IPv6 Configuration Commands

Table of Contents

Table of Contents I

Chapter 1 IPv6 Configuration Commands 1

1.1 IPv6 Configuration Commands 1

1.1.1 ipv6 address 1

1.1.2 ipv6 address anycast 2

1.1.3 ipv6 address autoconfig 3

1.1.4 ipv6 address eui-64 3

1.1.5 ipv6 address link-local 4

1.1.6 ipv6 enable 5

1.1.7 show ipv6 interface 6

1.1.8 ipv6 unicast-routing 7

Chapter 2 IPv6 Configuration Commands 8

2.1 IPv6 Configuration Commands 8

2.1.1 clear ipv6 traffic 8

2.1.2 debug ipv6 packet 9

2.1.3 ipv6 route-cache 10

2.1.4 ipv6 fast-switch 10

2.1.5 ipv6 fast-tunnel 11

2.1.6 ipv6 cur-hoplimit 11

2.1.7 ipv6 general-prefix 12

2.1.8 ipv6 icmp-ratelimit 13

2.1.9 ipv6 mtu 13

2.1.10 ipv6 redirects 14

2.1.11 ipv6 source-route 15

2.1.12 ipv6 traffic-filter 15

2.1.13 ipv6 unreachables 16

2.1.14 show ipv6 general-prefix 17

2.1.15 show ipv6 pmtu 17

2.1.16 show ipv6 traffic 18

Chapter 3 IPv6 ACL Configuration Commands 20

3.1 IPv6 ACL Configuration Commands 20

3.1.1 ipv6 access-list 20

3.1.2 ipv6 traffic-filter 21

3.1.3 deny/permit 22

3.1.4 sequence 28

3.1.5 show ipv6 access-list 30

3.1.6 clear ipv6 access-list 31

Chapter 4 IPv6IP tunnel Configuration Commands 33

4.1 Tunnel Interface Configuration Commands 33

4.1.1 Interface tunnel 33

4.1.2 Tunnel mode ipv6ip 33

4.1.3 Tunnel source 34

4.1.4 Tunnel destination 35
4.2 IPv6 IP Debug Configuration Commands 36
4.2.1 Debug ipv6ip 36
Chapter 5 DHCPv6 Configuration Commands 37
5.1 DHCPv6 Client Configuration Commands 37
5.1.1 ipv6 dhcp client pd 37
5.1.2 ipv6 dhcp client pd hint 38
5.2 DHCPv6 Relay Configuration Commands 38
5.2.1 ipv6 dhcp relay destination 38
5.3 DHCPv6 Server Configuration Commands 39
5.3.1 ipv6 dhcp server 39
5.3.2 ipv6 dhcp pool 40
5.3.3 ipv6 local pool 41
5.4 DHCPv6 Pool Configuration Commands 42
5.4.1 Dns-server 42
5.4.2 domain-name 42
5.4.3 prefix-delegation 43
5.4.4 prefix-delegation pool 44
5.4.5 lifetime 45
5.5 DHCPv6 Debug Configuration Commands 45
5.5.1 Debug ipv6 dhcp 45
5.5.2 Debug ipv6 dhcp relay 46
5.6 DHCPv6 Management Configuration Commands 47
5.6.1 Show ipv6 dhcp 47
5.6.2 Show ipv6 dhcp interface 47
5.6.3 Show ipv6 dhcp pool 48
5.6.4 Show ipv6 dhcp binding 49
5.6.5 Show ipv6 local pool 49
5.6.6 Clear ipv6 dhcp binding 50
Chapter 6 Neighbor Discovery Commands 51
6.1 ND Commands 51
6.1.1 debug ipv6 nd 51
6.1.2 show ipv6 neighbors 52
6.1.3 clear ipv6 neighbors 52
6.1.4 ipv6 neighbor 53
6.1.5 ipv6 nd dad attempts 53
6.1.6 ipv6 nd managed-flag 54
6.1.7 ipv6 nd ns-interval 54
6.1.8 ipv6 nd other-flag 55
6.1.9 ipv6 nd prefix 55
6.1.10 Ipv6 nd ra interval 57
6.1.11 ipv6 nd ra-interval 57
6.1.12 ipv6 nd ra-lifetime 58
6.1.13 ipv6 nd reachable-time 59
6.1.14 ipv6 nd router-preference 59
6.1.15 ipv6 nd suppress-ra 60

Chapter 7 OSPFv3 Configuration Commands 61
7.1 OSPFv3 Configuration Commands 61
7.1.1 area default-cost 62
7.1.2 area range 63
7.1.3 area stub 64
7.1.4 area virtual-link 65
7.1.5 debug ipv6 ospf 66
7.1.6 debug ipv6 ospf events 68
7.1.7 debug ipv6 ospf ifsm 69
7.1.8 debug ipv6 ospf lsa 71
7.1.9 debug ipv6 ospf nfsm 73
7.1.10 debug ipv6 ospf nsm 75
7.1.11 debug ipv6 ospf packet 76
7.1.12 debug ipv6 ospf route 78
7.1.13 default-metric 79
7.1.14 ipv6 ospf area 80
7.1.16 ipv6 ospf authentication 80
7.1.17 ipv6 ospf encryption 81
7.1.18 ipv6 ospf cost 82
7.1.19 ipv6 ospf dead-interval 82
7.1.20 ipv6 ospf hello-interval 83
7.1.21 ipv6 ospf priority 84
7.1.22 ipv6 ospf retransmit-interval 85
7.1.23 ipv6 ospf transmit-delay 85
7.1.24 ipv6 router ospf 86
7.1.25 redistribute 87
7.1.26 router-id 88
7.1.27 show ipv6 ospf 88
7.1.28 show ipv6 ospf database 89
7.1.29 show ipv6 ospf interface 91
7.1.30 show ipv6 ospf neighbor 92
7.1.31 show ipv6 ospf route 93
7.1.32 show ipv6 ospf virtual-link 94
7.1.33 summary-prefix 96
7.1.34 timers delay 96
7.1.35 timers hold 97
Chapter 8 Ripng Configuration Commands 99
8.1 Ripng Configuration Commands 99
8.1.1 clear ipv6 rip route 99
8.1.2 debug ipv6 rip 100
8.1.3 default-metric 101
8.1.4 distance 101
8.1.5 distribut-list prefix-list 102
8.1.6 ipv6 rip enable 103
8.1.7 ipv6 rip poison-reverse 103
8.1.8 ipv6 rip split-horizon 104

8.1.9 ipv6 rip summary-address 104
8.1.10 ipv6 route default-information 105
8.1.11 ipv6 router rip 106
8.1.12 maximum-paths 106
8.1.13 maximum-routes 107
8.1.14 neighbor 107
8.1.15 offset 108
8.1.16 passive interface 109
8.1.17 Port 109
8.1.18 redistribute 110
8.1.19 show ipv6 rip 111
8.1.20 show ipv6 rip interface 112
8.1.21 timers 112
Chapter 9 rtv6 Configuration Command Contents 114
9.1 rtv6 Configuration Commands 114
9.1.1 clear ipv6 route static 114
9.1.2 debug ipv6 routing 114
9.1.3 ipv6 route cache-check 115
9.1.4 ipv6 route default 116
9.1.5 ipv6 route equal-cost-paths 116
9.1.6 ipv6 route max-number 117
9.1.7 ipv6 route 117
9.1.8 show ipv6 route 118
Chapter 10 NATPT Protocol Configuration Commands 119
10.1 NATPT Protocol Configuration Commands 119
10.1.1 ipv6 nat 119
10.1.2 ipv6 nat max-entries 120
10.1.3 ipv6 nat prefix 121
10.1.4 ipv6 nat prefix v4-mapped 122
10.1.5 ipv6 nat translations 123
10.1.6 ipv6 nat v4v6 pool 124
10.1.7 ipv6 nat v4v6 source 125
10.1.8 ipv6 nat v6v4 pool 127
10.1.9 ipv6 nat v6v4 source 128
Chapter 11 NATPT Configuration Commands 130
11.1 NATPT Configuration Commands 130
11.1.1 debug ipv6 nat 130
11.1.2 show ipv6 nat translations 131
11.1.3 show ipv6 nat statistics 131
11.1.4 show ipv6 nat pools 132
11.1.5 clear ipv6 nat translations 132

Chapter 1 IPv6 Configuration Commands

1.1 IPv6 Configuration Commands

IPv6 configuration commands include the following ones:

- ipv6 address
- ipv6 address anycast
- ipv6 address autoconfig
- ipv6 address eui-64
- ipv6 address link-local
- ipv6 enable
- show ipv6 interface

1.1.1 ipv6 address

To configure an IPv6 address in the interface configuration mode and enable IPv6, run the first one of the following two commands. To disable this feature, use the no form of this command.

ipv6 address { *ipv6-address/prefix-length* | *prefix-name sub-bits/prefix-length* **}**

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

Parameters

Parameters	Description
ipv6-address	The IPv6 address to be used.
/prefix-length	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
Prefix-name	The name assigned to the prefix of IPv6 address.
Sub-bits	The subprefix bits and host bits of the address to be concatenated with the prefixes provided by the general prefix specified with the prefix-name argument. The sub-bits argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Command Default

No IPv6 addresses are defined for any interface.

Command Mode

Interface configuration

Usage Guidelines

Using the no ipv6 address autoconfig command without arguments removes all IPv6 addresses from an interface.

Example

The following example shows how to enable IPv6 processing on the interface and configure an address based on the general prefix called my-prefix and the directly specified bits:

```
Router_config_f0/1# ipv6 address 2001:0:0:0:0DB8:800:200C:417A/64
```

Related Commands

ipv6 address anycast

ipv6 address eui-64

ipv6 address link-local

show ipv6 interface

1.1.2 ipv6 address anycast

To configure an IPv6 anycast address and enable IPv6 processing on an interface, use the ipv6 address anycast command in interface configuration mode. To remove the address from the interface, use the no form of this command.

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

no ipv6 address [*ipv6-prefix/prefix-length* **anycast]**

Parameters

Parameters	Description
Ipv6-prefix	The IPv6 network assigned to the interface.
/prefix-length	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default

anycast address is configured.

Command Mode

Interface configuration

Usage Guidelines

Using the **no ipv6 address** command without arguments removes all manually configured IPv6 addresses from an interface.

Example

```
Router_config# ipv6 address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE/64 anycast
```

Related Commands

ipv6 address aui-64

ipv6 address link-local

show ipv6 interface

1.1.3 ipv6 address autoconfig

To enable automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface and enable IPv6 processing on the interface, use the ipv6 address autoconfig command in interface configuration mode. To remove the address from the interface, use the no form of this command.

Ipv6 address autoconfig

no ipv6 address autoconfig

Parameters

None

Command Default

No IPv6 address is defined for the interface.

Command Mode

Interface configuration

Example

```
Router_config_f0/1# ipv6 address autoconfig
```

1.1.4 ipv6 address eui-64

To enable an IPv6 address in VLAN interface configuration mode, run **ipv6 address eui-64**. Enable IPv6 protocol on the port simultaneously. To remove the ipv6 address, run **no ipv6 address eui-64**.

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

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

Parameters

Parameters	Description
Ipv6-prefix	The IPv6 network assigned to the interface.
/prefix-length	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default

The IPv6 address in the eui-64 form is not configured on the interface.

Command Mode

Interface configuration

Usage Guidelines

If you run **no ipv6 address**, which has no parameters, all manually configured IPv6 addresses on the interface will be deleted.

If the ***prefix-length*** parameter is bigger than 64 bits, the ***prefix-length*** is prior to the length of the interface ID.

Example

```
Router_config_f0/1# ipv6 address 2001:0:0:0:0DB8::/64 eui-64
```

Related Commands

ipv6 address link-local
show ipv6 interface

1.1.5 ipv6 address link-local

To set a link-local address in VLAN interface configuration mode and meanwhile enable IPv6 on the interface, run the following command. To delete link-local address, use the no form of the command.

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

no ipv6 address [*ipv6-address* **link-local]**

Parameters

Parameters	Description
ipv6-address	To-be-added IPv6 address. The format of this address must conform to the definition in RFC 4291 strictly.
link-local	A link-local address. The link-local address designated by the ipv6-address command will automatically replace the automatically configured link-local address.

Command Default

No default IPv6 link-local address exists on the interface.

Command Mode

Interface configuration

Usage Guidelines

If you run no ipv6 address, which has no parameters, all manually configured IPv6 addresses on the interface will be deleted. If you run ipv6 enable, a link-local address will be automatically set. Of course you can set the link-local address manually, the command you will use is ipv6 address link-local.

Example

The following example shows how to set a link-local address manually on the VLAN interface:

```
Router_config_f0/1# ipv6 address FE80::A00:3EFF:FE12:3457 link-local
```

Related Commands

ipv6 address eui-64

show ipv6 interface

1.1.6 ipv6 enable

If the IPv6 address is not set on the interface but users want to enable the IPv6 protocol on this interface, run ipv6 enable. To disable IPv6 protocol, run **no ipv6 enable**.

ipv6 enable

no ipv6 enable

Parameters

None

Command Default

The IPv6 protocol is forbidden on the interface.

Command Mode

Interface configuration

Usage Guidelines

After the ipv6 enable command is run, the system will add a link-local address on the interface automatically. At the same time, the communication range of the IPv6 protocol on the interface is confined to the links that the interface connects. If the IPv6 address has already configured on the interface explicitly, you cannot forbid IPv6 processing on the interface even though you use the no ipv6 enable command.

Example

```
Router_config# interface fastethernet 0/1
Router_config_f0/1# ipv6 enable
```

Related Commands

ipv6 address link-local

ipv6 address eui-64

show ipv6 interface

1.1.7 show ipv6 interface

To show the information about the interface on which the IPv6 protocol is enabled, run the following command:

show ipv6 interface [*interface-type interface-number* **] | [brief]**

Parameters

Parameters	Description
interface-type	The interface type
interface-number	The interface ID

Command Default

Those interfaces on which the IPv6 protocol is enabled will all be displayed.

Command Mode

Global configuration

Usage Guidelines

This command can be used to display the state of IPv6 on the interface, the configured IPv6 address and other IPv6 related parameters.

Example

To show the state of IPv6 of fastethernet 0/1, run following commands:

```
Router# show ipv6 interface fastEthernet 0/1

FastEthernet0/1 is down, line protocol is down
  IPv6 is enabled, link-local address is FE80::A00:3EFF:FE12:3457
  [TENTATIVE] Global unicast address(es):
    5678::111, subnet is 5678::/64
  [TENTATIVE] Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF12:3457
    FF02::1:FF00:111
  MTU is 1500 bytes
  ICMP error messages limited to one every 100
  milliseconds ICMP redirects are enabled
  ICMP unreachables are enabled
```

Field	Description
FastEthernet0/1 is up(down/administratively down)	Indicates whether the physical layer of the interface is accessible or whether it can be shut down manageably.

line protocol is up (down)	Indicates whether the line protocol (the software layer) is accessible.
IPv6 is enabled	Enables the IPv6 protocol.
link-local address	Shows the link-local address of an interface.
Global unicast address(es):	Shows the unicast address of an interface.
Joined group address(es):	Shows the multicast address of an interface.
MTU	Shows the MTU of an interface.
ICMP error messages	Shows the transmission frequency of ICMPv6 error packets (the minimum interval).
ICMP redirects	Shows whether the redirection packet will be sent or not.
ICMP unreachables	Shows whether the destination unreachable packet will be enabled or shut down.

Related Commands

1.1.8 ipv6 unicast-routing

To configure unicast routing protocol, run the first one of the following two commands. To return to the default value, use the no form of the command.

ipv6 unicast-routing no

ipv6 unicast-routing

Parameters

None

Command Default

No default behavior or

values. Command Mode

Global configuration

Usage Guidelines

The command is used to enable ipv6 unicast routing protocol. Enable the command before enabling ipv6 unicast routing.

Example

None

Related Commands

None

Chapter 2 IPv6 Configuration Commands

2.1 IPv6 Configuration Commands

IPv6 configuration commands include following ones:

- clear ipv6 traffic
- debug ipv6 packet
- ipv6 cur-hoplimit
- ipv6 icmp6-ratelimit
- ipv6 mtu
- ipv6 redirect
- ipv6 source-route
- show ipv6 pmtu
- show ipv6 traffic

2.1.1 clear ipv6 traffic

To reset IPv6 traffic counters, use the clear ipv6 traffic command in privileged EXEC mode.

clear ipv6 traffic

Parameters

None

Command Mode

EXEC

Usage Guidelines

Using this command resets the counters in the output from the show ipv6 traffic command.

Example

The following example shows how to delete the statistics information about IPv6 flow:

```
Router# clear ipv6 traffic
Router#     show     ipv6
traffic IPv6 statistics:
   Rcvd: 0 total, 0 local destination
             0 badhdrs, 0 badvers
             0 tooshort, 0 toosmall, 0 toomanyhdrs
             0 source-routed, 0 badscope
             0 badopts, 0 unknowopts, 0 exthdrtoolong
             0 fragments, 0 total reassembled
             0 reassembly timeouts, 0 reassembly failures
```

```
  Sent: 0 generated, 0 forwarded, 0 cant forwarded
          0 fragmented into 0 fragments, 0 failed
          0 no route Mcast:
  0 received, 0 sent

ICMP statistics:
  Rcvd: 0 total, 0 format errors, 0 checksum errors
          0 unreachable, 0 packet too big
          0 time exceeded, 0 parameter problem
          0 echos, 0 echo replies
          0 membership query, 0 membership reinterface, 0 membership reduction
          0 router solicitations, 0 router advertisements
          0 neighbor solicitations, 0 neighbor advertisements, 0 redirect
  Sent: 0 total, 0 bandwidth limit
          0 unreachable, 0 packet too big
          0 time exceeded, 0 parameter problem
          0 echos, 0 echo replies
          0 membership query, 0 membership reinterface, 0 membership reduction
          0 router solicitations, 0 router advertisements
          0 neighbor solicitations, 0 neighbor advertisements, 0 redirect
```

Related Commands

show ipv6 traffic

2.1.2 debug ipv6 packet

To show debug messages for IPv6 packets, use the debug ipv6 packet command in privileged EXEC mode. To disable debug messages for IPv6 packets, use the no form of this command.

debug ipv6 packet [*interface-type interface-number* **| access-list** [access-list-namae] **]**

no debug ipv6 packet

Parameters

Parameters	Description
Interface-type	(optional) interface type
Interface-number	ID of an interface (optional)
access-list-name	Name of ACL (optional)

Command Default

The debug information is disabled in default state.

Command Mode

EXEC

Example

The following example shows how to export the IPv6 debug information:

```
Router# debug ipv6 packet
2002-1-1 05:07:16
IPv6: source FE80::A00:3EFF:FE12:3459, dest FF02::1
        plen 32, proto 58, hops 255
        sending on Ethernet1/0
```

Field	Description
source	Source address in the IPv6 packet
dest	Destination address in the IPv6 packet
plen	Load length in the IPv6 packet
proto	Protocol for the next header encapsulation, which is presented by next-header in the IPv6 packet
hops	Value of hop-limit in the IPv6 packet
Sending (receving, forwarding) on Ethernet	Shows packet transmission, reception and forwarding on an interface

Related Commands

None

2.1.3 ipv6 route-cache

To enable cache of ipv6, run **ipv6 route-cache**. To return to the default value, use the no form of the command.

ipv6 route-cache

no ipv6 route-cache

Parameters

None

Command Default

The command is disabled by default.

Command Mode

Global configuration

Example

None

2.1.4 ipv6 fast-switch

To enable v6 fast switching, run **ipv6 fast-switch**. The command is better to be used with **ipv6 route-cache**. Most applications exceptv6 acl are not available. To resume the default, run no ipv6 fast-switch.

ipv6 fast-switch

no ipv6 fast-switch

Parameters

None

Command Default

The command is disabled by default.

Command Mode

Global configuration

Example

None

2.1.5 ipv6 fast-tunnel

To enable v6 gre, enable ipv6 fast-tunnel. Meanwhile, enable ip **fast-switch** and **ipv6 fast-switch**. The command is better to be used with **ipv6 route-cache**. To return to the default value, use the no form of the command.

ipv6 fast-tunnel

no ipv6 fast-tunnel

Parameters

None

Command Default

The command is disabled by default.

Command Mode

Global configuration

Example

None

2.1.6 ipv6 cur-hoplimit

To configure the maximum hop-limit value in the RA (router advertisements) packet and the hop-limit value which is applied in the IPv6 header of packet transmission, run the first one of the following two commands: To return to the default value, use the no form of the command.

ipv6 cur-hoplimit *values*

no ipv6 cur-hoplimit *values*

Parameters

Parameters	Description
values	The maximum value of hop-limit (1-255).

Command Default

The default hop-limit is 64.

Command Mode

Interface configuration

Example

The following example shows how to set the maximum hop-limit value in the RA packet and the hop-limit value which is applied in the IPv6 header of all transmitted packets.

Router_config_f0/1# ipv6 cur-hoplimit 16

2.1.7 ipv6 general-prefix

To define a general IPv6 prefix, run the first one of the following two commands. To delete general prefix, use the no form of the command.

ipv6 general-prefix *prefix-name ipv6-prefix/prefix-length*

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

Parameters

Parameters	Description
Prefix-name	The name assigned to the prefix.
Ipv6-prefix	The IPv6 network assigned to the general prefix. This argument must be in the form documented in RFC 2373.
/Prefix-length	The length of ipv6 prefix. It is a decimal value behind the symbol "/", meaning the successive bits in the network part in an address.

Command Default

No general prefix is defined.

Command Mode

Global configuration

Example

The following example shows how to set a general IPv6 prefix:

Router_config# ipv6 general-prefix my-prefix 2001:DB8:2222::/48

2.1.8 ipv6 icmp-ratelimit

To set the minimum interval of ICMPv6 error packet transmission, run the first one of the following two commands. To return to the default value, use the no form of the command.

ipv6 icmp-ratelimit *us*

no ipv6 icmp-ratelimit

Parameters

Parameters	Description
us	The minimum interval (unit: milisecond).

