IPv6 Configuration Commands

Table of Contents

Chapter 1 IPv6 Configuration Commands

1.1 IPv6 Configuration Commands

IPv6 configuration commands include:

- 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

Syntax

To set an IPv6 address in port configuration mode and meanwhile enable IPv6 on a port, run ipv6 address { ipv6-address/prefix-length | general-prefix prefix-name sub-bits/prefix-length }. To delete the IPv6 address on a port, run no ipv6 address [ipv6-address/prefix-length | general-prefix prefix-name sub-bits/prefix-length].

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

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

Parameters

Parameters	Description
ipv6-address	Means the to-be-added IPv6 address.
/prefix-length	Means the IPv6 prefix' length. It is a decimal value behind the symbol "/", meaning the successive bits in the network part in an address.
Prefix-name	Means a general prefix, defining the network part of the IPv6 address.

Sub-bits	Means the host part of the IPv6 address. It combines with the prefix, which
	is defined by prefix-name, to form an IPv6 address. This parameter must support the IPv6 address format regulated in RFC2373.

Default Value

No default IPv6 address exists on the VLAN port.

Command Mode

VLAN interface configuration mode

Usage Guidelines

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

Example

The following example shows how to set an IPv6 address in VLAN port configuration mode and meanwhile enable IPv6 on the VLAN port.

Switch_config_v1# ipv6 address 2001:0:0:0:0DB8:800:200C:417A/64

Related   Command   **ipv6**

address anycast ipv6

address   eui-64   ipv6

address   link-local

show ipv6 interface

1.1.2   ipv6 address anycast

Syntax

To set an anycast address, run ipv6 address ipv6-prefix/prefix-length anycast in interface configuration command. Meanwhile, the command can enable IPv6 protocol of the VLAN interface. To delete an anycast address, run no ipv6 address
[ipv6-prefix/prefix-length anycast].

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

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

Parameters

Parameters	Description
lpv6-prefix	Means the network part of the IPv6 address.
/prefix-length	Means the IPv6 prefix' length. It is a decimal value behind the symbol "/", meaning the successive bits in the network part in an address.

Default Value

The command is used to set as an anycast address on the VLAN port by default.

Command Mode

VLAN interface configuration mode

Usage Guidelines

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

Example

Switch_config_v1# ipv6 address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE/64 anycast

Related   Command   **ipv6**

address   eui-64   ipv6

address   link-local

show ipv6 interface

1.1.3   ipv6 address autoconfig

Syntax

To use the stateless auto-configuration protocol to set an IPv6 address, run ipv6 address autoconfig in VLAN port configuration mode. Meanwhile, the command can enable IPv6 protocol of the VLAN interface. To delete the automatically configured address, run no ipv6 address autoconfig. **lpv6 address autoconfig no ipv6 address autoconfig**

Parameters

None

Default Value

By default, IPv6 address auto-configuration is not used.

Command Mode

VLAN interface configuration mode

Example

Switch_config_v1# ipv6 address autoconfig

1.1.4 ipv6 address eui-64

Syntax

To set an IPv6 address in VLAN port configuration mode, run ipv6 address eui-64. Meanwhile, the command can enable IPv6 protocol of the VLAN interface. To delete the configuration, run no ipv6 address eui-64. **ipv6 address** *ipv6-prefix/prefix-length* **eui-64 no ipv6 address [** *ipv6-prefix/prefix-length* **eui-64]**

Parameters

Parameters	Description
Ipv6-prefix	Means the network part of the IPv6 address.
/prefix-length	Means the IPv6 prefix' length. It is a decimal value behind the symbol "/", meaning the successive bits in the network part in an address.

Default Value

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

Command Mode

VLAN interface configuration mode

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

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

Example

Switch_config_v1# ipv6 address 2001:0:0:0:0DB8::/64 eui-64

Related Command

ipv6 address link-local   show ipv6 interface

1.1.5   ipv6 address link-local

Syntax

To set a link-local address in VLAN port configuration mode and meanwhile enable IPv6 on the VLAN port, run the first one of the following two commands: To delete link-local address, run no ipv6 address [ipv6-address link-local].

ipv6 address *ipv6-address* **link-local no**

ipv6 address [*ipv6-address* **link-local]**

Parameters

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

Default Value

No default IPv6 link-local address exists on the VLAN port.

