Configuring IPv4 IMPB

CHAPTERS

1. IPv4 IMPB
2. IP-MAC Binding Configuration
3. ARP Detection Configuration
4. IPv4 Source Guard Configuration
5. Configuration Examples
6. Appendix: Default Parameters
1 IPv4 IMPB

1.1 Overview

IPv4 IMPB (IP-MAC-Port Binding) is used to bind the IP address, MAC address, VLAN ID and the connected port number of the specified host. Basing on the binding table, the switch can prevent the ARP cheating attacks with the ARP Detection feature and filter the packets that don’t match the binding entries with the IP Source Guard feature.

1.2 Supported Features

IP-MAC Binding

This feature is used to add binding entries. The binding entries can be manually configured, or learned by ARP scanning or DHCP snooping. The features ARP Detection and IPv4 Source Guard are based on the IP-MAC Binding entries.

ARP Detection

In an actual complex network, there are high security risks during ARP implementation procedure. The cheating attacks against ARP, such as imitating gateway, cheating gateway, cheating terminal hosts and ARP flooding attack, frequently occur to the network. ARP Detection can prevent the network from these ARP attacks.

- Prevent ARP Cheating Attacks

Based on the IP-MAC Binding entries, the ARP Detection can be configured to detect the ARP packets and filter the illegal ones so as to prevent the network from ARP cheating attacks.

- Prevent ARP Flooding Attack

You can limit the receiving speed of the legal ARP packets on the port to avoid ARP flooding attack.
IPv4 Source Guard

IPv4 Source Guard is used to filter the IPv4 packets based on the IP-MAC Binding table. Only the packets that match the binding rules are forwarded.
2 IP-MAC Binding Configuration

You can add IP-MAC Binding entries in three ways:

- Manual Binding
- Via ARP Scanning
- Via DHCP Snooping

Additionally, you can view, search and edit the entries in the Binding Table.

2.1 Using the GUI

2.1.1 Binding Entries Manually

You can manually bind the IP address, MAC address, VLAN ID and the Port number together on the condition that you have got the detailed information of the hosts.
Choose the menu **SECURITY > IPv4 IMPB > IP-MAC Binding > Manual Binding** and click **Add** to load the following page.

Figure 2-1  Manual Binding

**IPv4-MAC Binding**

- **Host Name**: Enter the host name for identification.
- **IP Address**: Enter the IP address.
- **MAC Address**: Enter the MAC address.
- **VLAN ID**: Enter the VLAN ID.
- **Protect Type**: Select the protect type for the entry. The entry will be applied to the specific feature. The following options are provided:
  - **None**: This entry will not be applied to any feature.
  - **ARP Detection**: This entry will be applied to the ARP Detection feature.
  - **IP Source Guard**: This entry will be applied to the IPv4 Source Guard feature.
  - **Both**: This entry will be applied to both of the features.
3) Enter or select the port that is connected to this host.
4) Click **Apply**.

### 2.1.2 Binding Entries via ARP Scanning

With ARP Scanning, the switch sends the ARP request packets of the specified IP field to the hosts. Upon receiving the ARP reply packet, the switch can get the IP address, MAC address, VLAN ID and the connected port number of the host. You can bind these entries conveniently.

**Note:**
Before using this feature, make sure that your network is safe and the hosts are not suffering from ARP attacks at present; otherwise, you may obtain incorrect IP-MAC Binding entries. If your network is being attacked, it’s recommended to bind the entries manually.

Choose the menu **SECURITY > IPv4 IMPB > IP-MAC Binding > ARP Scanning** to load the following page.

![ARP Scanning](image)

Follow these steps to configure IP-MAC Binding via ARP scanning:

1) In the **Scanning Option** section, specify an IP address range and a VLAN ID. Then click **Scan** to scan the entries in the specified IP address range and VLAN.

<table>
<thead>
<tr>
<th>Starting IP Address</th>
<th>Ending IP Address</th>
<th>VLAN ID</th>
<th>Port</th>
<th>Protect Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.1</td>
<td>192.168.0.254</td>
<td>1</td>
<td>1/020</td>
<td>None</td>
</tr>
</tbody>
</table>

Specify an IP range by entering a start and end IP address.
VLAN ID
Specify a VLAN ID.

2) In the Scanning Result section, select one or more entries and configure the relevant parameters. Then click Bind.