Command Default

1000ms

Command Mode

Global configuration

Usage Guidelines

This command can be used to set the transmission frequency of ICMPv6 error packets.

Example

```
Router_config# ipv6 icmp6-ratelimit 2000
```

2.1.9 ipv6 mtu

To set the MTU of the interface, run the first one of the following two commands. To return to the default value, use the no form of the command.

ipv6 mtu *bytes* **no**

ipv6 mtu *bytes*

Parameters

Parameters	Description
bytes	MTU (unit: byte)

Command Default

The default value depends on the interface type, but the minimum value of any interface is 1280 bytes.

Command Mode

Interface configuration

Usage Guidelines

When MTU is the default value, RA has the MTU option.

When a router forwards packet, a packet will not be fragmented just because the MTU of the egress is smaller than the packet's length. But it will be fragmented only when the transmitted packet is generated.

Example

The following example shows how to set the MTU of an interface:

```
Router_config_f0/1# ipv6 mtu 2000
```

Related Commands

show ipv6 interface

2.1.10 ipv6 redirects

To control whether to transmit a redirection packet after the packet is forwarded, run ipv6 redirects. To disable redirection packets, enable “no ipv6 redirects”.

ipv6 redirects

no ipv6 redirects

Parameters

None

Command Default

The redirection packet will be transmitted by default.

Command Mode

Interface configuration

Usage Guidelines

The redirection packets are transmitted through the ICMPv6 protocol. As the limit of ipv6 icmp-ratelimit, redirection packet is not likely to be forwarded.

Example

The following example shows how to disable an interface to transmit the redirection packet.

```
Router_config_f0/1# no ipv6 redirects
```

To observe whether the interface will forward redirection packets, run **show ipv6 interface**.

Related Commands

ipv6 icmp-ratelimit

show ipv6 interface

2.1.11 ipv6 source-route

To enable a router to process the packets with type0 source route (route header), run **ipv6 source-route**. To disable the feature, use the no form of the command.

ipv6 source-route

no ipv6 source-route

Parameters

None

Command Default

The type 0 source route is handled in default settings.

Command Mode

Global configuration

Usage Guidelines

If you want to forbid a router to handle the source routes of type 0, you can use the no ipv6 source-route command. After the running of this command, the router will drop this kind of packets if they are received, and send an ICMPv6 unreachable packet.

As the limit of ipv6 icmp-ratelimit, ICMPv6 error packet is not likely to be forwarded.

Example

The following command disables handling of type-0 source route

```
Router_config# no ipv6 source-route
```

Related Commands

ipv6 icmp-ratelimit

2.1.12 ipv6 traffic-filter

To filter the packet an interface forwards and receives, run **ipv6 traffic-filter**. To disable the function, run no ipv6 traffic-filter.

ipv6 traffic-filter *access-list-name* **{ in | out }**

no ipv6 traffic-filter { in | out }

Parameters

Parameters	Description
access-list-name	*access list name*
In	*filtration direction, receiving packet*
Out	*filtration direction, forwarding packet*

Command Default

Filtration function is not configured by default.

Command Mode

Interface configuration

Usage Guidelines

Example

The following command is to use access list router to filter received packet on interface f0/1

```
Router_config_f0/1# ipv6 traffic-filter router in
```

Related Commands

Ipv6 access-list

Show ipv6 interface

2.1.13 ipv6 unreachables

To enable the generation of Internet Control Message Protocol for IPv6 (ICMPv6) unreachable messages for any packets arriving on a specified interface, use the ipv6 unreachables command in interface configuration mode. To prevent the generation of unreachable messages, use the no form of this command.

ipv6 unreachables

no ipv6 unreachables

Parameters

None

Command Default

ICMPv6 unreachable messages can be generated for any packets arriving on that interface.

Command Mode

Interface configuration

Usage Guidelines

The unreachable packets are transmitted through the ICMPv6 protocol. As the limit of ipv6 icmp-ratelimit, redirection packet is not likely to be forwarded.

Example

The following example shows how to shut down an interface to transmit the redirection packet.

```
Router_config_f0/1# no ipv6 unreachables
```

To observe whether the interface will forward destination unreachable packets, run **show ipv6 interface**.

Related Commands

None

2.1.14 show ipv6 general-prefix

To show details of general-prefix, run the following command:

show ipv6 general-prefix

Parameters

None

Command Mode

EXEC

Example

```
Router_config#show ipv6 general-prefix
IPv6 Prefix my-prefix, acquired via
manual 2002::/64
  Fastethernet0/0 (Address command)
```

Field	Remarks
IPv6 Prefix	User-defined IPv6 general prefix
Acquire via	Configuration mode of general-prefix Manual configuration and DHCP automatic acquisition are supported now.
Fastethernet0/0 (Address command)	Enable interface list of general prefix.

Related Commands

ipv6 general-prefix

2.1.15 show ipv6 pmtu

IPv6 router supports path MTU (Refer to RFC 1981). To show MTU buffer item, run **show ipv6 pmtu**.

show ipv6 pmtu

Parameters

None

Command Mode

EXEC

Example

```
Router_config#show ipv6 pmtu
PMTU   Expired     Destination Address
00:04:00   2002:1::1
00:01:00   2001:2::2
```

Path MTU buffer saves the destination address used by path MTU. The forwarding packet will be fragmented if the forwarded packet of all routers greater than path MTU.

A record of path MTU will be created when the router receives ICMPv6 "too-big" packet.

Field	Remarks
MTU	Path MTU value MTU included in ICMPv6 "too-big" packet
Expired	Timeout: Timer from receiving ICMPv6 "too-big" packet. Delete the record when expired is 0.
Destination Address	Destination address: Address included in ICMPv6 "too-big" packet

Related Commands

ipv6 mtu

2.1.16 show ipv6 traffic

To show statistics about IPv6 traffic, use the show ipv6 traffic command in privileged EXEC mode.

show ipv6 traffic

Parameters

None

Command Mode

EXEC

Example

```
Router#show ipv6 traffic
IPv6 statistics:
  Rcvd: 0 total, 0 local destination
         0 badhdrs, 0 badvers
         0 tooshort, 0 toosmall, 0 toomanyhdrs
         0 source-routed, 0 badscope
```

```
           0 badopts, 0 unknowopts, 0 exthdrtoolong
           0 fragments, 0 total reassembled
           0 reassembly timeouts, 0 reassembly failures
   Sent: 25 generated, 0 forwarded, 0 cant forwarded
           0 fragmented into 0 fragments, 0 failed
           0 no route
   Mcast: 0 received, 25 sent

 ICMP statistics:
   Rcvd: 25 total, 0 format errors, 0 checksum errors
           0 unreachable, 0 packet too big
           0 time exceeded, 0 parameter problem
           0 echos, 0 echo replies
           0 membership query, 0 membership reinterface, 0 membership reduction
           0 router solicitations, 0 router advertisements
           0 neighbor solicitations, 0 neighbor advertisements, 0
   redirect Sent: 0 total, 0 bandwidth limit
           0 unreachable, 0 packet too big
           0 time exceeded, 0 parameter problem
           0 echos, 0 echo replies
           0 membership query, 0 membership reinterface, 0 membership reduction
           0 router solicitations, 0 router advertisements
           0 neighbor solicitations, 0 neighbor advertisements, 0 redirect
```

Related Commands

clear ipv6 traffic

Chapter 3 IPv6 ACL Configuration Commands

This chapter gives a description of commands and relative configuration methods for configuring IPv6 access control list. These commands consist of three parts: Deny, Permit and Sequence.

3.1 IPv6 ACL Configuration Commands

3.1.1 ipv6 access-list

To configure the name of the access control list, run the first one of the two following commands. To cancel the access control list, use the no form of the command.

ipv6 access-list *access-list-name*

no ipv6 access-list *access-list-name*

Parameters

Parameters	Description
access-list-name	The name of the access control list

Command Default

There is no default access control list and the name of an access control list must be configured.

Command Mode

No default ACL (The ACL name must be configured.)

Usage Guidelines

1. IPv6 stops adopting number access list and number access list will be treated as name access list. The access lists of IPv4 and IPv6 should not adopt the same name, or the interface cannot be identified.
2. IPv6 ACL default configuration allows ND packet of ICMPv6 (equivals with ARP of IPv4), but forbids other IPv6 packets. Put it in another way, add “permit any any” to the last of deny configuration rules. Configuration rules are as follows:

```
permit icmpv6 any any nd-na
permit icmpv6 any any nd-ns
deny ipv6 any any
```

Example

The following example shows how to create a IPv6 access control list: to deny the destination address with prefix FEC0:0:0:2::/64 being any value, but permit any other packet. The command is used on Ethernet interface 0.

```
ipv6 access-list list2
```

```
        deny FEC0:0:0:2::/64 any
        permit ipv6 any any

interface ethernet 0
        ipv6 traffic-filter list2 out
```

Related Commands

deny (IPv6)

permit (IPv6)

ipv6 traffic-filter

show ipv6 access-list

3.1.2 ipv6 traffic-filter

The command allows the access control list with certain names be applied to certain interfaces. To cancel the function, use the no form of the command.

ipv6 traffic-filter *access-list-name* {**in | out**}

no ipv6 traffic-filter *access-list-name*

Parameters

Parameters	Description
access-list-name	The name of access list in **ipv6 access-list** ***access-list-name****.*
In	Filters the incoming packets.
Out	Filters the outgoing packets.

Command Default

The filtration function is not set by default. The command is effective when the access list name is applied to a designated interface.

Command Mode

Interface configuration

Usage Guidelines

Ipv6 traffic-filter applies only IPv6 ACL rules to certain interfaces. Other applications need to use access list filtration should be realized with other functions.

Ipv6 traffic-filter is to filter the packet forwarded by the router, not the packet generated by the router itself.

Example

The following example is to apply access list rule to the packet rule of the ongoing interface.

```
Router_config# interface ethernet 0/0
```

```
Router_config_e0/0# ipv6 traffic-filter router in
```

Related Commands

Ipv6 access-list

show ipv6 access-list

3.1.3 deny/permit

To deny the packet, run following commands. To cancel the ACL, use the no form of the command.

deny *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*interface-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*interface-number*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**sequence** *value*] [**time-range** *name*] [**undetermined-transinterface**]

no deny *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*interface-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*interface-number*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**sequence** *value*] [**time-range** *name*] [**undetermined-transinterface**]

deny icmpv6 {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*interface-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address*} [*icmpv6-type* [*icmpv6-code*] | *icmpv6-message*] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**sequence** *value*] [**time-range** *name*]

deny tcp {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*interface-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*interface-number*]] [**ack**] [**dscp** *value*] [**established**] [**fin**] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**neq** {*interface* | *protocol*}] [**psh**] [**range** {*interface* | *protocol*}] [**routing**] [**rst**] [**sequence** *value*] [**syn**] [**time-range** *name*] [**urg**]

deny udp {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*interface-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*interface-number*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**neq** {*interface* | *protocol*}] [**range** {*interface* | *protocol*}] [**routing**] [**sequence** *value*] [**time-range** *name*]

To deny the packet, run following commands: To cancel the ACL, use the no form of the command.

permit *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*interface-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address*} [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**sequence** *value*] [**time-range** *name*] [**undetermined-transinterface**]

no permit *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*interface-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address*} [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**sequence** *value*] [**time-range** *name*] [**undetermined-transinterface**]

permit icmpv6 {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*interface-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address*} [*icmpv6-type* [*icmpv6-code*] | *icmpv6-message*] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**sequence** *value*] [**time-range** *name*]

permit tcp {*source-ipv6-prefix***/***prefix-length* **| any | host** *source-ipv6-address*} [*operator* [*interface-number*]] {*destination-ipv6-prefix***/***prefix-length* **| any | host** *destination-ipv6-address*} [*operator* [*interface-number*]] [**ack**] [**dscp** *value*] [**established**] [**fin**] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**neq** {*interface* **|** *protocol*}] [**psh**] [**range** {*interface* **|** *protocol*}] [**routing**] [**rst**] [**sequence** *value*] [**syn**] [**time-range** *name*] [**urg**]

permit udp {*source-ipv6-prefix***/***prefix-length* **| any | host** *source-ipv6-address*} [*operator* [*interface-number*]] {*destination-ipv6-prefix***/***prefix-length* **| any | host** *destination-ipv6-address*} [*operator* [*interface-number*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**neq** {*interface* **|** *protocol*}] [**range** {*interface* **|** *protocol*}] [**routing**] [**sequence** *value*] [**time-range** *name*]

Parameters

Parameters	Description
protocol	Network protocol name or number Supported protocol names now are ahp(51), esp(50), icmpv6(58), ipv6(41), pcp(108), sctp(132), tcp(6) and udp(17).
*source-ipv6-prefix***/***prefix length*	*source-ipv6-prefix***/***prefix length*
any	Abbreviation of IPv6 prefix::/0.
host *source-ipv6-address*	Source IPv6 host address
operator [*interface-number*]	(optional) Comparative operator and interface number, which are only efficient for tcp protocol and udp protocol. *operator* includes **lt** (less than), **gt** (greater than), **eq**(equal), **neq**(not equal) and **range**(inclusive range). The operator of range is with two interface numbers, while other operators with only one. The range of *interface-number*: 0-65535.
*destination-ipv6-prefix***/***prefix-length*	ipv6-prefix/prefix length
host *destination-ipv6-address*	Destination IPv6 host address
dscp *value*	(optional)(dscp, differentiated services code point). It is used for matching IPv6 packet header Traffic Class Domain, 0-63. Defined traffic class domains: af11(001010), af12(001100), af13(001110), af21(010010), af22(010100), af23(010110), af31(011010), af32(011100), af33(011110), af41(100010), af42(100100), af43(100110), cs1(001000), cs2(010000), cs3(011000), cs4(100000), cs5(101000), cs6(110000), cs7(111000), ef(101110), default(000000)
flow-label *value*	(optional) IPv6packet flow-label, 1-1048575(1024*1024-1).
fragments	When the fragmented extension header includes offset of non-0, uninitialized fragments will be matched. **fragments** are optional, only when *operator* [*interface-number*] is not claimed.
log	(optional) Forward log information to console interface, when fragments are matching. Log information includes access list name, serial number and fragments (deny/permit), protocol/protocol number (TCP, UDP, ICMPv6, etc.), source address/destination address, source interface number/destination interface number.

log-input	(optional) Log-input is the same with log in function. Besides, it includes packet ongoing interface.
routing	(optional) Matches routing extension header of IPv6 fragment of source route.
sequence *value*	(optional) Sets the sequence number of access list: 1-4294967295 (65536*65536-1). IPv4 access list can only add the rule to the last, while IPv6 can add the rule to any position by way of sequence. The new added rule will overlay the already existed rule in the position.
time-range *name*	(optional) Sets the time range of access list. In time-range command, apply time-range name to the access list by way of **absolute/periodic** key words.
undetermined-transinterface	(optional) It is used for matching the fragment of layer-4 protocol cannot identify. **undetermined-transinterface** is optional only when *protocol* is not claimed. If *protocol* is ipv6, layer-4 protocol of IPv6 is not claimed.
icmpv6-type	(optional) ICMPv6 packet type, 0-255.
icmpv6-code	(optional) ICMPv6 packet code, 0-255.
icmpv6-message	(optional) by ICMPv6 packet name (ICMP packet type composed of RFC prescribed packet name and packet code, for instance, unreachable destination), 0-255.
ack	(optional) Sets TCP packet and acknowledgment (ACK) matching.
fin	(optional) Sets TCP packet and finish (FIN) matching.
psh	(optional) Sets TCP packet and push (PSH) matching.
rst	(optional) Sets TCP packet and push (PSH) matching.
syn	(optional) Sets TCP packet and synchronize (SYN) matching.
urg	(optional) Sets TCP packet and urgent (URG) matching.
established	(optional) Sets TCP packet matching (established) when ACK or RST position of TCP packet is set. When the parameter is set to be deny, it denies connection from external networks to internal networks, but allows connection from internal network to external network.
eq{*interface* | *protocol*}	(optional) It only matches fragment of designated interface number. Protocol is specified protocol name.
gt{*interface* | *protocol*}	(optional) It only matches fragment larger than designated interface number. Protocol is specified protocol name.
lt {*interface* | *protocol*}	(optional) It only matches fragment smaller than designated interface number. Protocol is specified protocol name.
neq {*interface* | *protocol*}	(optional) It only matches fragment not in the designated interface number. Protocol is specified protocol name.
range {*interface* | *protocol*}	(optional) It only matches fragment of designated interface number ranges. Protocol is specified protocol name.

Command Default

1. sequence number

Different with IPv4 ACL, IPv6 ACL can be added to any position with **permit**, **deny**, **sequence**, not only limit to the end of ACL. Therefore, the access list should be numbered. If the user does not manually configure the sequence number of the access list, the default first ACL sequence number is 10 and the latter access list sequence number increases 10 than the former in turn; if the user designated sequence number is the same with the current ACL's, the current ACL will be overlaid; the sequence number of the last access list may not be an integer multiple of 10 when the user designates the sequence number, the sequence number of the new added ACL will be 10+ the sequence number of the last access list.

2. Default rules:

Similar to IPv4 ACL, the access list will not forbid any rule when only configuring the name of ACL but not the rule:

permit icmpv6 any any nd-na

permit icmpv6 any any nd-ns

permit ipv6 any any

Note: As what ICMP for IPv6 is what ARP to IPv4, neighbor inform packet and neighbor request packet of the neighbor discovery are allowed to forward by default. If only one rule configured in IPv6 ACL rule, packets don't satisfy the rule indicate that ICMPv6 packets are allowed, but all IPv6 packets are forbidden.

permit icmp any any nd-na

permit icmp any any nd-ns

deny ipv6 any any

Therefore, to allow packets don't satisfy the rule to forward, run **permit ipv6 any any** to the end of IPv6 ACL.

Command Mode

IPv6 ACL configuration

Usage Guidelines

1. Packet names of ICMPv6 are as follows:

- beyond-scope
- destination-unreachable
- echo-reply
- echo-request
- header
- hop-limit
- mld-query
- mld-reduction
- mld-reinterface
- nd-na
- nd-ns
- next-header

- no-admin
- no-route
- packet-too-big
- parameter-option
- parameter-problem
- interface-unreachable
- reassembly-timeout
- renum-command
- renum-result
- renum-seq-number
- router-advertisement
- router-renumbering
- router-solicitation
- time-exceeded
- unreachable

2. Defined protocols of TCP interface numbers:

- bgp(179)
- chargen(19)
- cmd(514)
- daytime(13)
- discard(9)
- domain(53)
- echo(7)
- exec(512)
- finger(79)
- ftp(21)
- ftp-data (20)
- gopher (70)
- hostname (101)
- ident (113)
- irc (194)
- klogin (543)
- kshell (544)
- login (513)
- lpd (515)
- nntp (119)
- pim-auto-rp (496)
- pop2 (109)

- pop3 (110)
- smtp (25)
- sunrpc (111)
- syslog (514)
- talk (517)
- time (37)
- uucp (540)
- whois (43)
- www (80)

3. Defined protocols of UDP interface numbers:

- biff (512)
- bootpc (68)
- bootps (67)
- discard (9)
- dnsix (195)
- domain(53)
- echo(7)
- isakmp (500)
- netbios-dgm (138)
- netbios-ns (137)
- netbios-ss (139)
- ntp (123)
- pim-auto-rp (496)
- rip (520)
- snmp (512)
- snmptrap (162)
- sunrpc (111)
- syslog (514)
- talk (517)
- tftp (69)
- time (37)
- who (513)
- xdmcp (177)

Example

The following example shows how to create an IPv6 access list “ROUTER” and set 4 rules.

The frist rule denies tcp connected packets whose destination numbers are larger than 5000;

The second rule denies udp packets whose destination numbers are smaller than 5000 and forward log to console interface when the rule is matching;

The third rule allows all icmpv6 packets;

The fourth rule allows all packets do not conform to the rule.

Note: Add the fourth rule if the user hopes all packets which do not conform to the rule are allowed.

Lastly, apply the rule to the egress of Ethernet interface 0 of the router in interface configuration mode.

```
ipv6 access-list ROUTER deny
     tcp any any gt 5000
     deny udp ::/0 lt 5000 ::/0 log
     permit icmpv6 any any
     permit any any

interface ethernet 0
     ipv6 traffic-filter ROUTER out
```

Related Commands

Ipv6 access-list ipv6

traffic-filter show

ipv6 access-list clear

ipv6 access-list

3.1.4 sequence

Sequence allows an access list is added to any position of the existed access lists. (In IPv4, an access list can only add to the end of the existed access lists.) To delete the set rules, run the no form of the commands:

sequence *value* {**deny | permit**} *protocol* {*source-ipv6-prefix/prefix-length* **| any | host** *source-ipv6-address*} [*operator* [*interface-number*]] {*destination-ipv6-prefix/prefix-length* **| any | host** *destination-ipv6-address*} [*operator* [*interface-number*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**time-range** *name*] [**undetermined-transinterface**]

no sequence *value* {**deny | permit**} *protocol* {*source-ipv6-prefix/prefix-length* **| any | host** *source-ipv6-address*} [*operator* [*interface-number*]] {*destination-ipv6-prefix/ prefix-length* **| any | host** *destination-ipv6-address*} [*operator* [*interface-number*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**time-range** *name*] [**undetermined-transinterface**]

sequence {**deny | permit**} **icmpv6** {*source-ipv6-prefix/prefix-length* **| any | host** *source-ipv6-address*} [*operator* [*interface-number*]] {*destination-ipv6-prefix/prefix-length* **| any | host** *destination-ipv6-address*} [*icmpv6-type* [*icmpv6-code*] **|** *icmpv6-message*] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**time-range** *name*]

sequence {**deny | permit**} **tcp** {*source-ipv6-prefix/prefix-length* **| any | host** *source-ipv6-address*} [*operator* [*interface-number*]] {*destination-ipv6-prefix/prefix-length* **| any | host** *destination-ipv6-address*} [*operator* [*interface-number*]] [**ack**] [**dscp** *value*] [**established**] [**fin**] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**neq** {*interface* **|**

protocol}] [**psh**] [**range** {*interface* **|** *protocol*}] [**routing**] [**rst**] [**syn**] [**time-range** *name*] [**urg**]

sequence {**deny | permit**} **udp** {*source-ipv6-prefix***/***prefix-length* **| any | host** *source-ipv6-address*} [*operator* [*interface-number*]] {*destination-ipv6-prefix***/***prefix-length* **| any | host** *destination-ipv6-address*} [*operator* [*interface-number*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**neq** {*interface* **|** *protocol*}] [**range** {*interface* **|** *protocol*}] [**routing**] [**time-range** *name*]

Parameters

The explanation of the parameter is the same with deny/permit in section 3.1.3, but put the sequence command keywords in the front.

