QUANTUM® NETWORKS


QASA CLI GUIDE

# Layer3 and ARP

# Contents

# 1. Commands for Layer 3 Interface

### description

| | |
|---|---|
| **Command** | **description <*text*>**<br>**no description** |
| **Parameter** | ***text***: is the description information of VLAN interface, the length should not exceed to 256 characters. |
| **Default** | Do not configure. |
| **Mode** | VLAN interface mode. |
| **Usage** | Specifies a comment or a description of the vlan to assist the user. (Length: 1–256 characters). |
| **Example** | Configure the description information of VLAN interface as test vlan.<br><br>**Switch(config)#interface vlan 2**<br>**Switch(config-if-vlan2)#description test vlan** |

### interface vlan

| | |
|---|---|
| **Command** | **interface vlan *<vlan-id>***<br>**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** | This command is used to create the 3-layer interface. No form of this command is used to delete the 3-layer interface. |
| **Example** | Create a VLAN interface (layer 3 interface).<br><br>**Switch(config)#interface vlan 1**<br>**Switch(Config-if-Vlan1)#** |

### no interface IFNAME

| | |
|---|---|
| **Command** | **no interface IFNAME** |
| **Parameter** | **IFNAME** : Interface Name |
| **Default** | - |
| **Mode** | Global Mode. |
| **Usage** | This command is used to delete the layer 3 interface. It can deal with the situation when 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.<br><br>**switch(config)# no interface vlan1** |

### show ip route

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

### clear ipv6 neighbor

| | |
|---|---|
| **Command** | **clear ipv6 neighbors** |
| **Parameter** | **-** |
| **Default** | - |
| **Mode** | Admin Mode. |
| **Usage** | This command used to clear ipv6 neighbors. |
| **Example** | Clear neighbor list.<br><br>**Switch#clear ipv6 neighbors** |

### ip address

| | |
|---|---|
| **Command** | **ip address *<ip-address><mask>*[secondary]**<br>**no ip address [*<ip-address><mask>*] [secondary]** |
| **Parameter** | ***ip-address* :** is IP address, dotted decimal notation;<br>***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** | 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.<br><br>**Switch(Config-if-Vlan1)#ip address 192.168.1.10 255.255.255.0** |

### ipv6 address

| | |
|---|---|
| **Command** | **ipv6 address <ipv6-address\|prefix-length> [eui-64]**<br>**no ipv6 address <ipv6-address\|prefix-length> [eui-64]** |
| **Parameter** | **ipv6-address:** is the prefix of IPv6 address, parameter<br>**prefix-length:** is the prefix length of IPv6 address, which is between 3-128.<br>**eui-64:** means IPv6 address is generated automatically based on eui64 interface identifier of the interface. |
| **Default** | - |
| **Mode** | Interface Configuration Mode. |
| **Usage** | 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.<br><br>**Switch(Config-if-Vlan1)#ipv6 address 2001:3f:ed8::99/64** |

## ipv6 nd dad attempts

| | |
|---|---|
| **Command** | **ipv6 nd dad attempts *<value>***<br>**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** | 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.<br><br>**Switch(Config-if-Vlan1)# ipv6 nd dad attempts 3** |

## ipv6 nd ns-interval

| | |
|---|---|
| **Command** | **ipv6 nd ns-interval *<seconds>***<br>**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** | 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.<br><br>**Switch(Config-if-Vlan1)#ipv6 nd ns-interval 8** |

### ipv6 neighbor

| | |
|---|---|
| **Command** | **ipv6 neighbor *<ipv6-address><hardware-address>*interface *<interface-type interface-name>***<br>**no ipv6 neighbor *<ipv6-address>*** |
| **Parameter** | ***ipv6-address* :** is static neighbor IPv6 address<br>***hardware-address* :** is static neighbor hardware address<br>***interface-type* :** is Ethernet type<br>***interface-name* :** is Layer 2 interface name |
| **Default** | There is not static neighbor table entry. |
| **Mode** | Interface Configuration Mode. |
| **Usage** | 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.<br><br>**Switch(Config-if-Vlan1)#ipv6 neighbor 2001:1:2::4 00-03-0f-89-44-bc interface Ethernet1/0/1** |