<table>
<thead>
<tr>
<th>Host Name</th>
<th>Enter a host name for identification.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Displays the IP address.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Displays the MAC address.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>Displays the VLAN ID.</td>
</tr>
<tr>
<td>Port</td>
<td>Displays the port number.</td>
</tr>
<tr>
<td>Protect Type</td>
<td>Select the protect type for the entry. The entry will be applied to the specific feature. The following options are provided:</td>
</tr>
<tr>
<td></td>
<td>None: This entry will not be applied to any feature.</td>
</tr>
<tr>
<td></td>
<td>ARP Detection: This entry will be applied to the ARP Detection feature.</td>
</tr>
<tr>
<td></td>
<td>IP Source Guard: This entry will be applied to the IP Source Guard feature.</td>
</tr>
<tr>
<td></td>
<td>Both: This entry will be applied to both of the features.</td>
</tr>
</tbody>
</table>

2.1.3 Binding Entries via DHCP Snooping

With DHCP Snooping enabled, the switch can monitor the IP address obtaining process of the host, and record the IP address, MAC address, VLAN ID and the connected port number of the host.
Choose the menu **SECURITY > IPv4 IMPB > IP-MAC Binding > DHCP Snooping** to load the following page.

![DHCP Snooping](image)

Follow these steps to configure IP-MAC Binding via DHCP Snooping:

1) In the **Global Config** section, globally enable DHCP Snooping. Click **Apply**.

2) In the **VLAN Config** section, enable DHCP Snooping on a VLAN or range of VLANs. Click **Apply**.

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

3) In the **Port Config** section, configure the maximum number of binding entries a port can learn via DHCP snooping. Click **Apply**.

<table>
<thead>
<tr>
<th>Port</th>
<th>Maximum Entries</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/1</td>
<td>512</td>
</tr>
<tr>
<td>1/0/2</td>
<td>512</td>
</tr>
<tr>
<td>1/0/3</td>
<td>512</td>
</tr>
<tr>
<td>1/0/4</td>
<td>512</td>
</tr>
<tr>
<td>1/0/5</td>
<td>512</td>
</tr>
<tr>
<td>1/0/6</td>
<td>512</td>
</tr>
<tr>
<td>1/0/7</td>
<td>512</td>
</tr>
<tr>
<td>1/0/8</td>
<td>512</td>
</tr>
<tr>
<td>1/0/9</td>
<td>512</td>
</tr>
<tr>
<td>1/0/10</td>
<td>512</td>
</tr>
</tbody>
</table>

Total: 28, 1 entry selected.
### 2.1.4 Viewing the Binding Entries

In the Binding Table, you can view, search and edit the specified binding entries.

Choose the menu SECURITY > IPv4 IMPB > IP-MAC Binding > Binding Table to load the following page.

Figure 2-4  Binding Table

You can specify the search criteria to search your desired entries.

**Source**

- **All**: Displays the entries from all sources.
- **Manual Binding**: Displays the manually bound entries.
- **ARP Scanning**: Displays the binding entries learned from ARP Scanning.
- **DHCP Snooping**: Displays the binding entries learned from DHCP Snooping.

**IP**

Enter an IP address and click Search to search the specific entry.

Additionally, you select one or more entries to edit the host name and protect type and click Apply.

**Host Name**

Enter a host name for identification.

**IP Address**

Displays the IP address.

**MAC Address**

Displays the MAC address.
<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Displays the VLAN ID.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Displays the port number.</td>
</tr>
<tr>
<td>Protect Type</td>
<td>Select the protect type for the entry. The entry will be applied to the specific feature. The following options are provided:</td>
</tr>
<tr>
<td>None</td>
<td>This entry will not be applied to any feature.</td>
</tr>
<tr>
<td>ARP Detection</td>
<td>This entry will be applied to the ARP Detection feature.</td>
</tr>
<tr>
<td>IP Source Guard</td>
<td>This entry will be applied to the IP Source Guard feature.</td>
</tr>
<tr>
<td>Both</td>
<td>This entry will be applied to both of the features.</td>
</tr>
<tr>
<td>Source</td>
<td>Displays the source of the entry.</td>
</tr>
</tbody>
</table>

### 2.2 Using the CLI

Binding entries via ARP scanning is not supported by the CLI. The following sections introduce how to bind entries manually and via DHCP Snooping and view the binding entries.

#### 2.2.1 Binding Entries Manually

You can manually bind the IP address, MAC address, VLAN ID and the Port number together on the condition that you have got the detailed information of the hosts.

Follow these steps to manually bind entries:

1. `configure`
   - Enter global configuration mode.
Step 2  

```
ip source binding hostname ip-addr mac-addr vlan vlan-id interface { fastEthernet port | gigabitEthernet port | ten-gigabitEthernet port | port-channel port-channel-id } { none | arp-detection | ip-verify-source | both }
```

Manually bind the host name, IP address, MAC address, VLAN ID and port number of the host, and configure the protect type for the host.

