Content

Chapter 1 Commands for Layer 3 Management

1.1 Commands for Layer 3 Interface

1.1.1 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

1.1.2 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. Configure 16 interface vlan to manage device that is supported by layer 2 switch, but layer 3 forward is not supported.
Example: Create a VLAN interface (layer 3 interface).

Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#

1.1.3 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

1.1.4 show ip route

Command: show ip route [database]
Function: Display routing table.
Parameter: database is database information.
Command Mode: Admin Mode
Usage Guide: Show kernal routing table, include: routing type, destination network, mask, next-hop address, interface, etc.
Example:
Switch#show ip route
Codes: C - connected, S - static, R - RIP derived, O - OSPF derived
A - OSPF ASE, B - BGP derived
Destination Mask Nexthop Interface Pref
C 2.2.2.0 255.255.255.0 0.0.0.0 vlan2 0
C 4.4.4.0 255.255.255.0 0.0.0.0 vlan4 0
S 6.6.6.0 255.255.255.0 9.9.9.9 vlan9 1

Displayed information	Explanation
C –connected	Direct route, namely the segment directly connected with the layer 3 switch
S –static	Static route, the route manually configured by users
R - RIP derived	RIP route, acquired by layer 3 switch through the RIP protocol.
O - OSPF derived	OSPF route, acquired by layer 3 switch through the OSPF protocol
A- OSPF ASE	Route introduced by OSPF
B- BGP derived	BGP route, acquired by the BGP protocol.

Destination	Target network
Mask	Target network mask
Nexthop	Next-hop IP address
Interface	Next-hop pass-by layer 3 swtich interfaces
Preference	Route priority. If other types of route to the target network exists, the kernel route will only shows those with high priority.

1.2 Commands for IPv4/v6 configuration

1.2.1 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

1.2.2 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

1.2.3 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

1.2.4 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

1.2.5 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

1.2.6 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

1.2.7 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

1.2.8 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

1.2.9 ip default-gateway

This command is not supported by the switch.

1.2.10 ip route

Command: ip route {<ip-prefix> <mask> | <ip-prefix>/<prefix-length>} {<gateway-address> | <gateway-interface>} [<distance>]

no ip route {*<ip-prefix>* *<mask>* | *<ip-prefix>/<prefix-length>*} [*<gateway-address>* | *<gateway-interface>*] [*<distance>*]

Function: Configure the static route. The no command deletes the static route.

Parameter: ***<ip-prefix>*** and ***<mask>*** are respectively destination IP address and subnet mask, shown in dotted decimal notation; ***<ip-prefix>*** and ***<prefix-length>*** are respectively the destination IP address and the length of prefix; ***<gateway-address>*** is the next-hop IP address shown in dotted decimal notation; ***<gateway-interface>*** is the next-hop interface; ***< distance >*** is the distance value of route management, the range is 1 to 255.

Default: The default distance value of route management is 1.

Command Mode: Global Mode.

Usage Guide: When configuring the next-hop of static route, the next-hop IP address of route packets and the manner of egress or interface can be appointed.

The distance values of all kinds of the switch routes are the following:

Route Type	Distance Value
Directly Connected Routes	0
Static Routes	1
OSPF	110
RIP	120
IBGP	200
EBGP	20

At the case of no chaging the distance value of all kinds of routes, the priority of directly connected routes is the highest, the static routes, EBGP, OSPF, RIP and IBGP are followed.

Example:

1. Add a static route.

Switch(config)#ip route 1.1.1.0 255.255.255.0 2.1.1.1

2. Add the default route.

Switch(config)#ip route 0.0.0.0 0.0.0.0 2.2.2.1

1.2.11 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.

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

1.2.12 ipv6 default-gateway

This command is not supported by the switch.

