Content

CHAPTER 2 COMMANDS FOR ARP SCANNING PREVENTION

CHAPTER 3 COMMANDS FOR PREVENTING ARP, ND SPOOFING

Chapter 1 Commands for Layer 3 Forwarding

Explanation：

The layer 3 switch in this chapter represents the a general sense of router or wireless controller which is running routing protocol.

1.1 Commands for Layer 3 Interface

1.1.1 bandwidth

Command: bandwidth *<bandwidth>*

        no bandwidth

Function: Configure the bandwidth for Interface vlan. The "**no bandwidth**" command recovery the default value. The bandwidth of interface vlan is used to protocol account but not control the bandwidth of port. For instance, it is use the interface bandwidth （cost=10^8/bandwidth） when OSPF account the link cost, so change the bandwidth can result in OSPF link cost changed.

Parameters: *<bandwidth>* is the bandwidth for interface vlan. Range from 1bits to 10000000000 bits. It is can use unit "k, m, g". There are no decimal numbers after conversion.

Command mode: VLAN Interface Mode

Default: The default bandwidth for interface VLAN is 100,000,000bit.

Usage Guide: This command only can be used at interface VLAN mode. The conversion of unit: 1g=1,000m=1,000,000k=1,000,000,000bit.

Example: Configure the bandwidth for vlan1 is 50,000,000bit.

Switch(Config-if-Vlan1)#bandwidth 50m

1.1.2 description

Command: description *<text>*

        no description

Function: Configure the description information of VLAN interface. The no command will cancel the description information of VLAN interface.

Parameter: *<text>* is the description information of VLAN interface, the length should not

exceed 256 characters.

Default: Do not configure.

Command Mode: VLAN interface mode

Usage Guide: The description information of VLAN interface behind description and shown under the configured VLAN.

Example: Configure the description information of VLAN interface as test vlan.

Switch(config)#interface vlan 2

Switch(config-if-vlan2)#description test vlan

1.1.3 interface loopback

Command: interface loopback <*loopback-id*>

          no interface loopback <*loopback-id*>

Function: Create a Loopback interface; the no operation of this command will delete the specified Loopback interface.

Parameters: <*loopback-id*> is the ID of the new created Loopback interface.

Default: There is no Loopback interface in factory defaults.

Command Mode: Global Configuration Mode.

Usage Guide: IDs of the VLANs taken up by a Loopback interfaces start from 1006. If Loopback take up a VLAN whose ID is larger than or equal with1006, users are forbidden to configure the corresponding VLAN. If a VLAN after VLAN 1006 is already configured, such as VLAN 1006, then the Loopback interface will take up the first available VLAN after that VLAN, such as VLAN 1007.

Examples: Enter the interface configuration mode of Loopback 1.

Switch(config)#interface loopback 1

Switch(Config-if-Loopback1)#

1.1.4 interface vlan

Command: interface vlan <*vlan-id*>

          no interface vlan <*vlan-id*>

Function: Create a VLAN interface (a Layer 3 interface); the "**no interface vlan <*vlan-id*>**" command deletes the Layer 3 interface specified.

Parameters: <*vlan-id*> is the VLAN ID of the established VLAN, ranging from 1 to 4094.

Default: No Layer 3 interface is configured upon switch shipment.

Command mode: Global Mode

Usage Guide: When creating a VLAN interface (Layer 3 interface), VLANs should be configured first, for details, see the VLAN chapters. When VLAN interface (Layer 3 interface) is created with this command, the VLAN interface (Layer 3 interface)

configuration mode will be entered. After the creation of the VLAN interface (Layer 3 interface), interface vlan command can still be used to enter Layer 3 Port Mode.

Example: Create a VLAN interface (layer 3 interface).

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#

1.1.5 no interface IFNAME

Command: no interface IFNAME

Function: Delete the interface, deal with the interface vlan and interface loopback only.

Parameters: IFNAME: interface name.

Command Mode: Global mode.

Usage Guide: This command is used to delete the layer 3 interface. It can deal with the situation that the interface name is spelt in special way. IFNAME can match multiple ways, such as vlan1, Vlan1, v1, V1 and etc.

Example: Delete interface vlan1.

(config)# no interface vlan1

1.1.6 shutdown

Command: shutdown

          no shutdown

Function: Shut down the specified VLAN interface of the switch. The no operation of the command will enable the VLAN interface.

Command Mode: VLAN Interface Configuration Mode.

Default: The VLAN interface is enabled by default.

Usage Guide: While shutting down the VLAN interface of the switch, it will not send data frames. If this interface needs to obtain an IP address via BOOTP/DHCP protocol, it should be enabled.

Example: Enable the VLAN1 interface of the switch.

Switch(Config-if-Vlan1)#no shutdown

1.2 Commands for IPv4/v6 configuration

1.2.1 ipv4 hardware forwarding enable

This command is not supported by this switch.

1.2.2 ipv4 hardware forwarding l3 <1-256>

This command is not supported by this switch.

1.2.3 ipv4 hardware forwarding lpm <1-128>

This command is not supported by this switch.

1.2.4 ipv6 hardware forwarding enable

This command is not supported by this switch.

1.2.5 ipv6 hardware forwarding l3 <1-256>

This command is not supported by this switch.

1.2.6 ipv6 hardware forwarding lpm <1-128>

This command is not supported by this switch.

1.2.7 clear ip traffic

Command: clear ip traffic

Function: Clear the statistic information of IP protocol.

Parameter: None.

Command mode: Admin Mode.

Default: None.

Usage guide: Clear the statistic information of receiving and sending packets for IP kernel protocol, including the statistic of receiving packets, sending packets and dropping packets and the error information of receiving and sending packets for IP protocol, ICMP protocol, TCP protocol and UDP protocol.

Example: Clear statistic information of IP protocol.

Switch#clear ip traffic

1.2.8 clear ipv6 neighbor

Command: clear ipv6 neighbors

Function: Clear the neighbor cache of IPv6.

Parameter: None

Command Mode: Admin Mode

Default: None

Usage Guide: This command cannot clear static neighbor.

Example: Clear neighbor list.

Switch#clear ipv6 neighbors

1.2.9 debug ip icmp

Command: debug ip icmp

          no debug ip icmp

Function: The debugging for receiving and sending ICMP packets.

Parameter: None.

Default: None.

Command mode: Admin Mode

Usage Guide: None.

Example:

Switch#debug ip icmp

IP ICMP: sent, type 8, src 0.0.0.0, dst 20.1.1.1

Display	Description
IP ICMP: sent	Send ICMP packets
type 8	Type is 8（PING request）
src 0.0.0.0	Source IPv4 address
dst 20.1.1.1	Destination IPv4 address

1.2.10 debug ip packet

Command: debug ip packet

          no debug ip packet

Function: Enable the IP packet debug function: the "**no debug IP packet**" command disables this debug function.

Parameter: None

Default: IP packet debugging information is disabled by default.

Command mode: Admin Mode

Usage Guide: Displays statistics for IP packets received/sent, including source/destination address and bytes, etc.

Example: Enable IP packet debug.

Switch #debug ip packet

IP PACKET: sent, src 200.1.1.35, dst 224.0.0.9, size 312, proto 17, vrf 0

IP PACKET: rcvd, src 101.1.1.1, dst 224.0.0.9, size 312, proto 17, from Vlan200, vrf 0

1.2.11 debug ipv6 packet

Command: debug ipv6 packet

no debug ipv6 packet

Function: IPv6 data packets receive/send debug message.

Parameter: None

Default: None

Command Mode: Admin Mode

Usage Guide:

Example:

Switch#debug ipv6 packet

IPv6 PACKET: rcvd, src <fe80::203:fff:fe01:2786>, dst <fe80::1>, size <64>, proto <58>, from Vlan1

Displayed information	Explanation
IPv6 PACKET: rcvd	Receive IPv6 data report
Src <fe80::203:fff:fe01:2786>	Source IPv6 address
Dst <fe80::1>	Destination IPv6 address
size <64>	Size of data report
proto <58>	Protocol field in IPv6 header
from Vlan1	IPv6 data report is collected from Layer 3 port vlan1

1.2.12 debug ipv6 icmp

Command: debug ipv6 icmp

no debug ipv6 icmp

Function: ICMP data packets receive/send debug message.

Parameter: None

Default: None

Command Mode: Admin Mode

Usage Guide: None

Example:

Switch#debug ipv6 icmp

IPv6 ICMP: sent, type <129>, src <2003::1>, dst <2003::20a:ebff:fe26:8a49> from Vlan1

Displayed information	Explanation
IPv6 ICMP: sent	Send IPv6 data report
type <129>	Ping protocol No.

Src <2003::1>	Source IPv6 address
Dst <2003::20a:ebff:fe26:8a49>	Destination IPv6 address
from Vlan1	Layer 3 port being sent

1.2.13 debug ipv6 nd

Command: debug ipv6 nd [ns | na | rs | ra | redirect]

          no debug ipv6 nd [ns | na | rs | ra | redirect]

Function: Enable the debug of receiving and sending operations for specified types of IPv6 ND messages. The ns, na, rs, ra and redirect parameters represent neighbor solicitation, neighbor advertisement, route solicitation, route advertisement and route redirect. No specification means to enable the debug for all five types of ND message. The no operation of this command will disable debug of receiving and sending operations for specified types of IPv6 ND messages, while no specification means to disable that for all five types of ND message.

Parameter: None.

Default: The debug of receiving and sending operations for all five types of IPv6 ND messages is disabled by default.

Command Mode: Admin Mode

Usage Guide: The ND protocol is an essential part of IPv6. This command can display the ND message of a specified type for troubleshooting.

Example:

Switch#debug ipv6 nd

IPv6 ND: rcvd, type <136>, src <fe80::203:fff:fe01:2786>, dst <fe80::203:fff:fe01:59ba>

Displayed information	Explanation
IPv6 ND: rcvd	Receive ND data report
type <136>	ND Type
src <fe80::203:fff:fe01:2786>	Source IPv6 address
dst <fe80::203:fff:fe01:59ba>	Destination IPv6 address

1.2.14 debug ipv6 tunnel packet

Command: debug ipv6 tunnel packet

          no debug ipv6 tunnel packet

Function: tunnel data packets receive/send debug message.

Parameter: None

Default: None

Command Mode: Admin Mode

Usage Guide: None

Example:

Switch#debug ipv6 tunnel packet

IPv6 tunnel: rcvd, type <136>, src <fe80::203:fff:fe01:2786>, dst <fe80::203:fff:fe01:59ba>

IPv6 tunnel packet : rcvd   src 178.1.1.1 dst 179.2.2.2 size 128 from tunnel1

Displayed information	Explanation
IPv6 tunnel packet : rcvd	Receive tunnel data report
type <136>	ND type
src 178.1.1.1 dst	Tunnel source IPv4 address
dst 179.2.2.2	Tunnel destination IPv4 address

1.2.15 description

Command: description <*desc*>

        no description

Function: Configure the tunnel description. The no operation of this command will delete the tunnel description.

Parameters: <*desc*> is the tunnel description, its length can not exceed 256 characters.

Command Mode: Tunnel Configuration Mode.