Command Default

It is the same with the default rule of deny/permit in section 3.1.3.

Command Mode

IPv6 access list configuration commands

Usage Guidelines

It is the same with the instruction of deny/permit in section 3.1.3.

Example

The following example is the same with the configuration in section 3.1.3, but the sequence number is added to the front of each rule.

```
ipv6 access-list ROUTER
    sequence 30 deny tcp any any gt 5000
    sequence 70 deny udp ::/0 lt 5000 ::/0 log
    sequence 75 permit icmpv6 any any
    sequence 76 permit any any
```

Add a new rule to the existed rules:

```
    deny ipv6 FE80::/64 any range 80 110 log-input
```

The rule will be added to the end of the access list and the sequence will be automatically numbered as 76+10=86. As the rule does not designate the sequence clearly, the sequence will not show when run **show running**. If the user has designated the sequence in adding the new rule, as the following command:

```
    sequence 50 deny ahp any any
    or deny ahp any any sequence 50
```

The rule will be inserted in the middle of sequence 30 and sequence 70. If the user designates the sequence is the same with the original sequence, as the following command:

```
    sequence 75 deny esp any any log
    or deny esp any any log sequence 75
```

The rule of sequence 75 in the original access list will be overlaid. The following is changes to the access list with 3 new added rules:

```
ipv6 access-list ROUTER
    sequence 30 deny tcp any any gt 5000
    sequence 50 deny ahp any any
    sequence 70 deny udp ::/0 lt 5000 ::/0 log
    sequence 75 deny esp any any log
    sequence 76 permit any any
    deny ipv6 FE80::/64 any range 80 110 log-input
```

deny(IPv6)

permit(IPv6)

Ipv6 access-list

ipv6 traffic-filter

show ipv6 access-list

clear ipv6 access-list

3.1.5 show ipv6 access-list

To clear IPv6 access list counters, use the clear access-list ipv6 command.

show ipv6 access-list [*access-list-name*]

Parameters

Parameters	Description
access-list-name	access list name

Command Default

All access lists will be showed if no access list name is entered.

Command Mode

Global configuration or EXE

Usage Guidelines

Show the format of IPv6 access list with command “show ipv6 access-list” is different with show the format of IPv6 ACL with command “show running”. With command “show running”, the rule with designated sequence will show its sequence in the beginning, while the rule without designated sequence will not show its sequence. See the example in section 1.1.4. With command "show ipv6 access-list", the sequence will show in the end of the rule whether the sequence is designated when entering the rule. See the example in this section.

Example

To show ROUTER1 and ROUTER2, run **show ipv6 access-list**.

```
ipv6 access-list ROUTER1
```

```
    permit ipv6 any any sequence 10
    deny icmpv6 any any 255 255 routing sequence
    20 permit any any sequence 30

ipv6 access-list ROUTER2
    permit icmpv6 12::/0 host 34:: header dscp ef fragments sequence 20
    permit icmpv6 any any header flow-label 987 sequence 30
    deny ahp any any routing log time-range ROUTER_TIMER sequence 50
    deny icmpv6 any any 255 255 sequence 8918
    permit any any sequence 8928
```

To show ROUTER1, run **show ipv6 access-list ROUTER1.**

```
ipv6 access-list ROUTER1
    permit ipv6 any any sequence 10
    deny icmpv6 any any 255 255 routing sequence
    20 permit any any sequence 30
```

Related Commands

clear ipv6 access-list

3.1.6 clear ipv6 access-list

The command shows how to clear ipv6 access lists.

clear ipv6 access-list [*access-list-name*]

Parameters

Parameters	Description
access-list-name	access list name

Command Default

All access lists will be cleared if no access list name is entered.

Command Mode

Global configuration and EXE

Usage Guidelines

If an access list name is entered, its corresponding rule will be cleared; if no access list is entered, all access list rules will be cleared.

Example

The following command is to clear all rules of the access list named marketing.

```
Router# clear ipv6 access-list marketing
```

Related Commands

Ipv6 access-list

show ipv6 access-list

Chapter 4 IPv6IP tunnel Configuration Commands

4.1 Tunnel Interface Configuration Commands

4.1.1 Interface tunnel

To configure tunnel interface, run **interface tunnel**; to return to the default value, use the no form of the command.

Interface tunnel *number*

no Interface tunnel *number*

Parameters

Parameters	Description
Number	Tunnel interface number, range: 0-32767.

Command Default

No tunnel interface

Command Mode

Global configuration

Usage Guidelines

The command shows how to add a tunnel interface and enter the interface configuration mode.

Example

Configure a tunnel interface:
Interface tunnel 1

Related Commands

show interface

4.1.2 Tunnel mode ipv6ip

To configure IPv6 in IP tunnel interface and designate tunnel working protocol mode, run **tunnel mode ipv6ip**.

Tunnel mode ipv6ip [isatap|6to4]

Parameters

Parameters	Description
isatap	The mode of IPv6 in IP tunnel is ISATAP

6to4	The mode of IPv6 in IP tunnel is 6T04.

Command Default

The default of **ipv6ip tunnel** interface is manually configuration mode.

Command Mode

Tunnel Interface configuration

Usage Guidelines

The command **tunnel mode ipv6ip** shows how to configure the interface to be IPv6 in IP tunnel interface. If there is no other key word, the command is in manual configuration mode; if there are keywords **isatap** or **6to4**, the command is in **isatap** or **6to4** mode. To configure the tunnel interface as IPv4 interface, run **no tunnel mode**.

Example

Configure one tunnel interface as IPv6 in IP tunnel interface of the manual mode:

```
tunnel mode ipv6ip
```

Configure one tunnel interface as IPv6 in IP tunnel interface of the ISATAP mode:

```
tunnel mode ipv6ip isatap
```

Configure one tunnel interface as IPv6 in IP tunnel interface of the 6TO4 mode:

```
tunnel mode ipv6ip 6to4
```

Related Commands

Tunnel source

Tunnel destination

4.1.3 Tunnel source

To configure the source address of IPv6 in IP tunnel interface, run **tunnel source**.

Tunnel source *ipv4-addr*

Parameters

Parameters	Description
Ipv6-addr	Source ipv4 address of IPv6 in IP tunnel interface.

Command Default

There is no source address by default.

Command Mode

Tunnel Interface configuration

Usage Guidelines

To configure the source address of IPv6 in IP tunnel interface, run **tunnel source**. The source address of 6to4 ipv6tunel cannot configure private addresses such as 10.X.X.X, 172.16.X.X, 192.168.X.X.

Example

To configure the source address of IPv6 in IP tunnel
interface: run tunnel source 1.1.1.1.

Related Commands

Tunnel mode ipv6

Tunnel destination

4.1.4 Tunnel destination

To configure the destination address of IPv6 in IP tunnel interface, run **tunnel source**.

Tunnel destination *ipv4-addr*

Parameters

Parameters	Description
Ipv6-addr	Destination ipv4 address of IPv6 in IP tunnel interface.

Command Default

There is no destination address by default.

Command Mode

Tunnel Interface configuration

Usage Guidelines

To configure the destination address of IPv6 in IP tunnel interface, run **tunnel source**.

Example

To configure the destination address of IPv6 in IP tunnel
interface: run **tunnel destination 1.1.1.2.**

Related Commands

Tunnel mode ipv6

Tunnel source

4.2 IPv6 IP Debug Configuration Commands

4.2.1 Debug ipv6ip

To show the debug information of IPv6 in IP, run **debug ipv6ip**. To disable this feature, use the no form of this command.

Debug ipv6ip [isatap|6to4]

Parameters

Parameters	Description
isatap	Shows the debug information of ISATAP tunnel.
6to4	Shows the debug information of 6to4 tunnel.

Command Default

The debug information is not shown.

Command Mode

EXEC

Usage Guidelines

To show the debug information of IPv6 in IP, run **debug ipv6ip**. Show manually configured debug information of IPv6 in IP tunnel, if there is no other key word; show the debug information of isatap tunnel or 6to4 tunnel, if there is keyword isatap or 6to4.

Example

Show the debug information of isatap tunnel.

```
debug ipv6ip isatap
```

Show the debug information of 6to4 tunnel.

```
debug ipv6ip 6to4
```

Show the manually configured debug information of IPv6 in IP tunnel:

```
debug ipv6ip
```

Related Commands

Tunnel mode ipv6

Chapter 5 DHCPv6 Configuration Commands

5.1 DHCPv6 Client Configuration Commands

5.1.1 ipv6 dhcp client pd

To enable prefix agent request by Dynamic Host Configuration Protocol for IPv6（DHCPv6）protocol, run ipv6 dhcp pd. To disable this feature, use the no form of the command.

Ipv6 dhcp pd *prefix_name* [rapid-commit]

no ipv6 dhcp pd *prefix_name*

Parameters

Parameters	Description
prefix_name	The prefix name after acquiring the prefix.
rapid-commit	The fast finish prefix agent (by one interaction is enough)

Command Default

The interface disable DHCPv6 prefix agent request.

Command Mode

Interface configuration mode

Usage Guidelines

Ipv6 dhcp client pd prefix_name shows how to enable router acquire agent prefix by DHCPv6 protocol and save the prefix_name in the general prefix pool. Once the prefix is acquired, the prefix in the general prefix pool can be quoted by other commands (For instance, ipv6 address command).

rapid-commit key words enable the router to finish the prefix agent process by one interaction (two information). If rapid-commit is configured, the client will have rapid commit included in SOLICIT.

client, relay, server of DHCPv6 are mutually exclusive, which means one interface can only configure one mode.

Example

To finish prefix agent handling process, run **Ipv6 dhcp client pd** dhcp_prefix. The acquired name ofdhcp_prefix is saved in the router general-prefix table.

To finish prefix agent handling process through DHCPv6 one time, run **Ipv6 dhcp client pd dhcp_prefix**. The acquired name of **dhcp_prefix** is saved in the router **general-prefix** table.

Related Commands

show ipv6 general-prefix

show ipv6 dhcp interface

5.1.2 ipv6 dhcp client pd hint

In prefix agent, the client can inform the server to acquire the prefix it hopes. To configure the prefix the client hopes to acquire, run **ipv6 dhcp client pd hint**. To delete the prefix, use the no form of the command.

ip address pd hint *prefix*

no ip address pd hint *prefix*

Parameters

Parameters	Description
prefix	The prefix of IPv6.

Command Default

The expected prefix is not configured.

Command Mode

Interface configuration

Usage Guidelines

To configure the prefix the client hopes to acquire, run **ipv6 dhcp client pd hint**. To acquire more than one prefix, configure the command repeatedly.

Following functions of DHCPv6 including client, relay and server are mutually exclusive, which means one interface can only configure one mode.

Example

To acquire the client expected prefix, run following command:

Ipv6 dhcp client pd hint 1:1:1:1::/64

Related Commands

show ipv6 dhcp interface

5.2 DHCPv6 Relay Configuration Commands

5.2.1 ipv6 dhcp relay destination

To specify a destination address to which client packets are forwarded and enable DHCPv6 relay service on the interface. To delete one destination address, use the no form of the command.

ipv6 dhcp relay destination *ipv6_address* **no**

ipv6 dhcp relay destination *ipv6_address*

Parameters

Parameters	Description

ipv6_address	Destination IPv6 address of Relay

Command Default

DHCPv6 relay service is not enabled and destination IPv6 address of Relay is not configured.

Command Mode

Interface configuration

Usage Guidelines

To configure the destination address of relay, run **ipv6 dhcp relay destination**. It can be other address of relay agent and address of the server.

To configure multiple destination addresses, run the command repeatedly.

Following functions of client, relay and server are mutually exclusive, which means one interface can only configure one mode.

Example

To configure relay destination address 1:1:1:1::/64, use the following command: **ipv6 dhcp relay destination** 1:1:1:1::1/64

Related Commands

show ipv6 dhcp interface

5.3 DHCPv6 Server Configuration Commands

5.3.1 ipv6 dhcp server

To enable DHCPv6 server service, run **ipv6 dhcp server**; to disable this feature, use the no form of this command.

ipv6 dhcp server *poolname* [allow-hint **|** preference *num*| rapid-commit]

no ipv6 dhcp server *name*

Parameters

Parameters	Description
poolname	DHCPv6 poolname
allow-hint	Supports the priority of the client
preference *num*	Sets the priority of the server. The num parameter stands for the priority, which ranges between 0 and 255 and whose default value is 0.
rapid-commit	Supports the rapid DHCPv6 process (one interaction) which is not supported by default.

Command Default

The DHCPv6 server is disabled on the interface.

Command Mode

Interface configuration

Usage Guidelines

To enable DHCPv6 server which adopts the parameters of poolname, run **ipv6 dhcp server poolname**.

Following functions including client, relay, server of DHCPv6 are mutually exclusive, which means one interface can only configure one mode.

Example

To enable DHCPv6 server which adopts the parameters of poolname, run following command.

```
ipv6 dhcp server dhcppool
```

Related Commands

show ipv6 dhcp interface

ipv6 dhcp pool

5.3.2 ipv6 dhcp pool

To configure DHCPv6 pool and enter DHCPv6 pool configuration mode, run **ipv6 dhcp pool**; to delete DHCPv6 pool, use the no form of the command.

ipv6 dhcp pool *poolname*

no ipv6 dhcp pool *name*

Parameters

Parameters	Description
poolname	DHCPv6 poolname

Command Default

DHCPv6 pool is not configured.

Command Mode

Global configuration mode

Usage Guidelines

The command shows how to add DHCPv6 pool and how to enter DHCPv6 pool configuration mode.

To use DHCPv6 pool after configuring DHCPv6 pool, run **ipv6 dhcp server** in interface configuration mode.

Example

To configure DHCPv6 pool and enter DHCPv6 pool configuration mode, run following command:

```
ipv6 dhcp pool dhcppool
```

Related Commands

ipv6 dhcp server

show ipv6 dhcp pool

5.3.3 ipv6 local pool

To configure prefix pool, run **ipv6 local poo**. To disable this feature, use the no form of this command.

ipv6 local pool *poolname prefix***/***prefix-length assigned-length*

no ipv6 local pool poolname

Parameters

Parameters	Description
poolname	The prefix pool name
prefix	The prefix of the prefix pool
prefix-length	The length of the prefix
assigned-length	The prefix length of the user who is assigned to use the pool; the assigned-length of the prefix should not be shorter than prefix-length.

Command Default

The prefix pool is not configured.

Command Mode

Global configuration

Usage Guidelines

Names of all prefix pool must be exclusive. The prefix pool should not be overlapped.

Example

Configure prefix pool pool1:

```
ipv6 local pool pool1 1:1:1::1/48 64
```

Related Commands

prefix-delegation pool

show ipv6 local pool

5.4 DHCPv6 Pool Configuration Commands

5.4.1 Dns-server

To configure DNS IPv6 server address, run dns-server. To delete the server address, use the no form of the command.

Dns-server *ipv6_address*

no dns-server*s*

Parameters

Parameters	Description
ipv6_address	DNS Server IPv6 Address

Command Default

There is no DNS IPv6 server address by default.

Command Mode

DHCPv6 pool configuration

Usage Guidelines

To configure multiple DNS IPv6 server address, run the command repeatedly.

Example

Configure DNS IPv6 server address

```
dns-server 2001:0DB8:3000:3000::42
```

Related Commands

show ipv6 dhcp pool

domain-name

5.4.2 domain-name

To configure DNS IPv6 domain name, run **domain-name**. To delete the domain name, use the no form of the command.

Domain-name *domain*

no domain-name

Parameters

Parameters	Description
domain	DNS domain name

Command Default

There is no DNS IPv6 domain name by default.

Command Mode

DHCPv6 pool configuration

Usage Guidelines

To configure multiple DNS IPv6 domain names, run the command repeatedly.

Example

Configure DNS IPv6 domain name

```
Domain-name 2001:0DB8:3000:3000::42
```

Related Commands

ipv6 dhcp pool

dns-server

5.4.3 prefix-delegation

To bind a certain client with some prefixes, run the command manually. To delete the prefix static binding, use the no form of the command.

prefix-delegation *ipv6_prefix/prefix_length client_DUID* [**iaid** *IAID*]

no prefix-delegation *ipv6_prefix/prefix_length client_DUID* [**iaid** *IAID*]

Parameters

Parameters	Description
Prefix	Specified prefix
Prefix_length	The length of the prefix.
Client-DUID	Client DUID
IAID	Client IAID

Command Default

There is static binding after DHCPv6 is configured.

Command Mode

DHCPv6 pool configuration

Usage Guidelines

The command shows how to enable the static binding between an IPv6 prefix and a client. Any IA of the client can acquire the prefix if IAID is not configured.

Example

To specify a prefix to bind the client, run following command:

prefix-delegation 2001:0DB8::/64 00e00f262388

Related Commands

ipv6 local pool

ipv6 dhcp pool

show ipv6 dhcp pool

5.4.4 prefix-delegation pool

The command shows how to delegate the prefix name of DHCPv6 pool. To delete the prefix pool name, use the no form of the command.

prefix-delegation pool *poolname*

no prefix-delegation pool

Parameters

Parameters	Description
poolname	Specified prefix pool name

Command Default

There is no prefix pool name after configuring the DHCPv6 pool.

Command Mode

DHCPv6 pool configuration mode

Usage Guidelines

The command shows how to delegate the prefix name of DHCPv6 pool. To configure prefix pool, run **ipv6 local pool**.

Example

To delegate DHCPv6 pool, run **Prefix-delegation pool localpool**.

Prefix-delegation pool localpool

Related Commands

ipv6 local pool

ipv6 dhcp pool

show ipv6 dhcp pool

5.4.5 lifetime

The command shows how to designate lifetime of DHCPv6 pool dynamically allocating prefix. To delete the lifetime configuration, run the no form of the command.

Lifetime *valid-time preferred-time*

no lifetime

Parameters

Parameters	Description
Valid-time	Valid-Time of dynamically allocating prefix; unit: mins (1-525600).
Preferred-time	Preferred-Time of dynamically allocating prefix; unit: mins (1-525600).

Command Default

Valid-time default 43200 (30 days)

Preferred-time default 10080 (7 days)

Command Mode

DHCPv6 pool configuration

Usage Guidelines

The command shows how to specify lifetime of DHCPv6 pool dynamically allocating prefix. Preferred-time must be not greater than valid-time.

Example

To configure DHCPv6 lifetime, run following command:

Lifetime 300 240

Related Commands

Ipv6 dhcp pool

Show ipv6 dhcp pool

5.5 DHCPv6 Debug Configuration Commands

5.5.1 Debug ipv6 dhcp

To show DHCPv6 debug information, run **debug ipv6 dhcp [detail]**. To disable this feature, use the no form of the command.

debug ipv6 dhcp [detail]

no debug ipv6 dhcp [detail]

Parameters

Parameters	Description
Detail	Show more details of debug information.

Command Default

There is no debug information.

Command Mode

EXEC

Usage Guidelines

The command is used to show DHCPv6 debug information.

Example

To show DHCPv6 debug information, run following command:

Debug ipv6 dhcp

Related Commands

None

5.5.2 Debug ipv6 dhcp relay

To show DHCPv6 relay agent information, run **debug ipv6 dhcp relay**. To disable DHCPv6 relay information, run **no debug ipv6 dhcp relay**.

debug ipv6 dhcp relay

no debug ipv6 dhcp relay

Parameters

None

Command Default

There is no debug information.

Command Mode

EXEC

Usage Guidelines

The command is used to show DHCPv6 relay agent debug information.

Example

To show DHCPv6 relay agent information, run following command:

Debug ipv6 dhcp

5.6 DHCPv6 Management Configuration Commands

5.6.1 Show ipv6 dhcp

Show DUID

Show ipv6 dhcp

Parameters

None

Command Default

None

Command Mode

All modes except the user mode

Usage Guidelines

The command shows how to show DHCPv6 DUID information. DUID is created when first enable DHCPv6 service.

Example

To show DUID, run following command:

```
Show ipv6 dhcp
```

5.6.2 Show ipv6 dhcp interface

To show DHCPv6 interface information, run following command:

show ipv6 dhcp interface [*interface-type interface-number*]

Parameters

Parameters	Description
interface-type *interface-number*	The interface type and the interface ID.

Command Default

To show DHCPv6 interface information.

Command Mode

All modes except the user mode

Usage Guidelines

The command can be used to show DHCPv6 interface information, including all interface modes (client, server, relay) and the relevant configuration information of all modes.

Example

To show DHCPv6 interface information, run following command:

```
show ipv6 dhcp interface
```

To show DHCPv6 interface information, run following command:

```
show ipv6 dhcp interface FastEthernet0/0
```

Related Commands

ipv6 dhcp client pd

ipv6 dhcp relay destination

ipv6 dhcp server

5.6.3 Show ipv6 dhcp pool

To show DHCPv6 pool information and statistics:

Show ipv6 dhcp pool [poolname]

Parameters

Parameters	Description
poolname	Shows the name of DHCPv6 pool

Command Default

Information of all DHCPv6 pool is shown.