- **hostname**: Specify a name for the host. It contains 20 characters at most.
- **ip-addr**: Enter the IP address of the host.
- **mac-addr**: Enter the MAC address of the host, in the format of xx:xx:xx:xx:xx:xx.
- **vlan-id**: Enter the VLAN ID of the host.
- **port**: Enter the number of the port on which the host is connected.
- **none | arp-detection | ip-verify-source | both**: Specify the protect type for the entry. None indicates this entry will not be applied to any feature; arp-detection indicates this entry will be applied to ARP Detection; ip-verify-source indicates this entry will be applied to IPv4 Source Guard.

Step 3  

```
show ip source binding
```

Verify the binding entry.

Step 4  

```
end
```

Return to privileged EXEC mode.

Step 5  

```
copy running-config startup-config
```

Save the settings in the configuration file.

The following example shows how to bind an entry with the hostname host1, IP address 192.168.0.55, MAC address 74:d4:35:76:a4:d8, VLAN ID 10, port number 1/0/5, and enable this entry for the ARP detection feature.

```
Switch#configure
Switch(config)#ip source binding host1 192.168.0.55 74:d4:35:76:a4:d8 vlan 10 interface gigabitEthernet 1/0/5 arp-detection
Switch(config)#show ip source binding
U     Host              IP-Addr                MAC-Addr                      VID      Port           ACL        SOURCE
-      ----                 -------                   --------                              ---       ----              ---            ------
1     host1           192.168.0.55      74:d4:35:76:a4:d8       10       Gi1/0/5      ARP-D   Manual
```

Notice:

1. Here, 'ARP-D' for 'ARP-Detection', and 'IP-V-S' for 'IP-Verify-Source'.

```
Switch(config)#end
Switch#copy running-config startup-config
```
### 2.2.2 Binding Entries via DHCP Snooping

Follow these steps to bind entries via DHCP Snooping:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>ip dhcp snooping</td>
<td>Globally enable DHCP Snooping.</td>
</tr>
<tr>
<td>3</td>
<td>ip dhcp snooping vlan vlan-range</td>
<td>Enable DHCP Snooping on the specified VLAN.</td>
</tr>
<tr>
<td></td>
<td>vlan-range: Enter the vlan range in the format of 1-3, 5.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>interface { fastEthernet port</td>
<td>range fastEthernet port-list</td>
</tr>
<tr>
<td>5</td>
<td>ip dhcp snooping max-entries value</td>
<td>Configure the maximum number of binding entries the port can learn via DHCP snooping.</td>
</tr>
<tr>
<td></td>
<td>value: Enter the value of maximum number of entries. The valid values are from 0 to 512.</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>show ip dhcp snooping</td>
<td>Verify global configuration of DHCP Snooping.</td>
</tr>
<tr>
<td>7</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>8</td>
<td>copy running-config startup-config</td>
<td>Save the settings in the configuration file.</td>
</tr>
</tbody>
</table>

The following example shows how to enable DHCP Snooping globally and on VLAN 5, and set the maximum number of binding entries port 1/0/1 can learn via DHCP snooping as 100:

```
Switch#configure
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 5
Switch(config)#interface gigabitEthernet 1/0/1
Switch(config-if)#ip dhcp snooping max-entries 100
Switch(config-if)#show ip dhcp snooping
Global Status: Enable
```
VLAN ID: 5

Switch(config-if)#show ip dhcp snooping interface gigabitEthernet 1/0/1

<table>
<thead>
<tr>
<th>Interface</th>
<th>max-entries</th>
<th>LAG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>100</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Switch(config-if)#end

Switch#copy running-config startup-config

### 2.2.3 Viewing Binding Entries

On privileged EXEC mode or any other configuration mode, you can use the following command to view binding entries:

```plaintext
show ip source binding
```

View the information of binding entries, including the host name, IP address, MAC address, VLAN ID, port number and protect type.
### 3 ARP Detection Configuration

To complete ARP Detection configuration, follow these steps:

1) Add IP-MAC Binding entries.
2) Enable ARP Detection.
3) Configure ARP Detection on ports.
4) View ARP statistics.

## 3.1 Using the GUI

### 3.1.1 Adding IP-MAC Binding Entries

In ARP Detection, the switch detects the ARP packets based on the binding entries in the IP-MAC Binding Table. So before configuring ARP Detection, you need to complete IP-MAC Binding configuration.

### 3.1.2 Enabling ARP Detection

Choose the menu **SECURITY > IPv4 IMPB > ARP Detection > Global Config** to load the following page.

