Ethernet Switching Security

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Foreword

- Currently, Ethernet technologies are widely used on networks. Network attacks often occur, for example, attacks based on the Address Resolution Protocol (ARP) and Dynamic Host Configuration Protocol (DHCP). Such attacks cause authorized users' failure to access network resources and threaten network information security. In this situation, Ethernet switching security becomes increasingly important.
- This course describes common Ethernet switching security technologies, including port isolation, port security, MAC address flapping detection, storm control, interface rate limiting, MAC address table security, DHCP snooping, and IP source guard.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Objectives

- Upon completion of this course, you will be able to:
  - Describe types and configurations of port isolation.
  - Illustrate the working mechanism of port security.
  - Describe MAC address flapping detection.
  - Explain traffic suppression and storm control functions of switches.
  - Describe application scenarios of DHCP snooping.
  - Illustrate the working mechanism of IP source guard.

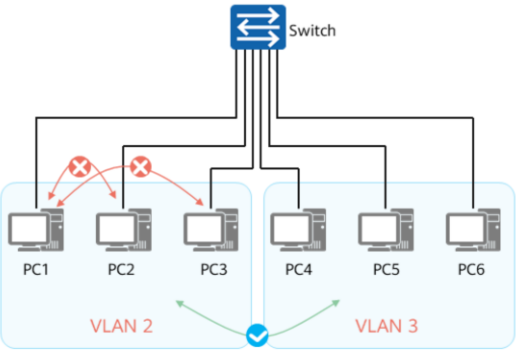
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Background of Port Isolation

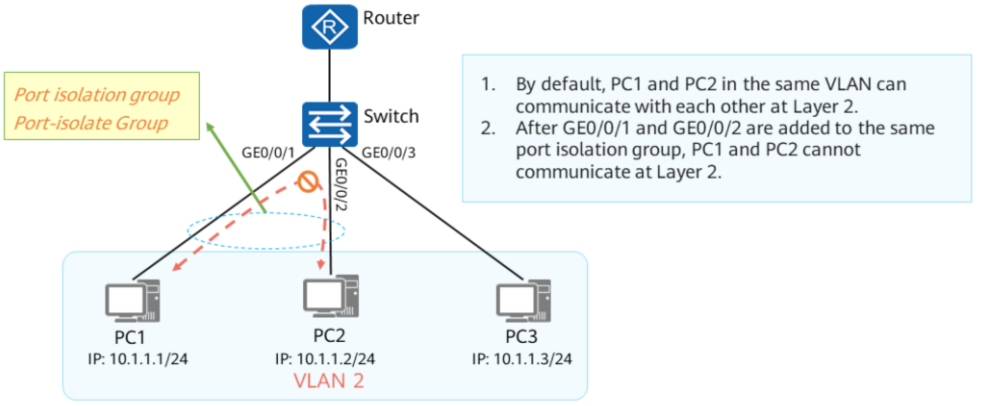
- On an Ethernet switching network, to implement Layer 2 isolation between packets, users usually add different interfaces to different VLANs to isolate Layer 2 broadcast domains.
- On a large-scale network, there are various service requirements. Simply using VLANs to implement Layer 2 isolation of packets wastes limited VLAN resources.
- As shown in the following figure, although PC1 and PC2 belong to the same VLAN, they cannot communicate with each other at Layer 2 but can communicate with each other at Layer 3. PC1 and PC3 cannot communicate with each other in any case, but hosts in VLAN 3 can access hosts in VLAN 2. How is this problem solved?



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

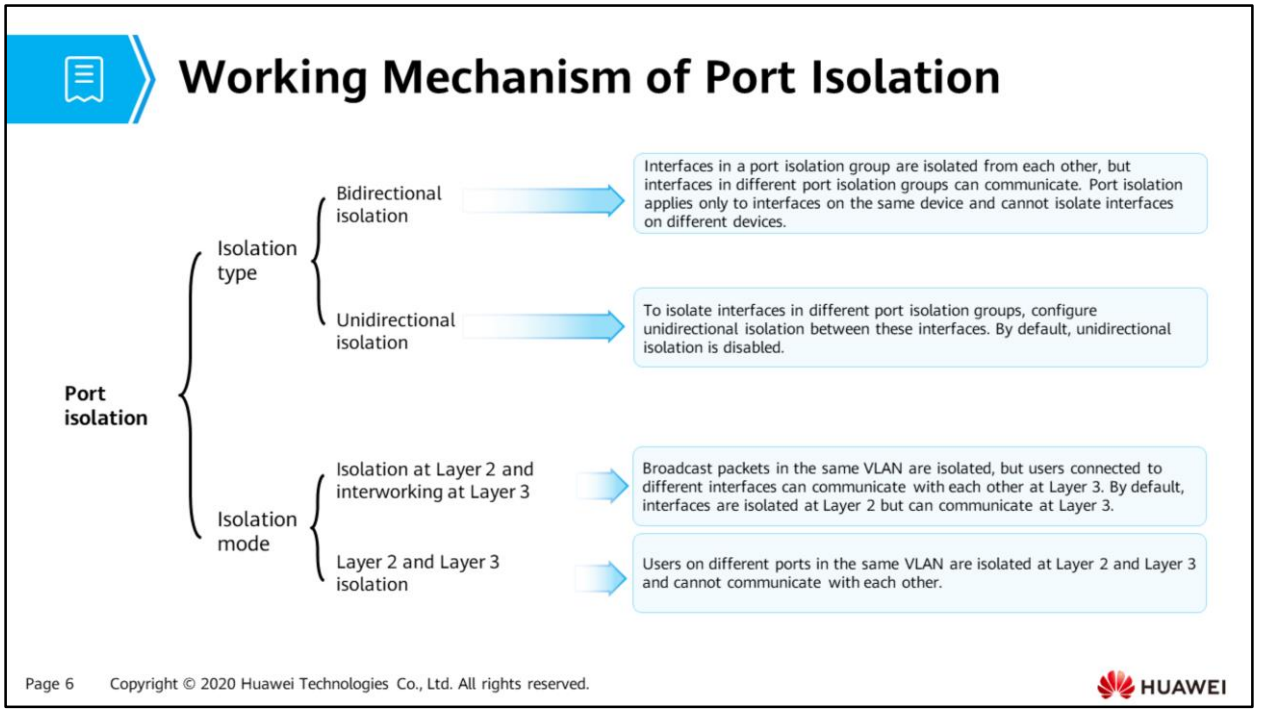
Overview of Port Isolation

Port isolation can isolate interfaces in a VLAN. That is, you only need to add interfaces to a port isolation group to implement Layer 2 isolation between these interfaces. Port isolation provides secure and flexible networking schemes for customers.



1. By default, PC1 and PC2 in the same VLAN can communicate with each other at Layer 2.
2. After GE0/0/1 and GE0/0/2 are added to the same port isolation group, PC1 and PC2 cannot communicate at Layer 2.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



- When Layer 2 isolation and Layer 3 interworking are used, you can enable intra-VLAN proxy ARP on the VLANIF interface and configure **arp-proxy inner-sub-vlan-proxy enable** to implement communication between hosts in the same VLAN.

Port Isolation Configuration Commands

1. Enable port isolation.

   [Huawei-GigabitEthernet0/0/1] **port-isolate enable** [**group** *group-id*]

   By default, port isolation is disabled on an interface. If *group-id* is not specified, an interface is added to port isolation group 1 by default.

2. (Optional) Configure a port isolation mode.

   [Huawei] **port-isolate mode** { **l2** | **all** }

   By default, the port isolation mode is Layer 2 isolation and Layer 3 interworking.

   l2: Layer 2 isolation and Layer 3 interworking

   all: Layer 2 and Layer 3 isolation

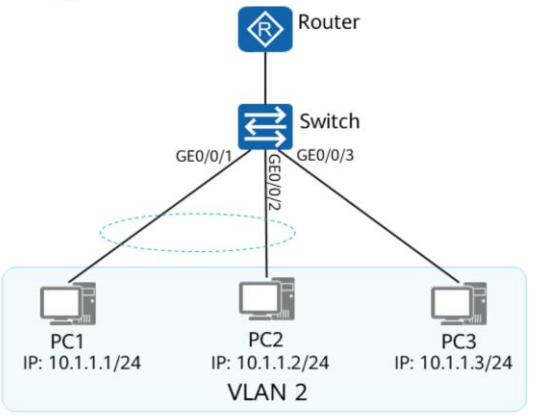
3. Configure unidirectional isolation.

   [Huawei-GigabitEthernet0/0/1] **am isolate** {*interface-type interface-number*}&<1-8>

   This command is used to unidirectionally isolate the current interface from a specified interface. If interface A is isolated from interface B unidirectionally, packets sent from interface A cannot reach interface B, but packets sent from interface B can reach interface A. By default, unidirectional isolation is disabled.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Example for Configuring Port Isolation



As shown in the figure, PC1, PC2, and PC3 belong to VLAN 2. After port isolation is configured, PC3 can communicate with PC1 and PC2, but PC1 and PC2 cannot communicate with each other.

Switch configuration:

```
[Switch] vlan 2
[Switch] port-isolate mode all
[Switch] interface GigabitEthernet 0/0/1
[Switch-GigabitEthernet0/0/1] port link-type access
[Switch-GigabitEthernet0/0/1] port default vlan 2
[Switch-GigabitEthernet0/0/1] port-isolate enable group 2
[Switch] interface GigabitEthernet 0/0/2
[Switch-GigabitEthernet0/0/2] port link-type access
[Switch-GigabitEthernet0/0/2] port default vlan 2
[Switch-GigabitEthernet0/0/2] port-isolate enable group 2
[Switch] interface GigabitEthernet 0/0/3
[Switch-GigabitEthernet0/0/3] port link-type access
[Switch-GigabitEthernet0/0/3] port default vlan 2
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- **display port-isolate group { *group-id* | all }**: displays the configuration of a port isolation group.
- **clear configuration port-isolate**: clears all the interface isolation configurations on the device.
- **port-isolate exclude vlan**: excludes a VLAN where port isolation needs to be disabled.

Verifying the Configuration

1. Run the **display port-isolate group** *group-number* command to check interfaces in the port isolation group.

```
[SW]display port-isolate group 2
  The ports in isolate group 2:
GigabitEthernet0/0/1     GigabitEthernet0/0/2
```

2. Verify that hosts in the same port isolation group cannot communicate with each other.

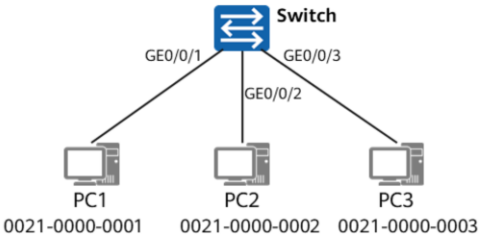
```
PC1>ping 10.1.1.2
Ping 10.1.1.2: 32 data bytes, Press Ctrl_C to break
From 10.1.1.1: Destination host unreachable
From 10.1.1.1: Destination host unreachable
From 10.1.1.1: Destination host unreachable
From 10.1.1.1: Destination host unreachable
From 10.1.1.1: Destination host unreachable
--- 10.1.1.2 ping statistics ---
  5 packet(s) transmitted
  0 packet(s) received
  100.00% packet loss
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Types of MAC Address Entries