Default: There is no tunnel description by default.

Usage Guide: When there is more than one tunnel in the system, configuring description will help user with identifying the purposes of different tunnels.

Examples: Set the tunnel description as toCernet2.

Switch(Config-if-Tunnel1)#description toCernet2

1.2.16 ipv6 proxy enable

The command is not supported by switch.

1.2.17 ip address

Command: ip address <*ip-address*> <*mask*> [secondary]

        no ip address [<*ip-address*> <*mask*>] [secondary]

Function: Set IP address and net mask of switch; the "**no ip address [<*ip-address*> <*mask*>] [secondary]**" command deletes the IP address configuration.

Parameter: *<ip-address>* is IP address, dotted decimal notation; *<mask>* is subnet mask, dotted decimal notation; **[secondary]** indicates that the IP address is configured as secondary IP address.

Command Mode: VLAN interface configuration mode

Default: The system default is no IP address configuration.

Usage Guide: This command configures IP address on VLAN interface manually. If optional parameter **secondary** is not configured, then it is configured as the primary IP address of VLAN interface; if optional parameter **secondary** is configured, then that means the IP address is the secondary IP address of VLAN. One VLAN interface can only have one primary IP address and more than one secondary IP addresses. Primary IP and Secondary IP all can be used on SNMP/Web/Telnet management. Furthermore, the switch also provides BOOTP/DHCP manner to get IP address.

Example: The IP address of switch VLAN1 interface is set to 192.168.1.10/24.

Switch(Config-if-Vlan1)#ip address 192.168.1.10 255.255.255.0

1.2.18 ipv6 address

Command: ipv6 address *<ipv6-address|prefix-length>* **[eui-64]**

          no ipv6 address *<ipv6-address|prefix-length>* **[eui-64]**

Function: Configure aggregately global unicast address, site-local address and link-local address for the interface.

Parameter: Parameter *<ipv6-address>* is the prefix of IPv6 address, parameter *<prefix-length>* is the prefix length of IPv6 address, which is between 3-128, **eui-64** means IPv6 address is generated automatically based on eui64 interface identifier of the interface.

Command Mode: Interface Configuration Mode.

Default: None.

Usage Guide: IPv6 address prefix can not be multicast address or any other specific IPv6 address, and different layer 3 interfaces can not configure the same address prefix. For global unicast address, the length of the prefix must be greater than or equal to 3. For site-local address and link-local address, the length of the prefix must be greater than or equal to 10. For interface loopback port, the length of the prefix must be equaled to 128.

Example: Configure an IPv6 address on VLAN1 Layer 3 interface: the prefix is 2001:3f:ed8::99 and the length of the prefix is 64.

Switch(Config-if-Vlan1)#ipv6 address 2001:3f:ed8::99/64

1.2.19 ipv6 route

Command: ipv6 route *<ipv6-prefix | prefix-length>* **{***<ipv6address>* **|** *<interface-type*

interface-number> **|** *{<ipv6address> <interface-type interface-number>}* **| tunnel**
<tunnel no> } **[*<precedence>*]**

    no ipv6 route *<ipv6-prefix | prefix-length>* **{*<ipv6address>* |**
<interface-type interface-number> **|** **{*<ipv6address>* *<interface-type*
interface-number>} **| tunnel *<tunnel no>* } [*<precedence>*]**

Function: Set IPv6 static route.

Parameters: Parameter *<ipv6-prefix>* is the destination prefix of IPv6 static route, parameter *<prefix-length>* is the length of IPv6 prefix, parameter *<ipv6-address>* is the next hop IPv6 address of the reachable network, parameter *<interface-type interface-number>* is the name of interface from which to reach the destination, *<tunnel no>* is the output tunnel number of the tunnel route, parameter *<precedence>* is the weight of this route, the range is 1-255, the default is 1

Default: There is not any IPv6 static route which is configured by default.

Command Mode: Global Mode

Usage Guide: When the next hop IPv6 address is link-local address, the interface name must be specified. When the next hop IPv6 address is global aggregatable unicast address and site-local address, if no interface name of the exit is specified, it must be assured that the IP address of the next hop and the address of some interface of the switch must be in the same network segment. As for tunnel route, interface name can be directly specified.

Example: Configure static route 1 with destination address 3ffe:589:dfc::88, prefix length 64 and next hop 2001:8fd:c32::99 (the router has been configured IPv6 address of 2001:8fd:c32::34/64).

Switch(config)#ipv6 route 3ffe:589:dfc::88/64 2001:8fd:c32::99

Configure static route 2 with destination 3ffe:ff7:123::55, prefix length 64, next hop fe80::203:ff:89fd:46ac and exit interface name Vlan1.

Switch(config)#ipv6 route 3ffe:ff7:123::55/64 fe80::203:ff:89fd:46ac Vlan1

1.2.20 ipv6 redirect

Command: ipv6 redirect

    no ipv6 redirect

Function: Enable IPv6 router redirect function. The no operation of this command will disable the function.

Parameters: None.

Command Mode: Global Configuration Mode.

Default Settings: IPv6 router redirect function is disabled by default.

Usage Guide: If router A, router B, and node C are on the same network link, and router A forwards IPv6 packets from node C to router B, expecting router B to continue the

forwarding, then router A will send an IPv6 ICMPv6 redirect message to node C-source of the packet, notifying it that the best next hop of this destination address is router B. By doing so, the forwarding overhead of router A will be decreased, so is the network transmission delay of node C.

Examples: Enable IPv6 router redirect function.

Switch(config)# ipv6 redirect

1.2.21 ipv6 nd dad attempts

Command: ipv6 nd dad attempts *<value>*

            no ipv6 nd dad attempts

Function: Set Neighbor Solicitation Message number sent in succession by interface when setting Duplicate Address Detection.

Parameter: *<value>* is the Neighbor Solicitation Message number sent in succession by Duplicate Address Detection, and the value of *<value>* must be in 0-10, NO command restores to default value 1.

Command Mode: Interface Configuration Mode

Default: The default request message number is 1.

Usage Guide: When configuring an IPv6 address, it is required to process IPv6 Duplicate Address Detection, this command is used to configure the ND message number of Duplicate Address Detection to be sent, *value* being 0 means no Duplicate Address Detection is executed.

Example: The Neighbor Solicitation Message number sent in succession by interface when setting Duplicate Address Detection is 3.

Switch(Config-if-Vlan1)# ipv6 nd dad attempts 3

1.2.22 ipv6 nd ns-interval

Command: ipv6 nd ns-interval *<seconds>*

          no ipv6 nd ns-interval

Function: Set the time interval of Neighbor Solicitation Message sent by the interface.

Parameter: parameter *<seconds>* is the time interval of sending Neighbor Solicitation Message, *<seconds>* value must be between 1-3600 seconds, **no** command restores the default value 1 second.

Command Mode: Interface Configuration Mode

Default: The default Request Message time interval is 1 second.

Usage Guide: The value to be set will include the situation in all routing announcement on the interface. Generally, very short time interval is not recommended.

Example: Set Vlan1 interface to send out Neighbor Solicitation Message time interval to

be 8 seconds.

Switch(Config-if-Vlan1)#ipv6 nd ns-interval 8

1.2.23 ipv6 nd suppress-ra

Command: ipv6 nd suppress-ra

        no ipv6 nd suppress-ra

Function: Prohibit router announcement.

Parameter: None

Command Mode: Interface Configuration Mode

Default: Router Announcement function is disabled.

Usage Guide: no ipv6 nd suppress-ra command enable router announcement function.

Example: Enable router announcement function.

Switch(Config-if-Vlan1)#no ipv6 nd suppress-ra

1.2.24 ipv6 nd ra-lifetime

Command: ipv6 nd ra-lifetime <*seconds*>

        no ipv6 nd ra-lifetime

Function: Configure the lifetime of router announcement.

Parameter: parameter **<*seconds*>** stands for the number of seconds of router announcement lifetime, **<*seconds*>** value must be between 0-9000.

Command Mode: Interface Configuration Mode

Default: The number of seconds of router default announcement lifetime is 1800.

Usage Guide: This command is used to configure the lifetime of the router on Layer 3 interface, seconds being 0 means this interface can not be used for default router, otherwise the value should not be smaller than the maximum time interval of sending router announcement. If no configuration is made, this value is equal to 3 times of the maximum time interval of sending routing announcement.

Example: Set the lifetime of routing announcement is 100 seconds.

Switch(Config-if-Vlan1)#ipv6 nd ra-lifetime 100

1.2.25 ipv6 nd min-ra-interval

Command: ipv6 nd min-ra-interval <*seconds*>

        no ipv6 nd min-ra-interval

Function: Set the minimum time interval of sending routing message.

Parameter: Parameter **<*seconds*>** is number of seconds of the minimum time interval of sending routing announcement, **<*seconds*>** must be between 3-1350 seconds.

Command Mode: Interface Configuration Mode

Default: The default minimum time interval of sending routing announcement is 200 seconds.

Usage Guide: The minimum time interval of routing announcement should not exceed 3/4 of the maximum time interval.

Example: Set the minimum time interval of sending routing announcement is 10 seconds.

Switch(Config-if-Vlan1)#ipv6 nd min-ra-interval 10

1.2.26 ipv6 nd max-ra-interval

Command: ipv6 nd max-ra-interval <*seconds*>

　　　　　　no ipv6 nd max-ra-interval

Function: Set the maximum time interval of sending routing message.

Parameter: Parameter **<*seconds*>** is number of seconds of the time interval of sending routing announcement, **<*seconds*>** must be between 4-1800 seconds.

Command Mode: Interface Configuration Mode

Default: The default maximum time interval of sending routing announcement is 600 seconds.

Usage Guide: The maximum time interval of routing announcement should be smaller than the lifetime value routing announcement.

Example: Set the maximum time interval of sending routing announcement is 20 seconds.

Switch(Config-if-Vlan1)#ipv6 nd max-ra-interval 20

1.2.27 ipv6 nd prefix

Command: ipv6 nd prefix <*ipv6-prefix | prefix-length*>{ [<*valid-lifetime*> <*preferred-lifetime*>] [no-autoconfig / off-link[no-autoconfig]]}

　　　　　　no ipv6 nd prefix <*ipv6-prefix | prefix-length*>

Function: Configure the address prefix and relative parameters for router announcement.

Parameter: Parameter **<*ipv6-prefix*>** is the address prefix of the specified announcement, parameter **<*prefix-length*>** is the length of the address prefix of the specified announcement, parameter **<*valid-lifetime*>** is the valid lifetime of the prefix, parameter **<*preferred-lifetime*>** is the preferred lifetime of the prefix, and the valid lifetime must be no smaller than preferred lifetime. Parameter **no-autoconfig** says this prefix can not be used to automatically configure IPv6 address on the host in link-local. Parameter **off-link** says the prefix specified by router announcement message is not assigned to link-local, the node which sends data to the address including this prefix consider link-local as unreachable.

Command Mode: Interface Configuration Mode

Default: The default value of *valid-lifetime* is 2592000 seconds (30 days), the default value of *preferred-lifetime* is 604800 seconds (7 days). **off-link** is off by default, **no-autoconfig** is off by default.

