07-Commands for Layer 3 Forward and ARP

Directory

1.Commands for Layer 3 Interface 1
description 1
interface vlan 1
no interface IFNAME 1
show ip route 2
2.Commands for IPv4/v6 configuration 3
clear ip traffic 3
clear ipv6 neighbor 3
ip address 4
ip default-gateway 4
ipv6 address 5
ipv6 nd dad attempts 5
ipv6 nd ns-interval 6
ipv6 neighbor 6
show ip interface 7
show ip traffic 7
show ipv6 interface 9
show ipv6 route 10
show ipv6 neighbors 11
show ipv6 traffic 11
ip route 13
3.Commands for ARP Configuration 13
arp 13
clear arp-cache 14
clear arp traffic 14
show arp 14
show arp traffic 16
4.Commands for ARP Scanning Prevention 16
anti-arpscan enable 16
anti-arpscan port-based threshold 16
anti-arpscan ip-based threshold 17
anti-arpscan trust 17
anti-arpscan trust ip 18
anti-arpscan recovery enable 18
anti-arpscan recovery time 19
anti-arpscan log enable 19
anti-arpscan trap enable 19
show anti-arpscan 20
5.Commands for Preventing ARP Spoofing 21
ip arp-security updateprotect 21
ip arp-security learnprotect 21
ip arp-security convert 22
clear ip arp dynamic 22
clear ipv6 nd dynamic 22
6.Command for ARP GUARD 23
arp-guard ip 23
7.Commands for Gratuitous ARP Configuration 23
ip gratuitous-arp 23

show ip gratuitous-arp..... 24
8.Commands for Dynamic ARP Inspection 25
ip arp inspection 25
ip arp inspection trust..... 25
ip arp inspection limit-rate 25

1.Commands for Layer 3 Interface

description

Command	**description <*text*>** **no description**	
parameter	***text***	is the description information of VLAN interface, the length should not exceed 256 characters
default	Do not configure	
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	

interface vlan

Command	**interface vlan <*vlan-id*>** **no interface vlan <*vlan-id*>**	
parameter	***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.	
Mode	Global Mode	
Usage Guide	this command is used to create the 3-layer interface, no the command is used to delete the 3-layer interface.	
Example	Create a VLAN interface (layer 3 interface). Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#	

no interface IFNAME

Command	**no interface IFNAME**

parameter	**IFNAME** Interface Name
default	-
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

show ip route

Command	**show ip route [database]**
parameter	**database** is database information.
default	-
Mode	Admin Mode
Usage Guide	Show kernal routing table, include: routing type, destination network, mask, next-hop address, interface, etc.
Example	shows the routing table. Switch#show ip route Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default C 127.0.0.0/8 is directly connected, Loopback tag:0 Total routes are : 1 item(s)

Display information	describe
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.

2.Commands for IPv4/v6 configuration

clear ip traffic

Command	**clear ip traffic**
parameter	-
default	-
Mode	Admin Mode.
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

clear ipv6 neighbor

Command	**clear ipv6 neighbors**
parameter	-
default	-
Mode	Admin Mode.
Usage Guide	This command can not clear static neighbor
Example	Clear neighbor list. Switch#clear ipv6 neighbors

ip address

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

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.

default	The system default is no IP address configuration.
Mode	VLAN interface configuration mode
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

ip default-gateway

Command	**ip default-gateway <A.B.C.D>** **no ip default-gateway <A.B.C.D>**

parameter

A.B.C.D	is gateway address, for example 10.1.1.10.

default	There is no default gateway.
Mode	Global mode.
Usage Guide	Configure the default gateway of the router to specify the default next hop address to which the packets will be sent.
Example	Specifies the default gateway.Switch(config)# ip default-gateway 10.1.1.10

ipv6 address

Command	**ipv6 address <ipv6-address|prefix-length> [eui-64]** **no ipv6 address <ipv6-address|prefix-length> [eui-64]**	
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.
default	-	
Mode	Interface Configuration Mode	
Usage Guide	IPv6 address prefix cannot be multicast address or any other specific IPv6 address, and different layer 3 interfaces cannot 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	

ipv6 nd dad attempts

Command	**ipv6 nd dad attempts <*value*>** **no ipv6 nd dad attempts**	
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.
default	The default request message number is 1	
Mode	Interface Configuration Mode	
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	

ipv6 nd ns-interval

Command	**ipv6 nd ns-interval <*seconds*>** **no ipv6 nd ns-interval**

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.