### show ip interface

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

## show ip traffic

<table>
<tr><td>Command</td><td>show ip traffic</td></tr>
<tr><td>Parameter</td><td>-</td></tr>
<tr><td>Default</td><td>-</td></tr>
<tr><td>Mode</td><td>Admin Mode.</td></tr>
<tr><td>Usage</td><td>Displays statistics for IP, ICMP, TCP, UDP packets received/sent.</td></tr>
<tr><td>Example</td><td>Displays statistics for IP packets.<br>Switch#show ip traffic<br>IP statistics:<br>Rcvd: 3249810 total, 3180 local destination<br>0 header errors, 0 address errors<br>0 unknown protocol, 0 discards<br>Frags: 0 reassembled, 0 timeouts<br>0 fragment rcvd, 0 fragment dropped<br>0 fragmented, 0 couldn't fragment, 0 fragment sent<br>Sent: 0 generated, 3230439 forwarded<br>0 dropped, 0 no route<br>ICMP statistics:<br>Rcvd: 0 total 0 errors 0 time exceeded<br>0 redirects, 0 unreachable, 0 echo, 0 echo replies<br>0 mask requests, 0 mask replies, 0 quench<br>0 parameter, 0 timestamp, 0 timestamp replies<br>Sent: 0 total 0 errors 0 time exceeded<br>0 redirects, 0 unreachable, 0 echo, 0 echo replies<br>0 mask requests, 0 mask replies, 0 quench<br>0 parameter, 0 timestamp, 0 timestamp replies<br>TCP statistics:<br>TcpActiveOpens 0, TcpAttemptFails 0<br>TcpCurrEstab 0, TcpEstabResets 0<br>TcpInErrs 0, TcpInSegs 3180<br>TcpMaxConn 0, TcpOutRsts 3<br>TcpOutSegs 0, TcpPassiveOpens 8<br>TcpRetransSegs 0, TcpRtoAlgorithm 0<br>TcpRtoMax 0, TcpRtoMin 0<br>UDP statics:<br>UdpInDatagrams 0, UdpInErrors 0<br>UdpNoPorts 0, UdpOutDatagrams 0<br><br><table><tr><td>Display content</td><td>describe</td></tr><tr><td>IP statistics：</td><td>IP packet statistics</td></tr></table></td></tr>
</table>

| | | |
|---|---|---|
| | Rcvd: 3249810 total, 3180 local destination<br>0 header errors, 0 address errors<br>0 unknown protocol, 0 discards | Statistics of total packets received,<br>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<br>0 fragment rcvd, 0 fragment dropped<br>0 fragmented, 0 couldn't fragment, 0<br>fragment sent | Fragmentation statistics: number of<br>packets reassembled, timeouts, fragments received, fragments discarded, packets that cannot be fragmented, number of fragments<br>sent, etc. |
| | Sent： 0 generated, 0 forwarded<br>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<br>0 redirects, 0 unreachable, 0 echo, 0<br>echo replies<br>0 mask requests, 0 mask replies, 0<br>quench<br>0 parameter, 0 timestamp, 0 timestamp<br>replies | Statistics of total ICMP packets received and classified information |
| | Sent： 0 total 0 errors 0 time exceeded<br>0 redirects, 0 unreachable, 0 echo, 0<br>echo replies<br>0 mask requests, 0 mask replies, 0<br>quench<br>0 parameter, 0 timestamp, 0 timestamp<br>replies | Statistics of total ICMP packets sent<br>and classified information |
| | TCP statistics: | TCP packet statistics. |
| | UDP statistics: | UDP packet statistics. |