![ARP Detection Global Config](image)

Follow these steps to enable ARP Detection:

1) In the **Global Config** section, enable ARP Detection and configure the related parameters. Click **Apply**.
1.4 Configuring IPv4 IMPB

**ARP Detection Configuration**

| ARP Detect | Enable or disable ARP Detection globally. |
| Validate Source MAC | Enable or disable the switch to check whether the source MAC address and the sender MAC address are the same when receiving an ARP packet. If not, the ARP packet will be discarded. |
| Validate Destination MAC | Enable or disable the switch to check whether the destination MAC address and the target MAC address are the same when receiving an ARP reply packet. If not, the ARP packet will be discarded. |
| Validate IP | Enable or disable the switch to check whether the sender IP address of all ARP packets and the target IP address of ARP reply packets are legal. The illegal ARP packets will be discarded, including broadcast addresses, multicast addresses, Class E addresses, loopback addresses (127.0.0.0/8) and the following address: 0.0.0.0. |

2) In the **VLAN Config** section, enable ARP Detection on the selected VLANs. Click **Apply**.

| VLAN ID | Displays the VLAN ID. |
| Status | Enable or disable ARP Detection on the VLAN. |
| Log Status | Enable or disable Log feature on the VLAN. With this feature enabled, the switch generates a log when an illegal ARP packet is discarded. |

### 3.1.3 Configuring ARP Detection on Ports

Choose the menu **SECURITY > IPv4 IMPB > ARP Detection >Port Config** to load the following page.

![Figure 3-2 - ARP Detection on Port](image)
Follow these steps to configure ARP Detection on ports:

1) Select one or more ports and configure the parameters.

<table>
<thead>
<tr>
<th><strong>Trust Status</strong></th>
<th>Enable or disable this port to be a trusted port. On a trusted port, the ARP packets are forwarded directly without checked. The specific ports, such as up-link ports and routing ports are suggested to be set as trusted.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Limit Rate</strong></td>
<td>Specify the maximum number of the ARP packets that can be received on the port per second.</td>
</tr>
<tr>
<td><strong>Current Speed</strong></td>
<td>Displays the current speed of receiving the ARP packets on the port.</td>
</tr>
<tr>
<td><strong>Burst Interval</strong></td>
<td>Specify a time range. If the average speed of received ARP packets in this time range reaches the limit, the port will be shut down.</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>Displays the status of the ARP attack:</td>
</tr>
<tr>
<td></td>
<td><strong>Normal</strong>: The forwarding of ARP packets on the port is normal.</td>
</tr>
<tr>
<td></td>
<td><strong>Down</strong>: The transmission speed of the legal ARP packet exceeds the defined value. The port will be shut down for 300 seconds. You can also click the Recovery button to recover</td>
</tr>
<tr>
<td><strong>Operation</strong></td>
<td>If Status is changed to Down, there will be a <strong>Recover</strong> button. You can click the button to restore the port to the normal status.</td>
</tr>
<tr>
<td><strong>LAG</strong></td>
<td>Displays the LAG that the port is in.</td>
</tr>
</tbody>
</table>

2) Click **Apply**.

### 3.1.4 Viewing ARP Statistics

You can view the number of the illegal ARP packets received on each port, which facilitates you to locate the network malfunction and take the related protection measures.

Choose the menu **SECURITY > IPv4 IMPB > ARP Detection > ARP Statistics** to load the following page.

**Figure 3-3** View ARP Statistics
In the **Auto Refresh** section, you can enable the auto refresh feature and specify the refresh interval, and thus the web page will be automatically refreshed.

In the **Illegal ARP Packet** section, you can view the number of illegal ARP packets in each VLAN.

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Displays the VLAN ID.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forwarded</td>
<td>Displays the number of forwarded ARP packets in this VLAN.</td>
</tr>
<tr>
<td>Dropped</td>
<td>Displays the number of dropped ARP packets in this VLAN.</td>
</tr>
</tbody>
</table>

### 3.2 Using the CLI

#### 3.2.1 Adding IP-MAC Binding Entries

In ARP Detection, the switch detects the ARP packets based on the binding entries in the IP-MAC Binding Table. So before configuring ARP Detection, you need to complete IP-MAC Binding configuration.

#### 3.2.2 Enabling ARP Detection

Follow these steps to enable ARP Detection:

**Step 1**  
`configure`  
Enter global configuration mode.

**Step 2**  
`ip arp inspection`  
Globally enable the ARP Detection feature.

**Step 3**  
`ip arp inspection validate { src-mac | dst-mac | ip }`  
Configure the switch to check the IP address or MAC address of the received packets.

- **src-mac**: Enable the switch to check whether the source MAC address and the sender MAC address are the same when receiving an ARP packet. If not, the ARP packet will be discarded.