default	The default Request Message time interval is 1 second.
Mode	Interface Configuration Mode
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

ipv6 neighbor

Command	**ipv6 neighbor <*ipv6-address*> <*hardware-address*> interface <*interface-type interface-name*>** **no ipv6 neighbor <*ipv6-address*>**

parameter	***ipv6-address***	is static neighbor IPv6 address
	hardware-address	is static neighbor hardware address
	interface-type	is Ethernet type,
	interface-name	is Layer 2 interface name

default	There is not static neighbor table entry
Mode	Interface Configuration Mode
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

show ip interface

Command	**show ip interface [<*ifname*> | vlan <*vlan-id*>] brief**
parameter	***ifname*** Interface name ***vlan-id*** VLAN ID
default	Show all brief information of the configured layer 3 interface when no parameter is specified.
Mode	All modes.
Usage Guide	This command is used to view brief information on the configured Layer 3 interface.
Example	view brief information on vlan1 interface configuration. Switch#show ip interface vlan 1 brief Index Interface IP-Address Protocol 11001 Vlan1 192.168.2.1 up

show ip traffic

Command	**show ip traffic**
parameter	-
default	-
Mode	Admin Mode
Usage Guide	Display statistics for IP, ICMP, TCP, UDP packets received/sent.
Example	Displays statistics for IP packets. 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

Display content	describe
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 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.

show ipv6 interface

Command

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

parameter

brief	is the brief summarization of IPv6 status and configuration
interface-name	is Layer 3 interface name

default

-

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

View information ipv6 the vlan1 interface.

```
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)

Display content	describe
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

show ipv6 route

Command **show ipv6 route [database]**

parameter

database	is router database

default -

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

Display IPv6 Routing Table.
Switch#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
I - IS-IS, B - BGP
Timers: Uptime

C ::1/128 via ::, Loopback, 02:55:37 tag:0

Display content	describe
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	Abbreviation display sign of every entry

show ipv6 neighbors

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

parameter

{vlan|ethernet} interface-number	specify the lookup based on interface
ipv6address	specifies the lookup based on IPv6 address. It displays the whole neighbor table entry if without parameter.

default

-

Mode

Admin and Configuration Mode

Usage Guide

Displays neighbor table information. If there are no parameters, the entire neighbor table entry is displayed.

Example

Check ipv6 Neighbor Table Information.

```
Switch#show ipv6 neighbors
IPv6 neighbour unicast items: 2, valid: 1, matched: 1, incomplete: 0, delayed: 0,
        manage items: 0
IPv6  Address                                  Hardware  Addr          Interface
Port                    State       Age-time(sec)
fe80::d8e4:a662:88e4:dc24                      00-e0-4c-21-00-34       Vlan1
Ethernet1/0/18          reachable   563

IPv6 neighbour table: 1 entries
```

Display content	describe
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)

show ipv6 traffic

Command	**show ipv6 traffic**

parameter

-

default

-

Mode

Admin and Configuration Mode

Usage Guide

Display IPv6 transmit packet statistics.

Example

Display IPv6 transmit packet statistics.

