

Contents

IPv6 basics commands	1
display ipv6 fib	1
display ipv6 icmp statistics	2
display ipv6 interface	3
display ipv6 interface prefix	7
display ipv6 neighbors	8
display ipv6 neighbors count	10
display ipv6 pathmtu	10
display ipv6 prefix	11
display ipv6 rawip	13
display ipv6 rawip verbose	13
display ipv6 statistics	17
display ipv6 tcp	18
display ipv6 tcp-proxy	19
display ipv6 tcp-proxy port-info	21
display ipv6 tcp verbose	23
display ipv6 udp	26
display ipv6 udp verbose	27
ipv6 address	30
ipv6 address anycast	31
ipv6 address auto	31
ipv6 address auto link-local	32
ipv6 address eui-64	33
ipv6 address <i>prefix-number</i>	34
ipv6 address link-local	35
ipv6 option drop enable	36
ipv6 hop-limit	36
ipv6 hoplimit-expires enable	37
ipv6 icmpv6 error-interval	37
ipv6 icmpv6 multicast-echo-reply enable	38
ipv6 icmpv6 source	39
ipv6 mtu	39
ipv6 nd autoconfig managed-address-flag	40
ipv6 nd autoconfig other-flag	41
ipv6 nd dad attempts	41
ipv6 nd mode uni	42
ipv6 nd ns retrans-timer	43
ipv6 nd nud reachable-time	44
ipv6 nd ra halt	45
ipv6 nd ra hop-limit unspecified	45
ipv6 nd ra interval	46
ipv6 nd ra no-advlinkmtu	47
ipv6 nd ra prefix	47
ipv6 nd ra router-lifetime	48
ipv6 nd router-preference	49
ipv6 neighbor	50
ipv6 neighbor link-local minimize	51
ipv6 neighbor stale-aging	51
ipv6 neighbors max-learning-num	52
ipv6 pathmtu	54
ipv6 pathmtu age	55
ipv6 prefer temporary-address	56
ipv6 prefix	56
ipv6 reassemble local enable	57
ipv6 redirects enable	57
ipv6 temporary-address	58
ipv6 unreachable enable	59

local-proxy-nd enable	60
proxy-nd enable	60
reset ipv6 neighbors	61
reset ipv6 pathmtu	62
reset ipv6 statistics	62

IPv6 basics commands

The WX1800H series, WX2500H series, and WX3000H series access controllers do not support the **slot** keyword or the *slot-number* argument.

display ipv6 fib

Use **display ipv6 fib** to display IPv6 FIB entries.

Syntax

```
display ipv6 fib [ ipv6-address [ prefix-length ] ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-address: Specifies an IPv6 address.

prefix-length: Specifies a prefix length for the IPv6 address, in the range of 0 to 128.

Usage guidelines

If you do not specify the prefix length, this command displays the IPv6 FIB entry longest matching the IPv6 address. If you specify a prefix, this command displays the IPv6 FIB entry that exactly matches the IPv6 address and prefix length.

If you do not specify any parameters, this command displays all IPv6 FIB entries for the public network.

Examples

```
# Display all IPv6 FIB entries for the public network.
```

```
<Sysname> display ipv6 fib
```

```
Destination count: 1 FIB entry count: 1
```

```
Flag:
```

```
U:Useable G:Gateway H:Host B:Blackhole D:Dynamic S:Static
```

```
R:Relay F:FRR
```

```
Destination: ::1
```

```
Prefix length: 128
```

```
Nexthop : ::1
```

```
Flags: UH
```

```
Time stamp : 0x1
```

```
Label: Null
```

```
Interface : InLoop0
```

```
Token: Invalid
```

Table 1 Command output

Field	Description
Destination count	Total number of destination addresses.
FIB entry count	Total number of IPv6 FIB entries.

Field	Description
Destination	Destination address.
Prefix length	Prefix length of the destination address.
Nexthop	Next hop.
Flags	Route flag: <ul style="list-style-type: none"> • U—Usable route. • G—Gateway route. • H—Host route. • B—Black hole route. • D—Dynamic route. • S—Static route. • R—Recursive route. • F—Fast re-route.
Time stamp	Time when the IPv6 FIB entry was generated.
Label	Inner MPLS label. This field is not supported in the current software version.
Interface	Outgoing interface.
Token	Label switched path index number.

display ipv6 icmp statistics

Use **display ipv6 icmp statistics** to display ICMPv6 packet statistics.

Syntax

```
display ipv6 icmp statistics [ slot slot-number ]
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

slot slot-number. Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays ICMPv6 packet statistics for all member devices.

Usage guidelines

This command displays statistics about received and sent ICMPv6 packets.

Examples

```
# Display ICMPv6 packet statistics.
```

```
<Sysname> display ipv6 icmp statistics
  Input: bad code          0          too short          0
         checksum error    0          bad length         0
         path MTU changed  0          destination unreachable 0
         too big           0          parameter problem  0
         echo request      0          echo reply         0
         neighbor solicit  0          neighbor advertisement 0
```

router solicit	0	router advertisement	0
redirect	0	router renumbering	0
output: parameter problem	0	echo request	0
echo reply	0	unreachable no route	0
unreachable admin	0	unreachable beyond scope	0
unreachable address	0	unreachable no port	0
too big	0	time exceed transit	0
time exceed reassembly	0	redirect	0
ratelimited	0	other errors	0

display ipv6 interface

Use **display ipv6 interface** to display IPv6 interface information.

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type: Specifies an interface by its type.

interface-number: Specifies an interface by its number.

brief: Displays brief information.

Usage guidelines

If you specify the **brief** keyword, this command displays brief IPv6 interface information, including physical status, link-layer protocols, and IPv6 address.

If you do not specify the **brief** keyword, this command displays detailed IPv6 interface information, including IPv6 configuration and operating information, and IPv6 packet statistics.

If you do not specify an interface, this command displays IPv6 information about all interfaces.

If you specify only the *interface-type* argument, this command displays IPv6 information about the interfaces of the specified type.

If you specify both the *interface-type* and the *interface-number* arguments, this command displays IPv6 information about the specified interface.

Examples

Display IPv6 information about VLAN-interface 2.

```
<Sysname> display ipv6 interface vlan-interface 2
Vlan-interface2 current state: UP
Line protocol current state: UP
IPv6 is enabled, link-local address is FE80::1234:56FF:FE65:4322 [TENTATIVE]
Global unicast address(es):
  10::1234:56FF:FE65:4322, subnet is 10::/64 [TENTATIVE] [AUTOCFG]
  [valid lifetime 4641s/preferred lifetime 4637s]
  20::1234:56ff:fe65:4322, subnet is 20::/64 [TENTATIVE] [EUI-64]
```

```

30::1, subnet is 30::/64 [TENTATIVE] [ANYCAST]
40::2, subnet is 40::/64 [TENTATIVE] [DHCP]
50::3, subnet is 50::/64 [TENTATIVE]
Joined group address(es):
FF02::1
FF02::2
FF02::1:FF00:1
FF02::1:FF65:4322
MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND retransmit interval is 1000 milliseconds
Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
InReceives:                0
InTooShorts:               0
InTruncatedPkts:          0
InHopLimitExceeds:        0
InBadHeaders:              0
InBadOptions:              0
ReasmReqds:                0
ReasmOKs:                  0
InFragDrops:               0
InFragTimeouts:           0
OutFragFails:              0
InUnknownProtos:          0
InDelivers:                 0
OutRequests:               0
OutForwDatagrams:         0
InNoRoutes:                0
InTooBigErrors:            0
OutFragOKs:                0
OutFragCreates:           0
InMcastPkts:               0
InMcastNotMembers:        0
OutMcastPkts:              0
InAddrErrors:              0
InDiscards:                0
OutDiscards:               0

```

Table 2 Command output

Field	Description
Vlan-interface2 current state	Physical state of the interface: <ul style="list-style-type: none"> • Administratively DOWN—The VLAN interface has been administratively shut down by using the shutdown command. • DOWN—The VLAN interface is administratively up but its physical state is down because all ports in the VLAN are down. • UP—The administrative and physical states of the VLAN interface are both up.

Field	Description
Line protocol current state	Link layer protocol state of the interface: <ul style="list-style-type: none"> • DOWN—The link layer protocol state of the VLAN interface is down. • UP—The link layer protocol state of the VLAN interface is up.
IPv6 is enabled	IPv6 is enabled on the interface. This feature is automatically enabled after an IPv6 address is configured for an interface.
link-local address	Link-local address of the interface.
Global unicast address(es)	Global unicast addresses of the interface. IPv6 address states: <ul style="list-style-type: none"> • TENTATIVE—Initial state. DAD is being performed or is to be performed on the address. • DUPLICATE—The address is not unique on the link. • PREFERRED—The address is preferred and can be used as the source or destination address of a packet. If an address is in this state, the command does not display the address state. • DEPRECATED—The address is beyond the preferred lifetime but in the valid lifetime. It is valid, but it cannot be used as the source address for a new connection. Packets destined to the address are processed correctly. <p>If a global unicast address is not manually configured, the following indicates how the address is obtained:</p> <ul style="list-style-type: none"> • AUTOCFG—Stateless autoconfigured. • DHCP—Assigned by a DHCPv6 server. • EUI-64—Manually configured EUI-64 IPv6 address. • RANDOM—Random address automatically generated. <p>If the address is a manually configured anycast address, ANYCAST is marked.</p>
valid lifetime	Specifies how long autoconfigured global unicast addresses using a prefix are valid.
preferred lifetime	Specifies how long autoconfigured global unicast addresses using a prefix are preferred.
Joined group address(es)	Addresses of multicast groups that the interface has joined.
MTU	Maximum transmission unit (MTU) of the interface.
ND DAD is enabled, number of DAD attempts	DAD is enabled. <ul style="list-style-type: none"> • If DAD is enabled, this field displays the number of attempts to send an NS message for DAD (set by using the ipv6 nd dad attempts command). • If DAD is disabled, this field displays ND DAD is disabled. To disable DAD, set the number of attempts to 0.
ND reachable time	Time during which a neighboring device is reachable.
ND retransmit interval	Interval for retransmitting an NS message.
Hosts use stateless autoconfig for addresses	Hosts obtained IPv6 addresses through stateless autoconfiguration.
InReceives	Received IPv6 packets, including error messages.
InTooShorts	Received IPv6 packets that are too short. For example, the received IPv6 packet is less than 40 bytes.
InTruncatedPkts	Received IPv6 packets with a length less than the payload length field specified in the packet header.

Field	Description
InHopLimitExceeds	Received IPv6 packets with a hop count exceeding the hop limit field specified in the packet header.
InBadHeaders	Received IPv6 packets with incorrect basic headers.
InBadOptions	Received IPv6 packets with incorrect extension headers.
ReasmReqds	Received IPv6 fragments.
ReasmOKs	Number of reassembled IPv6 packets.
InFragDrops	Received IPv6 fragments that are discarded because of certain errors.
InFragTimeouts	Received IPv6 fragments that are discarded because the amount of time they stay in the system buffer exceeds the specified interval.
OutFragFails	IPv6 packets that fail to be fragmented on the output interface.
InUnknownProtos	Received IPv6 packets with unknown or unsupported protocol type.
InDelivers	Received IPv6 packets that are delivered to user protocols (such as ICMPv6, TCP, and UDP).
OutRequests	Local IPv6 packets sent by IPv6 user protocols.
OutForwDatagrams	IPv6 packets forwarded by the output interface.
InNoRoutes	Received IPv6 packets that are discarded because no matching route can be found.
InTooBigErrors	Received IPv6 packets that fail to be forwarded because they exceeded the Path MTU.
OutFragOKs	Fragmented IPv6 packets on the output interface.
OutFragCreates	Number of IPv6 fragments on the output interface.
InMcastPkts	Received IPv6 multicast packets.
InMcastNotMembers	Received IPv6 multicast packets that are discarded because the interface is not in the multicast group.
OutMcastPkts	IPv6 multicast packets sent by the interface.
InAddrErrors	Received IPv6 packets that are discarded due to invalid destination addresses.
InDiscards	Received IPv6 packets that are discarded due to resource problems rather than packet errors.
OutDiscards	IPv6 packets that fail to be sent due to resource problems rather than packet errors.

