IPv6 Configuration

Table of Contents

Chapter 1   IPv6 Protocol's Configuration

1.1   IPv6 Protocol's Configuration

The configuration of the IPv6 address of the router only takes effect on the VLAN interface, not on the physical interface.

The IPv6 protocol is disabled in default state. If the IPv6 protocol need be used on a VLAN interface, this protocol should be first enabled in VLAN interface configuration mode. To enable the IPv6 protocol, users have to set the IPv6 address. If on a VLAN interface at least one IPv6 address is set, the VLAN interface can handle the IPv6 packets and communicates with other IPv6 devices.

To enable the IPv6 protocol, users should finish the following task:

● Setting at least one IPv6 address in VLAN interface configuration mode

1.2   Enabling IPv6

1.2.1   Setting the IPv6 Address

The IPv6 address is used to determine the destination address to which the IPv6 packets can be sent. There are three kinds of IPv6 addresses.

Kind	Referred Format	Remarks
Unicast address	2001:0:0:0:0DB8:800:200C:417A/64	**2001:0:0:0:0DB8:800:200C:417A** stands for a unicast address, while **64** stands for the length of the prefix of this address.
Multicast address	FF01:0:0:0:0:0:0:101	All multicast addresses begin with FF.
Any address	2002:0:0:0:0DB8:800:200C:417A/64	The format of this address is the same as that of the unicast address. Different VLAN interfaces can be set to have the same address, no matter it is a unicast/broadcast/multicast address.

For the further details of the IPv6 address, see RFC 4291.

In order to enable IPv6, users must set a unicast address in VLAN interface configuration mode. The set unicast address must be one or multiple addresses of the following type:

● IPv6 link-local address

● Global IPv6 address

To set an IPv6 link-local address in VLAN interface configuration mode, run the following commands.

Command	Purpose
ipv6 enable	Sets a link-local address automatically.
ipv6 address fe80::x link-local	Sets a link-local address manually.

Note:

● The link-local address must begin with fe80. The default length of the prefix is 64 bit. At manual settings only the values at the last 64 bits can be designated.

● On a VLAN interface can only one link-local address be set.

● After IPv6 is enabled through the configuration of the link-local address, IPv6 only takes effect on the local link.

To set a global IPv6 address in VLAN interface configuration mode, run the following commands.

Command	Purpose
ipv6 address autoconfig	Sets a global address automatically.
ipv6 address [ipv6-address/prefix-length | prefix-name sub-bits/prefix-length] | [eui-64]	Sets a global address.
ipv6 address X:X:X:X::X/<0-128> anycast	Sets an address of unicast/broadcast/multicast.

Note:

● When IPv6 is enabled through the configuration of a global address, all interconnected IPv6 device can be handled by IPv6.

● If a link-local address has not been set before the configuration of the global address, the system will set a link-local address automatically.

Chapter 2　　Setting the IPv6 Services

2.1　Setting the IPv6 Services

After IPv6 is enabled, all services provided by IPv6 can be set. The configurable IPv6 service is shown below:

(1)　　Managing the IPv6 Link

2.1.1　Managing the IPv6 Link

IPv6 provides a series of services to control and manage the IPv6 link. This series of services includes:

(1)　　Setting the transmission frequency of the ICMPv6 packet

(2)　　Setting the source IPv6 route

(3)　　Setting the MTU of IPv6

(4)　　Setting IPv6 redirection

(5)　　Setting IPv6 destination unreachablity

(6)　　Setting IPv6 ACL

(7)　　Setting IPv6 Hop-Limit

1.　Setting the transmission frequency of the ICMPv6 packet

If you want to limit the transmission frequency of the ICMPv6 packet, run the command in the following table. If the ICMPv6 transmission frequency is larger than the set value, the transmission frequency will be limited.

The default transmission frequency is 1000us. If you want to modify the transmission frequency, run the following command in global mode:

Command	Purpose
ipv6 icmp6-ratelimit *ratelimit*	Sets the transmission frequency of the ICMPv6 packet.

2.　Setting the source IPv6 route

IPv6 allows a host to designate the route of an IPv6 network, that is, the source route. The host can realize the source route through using the routing header in the IPv6 packets. The router can

forward packets according to the routing header, or desert this kind of packets considering security.

The router supports the source route by default. If the source route is closed, users can run the following command in global configuration mode to open the source route.

Command	Purpose
ipv6 source-route	Allows the source IPv6 route.

3. Setting the MTU of IPv6

All interfaces have a default IPv6 MTU. If the length of an IPv6 packet exceeds MTU, the router will fragment this IPv6 packet.

To set IPv6 MTU on a specific interface, run the following command in interface configuration mode:

Command	Purpose
ipv6 mtu *bytes*	Sets IPv6 MTU on an interface.