```
Switch#show ipv6 traffic
IPv6 statistics:
  Rcvd:  27 total, 21 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:  24 generated, 0 forwarded
         0 dropped, 0 no route
ICMPv6 statistics:
  Rcvd:  21 total, 0 errors
         0 unreachable, 0 too big, 0 time exceeded, 0 parameter problems
         0 echo requests, 0 echo replies
         0 group queries, 0 group responses, 0 group reduces
         0 router solicits, 0 router adverts, 0 redirects
         9 neighbor solicits, 12 neighbor adverts
  Sent:  24 total, 0 errors
         0 unreachable, 0 too big, 0 time exceeded, 0 parameter problems
         0 echo requests, 0 echo replies
         0 group queries, 0 group responses, 0 group reduces
         0 router solicits, 0 router adverts, 0 redirects
         9 neighbor solicits, 9 neighbor adverts
TCP statistics:
  Rcvd:  0 total segments, 0 errors
  Sent:  0 total segments, 0 retransmitted segments
UDP statics:
  Rcvd:  0 total, 0 errors, 0 no port
  Sent:  0 total
```

Display content	describe
IPv6 statistics:	IPv6 data report statistics
Rcvd: 27 total, 21 local destination 0 header errors, 0 address errors 0 unknown protocol, 0 discards	IPv6 received packets statistics
Frags: 0 reassembled, 0 timeouts 0 fragment rcvd, 0 fragment dropped 0 fragmented, 0 couldn't fragment, 0 fragment sent	IPv6 fragmenting statistics
Sent: 24 total, 0 errors 0 unreachable, 0 too big, 0 time exceeded, 0 parameter problems 0 echo requests, 0 echo replies 0 group queries, 0 group	IPv6 sent packets statistics

responses, 0 group reduces 0 router solicits, 0 router adverts, 0 redirects 9 neighbor solicits, 9 neighbor adverts	

ip route

Command

ip route {<*ip-prefix*> <*mask*> | <*ip-prefix*>/<*prefix-length*>} {<*gateway-address*> | null0} [<*distance*>]

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

parameter

ip-prefix	Routing destination address, for example :1.1.1.1
mask	Routing destination address subnet mask, for example :255.255.255.0
prefix-length	Routing destination address prefix
gateway-address	Address IP next hop, for example :1.1.1.1
null0	Forwarding interface
distance	Routing priority, size range :1-255

default

Default static routing has a priority of 1

Mode

Global mode.

Usage Guide

This command can be used to configure switch static routing. both the address and the forwarding interface are available by specifying the next hop IP the routing packet when configuring the next hop of the static route.

Example

Add static routing to the switch.

Switch(config)#ip route 192.168.2.8/24 null0

3.Commands for ARP Configuration

arp

Command

arp <*ip_address*> <*mac_address*> {interface [ethernet] <*portName*>}

no arp <*ip_address*>

parameter

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.
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

clear arp-cache

Command	**clear arp-cache**
parameter	-
default	-
Mode	Admin Mode
Usage Guide	this command is used to clear the arp table.
Example	Clear the arp table. Switch#clear arp-cache

clear arp traffic

Command	**clear arp traffic**
parameter	-
default	-
Mode	Admin Mode
Usage Guide	Clear the switch ARP message statistics. box switches, this command only clears the statistics of APP messages received and sent from the current card.
Example	Clear switch ARP message statistics. Switch#clear arp traffic

show arp

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

[count] [vrf word]

parameter

ipaddress	is a specified IP address
vlan-id	Vlan id
hw-addr	for entry of specified MAC address
static	for static ARP entry
dynamic	for dynamic ARP entry
count	displays number of ARP entries
vrf word	is the specified vrf name

default

-

Mode

Admin Mode

Usage Guide

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

Example

Displays the current ARP table content information.