Display brief IPv6 information about all interfaces.

```
<Sysname> display ipv6 interface brief
*down: administratively down
(s): spoofing
Interface                Physical Protocol IPv6 Address
Vlan-interface1          down    down    Unassigned
Vlan-interface2          up      up      2001::1
Vlan-interface100        up      up      Unassigned
```


Table 3 Command output

Field	Description
*down: administratively down	The interface has been administratively shut down by using the shutdown command.
(s): spoofing	Spoofing attribute of the interface. The link protocol state of the interface is up, but the link is temporarily established on demand or does not exist.
Interface	Name of the interface.
Physical	Physical state of the interface: <ul style="list-style-type: none"> • *down—The interface has been shut down by using the shutdown command. • down—The interface is up but its physical state is down because all ports in the VLAN are down. • up—The administrative and physical states of the interface are both up.
Protocol	Link layer protocol state of the interface: <ul style="list-style-type: none"> • down—The network layer protocol state of the interface is down. • up—The network layer protocol state of the interface is up.
IPv6 Address	IPv6 address of the interface. <ul style="list-style-type: none"> • If multiple global unicast addresses are configured, this field displays the lowest address. • If no global unicast address is configured, this field displays the link-local address. • If no address is configured, this field displays Unassigned.

display ipv6 interface prefix

Use **display ipv6 interface prefix** to display IPv6 prefix information for an interface.

Syntax

display ipv6 interface *interface-type interface-number* **prefix**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number. Specifies an interface by its type and number.

Examples

Display IPv6 prefix information for VLAN-interface 10.

```
<Sysname> display ipv6 interface vlan-interface10 prefix
Prefix: 1001::/65                               Origin: ADDRESS
Age: -                                           Flag: AL
Lifetime(Valid/Preferred): 2592000/604800

Prefix: 2001::/64                               Origin: STATIC
Age: -                                           Flag: L
```

Lifetime(Valid/Preferred): 3000/2000

Prefix: 3001::/64

Origin: RA

Age: 600

Flag: A

Lifetime(Valid/Preferred): -

Table 4 Command output

Filed	Description
Prefix	IPv6 address prefix.
Origin	How the prefix is generated: <ul style="list-style-type: none">• STATIC—Manually configured by using the ipv6 nd ra prefix command.• RA—Advertised in RA messages after stateless autoconfiguration is enabled.• ADDRESS—Generated by a manually configured address.
Age	Aging time in seconds. If the prefix does not age out, this field displays a hyphen (-).
Flag	Flags advertised in RA messages. If no flags are available, this field displays a hyphen (-). <ul style="list-style-type: none">• L—The address with the prefix is directly reachable on the link.• A—The prefix is used for stateless autoconfiguration.
Lifetime	Lifetime in seconds advertised in RA messages. If the prefix does not need to be advertised, this field displays a hyphen (-). <ul style="list-style-type: none">• Valid—Valid lifetime of the prefix.• Preferred—Preferred lifetime of the prefix.

Related commands

ipv6 nd ra prefix

display ipv6 neighbors

Use **display ipv6 neighbors** to display IPv6 neighbor information.

Syntax

```
display ipv6 neighbors { { ipv6-address | all | dynamic | static } [ slot slot-number ] | interface interface-type interface-number | vlan vlan-id } [ verbose ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-address: Specifies the IPv6 address of a neighbor whose information is displayed.

all: Displays information about all neighbors, including neighbors acquired dynamically and configured statically on the public network and all private networks.

dynamic: Displays information about all neighbors acquired dynamically.

static: Displays information about all neighbors configured statically.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 neighbor information for all member devices.

interface *interface-type interface-number*: Specifies an interface by its type and number.

vlan *vlan-id*: Displays information about neighbors in the specified VLAN. The value range for VLAN ID is 1 to 4094.

verbose: Displays detailed neighbor information.

Usage guidelines

You can use the **reset ipv6 neighbors** command to clear IPv6 neighbor information.

Examples

Display all neighbor information.

```
<Sysname> display ipv6 neighbors all
Type: S-Static   D-Dynamic   O-Openflow   R-Rule   I-Invalid
IPv6 Address           Link Layer           VID   Interface           State T   Age
FE80::200:5EFF:FE32:B800  0000-5e32-b800   1     WLAN-BSS1/0/1     REACH D   10
```

Display detailed information about all neighbors.

```
<Sysname> display ipv6 neighbors all verbose
Type: S-Static   D-Dynamic   O-Openflow   R-Rule   I-Invalid
IPv6 Address : 1::30
Link Layer   : 70f9-6d81-1327   VID : 1   Interface: GE1/0/2
State       : STALE           Type: D   Age      : 2508
Vpn-instance: [No Vrf]
NickName    : 0x0
```

Table 5 Command output

Field	Description
IPv6 Address	IPv6 address of a neighbor.
Link Layer	Link layer address (MAC address) of a neighbor.
VID	VLAN to which the interface connected to a neighbor belongs.
Interface	Interface connected to a neighbor.
State	State of a neighbor: <ul style="list-style-type: none"> • INCMP—The address is being resolved. The link layer address of the neighbor is unknown. • REACH—The neighbor is reachable. • STALE—Whether the neighbor is reachable is unknown. The device does not verify the reachability any longer unless data is sent to the neighbor. • DELAY—Whether the neighbor is reachable is unknown. The device sends an NS message after a delay. • PROBE—Whether the neighbor is reachable is unknown. The device sends an NS message to verify the reachability of the neighbor.
Type	Neighbor information type: <ul style="list-style-type: none"> • S—Statically configured. • D—Dynamically obtained. • O—Learned from the OpenFlow module. This field is not supported in the current software version. • R—Learned from the IPoE or Portal module. This field is not supported in the current software version. • I—Invalid.

Field	Description
Age	A hyphen (-) indicates a static entry. For a dynamic entry, this field displays the elapsed time in seconds. If the neighbor is never reachable, this field displays a pound sign (#).
Vpn-instance	Name of a VPN or [No Vrf] with no VPN configured. The device does not support this field in the current software version.
NickName	Nickname of a neighboring entry. The name is a 4-bit hexadecimal number. This field is not supported in the current software version.

Related commands

- **ipv6 neighbor**
- **reset ipv6 neighbors**

display ipv6 neighbors count

Use **display ipv6 neighbors count** to display the number of neighbor entries.

Syntax

```
display ipv6 neighbors { { all | dynamic | static } [ slot slot-number ] | interface interface-type
interface-number | vlan vlan-id } count
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

all: Displays the total number of all neighbor entries, including neighbor entries created dynamically and configured statically.

dynamic: Displays the total number of neighbor entries created dynamically.

static: Displays the total number of neighbor entries configured statically.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the number of neighbor entries for all member devices.

interface *interface-type interface-number*: Specifies an interface by its type and number.

vlan *vlan-id*: Displays the total number of neighbor entries in the specified VLAN. The value range for VLAN ID is 1 to 4094.

Examples

Display the total number of neighbor entries created dynamically.

```
<Sysname> display ipv6 neighbors dynamic count
Total number of dynamic entries: 2
```

display ipv6 pathmtu

Use the **display ipv6 pathmtu** command to display IPv6 Path MTU information.

Syntax

```
display ipv6 pathmtu { ipv6-address | { all | dynamic | static } [ count ] }
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-address: Specifies the destination IPv6 address for which the Path MTU information is to be displayed.

all: Displays all Path MTU information for the public network.

dynamic: Displays all dynamic Path MTU information.

static: Displays all static Path MTU information.

count: Displays the total number of Path MTU entries.

Usage guidelines

Use **display ipv6 pathmtu** to display the IPv6 Path MTU information, including the dynamic Path MTUs and the static Path MTUs.

Examples

Display all Path MTU information.

```
<Sysname> display ipv6 pathmtu all
```

IPv6 destination address	PathMTU	Age	Type
1:2::3:2	1800	-	Static
1:2::4:2	1400	10	Dynamic
1:2::5:2	1280	10	Dynamic

Displays the total number of Path MTU entries.

```
<Sysname> display ipv6 pathmtu all count
```

```
Total number of entries: 3
```

Table 6 Command output

Field	Description
PathMTU	Path MTU value on the network path to an IPv6 address.
Age	Time for a Path MTU to live. For a static Path MTU, this field displays a hyphen (-).
Type	Whether the Path MTU is dynamically negotiated or statically configured.
Total number of entries	Total number of Path MTU entries.

Related commands

- **ipv6 pathmtu**
- **reset ipv6 pathmtu**

display ipv6 prefix

Use **display ipv6 prefix** to display information about IPv6 prefixes, including dynamic and static prefixes.

Syntax

```
display ipv6 prefix [ prefix-number ]
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

prefix-number: Specifies the ID of an IPv6 prefix, in the range of 1 to 1024. If this argument is not specified, the command displays information about all IPv6 prefixes.

Usage guidelines

A static IPv6 prefix is configured by using the **ipv6 prefix** command.

A dynamic IPv6 prefix is obtained from the DHCPv6 server, and its prefix ID is configured by using the **ipv6 dhcp client pd** command.

Examples

```
# Display information about all IPv6 prefixes.
```

```
<Sysname> display ipv6 prefix
Number Prefix                               Type
1       1::/16                               Static
2       11:77::/32                           Dynamic
```

```
# Display information about the IPv6 prefix with prefix ID 1.
```

```
<Sysname> display ipv6 prefix 1
Number: 1
Type : Dynamic
Prefix: ABCD:77D8::/32
Preferred lifetime 90 sec, valid lifetime 120 sec
```

Table 7 Command output

Field	Description
Number	Prefix ID.
Type	Prefix type: <ul style="list-style-type: none">• Static—Static IPv6 prefix.• Dynamic—Dynamic IPv6 prefix.
Prefix	Prefix and its length. If no prefix is obtained, this field displays Not-available .
Preferred lifetime 90 sec	Preferred lifetime in seconds. For a static IPv6 prefix, this field is not displayed.
valid lifetime 120 sec	Valid lifetime in seconds. For a static IPv6 prefix, this field is not displayed.

Related commands

- **ipv6 dhcp client pd**
- **ipv6 prefix**

display ipv6 rawip

Use **display ipv6 rawip** to display brief information about IPv6 RawIP connections.

Syntax

```
display ipv6 rawip [ slot slot-number ]
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

slot slot-number: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays brief information about IPv6 RawIP connections for all member devices.

Usage guidelines

Brief information about IPv6 RawIP connections includes the local and peer IPv6 addresses, protocol number, and PCB.

Examples

Display brief information about IPv6 RawIP connections.

```
<Sysname> display ipv6 rawip
```

```
Local Addr      Foreign Addr      Protocol Slot  PCB
2001:2002:2003:2 3001:3002:3003:3 58      1    0x0000000000000009
004:2005:2006:20 004:3005:3006:30
07:2008         07:3008
```

Table 8 Command output

Field	Description
Local Addr	Local IPv6 address.
Foreign Addr	Peer IPv6 address.
Protocol	Protocol number.
Slot	ID of the IRF member device.
PCB	PCB index.

display ipv6 rawip verbose

Use **display ipv6 rawip verbose** to display detailed information about IPv6 RawIP connections.

Syntax

```
display ipv6 rawip verbose [ slot slot-number [ pcb pcb-index ] ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pcb *pcb-index*: Displays detailed information about IPv6 RawIP connections of the specified PCB. The value range for the *pcb-index* argument is 1 to 16.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays detailed information about IPv6 RawIP connections for all member devices.

Usage guidelines

Detailed information about an IPv6 RawIP connection includes socket's creator, state, option, type, and protocol number, and source and destination IPv6 addresses of the connection.

Examples

Display detailed information about an IPv6 RawIP connection.

```
<Sysname> display ipv6 rawip verbose
```

```
Total RawIP socket number: 1
```

```
Location: slot: 1
```

```
Creator: ip6stackd[430]
```

```
State: N/A
```

```
Options: N/A
```

```
Error: 0
```

```
Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 9216 / 1 / 0 / N/A
```

```
Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
```

```
Type: 3
```

```
Protocol: 58
```

```
Connection info: src = ::, dst = ::
```

```
Inpcb flags: N/A
```

```
Inpcb extflag: N/A
```

```
Inpcb vflag: INP_IPV6
```

```
Hop limit: 255 (minimum hop limit: 0)
```

```
Send VRF: 0xffff
```

```
Receive VRF: 0xffff
```

Table 9 Command output

Field	Description
Total RawIP socket number	Total number of IPv6 RawIP sockets.
Location	Location of the device.
Slot	ID of the IRF member device.
Creator	Task name of the socket. The process number is in the square brackets.
State	Socket state.
Options	Socket options.