### show ipv6 route

| | |
|---|---|
| **Command** | **show ipv6 route [database]** |
| **Parameter** | **database** : is router database |
| **Default** | - |
| **Mode** | Admin and Configuration Mode. |
| **Usage** | Only shows IPv6 kernal routing table (routing table in tcp, ip), database shows all routers except the local router. |
| **Example** | Displays IPv6 Routing Table.<br>Switch#show ipv6 route<br>IPv6 Routing Table<br>Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B - BGP<br>Timers: Uptime<br><br>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<br>\| address *<ipv6address>*]** |
| **Parameter** | **{vlan\|ethernet} interface-number** : specify the lookup based on interface<br>***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** | Displays neighbor table information. If there are no parameters, the entire neighbor table entry is displayed. |

<table>
<tr><td>Example</td><td>Check ipv6 Neighbor Table Information.<br>Switch#show ipv6 neighbors<br>IPv6 neighbour unicast items: 2, valid: 1, matched: 1, incomplete: 0, delayed: 0,<br>manage items: 0<br>IPv6 Address Hardware Addr Interface Port State Age-time(sec)<br>fe80::d8e4:a662:88e4:dc24 00-e0-4c-21-00-34 Vlan1<br>Ethernet1/0/18 reachable 563<br><br>IPv6 neighbour table: 1 entries<br><br>
<table>
<tr><td>Display content</td><td>describe</td></tr>
<tr><td>IPv6 Addres</td><td>Neighbor IPv6 address</td></tr>
<tr><td>Hardware Addr</td><td>Neighbor MAC address</td></tr>
<tr><td>Interface</td><td>Exit interface name</td></tr>
<tr><td>Port</td><td>Exit interface name</td></tr>
<tr><td>State</td><td>Neighbor status (reachable. state. delay. Probe. Permanent. Incomplete. unknown)</td></tr>
</table>
</td></tr>
</table>

## show ipv6 traffic

| | |
|---|---|
| **Command** | **show ipv6 traffic** |
| **Parameter** | **-** |
| **Default** | - |
| **Mode** | Admin and Configuration Mode. |
| **Usage** | Display IPv6 transmit packet statistics. Neighbor table entry is displayed. |
| **Example** | Display IPv6 transmit packet statistics.<br>**Switch#show ipv6 traffic**<br>IPv6 statistics:<br>Rcvd: 27 total, 21 local destination<br>0 header errors, 0 address errors<br>0 unknown protocol, 0 discards<br>Frags: 0 reassembled, 0 timeouts<br>0 fragment rcvd, 0 fragment dropped<br>0 fragmented, 0 couldn't fragment, 0 fragment sent<br>Sent: 24 generated, 0 forwarded<br>0 dropped, 0 no route<br>ICMPv6 statistics:<br>Rcvd: 21 total, 0 errors<br>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<br>0 header errors, 0 address errors<br>0 unknown protocol, 0 discards | IPv6 received packets statistics |
| Frags: 0 reassembled, 0 timeouts<br>0 fragment rcvd, 0 fragment dropped<br>0 fragmented, 0 couldn't fragment, 0 fragment sent | IPv6 fragmenting statistics |
| Sent: 24 total, 0 errors<br>0 unreachable, 0 too big, 0 time exceeded, 0 parameter problems<br>0 echo requests, 0 echo replies<br>0 group queries, 0 group responses, 0 group reduces<br>0 router solicits, 0 router adverts, 0 redirects<br>9 neighbor solicits, 9 neighbor adverts | IPv6 sent packets statistics |