- **dst-mac**: Enable the switch to check whether the sender IP address of all ARP packets and the target IP address of ARP reply packets are legal. The illegal packets will be discarded.

- **ip**: Enable or disable the switch to check whether the sender IP address of all ARP packets and the target IP address of ARP reply packets are legal. The illegal ARP packets will be discarded, including broadcast addresses, multicast addresses, Class E addresses, loopback addresses (127.0.0.0/8) and the following address: 0.0.0.0.
Step 4  `ip arp inspection vlan vlan-list [logging]`
Enable ARP Detection on one or more 802.1Q VLANs that already exist.

- **vlan-list**: Enter the VLAN ID. The format is 1-9.
- **logging**: Enable the Log feature to make the switch generate a log when an ARP packet is discarded.

Step 5  `show ip arp inspection`
Verify the ARP Detection configuration.

Step 6  `end`
Return to privileged EXEC mode.

Step 7  `copy running-config startup-config`
Save the settings in the configuration file.

The following example shows how to enable ARP Detection globally and on VLAN 2, and enable the switch to check whether the source MAC address and the sender MAC address are the same when receiving an ARP packet:

```
Switch#configure
Switch(config)#ip arp inspection
Switch(config)#ip arp inspection validate src-mac
Switch(config)#ip arp inspection vlan 2
Switch(config)#show ip arp inspection
Global Status: Enable
Verify SMAC: Enable
Verify DMAC: Disable
Verify IP: Disable
Switch(config)#show ip arp inspection vlan
<table>
<thead>
<tr>
<th>VID</th>
<th>Enable status</th>
<th>Log Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Disable</td>
<td>Disable</td>
</tr>
<tr>
<td>2</td>
<td>Enable</td>
<td>Disable</td>
</tr>
</tbody>
</table>
Switch(config)#end
Switch#copy running-config startup-config
```
3.2.3 Configuring ARP Detection on Ports

Follow these steps to configure ARP Detection on ports:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>interface { fastEthernet port</td>
<td>range fastEthernet port-list</td>
</tr>
<tr>
<td>3</td>
<td>ip arp inspection trust</td>
<td>Configure the port as a trusted port, on which the ARP Detection function will not take effect. The specific ports, such as up-linked ports and routing ports are suggested to be set as trusted ports.</td>
</tr>
<tr>
<td>4</td>
<td>ip arp inspection limit-rate value</td>
<td>Specify the maximum number of the ARP packets can be received on the port per second.</td>
</tr>
<tr>
<td>5</td>
<td>ip arp inspection burst-interval value</td>
<td>Specify a time range. If the average speed of received ARP packets in this time range reach the limit, the port will be shut down.</td>
</tr>
<tr>
<td>6</td>
<td>show ip arp inspection interface</td>
<td>View the configurations and status of the ports.</td>
</tr>
<tr>
<td>7</td>
<td>ip arp inspection recover</td>
<td>(Optional) For ports on which the speed of receiving ARP packets has exceeded the limit, use this command to restore the port from Down status to Normal status.</td>
</tr>
<tr>
<td>8</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>9</td>
<td>copy running-config startup-config</td>
<td>Save the settings in the configuration file.</td>
</tr>
</tbody>
</table>

The following example shows how to set port 1/02 as a trusted port, and set limit-rate as 20 pps and burst interval as 2 seconds on port 1/0/2:

Switch#configure  
Switch(config)#interface gigabitEthernet 1/0/2  
Switch(config-if)#ip arp inspection trust  
Switch(config-if)#ip arp inspection limit-rate 20
Switch(config-if)#ip arp inspection burst-interval 2
Switch(config-if)#show ip arp inspection interface gigabitEthernet 1/0/2

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trust state</th>
<th>limit Rate(pps)</th>
<th>Current speed(pps)</th>
<th>Burst Interval</th>
<th>Status</th>
<th>LAG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/2</td>
<td>Enable</td>
<td>20</td>
<td>0</td>
<td>2</td>
<td>---</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Switch(config-if)#end
Switch#copy running-config startup-config

The following example shows how to restore the port 1/0/1 that is in Down status to Normal status:

Switch#configure
Switch(config)#interface gigabitEthernet 1/0/1
Switch(config-if)#ip arp inspection recover
Switch(config-if)#end
Switch#copy running-config startup-config

3.2.4 Viewing ARP Statistics

On privileged EXEC mode or any other configuration mode, you can use the following command to view ARP statistics:

  show ip arp inspection statistics

View the ARP statistics on each port, including the number of forwarded ARP packets and the number of dropped ARP packets.
IPv4 Source Guard Configuration

To complete IPv4 Source Guard configuration, follow these steps:
1) Add IP-MAC Binding entries.
2) Configure IPv4 Source Guard.