Usage Guide: This command allows controlling the router announcement parameters of every IPv6 prefix. Note that valid lifetime and preferred lifetime must be configured simultaneously.

Example: Configure IPv6 announcement prefix as 2001:410:0:1::/64 on Vlan1, the valid lifetime of this prefix is 8640 seconds, and its preferred lifetime is 4320 seconds.

Switch(Config-if-Vlan1)#ipv6 nd prefix 2001:410:0:1::/64 8640 4320

1.2.28 ipv6 nd ra-hoplimit

Command: ipv6 nd ra-hoplimit <value>

Function: Set the hoplimit of sending router advertisement.

Parameters: <value> is the hoplimit of sending router advertisement, ranging from 0 to 255.

Command Mode： Interface Configuration Mode.

Default: The default hoplimit of sending router advertisement is 64.

Example: Set the hoplimit of sending router advertisement in interface vlan 1 as 128.

Switch#(Config-if-Vlan1)#ipv6 nd ra-hoplimit 128

1.2.29 ipv6 nd ra-mtu

Command: ipv6 nd ra-mtu <value>

Function: Set the mtu of sending router advertisement.

Parameters: <value> is the mtu of sending router advertisement, ranging from 0 to 1500.

Command Mode： Interface Configuration Mode.

Default: The default mtu of sending router advertisement is 1500.

Example: Set the mtu of sending router advertisement in interface vlan 1 as 500.

Switch#(Config-if-Vlan1)#ipv6 nd ra-mtu 500

1.2.30 ipv6 nd reachable-time

Command: ipv6 nd reachable-time <seconds>

Function: Set the reachable-time of sending router advertisement.

Parameters: <value> is the reachable-time of sending router advertisement, ranging from 0 to 3600000 milliseconds.

Command Mode: Interface Configuration Mode.

Default Settings: The default reachable-time of sending router advertisement is 30000 milliseconds.

Example: Set the reachable-time of sending router advertisement in interface vlan 1 as 100000 milliseconds.

Switch(Config-if-Vlan1)#ipv6 nd reachable-time 100000

1.2.31 ipv6 nd retrans-timer

Command: ipv6 nd retrans-timer <seconds>

Function: Set the retrans-timer of sending router advertisement.

Parameters: <value> is the retrans-timer of sending router advertisement, ranging from 0 to 4294967295 milliseconds.

Command Mode: Interface Configuration Mode.

Default: The default retrans-timer of sending router advertisement is 1000 milliseconds.

Example: Set the reachable-time of sending router advertisement in interface vlan 1 as 10000 milliseconds.

Switch(Config-if-Vlan1)#ipv6 nd retrans-timer 10000

1.2.32 ipv6 nd other-config-flag

Command: ipv6 nd other-config-flag

Function: Set the flag representing whether information other than the address information will be obtained via DHCPv6.

Parameters: None.

Command Mode: Interface Configuration Mode.

Default: Information other than the address information won't be obtained via DHCPv6.

Examples: Set IPv6 information other than the address information in interface vlan 1 will be obtained via DHCPv6.

Switch(Config-if-Vlan1)#ipv6 nd other-config-flag

1.2.33 ipv6 nd managed-config-flag

Command: ipv6 nd managed-config-flag

Function: Set the flag representing whether the address information will be obtained via DHCPv6.

Parameters: None.

Command Mode: Interface Configuration Mode.

Default: The address information won't be obtained via DHCPv6.

Examples: Set IPv6 address information in interface vlan 1 will be obtained via DHCPv6.

Switch(Config-if-Vlan1)#ipv6 nd managed-config-flag

1.2.34 ipv6 neighbor

Command: ipv6 neighbor *<ipv6-address>* *<hardware-address>* interface *<interface-type interface-name>*

no ipv6 neighbor *<ipv6-address>*

Function: Set static neighbor table entry.

Parameters: Parameter *ipv6-address* is static neighbor IPv6 address, same to interface prefix parameter, parameter *hardware-address* is static neighbor hardware address, *interface-type* is Ethernet type, *interface-name* is Layer 2 interface name.

Command Mode: Interface Configuration Mode

Default Situation: There is not static neighbor table entry.

Usage Guide: IPv6 address and multicast address for specific purpose and local address cannot be set as neighbor.

Example: Set static neighbor 2001:1:2::4 on port E1/0/1, and the hardware MAC address is 00-03-0f-89-44-bc.

Switch(Config-if-Vlan1)#ipv6 neighbor 2001:1:2::4 00-03-0f-89-44-bc interface Ethernet 1/0/1

1.2.35 interface tunnel

Command: interface tunnel *<tnl-id>*

no interface tunnel *<tnl-id>*

Function: Create/Delete tunnel.

Parameter: Parameter <tnl-id> is tunnel No.

Command Mode: Global Mode.

Default: None.

Usage Guide: This command creates a virtual tunnel interface. Since there is not information such as specific tunnel mode and tunnel source, *show ipv6 tunnel* does not show the tunnel, enter tunnel mode after creating, under that model information such as tunnel source and destination can be specified. No command deletes a tunnel.

Example: Create tunnel 1.

Switch(Config)#interface tunnel 1

1.2.36 show ip interface

Command: show ip interface [*<ifname>* | vlan *<vlan-id>*] brief

Function: Show the brief information of the configured layer 3 interface.

Parameters: *<ifname>* Interface name; *<vlan-id>* VLAN ID.

Default: Show all brief information of the configured layer 3 interface when no parameter is specified.

Command mode: All modes.

Usage Guide: None.

Example:

Restarter#show ip interface vlan1 brief

Index	Interface	IP-Address	Protocol
3001	Vlan1	192.168.2.11	up

1.2.37 show ip traffic

Command: show ip traffic

Function: Display statistics for IP packets.

Command mode: Admin Mode

Usage Guide: Display statistics for IP, ICMP, TCP, UDP packets received/sent.

Example:

Switch#show ip traffic

IP statistics:

Rcvd: 3249810 total, 3180 local destination

        0 header errors, 0 address errors

        0 unknown protocol, 0 discards

Frags: 0 reassembled, 0 timeouts

        0 fragment rcvd, 0 fragment dropped

        0 fragmented, 0 couldn't fragment, 0 fragment sent

Sent: 0 generated, 3230439 forwarded

         0 dropped, 0 no route

ICMP statistics:

Rcvd: 0 total 0 errors 0 time exceeded

        0 redirects, 0 unreachable, 0 echo, 0 echo replies

        0 mask requests, 0 mask replies, 0 quench

        0 parameter, 0 timestamp, 0 timestamp replies

Sent: 0 total 0 errors 0 time exceeded

        0 redirects, 0 unreachable, 0 echo, 0 echo replies

        0 mask requests, 0 mask replies, 0 quench

        0 parameter, 0 timestamp, 0 timestamp replies

TCP statistics:

TcpActiveOpens   0, TcpAttemptFails   0

TcpCurrEstab   0, TcpEstabResets   0

TcpInErrs	0, TcpInSegs	3180
TcpMaxConn	0, TcpOutRsts	3
TcpOutSegs	0, TcpPassiveOpens	8
TcpRetransSegs	0, TcpRtoAlgorithm	0
TcpRtoMax	0, TcpRtoMin	0

UDP statics:

UdpInDatagrams	0, UdpInErrors	0
UdpNoPorts	0, UdpOutDatagrams	0

Displayed information	Explanation
IP statistics：	IP packet statistics.
Rcvd:　3249810 total, 3180 local destination 　　　　0 header errors, 0 address errors 　　　　0 unknown protocol, 0 discards	Statistics of total packets received, number of packets reached local destination, number of packets have header errors, number of erroneous addresses, number of packets of unknown protocols; number of packets dropped.
Frags：　0 reassembled, 0 timeouts 　　　　0 fragment rcvd, 0 fragment dropped 　　　　0 fragmented, 0 couldn't fragment, 0 fragment sent	Fragmentation statistics: number of packets reassembled, timeouts, fragments received, fragments discarded, packets that cannot be fragmented, number of fragments sent, etc.
Sent：　0 generated, 0 forwarded 　　　　0 dropped, 0 no route	Statistics for total packets sent, including number of local packets, forwarded packets, dropped packets and packets without route.
ICMP statistics：	ICMP packet statistics.
Rcvd：　　0 total 0 errors 0 time exceeded 　　　　0 redirects, 0 unreachable, 0 echo, 0 echo replies 　　　　0 mask requests, 0 mask replies, 0 quench 　　　　0 parameter, 0 timestamp, 0 timestamp replies	Statistics of total ICMP packets received and classified information
Sent：　0 total 0 errors 0 time exceeded 　　　　0 redirects, 0 unreachable, 0 echo, 0 echo replies	Statistics of total ICMP packets sent and classified information

0 mask requests, 0 mask replies, 0 quench 0 parameter, 0 timestamp, 0 timestamp replies	
TCP statistics:	TCP packet statistics.
UDP statistics:	UDP packet statistics.

1.2.38 show ipv6 interface

Command: show ipv6 interface {brief|*<interface-name>*}

Function: Show interface IPv6 parameters.

Parameter: Parameter brief is the brief summarization of IPv6 status and configuration, and parameter interface-name is Layer 3 interface name.

Default: None

Command Mode: Admin and Configuration Mode

Usage Guide: If only brief is specified, then information of all L3 is displayed, and you can also specify a specific Layer 3 interface.

Example:

Switch#show ipv6 interface Vlan1

Vlan1 is up, line protocol is up, dev index is 2004

Device flag 0x1203(UP BROADCAST ALLMULTI MULTICAST)

IPv6 is enabled

Link-local address(es):

fe80::203:fff:fe00:10   PERMANENT

Global unicast address(es):

3001::1   subnet is 3001::1/64   PERMANENT

Joined group address(es):

ff02::1

ff02::16

ff02::2

ff02::5

ff02::6

ff02::9

ff02::d

ff02::1:ff00:10

ff02::1:ff00:1

MTU is 1500 bytes

ND DAD is enabled,   number of DAD attempts is 1

ND managed_config_flag is unset

ND other_config_flag is unset

ND NS interval is 1 second(s)

ND router advertisements is disabled

ND RA min-interval is 200 second(s)

ND RA max-interval is 600 second(s)

ND RA hoplimit is 64

ND RA lifetime is 1800 second(s)

ND RA MTU is 0

ND advertised reachable time is 0 millisecond(s)

ND advertised retransmit time is 0 millisecond(s)

Displayed information	Explanation
Vlan1	Layer 3 interface name
[up/up]	Layer 3 interface status
dev index	Internal index No.
fe80::203:fff:fe00:10	Automatically configured IPv6 address of Layer 3 interface
3001::1	Configured IPv6 address of Layer 3 interface