Field	Description
Receiving buffer (cc/hiwat/lowat/drop/state)	<p>Displays receive buffer information in the following order:</p> <ul style="list-style-type: none"> • cc—Used space. • hiwat—Maximum space. • lowat—Minimum space. • drop—Number of dropped packets. • state—Buffer state: <ul style="list-style-type: none"> ○ CANTSENDMORE—Unable to send data to the peer. ○ CANTRCVMORE—Unable to receive data from the peer. ○ RCVATMARK—Receiving tag. ○ N/A—None of the above states.
Sending buffer(cc/hiwat/lowat/state)	<p>Displays send buffer information in the following order:</p> <ul style="list-style-type: none"> • cc—Used space. • hiwat—Maximum space. • lowat—Minimum space. • state—Buffer state: <ul style="list-style-type: none"> ○ CANTSENDMORE—Unable to send data to the peer. ○ CANTRCVMORE—Unable to receive data from the peer. ○ RCVATMARK—Receiving tag. ○ N/A—None of the above states.
Type	<p>Socket type:</p> <ul style="list-style-type: none"> • 1—SOCK_STREAM. This socket uses TCP to provide reliable transmission of byte streams. • 2—SOCK_DGRAM. This socket uses UDP to provide datagram transmission. • 3—SOCK_RAW. This socket allows an application to change the next upper-layer protocol header. • N/A—None of the above types.
Protocol	Number of protocol using the socket. 58 represents ICMP.
Connection info	Connection information, including the source and destination IPv6 addresses.

Field	Description
Inpcb flags	<p>Flags in the Internet PCB:</p> <ul style="list-style-type: none"> • INP_RECVOPTS—Receives IPv6 options. • INP_RECVRETOPTS—Receives replied IPv6 options. • INP_RECVDSTADDR—Receives destination IPv6 address. • INP_HDRINCL—Provides the entire IPv6 header. • INP_REUSEADDR—Reuses the IPv6 address. • INP_REUSEPORT—Reuses the port number. • INP_ANONPORT—Port number not specified. • INP_PROTOCOL_PACKET—Identifies a protocol packet. • INP_RCVVLANID—Receives the VLAN ID of the packet. Only UDP and RawIP support this flag. • IN6P_IPV6_V6ONLY—Only supports IPv6 protocol stack. • IN6P_PKTINFO—Receives the source IPv6 address and input interface of the packet. • IN6P_HOPLIMIT—Receives the hop limit. • IN6P_HOPOPTS—Receives the hop-by-hop options extension header. • IN6P_DSTOPTS—Receives the destination options extension header. • IN6P_RTHDR—Receives the routing extension header. • IN6P_RTHDRDSTOPTS—Receives the destination options extension header preceding the routing extension header. • IN6P_TCLASS—Receives the traffic class of the packet. • IN6P_AUTOFLOWLABEL—Attaches a flow label automatically. • IN6P_RFC2292—Uses the API specified in RFC 2292. • IN6P_MTU—Discovers differences in the MTU size of every link along a given data path. TCP does not support this flag. • INP_RCVMACADDR—Receives the MAC address of the frame. • INP_USEICMPSRC—Uses the specified IPv6 address as the source IPv6 address for outgoing ICMP packets. • INP_SYNCPCB—Waits until Internet PCB is synchronized. • INP_EXTDONTDROP—Does not drop the received packet. • N/A—None of the above flags.
Inpcb extflag	<p>Extension flags in the Internet PCB:</p> <ul style="list-style-type: none"> • INP_EXTRCVPVCIDX—Records the PVC index of the received packet. • INP_RCVPWID—Records the PW ID of the received packet. • N/A—None of the above flags.
Inpcb vflag	<p>IP version flag in the Internet PCB:</p> <ul style="list-style-type: none"> • INP_IPV4—IPv4 protocol. • INP_IPV6—IPv6 protocol. • INP_IPV6PROTO—Creates an Internet PCB based on IPv6 protocol. • INP_TIMEWAIT—In TIMEWAIT state. • INP_ONESBCAST—Sends broadcast packets. • INP_DROPPED—Protocol dropped flag. • INP SOCKREF—Strong socket reference. • INP_DONTBLOCK—Do not block synchronization of the Internet PCB. • N/A—None of the above flags.
Hop limit(minimum hop limit)	Hop limit in the Internet PCB. The minimum number of hops is displayed in the parentheses.

Field	Description
Send VRF	Sent instances.
Receive VRF	Received instances.

display ipv6 statistics

Use **display ipv6 statistics** to display IPv6 and ICMPv6 packet statistics.

Syntax

display ipv6 statistics [slot *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 and ICMPv6 packet statistics for all member devices.

Usage guidelines

This command displays statistics about received and sent IPv6 and ICMPv6 packets.

Use the **reset ipv6 statistics** command to clear the statistics of all IPv6 and ICMPv6 packets.

Examples

Display IPv6 and ICMPv6 packet statistics.

```
<Sysname> display ipv6 statistics
```

```
IPv6 statistics:
```

```
Sent packets:
```

```
Total:      0
```

```
Sent locally: 0          Forwarded:      0
```

```
Raw packets:  0          Discarded:     0
```

```
Fragments:   0          Fragments failed: 0
```

```
Routing failed: 0
```

```
Received packets:
```

```
Total:      0
```

```
Received locally: 0          Hop limit exceeded: 0
```

```
Fragments:      0          Reassembled:       0
```

```
Reassembly failures: 0          Reassembly timeout: 0
```

```
Format errors:  0          Option errors:     0
```

```
Protocol errors: 0
```

```
ICMPv6 statistics:
```

```
Sent packets:
```

```

Total:      0
  Unreachable:      0          Too big:      0
  Hop limit exceeded: 0          Reassembly timeouts: 0
  Parameter problems: 0
  Echo requests:    0          Echo replies:    0
  Neighbor solicits: 0          Neighbor adverts: 0
  Router solicits:  0          Router adverts:  0
  Redirects:        0          Router renumbering: 0
Send failed:
  Rate limitation:  0          Other errors:    0

Received packets:
Total:      0
  Checksum errors:  0          Too short:      0
  Bad codes:        0
  Unreachable:      0          Too big:      0
  Hop limit exceeded: 0          Reassembly timeouts: 0
  Parameter problems: 0          Unknown error types: 0
  Echo requests:    0          Echo replies:    0
  Neighbor solicits: 0          Neighbor adverts: 0
  Router solicits:  0          Router adverts:  0
  Redirects:        0          Router renumbering: 0
  Unknown info types: 0
Deliver failed:
  Bad length:      0

```

Related commands

reset ipv6 statistics

display ipv6 tcp

Use **display ipv6 tcp** to display brief information about IPv6 TCP connections.

Syntax

display ipv6 tcp [slot *slot-number*]

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays brief information about IPv6 TCP connections for all member devices.

Usage guidelines

Brief information about IPv6 TCP connections includes the local IPv6 address and port number, peer IPv6 address and port number, and TCP connection state.

Examples

Display brief information about IPv6 TCP connections.

```
<Sysname> display ipv6 tcp
```

```
*: TCP MD5 Connection
```

```
  LAddr->port      FAddr->port      State      Slot  PCB
*2001:2002:2003:2  3001:3002:3003:3 ESTABLISHED 1     0x000000000000c387
004:2005:2006:20   004:3005:3006:30
07:2008->1200      07:3008->1200
```

Table 10 Command output

Field	Description
*	Indicates that the TCP connection uses MD5 authentication.
LAddr->port	Local IPv6 address and port number.
FAddr->port	Peer IPv6 address and port number.
State	IPv6 TCP connection state.
Slot	ID of the IRF member device.
PCB	PCB index.

display ipv6 tcp-proxy

Use **display ipv6 tcp-proxy** to display brief information about IPv6 TCP proxy.

Syntax

```
display ipv6 tcp-proxy slot slot-number
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

The following matrix shows the command and hardware compatibility:

Hardware series	Model	Command compatibility
WX1800H series	WX1804H WX1810H WX1820H	Yes
WX2500H series	WX2510H WX2540H WX2560H	Yes: • WX2540H • WX2560H No: • WX2510H

Hardware series	Model	Command compatibility
WX3000H series	WX3010H WX3010H-L WX3010H-X WX3024H WX3024H-L	Yes: <ul style="list-style-type: none"> WX3010H WX3024H No: <ul style="list-style-type: none"> WX3010H-L WX3010H-X WX3024H-L
WX3500H series	WX3508H WX3510H WX3520H WX3540H	Yes
WX5500E series	WX5510E WX5540E	Yes: WX5510E No: WX5540E
WX5500H series	WX5540H WX5560H WX5580H	No
Access controller modules	EWPXM1MAC0F EWPXM1WCME0 EWPXM2WCMD0F LSQM1WCMX20 LSQM1WCMX40 LSUM1WCME0 LSUM1WCMX20RT LSUM1WCMX40RT	No

IPv6 TCP proxy splits every IPv6 TCP connection that passes through it into two IPv6 TCP connections to relay data packets between servers and clients. The split is transparent to the servers and client. This feature reduces bandwidth use and improves IPv6 TCP performance. It is used for services such as load balancing.

Examples

Display brief information about IPv6 TCP proxy.

```
<Sysname> display ipv6 tcp-proxy
```

```

LAddr->port      FAddr->port      State      Service type
2001::1->45      11:22:33:44->54602  ESTABLISHED WAAS
11:22:33:44->54602  2001::1->45      ESTABLISHED WAAS

```

Table 11 Command output

Field	Description
Local Addr:port	Local IPv6 address and port number.
Foreign Addr:port	Peer IPv6 address and port number.
State	IPv6 TCP connection state.

Field	Description
Service type	Type of services that the IPv6 TCP proxy is used for: <ul style="list-style-type: none"> • LB—Load balancing services. This field is not supported in the current software version. • WAAS—Wide area application services. This field is not supported in the current software version.

display ipv6 tcp-proxy port-info

Use **display ipv6 tcp-proxy port-info** to display the usage of non-well known ports for IPv6 TCP proxy.

Syntax

display ipv6 tcp-proxy port-info slot slot-number

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot slot-number. Specifies an IRF member device by its member ID.

Usage guidelines

The following matrix shows the command and hardware compatibility:

Hardware series	Model	Command compatibility
WX1800H series	WX1804H WX1810H WX1820H	Yes
WX2500H series	WX2510H WX2540H WX2560H	Yes: • WX2540H • WX2560H No: WX2510H
WX3000H series	WX3010H WX3010H-L WX3010H-X WX3024H WX3024H-L	Yes: • WX3010H • WX3024H No: • WX3010H-L • WX3010H-X • WX3024H-L
WX3500H series	WX3508H WX3510H WX3520H WX3540H	Yes
WX5500E series	WX5510E WX5540E	Yes: WX5510E No: WX5540E

Hardware series	Model	Command compatibility
WX5500H series	WX5540H WX5560H WX5580H	No
Access controller modules	EWPXM1MAC0F EWPXM1WCME0 EWPXM2WCMD0F LSQM1WCMX20 LSQM1WCMX40 LSUM1WCME0 LSUM1WCMX20RT LSUM1WCMX40RT	No

The TCP ports are divided into well known ports (port numbers from 0 through 1023) and non-well known ports (port numbers from 1024 through 65535).

- Well known ports are for certain services, for example, port 23 for Telnet service, ports 20 and 21 for FTP service, and port 80 for HTTP service.
- Non-well known ports are available for various services. You can use the **display ipv6 tcp-proxy port-info** command to display the usage of these ports.

Examples

Display the usage of non-well known ports for IPv6 TCP proxy.

```
<Sysname> display ipv6 tcp-proxy port-info
```

```
Index  Range          State
16     [1024, 1087]    USABLE
17     [1088, 1151]    USABLE
18     [1152, 1215]    USABLE
19     [1216, 1279]    USABLE
20     [1280, 1343]    USABLE
...
1020   [65280, 65343]  USABLE
1021   [65344, 65407]  USABLE
1022   [65408, 65471]  USABLE
1023   [65472, 65535]  USABLE
```

Table 12 Command output

Field	Description
Index	Index of the port range.
Range	Start port number and end port number.
State	<p>State of the port range:</p> <ul style="list-style-type: none"> • USABLE—The ports are assignable. • ASSIGNED—Some ports are dynamically assigned and some ports are not. • ALLASSIGNED—All ports are dynamically assigned. The assigned ports can be reclaimed. • TO RECLAIM—Some ports are statically assigned. The assigned ports can be reclaimed. • RESERVED—The ports are reserved. The reserved ports cannot be dynamically assigned.

display ipv6 tcp verbose

Use **display ipv6 tcp verbose** to display detailed information about IPv6 TCP connections.

Syntax

```
display ipv6 tcp verbose [ slot slot-number [ pcb pcb-index ] ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pcb *pcb-index*: Displays detailed information about IPv6 TCP connections of the specified PCB. The value range for the *pcb-index* argument is 1 to 16.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays detailed information about IPv6 TCP connections for all member devices.