4.1 Using the GUI

4.1.1 Adding IP-MAC Binding Entries

In IPv4 Source Guard, the switch filters the packets that do not match the rules of IPv4-MAC Binding Table. So before configuring ARP Detection, you need to complete IP-MAC Binding configuration.

4.1.2 Configuring IPv4 Source Guard

Choose the menu SECURITY > IPv4 IMPB > IPv4 Source Guard to load the following page.

Figure 4-1 IPv4 Source Guard Config
Follow these steps to configure IPv4 Source Guard:

1) In the **Global Config** section, choose whether to enable the Log feature. Click **Apply**.

| IPv4 Source Guard Log | Enable or disable IPv4 Source Guard Log feature. With this feature enabled, the switch generates a log when illegal packets are received. |

2) In the **Port Config** section, configure the protect type for ports and click **Apply**.

| Port | Displays the port number. |
| Security Type | Select Security Type on the port for IPv4 packets. The following options are provided: |
| Security Type (continued) | **Disable**: The IP Source Guard feature is disabled on the port. |
| Security Type (continued) | **SIP+MAC**: Only the packet with its source IP address, source MAC address and port number matching the IPv4-MAC binding rules can be processed, otherwise the packet will be discarded. |
| Security Type (continued) | **SIP**: Only the packet with its source IP address and port number matching the IPv4-MAC binding rules can be processed, otherwise the packet will be discarded. |
| LAG | Displays the LAG that the port is in. |

4.2 Using the CLI

4.2.1 Adding IP-MAC Binding Entries

In IPv4 Source Guard, the switch filters the packets that do not match the rules of IPv4-MAC Binding Table. So before configuring ARP Detection, you need to complete IP-MAC Binding configuration.

4.2.2 Configuring IPv4 Source Guard

Follow these steps to configure IPv4 Source Guard:

Step 1  
```
configure
```
Enter global configuration mode.

Step 2  
```
interface { fastEthernet port | range fastEthernet port-list | gigabitEthernet port | range gigabitEthernet port-list | ten-gigabitEthernet port | range ten-gigabitEthernet port-list }
```
Enter interface configuration mode.
### IPv4 Source Guard Configuration

#### Step 3

**ip verify source** `{ sip+mac | sip }`

Enable IP Source Guard for IPv4 packets.

- **sip+mac**: Only the packet with its source IP address, source MAC address and port number matching the IP-MAC binding rules can be processed, otherwise the packet will be discarded.

- **sip**: Only the packet with its source IP address and port number matching the IPv4-MAC binding rules can be processed, otherwise the packet will be discarded.

**Note**: Only T1500&T1500G&T1600G series switch supports this feature.

#### Step 4

**show ip verify source** `[ interface { fastEthernet port | gigabitEthernet port | ten-gigabitEthernet port | port-channel port-channel-id } ]`

Verify the IP Source Guard configuration for IPv4 packets.

#### Step 5

**end**

Return to privileged EXEC mode.

#### Step 6

**copy running-config startup-config**

Save the settings in the configuration file.

The following example shows how to enable IPv4 Source Guard on port 1/0/1:

```
Switch#configure
Switch(config)#interface gigabitEthernet 1/0/1
Switch(config-if)#ip verify source sip+mac
Switch(config-if)#show ip verify source interface gigabitEthernet 1/0/1
Port    Security-Type   LAG
---      -------------   ----
Gi1/0/1  SIP+MAC       N/A
Switch(config-if)#end
Switch#copy running-config startup-config
```
5 Configuration Examples

5.1 Example for ARP Detection

5.1.1 Network Requirements

As shown below, User 1 and User 2 are legal users in the LAN and connected to port 1/0/1 and port 1/0/2. Both of them are in the default VLAN 1. The router has been configured with security feature to prevent attacks from the WAN. Now the network administrator wants to configure Switch A to prevent ARP attacks from the LAN.

![Network Topology](image)

5.1.2 Configuration Scheme

To meet the requirement, you can configure ARP Detection to prevent the network from ARP attacks in the LAN.

The overview of configurations on the switch is as follows:

1) Configure IP-MAC Binding. The binding entries for User 1 and User 2 should be manually bound.

2) Configure ARP Detection globally.
3) Configure ARP Detection on ports. Since port 1/0/3 is connected to the gateway router, set port 1/0/3 as trusted port. To prevent ARP flooding attacks, limit the speed of receiving the legal ARP packets on all ports.