1.2.39 show ipv6 route

Command: show ipv6 route [<destination>|<*destination* >|<*length*>|/ database| fib [local]| nsm [connected | static | rip| ospf | bgp | isis| kernel| database]|statistics]
Function: Display IPv6 routing table.
Parameter: *<destination>* is destination network address; *<destination>|<length>* is destination network address plus prefix length; **connected** is directly connected router; **static** is static router; **rip** is RIP router; **ospf** is OSPF router; **bgp** is BGP router; **isis** is ISIS router; **kernel** is kernel router; **statistics** shows router number; **database** is router database.
Default Situation: None.
Command Mode: Admin and Configuration Mode.
Usage Guide: show ipv6 route only shows IPv6 kernal routing table (routing table in tcpip), database shows all routers except the local router, fib local shows the local router, statistics shows router statistics information.
Example:

Switch#show ipv6 route

Codes: C - connected, L - Local, S - static, R - RIP, O - OSPF,

     I - IS-IS, B - BGP

C   ::/0   via ::,   tunnel3   256

S   2001:2::/32   via fe80::789,   Vlan2   1024

S   2001:2:3:4::/64   via fe80::123,   Vlan2   1024

O   2002:ca60:c801:1::/64   via ::,   Vlan1   1024

C   2002:ca60:c802:1::/64   via ::,   tunnel49   256

C   2003:1::/64   via ::,   Vlan4   256

C   2003:1::5efe:0:0/96   via ::,   tunnel26   256

S   2004:1:2:3::/64   via fe80:1::88,   Vlan2   1024

O   2006:1::/64   via ::,   Vlan1   1024

S   2008:1:2:3::/64   via fe80::250:baff:fef2:a4f4,   Vlan1   1024

C   2008:2005:5:8::/64   via ::,   Ethernet0   256

S   2009:1::/64   via fe80::250:baff:fef2:a4f4,   Vlan1   1024

C   2022:1::/64   via ::,   Ethernet0   256

O   3333:1:2:3::/64   via fe80::20c:ceff:fe13:eac1,   Vlan12   1024

C   3ffe:501:ffff:1::/64   via ::,   Vlan4   256

O   3ffe:501:ffff:100::/64   via ::,   Vlan5   1024

O   3ffe:3240:800d:1::/64   via ::,   Vlan1   1024

O   3ffe:3240:800d:2::/64   via ::,   Vlan2   1024

O   3ffe:3240:800d:10::/64   via ::,   Vlan12   1024

O   3ffe:3240:800d:20::/64   via fe80::20c:ceff:fe13:eac1,   Vlan12   1024

C   fe80::/64   via ::,   Vlan1   256

C   fe80::5efe:0:0/96   via ::,   tunnel26   256

C   ff00::/8   via ::,   Vlan1   256

Displayed information	Explanation
IPv6 Routing Table	IPv6 routing table status
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,I - IS-IS, B - BGP > - selected route, * - FIB route, p - stale info	Abbreviation display sign of every entry
S 2009:1::/64 via fe80::250:baff:fef2:a4f4, Vlan1 1024	The static router in FIB table, of which the destination network segment is 2002::/64, via means passing fe80::250:baff:fef2:a4f4 is the next hop, VLAN1 is the exit interface name, 1024 is

	router weight.

1.2.40 show ipv6 neighbors

Command: show ipv6 neighbors [{vlan|ethernet|tunnel } interface-number | interface-name | address *<ipv6address>*]

Function: Display neighbor table entry information.

Parameter: Parameter **{vlan|ethernet|tunnel} interface-number|interface-name** specify the lookup based on interface. Parameter *ipv6-address* specifies the lookup based on IPv6 address. It displays the whole neighbor table entry if without parameter.

Default Situation: None

Command Mode: Admin and Configuration Mode

Usage Guide:

Example:

Switch#show ipv6 neighbors

IPv6 neighbour unicast items: 14, valid: 11, matched: 11, incomplete: 0, delayed: 0, manage items 5

IPv6 Address	Hardware Addr	Interface	Port
State			
2002:ca60:c801:1:250:baff:fef2:a4f4	00-50-ba-f2-a4-f4		Vlan1
Ethernet1/0/2 reachable			
3ffe:3240:800d:1::100	00-03-0f-01-27-86		Vlan1
Ethernet1/0/3 reachable			
3ffe:3240:800d:1::8888	00-02-01-00-00-00		Vlan1
Ethernet1/0/1 permanent			
3ffe:3240:800d:1:250:baff:fef2:a4f4	00-50-ba-f2-a4-f4		Vlan1
Ethernet1/0/4 reachable			
3ffe:3240:800d:2::8888	00-02-01-00-01-01		Vlan2
Ethernet1/0/16 permanent			
3ffe:3240:800d:2:203:fff:fefe:3045	00-03-0f-fe-30-45		Vlan2
Ethernet1/0/15 reachable			
fe80::203:fff:fe01:2786	00-03-0f-01-27-86		Vlan1
Ethernet1/0/5 reachable			
fe80::203:fff:fefe:3045	00-03-0f-fe-30-45		Vlan2
Ethernet1/0/17 reachable			
fe80::20c:ceff:fe13:eac1	00-0c-ce-13-ea-c1		Vlan12
Ethernet1/0/20 reachable			

fe80::250:baff:fef2:a4f4   00-50-ba-f2-a4-f4   Vlan1

Ethernet1/0/6   reachable

IPv6 neighbour table: 11 entries

Displayed information	Explanation
IPv6 Addres	Neighbor IPv6 address
Hardware Addr	Neighbor MAC address
Interface	Exit interface name
Port	Exit interface name
State	Neighbor status (reachable、 statle、 delay、 probe、 permanent、 incomplete、 unknow)

1.2.41 show ipv6 traffic

Command: show ipv6 traffic

Function: Display IPv6 transmission data packets statistics information.

Parameter: None

Default: None

Command Mode: Admin and Configuration Mode

Example:

Switch#show ipv6 traffic

IP statistics:

Rcvd: 90 total, 17 local destination

        0 header errors, 0 address errors

        0 unknown protocol, 13 discards

Frags: 0 reassembled, 0 timeouts

        0 fragment rcvd, 0 fragment dropped

        0 fragmented, 0 couldn't fragment, 0 fragment sent

Sent: 110 generated, 0 forwarded

        0 dropped, 0 no route

ICMP statistics:

  Rcvd: 0 total 0 errors 0 time exceeded

        0 redirects, 0 unreachable, 0 echo, 0 echo replies

Displayed information	Explanation
IP statistics	IPv6 data report statistics
Rcvd: 90 total, 17 local	IPv6 received packets statistics

destination0 header errors, 0 address errors0 unknown protocol, 13 discards	
Frags: 0 reassembled, 0 timeouts 0 fragment rcvd, 0 fragment dropped0 fragmented, 0 couldn't fragment, 0 fragment sent	IPv6 fragmenting statistics
Sent: 110 generated, 0 forwarded 0 dropped, 0 no route	IPv6 sent packets statistics

1.2.42 show ipv6 redirect

Command: show ipv6 redirect

Function: Display the state IPv6 redirect switch.

Parameters: None.

Default: None.

Command Mode: Admin and Configuration Mode.

Usage Guide: This command can be used to check whether the IPv6 redirect function in the system is enabled.

Examples:

Switch show ipv6 redirect

ipv6 redirect is disabled

1.2.43 show ipv6 tunnel

 Command: show ipv6 tunnel [<*tnl-id*>]

Function: Display tunnel information.

Parameter: Parameter *<tnl-id>* is tunnel No.

Default Situation: None.

Command Mode: Admin Mode.

Usage Guide: If there is not tunnel number, then information of all tunnels are shown. If there is tunnel number, then the detailed information of specified tunnel is shown.

Example:

Switch#show ipv6 tunnel

name	mode	source	destination	nexthop
tunnel3	6to4	178.1.1.1		

Displayed information	Explanation

Name	Tunnel name
Mode	Tunnel type
Source	Tunnel source ipv4 address
Destination	Tunnel destination ipv4 address
Nexthop	Tunnel next hop (only applies to ISATAP tunnel)

1.2.44 tunnel source

Command: tunnel source {*<ipaddress>* | *<ipv6address>* | *<interface-name>*}

no tunnel source

Function: Configure the IPv4/IPv6 address of the tunnel source.

Parameter: *<ipaddress>* is the IPv4 address of tunnel source, must be the unicast address; *<ipv6address>* is the IPv6 address of tunnel source; *<interface-name>* means the tunnel source address is the IPv4 address of the interface *<interface-name>*.

Command Mode: Tunnel Configuration Mode.

Default Situation: There is no IPv4/IPv6 address and interface name of tunnel source.

Usage Guide: Set the source IPv4/IPv6 address or specify an interface name of the tunnel source address to configure the tunnel.

Example: Configure tunnel source IPv4 address 202.89.176.6.

Switch(Config-if-Tunnel1)#tunnel source 202.89.176.6

1.2.45 tunnel destination

Command: tunnel destination *<ipaddress | ipv6address>*

no tunnel destination

Function: Configure the IPv4/IPv6 address of the tunnel destination.

Parameter: *<ipaddress>* is the IPv4 address of tunnel destination, *<ipv6address>* is the IPv6 address of tunnel destination.

Command Mode: Tunnel Configuration Mode.

Default Situation: There is no IPv4/IPv6 address of tunnel destination.

Usage Guide: This command is used to configure the IPv4/IPv6 address of tunnel destination.

Example: Configure tunnel destination 203.78.120.5.

Switch(Config-if-Tunnel1)#tunnel destination 203.78.120.5

1.2.46 tunnel nexthop

Command: tunnel nexthop <ipaddress>

no tunnel nexthop

Function: Configure tunnel nexthop.

Parameter: **<ipaddress>** is the IPv4 address of tunnel nexthop.

Command Mode: Tunnel Configuration Mode.

Default Situation: There is no IPv4 address of tunnel nexthop.

Usage Guide: This command is for ISATAP tunnel, other tunnels won't check the configuration of nexthop. Notice: IPv4 address of ISATAP tunnel nexthop and IPv4 address of tunnel source should be in same segment.

Example: Configure tunnel next hop 178.99.156.8.

Switch(Config-if-Tunnel1)#tunnel source 178.99.156.7

Switch(Config-if-Tunnel1)#tunnel nexthop 178.99.156.8

Switch(Config-if-Tunnel1)#tunnel mode ipv6ip isatap

1.2.47 tunnel 6to4-relay

Command: tunnel 6to4-relay <ipdaddress>

no tunnel 6to4-relay <ipdaddress>

Function: Configure the 6to4 tunnel relay IPv4 address.

Parameters: **<ipdaddress>** is the 6to4 tunnel relay IPv4 address.

Command Mode: Tunnel Configuration Mode.

Default: None.

Usage Guide: This command is used to configure the 6to4 tunnel relay IPv4 address, which will not be checked when configuring 6to4 tunnel relay. This relay IPv4 address will only be used when the packet uses default route with a destination address not starting with a prefix of 2002.

Examples: Configure the 6to4 tunnel relay IPv4 address as 178.99.156.8.

Switch (Config-if-Tunnel1)#tunnel 6to4-relay 178.99.156.8

1.2.48 tunnel mode

Command: tunnel mode [[gre] | ipv6ip [6to4 | isatap]]

no tunnel mode

Function: Configure Tunnel Mode.

Parameter: **gre** is GRE tunnel.

Command Mode: Tunnel Configuration Mode.

Default: None.