[Switch]display mac-address

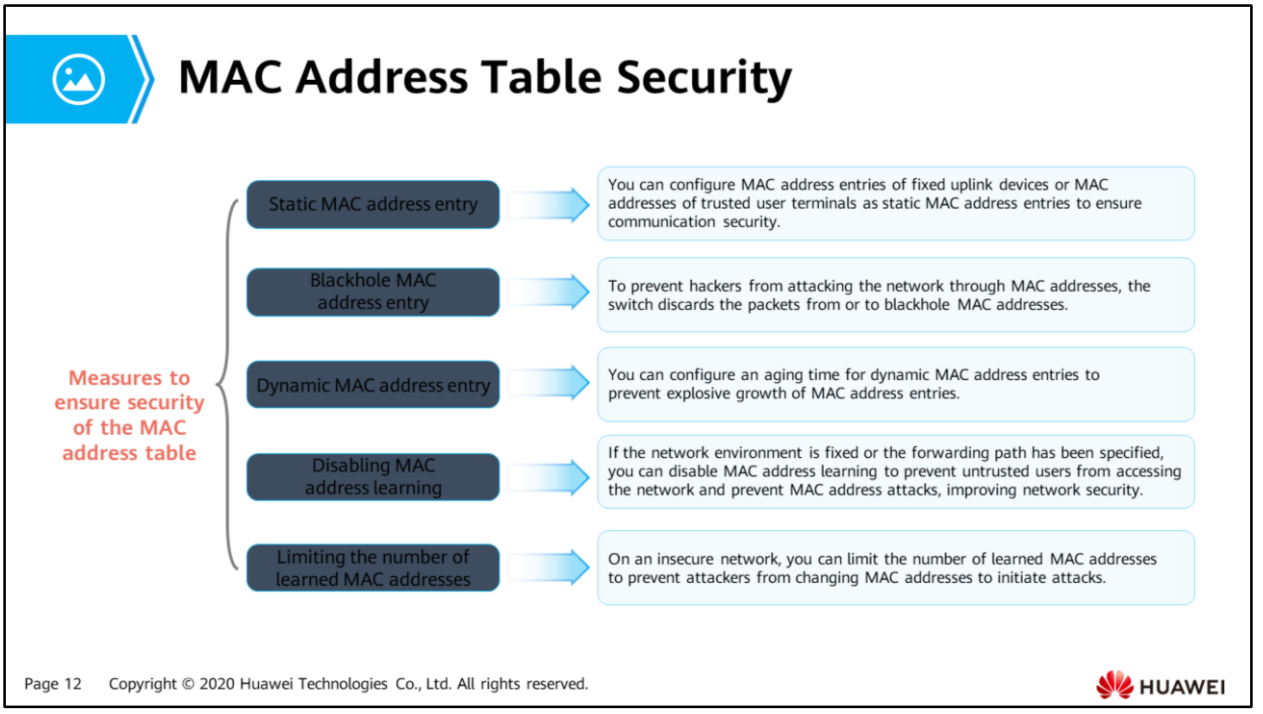
MAC Address	VLAN	Interface	Type
0021-0000-0001	10	GE0/0/1	Static
0021-0000-0002	10	GE0/0/2	Blackhole
0021-0000-0003	10	GE0/0/3	Dynamic

MAC address entries fall into the following types:

- Dynamic MAC address entries are obtained by learning source MAC addresses of packets received on an interface, and will age out. After a device resets or an interface board is hot swapped or resets, dynamic MAC address entries on the device or interface board are lost.
- Static MAC address entries that are manually configured by users and delivered to each interface card. Static MAC address entries will never age out. After a device resets or an interface board is hot swapped or resets, the static MAC address entries saved on the device or interface board are not lost. After an interface is statically bound to a MAC address, other interfaces discard packets originating from that source MAC address.
- Blackhole MAC address entries that are manually configured by users and delivered to each interface card. Blackhole MAC address entries will never age out. After blackhole MAC address entries are configured, packets with the source or destination MAC addresses being the blackhole MAC addresses are discarded.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- A MAC address table is used by the switch to record the mappings between learned MAC addresses of other devices and interfaces on which MAC addresses are learned, as well as VLANs to which the interfaces belong.
- When performing Layer 2 switching, the device searches the MAC address table according to the destination MAC address of the packet. If the MAC address table contains the entry corresponding to the destination MAC address of the packet and the interface that receives the packet is different from the interface corresponding to the entry, the packet is directly forwarded through the outbound interface in the entry. If they are the same, the packet is discarded.
- If the MAC address table does not contain the entry matching the destination MAC address of the packet, the device broadcasts the packet through all the interfaces in the VLAN except the interface that receives the packet.



- To prevent unauthorized users from modifying MAC address entries of some key devices (such as servers or uplink devices), you can configure the MAC address entries of these devices as static MAC address entries. Static MAC address entries take precedence over dynamic MAC address entries and can hardly be modified by unauthorized users.
- To prevent useless MAC address entries from occupying the MAC address table and prevent hackers from attacking user devices or networks using MAC addresses, you can configure untrusted MAC addresses as blackhole MAC addresses. In this way, when the device receives a packet with the destination or source MAC address as the blackhole MAC address, the device discards the packet without modifying the original MAC address entry or adding a MAC address entry.
- To reduce manual configuration of static MAC address entries, Huawei S series switches are enabled with dynamic MAC address learning by default. The aging time needs to be set properly for dynamic MAC address entries so that the switch can delete unneeded MAC address entries.
- To improve network security and prevent the device from learning invalid MAC addresses and incorrectly modifying the original MAC address entries in the MAC address table, you can disable MAC address learning on a specified interface or all interfaces in a specified VLAN so that the device does not learn new MAC addresses from these interfaces.
- You can limit the number of MAC address entries that can be learned on the device. When the number of learned MAC address entries reaches the limit, the device does not learn new MAC address entries. You can also configure an action to take when the number of learned MAC address entries reaches the limit. This prevents MAC address entries from being exhausted and improves network security.

Configuring MAC Address Entries

1. Configure a static MAC address entry.

   [Huawei] **mac-address static** *mac-address interface-type interface-number* **vlan** *vlan-id*

   The specified VLAN must have been created and added to the bound interface. The specified MAC address must be a unicast MAC address and cannot be a multicast or broadcast MAC address.

2. Configure a blackhole MAC address entry.

   [Huawei] **mac-address blackhole** *mac-address* **[vlan** *vlan-id* **]**

   The device discards the received packets originating from or destined for blackhole MAC addresses.

3. Set an aging time for a dynamic MAC address entry.

   [Huawei] **mac-address aging-time** *aging-time*

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Disabling MAC Address Learning

1. Disable MAC address limiting on an interface.

   [Huawei-GigabitEthernet0/0/1] **mac-address learning disable [action { discard | forward }]**

   By default, MAC address learning is enabled on an interface.
   - By default, the device takes the forward action after MAC address learning is disabled. That is, the device forwards packets according to the MAC address table.
   - When the action is set to discard, the device looks up the source MAC address of the packet in the MAC address table. If the interface and MAC address match the MAC address entry, the device forwards the packet according to the destination MAC address. If the interface and MAC address do not match the MAC address entry, the device discards the packet.

2. Disable MAC address learning in a VLAN.

   [Huawei-vlan2] **mac-address learning disable**

   By default, MAC address learning is enabled in a VLAN.
   If both interface-based and VLAN-based MAC address learning is disabled, the latter takes effect.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Limiting the Number of Learned MAC Address Entries

1. Limit the number of MAC address entries learned on an interface.

   [Huawei-GigabitEthernet0/0/1] **mac-limit maximum** *max-num*

   By default, the number of MAC address entries learned on an interface is not limited.

2. Configure an action for the device to take when the number of learned MAC addresses reaches the limit.

   [Huawei-GigabitEthernet0/0/1] **mac-limit action { discard | forward }**

   By default, the device discards packets with new MAC addresses when the number of learned MAC address entries reaches the limit on the interface.

3. Configure the device whether to generate an alarm when the number of learned MAC addresses reaches the limit.

   [Huawei-GigabitEthernet0/0/1] **mac-limit alarm { disable | enable }**

   By default, the device generates an alarm when the number of learned MAC address entries reaches the limit.

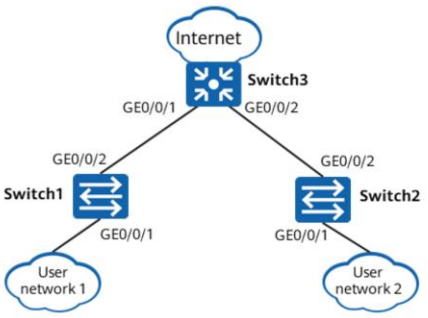
4. Limit the number of MAC address entries learned in a VLAN.

   [Huawei-vlan2] **mac-limit maximum** *max-num*

   By default, the number of MAC address entries learned in a VLAN is not limited.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Example for Configuring a MAC Address Table



Requirements:

- The basic configuration of the network topology is complete. User network 1 belongs to VLAN 10, and user network 2 belongs to VLAN 20.
- Switch3 is disabled from learning MAC addresses from user network 1.
- The maximum number of MAC addresses on user network 2 learned by Switch3 is set.

Switch3 configuration:

Method 1: Interface view

```
# Disable MAC address learning on GE0/0/1.
[Switch3-GigabitEthernet0/0/1] mac-address learning disable action discard
# Set the maximum number of MAC address entries learned on GE0/0/2, and configure the device to generate an alarm and set the action to discard when the number of learned MAC address entries reaches the limit.
[Switch3-GigabitEthernet0/0/2] mac-limit maximum 100
[Switch3-GigabitEthernet0/0/2] mac-limit alarm enable
[Switch3-GigabitEthernet0/0/2] mac-limit action discard
```

Method 2: VLAN view

```
# Disable MAC address learning in VLAN 10.
[Switch3-vlan10] mac-address learning disable
# Set the maximum number of MAC address entries learned in VLAN 20, and configure the device to generate an alarm when the number of learned MAC address entries reaches the limit.
[Switch3-vlan20] mac-limit maximum 100 alarm enable
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Verifying the Configuration

Run the **display mac-limit** command in any view to check whether MAC address limiting rules are configured successfully.

```
[Switch3]display mac-limit
MAC Limit is enabled
Total MAC Limit rule count : 2