Demonstrated with T2600G-28TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

5.1.3 Using the GUI

1) Choose the menu SECURITY > IPv4 IMBP > IP-MAC Binding > Manual Binding and click + Add to load the following page. Enter the host name, IP address, MAC address and VLAN ID of User 1, select the protect type as ARP Detection, and select port 1/0/1 on the panel. Click Apply.

Figure 5-2 Binding Entry for User 1

<table>
<thead>
<tr>
<th>IPv4–MAC Binding</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name: User1</td>
</tr>
<tr>
<td>IP Address: 192.168.0.31</td>
</tr>
<tr>
<td>MAC Address: 74-D3-45-32-B6-8D</td>
</tr>
<tr>
<td>VLAN ID: 1</td>
</tr>
<tr>
<td>Protect Type: ARP Detection</td>
</tr>
<tr>
<td>Port: 1/0/1</td>
</tr>
</tbody>
</table>

2) On the same page, add a binding entry for User 2. Enter the host name, IP address, MAC address and VLAN ID of User 2, select the protect type as ARP Detection, and select port 1/0/2 on the panel. Click Apply.
3) Choose the menu **SECURITY > IPv4 IMBP > ARP Detection > Global Config** to load the following page. Enable APP Detect, Validate Source MAC, Validate Destination MAC and Validate IP, and click **Apply**. Select VLAN 1, change Status as Enabled and click **Apply**.

4) Choose the menu **SECURITY > IPv4 IMBP > ARP Detection > Port Config** to load the following page. By default, all ports are enabled with ARP Detection and ARP flooding defend. Configure port 1/0/3 as trusted port and keep other defend parameters as default. Click **Apply**.
5) Click [Save] to save the settings.

5.1.4 Using the CLI

1) Manually bind the entries for User 1 and User 2.

   Switch_A#configure
   Switch_A(config)#ip source binding User1 192.168.0.31 74:d3:45:32:b6:8d vlan 1 interface gigabitEthernet 1/0/1 arp-detection
   Switch_A(config)#ip source binding User1 192.168.0.32 88:a9:d4:54:fd:c3 vlan 1 interface gigabitEthernet 1/0/2 arp-detection

2) Enable ARP Detection globally and on VLAN 1.

   Switch_A(config)#ip arp inspection
   Switch_A(config)#ip arp inspection vlan 1

3) Configure port 1/0/3 as trusted port.

   Switch_A(config)#interface gigabitEthernet 1/0/3
   Switch_A(config-if)#ip arp inspection trust
   Switch_A(config-if)#end
   Switch_A#copy running-config startup-config
Verify the Configuration

Verify the IP-MAC Binding entries:

Switch_A#show ip source binding

<table>
<thead>
<tr>
<th>U</th>
<th>Host</th>
<th>IP-Addr</th>
<th>MAC-Addr</th>
<th>VID</th>
<th>Port</th>
<th>ACL</th>
<th>SOURCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>User1</td>
<td>192.168.0.31</td>
<td>74:d3:45:32:b6:8d</td>
<td>1</td>
<td>Gi1/0/1</td>
<td>ARP-D</td>
<td>Manual</td>
</tr>
</tbody>
</table>

Notice:
1. Here, ‘ARP-D’ for ‘ARP-Detection’, and ‘IP-V-S’ for ‘IP-Verify-Source’.

Verify the global configuration of ARP Detection:

Switch_A#show ip arp inspection

Global Status: Enable
Verify SMAC: Enable
Verify DMAC: Enable
Verify IP: Enable

Verify the ARP Detection configuration on VLAN:

Switch_A#show ip arp inspection vlan

<table>
<thead>
<tr>
<th>VID</th>
<th>Enable status</th>
<th>Log Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enable</td>
<td>Disable</td>
</tr>
</tbody>
</table>

Verify the ARP Detection configuration on ports:

Switch_A#show ip arp inspection interface

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trust state</th>
<th>limit Rate(pps)</th>
<th>Current speed(pps)</th>
<th>Burst Interval</th>
<th>Status</th>
<th>LAG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>Disable</td>
<td>100</td>
<td>0</td>
<td>1</td>
<td>---</td>
<td>N/A</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>Disable</td>
<td>100</td>
<td>0</td>
<td>1</td>
<td>---</td>
<td>N/A</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>Enable</td>
<td>100</td>
<td>0</td>
<td>1</td>
<td>---</td>
<td>N/A</td>
</tr>
</tbody>
</table>

...
5.2 Example for IP Source Guard

5.2.1 Network Requirements

As shown below, the legal host connects to the switch via port 1/0/1 and belongs to the default VLAN 1. It is required that only the legal host can access the network via port 1/0/1, and other unknown hosts will be blocked when trying to access the network via ports 1/0/1-3.