Usage guidelines

The detailed information includes socket's creator, state, option, type, protocol number, source IPv6 address and port number, destination IPv6 address and port number, and the connection state.

Examples

Display detailed information about an IPv6 TCP connection.

```
<Sysname> display ipv6 tcp verbose
```

```
TCP inpcb number: 1(tcpcb number: 1)
```

```
Location: slot: 1
```

```
NSR standby: N/A
```

```
Creator: bgpd[199]
```

```
State: ISCONNECTED
```

```
Options: N/A
```

```
Error: 0
```

```
Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 65536 / 1 / 0 / N/A
```

```
Sending buffer(cc/hiwat/lowat/state): 0 / 65536 / 512 / N/A
```

```
Type: 1
```

```
Protocol: 6
```

```
Connection info: src = 2001::1->179 , dst = 2001::2->4181
```

```
Inpcb flags: N/A
```

```
Inpcb extflag: N/A
```

```
Inpcb vflag: INP_IPV6
```

```
Hop limit: 255 (minimum hop limit: 0)
```

```
Connection state: ESTABLISHED
```

```
TCP options: TF_REQ_SCALE TF_REQ_TSTMP TF_SACK_PERMIT TF_NS
```

```
NSR state: READY(M)
```

```
Send VRF: 0x0
```

```
Receive VRF: 0x0
```

Table 13 Command output

Field	Description
TCP inpcb number	Number of IPv6 TCP Internet PCBs.
tcpcb number	Number of IPv6 TCP PCBs (excluding PCBs of TCP in TIME_WAIT state).
Location	Location of the device.
Slot	ID of the IRF member device.
NSR standby:	ID of the IRF member device and number of the slot where the NSR standby card resides. This field displays N/A if no NSR standby card is present.
Creator	Task name of the socket. The process number is in the square brackets.
State	Socket state.
Options	Socket options.
Error	Error code.
Receiving buffer(cc/hiwat/lowat/drop/state)	<p>Displays receive buffer information in the following order:</p> <ul style="list-style-type: none"> • cc—Used space. • hiwat—Maximum space. • lowat—Minimum space. • drop—Number of dropped packets. • state—Buffer state: <ul style="list-style-type: none"> ○ CANTSENDMORE—Unable to send data to the peer. ○ CANTRCVMORE—Unable to receive data from the peer. ○ RCVATMARK—Receiving tag. ○ N/A—None of the above states.
Sending buffer(cc/hiwat/lowat/state)	<p>Displays send buffer information in the following order:</p> <ul style="list-style-type: none"> • cc—Used space. • hiwat—Maximum space. • lowat—Minimum space. • state—Buffer state: <ul style="list-style-type: none"> ○ CANTSENDMORE—Unable to send data to the peer. ○ CANTRCVMORE—Unable to receive data from the peer. ○ RCVATMARK—Receiving tag. ○ N/A—None of the above states.
Type	<p>Socket type:</p> <ul style="list-style-type: none"> • 1—SOCK_STREAM. This socket uses TCP to provide reliable transmission of byte streams. • 2—SOCK_DGRAM. This socket uses UDP to provide datagram transmission. • 3—SOCK_RAW. This socket allows an application to change the next upper-layer protocol header. • N/A—None of the above types.
Protocol	Number of the protocol using the socket. 6 represents TCP.
Connection info	Connection information, including source IPv6 address and port number, and destination IPv6 address and port number.

Field	Description
Inpcb flags	<p>Flags in the Internet PCB:</p> <ul style="list-style-type: none"> • INP_RECVOPTS—Receives IPv6 options. • INP_RECVRETOPTS—Receives replied IPv6 options. • INP_RECVDSTADDR—Receives destination IPv6 address. • INP_HDRINCL—Provides the entire IPv6 header. • INP_REUSEADDR—Reuses the IPv6 address. • INP_REUSEPORT—Reuses the port number. • INP_ANONPORT—Port number not specified. • INP_PROTOCOL_PACKET—Identifies a protocol packet. • INP_RCVVLANID—Receives the VLAN ID of the packet. Only UDP and RawIP support this flag. • IN6P_IPV6_V6ONLY—Only supports IPv6 protocol stack. • IN6P_PKTINFO—Receives the source IPv6 address and input interface of the packet. • IN6P_HOPLIMIT—Receives the hop limit. • IN6P_HOPOPTS—Receives the hop-by-hop options extension header. • IN6P_DSTOPTS—Receives the destination options extension header. • IN6P_RTHDR—Receives the routing extension header. • IN6P_RTHDRDSTOPTS—Receives the destination options extension header preceding the routing extension header. • IN6P_TCLASS—Receives the traffic class of the packet. • IN6P_AUTOFLOWLABEL—Attaches a flow label automatically. • IN6P_RFC2292—Uses the API specified in RFC 2292. • IN6P_MTU—Discovers differences in the MTU size of every link along a given data path. TCP does not support this flag. • INP_RCVMACADDR—Receives the MAC address of the frame. • INP_SYNCPCB—Waits until Internet PCB is synchronized. • N/A—None of the above flags.
Inpcb extflag	<p>Extension flags in the Internet PCB:</p> <ul style="list-style-type: none"> • INP_EXTRCVPVICDX—Records the PVC index of the received packet. • INP_RCVPWID—Records the PW ID of the received packet. • N/A—None of the above flags.
Inpcb vflag	<p>IP version flags in the Internet PCB:</p> <ul style="list-style-type: none"> • INP_IPV4—IPv4 protocol. • INP_IPV6—IPv6 protocol. • INP_IPV6PROTO—Creates an Internet PCB based on IPv6 protocol. • INP_TIMEWAIT—In TIMEWAIT state. • INP_ONESBCAST—Sends broadcast packets. • INP_DROPPED—Protocol dropped flag. • INP_SOCKREF—Strong socket reference. • INP_DONTBLOCK—Do not block synchronization of the Internet PCB. • N/A—None of the above flags.
Hop limit(minimum hop limit)	Hop limit in the Internet PCB. The minimum number of hops is in the parentheses.

Field	Description
Connection state	<p>TCP connection state:</p> <ul style="list-style-type: none"> • CLOSED—The server receives a disconnection request's reply from the client. • LISTEN—The server is waiting for connection requests. • SYN_SENT—The client is waiting for the server to reply to the connection request. • SYN_RCVD—The server receives a connection request. • ESTABLISHED—The server and client have established connections and can transmit data bidirectionally. • CLOSE_WAIT—The server receives a disconnection request from the client. • FIN_WAIT_1—The client is waiting for the server to reply to a disconnection request. • CLOSING—The server and client are waiting for peer's disconnection reply when receiving disconnection requests from each other. • LAST_ACK—The server is waiting for the client to reply to a disconnection request. • FIN_WAIT_2—The client receives a disconnection reply from the server. • TIME_WAIT—The client receives a disconnection request from the server.
NSR state	<p>State of the TCP connections.</p> <p>Between the parentheses is the role of the connection:</p> <ul style="list-style-type: none"> • M—Main connection. • S—Standby connection.
Send VRF	Sent instances.
Receive VRF	Received instances.

display ipv6 udp

Use **display ipv6 udp** to display brief information about IPv6 UDP connections.

Syntax

```
display ipv6 udp [ slot slot-number ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays brief information about IPv6 UDP connections for all member devices.

Usage guidelines

Brief information about an IPv6 UDP connection includes local IPv6 address and port number, and peer IPv6 address and port number.

Examples

Displays brief information about IPv6 UDP connections.

```
<Sysname> display ipv6 udp
LAddr->port      FAddr->port      Slot  PCB
2001:2002:2003:2 3001:3002:3003:3 1     0x0000000000000c387
004:2005:2006:20 004:3005:3006:30
07:2008->1200    07:3008->1200
```

Table 14 Command output

Field	Description
LAddr->port	Local IPv6 address and port number.
FAddr->port	Peer IPv6 address and port number.
Slot	ID of the IRF member device.
PCB	PCB index.

display ipv6 udp verbose

Use **display ipv6 udp verbose** to display detailed information about IPv6 UDP connections.

Syntax

```
display ipv6 udp verbose [ slot slot-number [ pcb pcb-index ] ]
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

pcb *pcb-index*: Displays detailed information about IPv6 UDP connections of the specified PCB. The value range for the *pcb-index* argument is 1 to 16.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays detailed information about IPv6 UDP connections for all member devices.

Usage guidelines

The detailed information includes socket's creator, state, option, type, protocol number, source IPv6 address and port number, destination IPv6 address and port number, and connection state.

Examples

Display detailed information about an IPv6 UDP connection.

```
<Sysname> display ipv6 udp verbose
Total UDP socket number: 1

Location: slot:1
Creator: sock_test_mips[250]
State: N/A
Options: N/A
```

```

Error: 0
Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 41600 / 1 / 0 / N/A
Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
Type: 2
Protocol: 17
Connection info: src = ::->69, dst = ::->0
Inpcb flags: N/A
Inpcb extflag: N/A
Inpcb vflag: INP_IPV6
Hop limit: 255 (minimum hop limit: 0)
Send VRF: 0xffff
Receive VRF: 0xffff

```

Table 15 Command output

Field	Description
Total UDP socket number	Total number of IPv6 UDP sockets.
Location	Location of the device.
Slot	ID of the IRF member device.
Creator	Task name of the socket. The progress number is in the square brackets.
State	Socket state.
Options	Socket options.
Error	Error code.
Receiving buffer(cc/hiwat/lowat/drop/state)	<p>Displays receive buffer information in the following order:</p> <ul style="list-style-type: none"> • cc—Used space. • hiwat—Maximum space. • lowat—Minimum space. • drop—Number of dropped packets. • state—Buffer state: <ul style="list-style-type: none"> ○ CANTSENDMORE—Unable to send data to the peer. ○ CANTRCVMORE—Unable to receive data from the peer. ○ RCVATMARK—Receiving tag. ○ N/A—None of the above states.
Sending buffer(cc/hiwat/lowat/state)	<p>Displays send buffer information in the following order:</p> <ul style="list-style-type: none"> • cc—Used space. • hiwat—Maximum space. • lowat—Minimum space. • state—Buffer state: <ul style="list-style-type: none"> ○ CANTSENDMORE—Unable to send data to the peer. ○ CANTRCVMORE—Unable to receive data from the peer. ○ RCVATMARK—Receiving tag. ○ N/A—None of the above states.

Field	Description
Type	Socket type: <ul style="list-style-type: none"> • 1—SOCK_STREAM. This socket uses TCP to provide reliable transmission of byte streams. • 2—SOCK_DGRAM. This socket uses UDP to provide datagram transmission. • 3—SOCK_RAW. This socket allows an application to change the next upper-layer protocol header. • N/A—None of the above types.
Protocol	Number of the protocol using the socket. 17 represents UDP.
Connection info	Connection information, including source IPv6 address and port number, and destination IPv6 address and port number.
Inpcb flags	Flags in the Internet PCB: <ul style="list-style-type: none"> • INP_RECVOPTS—Receives IPv6 options. • INP_RECVRETOPTS—Receives replied IPv6 options. • INP_RECVDSTADDR—Receives destination IPv6 address. • INP_HDRINCL—Provides the entire IPv6 header. • INP_REUSEADDR—Reuses the IPv6 address. • INP_REUSEPORT—Reuses the port number. • INP_ANONPORT—Port number not specified. • INP_PROTOCOL_PACKET—Identifies a protocol packet. • INP_RCVVLANID—Receives the VLAN ID of the packet. Only UDP and RawIP support this flag. • IN6P_IPV6_V6ONLY—Only supports IPv6 protocol stack. • IN6P_PKTINFO—Receives the source IPv6 address and input interface of the packet. • IN6P_HOPLIMIT—Receives the hop limit. • IN6P_HOPOPTS—Receives the hop-by-hop options extension header. • IN6P_DSTOPTS—Receives the destination options extension header. • IN6P_RTHDR—Receives the routing extension header. • IN6P_RTHDRDSTOPTS—Receives the destination options extension header preceding the routing extension header. • IN6P_TCLASS—Receives the traffic class of the packet. • IN6P_AUTOFLOWLABEL—Attaches a flow label automatically. • IN6P_RFC2292—Uses the API specified in RFC 2292. • IN6P_MTU—Discovers differences in the MTU size of every link along a given data path. TCP does not support this flag. • INP_RCVMACADDR—Receives the MAC address of the frame. • INP_SYNCPCB—Waits until Internet PCB is synchronized. • N/A—None of the above flags.
Inpcb extflag	Extension flags in the Internet PCB: <ul style="list-style-type: none"> • INP_EXTRCVPVCIDX—Records the PVC index of the received packet. • INP_RCVPWID—Records the PW ID of the received packet. • N/A—None of the above flags.