Command Mode

All modes except the user mode

Usage Guidelines

The command shows how to show the information of DHCPv6 pool, including DHCPv6 pool name, the static binding information of DHCPv6 pool, related prefix pool, DNS server of DHCPv6 pool and numbers of leased prefixes.

Example

The following example shows how to show the DHCPv6 pool statistics information.

```
show ipv6 dhcp pool
```

Related Commands

ipv6 dhcp pool

5.6.4 Show ipv6 dhcp binding

show ip dhcpd binding [prefix]

Parameters

Parameters	Description
prefix	The ipv6 prefix of the to-be-displayed binding information.

Command Default

All prefix binding information is shown.

Command Mode

All modes except the user mode

Usage Guidelines

The command shows how to show DHCPv6 binding information, type, DUID, IAID, prefix and lifetime.

Example

The following command shows how to show the DHCPv6 binding information.

Show ipv6 dhcp binding

To show DHCPv6 prefix binding information 1:1:1:1::/64,run following command:

Show ipv6 dhcp binding 1:1:1:1::/64

Related Commands

clear ipv6 dhcp bingding

5.6.5 Show ipv6 local pool

To show the information and statistics of prefix pool

Show ipv6 local pool [poolname]

Parameters

Parameters	Description
poolname	Shows the name of prefix pool

Command Default

To show the information of all prefix pools

Command Mode

All modes except the user mode

Usage Guidelines

The command can be used to show the information of the prefix pool, including prefix pool name, prefix, prefix length, allocated prefix length, numbers of free allocated prefixes, numbers of allocated prefixes and prefix information.

Example

The following example shows how to show the DHCPv6 pool statistics information.

```
show ip local pool
```

Related Commands

Show ipv6 local pool

5.6.6 Clear ipv6 dhcp binding

clear ipv6 dhcp binding [*prefix*]

Parameters

Parameters	Description
Prefix	The ipv6 prefix of the to-be-deleted binding information.

Command Default

To remove all prefix binding information.

Command Mode

EXEC

Usage Guidelines

The command shows how to bind the information.

Example

The following example shows how to delete the binding information of 1:1:1:1::/64.

```
clear ipv6 dhcp binding1:1:1:1::/64
```

The following example shows how to delete all binding information.

```
clear ipv6 dhcp binding *
```

Related Commands

Show ipv6 dhcp bingding

Chapter 6 Neighbor Discovery Commands

6.1 ND Commands

ND commands include:

- debug ipv6 nd
- show ipv6 neighbors
- clear ipv6 neighbors
- ipv6 neighbor
- ipv6 nd dad attempts
- ipv6 nd managed-flag
- ipv6 nd ns-interval
- ipv6 nd other-flag
- ipv6 nd prefix
- ipv6 nd ra interval
- ipv6 nd ra-interval
- ipv6 nd ra-lifetime
- ipv6 nd reachable-time
- ipv6 nd router-preference
- ipv6 nd suppress-ra

6.1.1 debug ipv6 nd

To set the on-off of the print ND debug information to "on", run debug ipv6 nd.

debug ipv6 nd

Parameters

None

Command Default

The on-off of the print ND debug information is set to "off".

Command Mode

EXEC

Usage Guidelines

None

Example

None

Related Commands

None

6.1.2 show ipv6 neighbors

To show ipv6 neighbor cache, run **show ipv6 neighbors**.

show ipv6 neighbors

Parameters

None

Command Default

No default behavior or values.

Command Mode

EXEC

Usage Guidelines

None

Related Commands

None

6.1.3 clear ipv6 neighbors

To clear all non-manual configured ipv6 neighbor cache, run **clear ipv6 neighbors**.

clear ipv6 neighbors

Parameters

None

Command Default

No default behavior or values.

Command Mode

EXEC

Usage Guidelines

The command can only clear the router automatically acquired all neighbor cache, but will not clear the neighbor cache manually configured by **ipv6 neighbor** command.

Related Commands

ipv6 neighbor

6.1.4 ipv6 neighbor

To configure ipv6 neighbor cache in global configuration mode, run following command:

ipv6 neighbor *address6 interface mac*

Parameters

Parameters	Description
address6	ipv6 address of the neighbor
interface	Port of the router
mac	link layer address of the neighbor

Command Default

No default behavior or values.

Command Mode

Global configuration

Usage Guidelines

The command shows how to configure the router's neighbor cache. Unless run the no form of the command, the neighbor buffer will not be cleared. It will never timeout and be reachable all the time.

Example

```
IPv6_config#ipv6 neighbor 1::1 e1/1 00:e0::4c:5a:78:eb
```

To configure one neighbor on interface e1/1. ipv6 neighbor address is 1::1 and the link layer address of the neighbor is 00:e0:4c:5a:78:eb.

Related Commands

show ipv6 neighbors

6.1.5 ipv6 nd dad attempts

Configures the number of IPv6 Neighbor Discovery Neighbor Solicitation (NS) messages to be sent as part of duplicate address detection (DAD).

ipv6 nd dad attempts *num*

Parameters

Parameters	Description
num	Number of solicitations.

Command Default

1

Command Mode

Interface configuration

Usage Guidelines

To return to the default value, use the no form of the command.

Related Commands

None

6.1.6 ipv6 nd managed-flag

To set the M flag in the RA message transmitted by the local interface, run the following command.

ipv6 nd managed-flag

Parameters

None

Command Default

M flag is 0.

Command Mode

Interface configuration mode

Usage Guidelines

This command can be used to set the M flag in the RA message, which is transmitted by the local interface, to 1, and its “no” form can be used to cancel this settings and resume the default settings.

Related Commands

None

6.1.7 ipv6 nd ns-interval

The command shows how to configure the interval of forwarding NS and retrans-timer in RA message.

ipv6 nd ns-interval *milliseconds*

Parameters

Parameters	Description

milliseconds	Unit: milliseconds.

Command Default

Interval, in milliseconds, at which NS messages are sent. The default is 1000 milliseconds, i.e. 1 second. retrans-timer in RA is 0 by default, which means uncertain.

Command Mode

Interface configuration

Usage Guidelines

The command configures the interval of forwarding NS and retrans-timer in RA message.

To return to the default value, use the no form of the command.

Related Commands

None

6.1.8 ipv6 nd other-flag

To set the O flag in the RA message transmitted by the local interface, run the following command.

ipv6 nd other-flag

Parameters

None

Command Default

The O flag in the transmitted RA message is 0 by default.

Command Mode

Interface configuration

Usage Guidelines

This command can be used to set the O flag in the RA message, which is transmitted by the local interface, to 1, and its “no” form can be used to cancel this settings and resume the default settings.

Related Commands

None

6.1.9 ipv6 nd prefix

To configure the prefix of the RA message, run the first one of the following two commands:

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

Parameters

Parameters	Description
Ipv6-prefix	IPv6 prefix
Prefix-length	The length of IPv6 prefix.
Valid-lifetime	The valid time.
Preferred-lifetime	The preferred lifetime

Command Default

The default valid-lifetime is 2592000 seconds and the default preferred-lifetime is 604800 seconds.

Command Mode

Interface configuration

Usage Guidelines

no-advertise stands for the prefix is not included in RA message forwarded by the interface.

off-link means that the ON-Link flag in the prefix of the RA message is 0, and no-autoconfig means that the AUTO-CONFIG in the prefix of the RA message is 0.

You can configure the prefix on an interface by using ipv6 nd prefix ipv6-prefix/prefix-length… and cancel this prefix by using the “no” form of this command.

You can configure the default value of the prefix by using ipv6 nd prefix default … and cancel this settings by running the “no” form of this command.

Example

1. IPv6_config_e1/0#ipv6 nd prefix 1::/64

The prefix “1::0/64” is added on an interface and the other fields will be attributed with default values. The following RA messages will all be added with this prefix.

2. IPv6_config_e1/0#ipv6 nd prefix 2::/64 off-link

The prefix “2::/64” is added, the ON-LINK flag is 0, and other protocols are their default values.

3. IPv6_config_e1/0#ipv6 nd prefix default no-autoconfig

The default value on this interface is changed to NO-AUTOCONFIG, and other protocols are their default values. If the three commands are used successively, the third command will not influence the prefix “2::/64” configured by the second command but the prefix “1::/64” configured by the first command will change to NO-AUTOCONFIG.

Related Commands

None

6.1.10 Ipv6 nd ra interval

To configure the maximum or minimum interval of RA transmission, run the following command:

ipv6 nd ra interval *max [min]*

Parameters

Parameters	Description
max	Specifies maximum interval of RA transmission in seconds
Min	Specifies the minimum interval of RA transmission in seconds

Command Default

The default maximum interval is 600 seconds and the default minimum interval is only 1/3 of the default maximum interval.

Command Mode

Interface configuration

Usage Guidelines

This command is always used to set the range of the RA transmission interval.

To return to the default value, use the no form of the command.

Related Commands

ipv6 nd ra-interval

ipv6 nd ra-lifetime

6.1.11 ipv6 nd ra-interval

To configure the interval of RA transmission on the local interface, run the following command:

ipv6 nd ra-interval *seconds*

Parameters

Parameters	Description
seconds	Specifies the interval of RA transmission in seconds.

Command Default

The interval for the local interface to transmit the first three messages cannot be more than 16 seconds, while that to transmit the following messages varies between the maximum interval (600 seconds) and the minimum interval (200 seconds).

Command Mode

Interface configuration mode

Usage Guidelines

This command is always used to set the range of the RA transmission interval for the local interface. For the first 3 RA messages the interface forwarded, adopt the configured interval if the time configured is less than 16 seconds. Or the interval of the first 3 RA messages is 16 seconds. The interval of the subsequent RA messages adopt the configured time.

To return to the default value, use the no form of the command.

Related Commands

ipv6 nd ra interval

6.1.12 ipv6 nd ra-lifetime

To configure the router-lifetime field in the RA message transmitted by the local interface, run the following command.

ipv6 nd ra-lifetime *seconds*

Parameters

Parameters	Description
seconds	The value in the router-lifetime field in the RA message, whose unit is second.

Command Default

1800 seconds or triple of the maximum RA transmission interval configured by ipv6 nd ra interval max

Command Mode

Interface configuration

Usage Guidelines

To return to the default value, use the no form of the command.

Related Commands

ipv6 nd ra interval

6.1.13 ipv6 nd reachable-time

To set the reachable-time field of the RA message and the reachable time of all automatically configured neighbor caches on the local interface, run the following command:

ipv6 nd reachable-time *milliseconds*

Parameters

Parameters	Description
milliseconds	Time; Unit: milliseconds

Command Default

The reachable-time is 0 by default and the default reachable time for the neighbor cache is a value between 15 seconds and 45 seconds.

Command Mode

Interface configuration

Usage Guidelines

To return to the default value, use the no form of the command.

Related Commands

None

6.1.14 ipv6 nd router-preference

To configure the value of the router preference in the RA message, run the following command:

ipv6 nd router-preference *preference*

Parameters

Parameters	Description
Preference	The preference of a router, which can be one of the three values: high, medium and low.

Command Default

medium

Command Mode

Interface configuration

Usage Guidelines

To return to the default value, use the no form of the command.

Related Commands

None

6.1.15 ipv6 nd suppress-ra

To stop an interface to be the notification interface of a router, run the following command:

ipv6 nd suppress-ra

Parameters

None

Command Default

The interface works as the notification interface of the router.

Command Mode

Interface configuration

Usage Guidelines

To return to the default value, use the no form of the command.

Related Commands

None

Chapter 7 OSPFv3 Configuration Commands

7.1 OSPFv3 Configuration Commands

The OSPFv3 configuration commands include:

- area default-cost
- area range
- area stub
- area virtual-link
- debug ipv6 ospf
- debug ipv6 ospf events
- debug ipv6 ospf IFSM
- debug ipv6 ospf LSA
- debug ipv6 ospf NFSM
- debug ipv6 ospf NSM
- debug ipv6 ospf packet
- debug ipv6 ospf route
- default-metric
- ipv6 ospf area
- ipv6 ospf authentication
- ipv6 ospf encryption
- ipv6 ospf cost
- ipv6 ospf dead-interval
- ipv6 ospf hello-interval
- ipv6 ospf priority
- ipv6 ospf retransmit-interval
- ipv6 ospf transmit-delay
- ipv6 router ospf
- redistribute
- router-id
- show ipv6 ospf
- show ipv6 ospf database
- show ipv6 ospf interface
- show ipv6 ospf neighbor
- show ipv6 ospf route
- show ipv6 ospf virtual-link
- summary-prefix

- timers delay
- timers hold

7.1.1 area default-cost

To specify a cost for the default summary route sent into a stub or not so stubby area (NSSA), use the area default-cost command in router configuration mode. To remove the assigned default route cost, use the no form of this command.

area *area-id* **default-cost** cost

no area *area-id* **default-cost**

Parameters

Parameters	Description
area-id	Identifier for the stub or NSSA.
cost	Cost for the default summary route used for a stub or NSSA.

Command Default

Cost: 1

Command Mode

Ipv6 OSPF routing configuration

Usage Guidelines

The command can only be used on the boundary router connecting the NASSA area or the STUB area.

After the area stub default-information-originate command is configured, the cost configured by the cost will be used in LSA (type-3 inter-area-prefix-LSA) to set the corresponding cost.

Example

The following example assigns a default cost of 20 to stub network 36.0.0.0:

```
interface ethernet
1/0 ipv6 enable
ipv6 ospf 1 area 36.0.0.0
!
Ipv6 router ospf 1
router-id 2.2.2.2
area 36.0.0.0 stub
area 36.0.0.0 default-cost 20
```

Related Commands

area nssa

area stub

7.1.2 area range

To consolidate and summarize routes at an area boundary, use the area range command in router configuration mode. To disable this feature, use the no form of this command.

area *area-id* **range {***ipv6-prefix /prefix-length***} [advertise | not-advertise]**

no area *area-id* **range {***ipv6-prefix /prefix-length***} [advertise | not-advertise]**

Parameters

Parameters	Description
area-id	Identifier of the area about which routes are to be summarized. It can be specified as either a decimal value or as an IP address.
ipv6-prefix	The prefix of the IPv6 address.
prefix-length	The length of the IPv6 address.
advertise	Sets the address range status to advertise.
not-advertise	Sets the address range status to Do Not Advertise.

Command Default

This command is disabled by default.

Command Mode

Ipv6 OSPF router configuration

Usage Guidelines

The area range command is used only with Area Border Routers (ABRs). It is used to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the ABR. Routing information is condensed at area boundaries. External to the area, a single route is advertised for each address range. This behavior is called route summarization.

Multiple area router configuration commands specifying the range option can be configured. Thus, OSPF can summarize addresses for many different sets of address ranges.

Example

The following example shows how to set the prefix of the summarized IPv6 address in area 1, 2001:0DB8:0:1::/64: The following example specifies one summary route to be advertised by the ABR to area 1 for all subnets on network 2001:0DB8:0:1::/64:

```
interface Ethernet0/0
no ip address
ipv6 enable
ipv6 ospf 1 area 1
!
ipv6 router ospf 1
router-id 192.168.255.5
log-adjacency-changes
```

```
area 1 range 2001:0DB8:0:1::/64
```

7.1.3 area stub

To define an area as a stub area, use the area stub command in router configuration mode. To disable this feature, use the no form of this command.

area *area-id* **stub** [**no-summary**] **no**

area *area-id* **stub** [**no-summary**]

Parameters

Parameters	Description
area-id	Identifier for the stub area; either a decimal value or an IP address.
no-summary	(optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.

Command Default

No stub area is defined.

Command Mode

Ipv6 OSPF router configuration

Usage Guidelines

You must configure the area stub command on all routers and access servers in the stub area. Use the area router configuration command with the default-cost option to specify the cost of a default internal router sent into a stub area by an ABR.

There are two stub area router configuration commands: the stub and default-cost options of the area router configuration command. In all routers attached to the stub area, the area should be configured as a stub area using the stub option of the area command. Use the default-cost option only on an ABR attached to the stub area. The default-cost option provides the metric for the summary default route generated by the ABR into the stub area.

To further reduce the number of link-state advertisements (LSAs) sent into a stub area, you can configure the no-summary keyword on the ABR to prevent it from sending summary LSAs (LSA type 3) into the stub area.

Example

The following example shows how to set the STUB area of 36.0.0.0:

```
interface ethernet 0
ipv6 enable
ipv6 ospf 1 area 36.0.0.0
!
router ospf 1
router-id 2.2.2.2
area 36.0.0.0 stub
!
```

Related Commands

area nssa

7.1.4 area virtual-link

To define an OSPF virtual link, use the area virtual-link command in router configuration mode with the optional parameters. To remove a virtual link, use the no form of this command.

area *area-id* **virtual-link** *neighbor-ID* [**dead-interval** *dead-value*][**hello-interval** *hello-value*][**retransmit-interval** *retrans-value*][**transdly** *dly-value*]

no area *area-id* **virtual-link** *neighbor-ID*

Parameters

Parameters	Description
area-id	Area ID assigned to the transit area for the virtual link. This can be either a decimal value or a valid IP address. There is no default.
neighbor-id	Router ID associated with the virtual link neighbor. The router ID appears in the show ip ospf display. The router ID is internally derived by each router from the interface IP addresses. This value must be entered in the format of an IP address. There is no default.
dead-value	Time (in seconds) that hello packets are not seen before a neighbor declares the router down. Unsigned integer value.
hello-value	Time (in seconds) between the hello packets that the the software sends on an interface. Unsigned integer value to be advertised in the hello packets.
retrans-value	Interval for the router to transmit the re-transmit packet on the virtual link, whose unit is second The values configured at the two terminals of the virtual link must be same.
dly-value	Interval for the router to transmit the re-transmit packet on the virtual link, whose unit is second The values configured at the two terminals of the virtual link must be same.

Command Default

The virtual link is not configured.

The default values of other parameters are shown in the following:

Hello-value: 10s, Dead-value : 40s, Retrans-value : 5s, dly-value : 1s,

Command Mode

Ipv6 OSPF router configuration

Usage Guidelines

In order to create a virtual link, you have to perform configuration at the two terminals of the virtual link. If only one terminal need be configured, the virtual link cannot function.

The area-id parameter cannot be zero because the transit area of the virtual link must not be the backbone area. The area-id configured at the two terminals of the virtual link must be same.

In configuration, neighbor-ID must be the ospf router-id of the peer router. Or virtual link is impossible to establish.

Parameters configured at the two terminals of the virtual link must be same.

After the virtual link is created (the neighborhood is in the FULL state), the virtual link works in the Demand Circuit mode, that is, the periodical Hello packet and the LSA refresh packet are not transmitted.

You can run no area area-id virtual-link neighbor-ID to cancel the previous configuration of the virtual link.

You also can run show ip ospf virtual-link to check the state of the virtual link.

Example

The following example shows how to create a virtual link between router A and router B.

Configuration on router A (router-id: 200.200.200.1) :

```
!
interface Ethernet0/0
no ip address
ipv6 enable
ipv6 ospf 1 area 1
!
ipv6 router ospf 1
router-id 200.200.200.1
area 1 virtual-link 200.200.200.2
!
```

Configuration on router B (router-id: 200.200.200.2) :

```
!
interface Ethernet0/0
no ip address
ipv6 enable
ipv6 ospf 1 area 1
!
ipv6 router ospf 1
router-id 200.200.200.2
area 1 virtual-link 200.200.200.1
!
```

Related Commands

show ipv6 ospf virtual-link

7.1.5 debug ipv6 ospf

To show debugging information for Open Shortest Path First (OSPF) for IPv6, use the debug ipv6 ospf command in EXEC mode. To disable debugging output, use the no form of this command.

debug ipv6 ospf

no debug ipv6 ospf

Parameters

None

Command Default

No default behavior or values.

Command Mode

EXEC

Usage Guidelines

This command can be used to collect all debugging information about the OSPFv3 for the R&D engineers and technical support staff.

Example

```
Router# debug ipv6 ospf
LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 *]: Install Intra-Area-Prefix-LSA to Area
0.0.0.1
LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 *]: consider flooding through
interface[FastEthernet0/0]
LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 *]: Intra-Area-Prefix-LSA(0x38110c0)
originated
VLINK[VLINK1]: local address is 101::1VLINK[VLINK1]: peer 200.200.200.2 link
upLSA[Link(FastEthernet0/0):Type(0x0008):0.0.0.4:200.200.200.1 *]: Install Link-LSA to Link
FastEthernet0/0
LSA[Link(FastEthernet0/0):Type(0x0008):0.0.0.4:200.200.200.1 *]: consider flooding through
interface[FastEthernet0/0]
LSA[Link(FastEthernet0/0):Type(0x0008):0.0.0.4:200.200.200.1 *]: Link-LSA(0x381ec40)
originated
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.
LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: Install Router-LSA to Area 0.0.0.1
LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: consider flooding through
interface[FastEthernet0/0]
LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: Router-LSA(0x381ec20) originated
IFSM[FastEthernet0/0]: Down (InterfaceUp)
IFSM[FastEthernet0/0]: Status change Down -> Waiting
SPF[0.0.0.0]: Calculation timer scheduled [delay 5 secs]
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: Install Router-LSA to Area 0.0.0.0
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: consider flooding through
interface[VLINK1]
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: Router-LSA(0x38297e0)
originated IFSM[VLINK1]: Down (InterfaceUp)
IFSM[VLINK1]: Status change Down -> Point-To-
Point ROUTER[1]: Change status to ABR
IFSM[FastEthernet0/0]: Hello timer expire
Packet[SEND]: src(fe80:4::2e0:fff:fe26:2d98) ->
dst(ff02::5) OSPFv3 Header
  Version 3 Type 1 (Hello) Packet length 36
  Router ID 200.200.200.1
  Area ID 0.0.0.1
  Checksum 0x0000 Instance ID 0
OSPFv3 Hello
```

```
  Interface ID 4
  RtrPriority 1 Options 0x000013 (-|R|-|-|E|V6)
  HelloInterval 10 RtrDeadInterval 40 DRouter
  0.0.0.0 BDRouter 0.0.0.0
  # Neighbors 0
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.
……
```

7.1.6 debug ipv6 ospf events

To show information on Open Shortest Path First (OSPF)-related events, such as designated router selection and shortest path first (SPF) calculation, use the debug ipv6 ospf events command in privileged EXEC command. To disable debugging output, use the no form of this command.

debug ipv6 ospf events {abr|asbr|vlink|os|router} **no**

debug ipv6 ospf IFSM { abr|asbr|vlink|os|router }

Parameters

Parameters	Description
abr	ABR event debugging
asbr	ASBR event debugging
vlink	Virtual link event debugging
os	Socket debugging
router	OSPF debugging

Command Default

None

Command Mode

EXEC

Usage Guidelines

According to the information exported by the command, you can check the OSPF interface and the neighbor trigger event.