Command Mode

VLAN interface configuration mode

If you run no ipv6 address, which has no parameters, all manually configured IPv6 addresses on the VLAN port 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 port:

Switch_config_v1# ipv6 address FE80::A00:3EFF:FE12:3457 link-local

Related Command **ipv6**

address   eui-64

show ipv6 interface

1.1.6   ipv6 enable

Syntax

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

ipv6 enable no

ipv6 enable

Parameters

None

Default Value

The IPv6 protocol is forbidden on the VLAN port.

Command Mode

VLAN interface configuration mode
After the ipv6 enable command is run, the system will add a link-local address on the VLAN port automatically. At the same time, the communication range of the IPv6

protocol on the VLAN port is confined to the links that the VLAN port connects. If the IPv6 address has already configured on the VLAN port explicitly, you cannot forbid IPv6 processing on the VLAN port even though you use the no ipv6 enable command.

Example

Switch_config# interface vlan 1
Switch_config_v1# ipv6 enable

Related Command

ipv6 address link-local

ipv6   address   eui-64

show ipv6 interface

1.1.7   show ipv6 interface

Syntax

To show the information about the VLAN port on which the IPv6 protocol is enabled, run the following command: **show ipv6 interface [** *interface-type interface-number* **] | [brief]**

Parameters

Parameters	Description
interface-type	Stands for the type of the VLAN interface port.
interface-number	Stands for the ID of the VLAN port.

Default Value

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

Command Mode

Global configuration mode

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

Example

The following example shows how to display the IPv6 state on port vlan1:

Switch# show ipv6 interface vlan 1

Vlan1 is up, 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
Vlan1 is up(down/administratively down)	Indicates whether the physical layer of the VLAN port 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	Displays the link-local address of a port.
Global unicast address(es):	Displays the unicast address of a port.
Joined group address(es)	Displays the multicast address of a port.
MTU	Displays the MTU of a port.
ICMP error messages	Displays the transmission frequency of ICMPv6 error packets (the minimum interval).
ICMP redirects	Displays whether the redirection packet will be sent or not.
ICMP unreachables	Displays whether the destination unreachable packet will be enabled or shut down.

Related Command

None

Chapter 2 IPv6 Configuration Commands

2.1 IPv6 Configuration Commands

IPv6 configuration commands include the following ones:

- clear ipv6 traffic

- debug ipv6 packet

- ipv6 mtu

- ipv6 redirect

- ipv6 access-group

- ipv6 unreachables

- ipv6 route default

- show ipv6 general-prefix

- show ipv6 pmtu

- show ipv6 traffic

2.1.1 clear ipv6 traffic

Syntax

To delete the statistics information about the IPv6 flow, run the following command: **clear ipv6 traffic**

Parameters

None

Command Mode

EXEC

Usage Guidelines

This command is used to delete all the statistics information about IPv6 flow.

Example

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

```
Switch# clear ipv6 traffic
Switch# 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 report, 0 membership reduction
        0 Switch solicitations, 0 Switch 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 report, 0 membership reduction
        0 Switch solicitations, 0 Switch advertisements
        0 neighbor solicitations, 0 neighbor advertisements, 0 redirect
```

Related Command

show ipv6 traffic

2.1.2   debug ipv6 packet

Syntax

To display the debug information about the IPv6 packet, run the first one of the following two commands: To disable the input of debug information, run no debug ipv6 packet.
debug ipv6 packet [interface *interface-type interface-number* | **access-list**
[access-list-name] | **detail] no**

debug ipv6 packet

Parameters

Parameters	Description
Interface-type	(Optional)The type of the VLAN port.
Interface-number	ID of an interface (optional)
access-list-name	Name of ACL (optional)

Default Value

The debug information is closed in default state.

Command Mode

EXEC

Example

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

Switch# 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	Displays packet transmission, reception and forwarding on an interface

2.1.3   ipv6 mtu

To set the MTU of the VLAN port, run the first one of the following two commands: To return to the default setting, run no ipv6 mtu.

ipv6 mtu *bytes* **no**

ipv6 mtu

Parameters

Parameters	Description
bytes	Stands for MTU, whose unit is byte.

Default Value

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

Command Mode

VLAN interface configuration mode

Usage Guidelines

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

When a switch 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 a port:

Switch_config_v1# ipv6 mtu 1400

Related Command

2.1.4 ipv6 redirects

To control whether to transmit a redirection packet after the packet is forwarded, run ipv6 redirects. To return to the default setting, use no ipv6 redirects.

ipv6 redirects   no

ipv6 redirects

Parameters

None

Default Value

The redirection packet will be transmitted by default.