4. Setting IPv6 redirection

Sometimes, the route selected by the host is not the best one. In this case, when a switch receives a packet from this route, the switch will transmit, according to the routing table, the packet from the interface where the packet is received, and forward it to another router which belongs to the same network segment with the host. Under this condition, the switch will notify the source host of sending the packets with the same destination address to another router directly, not by way of the switch itself. The redirection packet demands the source host to replace the original route with the more direct route contained in the redirection packet. The operating system of many hosts will add a host route to the routing table. However, the switch more trusts the information getting from the routing protocol and so the host route will not be added according to this information.

IPv6 redirection is opened by default. However, if a hot standby router protocol is configured on an interface, IPv6 redirection is automatically closed. If the hot standby router protocol is canceled, this function will not automatically opened.

To open IPv6 redirection, run the following command:

Command	Purpose
ipv6 redirects	Allows IPv6 to transmit the redirection packets.

5. Setting IPv6 destination unreachablity

In many cases, the system will automatically transmit the destination-unreachable packets. Users can close this function. If this function is closed, the system will not transmit the ICMP unreachable packets.

To enable this function, run the following command:

Command	Purpose
ipv6 unreachables	Allows IPv6 to transmit the destination unreachable packets.

6. Setting IPv6 ACL

Users can use ACL to control the reception and transmission of packets on a VLAN interface. If you introduce ACL on a VLAN interface in global configuration mode and designate the filtration's direction, the IPv6 packets will be filtered on this VLAN interface.

To filter the IPv6 packets, run the following command in interface configuration mode.

Command	Purpose
ipv6 traffic-filter *WORD* { in	out }	Filters the IPv6 packets in the reception or transmission direction (in: receive; out: transmit) on a VLAN interface.

7. Setting IPv6 Hop-Limit

Users can designate a router to transmit the value of the hop-limit field in the packets (except those forwarded packets). All those packets that this router transmits out, if the upper-level application does not apparently designate a hop-limit value, use the set value of hop-limit. At the same time, the value of the hop-limit field is added to the RA packets that this router transmits.

The default hop-limit value is 64. If you want to change this value, you can run the following command in interface configuration mode.

Command	Purpose
ipv6 cur-hoplimit *value*	Designates a router to transmit the hop-limit field of the packets.

Chapter 3   Configuring the Routing Management Modules

3.1   Overview

The static route is a special route and configured by the administrator manually; after a static route is set the packets with a designated destination will be forwarded along the path that is designated by the administrator.

In those networks with simple networking structures, only the configuration of the static routes can realize network interconnection. Properly setting and using static routes can improve the performance of networks and guarantee the bandwidth for important network application.

The shortage of the static route is that it cannot automatically adapt to the change of the network topology. When the network has trouble or the topology changes, the static routes are unreachable and the network then interrupts. In this case, the network administrator has to change the settings of static routes manually.

If the data packets that reach a designated network cannot find the corresponding items in the routing table in a device, the device will then discard these data packets.

After a default route is configured on the current device, those data packets that have no corresponding items in the routing table will not be discarded by the current device but forwarded to another device, which will forward these data packets.

The default route is used only when a device has not found a matching entry in the routing table.

If the destination address of a packet does not match up any entry in the routing table, this packet will select the default route.

If there is no default route and the destination of the packet is not in the routing table, this packet will be discarded and an ICMPv6 packet will be sent back to the source terminal, reporting that the destination address and the network are unreachable.

The default routes can be generated in two ways:

The first way is that the network administrator sets a static route to network 0::0/0. As to an incoming data packet, if the current device cannot find the corresponding routing item in the routing table, it will forward this packet to the designated next-hop port that is set in the static route.

The second way is that the default route is generated by the dynamic routing protocols. A device with strong routing ability forwards the default route to other devices, and the other devices generate in their own routing tables the default route that is oriented to the device with strong routing ability.

3.2   Configuration Task List of Routing Management Module

The routing management module has the following configuration tasks:

- Setting the static route

- Setting the threshold of routes in a routing table

- Checking whether the next hop of the static route is reachable

3.3 Routing Management Module's Configuration Tasks

3.3.1 Setting the Static Route

To set the static route, run the following command in global configuration mode:

Command	Purpose
Ipv6 route *prefix / prefixlen {ipv6-address | interface-type interface-number [ipv6-address]} [distance]*	Sets the static route.

When setting the static route, you can designate the type and number of the outgoing interfaces, and also the address of the next hop. It depends on actual requirements whether to designate an outgoing interface or the next-hop address. The next-hop address cannot be the IPv6 address of the local address, or the static route is invalid.

When you run **IPv6 route** to set the static route, if the destination address and the mask are set to 0::0/0, the configured route is a default one. The **prefixlen** parameter in the configured prefix should be less than or equal to 64, or be equal to 128 (host's route).

Different management distances can be set for different static routes and therefore these static routes can be flexibly applied on the routing management modules.

The next hop of the configured static route must be activated, otherwise the static route cannot be activated. When the next hop is an interface or an interface VLAN, the interface must be a v6 one; when the next hop is a gateway, this gateway must be in the directly-connected network segment.