```
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
```

Display content	describe
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.

show arp traffic

Command	**show arp traffic**
parameter	-
default	-
Mode	Admin and Config Mode
Usage Guide	Display statistics information of received and sent APP messages.
Example	Displays current ARP statistics. Switch#show arp traffic ARP statistics: Rcvd: 0 request, 0 response Sent: 0 request, 0 response

4.Commands for ARP Scanning Prevention

anti-arpscan enable

Command	**anti-arpscan enable** **no anti-arpscan enable**
parameter	-
default	Disable ARP scanning prevention function.
Mode	Global configuration mode
Usage 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

anti-arpscan port-based threshold

Command	**anti-arpscan port-based threshold <*threshold-value*>** **no anti-arpscan port-based threshold**

parameter	***threshold-value***	rate threshold, ranging from 2 to 200.
default	10 packets /second.	
Mode	Global Configuration Mode	
Usage 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	

anti-arpscan ip-based threshold

Command	**anti-arpscan ip-based threshold <*threshold-value*>** **no anti-arpscan ip-based threshold**	
parameter	***threshold-value***	rate threshold, ranging from 1 to 200.
default	3 packets/second.	
Mode	Global configuration mode	
Usage 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	

anti-arpscan trust

Command	**anti-arpscan trust [port | supertrust-port]** **no anti-arpscan trust [port | supertrust-port]**
parameter	-
default	By default all the ports are non- trustful.
Mode	Port configuration mode
Usage 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.
Example	Set port ethernet 4/5 of the switch as a trusted port. Switch(Config-If-Ethernet4/5)# anti-arpscan trust port

anti-arpscan trust ip

Command	**anti-arpscan trust ip <*ip-address*> [<*netmask*>]** **no anti-arpscan trust ip <*ip-address*> [<*netmask*>]**
parameter	***ip-address*** Configure trusted IP address ***netmask*** Net mask of the IP.
default	By default all the IP are non-trustful. Default mask is 255.255.255.255
Mode	Global configuration mode
Usage 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

anti-arpscan recovery enable

Command	**anti-arpscan recovery enable** **no anti-arpscan recovery enable**
parameter	-
default	Enable the automatic recovery function
Mode	Global configuration mode
Usage 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

anti-arpscan recovery time

Command	**anti-arpscan recovery time <*seconds*>** **no anti-arpscan recovery time**
parameter	***seconds*** Automatic recovery time, in second ranging from 5 to 86400.
default	300s
Mode	Global configuration mode
Usage Guide	this command is used to configure automatic recovery time, no command is used to restore default configuration.
Example	Set the automatic recovery time as 3600 seconds. Switch(config)#anti-arpscan recovery time 3600

anti-arpscan log enable

Command	**anti-arpscan log enable** **no anti-arpscan log enable**
parameter	-
default	Enable ARP scanning prevention log function.
Mode	Global configuration mode
Usage 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

anti-arpscan trap enable

Command	**anti-arpscan trap enable** **no anti-arpscan trap enable**
parameter	-

default	Disable ARP scanning prevention SNMP Trap function.
Mode	Global configuration mode
Usage 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

show anti-arpscan

Command	**show anti-arpscan [trust [ip | port | supertrust-port] |prohibited [ip | port]]**
parameter	-
default	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.
Mode	Admin Mode
Usage 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#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	trust	N	0
Ethernet1/0/5	trust	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	untrust	N	0
Ethernet1/0/17	untrust	N	0
Ethernet1/0/18	untrust	N	0

Ethernet1/0/19	untrust	N	0
Ethernet1/0/20	untrust	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

No prohibited IP.

Trust IP:
192.168.1.0 255.255.255.0

5.Commands for Preventing ARP Spoofing

ip arp-security updateprotect

Command	**ip arp-security updateprotect** **no ip arp-security updateprotect**
parameter	-
default	ARP table automatic update.
Mode	Global Mode/ Interface configuration.
Usage 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	Automatic update of ARP table is prohibited. Switch(Config-if-Vlan1)#ip arp-security updateprotect. Switch(config)#ip arp-security updateprotect

ip arp-security learnprotect

Command	**ip arp-security learnprotect** **no ip arp-security learnprotect**
parameter	-
default	ARP learning enabled.

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	Prohibit IPv4 version of the ARP learning function. Switch(config)# ip arp-security learnprotect

ip arp-security convert

Command	**ip arp-security convert**
parameter	-
default	-
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	To change all dynamic ARP to static ARP. Switch(config)#ip arp -security convert

clear ip arp dynamic

Command	**clear ip arp dynamic**
parameter	-
default	-
Mode	Interface Configuration
Usage Guide	This command will clear dynamic entries before binding ARP. Once implemented, this command will lose its effect.
Example	Clear all dynamic ARP. on the interface. Switch(Config-if-Vlan1)#clear ip arp dynamic

clear ipv6 nd dynamic

Command	**clear ipv6 nd dynamic**

parameter	-
default	-
Mode	Vlan Interface Mode
Usage Guide	It used in dynamic table when use ND bind function to clear. After executeit, the command will be useless.
Example	Clear all dynamic ND. in ports. Switch(Config-if-Vlan1)#clear ipv6 nd dynamic

6.Command for ARP GUARD

arp-guard ip

Command	**arp-guard ip <addr>** **no arp-guard ip <addr>**
parameter	**Addr** is the protected IP address, in dotted decimal notation
default	There is no ARP GUARD address by default
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

7.Commands for Gratuitous ARP Configuration

ip gratuitous-arp

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

	no ip gratuitous-arp

parameter	***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.

default	Gratuitous ARP is disabled by default.
Mode	Global configuration mode and vlan interface configuration mode
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	To enable gratuitous ARP in global configuration mode, and set the update interval to be 400 seconds. Switch#config Switch(config)#ip gratuitous-arp 400

show ip gratuitous-arp

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

parameter	***vlan-id***	VLAN ID

default	-
Mode	All the Configuration Modes.
Usage Guide	Displays gratuitous ARP configuration information.
Example	Displays gratuitous ARP configuration information. 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

8.Commands for Dynamic ARP Inspection

ip arp inspection

Command	**ip arp inspection vlan <vlan-id>** **no ip arp inspection vlan <vlan-id>**
parameter	**vlan-id** is the vlan which is enabled the dynamic ARP inspection function
default	Disable.
Mode	Global Mode.
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

ip arp inspection trust

Command	**ip arp inspection trust** **no ip arp inspection trust**
parameter	-
default	All the ports are the untrusted ports as default.
Mode	Port Mode
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

ip arp inspection limit-rate

Command	**ip arp inspection limit-rate <rate>**

no ip arp inspection limit-rate

parameter	**rate**	is the configured limited rate of the ARP packet of the untrusted port, the unit is pps

default

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

Mode

Port Mode

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
```