Example

```
Router# debug ip ospf events
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.
ROUTER[1]: Change status to ABR
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.
```

```
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.
VLINK[VLINK1]: peer 200.200.200.2 link downROUTER[1]: Change status to non-
ABR OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
ROUTER[Process:1]: GC timer expire
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
ROUTER[Process:1]: GC timer expire
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.
join AllDRouters on FastEthernet0/0OSPF6D: Received ospfv3 message:
OSPFV3_MSG_RCV_EVENT. OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.
……
```

7.1.7 debug ipv6 ospf ifsm

To show information on Open Shortest Path First (OSPF)-related ifsm, run the first one of the following two commands. To disable this feature, use the no form of the command.

debug ipv6 ospf ifsm {status|events|timers} **no**

debug ipv6 ospf ifsm {status|events|timers}

Parameters

Parameters	Description
status	Debug IFSM status information.
events	Debug IFSM event information.
timers	Debug IFSM timer information.

Command Default

None

Command Mode

EXEC

Usage Guidelines

According to the information output by the command, you can check the whole process of the state machine of the OSPF interface.

Example

```
Router# debug ipv6 ospf ifsm
IFSM[VLINK1]: Down (InterfaceUp)
IFSM[VLINK1]: Status change Down -> Point-To-Point
IFSM[FastEthernet0/0]: Down (InterfaceUp)
IFSM[FastEthernet0/0]: Status change Down -> Waiting
IFSM[FastEthernet0/0]: Hello timer expire
IFSM[VLINK1]: Hello timer expire
IFSM[VLINK1]: ifsm_ignore called
IFSM[VLINK1]: Point-To-Point (NeighborChange)
IFSM[FastEthernet0/0]: ifsm_ignore called
IFSM[FastEthernet0/0]: Waiting (NeighborChange)
IFSM[VLINK1]: LS ack timer expire
IFSM[VLINK1]: LS ack timer expire
IFSM[VLINK1]: Point-To-Point (InterfaceDown)
IFSM[VLINK1]: Status change Point-To-Point -> Down
IFSM[VLINK1]: ifsm_ignore called
IFSM[VLINK1]: Down (NeighborChange)
IFSM[FastEthernet0/0]: Hello timer expire
IFSM[FastEthernet0/0]: Hello timer expire
IFSM[FastEthernet0/0]: Hello timer expire
IFSM[FastEthernet0/0]: Wait timer expire
IFSM[FastEthernet0/0]: DR-Election[1st]: Backup 200.200.200.2
IFSM[FastEthernet0/0]: DR-Election[1st]: DR     200.200.200.2
IFSM[FastEthernet0/0]: Waiting (WaitTimer)
IFSM[FastEthernet0/0]: Status change Waiting -> DROther
IFSM[VLINK1]: Down (InterfaceUp)
IFSM[VLINK1]: Status change Down -> Point-To-Point
IFSM[FastEthernet0/0]: DR-Election[1st]: Backup 200.200.200.1
IFSM[FastEthernet0/0]: DR-Election[1st]: DR     200.200.200.2
IFSM[FastEthernet0/0]: DR-Election[2nd]: Backup 200.200.200.1
```

```
IFSM[FastEthernet0/0]: DR-Election[2nd]: DR        200.200.200.2
IFSM[FastEthernet0/0]: DROther (NeighborChange)
IFSM[FastEthernet0/0]: Status change DROther -> Backup
IFSM[FastEthernet0/0]: Hello timer expire
IFSM[FastEthernet0/0]: LS ack timer expire
IFSM[VLINK1]: Hello timer expire
IFSM[FastEthernet0/0]: LS ack timer expire
IFSM[VLINK1]: Point-To-Point (InterfaceDown)
IFSM[VLINK1]: Status change Point-To-Point -> Down
IFSM[VLINK1]: Down (InterfaceUp)
IFSM[VLINK1]: Status change Down -> Point-To-Point
IFSM[FastEthernet0/0]: LS ack timer expire
IFSM[VLINK1]: Hello timer expire
……
```

7.1.8 debug ipv6 ospf lsa

To show information on Open Shortest Path First (OSPF)-related lsa, run the first one of the following two commands. To disable this feature, use the no form of the command.

debug ipv6 ospf lsa { flooding|install|maxage|refresh}

no debug ipv6 ospf lsa { flooding|install|maxage|refresh}

Parameters

Parameters	Description
flooding	Debug lsa flooding information.
install	Debug lsa install information.
maxage	Debug lsa maxage information.
refresh	Debug lsa refresh information.

Command Default

No default behavior or values.

Command Mode

EXEC

Usage Guidelines

According to the information output by the command, you can browse the operation that OSPF performs to LSA and related events.

Example

```
router# debug ipv6 ospf lsa
LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 *]: Install Intra-Area-Prefix-LSA to Area 0.0.0.1
LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 *]: consider flooding through interface[FastEthernet0/0]
```

```
LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 *]: Intra-Area-Prefix-LSA(0x3824ba0)
originated
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: Install Router-LSA to Area 0.0.0.0
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: consider flooding through
interface[VLINK1]
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: consider flooding to
neighbor[200.200.200.2]
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: Router-LSA(0x3819be0) originated
LSA[Link(FastEthernet0/0):Type(0x0008):0.0.0.4:200.200.200.1 *]: Install Link-LSA to Link
FastEthernet0/0
LSA[Link(FastEthernet0/0):Type(0x0008):0.0.0.4:200.200.200.1 *]: consider flooding through
interface[FastEthernet0/0]
LSA[Link(FastEthernet0/0):Type(0x0008):0.0.0.4:200.200.200.1 *]: Link-LSA(0x3819bc0)
originated
LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: Install Router-LSA to Area 0.0.0.1
LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: consider flooding through
interface[FastEthernet0/0]
LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: Router-LSA(0x3824740) originated
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.2]: instance(0x380bf60) created with Link
State Update
LSA[Area(0.0.0.0):Type(0x2003):0.0.0.1:200.200.200.2]: instance(0x38246c0) created with Link
State Update
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.2]: flood started
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.2]: consider flooding through
interface[VLINK1]
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.2]: consider flooding to
neighbor[200.200.200.2]
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.2]: neighbor is not Full state
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.2]: Install Router-LSA to Area
0.0.0.0 LSA[Area(0.0.0.0):Type(0x2003):0.0.0.1:200.200.200.2]: flood started
LSA[Area(0.0.0.0):Type(0x2003):0.0.0.1:200.200.200.2]: consider flooding through
interface[VLINK1]
LSA[Area(0.0.0.0):Type(0x2003):0.0.0.1:200.200.200.2]: consider flooding to
neighbor[200.200.200.2]
LSA[Area(0.0.0.0):Type(0x2003):0.0.0.1:200.200.200.2]: neighbor is not Full state
LSA[Area(0.0.0.0):Type(0x2003):0.0.0.1:200.200.200.2]: Install Inter-Area-Prefix-LSA to Area
0.0.0.0
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: Install Router-LSA to Area 0.0.0.0
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: consider flooding through
interface[VLINK1]
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: consider flooding to
neighbor[200.200.200.2]
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: added to neighbor[200.200.200.2]'s
retransmit-list
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: sending update to interface[VLINK1]
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: Router-LSA refreshed
  OSPFv3 LSA
    Header LS age 0
    LS type 0x2001 (Router-LSA)
    Advertising Router 200.200.200.1
    Link State ID 0.0.0.0
    LS sequence number 0x80000002
    LS checksum 0x5ff7
    length 40
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: consider flooding through
interface[VLINK1]
LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: Install Router-LSA to Area 0.0.0.1
```

```
LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: consider flooding through
interface[FastEthernet0/0]
LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: Router-LSA
  refreshed OSPFv3 LSA Header
    LS age 0
    LS type 0x2001 (Router-LSA)
    Advertising Router 200.200.200.1
    Link State ID 0.0.0.0
    LS sequence number 0x80000002
    LS checksum 0x5382
    length 24
LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 *]: Install Intra-Area-Prefix-LSA to Area
0.0.0.1
LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 *]: consider flooding through
interface[FastEthernet0/0]
LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 *]: Intra-Area-Prefix-LSA
  refreshed OSPFv3 LSA Header
    LS age 0
    LS type 0x2009 (Intra-Area-Prefix-
    LSA) Advertising Router 200.200.200.1
    Link State ID 0.0.0.1
    LS sequence number 0x80000002
    LS checksum 0x3631
    length 64
    ……
```

7.1.9 debug ipv6 ospf nfsm

To show information on Open Shortest Path First (OSPF)-related nfsm, run the first one of the following two commands. To disable this feature, use the no form of the command.

debug ipv6 ospf packet

Parameters

Parameters	Description
status	Debug nfsm status information.
events	Debug nfsm event information.
timers	Debug nfsm timer information.

Command Default

No default behavior or values.

Command Mode

EXEC

Usage Guidelines

According to the information output by the command, you can check the whole process of the state machine of the OSPF interface.

Example

```
router# debug ipv6 ospf nfsm NFSM[200.200.200.2-
00000004]: Full (HelloReceived)
NFSM[200.200.200.2-00000004]: nfsm_ignore calledNFSM[200.200.200.2-00000004]: Full (2-
WayReceived)
NFSM[200.200.200.2-00000004]: Down (HelloReceived)
NFSM[200.200.200.2-00000004]: Status change Down -> Init
NFSM[200.200.200.2-00000004]: nfsm_ignore called
NFSM[200.200.200.2-00000004]: Init (1-WayReceived)
NFSM[200.200.200.2-00000004]: Init (HelloReceived)
NFSM[200.200.200.2-00000004]: Init (2-WayReceived)
NFSM[200.200.200.2-00000004]: Status change Init -> 2-Way
NFSM[200.200.200.2-00000004]: 2-Way (HelloReceived)
NFSM[200.200.200.2-00000004]: nfsm_ignore called
NFSM[200.200.200.2-00000004]: 2-Way (2-WayReceived)
NFSM[200.200.200.2-00000004]: 2-Way (AdjOK?)
NFSM[200.200.200.2-00000004]: Status change 2-Way -> ExStar
tNFSM[200.200.200.2-00000004]: ExStart (HelloReceived)
NFSM[200.200.200.2-00000004]: nfsm_ignore called
NFSM[200.200.200.2-00000004]: ExStart (2-WayReceived)
NFSM[200.200.200.2-00000004]: DD Retransmit timer expire
NFSM[200.200.200.2-00000004]: ExStart (NegotiationDone)
NFSM[200.200.200.2-00000004]: Status change ExStart -> Exchange
NFSM[200.200.200.2-00000004]: Exchange (ExchangeDone)
NFSM[200.200.200.2-00000004]: Status change Exchange ->
Loading NFSM[200.200.200.2-00000004]: nfsm_ignore called
NFSM[200.200.200.2-00000004]: Loading (LoadingDone)
NFSM[200.200.200.2-00000004]: Status change Loading -> Full
NFSM[200.200.200.2-80000001]: Down (HelloReceived)
NFSM[200.200.200.2-80000001]: Status change Down -> Init
NFSM[200.200.200.2-80000001]: Init (2-WayReceived)
NFSM[200.200.200.2-80000001]: Status change Init -> ExStart
NFSM[200.200.200.2-80000001]: ExStart (NegotiationDone)
NFSM[200.200.200.2-80000001]: Status change ExStart -> Exchange
NFSM[200.200.200.2-80000001]: Exchange (ExchangeDone)
NFSM[200.200.200.2-80000001]: Status change Exchange ->
Loading NFSM[200.200.200.2-80000001]: nfsm_ignore called
NFSM[200.200.200.2-80000001]: Loading (LoadingDone)
NFSM[200.200.200.2-80000001]: Status change Loading -> Full
NFSM[200.200.200.2-00000004]: Full (HelloReceived)
NFSM[200.200.200.2-00000004]: nfsm_ignore called
NFSM[200.200.200.2-00000004]: Full (2-WayReceived)
NFSM[200.200.200.2-00000004]: Full (AdjOK?)
NFSM[200.200.200.2-00000004]: LS update timer expire
NFSM[200.200.200.2-80000001]: LS update timer expire
NFSM[200.200.200.2-00000004]: LS update timer expire
NFSM[200.200.200.2-80000001]: LS update timer expire
NFSM[200.200.200.2-80000001]: Full (HelloReceived)
```

```
NFSM[200.200.200.2-80000001]: nfsm_ignore called
NFSM[200.200.200.2-80000001]: Full (2-WayReceived)
NFSM[200.200.200.2-00000004]: Full (HelloReceived)
NFSM[200.200.200.2-00000004]: nfsm_ignore called
NFSM[200.200.200.2-00000004]: Full (2-WayReceived)
NFSM[200.200.200.2-00000004]: LS update timer expire
NFSM[200.200.200.2-80000001]: LS update timer expire
……
```

7.1.10 debug ipv6 ospf nsm

To enable the debug switch of information transmission between the IPv6 routing table’s management module and the OSPFv3 module, run the first one of the following two commands:

debug ipv6 ospf nsm { redistribute **|** interface }

no debug ipv6 ospf nsm { redistribute **|** interface }

Parameters

Parameters	Description
redistribute	Debug nsm redistribute information.
interface	Debug nsm interface information.

Command Default

No default behavior or values.

Command Mode

EXEC

Usage Guidelines

According to the information output by this command, you can browse information exchange between OSPF and routing management module.

Example

```
router# debug ipv6 ospf nsm
Sep 17 16:43:53 OSPFv3: Received [NSM_MSG_ROUTE_CHG_NOTIFY:NSM_REDISTRIBUTE_DEL] message
Sep 17 16:43:53 OSPFv3: Received [NSM_MSG_ROUTE_CHG_NOTIFY:NSM_REDISTRIBUTE_DEL] message
Sep 17 16:43:53 OSPFv3: Received [NSM_MSG_ROUTE_CHG_NOTIFY:NSM_REDISTRIBUTE_DEL] message
Sep 17 16:43:53 OSPFv3: Received [NSM_MSG_ROUTE_CHG_NOTIFY:NSM_REDISTRIBUTE_DEL] message
Sep 17 16:43:53 OSPFv3: Receive [NSM_MSG_GLBL_ENAIPV6] message
……
```

7.1.11 debug ipv6 ospf packet

To show information about each Open Shortest Path First (OSPF) for IPv6 packet received, use the debug ipv6 ospf packet command in EXEC mode. To disable debugging output, use the no form of this command.

debug ipv6 ospf packet { hello|dd|ls-request|ls-update|ls-ack }

no debug ipv6 ospf packet { hello|dd|ls-request|ls-update|ls-ack }

Parameters

Parameters	Description
hello	Debug packet hello information.
dd	Debug packet dd information.
ls-request	Debug packet ls-request information.
ls-update	Debug packet ls-update information.
ls-ack	Debug packet ls-ack information.
Detail	Debug packet detail information.

Command Default

No default behavior or values.

Command Mode

EXEC

Usage Guidelines

According to the information output by the command, you can check the exchange of the OSPF packets.

Example

```
router# debug ipv6 ospf packet
Packet[SEND]: src(fe80:4::2e0:fff:fe26:2d98) ->
dst(ff02::5) OSPFv3 Header
  Version 3 Type 1 (Hello) Packet length 40
  Router ID 200.200.200.1
  Area ID 0.0.0.1
  Checksum 0x0000 Instance ID 0
OSPFv3 Hello
  Interface ID 4
  RtrPriority 1 Options 0x000013 (-|R|-|-|E|V6)
  HelloInterval 10 RtrDeadInterval 40
  DRouter 200.200.200.2   BDRouter 200.200.200.1
  # Neighbors 1
    Neighbor 200.200.200.2
Packet[RECV]: src(101::2) -> dst(101::1)
OSPFv3 Header
```

```
  Version 3   Type 1 (Hello)   Packet length 40
  Router ID 200.200.200.2
  Area ID 0.0.0.0
  Checksum 0x5774   Instance ID 0
OSPFv3 Hello
  Interface ID 2147483649
  RtrPriority 1   Options 0x000013 (-|R|-|-|E|V6)
  HelloInterval 10   RtrDeadInterval 40
  DRouter 0.0.0.0   BDRouter 0.0.0.0
  # Neighbors 1
    Neighbor 200.200.200.1
RECV[Hello]: Neighbor(200.200.200.2) declare 0.0.0.0 as DR, 0.0.0.0 as
Backup Packet[SEND]: src(101::1) -> dst(101::2)
OSPFv3 Header
  Version 3 Type 1 (Hello) Packet length 40
  Router ID 200.200.200.1
  Area ID 0.0.0.0
  Checksum 0x0000 Instance ID 0
OSPFv3 Hello
  Interface ID 2147483649
  RtrPriority 1   Options 0x000013 (-|R|-|-|E|V6)
  HelloInterval 10   RtrDeadInterval 40
  DRouter 0.0.0.0   BDRouter 0.0.0.0
  # Neighbors 1
    Neighbor 200.200.200.2
Packet[RECV]: src(fe80::2e0:fff:fe26:a8) -> dst(ff02::5)
OSPFv3 Header
  Version 3   Type 1 (Hello)   Packet length 40
  Router ID 200.200.200.2
  Area ID 0.0.0.1
  Checksum 0xa8a8   Instance ID 0
OSPFv3 Hello
  Interface ID 4
  RtrPriority 1   Options 0x000013 (-|R|-|-|E|V6)
  HelloInterval 10   RtrDeadInterval 40
  DRouter 200.200.200.2   BDRouter 200.200.200.1
  # Neighbors 1
    Neighbor 200.200.200.1
RECV[Hello]: Neighbor(200.200.200.2) declare 200.200.200.2 as DR, 200.200.200.1 as
Backup Packet[SEND]: src(fe80:4::2e0:fff:fe26:2d98) -> dst(ff02::5)
OSPFv3 Header
  Version 3 Type 1 (Hello) Packet length 40
  Router ID 200.200.200.1
  Area ID 0.0.0.1
  Checksum 0x0000 Instance ID 0
OSPFv3 Hello
  Interface ID 4
  RtrPriority 1 Options 0x000013 (-|R|-|-|E|V6)
  HelloInterval 10 RtrDeadInterval 40
  DRouter 200.200.200.2   BDRouter 200.200.200.1
  # Neighbors 1
    Neighbor 200.200.200.2
    ……
```

7.1.12 debug ipv6 ospf route

To enable the debug on-off of OSPFv3 routing information, run the first one of the following two commands:

debug ipv6 ospf route { ase|install|spf|ia }

no debug ipv6 ospf route { ase|install|spf|ia }

Parameters

Parameters	Description
ase	Configures the debug on-off of exterior routing calculation to "on".
install	Configures the debug on-off of routing installation procedure to "on".
spf	Configures the debug on-off of the debug switch of SPF calculation to "on".
ia	Configures the debug on-off of of between-domain routing calculation to "on".

Command Default

No default behavior or values.

Command Mode

EXEC

Usage Guidelines

According to the information output by the command, you can browse the calculation, deletion and addition of OSPF routes.

Example

```
router# debug ipv6 ospf route
Route[IA:0.0.0.0]: No SPF tree, schedule SPF calculationSPF[0.0.0.1]: SPF calculation timer
expire
SPF[0.0.0.1]:  SPF  calculation  (1st  STAGE)
SPF[0.0.0.1]:     Vertex[200.200.200.1-0.0.0.0]
SPF[0.0.0.1]:  SPF  calculation  (2nd  STAGE)
SPF[0.0.0.1]: SPF calculation (END)
Route[IA:0.0.0.1]: Cleanup IA route because of no ABRsRoute[IA:0.0.0.1]: Cleanup IA route
because of no ABRsSPF[0.0.0.1]: Calculation completed [0.170000 sec]
SPF[0.0.0.1]: Calculation timer scheduled [delay 9
secs] SPF[0.0.0.1]: SPF calculation timer expire
SPF[0.0.0.1]: SPF calculation (1st STAGE)
SPF[0.0.0.1]: Vertex[200.200.200.1-0.0.0.0]
SPF[0.0.0.1]: SPF calculation (2nd STAGE)
SPF[0.0.0.1]: SPF calculation (END)
Route[IA:0.0.0.1]: Cleanup IA route because of no ABRsSPF[0.0.0.1]: Calculation completed
[0.180000 sec]
SPF[0.0.0.1]: Calculation timer scheduled [delay 10 secs]
SPF[0.0.0.0]: Calculation timer scheduled [delay 5 secs]
```

```
Route[IA:0.0.0.1]: 888::/64 calculating Network routeRoute[IA:0.0.0.1]: 888::/64 Can't find route to ABR (200.200.200.2)Route[IA:0.0.0.0]: No SPF tree, schedule SPF calculationSPF[0.0.0.0]: SPF calculation timer expire
SPF[0.0.0.0]: SPF calculation (1st STAGE)
SPF[0.0.0.0]: Vertex[200.200.200.1-0.0.0.0]
SPF[0.0.0.0]:     Link[0] (200.200.200.2-128.0.0.1): Virtual-Link
SPF[0.0.0.0]:       Calculate nexthop for (200.200.200.2-0.0.0.0)
Route[0.0.0.0:SPF]: ADD Stub Route for (200.200.200.2)SPF[0.0.0.0]: Vertex[200.200.200.2-0.0.0.0]
SPF[0.0.0.0]:     Link[0] (200.200.200.1-128.0.0.1): Virtual-Link
SPF[0.0.0.0]:       LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *] is already in SPF tree
SPF[0.0.0.0]: SPF calculation (2nd STAGE)
SPF[0.0.0.0]: SPF calculation (END)
SPF[0.0.0.0]: Calculation completed [0.580000 sec]
……
```

7.1.13 default-metric

To set the default weight of the introduced route, run the first one of the following two commands:

default-metric *value*

no default-metric

Parameters

Parameters	Description
value	To-be-set route weight, ranging between 1 and 65535

Command Default

The default route weight is 10.