1.2.13 ipv6 route

Command: ipv6 route <*ipv6-prefix* | *prefix-length*> {<*ipv6address*> | <*interface-type interface-number*> | {<*ipv6address*> <*interface-type interface-number*>}} [<*precedence*>]

no ipv6 route <*ipv6-prefix* | *prefix-length*> {<*ipv6address*> | <*interface-type interface-number*> | {<*ipv6address*> <*interface-type interface-number*>}} [<*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, 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.

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

1.2.14 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

1.2.15 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

1.2.16 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

1.2.17 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

1.2.18 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

1.2.19 ipv6 nd min-ra-interval

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

no ipv6 nd min-ra-interval

Function: Set the minimum interval of sending routing message.

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

Command Mode: Interface Configuration Mode

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

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

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

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

1.2.20 ipv6 nd max-ra-interval

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

no ipv6 nd max-ra-interval

Function: Set the maximum interval of sending routing message.

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

Command Mode: Interface Configuration Mode

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

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

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

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

1.2.21 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

1.2.22 ipv6 nd other-config-flag

Command: ipv6 nd other-config-flag

Function: Set other-config-flag as 1 for sending route announcement.

Parameters: None.

Command Mode: Interface Configuration Mode.

Default: other-config-flag is 0.

Usage Guide: If other-config-flag is 1, the host (receive the route announcement) must use the address configuration protocol (such as DHCPv6) to obtain non-address configuration (such as DNS address).

Examples: Set other-config-flag that send route announcement.

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

1.2.23 ipv6 nd managed-config-flag

Command: ipv6 nd managed-config-flag

no ipv6 nd managed-config-flag

Function: Set managed-config-flag as 1 for sending route announcement.

Parameters: None.

Command Mode: Interface Configuration Mode.

Default: managed-config-flag is 0.

Usage Guide: If managed-config-flag is 1, the host (receive the route announcement) must use the address configuration protocol (such as DHCPv6) to obtain the address and may use the non-state address configuration protocol to obtain the address. If managed-config-flag is 0, the host use the non-state address configuration protocol to obtain the address only.

Examples: Set managed-config-flag that send route announcement.

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

1.2.24 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, 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

1.2.25 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

1.2.26 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	Statistics of total ICMP packets received and classified information

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	Statistics of total ICMP packets sent and classified information
TCP statistics:	TCP packet statistics.
UDP statistics:	UDP packet statistics.

1.2.27 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

1.2.28 show ipv6 route

Command: show ipv6 route [database]
Function: Display IPv6 routing table.
Parameter: 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.
Example:
Switch#show ipv6 route
Codes: C - connected, L - Local, S - static, R - RIP, O - OSPF,
I - IS-IS, B - BGP

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 2003:1::/64 via ::, Vlan4 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 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.

1.2.29 show ipv6 neighbors

Command: show ipv6 neighbors [{vlan|ethernet} interface-number | interface-name | address <*ipv6address*>]
Function: Display neighbor table entry information.
Parameter: Parameter **{vlan|ethernet} 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 Ethernet 1/0/3 reachable
3ffe:3240:800d:1::8888 00-02-01-00-00-00 Vlan1 Ethernet 1/0/1 permanent
3ffe:3240:800d:1:250:baff:fef2:a4f4 00-50-ba-f2-a4-f4 Vlan1 Ethernet 1/0/4 reachable
3ffe:3240:800d:2::8888 00-02-01-00-01-01 Vlan2 Ethernet 1/0/16 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 Ethernet 1/0/5 reachable
fe80::203:fff:fefe:3045 00-03-0f-fe-30-45 Vlan2 Ethernet 1/0/17 reachable
fe80::20c:ceff:fe13:eac1 00-0c-ce-13-ea-c1 Vlan12 Ethernet 1/0/20 reachable
fe80::250:baff:fef2:a4f4 00-50-ba-f2-a4-f4 Vlan1 Ethernet 1/0/6 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)

1.2.30 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 destination0 header errors, 0 address errors0 unknown protocol, 13 discards	IPv6 received packets statistics
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

1.2.31 show ipv6 redirect

This command is not supported by the switch.