Field	Description
Inpcb vflag	<p>IP version flags in the Internet PCB:</p> <ul style="list-style-type: none"> • INP_IPV4—IPv4 protocol. • INP_IPV6—IPv6 protocol. • INP_IPV6PROTO—Creates an Internet PCB based on IPv6 protocol. • INP_TIMEWAIT—In TIMEWAIT state. • INP_ONESBCAST—Sends broadcast packets. • INP_DROPPED—Protocol dropped flag. • INP_SOCKREF—Strong socket reference. • INP_DONTBLOCK—Do not block synchronization of the Internet PCB. • N/A—None of the above flags.
Hop limit(minimum hop limit)	Hop limit in the Internet PCB. The minimum number of hops is in the parentheses.
Send VRF	Sent instances.
Receive VRF	Received instances.

ipv6 address

Use **ipv6 address** to configure an IPv6 global unicast address for an interface.

Use **undo ipv6 address** to remove an IPv6 address of the interface.

Syntax

ipv6 address { *ipv6-address prefix-length* | *ipv6-address/prefix-length* }

undo ipv6 address [*ipv6-address prefix-length* | *ipv6-address/prefix-length*]

Default

No IPv6 global unicast address is configured for an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies an IPv6 address.

prefix-length: Specifies a prefix length in the range of 1 to 128.

Usage guidelines

Like public IPv4 addresses, IPv6 global unicast addresses are assigned to ISPs. This type of address allows for prefix aggregation to reduce the number of global routing entries.

If you do not specify any parameters, the **undo ipv6 address** command removes all IPv6 addresses of an interface.

Examples

Set the IPv6 global unicast address of VLAN-interface 100 to 2001::1 with prefix length 64.

Method 1:

```
<Sysname> system-view
```



```
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1/64

Method 2:
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1 64
```

ipv6 address anycast

Use **ipv6 address anycast** to configure an IPv6 anycast address for an interface.

Use **undo ipv6 address anycast** to remove the IPv6 anycast address of the interface.

Syntax

```
ipv6 address { ipv6-address prefix-length | ipv6-address/prefix-length } anycast
undo ipv6 address { ipv6-address prefix-length | ipv6-address/prefix-length } anycast
```

Default

No IPv6 anycast address is configured for an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies an IPv6 anycast address.

prefix-length: Specifies a prefix length in the range of 1 to 128.

Examples

Set the IPv6 anycast address of VLAN-interface 100 to 2001::1 with prefix length 64.

Method 1:

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1/64 anycast
```

Method 2:

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1 64 anycast
```

ipv6 address auto

Use **ipv6 address auto** to enable the stateless address autoconfiguration feature on an interface, so that the interface can automatically generate a global unicast address.

Use **undo ipv6 address auto** to disable this feature.

Syntax

```
ipv6 address auto
undo ipv6 address auto
```

Default

The stateless address autoconfiguration feature is disabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

After a global unicast address is generated through stateless autoconfiguration, a link-local address is generated automatically.

To remove the global unicast address and the link-local address that are automatically generated, use either of the following commands:

- **undo ipv6 address auto**
- **undo ipv6 address**

Examples

```
# Enable stateless address autoconfiguration on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address auto
```

ipv6 address auto link-local

Use **ipv6 address auto link-local** to automatically generate a link-local address for an interface.

Use **undo ipv6 address auto link-local** to remove the automatically generated link-local address for the interface.

Syntax

ipv6 address auto link-local

undo ipv6 address auto link-local

Default

No link-local address is configured on an interface. A link-local address is automatically generated after an IPv6 global unicast address is configured for the interface.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

Link-local addresses are used for neighbor discovery and stateless autoconfiguration on the local link. Packets using link-local addresses as the source or destination addresses cannot be forwarded to other links.

After an IPv6 global unicast address is configured for an interface, a link-local address is automatically generated. This link-local address is the same as the one generated by using the **ipv6 address auto link-local** command.

The **undo ipv6 address auto link-local** command removes only the link-local addresses generated through the **ipv6 address auto link-local** command. If the **undo** command is executed

on an interface with an IPv6 global unicast address configured the interface still has a link-local address.

You can also manually assign an IPv6 link-local address for an interface by using the **ipv6 address link-local** command. Manual assignment takes precedence over automatic generation for IPv6 link-local addresses.

- If you first use automatic generation and then manual assignment, the manually assigned link-local address overwrites the automatically generated address.
 - If you first use manual assignment and then automatic generation, both of the following occur:
 - The automatically generated link-local address does not take effect.
 - The link-local address of an interface is still the manually assigned address.
- If you delete the manually assigned address, the automatically generated link-local address takes effect.

Examples

```
# Configure VLAN-interface 100 to automatically generate a link-local address.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address auto link-local
```

Related commands

ipv6 address link-local

ipv6 address eui-64

Use **ipv6 address eui-64** to configure an EUI-64 IPv6 address for an interface.

Use **undo ipv6 address eui-64** to remove the EUI-64 IPv6 address of the interface.

Syntax

ipv6 address { *ipv6-address prefix-length* | *ipv6-address/prefix-length* } **eui-64**

undo ipv6 address [*ipv6-address prefix-length* | *ipv6-address/prefix-length*] **eui-64**

Default

No EUI-64 IPv6 address is configured for an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-address/prefix-length: Specifies an IPv6 address and IPv6 prefix length. The *ipv6-address* and *prefix-length* arguments jointly specify the prefix of an EUI-64 IPv6 address. The value range for the *prefix-length* argument is 1 to 64.

Usage guidelines

An EUI-64 IPv6 address is generated based on the specified prefix and the automatically generated interface ID. To display the EUI-64 IPv6 address, use the **display ipv6 interface** command.

The prefix length of an EUI-64 IPv6 address cannot be greater than 64.

Examples

```
# Configure an EUI-64 IPv6 address for VLAN-interface 100. The prefix of the address is the same as that of 2001::1/64, and the interface ID is generated based on the MAC address of the device.
```

Method 1:

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1/64 eui-64
```

Method 2:

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1 64 eui-64
```

Related commands

display ipv6 interface

ipv6 address *prefix-number*

Use **ipv6 address *prefix-number*** to specify an IPv6 prefix for an interface to automatically generate an IPv6 global unicast address and advertise the prefix.

Use **undo ipv6 address *prefix-number*** to restore the default.

Syntax

```
ipv6 address prefix-number sub-prefix/prefix-length
undo ipv6 address prefix-number
```

Default

No IPv6 prefix is specified for IPv6 address autoconfiguration.

Views

Interface view

Predefined user roles

network-admin

Parameters

prefix-number: Specifies an IPv6 prefix by its ID in the range of 1 to 1024. The specified IPv6 prefix can be manually configured or obtained through DHCPv6.

sub-prefix: Specifies the sub-prefix bit and host bit for the IPv6 global unicast address.

prefix-length: Specifies the sub-prefix length in the range of 1 to 128.

Usage guidelines

This command enables an interface to automatically generate an IPv6 global unicast address based on the specified IPv6 prefix, sub-prefix bit, and host bit.

An interface can generate only one IPv6 global unicast address based on the prefix specified by using the **ipv6 address** command. To configure the interface to generate a new IPv6 address, use the **undo ipv6 address** command and specify a new IPv6 prefix for the interface.

Examples

Configure a static IPv6 prefix AAAA::/16 and assign ID 1 to the prefix. Configure VLAN-interface 100 to use this prefix to generate the IPv6 address AAAA:CCCC:DDDD::10/32 and advertise this prefix.

```
<Sysname> system-view
[Sysname] ipv6 prefix 1 AAAA::/16
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 1 BBBB:CCCC:DDDD::10/32
```

Configure VLAN-interface 10 to obtain an IPv6 prefix through DHCPv6 and assign ID 2 to the obtained prefix. Configure VLAN-interface 100 to use the obtained prefix to generate an IPv6 address and advertise the prefix.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ipv6 dhcp client pd 2 rapid-commit option-group 1
[Sysname-Vlan-interface10] quit
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2 BBBB:CCCC:DDDD::10/32
```

Related commands

- **ipv6 prefix**
- **ipv6 dhcp client pd**

ipv6 address link-local

Use **ipv6 address link-local** to configure a link-local address for the interface.

Use **undo ipv6 address link-local** to remove the link-local address of the interface.

Syntax

ipv6 address *ipv6-address* **link-local**

undo ipv6 address *ipv6-address* **link-local**

Default

No link-local address is configured for the interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies an IPv6 link-local address. The first 10 bits of an address must be 1111111010 (binary). The first group of hexadecimals in the address must be FE80 to FEBF.

Usage guidelines

Manual assignment takes precedence over automatic generation.

If you use automatic generation, and then use manual assignment, the manually assigned link-local address overwrites the one that is automatically generated.

If you use manual assignment and then use automatic generation, both of the following occur:

- The automatically generated link-local address does not take effect.
- The manually assigned link-local address of an interface remains.

After you delete the manually assigned address, the automatically generated link-local address takes effect. For automatic generation of an IPv6 link-local address, see the **ipv6 address auto link-local** command.

Examples

Configure a link-local address for VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
```

```
[Sysname-Vlan-interface100] ipv6 address fe80::1 link-local
```

Related commands

ipv6 address auto link-local

ipv6 option drop enable

Use **ipv6 extension-header drop enable** to enable a device to discard IPv6 packets that contain extension headers.

Use **undo ipv6 extension-header drop enable** to restore the default.

Syntax

ipv6 extension-header drop enable

undo ipv6 extension-header drop enable

Default

A device does not discard IPv6 packets that contain extension headers.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This feature enables a device to discard a received IPv6 packet in which the extension headers cannot be processed by the device.

Examples

```
# Enable the device to discard IPv6 packets that contain extension headers.  
<Sysname> system-view  
[Sysname] ipv6 extension-header drop enable
```

ipv6 hop-limit

Use **ipv6 hop-limit** to set the Hop Limit field in the IPv6 header.

Use **undo ipv6 hop-limit** to restore the default.

Syntax

ipv6 hop-limit *value*

undo ipv6 hop-limit

Default

The hop limit is 64.

Views

System view

Predefined user roles

network-admin

Parameters

value: Specifies the number of hops, in the range of 1 to 255.

Usage guidelines

The hop limit determines the number of hops that an IPv6 packet generated by the device can travel.

The device advertises the hop limit in RA messages. All RA message receivers use the advertised value to fill in the Hop Limit field for IPv6 packets to be sent. To disable the device from advertising the hop limit, use the **ipv6 nd ra hop-limit unspecified** command.

Examples

```
# Set the maximum number of hops to 100.
<Sysname> system-view
[Sysname] ipv6 hop-limit 100
```

Related commands

ipv6 nd ra hop-limit unspecified

ipv6 hoplimit-expires enable

Use **ipv6 hoplimit-expires enable** to enable sending ICMPv6 time exceeded messages.

Use **undo ipv6 hoplimit-expires** to disable sending ICMPv6 time exceeded messages.

Syntax

```
ipv6 hoplimit-expires enable
undo ipv6 hoplimit-expires enable
```

Default

Sending ICMPv6 time exceeded messages is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

ICMPv6 time exceeded messages are sent to the source of IPv6 packets after the device discards IPv6 packets because hop or reassembly times out.

To prevent too many ICMPv6 error messages from affecting device performance, disable this feature. Even with the feature disabled, the device still sends fragment reassembly time exceeded messages.

Examples

```
# Disable sending ICMPv6 time exceeded messages.
<Sysname> system-view
[Sysname] undo ipv6 hoplimit-expires enable
```

ipv6 icmpv6 error-interval

Use **ipv6 icmpv6 error-interval** to set the bucket size and the interval for tokens to arrive in the bucket for ICMPv6 error messages.

Use **undo ipv6 icmpv6 error-interval** to restore the default.