Command Mode

Ipv6 OSPF routing configuration

Usage Guidelines

The default-metric command is used to set the default routing weight when the route of other routing protocol is guided into the OSPF packet. When the redistribute command is used to guide the route of other routing protocol, the default routing weight designated by the default-metric command will be guided the specific routing weight will not be specified.

Example

The following example shows how to introduce the static route and set the default route weight of other routing protocol to 3:

```
interface ethernet
1/0 ipv6 enable
ipv6 ospf 1 area 36.0.0.0
!
```

```
Ipv6 router ospf 1
router-id 2.2.2.2
default-metric 3
redistribute static
```

Related Commands

redistribute

7.1.14 ipv6 ospf area

To enable the OSPFv3 protocol on an interface and specify an area for this interface, run the first one of the following two commands. To disable the OSPFv3 protocol, run the no form of the first command:

ipv6 ospf *process-id* **area** *area-id* [**instance** *instance-id*]

no ipv6 ospf *process-id* **area** *area-id* [**instance** *instance-id*]

Parameters

Parameters	Description
process-id	The OSPF process.
area-id	The OSPF area ID, which is specified by the interface.
instance-id	Specifies neighbor ospf instance number

Command Default

No default behavior or values.

Command Mode

Interface configuration

Example

The following example shows how to enable OSPFv3 process 0 for interface vlan1/0 and set its area ID to 0.

```
interface ethernet
1/0 ipv6 enable
ipv6 ospf 1 area 0
!
Ipv6 router ospf 1
router-id 2.2.2.2
```

7.1.16 ipv6 ospf authentication

To enable ospfv3 authentication on the interface, run the first one of the following two commands. To disable the OSPFv3, run the no form of the first command:

Ipv6 ospf authentication ipsec spi *spi-num* **[md5 | sha1]** *num Hex-string* **No ipv6 ospf authentication ipsec spi** *spi-num*

Parameters

Parameters	Description
spi-num	SPI(Security Parameter Index)
num	The key type
Hex-string	hexadecimal key

Command Default

No default behavior or values.

Command Mode

Interface configuration

Example

The following example shows how to enable ospfv3 authentication on interface GigaEthernet0/0：

```
interface GigaEthernet0/0
 no ip address
 no ip directed-
 broadcast ipv6 enable
 ipv6 ospf authentication ipsec spi 256 md5 0 1234
```

7.1.17 ipv6 ospf encryption

To enable ospfv3 encryption on the interface, run the first one of the following two commands.To disable the OSPFv3 encryption, run the no form of the first command:

Ipv6 ospf encryption ipsec spi *spi-num* **esp [des | 3des | aes | null] authentication [md5 | sha1]** *num Hex-string*

No ipv6 ospf encryption ipsec spi *spi-num*

Parameters

Parameters	Description
spi-num	SPI(Security Parameter Index)
num	The key type
Hex-string	hexadecimal key

Command Default

No default behavior or values.

Command Mode

Interface configuration

Example

The following example shows how to enable ospfv3 encryption on interface GigaEthernet0/0：

```
interface GigaEthernet0/0
 no ip address
 no ip directed-
 broadcast ipv6 enable
  ipv6 ospf encryption ipsec spi 256 esp des authentication md5 0 1234
```

7.1.18 ipv6 ospf cost

To specify the cost for the OSPF protocol running on the interface, run **ip ospf cost cost**. To resume the default settings, run **no ip ospf cost**.

ipv6 ospf cost *cost* [**instance** *instance-id*]

no ipv6 ospf *cost* [**instance** *instance-id*]

Parameters

Parameters	Description
cost	Cost for the OSPF protocol running on the interface, which is an integer between 1 and 65535
instance-id	Specifies neighbor ospf instance number

Command Default

The default cost for the OSPF protocol running on the interface is obtained based on the rate of the interface.

Command Mode

Interface configuration

Example

The following example shows how to set the cost for the OSPF protocol running on interface serial 0 to 2:

```
ipv6 ospf cost 2
```

7.1.19 ipv6 ospf dead-interval

To designate the dead interval of the neighboring router, run **ipv6 ospf dead-interval seconds**. To resume the default value, run **no ipv6 ospf dead-interval**.

ipv6 ospf dead-interval *seconds* [**instance** *instance-id*]

ipv6 ospf dead-interval [**instance** *instance-id*]

Parameters

Parameters	Description

Seconds	Value of the dead interval for the neighboring router, which ranges from 1 to 65535 seconds.
instance-id	Specifies neighbor ospf instance number

Command Default

The dead interval for the neighboring router is 40 seconds by default.

Command Mode

Interface configuration

Usage Guidelines

The value of the dead-interval parameter will be written to the HELLO packet and will be transmitted along with the HELLO packet. It must be ensured that the dead-interval parameter must be identical with that between the neighboring routers and the value of the dead-interval parameter must be four times of the value of the hello-interval parameter.

Example

The following example shows how to set the dead interval of the neighboring router on interface serial0 to 60 seconds.

```
router_config_S1/0#ipv6 ospf dead-interval 60
```

Related Commands

ipv6 ospf hello-interval

7.1.20 ipv6 ospf hello-interval

To designate the interval for transmitting the HELLO packet on the interface, run **ipv6 ospf hello-interval seconds**. To resume the default settings, run **no ipv6 ospf hello-interval**.

ipv6 ospf hello-interval *seconds* [**instance** *instance-id*]

no ipv6 ospf hello-interval [**instance** *instance-id*]

Parameters

Parameters	Description
seconds	Transmission interval of the HELLO packet, ranging from 1 to 255 seconds
instance-id	Specifies neighbor ospf instance number

Command Default

The default interval for transmitting the HELLO packet on the interface is 10 seconds.

Command Mode

Interface configuration

Usage Guidelines

The value of the hello-interval parameter will be written to the Hello packet and will be transmitted along with the HELLO packet. The smaller the hello-interval is, the sooner the change of the network topology will be found. However, much more path cost will be paid. It must be ensured that the parameter must be identical with that between the neighboring routers.

Example

The following example shows that the interval for transmitting the HELLO packet on interface serial 1/0 is set to 20 seconds.

```
router_config_S1/0#ipv6 ospf hello-interval 20
```

Related Commands

ipv6 ospf dead-interval

7.1.21 ipv6 ospf priority

To configure the priority for the interface to choose the router, run **ipv6 ospf priority priority**. To return to the default value, use the no form of the command.

ipv6 ospf priority *priority* [**instance** *instance-id*]

no ipv6 ospf priority [**instance** *instance-id*]

Parameters

Parameters	Description
priority	Priority to choose the router, ranging between 0 and 255
instance-id	Specifies neighbor ospf instance number

Command Default

The default priority for the interface to choose the routers is 1.

Command Mode

Interface configuration

Usage Guidelines

When two routers in the same network segment want to be the selection router, the router with higher priority will be selected. If the priority of the two routers is the same, the router with a larger ID is selected. When the priority of one router is 0, the router will not be selected as “designated router” or “backup designated router”. The priority is effective only on the networks except the point-to-point network.

Example

The following example shows how to set the priority to 8 when interface Serial1/0 selects the selection router.

```
router_config_S1/0#ipv6 ospf priority 8
```

Related Commands

No default behavior or values.

7.1.22 ipv6 ospf retransmit-interval

To designate the retransmission interval for transmitting the link state broadcast between the interface and the neighboring router, run **ipv6 ospf retransmit** seconds. To resume the default value, run **no ipv6 ospf retransmit**.

ipv6 ospf retransmit *seconds* [**instance** *instance-id*]

no ipv6 ospf retransmit [**instance** *instance-id*]

Parameters

Parameters	Description
seconds	Transmission interval for transmitting the link state broadcast between the interface and the neighboring router, ranging between 1 and 65535 seconds
instance-id	Specifies neighbor ospf instance number

Command Default

The default interval for transmitting the link state broadcast between the interface and the neighboring router is 5 seconds.

Command Mode

Interface configuration

Usage Guidelines

When a router transmits the link-state broadcast to its neighbor, the command will maintain the link-state broadcast until the peer receives the acknowledgment. If the link-state broadcast is not received during the transmission interval, it will be retransmitted. The value of the seconds parameter must be larger than the round-trip time for a packet transmitting between two routers.

Example

The following example shows how the default interval for transmitting the link-state broadcast between interface Serial1/0 and the neighboring router is set to 8 seconds.

```
router_config_S1/0#ipv6 ospf retransmit 8
```

7.1.23 ipv6 ospf transmit-delay

To set the delay for the link-state broadcast to be transmitted on the interface, run **ipv6 ospf transit-delay time**. To return to the default value, run **no ipv6 ospf transit-delay**.

ipv6 ospf transit-delay *time* [**instance** *instance-id*]

no ipv6 ospf transit-delay [**instance** *instance-id*]

Parameters

Parameters	Description
time	The delay of link state broadcast transmission on an interface, which ranges from 1 to 65535 seconds.
instance-id	Specifies neighbor ospf instance number

Command Default

The default delay for the link-state broadcast to be transmitted on the interface is 1 second.

Command Mode

Interface configuration

Example

The following example shows how to set the delay for transmitting the link-state broadcast on interface Serial1/0 to 3 seconds.

```
router_config_S1/0#ipv6 ospf transit-delay 3
```

7.1.24 ipv6 router ospf

To configure the OSPF router, run router ospf. To disable the OSPF route on the router, run **no ipv6 router ospf**.

ipv6 router ospf *process-id*

no ipv6 router ospf *process-id*

Parameters

Parameters	Description
process-id	Identifies the OSPF process. It is a positive integer distributed by the local router. It only means an ospf process.

Command Default

No default behavior or values.

Command Mode

Global configuration

Usage Guidelines

One router may have multiple OSPF processes.

Example

The following example shows how to set an OSPF PROCESS, whose process ID is 109:

```
Ipv6 router ospf 109
```

Related Commands

ipv6 ospf area

7.1.25 redistribute

To configure the route where OSPF forwards other router protocols, run redistribute. To return to the default value, run no redistribute.

redistribute protocol [*as-number*] [**route-map** map-tag]

no redistribute protocol [*as-number*] [**route-map** map-tag]

Parameters

Parameters	Description
protocol	original protocol of forwarded learning
as_number	(Optional) Autonomous system number for the redistributed route, connect, rip and static are not included.
map-tag	(Optional) Identifier of a configured route map.

Command Default

OSPF does not forward the routes of other routing protocols.

Command Mode

Router configuration

Usage Guidelines

None

Example

The following example shows how to forward the static route in OSPF process 1:

```
interface ethernet
1/0 ipv6 enable
ipv6 ospf 1 area 0
!
Ipv6 router ospf 1
router-id 2.2.2.2
redistribute static
```

7.1.26 router-id

To configure the router ID in the autonomous system for the router on which the is OSPFv3 protocol running, run the first one of the following two commands. To disable the router ID, run **no router-id**.

router-id *router-id*

no router-id *router-id*

Parameters

Parameters	Description
router-id	The identifier of the router, which is in the IPv4 address format.

Command Default

If an IPv4 address has already configured on a router before OSPFv3 is enabled, the router will automatically choose an IPv4 address as its ID.

Command Mode

Router configuration

Usage Guidelines

Router ID is the only identifier of a router running OSPFv3 protocol in AS system. It must be ensured that the Router ID of any router is different from the other.

If the router has no Router ID, OSPFv3 process cannot be run.

Example

The following example shows how to set the router ID of OSPFv3 process 1 to 2.2.2.2:

```
ipv6 router ospf 1
router-id 2.2.2.2
```

7.1.27 show ipv6 ospf

To show the main OSPF information, run the following command:

show ipv6 ospf [*process-id*]

Parameters

Parameters	Description
process-id	ID of the process, which is an optional parameter

Command Default

No default behavior or values.

Command Mode

EXEC

Usage Guidelines

The information output by the command can help checking the OSPF faults. If the process-id parameter follows the command, the information about the global configuration of the OSPF process is displayed.

Example

The following example shows that the configuration information about all OSPF processes will be shown.

```
router# show ipv6 ospf
Routing Process "OSPFv3 0" with ID 1.2.3.4
SPF schedule delay 5 secs, Hold time between SPFs 10 secs Minimum LSA interval 5
secs, Minimum LSA arrival 1 secs Number of external LSA 3. Checksum Sum 0x2CD6F
Number of areas in this router is 1
Area BACKBONE(0)
Number of interfaces in this area is 1
SPF algorithm executed 3 times
Number of LSA 4. Checksum Sum
0x2A6AC router#
```

Relative fields are explained in the following table:

Domain	Description
Routing Process "OSPFv3 0"	ID of the OSPF process
with ID 1.2.3.4	ID of the router
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs	Two timer values relative with OSPF
Number of areas is 1	Number of the currently-configured fields, and parameters configured in each field
Number of LSA 4	The quantity of LSAs in the database.
Number of external LSA 3	The quantity of ASE LSAs in the database.
SPF algorithm executed 3 times	SPF algorithm execution statistics

7.1.28 show ipv6 ospf database

To show lists of information related to the Open Shortest Path First (OSPF) database for a specific router, use the show ipv6 ospf database command in user EXEC mode.

show ipv6 ospf database { router **|** network **|** inter-prefix **|** inter-router **|** external **|** link **|** intra-prefix } [ADVROUTER]

Parameters

Parameters	Description
router	Shows information only about the router LSAs.
network	Shows information only about the network LSAs.
inter-prefix	Shows information only about LSAs based on inter-area prefix LSAs.
inter-router	Shows information only about LSAs based on inter-area router LSAs.
external	Shows information only about the external LSAs.
link	Shows information about the link LSAs.
intra-prefix	Shows information only about LSAs based on intra-area prefix LSAs.
ADVROUTER	Shows all the LSAs of the advertising router.

Command Default

No default behavior or values.

Command Mode

EXEC

Usage Guidelines

The information output by the command can help to check the database information about the OSPF connection state and to find the reason of the faults.

Example

```
router#
router#show ipv6 ospf database
Link-LSA (Interface eth0)
Link State ID ADV Router Age Seq# CkSum
Prefix 0.0.0.3 1.2.3.4 104 0x80000004 0x889e 0
0.0.0.5 5.6.7.8 142 0x80000003 0xab70 2
Router-LSA (Area 0.0.0.0)
Link State ID ADV Router Age Seq# CkSum Link
0.0.0.1 1.2.3.4 94 0x80000014 0xeaea 1
0.0.0.1 5.6.7.8 105 0x80000019 0x8a32 1
Network-LSA (Area 0.0.0.0)
Link State ID ADV Router Age Seq# CkSum
0.0.0.5  5.6.7.8  105  0x80000001  0xa441
Intra-Area-Prefix-LSA (Area 0.0.0.0)
Link State ID ADV Router Age Seq# CkSum Prefix Reference
0.0.0.1 5.6.7.8 104 0x80000001 0x8d4f 2 Network-LSA
AS-external-LSA
Link State ID ADV Router Age Seq# CkSum
0.0.0.1 5.6.7.8 1229 0x80000002 0xe92d
0.0.0.2 5.6.7.8 1229 0x80000002 0xef25
0.0.0.3 5.6.7.8 1229 0x80000002 0xf51d
  router#
```

Relative fields are explained in the following table:

Domain	Description
AREA: 1	Current area
Router Link States/Net Link States/Summary Net Link States	LSA type
Link ID	LSA ID.
ADV Router	Releases the router.
Age	Releases the age.
Seq #	Generates the sequence ID.
Checksum	Checksum.

7.1.29 show ipv6 ospf interface

To show the information about the OSPF interface, run the following command:

show ipv6 ospf interface [type] [index]

Parameters

Parameters	Description
type	Port type
index	Port number

Command Default

No default behavior or values.

Command Mode

EXEC

Usage Guidelines

According to the information displayed by the command, you can check the OSPF configuration and its running state, which helps you to detect the OSPF faults.

Example

```
router#show ipv6 ospf interface
ethernet0/1 is up, line protocol is up
Interface ID 3, Instance ID 0, Area 0.0.0.0
IPv6 Link-Local Address fe80::248:54ff:fec0:f32d/10
Router ID 1.2.3.4, Network Type BROADCAST, Cost:
10 Transmit Delay is 1 sec, State Backup, Priority 1
Designated Router (ID) 5.6.7.8
Interface Address fe80::203:47ff:fe4c:776e
```

```
Backup Designated Router (ID) 1.2.3.4
Interface Address fe80::248:54ff:fec0:f32d
Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit
5 Hello due in 00:00:01
Neighbor Count is 1, Adjacent neighbor count is
1 router#
```

Relative fields are explained in the following table:

Domain	Description
IPv6 Link-Local Address	Address of interface IPv6 link-local
Nettype	Network type of the OSPF interface
OSPF process is	ID of the OSPF process
AREA	Current area
Router ID	ID of the router where the process belongs
Cost	Cost of the OSPF interface of the router
Transmit Delay is	Transmission delay
Priority	Priority for the interface of the router
Hello interval	Transmission interval of the Hello packet
Dead timer	Dead time
Retransmit	Retransmission interval
OSPF INTF State is	State of the OSPF interface
Designated Router id	IP of the designated router and the IP address of its interface
Backup Designated router id	ID of the backup designated router and the IP address of its interface
Neighbor Count is	Number of the neighboring routers
Adjacent neighbor count is	Number of neighbors that have established the neighborhood relation
Adjacent with neighbor	Neighbor lists that have established the neighborhood relation

7.1.30 show ipv6 ospf neighbor

Shows the information about OSPF neighbors.

show ipv6 ospf neighbor [interface_type interface_number | router-id | detail]

Parameters

Parameters	Description
interface_type	Port type
interface_number	Port number
router-id	Router ID

Detail	Show the details.

Command Default

No default behavior or values.

Command Mode

EXEC

Usage Guidelines

The information displayed by the command can help you to check whether the OSPF neighbor configuration is right and to detect the OSPF faults.

Example

```
router#show ipv6 ospf neighbor
OSPFv3 Process 1
Area 1
Neighbor ID   Pri    State   Dead Time    Interface    Instance ID
5.6.7.8 1            Full/DR 00:00:38          eth0             0
```

Relative fields are explained in the following table:

Domain	Description
OSPFv3 process	ID of the OSPF process
AREA	Local area
Neighbor	ID of a neighbor
Pri	Priority of a neighbor
State	Connection state related with the neighbor
DeadTime	Time of neighbor invalidation
Address	IP address of the neighbor
Interface	Port used by a router to reach its neighbor

7.1.31 show ipv6 ospf route

To show the information about the OSPF routing table, run the following command:

show ipv6 ospf route

Parameters

None

Command Default

No default behavior or values.

Command Mode

EXEC

Usage Guidelines

The information shown by the command can help you browse the OSPF routing table and confirm whether the OSPF trouble diagnosis is correctly carried out.

Example

```
router#show ipv6 ospf route
Destination Metric
Next-hop Interface
3ffe:1:1::/48 10
-- eth0
3ffe:2:1::/48 10
-- eth0
3ffe:2:2::/48 10
-- eth0
3ffe:3:1::/48 10
-- eth0
3ffe:3:2::/48 10
-- eth0
3ffe:3:3::/48 10
-- eth0
E2 3ffe:100:1::1/128 10/20
fe80::203:47ff:fe4c:776e eth0
E2 3ffe:100:2::1/128 10/20
fe80::203:47ff:fe4c:776e eth0
E2 3ffe:100:3::1/128 10/20
fe80::203:47ff:fe4c:776e eth0
IA 3ffe:101:1::/48 20
fe80::203:47ff:fe4c:776e eth0
IA 3ffe:101:2::/48 20
fe80::203:47ff:fe4c:776e eth0
IA 3ffe:101:3::/48 20
fe80::203:47ff:fe4c:776e eth0
```

Relative fields are explained in the following table:

Domain	Description
Destination	Destination network segment
Metric	Cost of a route
Next-hop	Address of the next hop
Interface	Interface of the next hop

7.1.32 show ipv6 ospf virtual-link

To show the information about the OSPF virtual link, run the following command:

show ipv6 ospf virtual-link

Parameters

None

Command Default

No default behavior or values

Command Mode

EXEC

Usage Guidelines

According to the information output by the command, you can check the state of the OSPF virtual link.

You can run show ipv6 ospf neighbor to check the detailed information about the adjacent neighbor.

Example

```
router#show ipv6 ospf virtual-link
Virtual Link VLINK1 to router 5.6.7.8 is up
Transit area 0.0.0.1 vian interface eth0, instance ID 0
Local address 3ffe:1234:1::1/128
Remote address 3ffe:5678:3::1/128
Transmit Delay is 1 sec, State Point-To-Point,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:01
Adjacency state Up
```

Relative fields are explained in the following table:

Domain	Description
neighbor ID	Neighbor ID of the peer
Neighbor State	Neighborhood state for the neighbor
TransArea	Transmission area
cost	Minimum cost for reaching the peer in the transmission area If the value of the cost is 0, it means that the peer is unreachable.
Hello Interval	Current transmission interval for the Hello packet
DeadTime	Time of neighbor invalidation
Retrans	Retransmission interval
Adjacency state	State of the virtual link interface

Related Commands

area vritual-link

show ipv6 ospf neighbor

7.1.33 summary-prefix

To configure the address for OSPF to create the route aggregation, run the first one of the following two commands. To disable the address of route aggregation, run no summary-prefix.

summary-prefix *ipv6-prefix /prefix-length*

no summary-prefix *ipv6-prefix /prefix-length*

Parameters

Parameters	Description
ipv6-prefix	Aggregation address with the designated address range
prefix-length	Subnet mask of the aggregation route

Command Default

No default behavior or values.