PORT            VLAN/VSI/SI     SLOT  Maximum  Rate(ms)      Action     Alarm
--------------------------------------------------------------------------------
GE0/0/2         -               -     100      -             forward    enable
-               20              -     100      -             forward    enable
```

VLAN-based MAC address limiting

Interface-based MAC address limiting

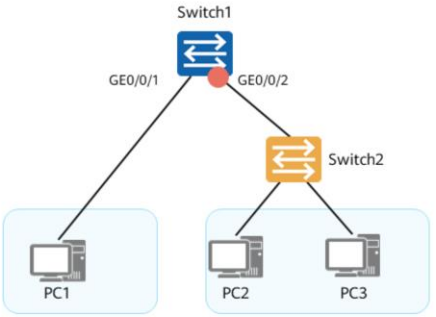
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

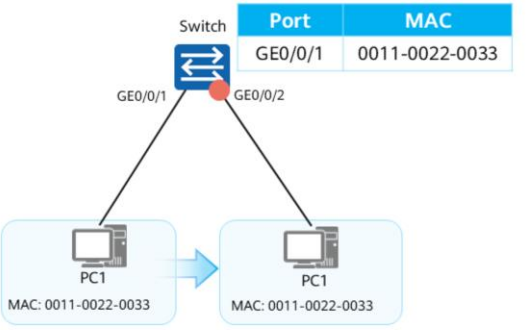
Contents

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Background of Port Security

- An enterprise requires that each access switch interface connected to terminals allow only one PC to access the network (the number of MAC address entries is limited). If an employee attempts to connect a small switch or hub to an interface, this behavior should be detected or prohibited, as shown in the figure on the left.
- In addition, some enterprises may require that only data frames sent by terminals with trusted MAC addresses can be forwarded to the upper-layer network by the switch. Employees cannot change their locations (change access interfaces of the switch), as shown in the figure on the right.
- Port security of the switch can solve the problems.





Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Introduction to Port Security

- You can configure port security on a specified interface of a switch to limit the number of MAC address entries learned by the interface and configure a punishment action when the number of learned MAC address entries exceeds the threshold.
- Port security converts dynamic MAC addresses learned on an interface into secure MAC addresses (including dynamic and static secure MAC addresses, and sticky MAC addresses). This function prevents unauthorized users from communicating with the switch using this interface and therefore enhances device security.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Working Mechanism of Port Security

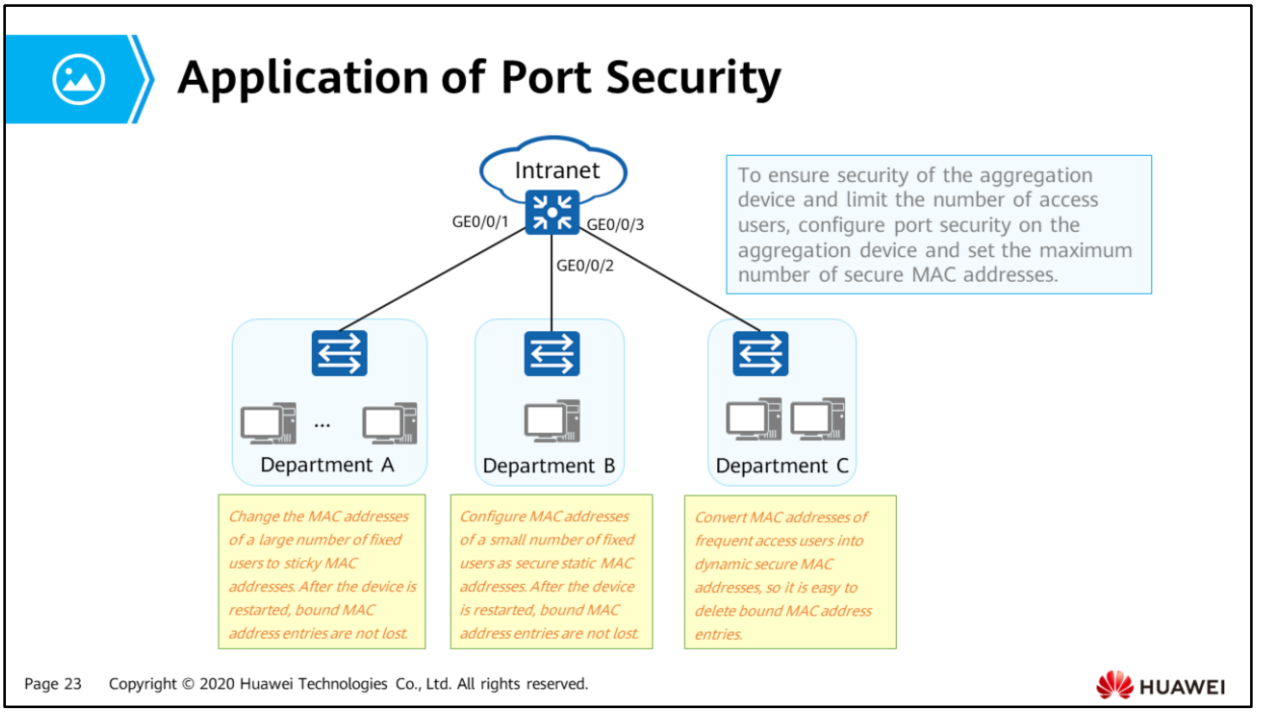
- Secure MAC addresses are classified into the following types.

Type	Definition	Characteristics
Secure dynamic MAC address	MAC address that is converted on an interface with port security enabled but sticky MAC disabled	After a device restarts, dynamic secure MAC addresses are lost and need to be relearned. By default, dynamic secure MAC addresses are not aged out, and can be aged out only when the aging time is set.
Secure static MAC address	MAC address that is manually configured on an interface with port security enabled	Secure static MAC addresses are not aged out and are not lost after a device restart.
Sticky MAC address	MAC address that is converted on an interface with both port security and sticky MAC enabled	Sticky MAC addresses are not aged out and are not lost after a device restart.

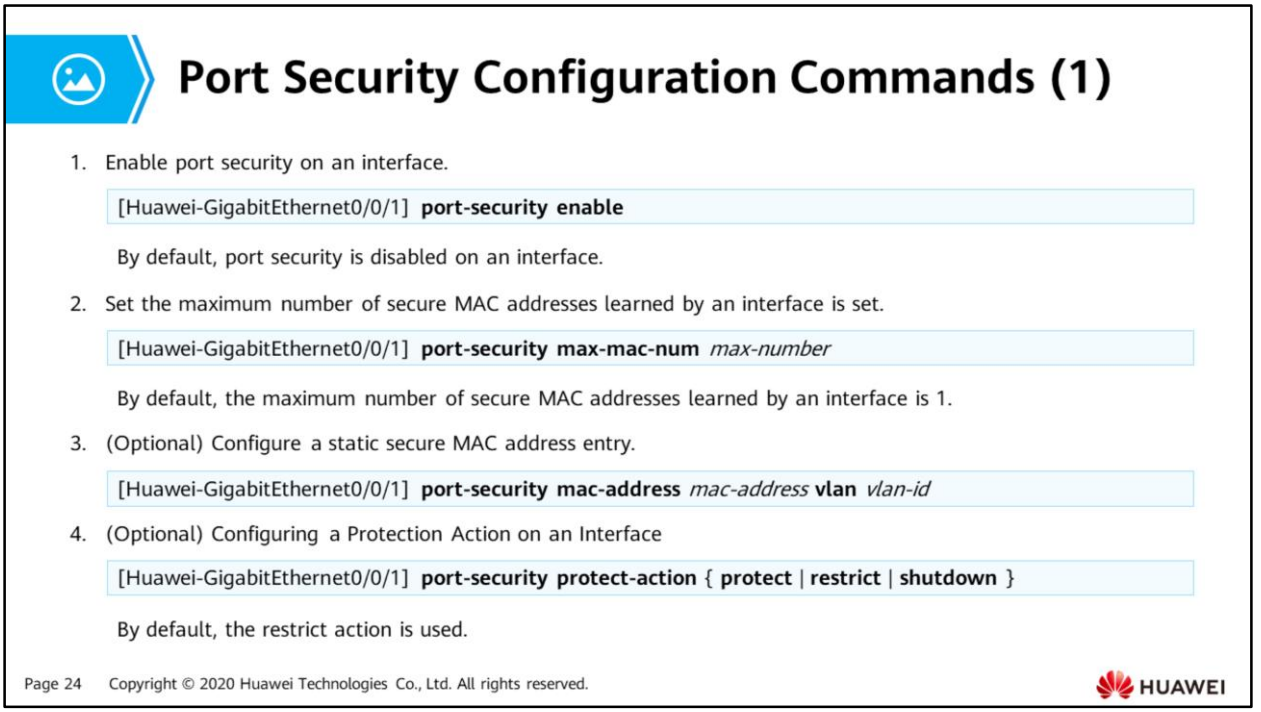
- Secure MAC addresses are usually used together with security protection actions. Common security protection actions are as follows:
  - Restrict: Discards packets with a nonexistent source MAC address and sends a trap.
  - Protect: Discards packets with a nonexistent source MAC address but does not send a trap.
  - Shutdown: Sets the interface state to error-down and generates an alarm.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

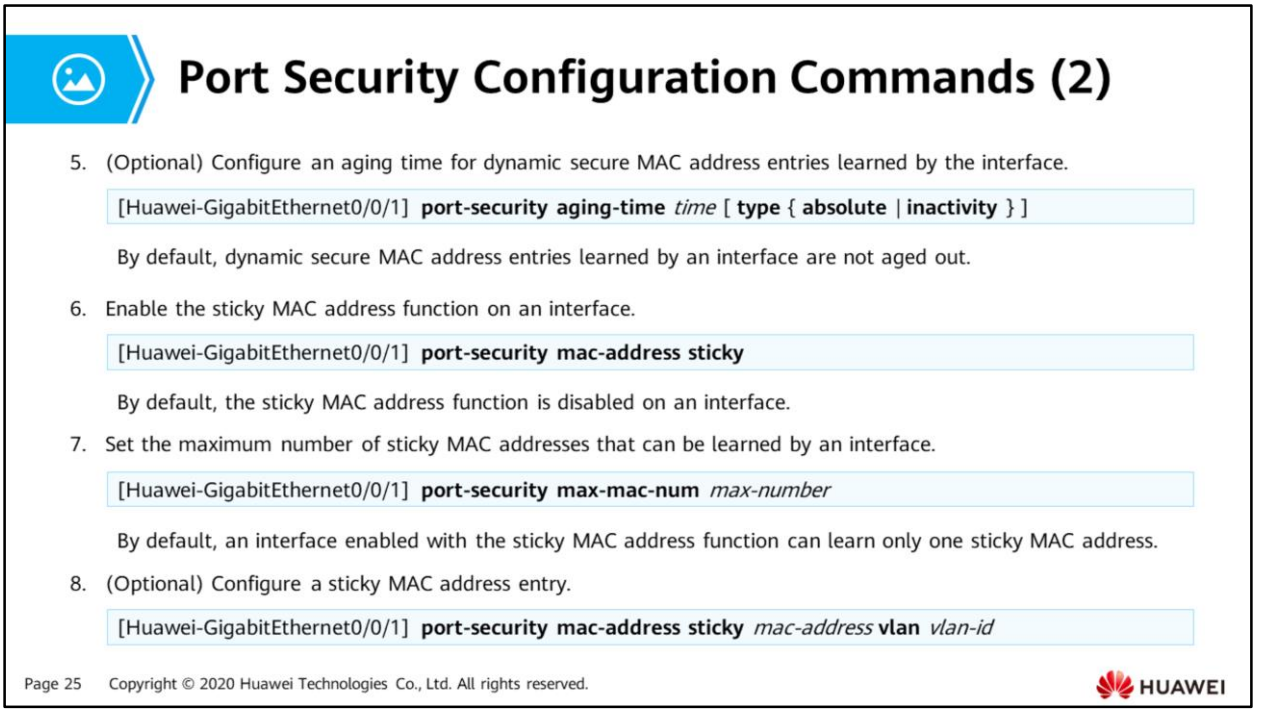
- Dynamic secure MAC addresses can be aged out using two modes: absolute aging and relative aging.
  - Absolute aging time: If the absolute aging time is set to 5 minutes, the system calculates the lifetime of each MAC address every minute. If the lifetime is larger than or equal to 5 minutes, the secure dynamic MAC address is aged immediately. If the lifetime is smaller than time minutes, the system determines whether to delete the secure dynamic MAC address after 1 minute.
  - Relative aging time: If the value is set to 5 minutes, the system checks whether there is traffic from a specified dynamic secure MAC address every 1 minute. If no traffic is received from the secure dynamic MAC address, this MAC address is aged out 5 minutes later.
- By default, an interface in error-down state can be restored only after the restart command is run in the interface view.
- To enable an interface in error-down state to automatically go Up after a period of time, run the **error-down auto-recovery cause port-security interval** *interval-value* command in the system view. In this command, *interval-value* specifies the period of time after which an interface in error-down state can automatically go Up.



- You can configure port security and set the maximum number of secure MAC addresses learned by an interface on networks demanding high access security. Port security enables the switch to convert MAC addresses learned by an interface into secure MAC addresses and to stop learning new MAC addresses after the maximum number of learned MAC addresses is reached. In this case, the switch can only communicate with devices with learned MAC addresses. If the switch receives packets with a nonexistent source MAC address after the number of secure MAC addresses reaches the limit, the switch considers that the packets are sent from an unauthorized user, regardless of whether the destination MAC address of packets is valid, and takes the configured action on the interface. This prevents untrusted users from accessing these interfaces, improving security of the switch and the network.
- Port security enables the switch to convert MAC addresses learned by an interface into secure MAC addresses and to stop learning new MAC addresses after the maximum number of learned MAC addresses is reached. In this case, the switch can only communicate with devices with learned MAC addresses. If the number of access users changes, you can restart the device or set the aging time of secure MAC address entries to update the MAC address entries. If you do not want to change the MAC address entries of stable access users, you can enable the sticky MAC function on the interface. After the configuration is saved, the MAC address entries will not be updated or lost.

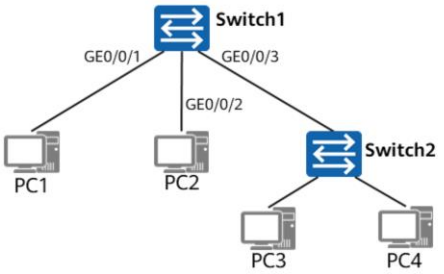


- The **port-security protect-action** command configures the protection action to be used when the number of learned MAC addresses on an interface exceeds the upper limit or static MAC address flapping is detected.
  - protect
    - Discards packets with new source MAC addresses when the number of learned MAC addresses exceeds the limit.
    - When static MAC address flapping occurs, the interface discards the packets with this MAC address.
  - restrict
    - Discards packets with new source MAC addresses and sends a trap message when the number of learned MAC addresses exceeds the limit.
    - When static MAC address flapping occurs, the interface discards the packets with this MAC address and sends a trap.
  - shutdown
    - Sets the interface state to error-down and generates a trap when the number of learned MAC addresses exceeds the limit.
    - Sets the interface state to error-down and generates a trap when static MAC address flapping occurs.



- Check secure MAC addresses.
  - Run the **display mac-address security [vlan vlan-id | interface-type interface-number] * [verbose]** command to check dynamic secure MAC address entries.
  - Run the **display mac-address sec-config [vlan vlan-id | interface-type interface-number] * [verbose]** command to check static secure MAC address entries.
  - Run the **display mac-address sticky [vlan vlan-id | interface-type interface-number] * [verbose]** command to check sticky MAC address entries.

Example for Configuring Port Security — Secure Dynamic MAC Addresses



- Requirements:
  - Configure port security on Switch1.
  - Set the maximum number of MAC addresses learned by GE0/0/1 and GE0/0/2 to 1. When the interface is connected to multiple PCs, Switch1 needs to send an alarm. In addition, interfaces can still forward data frames from authorized PCs.
  - Set the maximum number of MAC addresses that can be learned by GE0/0/3 to 2. When the number of learned MAC addresses exceeds the maximum number, the switch generates an alarm and shuts down GE0/0/3.

Switch1 configuration:

```
[Switch1] interface GigabitEthernet 0/0/1
[Switch1-GigabitEthernet 0/0/1] port-security enable
[Switch1-GigabitEthernet 0/0/1] port-security max-mac-num 1
[Switch1-GigabitEthernet 0/0/1] port-security protect-action restrict
[Switch1] interface GigabitEthernet 0/0/2
[Switch1-GigabitEthernet 0/0/2] port-security enable
[Switch1-GigabitEthernet 0/0/2] port-security max-mac-num 1
[Switch1-GigabitEthernet 0/0/2] port-security protect-action restrict
[Switch1] interface GigabitEthernet 0/0/3
[Switch1-GigabitEthernet 0/0/3] port-security enable
[Switch1-GigabitEthernet 0/0/3] port-security max-mac-num 2
[Switch1-GigabitEthernet 0/0/3] port-security protect-action shutdown
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

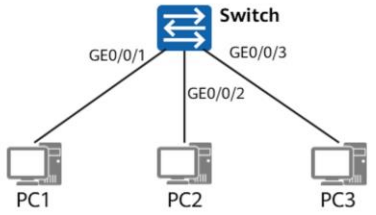
Verifying the Configuration

Run the **display mac-address security** command to check dynamic secure MAC address entries.

```
[Switch1]display mac-address security
MAC address table of slot 0:
-------------------------------------------------------------------------------
MAC Address    VLAN/      PEVLAN CEVLAN Port          Type          LSP/LSR-ID
               VSI/SI                                               MAC-Tunnel
-------------------------------------------------------------------------------
5489-98ac-71a9 1          -      -      GE0/0/3       security      -
5489-98b1-7b30 1          -      -      GE0/0/1       security      -
5489-9815-662b 1          -      -      GE0/0/2       security      -
-------------------------------------------------------------------------------
Total matching items on slot 0 displayed = 3
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Example for Configuring Port Security — Sticky MAC Addresses



- Requirements:
  - Configure port security on the switch. Enable port security on GE0/0/1 through GE0/0/3.
  - Set the maximum number of MAC addresses that can be learned by GE0/0/1 and GE0/0/2 to 1 and convert secure dynamic MAC addresses learned by GE0/0/1 and GE0/0/2 to sticky MAC addresses.
  - On GE0/0/3, set the maximum number of MAC addresses that can be learned to 1, manually create a sticky MAC address entry for the interface, and bind the interface to MAC address 5489-98ac-71a9. Retain the default penalty on each interface.

Switch configuration:

```
[Switch] interface GigabitEthernet 0/0/1
[Switch-GigabitEthernet 0/0/1] port-security enable
[Switch-GigabitEthernet 0/0/1] port-security max-mac-num 1
[Switch-GigabitEthernet 0/0/1] port-security mac-address sticky
[Switch] interface GigabitEthernet 0/0/2
[Switch-GigabitEthernet 0/0/2] port-security enable
[Switch-GigabitEthernet 0/0/2] port-security max-mac-num 1
[Switch-GigabitEthernet 0/0/2] port-security mac-address sticky
[Switch] interface GigabitEthernet 0/0/3
[Switch-GigabitEthernet 0/0/3] port-security enable
[Switch-GigabitEthernet 0/0/3] port-security max-mac-num 1
[Switch-GigabitEthernet 0/0/3] port-security mac-address sticky
[Switch-GigabitEthernet 0/0/3] port-security mac-address sticky
5489-98ac-71a9 vlan 1
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Verifying the Configuration

Run the **display mac-address sticky** command to check sticky MAC address entries.

```
[Switch1]display mac-address sticky
MAC address table of slot 0:
-------------------------------------------------------------------------------
MAC Address    VLAN/      PEVLAN CEVLAN  Port          Type      LSP/LSR-ID
               VSI/SI                                              MAC-Tunnel
-------------------------------------------------------------------------------
5489-98ac-71a9 1          -      -       GE0/0/3       sticky    -
5489-98b1-7b30 1          -      -       GE0/0/1       sticky    -
5489-9815-662b 1          -      -       GE0/0/2       sticky    -
-------------------------------------------------------------------------------
Total matching items on slot 0 displayed = 3
```

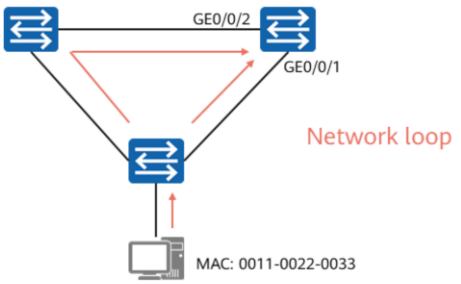

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

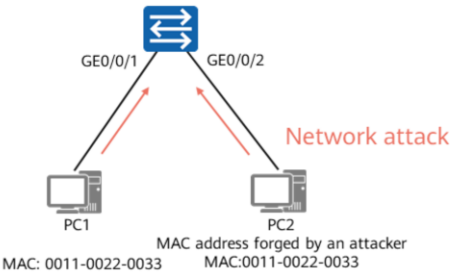
Contents

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

MAC Address Flapping Detection

- MAC address flapping occurs when a MAC address is learned by two interfaces in the same VLAN on a switch and the MAC address entry learned later overrides the earlier one.
- When a MAC address frequently switches between two interfaces, MAC address flapping occurs.
- MAC address flapping frequently occurs on networks where loops or network attacks occur.





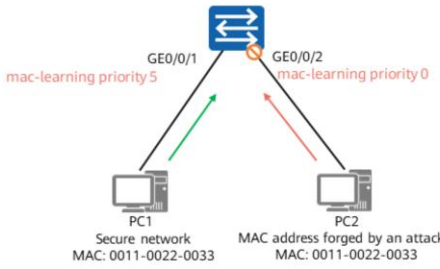
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

MAC Address Flapping Prevention

If MAC address flapping is caused by loops, deploy loop prevention technologies, such as STP, to eliminate Layer 2 loops. If MAC address flapping is caused by network attacks or other reasons, you can use the following MAC address flapping prevention measures.

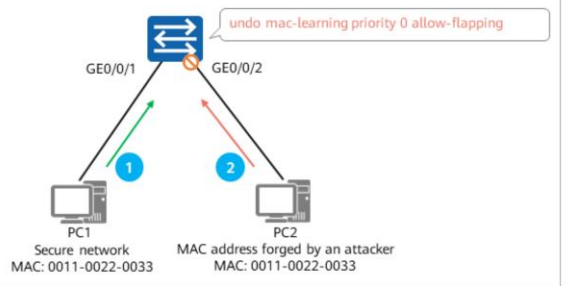
Configuring a MAC address learning priority for an interface

If the same MAC address is learned on interfaces that have different priorities, the MAC address entry on the interface with the highest priority overrides that on the other interfaces.



Preventing MAC address entries from being overridden on interfaces with the same priority

If the interface connected to a bogus network device has the same priority as the interface connected to an authorized device, the MAC address entry of the bogus device learned later does not override the original correct MAC address entry.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- By default, the MAC address learning priority of an interface is 0. A larger priority value indicates a higher MAC address learning priority. If the same MAC address is learned on interfaces that have different priorities, the MAC address entry on the interface with the highest priority overrides that on the other interfaces.
- When the device is configured to prevent MAC address entries from being overridden on interfaces with the same priority, if the authorized device is powered off, the MAC address entry of the bogus device is learned. After the authorized device is powered on again, its MAC address cannot be learned. Exercise caution when using this feature. If a switch interface is connected to a server, when the server is powered off, other interfaces can learn the same MAC address as the server. When the server is powered on again, the switch cannot learn the correct MAC address.

MAC Address Flapping Detection

The switch supports the following MAC address flapping detection mechanisms.

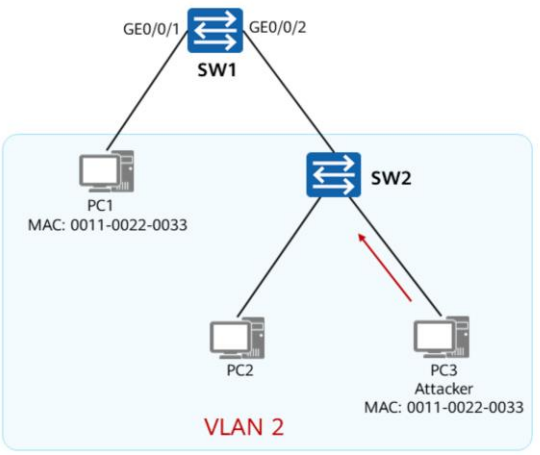
- VLAN-based MAC address flapping detection
  - After MAC address flapping detection is configured in a VLAN, the switch can detect MAC address flapping in a specified VLAN.
  - You can configure an action to take on an interface when MAC address flapping is detected on an interface, for example, sending a trap or blocking the interface or MAC address.
- Global MAC address flapping detection
  - The global MAC address flapping detection function detects all MAC addresses on the device.
  - If MAC address flapping occurs, the device will send a trap to the NMS.
  - You can also specify an action to take when MAC address flapping is detected, for example, shutting down the interface or removing the interface from the VLAN.

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Whether all Huawei switches support MAC address flapping detection depends on the switch model.

VLAN-based MAC Address Flapping Detection



When VLAN-based MAC address flapping detection is configured and detects MAC address flapping on an interface, you can configure one of the following actions:

1. Trap sending: The device only sends a trap to the NMS.
2. Interface blocking: The interface is blocked for a specified period of time and the interface is disabled from sending and receiving packets.
3. MAC address blocking: The device blocks only the current MAC address but not the physical interface. Communication of other MAC addresses on the current interface is not affected.

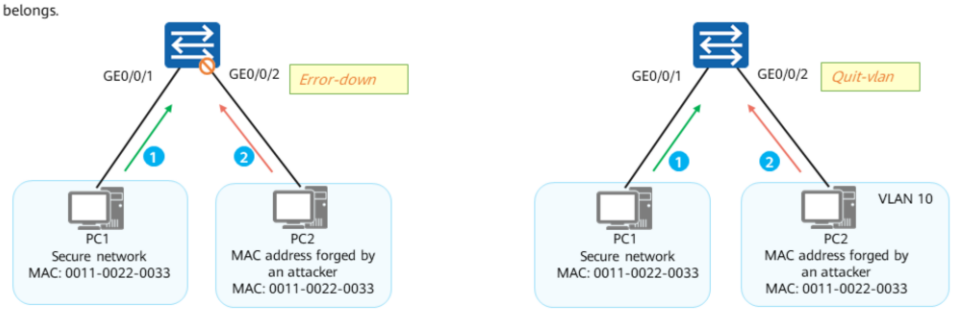
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- After MAC address flapping occurs, the following actions are performed: 1. A trap is generated and reported. 2. GE0/0/2 on SW1 is disabled from sending and receiving packets. 3. GE0/0/2 on SW1 is disabled from sending and receiving packets with a specified MAC address.
- When an interface is blocked:
  - When detecting MAC address flapping in VLAN 2, the device blocks the interface where MAC address flapping occurs.
  - The interface will be blocked for 10s (specified by the **block-time** keyword). The blocked interface cannot receive or send data.
  - After 10 seconds, the interface is unblocked and starts to send and receive data. If MAC address flapping is not detected within 20 seconds, the interface is unblocked. If MAC address flapping is detected again on the interface within 20 seconds, the switch blocks the interface again. If the switch still detects MAC address flapping on the interface, the switch permanently blocks the interface. The **retry-times** parameter specifies the number of times that MAC address flapping is detected.