## ip route

| | |
|---|---|
| **Command** | **ip route {*<ip-prefix>*<*mask*> \| *<ip-prefix>*/*<prefix-length>*} {*<gateway-address>* \| null0} [*<distance>*]**<br><br>**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<br>***mask :*** Routing destination address subnet mask, for example :255.255.255.0<br>***prefix-length :*** Routing destination address prefix<br>***gateway-address :*** Address IP next hop, for example :1.1.1.1<br>**null0 :** Forwarding interface<br>***distance :*** Routing priority, size range :1-255 |
| **Default** | Default static routing has a priority of 1. |
| **Mode** | Global mode. |
| **Usage** | 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.<br><br>**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>*}**<br>**no arp *<ip_address>*** |
| **Parameter** | ***ip_address*** : is the IP address, at the same field with interface address<br>***mac_address :*** is the MAC address<br>**ethernet :** stands for Ethernet port<br>***portName :*** for the name of layer2 port |
| **Default** | No static ARP entry is set by default. |
| **Mode** | VLAN Interface Mode. |
| **Usage** | By this command, Static ARP entries can be configured in the switch. |
| **Example** | Configuring static ARP for interface VLAN1.<br><br>**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** | This command is used to clear the arp table. |
| **Example** | Clear the arp table.<br><br>**Switch#clear arp-cache** |

### clear arp traffic

| | |
|---|---|
| **Command** | **clear arp traffic** |
| **Parameter** | **-** |
| **Default** | - |
| **Mode** | Admin Mode. |
| **Usage** | Clear the switch ARP message statistics, box switches. This command only clears the statistics of ARP messages received and sent from the current card. |
| **Example** | Clear switch ARP message statistics.<br><br>**Switch#clear arp traffic** |

### show arp

| | |
|---|---|
| **Command** | **show arp [<*ipaddress*>] [<*vlan-id*>] [<*hw-addr*>] [type {static \| dynamic}]**<br>**[count] [vrf word]** |
| **Parameter** | ***Ip address :*** is a specified IP address<br>***vlan-id :*** Vlan id<br>***hw-addr :*** for entry of specified MAC address<br>**static :** for static ARP entry<br>**dynamic :** for dynamic ARP entry<br>**count :** displays number of ARP entries<br>**vrf word :** is the specified vrf name |
| **Default** | - |
| **Mode** | Admin Mode. |
| **Usage** | 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.<br>**Switch#show arp**<br>ARP Unicast Items: 7, Valid: 7, Matched: 7, Verifying: 0, Incomplete: 0, Failed: 0, None: 0<br>Address Hardware Address Interface Port Flag<br>50.1.1.6 00-0a-eb-51-51-38 Vlan50 Ethernet1/0/11 Dynamic<br>50.1.1.9 00-00-00-00-00-09 Vlan50 Ethernet1/0/1 Static<br>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 |
| In Completed | 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** | Displays statistics information of received and sent APP messages. |
| **Example** | Displays current ARP statistics.<br><br>**Switch#show arp traffic**<br>ARP statistics:<br>Rcvd: 0 request, 0 response<br>Sent: 0 request, 0 response |

# 4. Commands for ARP Scanning Prevention

### anti-arpscan enable

| | |
|---|---|
| **Command** | **anti-arpscan enable**<br>**no anti-arpscan enable** |
| **Parameter** | **-** |
| **Default** | Disable ARP scanning prevention function. |
| **Mode** | Global configuration mode. |
| **Usage** | 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 shut down 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, Untrusted port. |
| **Example** | Displays current ARP statistics.<br><br>**Switch#show arp traffic**<br>ARP statistics:<br>Rcvd: 0 request, 0 response<br>Sent: 0 request, 0 response |

### anti-arpscan port-based threshold

| | |
|---|---|
| **Command** | **anti-arpscan port-based threshold *<threshold-value>***<br>**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** | 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.<br>**Switch(config)#anti-arpscan port-based threshold 10**<br>Sent: 0 request, 0 response |

### anti-arpscan ip-based threshold

| | |
|---|---|
| **Command** | **anti-arpscan ip-based threshold *<threshold-value>***<br>**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** | 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.<br><br>**Switch(config)#anti-arpscan ip-based threshold 6** |