Syntax

```
ipv6 icmpv6 error-interval milliseconds [ bucketsize ]  
undo ipv6 icmpv6 error-interval
```

Default

The bucket allows a maximum of 10 tokens, and a token is placed in the bucket every 100 milliseconds.

Views

System view

Predefined user roles

network-admin

Parameters

milliseconds: Specifies the interval for tokens to arrive in the bucket. The value range is 0 to 2147483647 milliseconds, and the default is 100 milliseconds. To disable the ICMPv6 rate limit, set the value to 0.

bucketsize: Specifies the maximum number of tokens allowed in the bucket. The value range is 1 to 200, and the default is 10.

Usage guidelines

This command limits the rate at which ICMPv6 error messages are sent. Use this command to prevent network congestion caused by excessive ICMPv6 error messages generated within a short period. A token bucket algorithm is used with one token representing one ICMPv6 error message.

A token is placed in the bucket at intervals until the maximum number of tokens that the bucket can hold is reached.

A token is removed from the bucket when an ICMPv6 error message is sent. When the bucket is empty, ICMPv6 error messages are not sent until a new token is placed in the bucket.

Examples

```
# Set the bucket size to 40 tokens and the interval for tokens to arrive in the bucket to 200 milliseconds for ICMPv6 error messages.
```

```
<Sysname> system-view  
[Sysname] ipv6 icmpv6 error-interval 200 40
```

ipv6 icmpv6 multicast-echo-reply enable

Use **ipv6 icmpv6 multicast-echo-reply enable** to enable replying to multicast echo requests.

Use **undo ipv6 icmpv6 multicast-echo-reply** to disable replying to multicast echo requests.

Syntax

```
ipv6 icmpv6 multicast-echo-reply enable  
undo ipv6 icmpv6 multicast-echo-reply enable
```

Default

The device is disabled from replying to multicast echo requests.

Views

System view

Predefined user roles

network-admin

Usage guidelines

If a host is configured to reply to multicast echo requests, an attacker can use this mechanism to attack the host. For example, the attacker can send an echo request to a multicast address with Host A as the source. All hosts in the multicast group will send echo replies to Host A.

To prevent attacks, do not enable the device to reply to multicast echo requests unless necessary.

Examples

```
# Enable replying to multicast echo requests.
<Sysname> system-view
[Sysname] ipv6 icmpv6 multicast-echo-reply enable
```

ipv6 icmpv6 source

Use **ipv6 icmpv6 source** to specify an IPv6 address as the source address for outgoing ICMPv6 packets.

Use **undo ipv6 icmpv6 source** to restore the default.

Syntax

```
ipv6 icmpv6 source ipv6-address
undo ipv6 icmpv6 source
```

Default

The device uses the IPv6 address of the sending interface as the source IPv6 address for outgoing ICMPv6 packets.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies an IPv6 address.

Usage guidelines

It is a good practice to specify the IPv6 address of the loopback interface as the source IPv6 address for outgoing ping echo request and ICMPv6 error messages. This feature helps users to easily locate the sending device.

Examples

```
# Specify IPv6 address 1::1 as the source address for outgoing ICMPv6 packets.
<Sysname> system-view
[Sysname] ipv6 icmpv6 source 1::1
```

ipv6 mtu

Use **ipv6 mtu** to set the MTU of IPv6 packets sent over an interface.

Use **undo ipv6 mtu** to restore the default MTU.

Syntax

```
ipv6 mtu mtu-size
undo ipv6 mtu
```

Default

No MTU is configured for an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

mtu-size: Specifies the size of the MTUs of an interface, in the range of 1280 to 1748 bytes.

Usage guidelines

IPv6 routers do not support packet fragmentation. After an IPv6 router receives an IPv6 packet, if the packet size is greater than the MTU of the forwarding interface, the router discards the packet. Meanwhile, the router sends the MTU to the source host through an ICMPv6 packet — Packet Too Big message. The source host fragments the packet according to the MTU and resends it. To reduce the extra flow overhead resulting from packet drops, set an appropriate interface MTU for your network.

Examples

```
# Set the MTU of IPv6 packets sent over VLAN-interface 100 to 1280 bytes.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 mtu 1280
```

ipv6 nd autoconfig managed-address-flag

Use **ipv6 nd autoconfig managed-address-flag** to set the managed address configuration flag (M) to 1 in RA advertisements to be sent.

Use **undo ipv6 nd autoconfig managed-address-flag** to restore the default.

Syntax

ipv6 nd autoconfig managed-address-flag

undo ipv6 nd autoconfig managed-address-flag

Default

The M flag is set to **0** in RA advertisements. Hosts receiving the advertisements will obtain IPv6 addresses through stateless autoconfiguration.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

The M flag in RA advertisements determines whether receiving hosts use stateful autoconfiguration to obtain IPv6 addresses.

- If the M flag is set to 1 in RA advertisements, receiving hosts use stateful autoconfiguration (for example, from an DHCPv6 server) to obtain IPv6 addresses.
- If the M flag is set to 0 in RA advertisements, receiving hosts use stateless autoconfiguration. Stateless autoconfiguration generates IPv6 addresses according to link-layer addresses and the prefix information in the RA advertisements.

Examples

```
# Set the M flag to 1 in RA advertisements to be sent.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd autoconfig managed-address-flag
```

ipv6 nd autoconfig other-flag

Use **ipv6 nd autoconfig other-flag** to set the other stateful configuration flag (O) to 1 in RA advertisements to be sent.

Use **undo ipv6 nd autoconfig other-flag** to restore the default.

Syntax

ipv6 nd autoconfig other-flag

undo ipv6 nd autoconfig other-flag

Default

The O flag is set to **0** in RA advertisements. Hosts receiving the advertisements will acquire other information through stateless autoconfiguration.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

The O flag in RA advertisements determines whether receiving hosts use stateful autoconfiguration to obtain configuration information other than IPv6 addresses.

- If the O flag is set to 1 in RA advertisements, receiving hosts use stateful autoconfiguration (for example, from a DHCPv6 server) to obtain configuration information other than IPv6 addresses.
- If the O flag is set to 0 in RA advertisements, receiving hosts use stateless autoconfiguration to obtain configuration information other than IPv6 addresses.

Examples

```
# Set the O flag to 0 in RA advertisements to be sent.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] undo ipv6 nd autoconfig other-flag
```

ipv6 nd dad attempts

Use **ipv6 nd dad attempts** to set the number of attempts to send an NS message for DAD.

Use **undo ipv6 nd dad attempts** to restore the default.

Syntax

ipv6 nd dad attempts *value*

undo ipv6 nd dad attempts

Default

The number of attempts to send an NS message for DAD is 1.

Views

Interface view

Predefined user roles

network-admin

Parameters

value: Specifies the number of attempts to send an NS message for DAD, in the range of 0 to 600. If it is set to 0, DAD is disabled.

Usage guidelines

An interface sends an NS message for DAD after obtaining an IPv6 address.

If the interface does not receive a response within the time specified by using **ipv6 nd ns retrans-timer**, it resends an NS message.

If the interface receives no response after making the maximum sending attempts (set by using **ipv6 nd dad attempts**), the interface uses the obtained address.

Examples

```
# Set the number of attempts to send an NS message for DAD to 20.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd dad attempts 20
```

Related commands

- **display ipv6 interface**
- **ipv6 nd ns retrans-timer**

ipv6 nd mode uni

Use **ipv6 nd mode uni** to configure a port as a customer-side port.

Use **undo ipv6 nd mode** to restore the default.

Syntax

```
ipv6 nd mode uni
```

```
undo ipv6 nd mode
```

Default

A port acts as a network-side port.

Views

VLAN interface view

Predefined user roles

network-admin

Usage guidelines

The following matrix shows the command and hardware compatibility:

Hardware series	Model	Command compatibility
WX1800H series	WX1804H WX1810H WX1820H	Yes

Hardware series	Model	Command compatibility
WX2500H series	WX2510H WX2540H WX2560H	Yes
WX3000H series	WX3010H WX3010H-L WX3010H-X WX3024H WX3024H-L	Yes: <ul style="list-style-type: none"> • WX3010H • WX3010H-L • WX3024H • WX3024H-L No: WX3010H-X
WX3500H series	WX3508H WX3510H WX3520H WX3540H	No
WX5500E series	WX5510E WX5540E	No
WX5500H series	WX5540H WX5560H WX5580H	No
Access controller modules	EWPXM1MAC0F EWPXM1WCME0 EWPXM2WCMD0F LSQM1WCMX20 LSQM1WCMX40 LSUM1WCME0 LSUM1WCMX20RT LSUM1WCMX40RT	No

By default, the device associates an ND entry with routing information when the device learns an ND entry. The ND entry provides the next hop information for routing. To save hardware resources, you can use this command to specify a port that connects to a user terminal as a customer-side port. The device will not associate the routing information with the learned ND entries.

Examples

Specify VLAN-interface 2 as a customer-side port.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ipv6 nd mode uni
```

ipv6 nd ns retrans-timer

Use **ipv6 nd ns retrans-timer** to set the interval for retransmitting an NS message.

Use **undo ipv6 nd ns retrans-timer** to restore the default.

Syntax

ipv6 nd ns retrans-timer *value*

undo ipv6 nd ns retrans-timer

Default

The local interface sends NS messages at every an interval of 1000 milliseconds, and the Retrans Timer field in the RA messages sent is 0. The interval for retransmitting an NS message is determined by the receiving device.

Views

Interface view

Predefined user roles

network-admin

Parameters

value: Specifies the interval value in the range of 1000 to 4294967295 milliseconds.

Usage guidelines

If a device does not receive a response from the peer within the specified interval, the device resends an NS message. The device retransmits an NS message at the specified interval and uses the interval value to fill the Retrans Timer field in RA messages to be sent.

Examples

```
# Specify VLAN-interface 100 to retransmit NS messages every 10000 milliseconds.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ns retrans-timer 10000
```

Related commands

display ipv6 interface

ipv6 nd nud reachable-time

Use **ipv6 nd nud reachable-time** to set the neighbor reachable time on an interface.

Use **undo ipv6 nd nud reachable-time** to restore the default.

Syntax

```
ipv6 nd nud reachable-time value
undo ipv6 nd nud reachable-time
```

Default

The neighbor reachable time on the local interface is 30000 milliseconds, and the value of the Reachable Time field in RA messages is 0. The reachable time is determined by the receiving device.

Views

Interface view

Predefined user roles

network-admin

Parameters

value: Specifies the neighbor reachable time in the range of 1 to 3600000 milliseconds.

Usage guidelines

If the neighbor reachability detection shows that a neighbor is reachable, the device considers the neighbor reachable within the specified reachable time. If the device must send a packet to the neighbor after the specified reachable time expires, the device reconfirms whether the neighbor is

reachable. The device sets the specified value as the neighbor reachable time on the local interface and uses the value to fill the Reachable Time field in RA messages to be sent.

Examples

```
# Set the neighbor reachable time on VLAN-interface 100 to 10000 milliseconds.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd nud reachable-time 10000
```

Related commands

display ipv6 interface

ipv6 nd ra halt

Use **ipv6 nd ra halt** to suppress an interface from advertising RA messages.

Use **undo ipv6 nd ra halt** to disable this feature.

Syntax

```
ipv6 nd ra halt
undo ipv6 nd ra halt
```

Default

An interface is suppressed from sending RA messages.

Views

Interface view

Predefined user roles

network-admin

Examples

```
# Disable RA message suppression on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] undo ipv6 nd ra halt
```

ipv6 nd ra hop-limit unspecified

Use **ipv6 nd ra hop-limit unspecified** to specify unlimited hops in RA messages.

Use **undo ipv6 nd ra hop-limit unspecified** to restore the default.

Syntax

```
ipv6 nd ra hop-limit unspecified
undo ipv6 nd ra hop-limit unspecified
```

Default

The maximum number of hops in the RA messages is limited to 64.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

To set the maximum number of hops to a value rather than the default setting, use the **ipv6 hop-limit** command.

Examples

```
# Specify unlimited hops in the RA messages on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ipv6 nd ra hop-limit unspecified
```

Related commands

ipv6 hop-limit

ipv6 nd ra interval

Use **ipv6 nd ra interval** to set the maximum and minimum intervals for advertising RA messages.

Use **undo ipv6 nd ra interval** to restore the default.

Syntax

ipv6 nd ra interval *max-interval-value min-interval-value*

undo ipv6 nd ra interval

Default

The maximum interval between RA messages is 600 seconds, and the minimum interval is 200 seconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

max-interval-value: Specifies the maximum interval value in seconds, in the range of 4 to 1800.

min-interval-value: Specifies the minimum interval value in the range of 3 seconds to three-fourths of the maximum interval.

Usage guidelines

The device advertises RA messages randomly between the maximum interval and the minimum interval.

The maximum interval for sending RA messages should be less than or equal to the router lifetime in RA messages.

Examples

```
# Set the maximum interval for advertising RA messages to 1000 seconds and the minimum interval to 700 seconds.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra interval 1000 700
```

Related commands

ipv6 nd ra router-lifetime

ipv6 nd ra no-advlinkmtu

Use **ipv6 nd ra no-advlinkmtu** to turn off the MTU option in RA messages.

Use **undo ipv6 nd ra no-advlinkmtu** to restore the default.

Syntax

ipv6 nd ra no-advlinkmtu

undo ipv6 nd ra no-advlinkmtu

Default

RA messages contain the MTU option.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

The MTU option in the RA messages specifies the link MTU to ensure that all nodes on the link use the same MTU.

Examples

Turn off the MTU option in RA messages on VLAN-interface 100.