Global MAC Address Flapping Detection

When a switch detects MAC address flapping, it only reports a trap by default and does not take other actions. In practice, you can define the following actions after MAC address flapping is detected:

- error-down
  - When an interface configured with MAC address flapping detection detects MAC address flapping, the interface is set to enter the Error-Down state and does not forward data.
- quit-vlan
  - When an interface configured with MAC address flapping detection detects MAC address flapping, the interface is removed from the VLAN to which the interface belongs.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- By default, global MAC address flapping detection is enabled on a Huawei switch. Therefore, the switch performs MAC address flapping detection in all VLANs by default.
- In some scenarios, MAC address flapping detection needs to be disabled in some VLANs. You can configure a VLAN whitelist for MAC address flapping detection.
- If an interface is set to enter the Error-Down state due to MAC address flapping, the interface does not automatically restore to the Up state by default.
- To enable an interface in Error-Down state to automatically go Up, run the **error-down auto-recovery cause mac-address-flapping interval** *time-value* command in the system view.

- If MAC address flapping occurs on an interface and the interface is removed from the VLAN, you can run the following command in the system view to implement automatic recovery of the interface:

  mac-address flapping quit-vlan recover-time time-value

Configuration Commands of MAC Address Flapping Prevention and Detection (1)

1. Configure a MAC address learning priority for an interface.

   [Huawei-GigabitEthernet0/0/1] **mac-learning priority** *priority-id*

   By default, the MAC address learning priority of an interface is 0. A larger priority value indicates a higher MAC address learning priority.

2. Configure the device to discard packets when the device is configured to prohibit MAC address flapping.

   [Huawei-GigabitEthernet0/0/1] **mac-learning priority flapping-defend action discard**

   By default, the action is **forward** when the device is configured to prohibit MAC address flapping.

3. Configure the device to prevent MAC address entries from being overridden on interfaces with the same priority.

   [Huawei] **undo mac-learning priority** *priority-id* **allow-flapping**

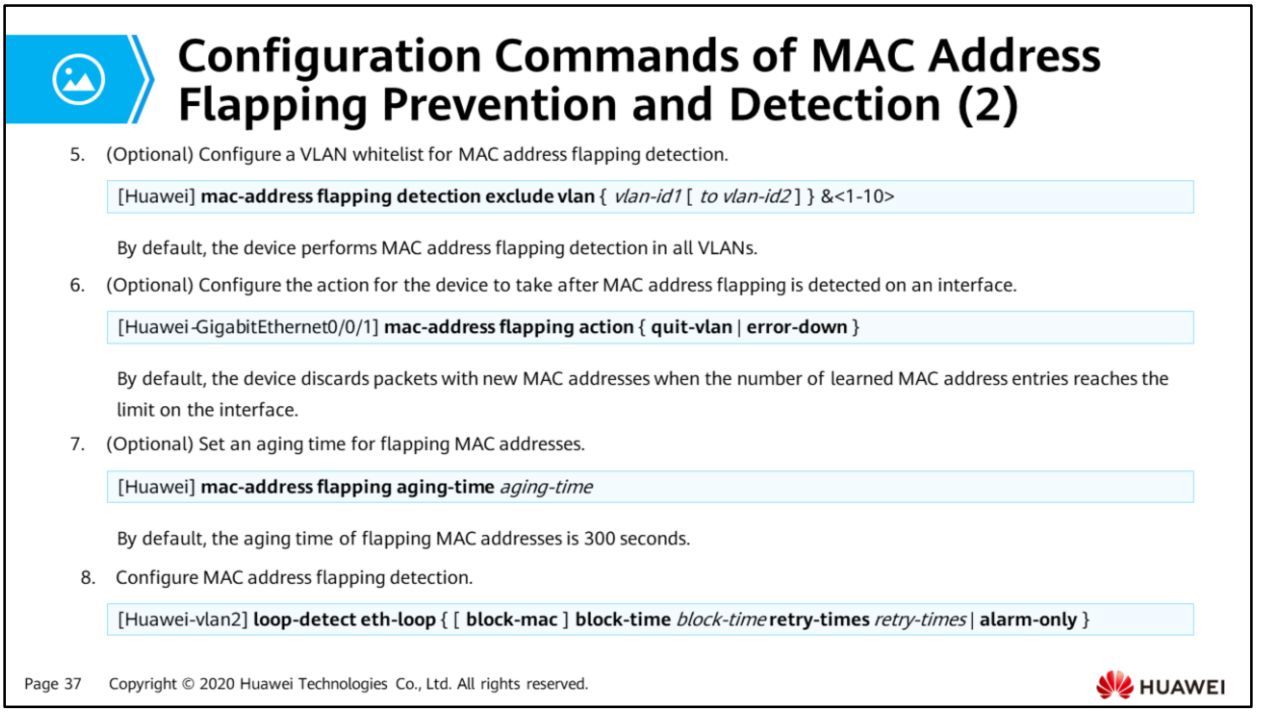
   By default, MAC address flapping between interfaces with the same priority is allowed.

4. Configuring MAC Address Flapping Detection

   [Huawei-vlan2] **mac-address flapping detection**

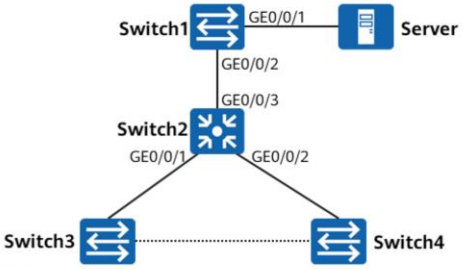
   By default, the device performs MAC address flapping detection in all VLANs.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



- Insecure networks are vulnerable to MAC address attacks. If attackers send large numbers of forged packets with different source MAC addresses to the switch, its MAC address table will be filled with unwanted address entries. As a result, the device is unable to learn the source MAC addresses of valid packets.
- You can limit the number of MAC address entries that can be learned on the device. When the number of learned MAC address entries reaches the limit, the device does not learn new MAC address entries. You can also configure an action to take when the number of learned MAC address entries reaches the limit. This prevents MAC address entries from being exhausted and improves network security.

Example for Configuring MAC Address Flapping Prevention and Detection



Requirements:

- Basic network configurations are complete, but an incorrect connection of a network cable between Switch3 and Switch4 causes a loop on the network.
- Configure MAC address flapping prevention on GE0/0/1 of Switch1 to prevent attacks from unauthorized users.
- Configure MAC address flapping detection on Switch2 to detect loops on the network and rectify the faults.

1. Set the MAC address learning priority of GE0/0/1 that connects Switch1 to the server to be higher than that of other interfaces. The default MAC address learning priority is 0.

```
[Switch1] interface GigabitEthernet 0/0/1
[Switch1-GigabitEthernet 0/0/1] mac-learning priority 3
```

2. Configure MAC address flapping detection on Switch2 and configure an action to taken when MAC address flapping is detected on an interface.

```
[Switch2] mac-address flapping detection
[Switch2] mac-address flapping aging-time 500
[Switch2-GigabitEthernet0/0/1] mac-address flapping action error-down
[Switch2-GigabitEthernet0/0/2] mac-address flapping action error-down
[Switch2] error-down auto-recovery cause mac-address-flapping interval 500
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- When Switch3 and Switch4 are incorrectly connected, the MAC address of GE0/0/1 on Switch2 is learned by GE0/0/2, causing GE0/0/2 to enter the Error-Down state.
- You can run the **display mac-address flapping record** command to check MAC address flapping records.

Verifying the Configuration

When the MAC address of GE0/0/1 on Switch2 is learned by GE0/0/2, GE0/0/2 is shut down. You can run the **display mac-address flapping record** command to check MAC address flapping records.

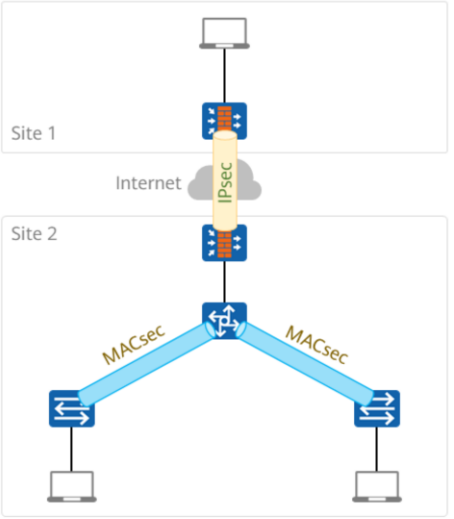
```
[Switch2] display mac-address flapping record
 S  : start time
 E  : end time
(Q) : quit vlan
(D) : error down
--------------------------------------------------------------------------------
Move-Time               VLAN MAC-Address     Original-Port   Move-Ports   MoveNum
--------------------------------------------------------------------------------
S:2020-06-22 17:22:36   1    5489-9815-662b  GE0/0/1         GE0/0/2(D)   83
E:2020-06-22 17:22:44
--------------------------------------------------------------------------------
Total items on slot 0: 1
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

MACsec Provides Secure Layer 2 Data Transmission



Background

Most data is transmitted in plain text on LAN links, posing security risks in scenarios demanding high security.

Overview of MACsec

Media Access Control Security (MACsec), in compliance with 802.1AE, defines an Ethernet-based data security communication method. It encrypts data hop by hop to ensure data transmission security.

- Data integrity check
- Data encryption
- Identity authentication
- Replay protection

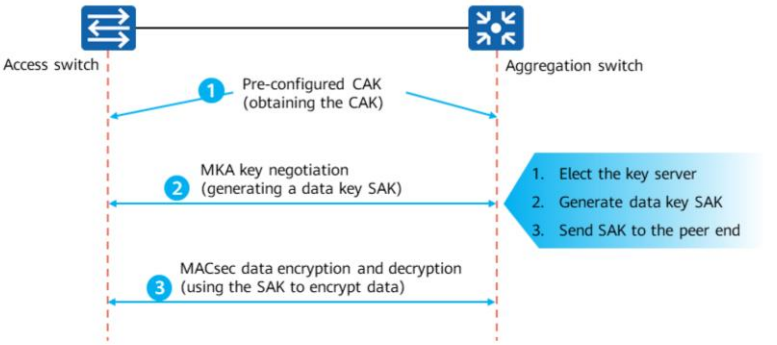
Typical Application Scenarios

- MACsec is deployed between switches to ensure data security. For example, MACsec is deployed between access switches and uplink aggregation or core switches.
- When transmission devices exist between switches, MACsec can be deployed to ensure data security.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Working Mechanism of MACsec

When the device runs point-to-point MACsec, a network administrator pre-configures the same Secure Connectivity Association Key (CAK) on the two devices using commands. The two devices use the MACsec Key Agreement (MKA) to elect a key server. The key server determines the encryption scheme, uses an encryption algorithm to generate a Secure Association Key (SAK) based on parameters such as the CAK, and distributes the SAK to the peer device. In this way, the two devices have the same SAK, which can be used to encrypt and decrypt MACsec data packets.



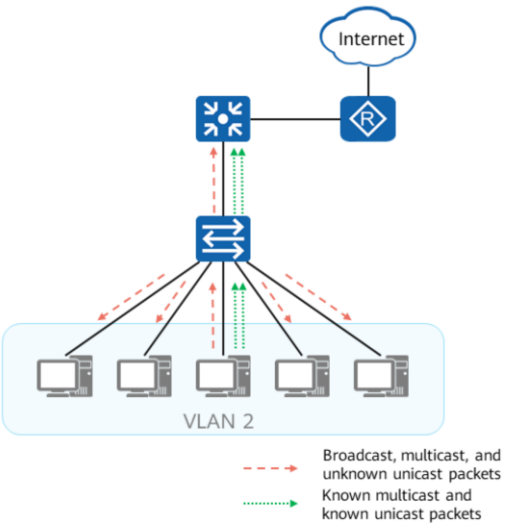
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- A CAK is not directly used to encrypt data packets. Instead, the CAK and other parameters derive the encryption key of data packets. The CAK can be delivered during 802.1X authentication or statically configured.
- MKA is used for negotiation of MACsec data encryption keys.
- The SAK is derived based on the CAK using an algorithm and is used to encrypt data transmitted over secure channels. The MKA limits the number of packets that can be encrypted by each SAK. When the PNs encrypted by a SAK are exhausted, the SAK is updated. For example, on a 10 Gbit/s link, the SAK can be updated every 4.8 minutes.
- The key server determines the encryption scheme and the MKA entity that distributes the key.