### anti-arpscan trust

| | |
|---|---|
| **Command** | **anti-arpscan trust [port \| supertrust-port]**<br>**no anti-arpscan trust [port \| supertrust-port]** |
| **Parameter** | **-** |
| **Default** | By default all the ports are non- trustful. |
| **Mode** | Port configuration mode. |
| **Usage** | 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.<br><br>**Switch(Config-If-Ethernet4/5)# anti-arpscan trust port** |

### anti-arpscan trust ip

| | |
|---|---|
| **Command** | **anti-arpscan trust ip *<ip-address>*[*<netmask>*]**<br>**no anti-arpscan trust ip *<ip-address>*[*<netmask>*]** |
| **Parameter** | ***ip-address :*** Configure trusted IP address<br>***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** | 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 to 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<br><br>**Switch(config)#anti-arpscan trust ip 192.168.1.0 255.255.255.0** |

### anti-arpscan recovery enable

| | |
|---|---|
| **Command** | **anti-arpscan recovery enable**<br>**no anti-arpscan recovery enable** |
| **Parameter** | **-** |
| **Default** | Enable the automatic recovery function. |
| **Mode** | Global configuration mode. |
| **Usage** | 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.<br><br>**Switch(config)#anti-arpscan recovery enable** |

### anti-arpscan recovery time

| | |
|---|---|
| **Command** | **anti-arpscan recovery time *<seconds>***<br>**no anti-arpscan recovery time** |
| **Parameter** | ***Seconds:*** Automatic recovery time, in second ranging from 5 to 86400. |
| **Default** | 300s. |
| **Mode** | Global configuration mode. |
| **Usage** | 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.<br><br>**Switch(config)#anti-arpscan recovery time 3600** |

### anti-arpscan log enable

| | |
|---|---|
| **Command** | **anti-arpscan log enable**<br>**no anti-arpscan log enable** |
| **Parameter** | **-** |
| **Default** | Enable ARP scanning prevention log function. |
| **Mode** | Global configuration mode. |
| **Usage** | 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.<br><br>**Switch(config)#anti-arpscan log enable** |

### anti-arpscan trap enable

| | |
|---|---|
| **Command** | **anti-arpscan trap enable**<br>**no anti-arpscan trap enable** |
| **Parameter** | **-** |
| **Default** | Disable ARP scanning prevention SNMP Trap function. |

| | |
|---|---|
| **Mode** | Global configuration mode. |
| **Usage** | 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.<br><br>**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** | 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.<br>Switch#show anti-arpscan<br>Total port: 28<br>Name Port-property beShut shutTime(seconds)<br>Ethernet1/0/1 untrust N 0<br>Ethernet1/0/2 untrust N 0<br>Ethernet1/0/3 untrust N 0<br>Ethernet1/0/4 trust N 0<br>Ethernet1/0/5 trust N 0<br>Ethernet1/0/6 untrust N 0<br>Ethernet1/0/7 untrust N 0<br>Ethernet1/0/8 untrust N 0<br>Ethernet1/0/9 untrust N 0<br>Ethernet1/0/10 untrust N 0<br>Ethernet1/0/11 untrust N 0<br>Ethernet1/0/12 untrust N 0<br>Ethernet1/0/13 untrust N 0<br>Ethernet1/0/14 untrust N 0<br>Ethernet1/0/15 untrust N 0 |

| | |
|---|---|
| | Ethernet1/0/16 untrust N 0<br>Ethernet1/0/17 untrust N 0<br>Ethernet1/0/18 untrust N 0<br>Ethernet1/0/19 untrust N 0<br>Ethernet1/0/20 untrust N 0<br>Ethernet1/0/21 untrust N 0<br>Ethernet1/0/22 untrust N 0<br>Ethernet1/0/23 untrust N 0<br>Ethernet1/0/24 untrust N 0<br>Ethernet1/0/25 untrust N 0<br>Ethernet1/0/26 untrust N 0<br>Ethernet1/0/27 untrust N 0<br>Ethernet1/0/28 untrust N 0<br><br>No prohibited IP.<br><br>Trust IP:<br>192.168.1.0 255.255.255.0 |

