion-snmpd
3      :::547                :::0            dhcp6.elf

```

**Table 1-1** Output Fields of the show ipv6 udp Command

Field	Description
Number	Serial number.
Local Address	Local IPv6 address and port.
Peer Address	Peer IPv6 address and port.
Process name	Process name.

## Notifications

N/A

## Platform Description

N/A

## Related Commands

N/A

## 1.56 show ipv6 udp statistics

### Function

Run the **show ipv6 udp statistics** command to display the statistics on IPv6 UDP sockets.

### Syntax

```
show ipv6 udp statistics
```

### Parameter Description

N/A

### Command Modes

All modes except the user EXEC mode

### Default Level

14

**Usage Guidelines**

N/A

**Examples**

The following example displays the statistics on all IPv6 UDP sockets.

```
Hostname> enable
Hostname# show ipv6 udp statistics
Number of Ipv6 UDP sockets is 3.
```

**Figure 1-1**Output Fields of the show ipv6 udp Command

Field	Description
Number of Ipv6 UDP sockets is x	The total number of IPv6 UDP sockets is x.

**Notifications**

N/A

**Platform Description**

N/A

**Related Commands**

N/A