5.2.2 Configuration Scheme

To implement this requirement, you can use IP-MAC Binding and IP Source Guard to filter out the packets received from the unknown hosts. The overview of configuration on the switch is as follows:

1) Bind the MAC address, IP address, connected port number and VLAN ID of the legal host with IP-MAC Binding.

2) Enable IP Source Guard on ports 1/0/1-3.

Demonstrated with T2600G-28TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

5.2.3 Using the GUI

1) Choose the menu SECURITY > IPv4 IMPB > IP-MAC Binding > Manual Binding and click Add to load the following page. Enter the host name, IP address, MAC address and VLAN ID of the legal host, select the protect type as , and select port 1/0/1 on the panel. Click Apply.
2) Choose the menu **SECURITY > IPv4 IMPB > IPv4 Source Guard** to load the following page. Enable IPv4 Source Guard Logging to make the switch generate logs when receiving illegal packets, and click **Apply**. Select ports 1/0/1-3, configure the Security Type as SIP+MAC, and click **Apply**.
3) Click \[Save\] to save the settings.

### 5.2.4 Using the CLI

1) Manually bind the IP address, MAC address, VLAN ID and connected port number of the legal host, and apply this entry to the IP Source Guard feature.

   Switch#configure

   Switch(config)#ip source binding legal-host 192.168.0.100 74:d3:45:32:b5:6d vlan 1 interface gigabitEthernet 1/0/1 ip-verify-source

2) Enable the log feature and IP Source Guard on ports 1/0/1-3.

   Switch(config)# ip verify source logging

   Switch(config)# interface range gigabitEthernet 1/0/1-3

   Switch(config-if-range)#ip verify source sip+mac

   Switch(config-if-range)#end

   Switch#copy running-config startup-config

### Verify the Configuration

Verify the binding entry:

Switch#show ip source binding
<table>
<thead>
<tr>
<th>U</th>
<th>Host</th>
<th>IP-Addr</th>
<th>MAC-Addr</th>
<th>VID</th>
<th>Port</th>
<th>ACL</th>
<th>SOURCE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>User1</td>
<td>192.168.0.100</td>
<td>74:d3:45:32:b5:6d</td>
<td>1</td>
<td>Gi1/0/1</td>
<td>IP-V-S</td>
<td>Manual</td>
</tr>
</tbody>
</table>

Notice:
1. Here, 'ARP-D' for 'ARP-Detection', and 'IP-V-S' for 'IP-Verify-Source'.

Verify the configuration of IP Source Guard:

Switch#show ip verify source

IP Source Guard log: Enabled

<table>
<thead>
<tr>
<th>Port</th>
<th>Security-Type</th>
<th>LAG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>SIP+MAC</td>
<td>N/A</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>SIP+MAC</td>
<td>N/A</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>SIP+MAC</td>
<td>N/A</td>
</tr>
</tbody>
</table>

...
Appendix: Default Parameters

Default settings of DHCP Snooping are listed in the following table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Config</td>
<td></td>
</tr>
<tr>
<td>DHCP Snooping</td>
<td>Disable</td>
</tr>
<tr>
<td>VLAN Config</td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>Disable</td>
</tr>
<tr>
<td>Port Config</td>
<td></td>
</tr>
<tr>
<td>Maximum Entry</td>
<td>512</td>
</tr>
</tbody>
</table>

Default settings of ARP Detection are listed in the following table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Config</td>
<td></td>
</tr>
<tr>
<td>ARP Detect</td>
<td>Disable</td>
</tr>
<tr>
<td>Validate Source MAC</td>
<td>Disable</td>
</tr>
<tr>
<td>Validate Destination MAC</td>
<td>Disable</td>
</tr>
<tr>
<td>Validate IP</td>
<td>Disable</td>
</tr>
<tr>
<td>VLAN Config</td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>Disable</td>
</tr>
<tr>
<td>Log Status</td>
<td>Disable</td>
</tr>
<tr>
<td>Port Config</td>
<td></td>
</tr>
<tr>
<td>Trust Status</td>
<td>Disable</td>
</tr>
<tr>
<td>Limit Rate</td>
<td>100 pps</td>
</tr>
<tr>
<td>Burst Interval</td>
<td>1 second</td>
</tr>
</tbody>
</table>

Default settings of IPv4 Source Guard are listed in the following table:
### Table 6-3 IPv4 Source Guard

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Config</td>
<td></td>
</tr>
<tr>
<td>IPv4 Source Guard Log</td>
<td>Disable</td>
</tr>
<tr>
<td>Port Config</td>
<td></td>
</tr>
<tr>
<td>Security Type</td>
<td>Disable</td>
</tr>
</tbody>
</table>