# 5. Commands for Preventing ARP Spoofing

### ip arp-security updateprotect

| | |
|---|---|
| **Command** | **ip arp-security updateprotect**<br>**no ip arp-security updateprotect** |
| **Parameter** | **-** |
| **Default** | ARP table automatic update. |
| **Mode** | Global Mode/ Interface configuration. |
| **Usage** | 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 to 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.<br><br>**Switch(Config-if-Vlan1)#ip arp-security updateprotect.**<br>**Switch(config)#ip arp-security updateprotect** |

### ip arp-security learnprotect

| | |
|---|---|
| **Command** | **ip arp-security learnprotect**<br>**no ip arp-security learnprotect** |
| **Parameter** | **-** |
| **Default** | ARP learning enabled. |
| **Mode** | Global Mode/ Interface Configuration. |
| **Usage** | This command is used for preventing the automatic learning and updating of ARP. Unlike ip arp-security update protect, 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.<br><br>**Switch(config)# ip arp-security learnprotect** |

### ip arp-security convert

| | |
|---|---|
| **Command** | **ip arp-security convert** |
| **Parameter** | **-** |
| **Default** | - |
| **Mode** | Global Mode/ Interface configuration |
| **Usage** | 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.<br><br>**Switch(config)#ip arp-security convert** |

### clear ip arp dynamic

| | |
|---|---|
| **Command** | **clear ip arp dynamic** |
| **Parameter** | **-** |
| **Default** | - |
| **Mode** | Vlan Interface Mode |
| **Usage** | This command is used in dynamic table when use ND bind function to clear. After execute it, the command will be useless. |
| **Example** | Clear all dynamic ND in ports.<br><br>**Switch(Config-if-Vlan1)#clear ipv6 nd dynamic** |

# 6. Command for ARP GUARD

## arp-guard ip

| | |
|---|---|
| **Command** | **arp-guard ip <addr>**<br>**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** | 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 message 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<br><br>**switch(config)#interface ethernet1/0/1**<br>**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*>]**<br>**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** | 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.<br><br>**Switch#config**<br>**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** | Displays gratuitous ARP configuration information. |
| **Example** | Displays gratuitous ARP configuration information.<br>**Switch#show ip gratuitous-arp**<br>Gratuitous ARP send is Global enabled, Interval-Time is 300(s)<br>Gratuitous ARP send enabled interface vlan information:<br>Name Interval-Time(seconds)<br>Vlan1 400<br>Vlan10 350 |

# 8. Commands for Dynamic ARP Inspection

## ip arp inspection

| | |
|---|---|
| **Command** | **ip arp inspection vlan <vlan-id>**<br>**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** | After configuring 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.<br><br>**Switch(config)#**<br>**Switch(config)#ip arp inspection vlan 10**<br>**Switch(config)#exit** |

## ip arp inspection trust

| | |
|---|---|
| **Command** | **ip arp inspection trust**<br>**no ip arp inspection trust** |
| **Parameter** | **-** |
| **Default** | All the ports are the untrusted ports as default. |
| **Mode** | Port Mode. |
| **Usage** | After configuring 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.<br><br>**Switch(config)#**<br>**Switch(config)# interface ethernet 1/0/1**<br>**Switch(config-if-ethernet1/0/1)#ip arp inspection trust** |

### ip arp inspection limit-rate

| | |
|---|---|
| **Command** | **ip arp inspection limit-rate <rate>**<br>**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** | 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.<br><br>**Switch(config)#**<br>**Switch(config)#in e 1/0/1**<br>**Switch(config-if-ethernet1/0/1)# ip arp inspection limit-rate 100**<br>**Switch(config-if-ethernet1/0/1)#exit** |