Contents

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Overview of Traffic Suppression

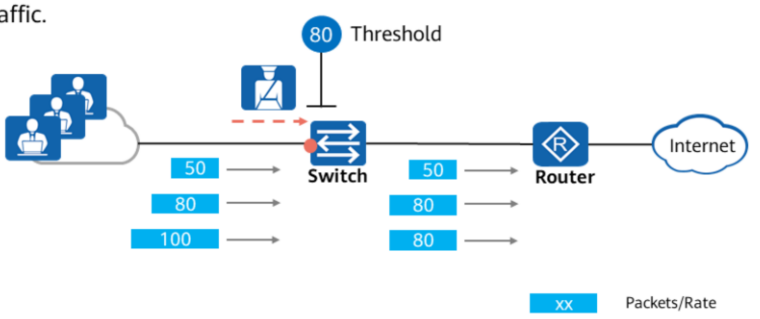


- **Issues on networks:**
  - In normal situations, when a Layer 2 Ethernet interface receives broadcast, unknown multicast, or unknown unicast packets, it forwards the packets to other Layer 2 Ethernet interfaces in the same VLAN. As a result, traffic flooding occurs and the forwarding performance of the device deteriorates.
  - When an Ethernet interface on the device receives known multicast or unicast packets, heavy traffic of a certain type of packets may affect the processing of other services on the switch.
- **Solution:**
  - Traffic suppression can rate-limit the broadcast, unknown multicast, unknown unicast, known multicast, and known unicast packets by setting thresholds. This prevents traffic flooding caused by broadcast, unknown multicast, and unknown unicast packets and the impact incurred by a large number of known multicast and known unicast packets.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Working Mechanism of Traffic Suppression (1)

In the inbound direction of an interface, the switch can suppress broadcast, unknown multicast, unknown unicast, known multicast, and known unicast packets based on the percentage, packet rate, and bit rate. The device monitors the rate of various types of packets on an interface and compares the rate with the threshold. When the traffic rate on the interface in the inbound direction reaches the threshold, the device discards excess traffic.

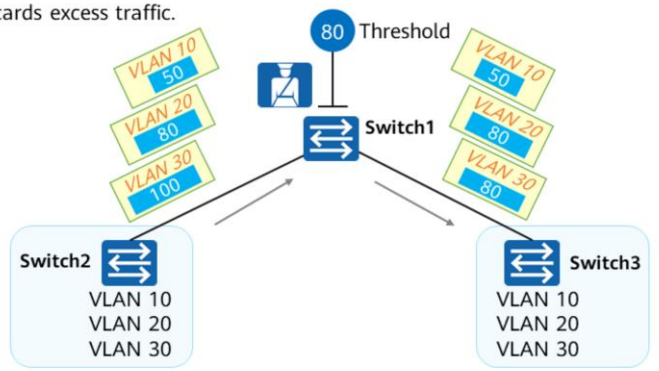


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- In the outbound direction of an interface, the device can block broadcast packets, unknown multicast packets, and unknown unicast packets.

Working Mechanism of Traffic Suppression (2)

In the VLAN view, the device can rate-limit broadcast packets by the bit rate. The device monitors the rate of broadcast packets in the same VLAN and compares the rate with the threshold. When the traffic rate in the VLAN reaches the threshold, the device discards excess traffic.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Traffic suppression can also rate-limit ICMP packets by setting a threshold. A large number of ICMP packets may be sent to the CPU without traffic suppression. When this happens, other service functions may become abnormal.

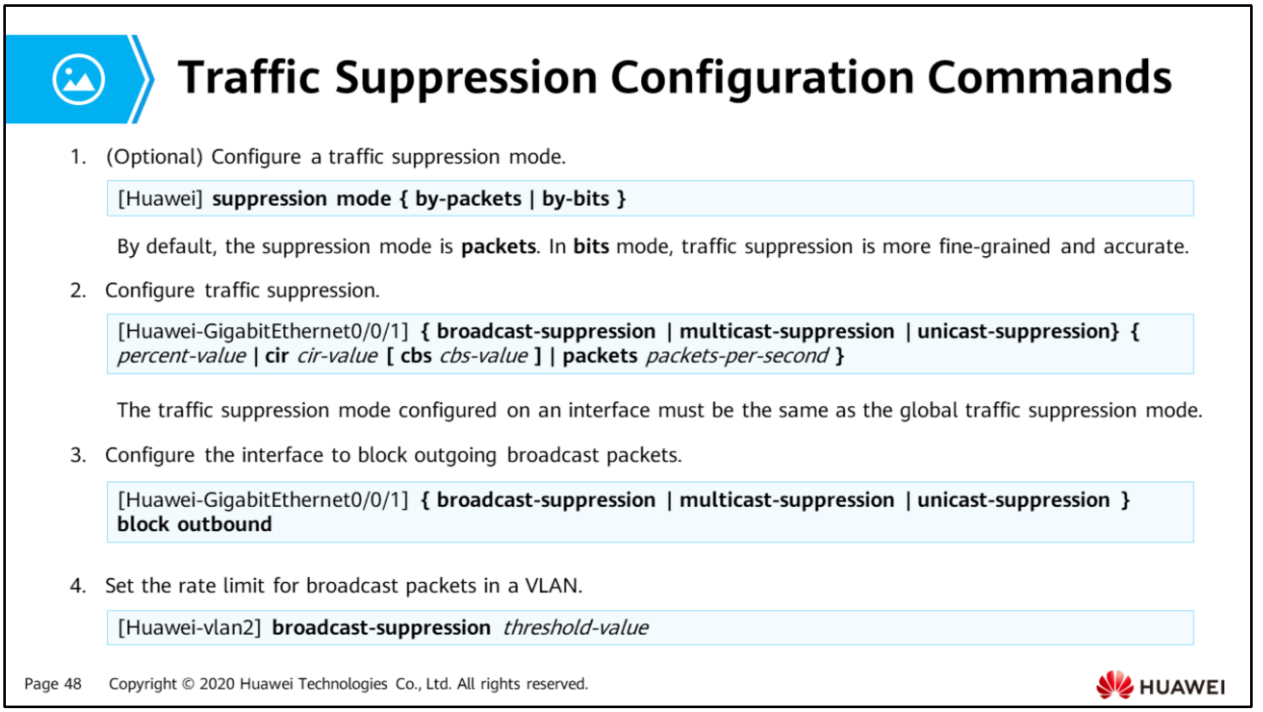
Application of Traffic Suppression

Traffic suppression limits the rate at which packets are sent by taking different measures for different types of packets. It involves the following situations:

1. In the inbound direction of a switch interface, for example, in the inbound direction of GE0/0/1 on SW1, traffic suppression can be used to limit the rate at which any packet is sent.
2. In the outbound direction of a switch interface, for example, in the outbound direction of GE0/0/1 on SW1, traffic suppression can be used to block broadcast, unknown multicast, and unknown unicast packets.
3. In the VLAN view of the switch, configure traffic suppression in a VLAN to limit the number of broadcast packets in the VLAN.

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- The threshold can be configured for incoming packets on interfaces. The system discards the traffic exceeding the threshold and forwards the traffic within the threshold. In this way, the system limits the traffic rate in an acceptable range.
- Note that traffic suppression can also block outgoing packets on interfaces.
- In storm control, rate thresholds are configured for incoming packets only on interfaces. When the traffic exceeds the threshold, the system rejects the packets of this particular type on the interface or shuts down the interface.



- Run the **display flow-suppression interface** *interface-type interface-number* command to check the traffic suppression configuration.
- When traffic suppression is configured in both the interface view and VLAN view, the configuration in the interface view takes precedence over the configuration in the VLAN view.

Example for Configuring Traffic Suppression

Requirements:

- Configure traffic suppression in the view of GE0/0/1 to limit the capability of forwarding broadcast, unknown multicast, and unknown unicast packets on the Layer 2 network.
- Set the bandwidth percentage for broadcast packets to 60%.
- Set the bandwidth percentage for unknown multicast packets to 70%.
- Set the bandwidth percentage for unknown unicast packets to 80%.

Switch configuration:

```
[Switch]suppression mode by-packets
[Switch-GigabitEthernet0/0/1] unicast-suppression 80
[Switch-GigabitEthernet0/0/1] multicast-suppression 70
[Switch-GigabitEthernet0/0/1] broadcast-suppression 60
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Verifying the Configuration

Run the **display flow-suppression interface** command to check the traffic suppression configuration.

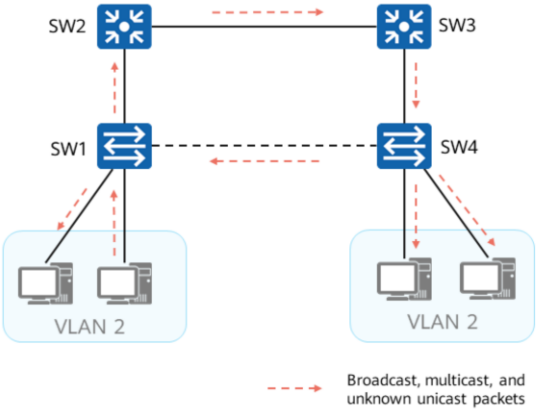
```
[Switch]dis flow-suppression interface GigabitEthernet 0/0/1
 storm type          rate mode          set rate value
-------------------------------------------------------------------------------
 unknown-unicast     percent            percent: 80%
 multicast           percent            percent: 70%
 broadcast           percent            percent: 60%
-------------------------------------------------------------------------------
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Overview of Storm Control

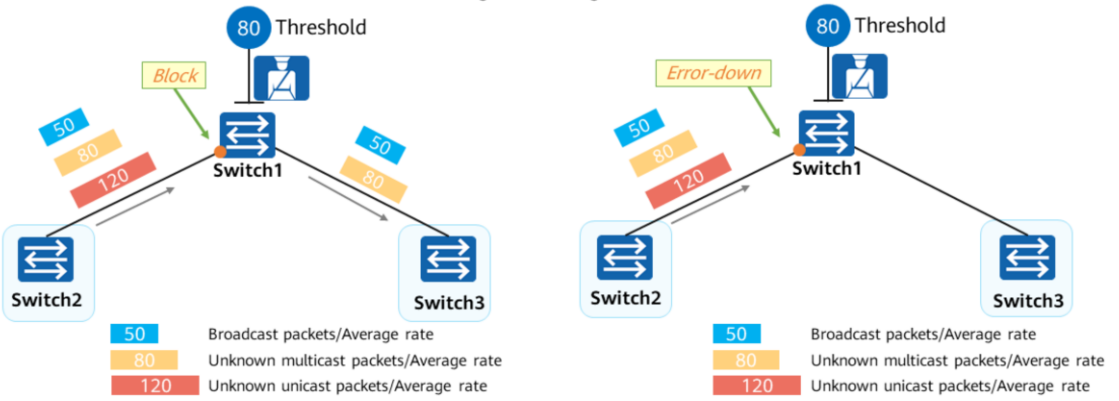


- **Issues on networks:**
  - In normal situations, when a Layer 2 Ethernet interface receives broadcast, unknown multicast, or unknown unicast packets, it forwards the packets to other Layer 2 Ethernet interfaces in the same VLAN. As a result, traffic flooding occurs and the forwarding performance of the device deteriorates.
- **Solution:**
  - Storm control blocks broadcast, unknown multicast, and unknown unicast packets by disabling related interfaces.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Working Mechanism of Storm Control

Storm control prevents broadcast storms caused by broadcast packets, unknown multicast packets, and unknown unicast packets. Within the storm detection interval, the device compares the average rate of the three types of packets received on the monitoring interface with the configured maximum threshold. When the packet rate reaches the threshold, the device configured with storm control blocks packets on the interface or shuts down the interface according to the configured action.