Usage Guide: In configuring tunnel mode, only specifying ipv6ip indicates configuring tunnel. Ipv6ip 6to4 indicates it is 6to4 tunnel, ipv6ip isatap indicates it is ISATAP tunnel.

Example: Configure tunnel mode.

1、Switch(Config-if-Tunnel1)#tunnel mode ipv6ip

2、Switch(Config-if-Tunnel1)#tunnel mode ipv6ip 6to4

3、Switch(Config-if-Tunnel1)#tunnel mode ipv6ip isatap

1.3 Commands for IP Route Aggregation

1.3.1 ip fib optimize

Command: ip fib optimize

    no ip fib optimize

Function: Enables the switch to use optimized IP route aggregation algorithm; the "**no ip fib optimize**" disables the optimized IP route aggregation algorithm.

Default: Optimized IP route aggregation algorithm is disabled by default.

Command mode: Global Mode.

Usage Guide: This command is used to optimize the aggregation algorithm: if the route table contains no default route, the next hop most frequently referred to will be used to construct a virtual default route to simplify the aggregation result. This method has the benefit of more effectively simplifying the aggregation result. However, while adding a virtual default route to the chip segment route table reduces CPU load, it may introduce unnecessary data stream to switches of the next hop. In fact, part of local switch CPU load is transferred to switches of the next hop.

Example: Disabling optimized IP route aggregation algorithm.

Switch(config)# no ip fib optimize

1.4 Commands for URPF

1.4.1 debug urpf

Command: debug urpf {notice | warn | error}

    no debug urpf {notice | warn | error}

Function: Enable the URPF debug function to display error information if failures occur during the installation of URPF rules.

Command Mode: Admin Mode

Parameters: None

Usage Guide: None

Example:

Switch#debug urpf error

1.4.2 ip urpf enable

Command: ip urpf enable {loose | strict} {allow-default-route}

          no ip urpf enable

Function: Enable the URPF function on the port.

Parameters: loose：the loose mode;

          strict：the strict mode;

          allow-default-route：allow the default route.

Command mode: Port Mode

Default: The URPF function is disabled on the port by default.

Usage Guide: Users should specify the mode: loose or strict.

Example:

Switch(config)#interface ethernet 1/0/4

Switch(Config-If-Ethernet1/0/4)#ip urpf enable strict

Switch(Config-If-Ethernet1/0/4)#interface ethernet 1/0/5

Switch(Config-If-Ethernet1/0/5)#ip urpf enable loose

Switch(Config-If-Ethernet1/0/5) #interface ethernet 1/0/6

Switch(Config-If-Ethernet1/0/6)#ip urpf enable loose allow-default-route

Switch(Config-If-Ethernet1/0/6)#interface ethernet 1/0/7

Switch(Config-If-Ethernet1/0/7)#ip urpf enable strict allow-default-route

1.4.3 show urpf rule ipv4 num

Command: show urpf rule ipv4 num interface {ethernet IFNAME | IFNAME}

Function: Display the number of IPv4 rules bonded to the port.

Parameters: IFNAME: specify the port name.

Command Mode: Admin and Configuration Mode

Usage Guide: None

Examples: Display the number of IPv4 rules bonded to the port Ethernet1/0/4.

Switch#show urpf rule ipv4 num interface ethernet 1/0/4

1.4.4 show urpf rule ipv6 num

Command: show urpf rule ipv6 num interface {ethernet IFNAME | IFNAME}

Function: Display the number of IPv6 rules bonded to the port.

Parameters: IFNAME: specify the port name.

Command Mode: Admin and Configuration Mode

Usage Guide: None

Example: Display the number of IPv6 rules bonded to the port Ethernet1/0/4.

Switch#show urpf rule ipv6 num interface ethernet 1/0/4

1.4.5 show urpf rule ipv4

Command: show urpf rule ipv4 interface {ethernet IFNAME | IFNAME}

Function: Display the details of IPv4 rules bonded to the port.

Parameters: IFNAME: specify the port name.

Command Mode: Admin and Configuration Mode

Usage Guide: Display the currently distributed rules.

Examples: Display the details of IPv4 rules bonded to the port Ethernet1/0/4.

Switch#show urpf rule ipv4 interface ethernet 1/0/4

1.4.6 show urpf rule ipv6

Command: show urpf rule ipv6 interface {ethernet IFNAME | IFNAME}

Function: Display the details of IPv6 rules bonded to the port.

Parameters: IFNAME: specify the port name.

Command Mode: Admin and Configuration Mode

Usage Guide: Display the currently distributed rules.

Examples: Display the details of IPv6 rules bonded to the port ethernet1/0/4.

Switch#show urpf rule ipv6 interface ethernet 1/0/4

1.4.7 show urpf

Command: show urpf

Function: Display which interfaces have been enabled with URPF function.

Command Mode: Admin and Configuration Mode

Parameters: None

Usage Guide: None

Example:

Switch#show urpf

1.4.8 urpf enable

Command: urpf enable
        no urpf enable

Function: Enable the global URPF function.

Parameters: None

Command mode: Global Mode

Default: The URPF protocol module is disabled by default.

Usage Guide: None

Example:

Switch(config)#urpf enable

1.5 Commands for ARP Configuration

1.5.1 arp

Command: arp *<ip_address>* *<mac_address>* {interface [ethernet] *<portName>*}
          no arp *<ip_address>*

Function: Configures a static ARP entry; the "**no arp *<ip_address>*****"** command deletes a
ARP entry of the specified IP address.

Parameters: *<ip_address>* is the IP address, at the same field with interface address;
<mac_address> is the MAC address; **ethernet** stands for Ethernet port; *<portName>* for
the name of layer2 port.

Default: No static ARP entry is set by default.

Command mode: VLAN Interface Mode

Usage Guide: Static ARP entries can be configured in the switch.

Example: Configuring static ARP for interface VLAN1.

Switch(Config-if-Vlan1)#arp 1.1.1.1 00-03-0f-f0-12-34 interface eth 1/0/2

1.5.2 clear arp-cache

Command: clear arp-cache

Function: Clears ARP table.

Command mode: Admin Mode

Example:

Switch#clear arp-cache

1.5.3 clear arp traffic

Command: clear arp traffic

Function: Clear the statistic information of ARP messages of the switch. For box switches,

this command will only clear statistics of APP messages received and sent from the current boardcard.

Command mode: Admin Mode

Example:

Switch#clear arp traffic

1.5.4 debug arp

Command: debug arp {receive|send|state}

          no debug arp {receive|send|state}

Function: Enables the ARP debugging function; the "**no debug arp {receive|send|state}**" command disables this debugging function.

Parameter: receive the debugging-switch of receiving ARP packets of the switch; **send** the debugging-switch of sending ARP packets of the switch; **state** the debugging-switch of APR state changing of the switch.

Default: ARP debug is disabled by default.

Command mode: Admin Mode.

Usage Guide: Display contents for ARP packets received/sent, including type, source and destination address, etc.

Example: Enable ARP debugging.

Switch#debug arp receive

%Jan 01 01:05:53 2006 IP ARP: rcvd, type REQUEST, src 172.16.1.251, 00-e0-4c-88-ad-bc, dst 172.16.1.110, 00-00-00-00-00-00 flag 0x0, pkt type 1, intf Vlan100.

%Jan 01 01:05:53 2006 IP ARP: rcvd, type REQUEST, src 172.16.1.251, 00-e0-4c-88-ad-bc, dst 172.16.1.110, 00-00-00-00-00-00 flag 0x0, pkt type 1, intf Vlan100.

e%Jan 01 01:05:53 2006 IP ARP: rcvd, type REQUEST, src 172.16.1.251, 00-e0-4c-88-ad-bc, dst 172.16.1.110, 00-00-00-00-00-00 flag 0x0, pkt type 1, intf Vlan100.

%Jan 01 01:05:53 2006 IP ARP: rcvd, type REQUEST, src 172.16.1.251, 00-e0-4c-88-ad-bc, dst172.16.1.110, 00-00-00-00-00-00 flag 0x0, pkt type 1, intf Vlan100.

1.5.5 ip proxy-arp

Command: ip proxy-arp

          no ip proxy-arp

Function: Enables proxy ARP for VLAN interface; the no command disables proxy ARP.

Default: Proxy ARP is disabled by default.

Command mode: VLAN Interface Mode

Usage Guide: When an ARP request is received on the layer 3 interface, requesting an IP address in the same IP segment of the interface but not the same physical network, and

the proxy ARP interface has been enabled, the interface will reply to the ARP with its own MAC address and forward the actual packets received. Enabling this function allows machines to physically be separated but in the same IP segment and communicate via the proxy ARP interface as if in the same physical network. Proxy ARP will check the route table to determine whether the destination network is reachable before responding to the ARP request; ARP request will only be responded if the destination is reachable.

Note: the ARP request matching default route will not use proxy.

Example: Enable proxy ARP for VLAN 1.

Switch(Config-if-Vlan1)#ip proxy-arp

1.5.6 l3 hashselect

Command: l3 hashselect [<crc16l | crc16u *| crc32l | crc32u | lsb >*]

Function: Set L3 table (hardware ARP table) HASH algorithm.

Parameters: <crc16l | crc16u | crc32l | crc32u | lsb> is a specified HASH algorithm. The system default value is crc32u.

Command Mode: Global Configuration Mode.

Usage Guide: HASH algorithm is a fast searching algorithm. Setting that of L3 table will change the storage location and order of ARP entries in the hardware. This command is mainly used to solve the conflicts of ARP entries in the hardware table. When using the command to change the HASH algorithms of L3 table, the new HASH algorithm will take effect after the consumers save the configuration and restart system. The system will use the primary HASH algorithms before restart system. Since all HASH algorithms may have HASH crashes under certain circumstances, particular network configuration requires particular HASH algorithm. After repeated tests and verifications, the recommended order of the five HASH algorithms mentioned above is: crc32u，crc32l，crc16u，crc16l. Generally speaking, lsb algorithm is not recommended.

When using this command to change the HASH algorithms of L3 table, users should make effective analysis of the network ARP configuration. That is why this command should uses under the guide of technicians from the vendor after they analyze the network ARP configuration.

Examples: Set the HASH algorithm as crc32u.

Switch(Config-if-Vlan1)#l3 hashselect crc32u

1.5.7 show arp

Command: show arp [<*ipaddress*>] [<*vlan-id*>] [<*hw-addr*>] [type {static | dynamic}] [count] [vrf word]

Function: Displays the ARP table.

Parameters: *<ipaddress>* is a specified IP address; *<vlan-id>* stands for the entry for the identifier of specified VLAN; *<hw-addr>* for entry of specified MAC address; **static** for static ARP entry; **dynamic** for dynamic ARP entry; **count** displays number of ARP entries; **word** is the specified vrf name.

Command mode: Admin Mode

Usage Guide: Displays the content of current ARP table such as IP address, MAC address, hardware type, interface name, etc.