Command Mode

VLAN interface configuration mode

Usage Guidelines

The redirection packets are transmitted through the ICMPv6 protocol.

Example

The following example shows how to shut down a port to transmit the redirection packet.

Switch_config_v1# no ipv6 redirects

To observe whether redirection packets are forwarded, run command show ipv6 interface.

Related Command

show ipv6 interface

2.1.5 ipv6 access-group

To filter the receiving and forwarding packets of a port, run ipv6 access-group. To disable the function, run no ipv6 access-group. **ipv6 access-group** *access-list-name* **{ in | out } no ipv6 access-group { in | out }**

Parameters

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

Default Value

Filtration function is not configured by default.

Command Mode

VLAN interface configuration mode

Usage Guidelines

Example

The following example shows how to use access list test to filter received packet on interface vlan 1.

Switch_config_v1# ipv6 access-group test in

Related Command

Ipv6 access-list

Show ipv6 interface

2.1.6   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

Default Value

Allows IPv6 to transmit the destination unreachable packets.

Command Mode

VLAN interface configuration mode

Usage Guidelines

The destination unreachable packets are forwarded by ICMPv6 protocol.

Example

The following example shows how to shut down the VLAN port to transmit the redirection packet.

Switch_config_v1# no ipv6 unreachables

To observe whether destination unreachable packets are forwarded, run command show ipv6 interface.

Related Command

None

2.1.7 ipv6 route default

To set the default ipv6 gateway of the switch, run this command.

ipv6 route default [*NULL | X:X:X:X::X]* **no**

ipv6 route default [*NULL | X:X:X:X::X]*

Parameters

Parameters	Description
NULL	NULL interface
X:X:X:X::X	Gateway's address

Default Value

There is no default configuration.

Command Mode

Global configuration mode

Example

The following example shows how to set the address of 2008::1 to the route default of the switch. ipv6 route default 2008::1

Related Command

None

2.1.8 show ipv6 general-prefix

Syntax

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

show ipv6 general-prefix

Parameters

None

Command Mode

EXEC

Example

Switch_config#show ipv6 general-prefix

IPv6 Prefix my-prefix, acquired via manual

2002::/64

Vlan1 (Address command)

Field	Usage Guidelines
IPv6 Prefix	User-defined IPv6 general prefix
Acquire via	Configuration mode of general-prefix Manual configuration and DHCP automatic acquisition are supported now.
Vlan1 (Address command)	Stands for a list of ports that use this general prefix.

Related Command

ipv6 general-prefix

2.1.9 show ipv6 pmtu

Syntax

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

Switch_config#show ipv6 pmtu

PMTU Expired   Destination Address

1300   00:04:00 2002:1::1

1280   12:01:00 AM 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 switches greater than path MTU.

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

Field	Usage Guidelines
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 Command

ipv6 mtu

2.1.10   show ipv6 traffic

Syntax

To show statistics about IPv6 traffic, use the show ipv6 traffic command. **show**