Command Mode

Router configuration

Usage Guidelines

Multiple groups of addresses are summarized. Routes learned from other routing protocols can also be summarized. After the aggregation, all covered networks cannot be transmitted to other routing fields. The cost of the summary route is the minimum value among the cost values of all summary routes. The command cannot be used to reduce the size of the routing table.

The command is used by OSPF to enable the ASBR to notify an external route of being an aggregation route to replace all external routes. The command is only used to aggregate the OSPF routes of other routing protocols. You can run area range in OSPF to summarize the routes.

Example

In the following example, the summary address 2001::/64 stands for addresses such as 2001::/80, 2001::1/64 and so on, and only address 2001::/64 is broadcasted.

```
summary-address 2001::/64
```

Related Commands

area range

7.1.34 timers delay

To specify a delay interval between OSPF receiving a topology change and starting a shortest path priority calculation, run timer delay spf-delay. To return to the default value, use the no form of the command.

timers delay *spf-delay*

no timers delay

Parameters

Parameters	Description
spf-delay	Delay between the topology change and calculation start. It ranges between 0 and 65535 seconds, and its default value is 5 seconds. Its default value is 5 seconds. If the value is 0, there is no delay. That is, the calculation will be promptly started if changes occur.

Command Default

spf-delay: 5 seconds

Command Mode

Router configuration

Usage Guidelines

The smaller value the delay is set to, the faster the network change is reflected. However, it will take the processor more time.

Example

```
timers delay 10
```

7.1.35 timers hold

To set the interval between two continuous SPF calculations, run timers hold. To disable this feature, use the no form of this command.

timers hold *spf-holdtime*

no timers hold

Parameters

Parameters	Description
spf-holdtime to 65535	Minimum value between two continuous calculations It ranges between 0 seconds. Its default value is 10 seconds; when it is 0, there is no interval between the two continuous calculations.

Command Default

spf-holdtime: 10 seconds

Command Mode

Router configuration

Usage Guidelines

The smaller value the delay is set to, the faster the network change is reflected. However, it will take the processor more time.

Example

```
timers hold 20
```

Chapter 8 Ripng Configuration Commands

8.1 Ripng Configuration Commands

RIPng configuration commands include:

1. clear ipv6 rip route
2. debug ipv6 rip
3. default-metric
4. distance
5. distribut-list prefix-list
6. ipv6 rip enable
7. ipv6 rip poison-reverse
8. ipv6 rip split-horizon
9. ipv6 rip summary-address
10. ipv6 route default-information
11. ipv6 router rip
12. maximum-paths
13. maximum-routes
14. neighbor
15. offset
16. passive interface
17. Port
18. redistribute
19. show ipv6 rip
20. show ipv6 rip interface
21. timers

8.1.1 clear ipv6 rip route

To delete certain route, run **clear ipv6 rip route**.

clear ipv6 rip *name* **route** { * | X:X::X:X/M | static | connected | rip | ospf | bgp | eigrp }

Parameters	Description
route	RIPng routing table
*	All routes
X:X::X:X	Specifies route network address

/M	Specifies route network mask
static	Removes forwarded static route from RIPng routing table
rip	Removes RIP route from RIPng routing table
ospf	Removes forwarded OSPFv3 route from RIPng routing table
bgp	Removes forwarded BGP+ route from RIPng routing table
eigrp	Removes forwarded eigrp route from RIPng routing table

Command Default

No default behavior or values.

Command Mode

Non-user mode

Usage Guidelines

The command shows how to delete a certain route in the routing table.

Example

None

Related Commands

None

8.1.2 debug ipv6 rip

To trace RIPng information, events and the interaction of main routing table, run the first one of the following two commands; to disable the debug information, run the no form of the first command.

debug ipv6 rip [word] **[** events | packet **[** [send | receive] [detail] **]]**
no debug ipv6 rip

Parameters	Description
word	The name of the RIPNG instance.
events	Shows the RIP event.
packet	Shows the RIP packet debug information.
send	Shows the forwarded RIP packet.
receive	Shows the received RIP packet.
detail	Shows the forwarded/received RIP packet.

Command Default

No default behavior or values.

Command Mode

EXEC

Usage Guidelines

This command can be used to trace the main procedures of RIPNG.

Example

None

Related Commands

None

8.1.3 default-metric

Specify metric which forwards a protocol route

default-metric protocol value

no default-metric protocol *[value]*

Parameters	Description
value	It is used to specify the default metric value for route forwarding, which ranges between <1-16>.
protocol	protocol name

Command Default

The default metric for route forwarding is 1.

Command Mode

Global configuration

Usage Guidelines

Specify metric which forwards a protocol route

Example

None

Related Commands

None

8.1.4 distance

To set the management distance, run the first one of the following two commands: **distance** *value* [*X:X:X:X::X/prefixlen* | [word]]

no distance *value* [*X:X:X:X::X/prefixlen*| [word]

Parameters	Description
value	Specifies management distance value
X:X:X:X::X/prefix	Specifies network prefix length

word	Specifies access list name

Command Default

The default RIPNG management distance is 120.

Command Mode

Global configuration

Usage Guidelines

The command is used to configure management distance.

Example

None

Related Commands

None

8.1.5 distribut-list prefix-list

prefix list for filtering route

distribute-list { prefix-list | access-list | gateway} *word* {in | out } [*interface-type interface-number*]

no distribute-list [prefix-list *word* | access-list *word* | gateway *word*] {in | out } [*interface-type interface-number*]

Parameters	Description
word	Prefix list name
in	Applies the prefix list to the received routing update packet
out	Applies the prefix list to the forwarded routing update packet
interface-type	(optional) Specifies interface type
interface-number	(optional) Specifies interface type

Command Default

No default behavior or values.

Command Mode

Global configuration

Usage Guidelines

None

Example

The following example applies the prefix list named bd_prefix to IPv6 RIP routing updates that are received on Ethernet interface2/1:

Router_config# ipv6 router rip ROUTER

Router_config_rip_ROUTER# distribute-list prefix-list bd_prefix in e2/1

Related Commands

ipv6 prefix-list

show ipv6 prefix-list

8.1.6 ipv6 rip enable

To enable a RIPng instance on an interface, run the first one of the following two commands; to delete ripng instance on the interface, run the no form of the first command.

ipv6 rip *word* **enable**

no ipv6 rip *word*

Parameters	Description
word	The name of the routing process instance

Command Default

No default behavior or values.

Command Mode

Port configuration

Usage Guidelines

None

Example

Router_config# int e2/1

Router_config_e2/1# ipv6 rip ROUTER enable

Related Commands

Show ipv6 rip

8.1.7 ipv6 rip poison-reverse

To apply poison reverse on an interface, run the first one of the following two commands:

ipv6 rip ***word*** **poison-reverse no**

ipv6 rip *word* **poison-reverse**

Parameters	Description
word	The name of the routing process instance
poison-reverse	It means to enable poison reverse on an interface.

Command Default

The command is disabled by default..

Command Mode

Port configuration

Usage Guidelines

None

Example

R142_config_e2/1# ipv6 rip ROUTER poinson-reverse

Related Commands

None.

8.1.8 ipv6 rip split-horizon

To apply horizontal split on an interface, run the first one of the following two commands:

ipv6 rip *word* split-horizon no

ipv6 rip *word* **split-horizon**

Parameters	**Description**
word	Specifies the name of the routing process instance
split-horizon	Applies horizontal split on an interface

Command Default

The default is enabled.

Command Mode

Port configuration

Usage Guidelines

No default behavior or values.

Example

R142_config_e2/1# no ipv6 rip ROUTER split-horizon

Related Commands

None

8.1.9 ipv6 rip summary-address

To specify the aggregation route of the RIPNG instances, run the following first one of the commands:

To return to the default value, use the no form of the command.

ipv6 rip *word* **summary-address** *ipv6-prefix***/***prefix-length*

no ipv6 rip *word* **summary-address**

Parameters

Parameters	Description
word	Specifies the name of the routing process instance
ipv6-prefix	Specifies IPv6 aggregation network
/prefix-length	Specifies the length of IPv6 prefix

Command Default

There is no aggregation

route. Command Mode

RIPNG configuration

Usage Guidelines

None

Example

```
R142_config# interface e2/1
R142_config_e2/1# 2001:1:1:1::132/64
R142_config_e2/1# ipv6 router rip ROUTER
R142_config_rip_ROUTER# ipv6 rip ROUTER summary-address
2001:1:1::/35 (Note: 2001:1::/35 will be shown when show run.)
```

The informed aggregation route is length of 35, but not length of

64. Related Commands

None

8.1.10 ipv6 route default-information

Configure inform default route on the interface.

ipv6 rip *word* default-information {only | originate}

no ipv6 rip *word* **default-information**

Parameters

Parameters	Description
word	Specifies the name of the routing process instance
Only	The interface only inform rip default route, but suppress other route.
Originate	Other route's inform will not be influenced, when the default route is informed.

Command Default

No default route

Command Mode

Port configuration

Usage Guidelines

None

Example

```
R142_config# interface e2/1
R142_config_e2/1# ipv6 rip ROUTER default-information only
```

Related Commands

None

8.1.11 ipv6 router rip

To configure a RIPng instance globally, run the first one of the following two commands: **ipv6 router rip** *word*

no ipv6 router rip *word*

Description

Parameters	Description
Rip	Enable IPv6 routing information protocol (RIPng)
word	The name of the routing process instance

Command Default

No default behavior or values.

Command Mode

Global configuration

Usage Guidelines

The command is similar to rip, but it is ripng of ipv6.

After the configuration command is entered, the router prompt changes to Router(config-rtr-rip)#.

Example

```
Router_config# ipv6 router rip ROUTER
```

Related Commands

ipv6 rip word enable	enable ripng instance on the interface

8.1.12 maximum-paths

To configure the number of equivalent routes allowed by the RIPng instance, run **maximum-path**; to cancel the limit on the number of equivalent routes allowed by the RIPng instance, run **no maximum-path**.

no maximum-path

Parameters	Description
Value	Sets the number of equivalent routes allowed by

	the RIPng instance

Default

Value 4

Command Mode

Global configuration

Usage Guidelines

Maximum Value 6

Example

None

Related Commands

None

8.1.13 maximum-routes

To configure the number of maximum routes allowed by the RIPng instance, run maximum-path; to cancel the limit on the number of maximum routes allowed by the RIPng instance, run **no maximum-routes**.

maximum-routes *value*

no maximum- routes

Description

Parameters	Description
Value	Sets the number of maximum routes allowed by the RIPng instance <1~8192>

Command Default

8192

Command Mode

Global configuration

Usage Guidelines

No default behavior or values.

Example

None

Related Commands

None

8.1.14 neighbor

Specify the neighbor connected to an interface, which is mainly used for dumb router. It only forwards updates to specific neighbors.

To disable this feature, use the no form of the command.

neighbor ipv6-addr interface-type interface-number

no neighbor ipv6-addr interface-type interface-number

Description

ipv6-addr	ipv6 link layer address
interface-type	(optional) Specifies interface type
interface-number	(optional) Specifies interface type

Command Default

No default behavior or values.

Command Mode

Global configuration

Usage Guidelines

None

Example

```
Router_config# ipv6 router rip ROUTER
Router_config_rip_ROUTER# neighbor FE80::133 e2/1
```

Related Commands

None

8.1.15 offset

To set the in/out metric of a RIPng instance on an interface, run the first one of the following two commands:

To return to the default value, use the no form of the first command.

offset interface-type interface-number **{in | out}** acl-name value

no offset *interface-type interface-number* **{in | out}** value

Description

interface-type	(optional) designate interface type
interface-number	(optional) designate interface number
in	Adds the metric for an incoming RIPng route.
out	Adds the metric for an outcoming RIPng route.
acl-name	IP access list name
value	Adds the specified metric for the received RIPng route.

Command Default

in The default value of the in parameter is 1.

out The default value of the out parameter is 0.

Command Mode

Global configuration

Usage Guidelines

This command is used to specify the metric for those received and to-be-transmitted RIPng routes.

Example

```
R142_config_e2/1# ipv6 router rip ROUTER
R142_config_rip_ROUTER# offset f0/0 in 10
```

Related Commands

None

8.1.16 passive interface

The command is used to configure passive interface which can receive non-forwarded route update.

passive interface-type interface-number

no passive *interface-type interface-number*

Description

interface-type	(optional) designate interface type
interface-number	(optional) designate interface number

Command Default

No default behavior or values.

Command Mode

Global configuration

Usage Guidelines

None

Example

```
Router_config# ipv6 router rip ROUTER
    Router_config_rip_ROUTER# passive e2/1
```

Related Commands

None

8.1.17 Port

To set a specific UDP interface and multicast address for the RIPng instance, run the following command:

To resume the interface and multicast address to the default setting, run the no form of the command. (521/FF02::9) udp interface numbers of multiple ripng instances cannot be the same, but the multicast addresses are the same.

interface *interface-number* **multicast-group** multicast-address

no interface *interface-number* **multicast-group** multicast-address

Description

The UDP interface ID, a value between 1 and 65535

multicast-group *multicast address*

Command Default

UDP: 521

multicast: FF02::9

Command Mode

RIPNG configuration mode

Usage Guidelines

Specify ripng instance UDP interface and multicast address

Example

Router_config# ipv6 router rip ROUTER

Router_config_rtr_rip# interface 200 multicast-group FF02::9

Related Commands

None

8.1.18 redistribute

To enable other routing domains to forward routes to RIPng, run the first one of the following two commands; to disable this feature, run the no form of the first command.

redistribute protocol [*protocol-id*] [*as-number*] [**route-map** *map-name*]

no redistribute protocol [*protocol-id*] [*as-number*] [**route-map**]

Description

Parameters	Description
Protocol	The type of the forwarded protocol
protocol-id	The ID of the forwarded process

Command Default

Disable

Command Mode

Global configuration

Usage Guidelines

None

Example

None

Related Commands

None

8.1.19 show ipv6 rip

To show the RIPng related information, run the following command: **show ipv6 rip** [*name*] [**database | next-hops**]

Description

Name	(optional) Name of RIP process
Database	(optional) Specifies the details of RIP routing table
Next-hop	Shows the designated detail of RIP process next hop address

Command Default

No default behavior or values.

Command Mode

Any non-user mode

Usage Guidelines

None

Example

```
 Router_config# #show ipv6 rip
RIP process "fsb1"， interface 252， multicast-group FF02::9， pid 147
    Administrative distance is 120.  Maximum paths is 16
    Updates every 30 seconds， expire after 180
    Holddown lasts 0 seconds， garbage collect after 120
    Split horizon is on; poison reverse is off
    Default routes are generated
    Periodic updates 229， trigger updates 6
    Interfaces:
    FastEthernet0/0
    FastEthernet0/1
    Loopback252
    Loopback152
    Redistribution:
    None.
RIP process "fsb2"， interface 152， multicast-group FF02::9， pid 151
    Administrative distance is 120.  Maximum paths is 16
    Updates every 30 seconds， expire after 180
    Holddown lasts 0 seconds， garbage collect after 120
    Split horizon is on; poison reverse is off
    Default routes are not generated
    Periodic updates 231， trigger updates 3
    Interfaces:
    FastEthernet0/0
    Redistribution:
```

None.

Related Commands

None

8.1.20 show ipv6 rip interface

Show ripng configuration information of an interface

show ipv6 rip interface [*interface-type interface-num*]

Description

Interface	Show the interface information of RIPng
interface-type	*interface type*
interface-num	designate interface number

Command Default

No default behavior or values.

Command Mode

Non-user mode

Usage Guidelines

None

Example

The following example shows information about RIPng interface:

```
Router# show ipv6 rip interface
Loopback132 is up, line protocol is up
RIPng is not enabled on this interface
Fastethernet0/0 is up, line protocol is up
RIPng is not enabled on this interface
Ethernet1/1 is down, line protocol is down
RIPng is not enabled on this interface
Ethernet2/1 is up, line protocol is up
Routing Protocol: RIPng
Passive interface: Disabled
Split horizon: Enabled with Poisoned
Reversed IP interface address:
3ffe:ffff::1/64
3ffe:fffe::1/64
```

Related Commands

None

8.1.21 timers

To adjust the timeout value in each clocks in RIPng, run the first one of the following two commands. To return to the default value, use the no form of the first command.

timers basic/update/timeout/garbage value

no timers basic/*update/timeout/garbage*

Description

Update	Specifies the interval, in seconds, that routing updates are transmitted.
Timeout	Specifies the routing information timeout timer in seconds.
Garbage	Specifies the routing garbage-collection timer in seconds.

Command Default

Update	30s
Timeout	180s
Garbage	120s

Command Mode

Global configuration

Usage Guidelines

None

Example

None

Related Commands

None

Chapter 9 rtv6 Configuration Command Contents

9.1 rtv6 Configuration Commands

- **clear ipv6 route static**
- **debug ipv6 routing**
- **ipv6 route cache-check**
- **ipv6 route default**
- **ipv6 route equal-cost-paths**
- **ipv6 route max-number**
- **ipv6 route**
- **show ipv6 route**

9.1.1 clear ipv6 route static

To clear the static route, run **clear ipv6 route static**. clear ipv6 route static

Description

None

Command Default

No default behavior or values.

Command Mode

EXEC

Usage Guidelines

The command can be used to clear static route.

Example

None

Related Commands

None

9.1.2 debug ipv6 routing

To trace ipv6-routing process, run **debug ipv6 routing**. To disable this feature, use the no form of the command.

debug ip routing [message **|** search **|** timer]

no debug ip routing [message **|** search **|** timer]

Description

message (optional) trace the receiving and forwarding of the routing information search (optional) trace the search of route

timer (optional) trace routing clock information

Command Default

No default behavior or values.

Command Mode

EXEC

Usage Guidelines

This command can be used to trace the main procedures of RIPNG.

Example

The following example shows the routing processing information.

Add an ipv6 address to interface e0/1

```
Router#debug ipv6 routing
2004-1-1 22:53:50 Rtv6: Receive msg NSM_MSG_ADDR_ADD[e0/1: aid=0, net=fc01::1/64] from Ipv6.
2004-1-1 22:53:50 Rtv6: Send msg NSM_MSG_ADDR_ADD[e0/1: aid=0, net=fc01::1/64] to PMs.
2004-1-1 22:53:50 Rtv6: Receive msg NSM_MSG_ROUTE_ADD[fc01::1/128] from PM Direct.
2004-1-1 22:53:50 Rtv6: Direct add fc01::1/128 to main routing table.
2004-1-1 22:53:50 Rtv6: Send msg NSM_MSG_ROUTE_CHG_NOTIFY[Add : fc01::1/128] to PMs.
2004-1-1 22:53:50 Rtv6: Receive msg NSM_MSG_ROUTE_ADD[fc01::/64] from PM Direct.
2004-1-1 22:53:50 Rtv6: Direct add fc01::/64 to main routing table.
2004-1-1 22:53:50 Rtv6: Send msg NSM_MSG_ROUTE_CHG_NOTIFY[Add : fc01::/64] to PMs.
```

Related Commands

None

9.1.3 ipv6 route cache-check

To check route cache when hoping to delete the route, run **ipv6 route cache-check**. To disable this feature, use the no form of the command.

ipv6 route cache-check

no ipv6 route cache-check

Description

None

Command Default

No default behavior or values

Command Mode

Global configuration

Usage Guidelines

The command shows how to check route cache.

Related Commands

None

9.1.4 ipv6 route default

To configure ipv6 default route, **runipv6 route default**. To disable this feature, use the no form of the command.

ipv6 route default [Ethernet **|** Serial **|** Null **|** X:X:X:X::X]

no ipv6 route default

Description

Ethernet:	Ethernet interface
Serial:	synchronous/asynchronous serial interface
Null:	Null interface
X:X:X:X::X	gateway address

Command Default

No default behavior or values.

Command

Global configuration

Usage Guidelines

No default behavior or values.

Example

None

Related Commands

None

9.1.5 ipv6 route equal-cost-paths

To configure the equivalent maximum item of ipv6 route equal-cost-paths, run **ipv6 route equal-cost-paths**. To delete the configuration, run the no form of the command.

ipv6 route equal-cost-paths ***value***

no ipv6 route equal-cost-paths

Description

value	corresponding items(<1~6>)

Command Default

the equivalent routing items are

6 Command Mode

Global configuration

Usage Guidelines

None

Example

None

Related Commands

None

9.1.6 ipv6 route max-number

To configure the maximum routing item, run **ipv6 route max-number**. To disable this feature, use the no form of the command.

pv6 route max-number {***value1*** **|** static ***value2*** **|** dynamic ***value3*** }

Description

value1:	max route number
value2:	max static route number
value3:	max dynamic route number

Command Default

The maximum route number is 128000.

The maximum static route number is 10000.

The maximum dynamic route number is 64000.

Command Mode

Global configuration

Usage Guidelines

None

Example

None

Related Commands

None

9.1.7 ipv6 route

To configure the static route, run **ipv6 route**. To disable this feature, use the no form of the command.

ipv6 route ***dest_address*** { Ethernet **|** Serial **|** Null **|** ***gateway_address*** } ***[distance***]

no ipv6 route

Description

dest_address:	destination address(X:X:X:X::X/<0-128>)
Ethernet:	Ethernet interface
Serial:	synchronous/asynchronous serial interface
Null:	Null interface
Gateway_address	gateway address (X:X:X:X::X)
Distance:	management distance

Command Default

No default behavior or values.