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

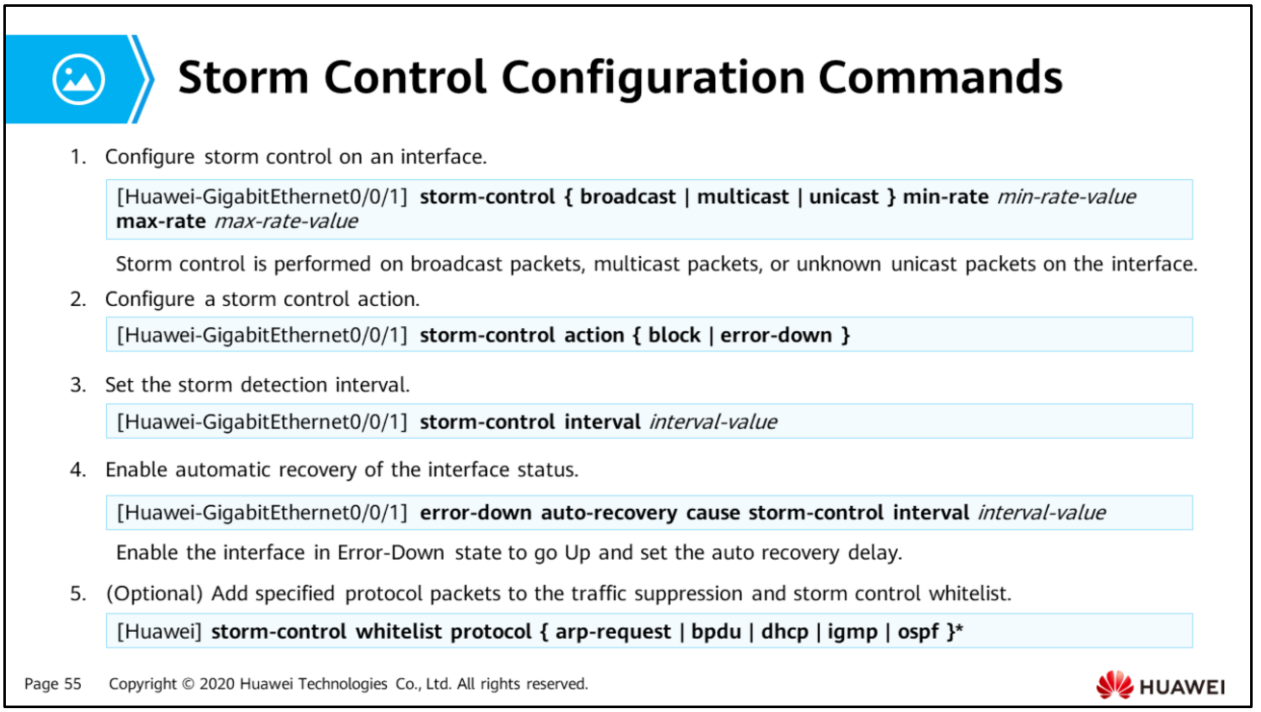
- The difference between traffic suppression and storm control is as follows: The storm control function can take the punishment action (**block** or **shutdown**) for an interface, whereas the traffic suppression function only limits the traffic on an interface.

Application of Storm Control

- Compared with traffic suppression, storm control monitors the average rates of broadcast packets, unknown multicast packets, and unknown unicast packets on an interface, and then blocks packets on the interface or shuts down the physical interface according to the threshold.
- As shown in the figure, the switch is connected to a Layer 2 network and a router. To limit the rates of broadcast packets, unknown multicast packets, and unknown unicast packets forwarded by the Layer 2 network, configure storm control on the Layer 2 Ethernet interface GE0/0/1 of the switch.

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- In traffic suppression, rate thresholds are configured for incoming packets on interfaces. When the traffic exceeds the threshold, the system discards excess traffic and allows the packets within the threshold to pass through. In this way, the traffic is limited within a proper range. Note that traffic suppression can also block outgoing packets on interfaces.
- In storm control, rate thresholds are configured for incoming packets only on interfaces. When the traffic exceeds the threshold, the system rejects the packets of this particular type on the interface or shuts down the interface.



- Run the **display storm-control** [**interface** *interface-type interface-number*] command to check the storm control configuration on an interface.
- **min-rate** *min-rate-value*
  - Specify the lower threshold in packet rate limit mode. If the value of *min-rate-value* (pps) is specified, packets received by an interface are forwarded when the rate of receiving packets is smaller than the value of *min-rate-value* in the storm detection interval.
- **min-rate cir** *min-rate-value-cir*
  - Specify the lower threshold in byte rate limit mode. If the value of *min-rate-value-cir* (kbit/s) is specified, packets received by an interface are forwarded when the rate of receiving packets is smaller than the value of *min-rate-value-cir* in the storm detection interval.
- **min-rate percent** *min-rate-value-percent*
  - Specify the lower threshold in percentage rate limit mode. If the value of *min-rate-value-percent* (percentage) is specified, packets received by an interface are forwarded when the rate of receiving packets is lower than the value of *min-rate-value-percent* in the storm detection interval.

Example for Configuring Storm Control

- Requirements
  - The switch is required to prevent broadcast storms caused by broadcast packets, unknown multicast packets, and unknown unicast packets forwarded on the Layer 2 network.
- Configuration roadmap:
  - Configure storm control on GE0/0/1 to prevent broadcast storms on the Layer 2 network.

Switch configuration:

```
[Switch] storm-control whitelist protocol arp-request
[Switch] interface gigabitethernet0/0/1
[Switch-GigabitEthernet0/0/1] storm-control broadcast min-rate 1000 max-rate 2000
[Switch-GigabitEthernet0/0/1] storm-control multicast min-rate 1000 max-rate 2000
[Switch-GigabitEthernet0/0/1] storm-control unicast min-rate 1000 max-rate 2000
[Switch-GigabitEthernet0/0/1] storm-control interval 90
[Switch-GigabitEthernet0/0/1] storm-control action block
[Switch-GigabitEthernet0/0/1] storm-control enable trap
# Enable the trap function for storm control.
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Verifying the Configuration

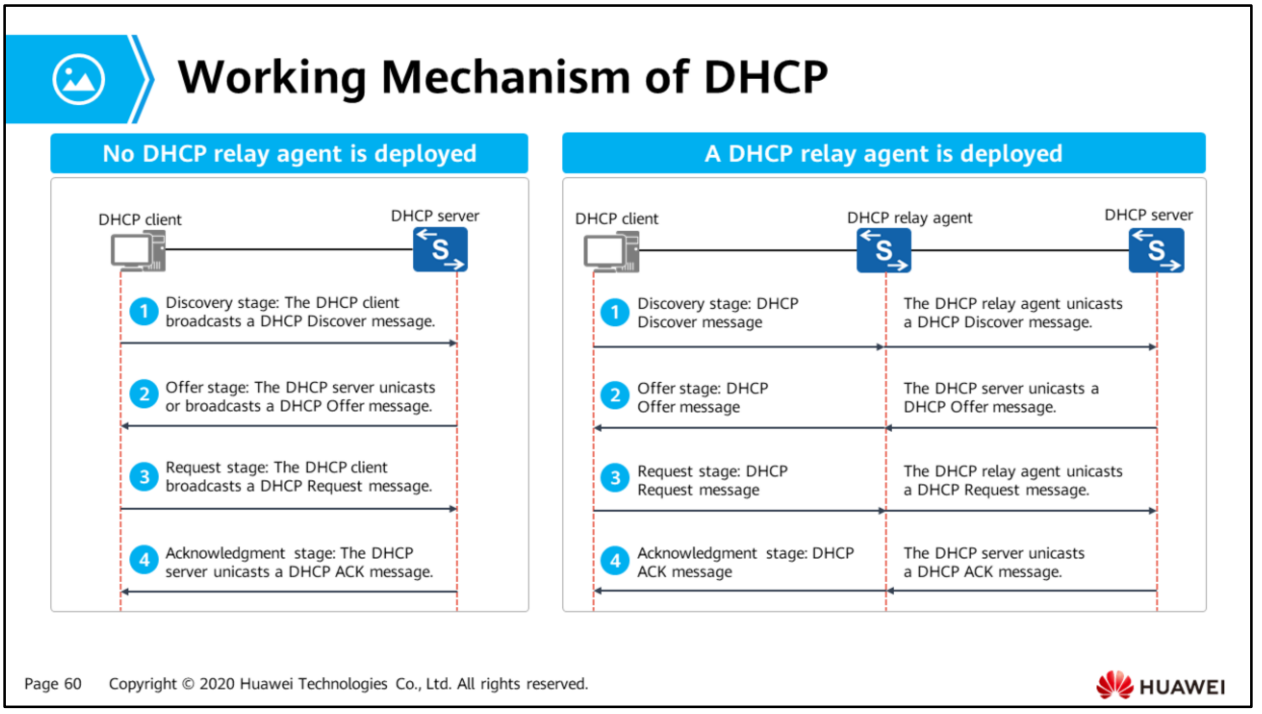
Run the **display storm-control interface** command to check the storm control configuration on GE0/0/1.

```
[Switch]display storm-control interface GigabitEthernet 0/0/1
PortName    Type      Rate        Mode    Action    Punish-  Trap Log Int  Last-
                      (Min/Max)                     Status                 Punish-Time
-------------------------------------------------------------------------------------------------
GE0/0/1     Multicast 1000        Pps     Block     Normal   On   Off      90
                      /2000
GE0/0/1     Broadcast 1000        Pps     Block     Normal   On   Off       90
                      /2000
GE0/0/1     Unicast    1000       Pps     Block     Normal   On   Off      90
                      /2000
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



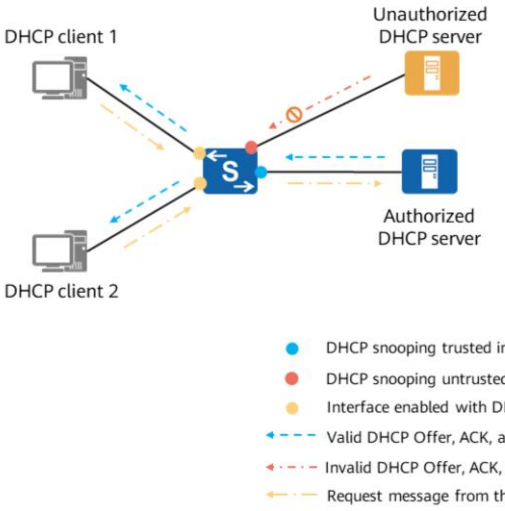
- No DHCP relay agent is deployed:
  - 1. In the discovery stage, the DHCP client broadcasts a DHCP Discover message to discover DHCP servers. Information carried in a DHCP Discover message includes the client's MAC address (Chaddr field), parameter request list (Option 55), and broadcast flag (Flags field, determining whether the response should be sent in unicast or broadcast mode).
  - 2. In the offer stage, a DHCP server selects an address pool on the same network segment as the IP address of the interface receiving the DHCP Discover message, and selects an idle IP address from the address pool. The DHCP server then sends a DHCP Offer message carrying the allocated IP address to the DHCP client.
  - 3. In the request stage, if multiple DHCP servers reply with a DHCP Offer message to the DHCP client, the client accepts only the first received DHCP Offer message. The client then broadcasts a DHCP Request message carrying the selected DHCP server identifier (Option 54) and IP address (Option 50, with the IP address specified in the Yiaddr field of the accepted DHCP Offer message). The DHCP Request message is broadcast so as to notify all the DHCP servers that the DHCP client has selected the IP address offered by a DHCP server. Then the other servers can allocate IP addresses to other clients.
  - 4. In the acknowledgement stage, after receiving the DHCP ACK message, the DHCP client broadcasts a gratuitous ARP packet to check whether any other terminal on the network segment uses the IP address allocated by the DHCP server.

Overview of DHCP Snooping

- DHCP snooping is equivalent to a firewall between DHCP clients and the DHCP server to defend against DHCP attacks on the network, ensuring security for communication services.
- DHCP snooping ensures that DHCP clients obtain IP addresses only from authorized DHCP servers and a DHCP snooping-enabled device records mappings between IP addresses and MAC addresses of DHCP clients, preventing DHCP attacks on the network.
- Some attacks are launched based on DHCP. These attacks include the bogus DHCP server attack, DHCP server DoS attack, and bogus DHCP message attack.
- DHCP snooping uses the DHCP snooping trusted interface and DHCP snooping binding table to ensure DHCP network security.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

DHCP Snooping Trust Function



- The DHCP snooping trust function ensures that DHCP clients obtain IP addresses from authorized DHCP servers.
- DHCP snooping involves two interface roles: trusted interface and untrusted interface.
  - DHCP ACK messages, NAK messages, and Offer messages are received from the trusted interface.
  - In addition, the device only forwards DHCP Request messages from DHCP clients to the authorized DHCP server through the trusted interface.
  - DHCP ACK messages, NAK messages, and Offer messages are discarded on untrusted interfaces.