Example:

Switch#show arp

ARP Unicast Items: 7, Valid: 7, Matched: 7, Verifying: 0, Incomplete: 0, Failed: 0, None: 0

Address	Hardware Addr	Interface	Port	Flag
50.1.1.6	00-0a-eb-51-51-38	Vlan50	Ethernet1/0/11	Dynamic
50.1.1.9	00-00-00-00-00-09	Vlan50	Ethernet1/0/1	Static
150.1.1.2	00-00-58-fc-48-9f	Vlan150	Ethernet1/0/4	Dynamic

Displayed information	Explanation
Total arp items	Total number of ARP entries.
Valid	ARP entry number matching the filter conditions and attributing the legality states.
Matched	ARP entry number matching the filter conditions.
Verifying	ARP entry number at verifying again validity for ARP.
InCompleted	ARP entry number have ARP request sent without ARP reply.
Failed	ARP entry number at failed state.
None	ARP entry number at begin-found state.
Address	IP address of ARP entries.
Hardware Address	MAC address of ARP entries.
Interface	Layer 3 interface corresponding to the ARP entry.
Port	Physical (Layer2) port corresponding to the ARP entry.
Flag	Describes whether ARP entry is dynamic or static.

1.5.8 show arp traffic

Command: show arp traffic

Function: Display the statistic information of ARP messages of the switch. For box

switches, this command will only show statistics of APP messages received and sent from the current boardcard.

Command mode: Admin and Config Mode

Usage Guide: Display statistics information of received and sent APP messages.

Example:

Switch#show arp traffic

ARP statistics:

   Rcvd: 10 request, 5 response

   Sent: 5 request, 10 response

Chapter 2 Commands for ARP Scanning Prevention

2.1 anti-arpscan enable

Command: anti-arpscan enable

                no anti-arpscan enable

Function: Globally enable ARP scanning prevention function; "**no anti-arpscan enable**" command globally disables ARP scanning prevention function.

Parameters: None.

Default Settings: Disable ARP scanning prevention function.

Command Mode: Global configuration mode

User Guide: When remotely managing a switch with a method like telnet, users should set the uplink port as a Super Trust port before enabling anti-ARP-scan function, preventing the port from being shutdown because of receiving too many ARP messages. After the anti-ARP-scan function is disabled, this port will be reset to its default attribute, that is, Untrust port.

Example: Enable the ARP scanning prevention function of the switch.

Switch(config)#anti-arpscan enable

2.2 anti-arpscan port-based threshold

Command: anti-arpscan port-based threshold *<threshold-value>*

                no anti-arpscan port-based threshold

Function: Set the threshold of received messages of the port-based ARP scanning prevention. If the rate of received ARP messages exceeds the threshold, the port will be closed. The unit is packet/second. The "no anti-arpscan port-based threshold" command will reset the default value, 10 packets/second.

Parameters: rate threshold, ranging from 2 to 200.

Default Settings: 10 packets /second.

Command Mode: Global Configuration Mode.

User Guide: the threshold of port-based ARP scanning prevention should be larger than the threshold of IP-based ARP scanning prevention, or, the IP-based ARP scanning prevention will fail.

Example: Set the threshold of port-based ARP scanning prevention as 10 packets

/second.

Switch(config)#anti-arpscan port-based threshold 10

2.3 anti-arpscan ip-based threshold

Command: anti-arpscan ip-based threshold *<threshold-value>*

　　　　no anti-arpscan ip-based threshold

Function: Set the threshold of received messages of the IP-based ARP scanning prevention. If the rate of received ARP messages exceeds the threshold, the IP messages from this IP will be blocked. The unit is packet/second. The "no anti-arpscan ip-based threshold" command will reset the default value, 3 packets/second.

Parameters: rate threshold, ranging from 1 to 200.

Default Settings: 3 packets/second.

Command Mode: Global configuration mode

User Guide: The threshold of port-based ARP scanning prevention should be larger than the threshold of IP-based ARP scanning prevention, or, the IP-based ARP scanning prevention will fail.

Example: Set the threshold of IP-based ARP scanning prevention as 6 packets/second.

Switch(config)#anti-arpscan ip-based threshold 6

2.4 anti-arpscan trust

Command: anti-arpscan trust [port | supertrust-port]

　　　　no anti-arpscan trust [port | supertrust-port]

Function: Configure a port as a trusted port or a super trusted port;" **no anti-arpscan trust <port | supertrust-port>**"command will reset the port as an untrusted port.

Parameters: None.

Default Settings: By default all the ports are non- trustful.

Command Mode: Port configuration mode

User Guide: If a port is configured as a trusted port, then the ARP scanning prevention function will not deal with this port, even if the rate of received ARP messages exceeds the set threshold, this port will not be closed, but the non- trustful IP of this port will still be checked. If a port is set as a super trusted port, then neither the port nor the IP of the port will be dealt with. If the port is already closed by ARP scanning prevention, it will be opened right after being set as a trusted port.

When remotely managing a switch with a method like telnet, users should set the uplink port as a Super Trust port before enabling anti-ARP-scan function, preventing the port

from being shutdown because of receiving too many ARP messages. After the anti-ARP-scan function is disabled, this port will be reset to its default attribute, that is, Untrust port.

Example: Set port ethernet 1/0/5 of the switch as a trusted port.

Switch(config)#in e1/0/5

Switch(Config-If-Ethernet1/0/5)# anti-arpscan trust port

2.5 anti-arpscan trust ip

Command: anti-arpscan trust ip *<ip-address>* [*<netmask>*]

　　　　　no anti-arpscan trust ip *<ip-address>* [*<netmask>*]

Function: Configure trusted IP;" **no anti-arpscan trust ip *<ip-address>* [*<netmask>*]**"command reset the IP to non-trustful IP.

Parameters: *<ip-address>*: Configure trusted IP address; *<netmask>*: Net mask of the IP.

Default Settings: By default all the IP are non-trustful. Default mask is 255.255.255.255

Command Mode: Global configuration mode

User Guide: If a port is configured as a trusted port, then the ARP scanning prevention function will not deal with this port, even if the rate of received ARP messages exceeds the set threshold, this port will not be closed. If the port is already closed by ARP scanning prevention, its traffic will be recovered right immediately.

Example: Set 192.168.1.0/24 as trusted IP.

Switch(config)#anti-arpscan trust ip 192.168.1.0 255.255.255.0

2.6 anti-arpscan recovery enable

Command: anti-arpscan recovery enable

　　　　　no anti-arpscan recovery enable

Function: Enable the automatic recovery function, "**no anti-arpscan recovery enable**" command will disable the function.

Parameters: None

Default Settings: Enable the automatic recovery function

Command Mode: Global configuration mode

User Guide: If the users want the normal state to be recovered after a while the port is closed or the IP is disabled, they can configure this function.

Example: Enable the automatic recovery function of the switch.

Switch(config)#anti-arpscan recovery enable

2.7 anti-arpscan recovery time

Command: anti-arpscan recovery time *<seconds>*

      no anti-arpscan recovery time

Function: Configure automatic recovery time; "**no anti-arpscan recovery time**" command resets the automatic recovery time to default value.

Parameters: Automatic recovery time, in second ranging from 5 to 86400.

Default Settings: 300 seconds.

Command Mode: Global configuration mode

User Guide: Automatic recovery function should be enabled first.

Example: Set the automatic recovery time as 3600 seconds.

Switch(config)#anti-arpscan recovery time 3600

2.8 anti-arpscan log enable

Command: anti-arpscan log enable

      no anti-arpscan log enable

Function: Enable ARP scanning prevention log function; "**no anti-arpscan log enable**" command will disable this function.

Parameters: None.

Default Settings: Enable ARP scanning prevention log function.

Command Mode: Global configuration mode

User Guide: After enabling ARP scanning prevention log function, users can check the detailed information of ports being closed or automatically recovered by ARP scanning prevention or IP being disabled and recovered by ARP scanning prevention. The level of the log is "Warning".

Example: Enable ARP scanning prevention log function of the switch.

Switch(config)#anti-arpscan log enable

2.9 anti-arpscan trap enable

Command: anti-arpscan trap enable

      no anti-arpscan trap enable

Function: Enable ARP scanning prevention SNMP Trap function; "**no anti-arpscan trap enable**" command disable ARP scanning prevention SNMP Trap function.

Parameters: None.

Default Settings: Disable ARP scanning prevention SNMP Trap function.

Command Mode: Global configuration mode

User Guide: After enabling ARP scanning prevention SNMP Trap function, users will receive Trap message whenever a port is closed or recovered by ARP scanning prevention, and whenever IP t is closed or recovered by ARP scanning prevention.

Example: Enable ARP scanning prevention SNMP Trap function of the switch.

Switch(config)#anti-arpscan trap enable

2.10 show anti-arpscan

Command: show anti-arpscan [trust [ip | port | supertrust-port] |prohibited [ip | port]]

Function: Display the operation information of ARP scanning prevention function.

Parameters: None.

Default Settings: Display every port to tell whether it is a trusted port and whether it is closed. If the port is closed, then display how long it has been closed. Display all the trusted IP and disabled IP.

Command Mode: Admin Mode

User Guide: Use "**show anti-arpscan trust port**" if users only want to check trusted ports. The reset follow the same rule.

Example: Check the operating state of ARP scanning prevention function after enabling it.

Switch(config)#show anti-arpscan

Total port: 28

Name	Port-property	beShut	shutTime(seconds)
Ethernet1/0/1	untrust	N	0
Ethernet1/0/2	untrust	N	0
Ethernet1/0/3	untrust	N	0
Ethernet1/0/4	untrust	N	0
Ethernet1/0/5	untrust	N	0
Ethernet1/0/6	untrust	N	0
Ethernet1/0/7	untrust	N	0
Ethernet1/0/8	untrust	N	0
Ethernet1/0/9	untrust	N	0
Ethernet1/0/10	untrust	N	0
Ethernet1/0/11	untrust	N	0
Ethernet1/0/12	untrust	N	0
Ethernet1/0/13	untrust	N	0
Ethernet1/0/14	untrust	N	0

Ethernet1/0/15	untrust	N	0
Ethernet1/0/16	trust	N	0
Ethernet1/0/17	untrust	N	0
Ethernet1/0/18	supertrust	N	0
Ethernet1/0/19	untrust	Y	30
Ethernet1/0/20	trust	N	0
Ethernet1/0/21	untrust	N	0
Ethernet1/0/22	untrust	N	0
Ethernet1/0/23	untrust	N	0
Ethernet1/0/24	untrust	N	0
Ethernet1/0/25	untrust	N	0
Ethernet1/0/26	untrust	N	0
Ethernet1/0/27	untrust	N	0
Ethernet1/0/28	untrust	N	0

Prohibited IP:

IP	shutTime(seconds)
1.1.1.2	132

Trust IP:

192.168.99.5	255.255.255.255
192.168.99.6	255.255.255.255

2.11 debug anti-arpscan

Command: debug anti-arpscan [port | ip]

              no debug anti-arpscan [port | ip]

Function: Enable the debug switch of ARP scanning prevention; "**no debug anti-arpscan [port | ip]**" command disables the switch.

Parameters: None.

Default Settings: Disable the debug switch of ARP scanning prevention

Command Mode: Admin Mode

User Guide: After enabling debug switch of ARP scanning prevention users can check corresponding debug information or enable the port-based or IP-based debug switch separately whenever a port is closed by ARP scanning prevention or recovered automatically, and whenever IP t is closed or recovered .