Command Mode

Global configuration

Usage Guidelines

None

Example

None

Related Commands

None

9.1.8 show ipv6 route

To show the route details, run **show ipv6 route**.

show ipv6 route [all **|** bgp **|** connect **|** information **|** ospf **|** rip **|** static **|**summary **|** ***dest_address*** **|** <cr>]

Description

All:	show all routes in the routing table
Bgp	show BGP protocol route
Connect	show direct route
Information	show route information
Ospf	show OSPF protocol route
Rip	show rip protocol route
Static	show static route
Summary	show the summary of the routing table
Dest_address	show all routes of destination IPv6 address(format: X:X:X:X::X)

Command Default

No default behavior or values.

Command

Global configuration, EXE

Usage Guidelines

None

Example

None

Related Commands

None

Chapter 10 NATPT Protocol Configuration Commands

10.1 NATPT Protocol Configuration Commands

IPv6 configuration commands include the following ones:

- ipv6 nat
- ipv6 nat max-entries
- ipv6 nat prefix
- ipv6 nat prefix v4-mapped
- ipv6 nat translations
- ipv6 nat v4v6 pool
- ipv6 nat v4v6 source
- ipv6 nat v6v4 pool
- ipv6 nat v6v4 source

10.1.1 ipv6 nat

To enable NATPT, run **ipv6 nat** in the interface configuration mode. To disable this feature, use the no form of the command.

ipv6 nat

no ipv6 nat

Parameters

None

Command Default

NATPT is disabled.

Command Mode

Interface configuration

Usage Guidelines

The command usually enables NATPT in an IPv4 interface and an IPv6 interface of the router at least.

Example

This example shows how to enable NATPT for an IPv6 interface and an IPv4 interface in the interface configuration mode.

```
interface fastethernet 1/0
  ip address 192.168.30.1
  255.255.255.0 ipv6 nat
!
```

```
interface fastethernet 2/0
  ipv6 address
  2001:0DB8:0:1::1/64 ipv6 nat
!
```

Related Commands

ipv6 address link-local

ipv6 address eui-64

show ipv6 interface

show ipv6 nat translations

10.1.2 ipv6 nat max-entries

To specify the maximum number of Network Address Translation--Protocol Translation (NAT-PT) translation entries stored by the router, use the ipv6 nat max-entries command in global configuration mode. To restore the default number of NAT-PT entries, use the no form of this command.

ipv6 nat max-entries *number*

no ipv6 nat max-entries

Parameters

Parameters	Description
Number	The maximum number of NAT-PT translation entries stored by the router(1-2147483647)

Command Default

Unlimited number of NAT-PT entries.

Command Mode

Global configuration

Usage Guidelines

Use the ipv6 nat max-entries command to set the maximum number of NAT-PT translation entries stored by the router when the router memory is limited, or the actual number of translations is important.

Example

The following example sets the maximum number of NAT-PT translation entries to 1000:

```
ipv6 nat max-entries 1000
```

Related Commands

clear ipv6 nat translations

show ipv6 nat translationss

10.1.3 ipv6 nat prefix

To assign an IPv6 prefix where matching IPv6 packets will be translated using Network Address Translation--Protocol Translation (NAT-PT), use the ipv6 nat prefix command in global configuration or interface configuration mode. To prevent the IPv6 prefix from being used by NAT-PT, use the no form of this command.

ipv6 nat prefix *ipv6-prefix/prefix-length*

no ipv6 nat prefix *ipv6-prefix/prefix-length*

Parameters

Parameters	Description
ipv6-prefix/	This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
prefix-length	The value can only be 96.

Command Default

No IPv6 prefixes are used by NAT-PT.

Command Mode

Global configuration or interface configuration

Usage Guidelines

The ipv6 nat prefix command is used to specify an IPv6 address prefix against which the destination prefix in an IPv6 packet is matched. If the match is successful, NAT-PT will translate the IPv6 packet to an IPv4 packet using the configured mapping rules. Use the ipv6 nat prefix command in global configuration mode to assign a global NAT-PTNAT-PT prefix, or in interface configuration mode to assign a different NAT-PT prefix for each interface. Using a different NAT-PT prefix on several interfaces allows the NAT-PT router to support an IPv6 network with multiple exit points to IPv4 networks.

The priority of IPv6 address configured in the interface configuration mode is higher than that of IPv6 address prefix on in the global configuration mode.

Example

The following example assigns the IPv6 prefix 2001:0DB8:1::/96 as the global NAT-PT prefix:

```
ipv6 nat prefix 2001:0DB8:1::/96
```

The following example assigns the IPv6 prefix 2001:0DB8:2::/96 as the NAT-PT prefix for the Fast Ethernet interface 1/0, and the IPv6 prefix 2001:0DB8:4::/96 as the NAT-PT prefix for the Fast Ethernet interface 2/0:

```
interface fastethernet 1/0
ipv6 address 2001:0DB8:2:1::1/64
  ipv6 nat prefix 2001:0DB8:2::/96
!
```

The following example assigns the IPv6 prefix 2001:0DB8:4::/96 as the NAT-PT prefix for the Fast Ethernet interface 1/0, and the IPv6 prefix 2001:0DB8:4::/96 as the NAT-PT prefix for the Fast Ethernet interface 2/0:

```
interface fastethernet 2/0
```

```
ipv6 address 2001:0DB8:4:1::1/64
ipv6 nat prefix 2001:0DB8:4::/96
```

Related Commands

ipv6 address link-local

ipv6 address eui-64

show ipv6 interface

show ipv6 nat translations

10.1.4 ipv6 nat prefix v4-mapped

To enable an IPv6 address in VLAN interface configuration mode, run **ipv6 address eui-64**. Enable IPv6 protocol on the interface simultaneously. To delete the ipv6 address, run **no ipv6 address eui-64**.

To enable customers to send traffic from their IPv6 network to an IPv4 network without configuring IPv6 destination address mapping, use the ipv6 nat prefix v4-mapped command in global configuration or interface configuration mode. To disable this feature, use the no form of this command.

ipv6 nat prefix *ipv6-prefix/prefix-length* **v4-mapped** *access-list-name*

no ipv6 nat prefix *ipv6-prefix/prefix-length* **v4-mapped** *access-list-name*

Parameters

Parameters	Description
Ipv6-prefix	This argument must be in the form documented in RFC 2373.
prefix-length	The length of the IPv6 address is a decimal value. The value can only be 96.
access-list-name	IPv6 Access Control List Name

Command Default

The function is disabled.

Command Mode

Global configuration or interface configuration

Usage Guidelines

The IPv6 target address of a packet arriving at an interface is checked to discover if it has a NAT-PT prefix that was configured with the ipv6 nat prefix v4-mapped command. If the prefix matches, source address translation is performed. If a rule has been configured for the source address translation, the last 32 bits of the destination IPv6 address is used as the IPv4 destination and a flow entry is created.

Example

In the following example, the access list permits any IPv6 source address with the prefix 2001::/96 to go to the destination with a 2000::/96 prefix. The destination is then translated to the last 32 bit of its IPv6 address; for example: source address = 2001::1, destination address = 2000::192.168.1.1. The destination then becomes 192.168.1.1 in the IPv4 network:

```
ipv6 nat prefix 2000::/96 v4-mapped v4map_acl
ipv6 access-list v4map_acl
  permit ipv6 2001::/96 2000::/96
```

Related Commands

No default behavior or values.

10.1.5 ipv6 nat translations

To set a link-local address in VLAN interface configuration mode and meanwhile enable IPv6 on the interface. To disable this feature, use the no form of this command.

To change the amount of time after which Network Address Translation--Protocol Translation (NAT-PT) translations time out, use the ipv6 nat translation command in global configuration mode. To disable the timeout, use the no form of this command.

ipv6 nat translations {timeout | udp-timeout | dns-timeout | tcp-timeout | finrst-timeout |

icmp-timeout | syn-timeout} {*seconds***}**

no ipv6 nat translations {timeout | udp-timeout | dns-timeout | tcp-timeout | finrst-timeout | icmp-timeout | syn-timeout}

Parameters

Parameters	Description
time-out	Specifies that the timeout value applies to dynamic translations. Default is 86400 seconds (24 hours).
udp-timeout	Specifies that the timeout value applies to the User Datagram Protocol (UDP) interface. Default is 300 seconds (5 minutes).
dns-timeout	Specifies that the timeout value applies to connections to the Domain Naming System (DNS). Default is 60 seconds.
tcp-timeout	Specifies that the timeout value applies to the TCP interface. Default is 86400 seconds (24 hours).
finrst-timeout	Specifies that the timeout value applies to Finish and Reset TCP packets, which terminate a connection. Default is 60 seconds.
icmp-timeout	Specifies the timeout value for Internet Control Message Protocol (ICMP) flows. Default is 60 seconds.
syn-timeout	Specifies that the timeout value applies when a TCP SYN (request to synchronize sequence numbers used when opening a connection) flag is received but the flag is not followed by data belonging to the same TCP session.
seconds	The default is 0.

Command Default

timeout: 86400 seconds (24 hours)

udp-timeout: 300 seconds (5 minutes)

dns-timeout: 60 seconds (1 minute)

tcp-timeout: 86400 seconds (24 hours)

finrst-timeout: 60 seconds (1 minute)

icmp-timeout: 60 seconds (1 minute)

Command Mode

Global configuration

Usage Guidelines

If you run no ipv6 address, which has no parameters, all manually configured IPv6 addresses on the interface will be deleted. If you run ipv6 enable, a link-local address will be automatically set. Of course you can set the link-local address manually, the command you will use is ipv6 address link-local.

Dynamic translations time out after a period of time without any translations. The default timeout period is 24 hours. When interface translation is configured, there is finer control over translation entry timeouts because each entry contains more context about the traffic that is using it.

Example

The following example causes UDP interface translation entries to time out after 10 minutes:

ipv6 nat translations udp-timeout 600

Related Commands

clear ipv6 nat translations

show ipv6 nat translations

10.1.6 ipv6 nat v4v6 pool

To define a pool of IPv6 addresses for Network Address Translation - Protocol Translation (NAT-PT), use the ipv6 nat v4v6 pool command in global configuration mode. To remove one or more addresses from the pool, use the no form of this command.

ipv6 nat v4v6 pool *name start-ipv6 end-ipv6* **prefix-length** *prefix-length* **no**

ipv6 nat v4v6 pool *name start-ipv6 end-ipv6* **prefix-length** *prefix-length*

Parameters

Parameters	Description
name	Name of the pool
start-ipv6	Starting IPv6 address that defines the range of IPv6 addresses in the address pool.
end-ipv6	Ending IPv6 address that defines the range of IPv6 addresses in the address pool.

prefix-length	Specifies the subnet of the network to which the pool addresses belong.

Command Default

No pool of addresses is defined.

Command Mode

Global configuration

Usage Guidelines

This command defines a pool of IPv6 addresses using start address, end address, and prefix length. The pool is used when NAT-PT needs a dynamic mapping of an IPv6 address to translate an IPv4 address.

Example

The following example configures a dynamic NAT-PT mapping to translate IPv4 addresses to IPv6 addresses using a pool of IPv6 addresses named v6pool. The packets to be translated by NAT-PT are filtered using an access list named pt-list2.

```
interface Ethernet3/1
 ipv6 address
 2001:0DB8:AABB:1::9/64 ipv6 enable
 ipv6 nat
!
interface Ethernet3/3
 ip address 192.168.30.9
 255.255.255.0 ipv6 nat
!
ipv6 nat v4v6 source list pt-list2 pool v6pool
ipv6 nat v4v6 pool v6pool 2001:0DB8:EEFF::1 2001:0DB8:EEFF::2 prefix-length 128
ipv6 nat prefix 2001:0DB8:EEFF::/96
!
access-list pt-list2 permit 192.168.30.0 0.0.0.255
```

Related Commands

clear ipv6 nat translations

show ipv6 nat translations

10.1.7 ipv6 nat v4v6 source

To configure IPv4 to IPv6 address translation using Network Address Translation--Protocol Translation (NAT-PT), use the ipv6 nat v4v6 source command in global configuration mode. To disable this feature, use the no form of this command.

ipv6 nat v4v6 source {list {*access-list-number* **|** *name*} **pool** *name* **|** *ipv4-address ipv6-address*}

no ipv6 nat v4v6 source {list {*access-list-number* **|** *name*} **pool** *name* **|** *ipv4-address ipv6-address*}

Parameters

Parameters	Description
list *access-list-number*	IPv4 Access Control List Name Standard IP access list number. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
list *name*	IPv4 Access Control List Name Standard IP access list number. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
pool *name*	Name of the pool from which global IP addresses are allocated dynamically.
ipv4-address	Sets up a single static translation. This argument establishes the local IP address assigned to a host on the inside network.
ipv6-address	Sets up a single static translation. This argument establishes the globally unique IP address of an inside host as it appears to the outside world.

Command Default

No NAT-PT translation of IPv4 to IPv6 addresses occurs.

Command Mode

Global configuration

Usage Guidelines

This command has two forms: dynamic and static address translation. The form with an IPv6 access list establishes dynamic translation. Packets from IPv4 addresses that match the standard access list are translated using IPv6 addresses allocated from the pool named with the ipv6 nat v4v6 pool command. The access list is used to specify which traffic is to be translated.

Example

```
interface Ethernet3/1
 ipv6 address
 2001:0DB8:AABB:1::9/64 ipv6 enable
 ipv6 nat
!
interface Ethernet3/3
 ip address 192.168.30.9
 255.255.255.0 ipv6 nat
!
ipv6 nat v4v6 source list pt-list2 pool v6pool
ipv6 nat v4v6 pool v6pool 2001:0DB8:EEFF::1 2001:0DB8:EEFF::2 prefix-length 128
ipv6 nat prefix 3ffe:c00:yyyy::/96
!
access-list pt-list2 permit 192.168.30.0 0.0.0.255
```

The following example shows a static translations where the IPv4 address 192.168.30.1 is translated into

the IPv6 address 2001:0DB8:EEFF::2:

```
ipv6 nat v4v6 source 192.168.30.1 2001:0DB8:EEFF::2
```

Related Commands

clear ipv6 nat translations

ipv6 nat v4v6 pool

ipv6 nat v6v4 source

show ipv6 nat translations

10.1.8 ipv6 nat v6v4 pool

To define a pool of IPv4 addresses for Network Address Translation--Protocol Translation (NAT-PT), use the ipv6 nat v6v4 pool global configuration command. To disable this feature, use the no form of this command.

ipv6 nat v6v4 pool *name start-ipv4 end-ipv4* **prefix-length** *prefix-length* **no**

ipv6 nat v6v4 pool *name start-ipv4 end-ipv4* **prefix-length** *prefix-length*

Parameters

Parameters	Description
name	Name of the pool
start-ipv4	Starting IPv4 address that defines the range of IPv4 addresses in the address pool.
end-ipv4	Ending IPv4 address that defines the range of IPv4 addresses in the address pool.
prefix-length	Specifies the subnet of the network to which the pool addresses belong.

Command Default

No pool of addresses is defined.

Command Mode

Global configuration

Usage Guidelines

This command defines a pool of IPv4 addresses using start address, end address, and prefix length. The pool is used when NAT-PT needs a dynamic mapping of IPv4 addresses to translate IPv6 addresses.

Example

The following example configures a dynamic NAT-PT mapping to translate IPv6 addresses to IPv4 addresses using a pool of IPv4 addresses named v4pool. The packets to be translated by NAT-PT are filtered using an IPv6 access list named pt-list1.

```
interface Ethernet3/1
 ipv6 address
 2001:0DB8:AABB:1::9/64 ipv6 enable
 ipv6 nat
!
```

```
interface Ethernet3/3
  ip address 192.168.30.9
  255.255.255.0 ipv6 nat
!
ipv6 nat v4v6 source 192.168.30.1 2001:0DB8:EEFF::2
ipv6 nat v6v4 source list pt-list1 pool v4pool
ipv6 nat v6v4 pool v4pool 10.21.8.1 10.21.8.10 prefix-length 24
ipv6 nat prefix 2001:0DB8:EEFF::/96
!
ipv6 access-list pt-list1
  permit ipv6 2001:0DB8:AABB:1::/64 any
```

Related Commands

clear ipv6 nat translations

show ipv6 nat translations

10.1.9 ipv6 nat v6v4 source

To configure IPv4 to IPv6 address translation using Network Address Translation--Protocol Translation (NAT-PT), use the ipv6 nat v4v6 source command in global configuration mode. To disable this feature, use the no form of this command.

ipv6 nat v6v4 source { list {*access-list-number* | *name*} **pool** *name* | *ipv6-address ipv4-address*} **[overload] } | { interface** *interface-name* **overload }**

no ipv6 nat v6v4 source { list {*access-list-number* | *name*} **pool** *name* | *ipv6-address ipv4-address*} **[overload] } | { interface** *interface-name* **overload }**

Parameters

Parameters	Description
list *access-list-number*	IPv4 Access Control List Name Standard IP access list number. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
list *name*	IPv4 Access Control List Name Standard IP access list number. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
pool *name*	Name of the pool from which global IP addresses are allocated dynamically.
interface *interface-name*	Specifies the main IP address of the interface as IPv4 packet source address.
ipv4-address	Sets up a single static translation. This argument establishes the local IP address assigned to a host on the inside network.
ipv6-address	Sets up a single static translation. This argument establishes the globally unique IP address of an inside host as it appears to the outside world.
overload	Enables multiplexing of IPv6 addresses to a single IPv4 address for TCP, UDP, and ICMP.

Command Default

No NAT-PT translation of IPv4 to IPv6 addresses occurs.

Command Mode

Global configuration

Usage Guidelines

This command has two forms: dynamic and static address translation. The form with an IPv6 access list establishes dynamic translation. Packets from IPv4 addresses that match the standard access list are translated using IPv6 addresses allocated from the pool named with the ipv6 nat v4v6 pool command. The access list is used to specify which traffic is to be translated.

Example

```
interface Ethernet3/1
  ipv6 address3
  ffe:aaaa:bbbb:1::9/64 ipv6 enable
  ipv6 nat
!
interface Ethernet3/3
  ip address 192.168.30.9
  255.255.255.0 ipv6 nat
!
ipv6 nat v6v4 source list pt-list1 pool v4pool
ipv6 nat v6v4 pool v4pool 10.21.8.1 10.21.8.10 prefix-length 24
ipv6 nat prefix 3ffe:c00:::/96
!
ipv6 access-list pt-list1
  permit ipv6 3ffe:aaaa:bbbb:1::/64 any
```

Static Translations for a Single Address Example

The following example shows a static translations where the IPv6 address 3ffe:aaaa:bbbb:1::1 is translated into the IPv4 address 10.21.8.10:

```
ipv6 nat v6v4 source 3ffe:aaaa:bbbb:1::1 10.21.8.10 Port
```

Address Translations to a Single Address Example

```
ipv6 nat v6v4 pool v6pool 128.1.1.1 128.1.1.10 subnetmask 255.255.255.0
ipv6 nat v6v4 source list v6list interface e1 overload
ipv6 accesslist v6list
permit 3000::/64 any
```

Related Commands

clear ipv6 nat translations

ipv6 nat v4v6 pool

ipv6 nat v6v4 source

show ipv6 nat translations

debug ipv6 nat

Chapter 11 NATPT Configuration Commands

11.1 NATPT Configuration Commands

IPv6 configuration commands include following ones:

- debug ipv6 nat
- show ipv6 nat translations
- show ipv6 nat statistics
- show ipv6 nat pools
- clear ipv6 nat translations

11.1.1 debug ipv6 nat

To show debug messages for Network Address Translation--Protocol Translation (NAT-PT) translation events, use the debug ipv6 nat command in privileged EXEC mode. To disable debug messages for NAT-PT translation events, use the no form of this command.

debug ipv6 nat [detailed]

no debug ipv6 nat [detailed]

Parameters

No default behavior or values.

Command Default

The debug information is closed in default state.

Command Mode

EXEC

Usage Guidelines

The debug ipv6 nat command can be used to troubleshoot NAT-PT translation issues. If no keywords are specified, debugging messages for all NAT-PT protocol translation events are displayed.

Example

Enable NATP Debugging Information:

```
debug ipv6 nat
```

Related Commands

None

11.1.2 show ipv6 nat translations

Shows active NAT-PT translations.

show ipv6 nat translationss [icmp | tcp | udp] [verbose]

Parameters

Parameters	Description
icmp	Shows detailed information about NAT-PT ICMP translation events.
tcp	Shows detailed information about NAT-PT TCP translation events.
udp	Shows detailed information about NAT-PT User Datagram Protocol (UDP) translation events.
verbose	Shows additional information for each translation table entry, including how long ago the entry was created and used.

Command Mode

EXEC

Example

The following is sample output from the show ip nat translations command:

Router# show ipv6 nat translations

Related Commands

show ipv6 nat translations

11.1.3 show ipv6 nat statistics

The following is sample output from the show ipv6 nat statistics command:

show ipv6 nat statistics

Parameters

None

Command Mode

EXEC

Example

The following is sample output from the show ipv6 nat statistics command: Router# show ipv6 nat statistics

Related Commands

show ipv6 nat translations

11.1.4 show ipv6 nat pools

The following is sample output from the show ipv6 nat pools

command: **show ipv6 nat pools [***name***]**

Parameters

Parameters	Description
name	Shows the pool name

Command Mode

EXEC

Usage Guidelines

If do not specify the name of the pool, show information of all address pools.

Example

The following is sample output from the Router# show ipv6 nat pools

command: Router# show ipv6 nat pools

The following is sample output from the Router# show ipv6 nat pools v4pool command (the name of the address pool is v4pool):

Router# show ipv6 nat pools v4pool

Related Commands

show ipv6 nat translations

11.1.5 clear ipv6 nat translations

Clear dynamic NAT-PT translations from the translation table.

clear ipv6 nat translations *

Parameters

None

Command Mode

EXEC

Example

The following is sample to clear dynamic NAT-PT translations from the translation table. Router# clear ipv6 nat translations *