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 ARP Configuration

1.4.1 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. **The** maximum **of static number is 1000.**

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

1.4.2 clear arp-cache

Command: clear arp-cache

Function: Clears ARP table.

Command mode: Admin Mode

Example:

Switch#clear arp-cache

1.4.3 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

1.4.4 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.

1.4.5 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

1.4.6 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

1.4.7 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.

1.4.8 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 4/5 of the switch as a trusted port.

Switch(config)#in e4/5

Switch(Config-If-Ethernet4/5)# 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
Ethernet4/1        untrust        N       0
Ethernet4/2        untrust        N       0
Ethernet4/3        untrust        N       0
Ethernet4/4        trust          N       0
Ethernet4/5        untrust        N       0
Ethernet4/6        supertrust     N       0
Ethernet4/7        untrust        Y       30
Ethernet4/8        trust          N       0
Ethernet4/9        untrust        N       0
Ethernet4/10       untrust        N       0
Ethernet4/11       untrust        N       0
Ethernet4/12       untrust        N       0
Ethernet4/13       untrust        N       0
Ethernet4/14       untrust        N       0
Ethernet4/15       untrust        N       0
Ethernet4/16       untrust        N       0
Ethernet4/17       untrust        N       0
Ethernet4/18       untrust        N       0
Ethernet4/19       untrust        N       0
Ethernet4/20       untrust        N       0
Ethernet4/21       untrust        N       0
Ethernet4/22       untrust        N       0
```

Ethernet4/23 untrust N 0
Ethernet4/24 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 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

This command is not supported by the switch.

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

This command is not supported by the switch.

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

This command is not supported by the switch.

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 Commands for Gratuitous ARP Configuration

5.1 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
```

5.2 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 6 Commands for Dynamic ARP Inspection

6.1 ip arp inspection

Command: ip arp inspection vlan <vlan-id>

no ip arp inspection vlan <vlan-id>

Function: Enable the dynamic ARP inspection function based on vlan.

Parameters: <vlan-id> is the vlan which is enabled the dynamic ARP inspection function.

Command Mode: Global Mode.

Default: Disable.

Usage Guide: After configured the dynamic ARP inspection function in global mode, the administrator can intercept, record and drop the ARP data packets which have the invalid MAC address/IP address.

Example: Enable the dynamic ARP inspection function of vlan10.

Switch(config)#

Switch(config)#ip arp inspection vlan 10

Switch(config)#exit

6.2 ip arp inspection trust

Command: ip arp inspection trust

no ip arp inspection trust

Function: Configure the port as the trusted port of the dynamic ARP inspection.

Parameters: None.

Command Mode: Port Mode.

Default: All the ports are the untrusted ports as default.

Usage Guide: After configured this command under the port mode, the configured port will not inspect the received ARP packet and it will forward it directly. If the ARP data packet is received from the untrusted port, the switch will only forward the lawful data packet. For the illegal data, it will drop the data directly and record this action.

Example: Configure the port 1/0/1 as the trusted port.

Switch(config)#

Switch(config)#in e 1/0/1

Switch(config-if-ethernet1/0/1)#ip arp inspection trust

Switch(config-if-ethernet1/0/1)#exit

6.3 ip arp inspection limit-rate

Command: ip arp inspection limit-rate <rate>

no ip arp inspection limit-rate

Function: Limit the ARP packet rate of the untrusted port.

Parameters: <rate> is the configured limited rate of the ARP packet of the untrusted port, the unit is pps.

Command Mode: Port Mode.

Default: Do not limit the rate for the ARP packets of the trusted or untrusted ports.

Usage Guide: This command can limit the ARP packet rate of the untrusted port. The rate of the lawful ARP data packets forwarding is in the limited range.

Example: Configure the rate of the ARP packet of the untrusted port 1/0/1 as 100pps.

Switch(config)#

Switch(config)#in e 1/0/1

Switch(config-if-ethernet1/0/1)# ip arp inspection limit-rate 100

Switch(config-if-ethernet1/0/1)#exit