```
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 100
```

```
[Sysname-Vlan-interface100] ipv6 nd ra no-advlinkmtu
```

ipv6 nd ra prefix

Use **ipv6 nd ra prefix** to configure the prefix information in RA messages.

Use **undo ipv6 nd ra prefix** to remove the prefix information from RA messages.

Syntax

ipv6 nd ra prefix { *ipv6-prefix prefix-length* | *ipv6-prefix/prefix-length* } *valid-lifetime preferred-lifetime* [**no-autoconfig** | **off-link**] *

undo ipv6 nd ra prefix { *ipv6-prefix* | *ipv6-prefix/prefix-length* }

Default

No prefix information is configured for RA messages. Instead, the IPv6 address of the interface sending RA messages is used as the prefix information.

If the IPv6 address is manually configured, the prefix uses the fixed valid lifetime 2592000 seconds (30 days) and preferred lifetime 604800 seconds (7 days).

If the IPv6 address is automatically obtained (through DHCP, for example), the prefix uses the valid and preferred lifetime of the IPv6 address.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-prefix: Specifies the IPv6 prefix.

prefix-length: Specifies the prefix length of the IPv6 address.

valid-lifetime: Specifies the valid lifetime of a prefix, in the range of 0 to 4294967295 seconds.

preferred-lifetime: Specifies the preferred lifetime of a prefix used for stateless autoconfiguration, in the range of 0 to 4294967295 seconds. The preferred lifetime cannot be greater than the valid lifetime.

no-autoconfig: Specifies a prefix not to be used for stateless autoconfiguration. If you do not specify this keyword, the prefix is used for stateless autoconfiguration.

off-link: Indicates that the address with the prefix is not directly reachable on the link. If you do not specify this keyword, the address with the prefix is directly reachable on the link.

Usage guidelines

After hosts on the same link receive RA messages, they can use the prefix information in the RA messages for stateless autoconfiguration.

Examples

Configure the prefix information in RA messages on VLAN-interface 100.

Method 1:

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra prefix 2001:10::100/64 100 10
```

Method 2:

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra prefix 2001:10::100 64 100 10
```

ipv6 nd ra router-lifetime

Use **ipv6 nd ra router-lifetime** to set the router lifetime in RA messages.

Use **undo ipv6 nd ra router-lifetime** to restore the default.

Syntax

ipv6 nd ra router-lifetime *value*

undo ipv6 nd ra router-lifetime

Default

The router lifetime in RA messages is 1800 seconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

value: Specifies the router lifetime in the range of 0 to 9000 seconds. If the value is set to 0, the router does not act as the default router.

Usage guidelines

The router lifetime in RA messages specifies how long the router sending the RA messages acts as the default router. Hosts receiving the RA messages check this value to determine whether to use the sending router as the default router. If the router lifetime is 0, the router cannot be used as the default router.

The router lifetime in RA messages must be greater than or equal to the advertising interval.

Examples

```
# Set the router lifetime in RA messages on VLAN-interface 100 to 1000 seconds.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra router-lifetime 1000
```

Related commands

ipv6 nd ra interval

ipv6 nd router-preference

Use **ipv6 nd router-preference** to set a router preference in RA messages.

Use **undo ipv6 nd router-preference** to restore the default.

Syntax

```
ipv6 nd router-preference { high | low | medium }
undo ipv6 nd router-preference
```

Default

The router preference is **medium**.

Views

Interface view

Predefined user roles

network-admin

Parameters

high: Sets the router preference to the highest setting.

low: Sets the router preference to the lowest setting.

medium: Sets the router preference to the medium setting.

Usage guidelines

A hosts selects a router with the highest preference as the default router.

When router preferences are the same in RA messages, a host selects the router corresponding to the first received RA message as the default gateway.

Examples

```
# Set the router preference in RA messages to the highest on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd router-preference high
```

ipv6 neighbor

Use **ipv6 neighbor** to configure a static neighbor entry.

Use **undo ipv6 neighbor** to remove a static neighbor entry.

Syntax

ipv6 neighbor *ipv6-address mac-address* { *vlan-id port-type port-number* | **interface** *interface-type interface-number* }

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

Default

No static neighbor entry is configured.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the IPv6 address of the static neighbor entry.

mac-address: Specifies the MAC address (48 bits) of the static neighbor entry, in the format of H-H-H.

vlan-id: Specifies the VLAN ID of the static neighbor entry, in the range of 1 to 4094.

port-type port-number: Specifies a Layer 2 port of the static neighbor entry by its type and number.

interface *interface-type interface-number*: Specifies a Layer 3 interface of the static neighbor entry by its type and number.

Usage guidelines

A neighbor entry stores information about a link-local node. The entry can be created dynamically through NS and NA messages, or configured statically.

The device uniquely identifies a static neighbor entry by using the neighbor's IPv6 address and the number of the Layer 3 interface that connects to the neighbor. You can configure a static neighbor entry by using either of the following methods:

- **Method 1**—Associate a neighbor IPv6 address and link-layer address with the Layer 3 interface of the local node.
- **Method 2**—Associate a neighbor IPv6 address and link-layer address with a Layer 2 port in a VLAN containing the local node.

You can use either of the previous configuration methods to configure a static neighbor entry for a VLAN interface.

- If Method 1 is used, the neighbor entry is in INCOMP state. After the device obtains the corresponding Layer 2 port information, the neighbor entry goes into REACH state.
- If Method 2 is used, the port specified by *port-type port-number* must belong to the VLAN specified by *vlan-id* and the corresponding VLAN interface must already exist. After the static neighbor entry is configured, the device associates the VLAN interface with the IPv6 address to uniquely identify the static neighbor entry. The entry will be in REACH state.

To remove a static neighbor entry for a VLAN interface, specify only the corresponding VLAN interface.

Examples

Configure a static neighbor entry for VLAN-interface 1.

```
<Sysname> system-view
[Sysname] ipv6 neighbor 2000::1 fe-e0-89 interface Vlan-interface 1
```

Related commands

- **display ipv6 neighbors**
- **reset ipv6 neighbors**

ipv6 neighbor link-local minimize

Use **ipv6 neighbor link-local minimize** to minimize link-local ND entries.

Use **undo ipv6 neighbor link-local minimize** to restore the default.

Syntax

```
ipv6 neighbor link-local minimize
undo ipv6 neighbor link-local minimize
```

Default

All ND entries are assigned to the driver.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Perform this command to minimize link-local ND entries assigned to the driver. Link-local ND entries refer to ND entries that contain link-local addresses.

By default, the device assigns all ND entries to the driver. With this feature enabled, the device does not add newly learned link-local ND entries whose link local addresses are not the next hop of any route to the driver. This saves driver resources.

This feature affects only newly learned link-local ND entries rather than existing ND entries.

Examples

```
# Minimize link-local ND entries.
<Sysname> system-view
[Sysname] ipv6 neighbor link-local minimize
```

ipv6 neighbor stale-aging

Use **ipv6 neighbor stale-aging** to set the aging timer for ND entries in stale state.

Use **undo ipv6 neighbor stale-aging** to restore the default.

Syntax

```
ipv6 neighbor stale-aging aging-time
undo ipv6 neighbor stale-aging
```

Default

The aging timer for ND entries in stale state is 240 minutes.

Views

System view

Predefined user roles

network-admin

Parameters

aging-time: Specifies the aging timer for ND entries in stale state, in the range of 1 to 1440 minutes.

Usage guidelines

This aging time applies to all ND entries in stale state. If an ND entry in stale state is not updated before the timer expires, it moves to the delay state. If it is still not updated in 5 seconds, the ND entry moves to the probe state. The device sends an NS message for detection a maximum of three times. If no response is received, the device deletes the ND entry.

Examples

```
# Set the aging timer for ND entries in stale state to 120 minutes.
```

```
<Sysname> system-view
```

```
[Sysname] ipv6 neighbor stale-aging 120
```

ipv6 neighbors max-learning-num

Use **ipv6 neighbors max-learning-num** to set the maximum number of dynamic neighbor entries that an interface can learn. This prevents the interface from occupying too many neighbor table resources.

Use **undo ipv6 neighbors max-learning-num** to restore the default.

Syntax

ipv6 neighbors max-learning-num *number*

undo ipv6 neighbors max-learning-num

Default

The following matrix shows the default values for the maximum number of dynamic neighbor entries that an interface can learn:

Hardware series	Model	Default
WX1800H series	WX1804H	512: WX1804H
	WX1810H	2048:
	WX1820H	<ul style="list-style-type: none">• WX1810H• WX1820H
WX2500H series	WX2510H	2048: WX2510H
	WX2540H	3072: WX2540H
	WX2560H	6144: WX2560H
WX3000H series	WX3010H	3072: WX3010H-X
	WX3010H-L	4096:
	WX3010H-X	<ul style="list-style-type: none">• WX3010H• WX3010H-L
	WX3024H	<ul style="list-style-type: none">• WX3024H-L
	WX3024H-L	8192: WX3024H
WX3500H series	WX3508H	8192
	WX3510H	16384

Hardware series	Model	Default
	WX3520H	32768
	WX3540H	40960
WX5500E series	WX5510E	20480
	WX5540E	61440
WX5500H series	WX5540H WX5560H WX5580H	61440: WX5540H 81920: <ul style="list-style-type: none"> • WX5560H • WX5580H
Access controller modules	EWPXM1MAC0F EWPXM1WCME0 EWPXM2WCMD0F LSQM1WCMX20 LSQM1WCMX40 LSUM1WCME0 LSUM1WCMX20RT LSUM1WCMX40RT	61440

Views

Layer 2/Layer 3 interface view

Layer 2/Layer 3 aggregate interface view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of dynamic neighbor entries that an interface can learn. The following matrix shows the value ranges for the *number* argument:

Hardware series	Model	Value range
WX1800H series	WX1804H	1 to 512: WX1804H
	WX1810H	1 to 2048: <ul style="list-style-type: none"> • WX1810H
	WX1820H	<ul style="list-style-type: none"> • WX1820H
WX2500H series	WX2510H	1 to 2048: WX2510H
	WX2540H	1 to 3072: WX2540H
	WX2560H	1 to 6144: WX2560H
WX3000H series	WX3010H	1 to 3072: WX3010H-X
	WX3010H-L	1 to 4096: <ul style="list-style-type: none"> • WX3010H
	WX3010H-X	<ul style="list-style-type: none"> • WX3010H-L
	WX3024H	<ul style="list-style-type: none"> • WX3024H-L
	WX3024H-L	1 to 8192: WX3024H

Hardware series	Model	Value range
WX3500H series	WX3508H WX3510H WX3520H WX3540H	1 to 8192: WX3508H 1 to 16384: WX3510H 1 to 32768: WX3520H 1 to 40960: WX3540H
WX5500E series	WX5510E	1 to 20480
	WX5540E	1 to 61440
WX5500H series	WX5540H WX5560H WX5580H	1 to 61440: WX5540H 1 to 81920: <ul style="list-style-type: none"> • WX5560H • WX5580H
Access controller modules	EWPXM1MAC0F EWPXM1WCME0 EWPXM2WCMD0F LSQM1WCMX20 LSQM1WCMX40 LSUM1WCME0 LSUM1WCMX20RT LSUM1WCMX40RT	1 to 61440

Usage guidelines

The device can dynamically acquire the link-layer address of a neighboring node through NS and NA messages and add it into the neighbor table.

When the number of dynamic neighbor entries reaches the threshold, the interface stops learning neighbor information.

Examples

Set the maximum number of dynamic neighbor entries that VLAN-interface 100 can learn to 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 neighbors max-learning-num 10
```

ipv6 pathmtu

Use **ipv6 pathmtu** to set a static Path MTU for an IPv6 address.