3.3.2 Setting the Threshold of Routes in a Routing Table

To a maximum number of routes in a routing table, that is, to set a threshold for routes in a routing table, run the following command in global configuration mode:

Command	Purpose

ipv6 route max-number <64-640000>	Sets the total number of routes, distributes systematic resources reasonably and provides a set speed.

3.3.3 Monitoring and Maintaining the State of the Routing Table

To display all kinds of statistics information about routes, run the following commands in EXEC mode:

| Command	Purpose
show ipv6 route	Displays the information in the main routing table.
show ipv6 route [*protocol*]	Displays the routing information of the corresponding routing protocol in the routing table.

show ipv6 route summary	Displays the statistics information about the main routing table.
show ipv6 fib route	Displays the items in the main forwarding table, FIB.
show ipv6 fib summary	Displays the statistics information about the forwarding table.
Show ipv6 route summary **(line card)**	Displays the statistics information about the routing table on the wire card.
Show ipv6 route information **(line card)**	Displays the information about the current state on the wire card.
**Show ipv6 route [delete	stale	un-lpm	no-lla	ipv6-address]** **(line card)**	Displays all kinds of routing information on the wire card.

To trace all related events and information on the route management module, run the following commands in EXEC mode.

Command	Purpose
debug ipv6 routing message	Traces the reception and transmission of the IPv6 information.
debug ipv6 routing search	Traces routing search.
debug ipv6 routing timer	Traces the IPv6 clock.
Debug ipv6 routing redis	Traces the IPv6-redistribute information.
debug ipv6 fib cache	Traces the IPv6-cache information.
Debug ipv6 fib message	Traces the information in the IPv6 forwarding table.
Debug ipv6 routing exf **(line card)**	Traces the EXF information that is added to the line card.
Debug ipv6 routing packet **(line card)**	Traces the packet interaction information between the wire card and the main-control line card.
Debug ipv6 routing message **(line card)**	Traces the interaction information between the line card and the main control unit.
Debug ipv6 routing cache **(line card)**	Traces the information about the cache on the line card.
Debug ipv6 routing route **(line card)**	Traces the information about route change on the line card.
Debug ipv6 routing search **(line card)**	Traces the routing search information on the line card.

3.4 Static Route's Configuration Example

As shown in the following figure, RA directly connects router RB.
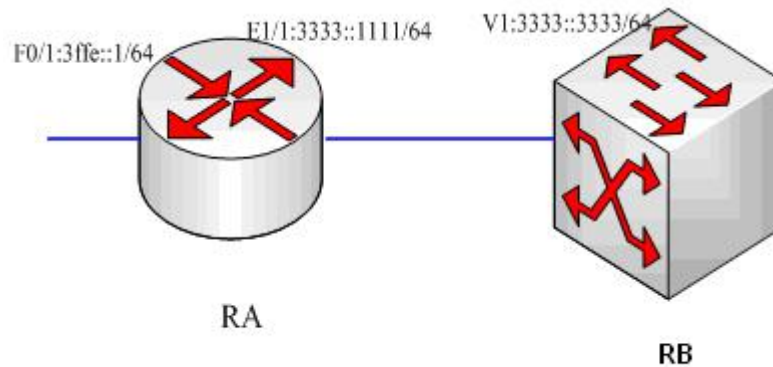
1) RA configuration:

```
interface    FastEthernet0/1
 no ip address

 no  ip   directed-broadcast
 ipv6 address 3FFE::1/64

!
interface    Ethernet1/1
 no ip address

 no  ip   directed-broadcast
 duplex half

 ipv6 address 3333::1111/64

!
```

2) RB configuration:

```
interface    VLAN1
 no ip address

 no  ip   directed-broadcast
 ipv6 address 3333::3333/64

!
```

!

3) Browsing the address of the local link of RA:

RA_config#show ipv6 route

Codes: C - Connected, L - Local, S - Static, R - Ripng, B - BGP

ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2 OE1 - OSPF external type 1, OE2 - OSPF external type 2

DHCP - DHCP type

VRF ID: 0

C   3333::/64[1]

is directly connected, C,Ethernet1/1
C   3333::1111/128[1]

is directly connected, L,Ethernet1/1
C   3ffe::/64[1]

is directly connected, C,FastEthernet0/1

```
C       3ffe::1/128[1]

         is directly connected, L,FastEthernet0/1
C       fe80::/10[1]

         is directly connected, L,Null0

C       fe80::/64[1]

         is directly connected, C,FastEthernet0/1
C       fe80::a00:3eff:fed5:effc/128[1]

         is directly connected, L,FastEthernet0/1
C       fe80::/64[1]

         is directly connected, C,Ethernet1/1
C       fe80::a00:3eff:fed5:effd/128[1]

         is directly connected, L,Ethernet1/1
C       ff00::/8[1]

         is directly connected, L,Null0

 !
```

Setting a static route, which leads to subnet **3ffe::/64** on RB:

!

ipv6 route 3ffe::/64 3333::1111

!

Or:

!

ipv6 route 3ffe::/64 VLAN1 fe80::a00:3eff:fed5:effd

!