Example: Enable the debug function for ARP scanning prevention of the switch.

Switch(config)#debug anti-arpscan

Chapter 3 Commands for Preventing ARP, ND Spoofing

3.1 ip arp-security updateprotect

Command: ip arp-security updateprotect

        no ip arp-security updateprotect

Function: Forbid ARP table automatic update. The "**no ip arp-security updateprotect**" command re-enables ARP table automatic update.

Parameter: None.

Default: ARP table automatic update.

Command Mode: Global Mode/ Interface configuration.

User Guide: Forbid ARP table automatic update, the ARP packets conflicting with current ARP item (e.g. with same IP but different MAC or port) will be dropped, the others will be received to update aging timer or create a new item; so, the current ARP item keep unchanged and the new item can still be learned.

Example:

Switch(Config-if-Vlan1)#ip arp-security updateprotect.

Switch(config)#ip arp-security updateprotect

3.2 ipv6 nd-security updateprotect

Command: ipv6 nd-security updateprotect

        no ipv6 nd-security updateprotect

Function: Forbid ND automatic update function of IPv6 Version, the no command resets ND automatic update function.

Parameter: None

Default: ND update normally.

Command Mode: Global Mode/ Interface configuration

User Guide: Forbid ND table automatic update, the ND packets conflicting with current ND item (e.g. with same IP but different MAC or port) will be droped, the others will be received to update aging timer or create a new item; so, the current ND item keep unchanged and the new item can still be learned.

Example:

Switch(Config-if-Vlan1)#ipv6 nd -security updateprotect

Switch(config)#ipv6 nd -security updateprotect

3.3 ip arp-security learnprotect

Command: ip arp-security learnprotect

            no ip arp-security learnprotect

Function: Forbid ARP learning function of IPv4 Version, the "**no ip arp-security learnprotect**" command re-enables ARP learning function.

Parameter: None.

Default: ARP learning enabled.

Command Mode: Global Mode/ Interface Configuration.

Usage Guide: This command is for preventing the automatic learning and updating of ARP. Unlike ip arp-security updateprotect, once this command implemented, there will still be timeout even if the switch keeps sending Request/Reply messages.

Example:

Switch(Config-if-Vlan1)# ip arp-security learnprotect

Switch(config)# ip arp-security learnprotect

3.4 ipv6 nd-security learnprotect

Command: ipv6 nd-security learnprotect

            no ipv6 nd-security learnprotect

Function: Forbid ND learning function of IPv6 Version, the no command re-enables ND learning function.

Parameter: None.

Default: ND learning enabled.

Command Mode: Global Mode/ Interface Configuration.

Usage Guide: This command is for preventing the automatic learning and updating of ND. Unlike ip nd-security updateprotect, once this command implemented, there will still be timeout even if the switch keeps sending Request/Reply messages.

Example:

Switch(Config-if-Vlan1)#ipv6 nd -security learnprotect

Switch(config)#ipv6 nd -security learnprotect

3.5 ip arp-security convert

Command: ip arp-security convert

Function: Change all of dynamic ARP to static ARP.

Parameter: None

Command Mode: Global Mode/ Interface configuration

Usage Guide: This command will convert the dynamic ARP entries to static ones, which, in combination with disabling automatic learning, can prevent ARP binding. Once implemented, this command will lose its effect.

Example:

Switch(Config-if-Vlan1)#ip arp -security convert

Switch(config)#ip arp -security convert

3.6 ipv6 nd-security convert

Command: ipv6 nd-security convert

Function: Change all dynamic ND to static ND.

Parameter: None

Command Mode: Global Mode/ Interface Configuration

Usage Guide: This command will convert the dynamic ND entries to static ones, which, in combination with disabling automatic learning, can prevent ND binding. Once implemented, this command will lose its effect.

Example:

Switch(Config-if-Vlan1)#ipv6 nd -security convert

Switch(config)#ipv6 nd -security convert

3.7 clear ip arp dynamic

Command: clear ip arp dynamic

Function: Clear all of dynamic ARP on interface.

Parameter: None

Command Mode: Interface Configuration

Usage Guide: This command will clear dynamic entries before binding ARP. Once implemented, this command will lose its effect.

Example:

Switch(Config-if-Vlan1)#clear ip arp dynamic

3.8 clear ipv6 nd dynamic

Command: clear ipv6 nd dynamic

Function: Clear all dynamic ND on interface.

Parameter: None

Command mode: Interface Configuration

Usage Guide: This command will clear dynamic entries before binding ND. Once implemented, this command will lose its effect.

Example:

Switch(Config-if-Vlan1)#clear ipv6 nd dynamic

Chapter 4 Command for ARP GUARD

4.1 arp-guard ip

Command: arp-guard ip <addr>
            no arp-guard ip <addr>
Function: Add an ARP GUARD address, the no command deletes ARP GUARD address.
Parameters: <addr> is the protected IP address, in dotted decimal notation.
Default: There is no ARP GUARD address by default.
Command Mode: Port configuration mode
Usage Guide: After configuring the ARP GUARD address, the ARP messages received from the ports configured ARP GUARD will be filtered. If the source IP addresses of the ARP messagse match the ARP GUARD address configured on this port, these messages will be judged as ARP cheating messages, which will be directly dropped instead of sending to the CPU of the switch or forwarding. 16 ARP GUARD addresses can be configured on each port.
Example:
Configure the ARP GUARD address on port ethernet1/0/1 as 100.1.1.1.
switch(config)#interface ethernet1/0/1
switch(Config-If-Ethernet 1/0/1)#arp-guard ip 100.1.1.1
Delete the ARP GUARD address on port ethernet1/0/1 as 100.1.1.1.
switch(config)#interface ethernet1/0/1
switch(Config-If-Ethernet 1/0/1)#no arp-guard ip 100.1.1.1

Chapter 5 Command for ARP Local Proxy

5.1 ip local proxy-arp

Command: ip local proxy-arp

        no ip local proxy-arp

Function: Enable/disable the local ARP Proxy function of a specified interface.

Parameters: None.

Default Settings: This function is disabled on all interfaces by default.

Command Mode: Interface VLAN Mode.

User Guide: This function is disabled on all interfaces by default, and differs from the original proxy-arp in that this function acts as an ARP Proxy inside the same layer-3 interface and thus directs the layer-3 forwarding of the switch.

Example: Enable the local ARP Proxy function of interface VLAN1.

Switch(Config-if-Vlan1)# ip local proxy-arp

Chapter 6 Commands for Gratuitous ARP Configuration

6.1 ip gratuitous-arp

Command: ip gratuitous-arp [<*interval-time*>]

          no ip gratuitous-arp

Function: To enabled gratuitous ARP, and specify update interval for gratuitous ARP. The no form of this command will disable the gratuitous ARP configuration.

Parameters: <*interval-time*> is the update interval for gratuitous ARP with its value limited between 5 and 1200 seconds and with default value as 300 seconds.

Command Mode: Global Configuration Mode and Interface Configuration Mode.

Default: Gratuitous ARP is disabled by default.

Usage Guide: When configuring gratuitous ARP in global configuration mode, all the Layer 3 interfaces in the switch will be enabled to send gratuitous ARP request. If gratuitous ARP is configured in interface configuration mode, then only the specified interface is able to send gratuitous ARP requests. When configuring the gratuitous ARP, the update interval configuration from interface configuration mode has higher preference than that from the global configuration mode.

Example:

1)   To enable gratuitous ARP in global configuration mode, and set the update interval to be 400 seconds.

Switch>enable

Switch#config

Switch(config)#ip gratuitous-arp 400

2)   To enable gratuitous ARP for interface VLAN 10 and set the update interval to be 350 seconds.

Switch(config)#interface vlan 10

Switch(Config-if-Vlan10)#ip gratuitous-arp 350

6.2 show ip gratuitous-arp

Command: show ip gratuitous-arp [interface vlan <*vlan-id*>]

Function: To display configuration information about gratuitous ARP.

Parameters: <*vlan-id*> is the VLAN ID. The valid range for <*vlan-id*> is between 1 and

4094.

Command Mode: All the Configuration Modes.

Usage Guide: In all the configuration modes, the command **show ip gratuitous arp** will display information about the gratuitous ARP configuration in global and interface configuration mode. The command **show ip gratuitous-arp interface vlan** *<vlan-id>* will display information about the gratuitous ARP configuration about the specified VLAN interface.

Example:

1) To display information about gratuitous ARP configuration in both global and interface configuration modes.

Switch#show ip gratuitous-arp

Gratuitous ARP send is Global enabled, Interval-Time is 300(s)

Gratuitous ARP send enabled interface vlan information:

Name	Interval-Time(seconds)
Vlan1	400
Vlan10	350

2) To display gratuitous ARP configuration information about interface VLAN 10.

Switch#show ip gratuitous-arp interface vlan 10

Gratuitous ARP send interface Vlan10 information:

Name	Interval-Time(seconds)
Vlan10	350

Chapter 7 Commands for ND Snooping

7.1 clear ipv6 nd snooping binding

Command: clear ipv6 nd snooping binding [<*interface-name*>]

Function: Clear all dynamic binding of ND Snooping.

Parameter: <*interface-name*> the name of an ethernet port.

Default: None.

Command mode: Admin Mode.

Usage Guide: Clear all ND Snooping binding table or binding entries of a port, the entries of the corresponding FFP hardware drive will also be cleared.

Example:

Switch(config)#ipv6 nd snooping enable

Switch# clear ipv6 nd snooping binding

7.2 debug ipv6 nd snooping

Command: debug ipv6 nd snooping {packet | event | binding}

              no debug ipv6 nd snooping {packet | event | binding}

Function: Open/close the debug of ND Snooping.

Parameter: packet shows debug information of received and sent ND packets, **event** shows debug information that ND snooping processes the packets and the timer event, **binding** shows the debug information of ND Snooping managing the binding table.

Default: Disable the debug information.

Command mode: Port Mode.

Usage Guide: Open the debug information switch of ND Snooping.

Example: Show the debug information of ND Snooping.

Switch#debug ipv6 nd snooping packet

        Receive packet, smac 00-21-27-aa-0f-46, dmac 00-03-0f-00-de-01,

        saddr fe80::221:27ff:feaa:f46, daddr 2001::1,

        interface Ethernet1/0/17(portID 0x1000011), vid 1, length 90,

        type 135, opcode 0, target address 2001::1

7.3 ipv6 nd snooping enable (Global mode)

Command: ipv6 nd snooping enable

        no ipv6 nd snooping enable

Function: Enable/disable the monitoring function of ND Snooping globally.

Parameter: None.

Command mode: Global Mode.

Default: Disable the global function of ND Snooping.

Usage Guide: Only after ND Snooping enabled globally, the port configuration of ND Snooping is allowed, NA/NS packets of all ports are not forwarded, but are copied to cpu. After being processed by ND Snooping, these packets are forwarded according to the set rules.

Example: Enable the ND Snooping globally.