ipv6 traffic

Parameters

None

Command Mode

```
Switch#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 report, 0 membership reduction

        0 Switch solicitations, 0 Switch 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 report, 0 membership reduction   0 Switch solicitations, 0 Switch advertisements

0 neighbor solicitations, 0 neighbor advertisements, 0 redirect

Related Command

clear ipv6 traffic

2.2 Network Testing Tool Commands

IPv6 Network Testing Tool Commands

- ping6

- traceroute6

2.2.1 ping6

Syntax

To test host accessibility and network connectivity, run the following command. After the ping command is run, an ICMP request message is sent to the destination host, and then the destination host returns an ICMP response message. **ping6** *host* [**-a**] [**-l** *length*] [-**n** *number*] [**-v**] [**–w** *waittime*] [-**b** *internal*]

Parameters

Parameters	Description
host	The destination host address or the host name
-a	icmp echo request packets are forwarded continuously until the user stops it manually.
-l *length*	Sets the length of ICMP data in the message. Default: 56 bytes
-n *number*	Sets the total number of messages. Default: 5 messages
-w *waittime*	Time for each message to wait for response Default: 2 seconds
-b *interval*	Sets the time interval of sending ping packet. Unit: 10ms; Value range: 0-65535; Default Value: 0.

Command Mode

EXEC and global configuration mode

Usage Guidelines

Press the Q key to stop the ping command.

Simple output is adopted by default.

Parameters	Description
!	A response message is received.
.	Response message is not received in the timeout time.
U	The message that the ICMP destination cannot be reached is received.
R	The ICMP redirection message is received.
T	The ICMP timeout message is received.
P	The ICMP parameter problem message is received.

The statistics information is exported:

Parameters	Description
packets transmitted	Number of transmitted messages
packets received	Number of received response messages, excluding other ICMPmessages
packet loss	Rate of messages that are not responded to
round-trip min/avg/max	Minimum/average/maximum time of a round trip (ms)

The routing switch supports the destination address to be link-local address or the multicast address. When ping this address, the vlan port must be specified at the end and forward ICMP packets on the specified port. The routing switch is to export the addresses of all response hosts.

Example

switch#ping6 2008::2 -l 10000 -n 30 PING
2008::2 (2008::2): 10000 data bytes

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

--- 2008::2 ping6 statistics ---

30 packets transmitted, 30 packets received, 0% packet loss round-trip
min/avg/max = 0/1/20 ms

·ping multicast address： switch#ping6

ff02::1 vlan 1 -n 2

PING 1 (FF02:1B::1): 56 data bytes

Reply to request 0 from FE80::2E0:FFF:FEDB:583F, <10 ms

Reply to request 0 from FE80::1EAF:F7FF:FE35:D02A, 10 ms

Reply to request 1 from FE80::2E0:FFF:FEDB:583F, <10 ms

Reply to request 1 from FE80::1EAF:F7FF:FE35:D02A, 10 ms

2.2.2   traceroute6

Syntax

To detect which routes have already reached the destination, run the following command.

You can transmit to the destination the UDP packets (or ICMP ECHO packets) of different TTLs to confirm which routes have come to the destination. Each router on this path has to deduct 1 from the TTL value before forwarding ICMP ECHO packets. Speaking from this aspect, TTL is an effective hop count. When the TTL value of a packet is deducted to zero, the router sends back to the source system the ICMP timeout message. Send the first response packet whose TTL is 1 and send TTL plus 1 subsequently until the target reaches to the max TTL.

By checking the ICMP timetout message sent back by inter medial routers, you can confirm the routers. At the arrival of the destination, the traceroute sends a UPD packet whose port ID is larger than 30000; the destination node hence can only transmit back a Port Unreachable ICMP message. This reception of this message means the arrival of destination.

traceroute6 *host* [**-i** *source-ip-address*] [**-p** *port-number*] [**-q** *probe-count*] [**-t** *ttl*] [**-w** *waittime*] [**-x icmp**]

Parameters

Parameters	Description
host	The destination host address or the host name
-i *source-ip-address*	Sets the source address.
-p *port-number*]	Sets the ID of destination port that transmits UDP packets. Default value: 33434 Default: 33434
-q *probe-count*	Sets the number of packets that you detect each time. Default: 3 messages
-t *ttl*	Sets IP TTL of the message to ttl. Default: the minimum and maximum TTLs are 1 and 30 respectively.
-w *waittime*	Time for each message to wait for response Default: 3 seconds

-x icmp	Sets the detection packet to be the ICMP ECHO packet. Default: UDP packet

Command Mode

EXEC and global configuration mode

Usage Guidelines

The UDP packet is used for detection by default, but you can run –x icmp to replace it with ICMP ECHO for detection.

If you want to stop traceroute, press q or Q.By default, the simple output information is as follows.

Simple output is adopted by default.

Parameters	Description
!N	Receives ICMP destination unreachable packets (route unreachable, code: 0)
!P	Receives ICMP destination unreachable packets (management forbid, code: 1)
!S	Receives ICMP destination unreachable packets (not neighbor, code: 2)
!A	Receives ICMP destination unreachable packets (address unreachable, code: 3)
!	Receives ICMP destination unreachable packets (port unreachable, code: 4)

The statistics information is exported:

Parameters	Description
hops max	Means the maximum detection hops (the threshold of ICMP).
byte datalen	Stands for the size of each detection packet.

Example

```
switch#traceroute6 2008::2     tracert6 to 2008::2 ,
30 hops max, 12 byte datalen

 1  2008::2  0 ms * 0 ms
```