Use **undo ipv6 pathmtu** to remove the Path MTU configuration for an IPv6 address.

Syntax

ipv6 pathmtu *ipv6-address value*

undo ipv6 pathmtu *ipv6-address*

Default

No static Path MTU is set.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies an IPv6 address.

value: Specifies the Path MTU of the specified IPv6 address, in the range of 1280 to 10240 bytes.

Usage guidelines

You can set a static Path MTU for a destination IPv6 address. When a source host sends a packet through an interface, it compares the interface MTU with the static Path MTU of the specified destination IPv6 address. If the packet size is larger than the smaller one of the two values, the host fragments the packet according to the smaller value.

Examples

```
# Set a static Path MTU for an IPv6 address.
<Sysname> system-view
[Sysname] ipv6 pathmtu fe80::12 1300
```

Related commands

- **display ipv6 pathmtu**
- **reset ipv6 pathmtu**

ipv6 pathmtu age

Use **ipv6 pathmtu age** to set the aging time for a dynamic Path MTU.

Use **undo ipv6 pathmtu age** to restore the default.

Syntax

```
ipv6 pathmtu age age-time
undo ipv6 pathmtu age
```

Default

The aging time for dynamic Path MTU is 10 minutes.

Views

System view

Predefined user roles

network-admin

Parameters

age-time: Specifies the aging time for Path MTU in minutes, in the range of 10 to 100.

Usage guidelines

After the path MTU from a source host to a destination host is dynamically determined, the source host sends subsequent packets to the destination host based on this MTU. After the aging time expires, the following events occur:

- The dynamic Path MTU is removed.
- The source host determines a dynamic path MTU through the Path MTU mechanism again.

The aging time is invalid for a static Path MTU.

Examples

```
# Set the aging time for a dynamic Path MTU to 40 minutes.
```

```
<Sysname> system-view
[Sysname] ipv6 pathmtu age 40
```

Related commands

display ipv6 pathmtu

ipv6 prefer temporary-address

Use **ipv6 prefer temporary-address** to enable the system to preferentially use the temporary IPv6 address of the sending interface as the source address of a packet.

Use **undo ipv6 prefer temporary-address** to restore the default.

Syntax

ipv6 prefer temporary-address

undo ipv6 prefer temporary-address

Default

The system does not preferentially use the temporary IPv6 address of the sending interface as the source address of a packet.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The temporary address feature enables the system to generate and preferentially use the temporary IPv6 address of the sending interface as the source address of a packet. If the temporary IPv6 address cannot be used because of a DAD conflict, the system uses the public IPv6 address.

Examples

Enable the system to preferentially use the temporary IPv6 address of the sending interface as the source address of the packet.

```
<Sysname> system-view
[Sysname] ipv6 prefer temporary-address
```

Related commands

- **ipv6 address auto**
- **ipv6 nd ra prefix**
- **ipv6 temporary-address**

ipv6 prefix

Use **ipv6 prefix** to configure a static IPv6 prefix.

Use **undo ipv6 prefix** to remove a static IPv6 prefix.

Syntax

ipv6 prefix *prefix-number* *ipv6-prefix/prefix-length*

undo ipv6 prefix *prefix-number*

Default

No static IPv6 prefix is configured on the device.

Views

System view

Predefined user roles

network-admin

Parameters

prefix-number: Specifies a prefix ID in the range of 1 to 1024.

ipv6-prefix/prefix-length: Specifies a prefix and its length. The value range for the *prefix-length* argument is 1 to 128.

Usage guidelines

You cannot use the **ipv6 prefix** command to modify an existing static prefix.

Dynamic IPv6 prefixes obtained from DHCPv6 servers cannot be manually removed or modified.

A static IPv6 prefix can have the same prefix ID with a dynamic IPv6 prefix, but the static one takes precedence over the dynamic one.

Examples

```
# Create static IPv6 prefix 2001:0410::/32 with prefix ID 1.  
<Sysname> system-view  
[Sysname] ipv6 prefix 1 2001:0410::/32
```

Related commands

display ipv6 prefix

ipv6 reassemble local enable

Use **ipv6 reassemble local enable** to enable IPv6 local fragment reassembly.

Use **undo ipv6 reassemble local enable** to restore the default.

Syntax

ipv6 reassemble local enable

undo ipv6 reassemble local enable

Default

IPv6 local fragment reassembly is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

In a multichassis IRF fabric, this feature enables the receiving subordinate to reassemble the received IPv6 fragments instead of delivering them to the master for reassembly. It improves the fragment reassembly performance. This feature applies only to fragments received by the same subordinate in the IRF fabric.

ipv6 redirects enable

Use **ipv6 redirects enable** to enable sending ICMPv6 redirect messages.

Use **undo ipv6 redirects enable** to disable sending ICMPv6 redirect messages.

Syntax

ipv6 redirects enable
undo ipv6 redirects enable

Default

Sending ICMPv6 redirect messages is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The default gateway sends an ICMPv6 redirect message to the source of an IPv6 packet to inform the source of a better first hop.

Sending ICMPv6 redirect messages enables hosts that hold few routes to establish routing tables and find the best route. Because this feature adds host routes into the routing tables, host performance degrades when there are too many host routes. As a result, sending ICMPv6 redirect messages is disabled by default.

Examples

```
# Enable sending ICMPv6 redirect messages.
```

```
<Sysname> system-view
```

```
[Sysname] ipv6 redirects enable
```

ipv6 temporary-address

Use **ipv6 temporary-address** to enable the temporary IPv6 address feature.

Use **undo ipv6 temporary-address** to disable temporary IPv6 address generation and remove the existing temporary addresses.

Syntax

ipv6 temporary-address [*valid-lifetime preferred-lifetime*]
undo ipv6 temporary-address

Default

The system does not generate any temporary IPv6 address.

Views

System view

Predefined user roles

network-admin

Parameters

valid-lifetime: Specifies the valid lifetime for temporary IPv6 addresses, in the range of 600 to 4294967295 seconds. The default valid lifetime is 604800 seconds (7 days). The valid lifetime must be greater than or equal to the preferred lifetime.

preferred-lifetime: Specifies the preferred lifetime for temporary IPv6 addresses, in the range of 600 to 4294967295 seconds. The default preferred lifetime is 86400 seconds (1 day).

Usage guidelines

You must enable stateless autoconfiguration before enabling the temporary address feature.

In stateless address autoconfiguration, an interface automatically generates an IPv6 global unicast address by using the address prefix in the received RA message and the interface ID. On an IEEE 802 interface (such as an Ethernet interface or a VLAN interface), the interface ID is generated based on the interface's MAC address and is globally unique. An attacker can exploit this rule to easily identify the sending device.

To fix the vulnerability, you can enable the temporary address feature. An IEEE 802 interface generates the following addresses:

- **Public IPv6 address**—Includes an address prefix in the RA message and a fixed interface ID generated based on the interface's MAC address.
- **Temporary IPv6 address**—Includes an address prefix in the RA message and a random interface ID generated through MD5.

When the valid lifetime of a temporary IPv6 address expires, the system removes the address and generates a new one. This enables the system to send packets with different source addresses through the same interface. The preferred lifetime and valid lifetime for a temporary IPv6 address are determined as follows:

- The preferred lifetime of a temporary IPv6 address takes the smaller of the following values:
 - The preferred lifetime of the address prefix in the RA message.
 - The preferred lifetime configured for temporary IPv6 addresses minus `DESYNC_FACTOR` (a random number in the range of 0 to 600 seconds).
- The valid lifetime of a temporary IPv6 address takes the smaller of the following values:
 - The valid lifetime of the address prefix.
 - The valid lifetime configured for temporary IPv6 addresses.

Examples

```
# Enable the system to generate a temporary IPv6 address.
```

```
<Sysname> system-view
```

```
[Sysname] ipv6 temporary-address
```

Related commands

- **ipv6 address auto**
- **ipv6 nd ra prefix**
- **ipv6 prefer temporary-address**

ipv6 unreachable enable

Use **ipv6 unreachable enable** to enable sending ICMPv6 destination unreachable messages.

Use **undo ipv6 unreachable** to disable sending ICMPv6 destination unreachable messages.

Syntax

```
ipv6 unreachable enable
```

```
undo ipv6 unreachable enable
```

Default

Sending ICMPv6 destination unreachable messages is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

If the device fails to forward a received IPv6 packet because of a destination unreachable error, it performs the following operations:

- Drops the packet.
- Sends an ICMPv6 destination unreachable message to the source.

If the device is generating ICMPv6 destination unreachable messages incorrectly, disable sending ICMPv6 destination unreachable messages to prevent attack risks.

Examples

```
# Enable sending ICMPv6 destination unreachable messages.
```

```
<Sysname> system-view
```

```
[Sysname] ipv6 unreachable enable
```

local-proxy-nd enable

Use **local-proxy-nd enable** to enable local ND proxy.

Use **undo local-proxy-nd enable** to restore the default.

Syntax

local-proxy-nd enable

undo local-proxy-nd enable

Default

Local ND proxy is disabled.

Views

VLAN interface view

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

Predefined user roles

network-admin

Examples

```
# Enable local ND proxy on VLAN-interface 100.
```

```
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 100
```

```
[Sysname-Vlan-interface100] local-proxy-nd enable
```

Related commands

proxy-nd enable

proxy-nd enable

Use **proxy-nd enable** to enable common ND proxy.

Use **undo proxy-nd enable** to restore the default.

Syntax

proxy-nd enable
undo proxy-nd enable

Default

Common ND proxy is disabled.

Views

VLAN interface view
Layer 3 Ethernet interface view
Layer 3 Ethernet subinterface view

Predefined user roles

network-admin

Examples

```
# Enable common ND proxy on VLAN-interface 100.  
<Sysname> system-view  
[Sysname] interface vlan-interface 100  
[Sysname-Vlan-interface100] proxy-nd enable
```

Related commands

local-proxy-nd enable

reset ipv6 neighbors

Use **reset ipv6 neighbors** to clear IPv6 neighbor information.

Syntax

```
reset ipv6 neighbors { all | dynamic | interface interface-type interface-number | slot slot-number  
| static }
```

Views

User view

Predefined user roles

network-admin

Parameters

all: Clears static and dynamic neighbor information for all interfaces.

dynamic: Clears dynamic neighbor information for all interfaces.

interface *interface-type interface-number*: Clears dynamic neighbor information for the interface specified by its type and number.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears dynamic neighbor information for all member devices.

static: Clears static neighbor information for all interfaces.

Usage guidelines

You can use the **display ipv6 neighbors** command to display IPv6 neighbor information.

Examples

```
# Clear neighbor information for all interfaces.  
<Sysname> reset ipv6 neighbors all
```

This will delete all the entries. Continue? [Y/N]:Y

Clear dynamic neighbor information for all interfaces.

```
<Sysname> reset ipv6 neighbors dynamic
```

This will delete all the dynamic entries. Continue? [Y/N]:Y

Clear all neighbor information for GigabitEthernet 1/0/1.

```
<Sysname> reset ipv6 neighbors interface gigabitethernet 1/0/1
```

This will delete all the dynamic entries by the interface you specified. Continue? [Y/N]:Y

Related commands

- **display ipv6 neighbors**
- **ipv6 neighbor**

reset ipv6 pathmtu

Use **reset ipv6 pathmtu** to clear the Path MTU information.

Syntax

```
reset ipv6 pathmtu { all | dynamic | static }
```

Views

User view

Predefined user roles

network-admin

Parameters

all: Clears all Path MTUs.

dynamic: Clears all dynamic Path MTUs.

static: Clears all static Path MTUs.

Examples

Clear all Path MTUs.

```
<Sysname> reset ipv6 pathmtu all
```

Related commands

```
display ipv6 pathmtu
```

reset ipv6 statistics

Use **reset ipv6 statistics** to clear IPv6 and ICMPv6 packet statistics.

Syntax

```
reset ipv6 statistics [ slot slot-number ]
```

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears IPv6 and ICMPv6 packet statistics for all member devices.

Examples

Clear IPv6 and ICMPv6 packet statistics.

```
<Sysname> reset ipv6 statistics
```

Related commands

display ipv6 statistics