Switch(config)#ipv6 nd snooping enable

7.4 ipv6 nd snooping mac-binding-limit

Command: ipv6 nd snooping mac-binding-limit *<number>*

        no ipv6 nd snooping mac-binding-limit

Function: Configure the max number of IPv6 addresses that can be bound to the same MAC address.

Parameter: *<number>* is the max value. It only includes the dynamic binding number, the corresponding static binding number is not limited, the range from 1 to 10.

Default: 10.

Command mode: Global Mode.

Usage Guide:

a) After receiving this configuration command, set globally the max number of dynamic binding which relate to the same MAC address.

b) Account the binding value which corresponds with each MAC address globally. If the corresponding dynamic binding number of one MAC address exceeds the configuration value, then delete some dynamic binding which have a high age until the number of the dynamic binding equals this configuration value, and stop the binding corresponding with this MAC address. If the numberr of binding is less than the configuration value, the new dynamic binding can still be created.

Example: Set the max number of the corresponding dynamic binding for the same MAC address.

Switch(config)#ipv6 nd snooping enable

Switch(config)# ipv6 nd snooping mac-binding-limit 10

7.5 ipv6 nd snooping max-dad-delay

Command: ipv6 nd snooping max-dad-delay *<max-dad-delay>*
               no ipv6 nd snooping max-dad-delay
Function: Set the lifetime of SAC_START state for a binding.
Parameter: *<max-dad-delay>* is the lifetime of SAC_START state, the range from 1 to 10, the unit is second.
Command mode: Global Mode.
Default: SAC_START state binds the lifetime as 1 second.
Usage Guide: Reset the binding lifetime of SAC_START state as *<max-dad-delay>* or 1 second.
Example: Configure the lifetime as 10 seconds.
Switch(config)#ipv6 nd snooping enable
Switch(config)#ipv6 nd snooping max-dad-delay 10

7.6 ipv6 nd snooping max-dad-prepare-delay

Command: ipv6 nd snooping max-dad-prepare-delay *<max-dad-prepare-delay>*
               no ipv6 nd snooping max-dad-prepare-delay
Function: Set the lifetime of SAC_QUERY state for a binding.
Parameter: *<max-dad-prepare-delay>* is the lifetime of SAC_QUERY state, the range from 1 to 10, the unit is second.
Command mode: Global Mode.
Default: SAC_QUERY state binds the lifetime as half a second.
Usage Guide: Reset the binding lifetime of SAC_QUERY state as *<max-dad-prepare-delay>* or half a second.
Example: Configure the lifetime as 10 seconds.
Switch(config)#ipv6 nd snooping enable
Switch(config)#ipv6 nd snooping max-dad-prepare-delay 10

7.7 ipv6 nd snooping max-sac-lifetime

Command: ipv6 nd snooping max-sac-lifetime *<max-sac-lifetime>*
               no ipv6 nd snooping max-sac-lifetime
Function: Set the lifetime of SAC_BOUND state for a binding.

Parameter: ***<max-sac-lifetime>*** is the lifetime of SAC_BOUND state, the range from 1 to 31536000, the unit is second.

Default Configuration: SAC_BOUND state binds the lifetime as 2 hours (7200 seconds).

Command mode: Global Mode.

Default: SAC_BOUND state binds the lifetime as 2 hours. (7200 seconds)

Usage Guide: Change the lifetime of SAC_BOUND state.

Example: Configure the lifetime as 36000 seconds.

Switch(config)#ipv6 nd snooping enable

Switch(config)#ipv6 nd snooping max-sac-lifetime 36000

7.8 ipv6 nd snooping policy

Command: ipv6 nd snooping policy {bind-eui64-address | bind-non-eui64-address}
          no ipv6 nd snooping policy

Function: Configure the dynamic binding policy of ND Snooping addresses.

Parameter: bind-eui64-address means only the address of the global unicast EUI-64 is bound, bind-non-eui64-address means the global unicast address of non EUI-64 is bound, default means the global unicast address is bound.

Command mode: Global Mode.

Default: Bind any global unicast addresses by default.

Usage Guide: After the policy is configured, only bind the IPv6 addresses which are specified by the policy, a message is displayed for a non policy specifies the global unicast address to report the conflict.

Example: Configure binding the global unicast EUI-64.

Switch(config)#ipv6 nd snooping enable

Switch(config)#ipv6 nd snooping policy bind-eui64-address

7.9 ipv6 nd snooping port-binding-limit

Command: ipv6 nd snooping port-binding-limit *<binding-number>*
          no ipv6 nd snooping port-binding-limit

Function: Configure the binding number of the port. This binding number only limits the dynamic binding number of the port, but do not limit the number of the static binding.

Parameter: binding-limit is the max number which can be bound for each port, the range from 1 to 100.

Command mode: Port Mode.

Default: 100

Usage Guide:

a) After receiving this configuration command, set the max value of the dynamic binding for this port.

b) Check the dynamic binding of this port and account the number of the dynamic binding. If the number exceeds this configuration value, then delete some dynamic binding which have a high age until the number of the dynamic binding equals this configuration value, and stop creating new dynamic binding of this port. If the number of the dynamic binding is less than this configuration value, new dynamic binding can still be created.

Example: Configure the number which can be bound by the port.

Switch(config)#ipv6 nd snooping enable

Switch(config-if-ethernet1/0/1)#ipv6 nd snooping port-binding-limit 100

7.10 ipv6 nd snooping static-binding

Command: ipv6 nd snooping static-binding *<ipv6-address>* hardware-address

<hardware-address> **interface *<interface-name >***

> **no ipv6 nd snooping static-binding *<ipv6-address>***

Function: Add a static binding.

Parameter: ipv6-address can bind the global unicast address only, can not bind the link local address , the unspecific address and the loopback address, **hardware-address** is the MAC address of IEEE802 hardware, **interface-name** is the corresponding port ID.

Command mode: Global Mode.

Default: None.

Usage Guide:

a) Check the configured IPv6 addresses, if the configured addresses are the multicast address of the nodes, the local address of the link, the unspecific address and the loopback address, then show the error information and return.

b) According to the IPv6 address and the MAC address of the configuration command to check the static binding table. If the IPv6 address binding exists, then give the binding information of this IPv6 address and return. If there is no IPv6 address binding, then create new static binding. If ND Snooping has been enabled in the binding port, then send the binding entries to FFP hardware drive.

c) Checking the dynamic binding table, if exist the dynamic binding for matching the static binding completely, then delete this dynamic binding and keep the entries in FFP hardware drive. If exist the binding corresponding with the IPv6 address, and the anchor information is different, then delete this dynamic binding and the entries in FFP hardware drive.

Example: Add a new type of the binding table in the static binding table.

Switch(config)#ipv6 nd snooping enable

Switch(config)#ipv6 nd snooping static-binding 2001::2:1 hardware-address 00-11-22-33-44-55 interface ethernet1/0/1

7.11 ipv6 nd snooping trust

Command: ipv6 nd snooping trust

            no ipv6 nd snooping trust

Function: Set the trust port of the switch.

Parameter: None.

Command mode: Port Mode.

Default: un-trusted port.

Usage Guide: This command sets a port or a group of ports as the trust port and deletes all dynamic binding corresponding with the port or ports, stop creating new binding of port or ports, and accessing of packets is also allowed.

Example: Set a port or a group of ports as the trust ports.

Switch(config)#interface ethernet1/0/1

Swithc(config-if-ethernet1/0/1)# ipv6 nd snooping trust

7.12 ipv6 nd snooping user-control

Command: ipv6 nd snooping user-control

            no ipv6 nd snooping user-control

Function: Enable the control function of the ports for ND Snooping.

Parameter: None.

Command mode: Port Mode.

Default: Disable the control function of ND Snooping.

Usage Guide: After the control function of ND Snooping is disabled, clear all FFP drive entries which are sent by ND Snooping for this port, but the binding information is not deleted.

Example: Configure ND Snooping function on the port.

Switch(config)#ipv6 nd snooping enable

Switch(config)#interface ethernet 1/0/1

Swithc(config-if-ethernet1/0/1)# ipv6 nd snooping user-control

7.13 show ipv6 nd snooping binding

Command: show ipv6 nd snooping binding [<*ipv6-address*> | <*hardware-address*> | <*interface-name*> | <*all*>]

Function: Show the global configuration and all binding information of ND Snooping, or the configuration and the binding information of a port.

Parameter: ipv6-address: Show the binding information according to the specified IPv6 address.

hardware-address: Show the binding information according to the specified MAC address.

interface-name: Show the binding information according to the specified port.

all: Show all information.

Default: None.

Command mode: Admin Mode.

Usage Guide: Show the configuration and the binding information of ND Snooping.

Example:

Switch#show ipv6 nd snooping binding all

ND Snooping is enabled

ND Snooping max-dad-delay: 1 s

ND Snooping max-sac-lifetime:7200 s

ND Snooping max-dad-prepare-delay: 0.5 s

ND Snooping max-mac-binding-num: 10

ND Snooping binding-policy: bind-all-type-address

ND Snooping auto binding count: 0, static binding count: 1

MAC	IPv6 address	Interface	Vlan ID	State
00-11-22-33-44-55	2001::2:1	Ethernet1/0/1	1	SAC_STATIC

Chapter 8 Commands for Keepalive Gateway

8.1 keepalive gateway

Command: keepalive gateway *<ip-address>* [{*<interval-seconds>* | msec *<interval-millisecond>*} [retry-count]]

            no keepalive gateway

Function: Enable keepalive gateway, configure the interval that ARP request packet is sent and the retry-count after detection is failing, the no command disables the function.

Parameters: ip-address: IP address of the gateway

        interval-seconds: The interval (unit is second) that ARP request packet is sent, ranging between 1 and 32767. If there is no configuration, the default is 10 seconds.

        interval-millisecond: The interval (unit is millisecond) that ARP request packet is sent, ranging between 160 and 999.

        retry-count: Determine the retry-count after detection is failing. If there is no configuration, the default is 5 times.

Default: Disable keepalive gateway.

Command Mode: Interface mode.

Usage Guide: This command is supported by layer 3 switch and the detection method is used to point-to-point topology mode only.

Example:

Switch(config)#interface vlan 1

Switch(config-if-vlan1)#keealive gateway 1.1.1.1 3 10

8.2 show ip interface

Command: show ip interface [interface-name]

Function: Show IPv4 running status of the specified interface.

Parameters: interface-name is the specified interface name. If there is no parameter, show IPv4 running status of all interfaces.

Default: None.

Command Mode: Admin and configuration mode.

Usage Guide: Show IPv4 running status of the interface.

Example:

Switch(config)#show ip interface brief

Index	Interface	IP-Address	Protocol
3001	Vlan1	1.1.1.2	up
9000	Loopback	127.0.0.1	up

8.3 show keepalive gateway

Command: show keepalive gateway [interface-name]

Function: Show keepalive running status of the specified interface.

Parameters: interface-name is the specified interface name. If there is no parameter, show keepalive running status of all interfaces.

Default: None.

Command Mode: Admin and configuration mode.

Usage Guide: Show keepalive running status of the interface.

Example:

Switch(config)#show keepalive gateway

interface Vlan1 gateway 1.1.1.1 time 10s retry 1 remain 4 now UP