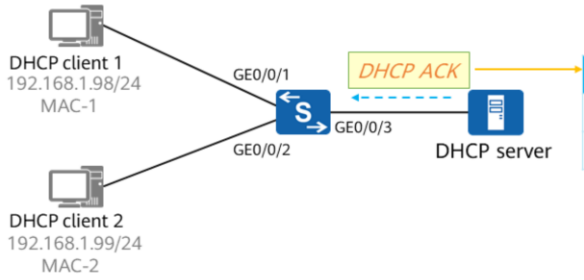
 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- After the **dhcp snooping enable** command is run on an interface, the interface forwards received DHCP Request messages to all trusted interfaces and discards received DHCP Reply messages.
- After an interface on which the **dhcp snooping trusted** command is run receives a DHCP Request message, it forwards the message to all other trusted interfaces. If there are no other trusted interfaces, it discards the message. After receiving a DHCP Reply message, it forwards the message only to the interfaces that are connected to clients and have the **dhcp snooping enable** command configured. If such interfaces cannot be found, it discards the DHCP Reply message.

DHCP Snooping Binding Table

- The Layer 2 access device enabled with DHCP snooping obtains required information, such as the PC's MAC address, IP address, and address lease, from the DHCP ACK messages, learns information (interface number and VLAN ID) about the DHCP snooping-enabled interface connected to the PC, and generates a DHCP snooping binding entry for the PC.
- The DHCP snooping binding table records the mapping between IP addresses and MAC addresses of DHCP clients. The device can check DHCP messages against the DHCP snooping binding table to prevent attacks initiated by unauthorized users.



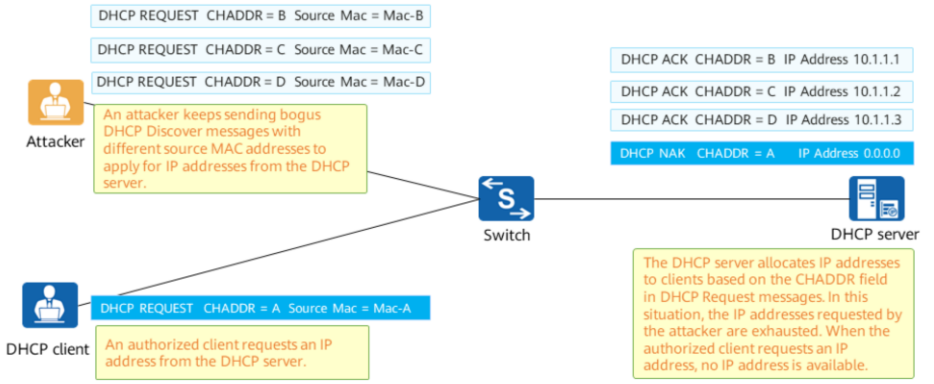
IP	MAC	VLAN	Interface	Lease
192.168.1.98	MAC-1	1	GE0/0/1	1
192.168.1.99	MAC-2	1	GE0/0/2	1

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- DHCP snooping binding entries are aged out when the DHCP release expires, or the entries are deleted when users send DHCP Release messages to release IP addresses.

DHCP Starvation Attacks

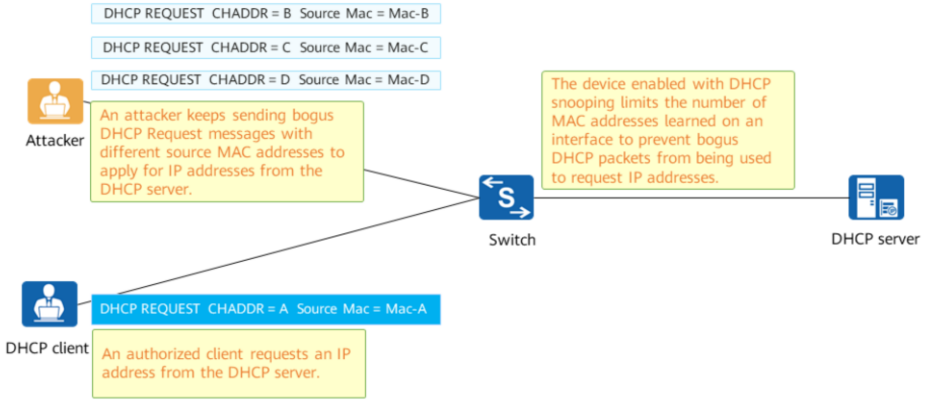
- An attacker continuously applies to the DHCP server for a large number of IP addresses until the IP addresses in the address pool of the DHCP server are exhausted. As a result, the DHCP server cannot allocate IP addresses to authorized users.
- Vulnerability analysis: When the DHCP server allocates IP addresses to clients, it cannot distinguish authorized and unauthorized users.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

Defense Against DHCP Starvation Attacks

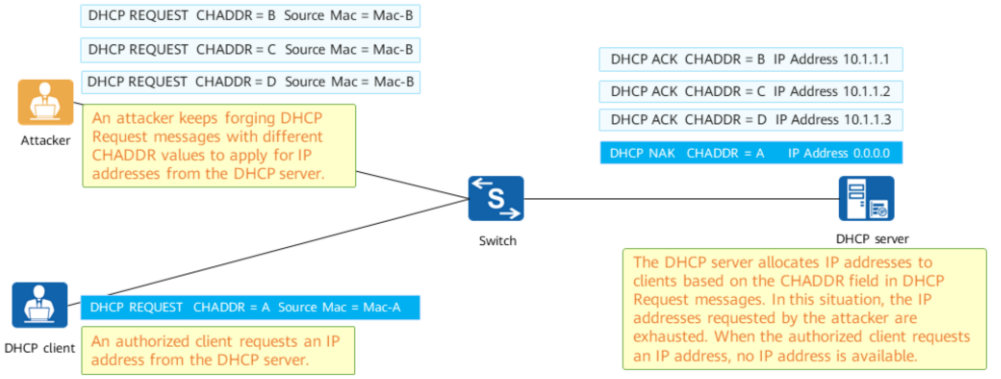
Solution: Configure MAC address limiting of DHCP snooping to prevent starvation attacks. This function limits the maximum number of MAC addresses that can be learned on an interface of a switch to prevent a large number of DHCP Request messages with variable MAC addresses from being sent.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

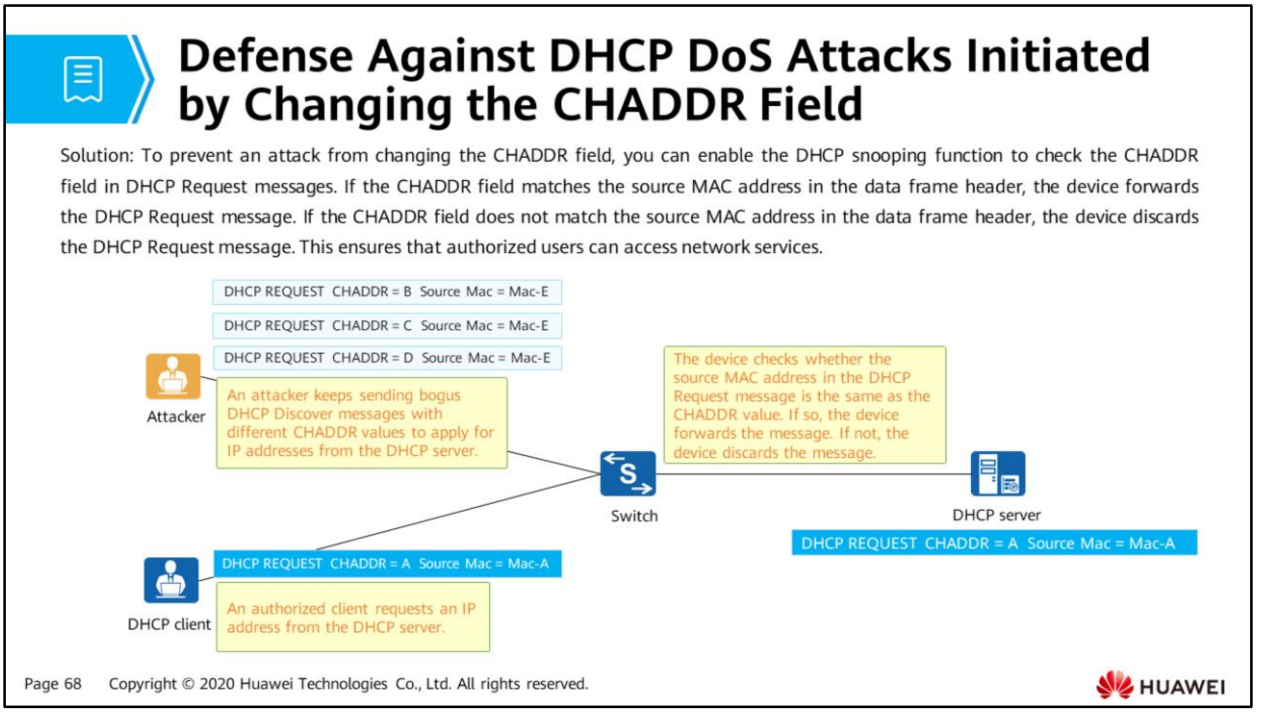
DoS Attacks by Changing the CHADDR Field

- An attacker continuously applies to the DHCP server for a large number of IP addresses until the IP addresses in the address pool of the DHCP server are exhausted. As a result, the DHCP server cannot allocate IP addresses to authorized users.
- Vulnerability analysis: When the DHCP server allocates IP addresses to clients, it cannot distinguish authorized and unauthorized users.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

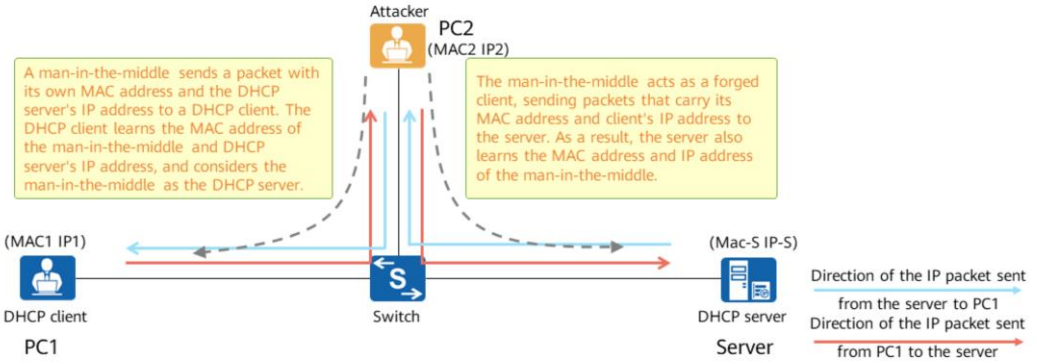
- In a DHCP starvation attack, an attacker continuously applies for a large number of IP addresses from the DHCP server to exhaust IP addresses in the address pool of the DHCP server. As a result, the DHCP server cannot allocate IP addresses to authorized users. The DHCP message contains the Client Hardware Address (CHADDR) field. This field is filled in by a DHCP client, indicating the hardware address of the client, that is, the MAC address of the client. The DHCP server assigns IP addresses based on the CHADDR field, and assigns different IP addresses if values of the CHADDR field are different. The DHCP server cannot distinguish valid CHADDR field. By exploiting this vulnerability, an attacker fills a different value in the CHADDR field of a DHCP message each time the attacker applies for an IP address. In this way, the attacker forges different users to request IP addresses.



- In a DHCP starvation attack, an attacker continuously applies for a large number of IP addresses from the DHCP server to exhaust IP addresses in the address pool of the DHCP server. As a result, the DHCP server cannot allocate IP addresses to authorized users. The DHCP message contains the Client Hardware Address (CHADDR) field. This field is filled in by a DHCP client, indicating the hardware address of the client, that is, the MAC address of the client. The DHCP server assigns IP addresses based on CHADDR values. The DHCP server cannot distinguish valid CHADDR values. By exploiting this vulnerability, an attacker fills a different value in the CHADDR field of a DHCP message each time the attacker applies for an IP address. In this way, the attacker forges different users to request IP addresses.
- To prevent starvation attacks, DHCP snooping checks whether the source MAC address of a DHCP Request message is the same as the CHADDR value on an interface. If they are the same, the interface forwards the DHCP Request message. If they are different, the interface discards the message. To check the consistency between the source MAC address and the CHADDR field on an interface, run the **dhcp snooping check dhcp-chaddr enable** command on the interface.
- An attacker may continuously change both the MAC address and CHADDR value simultaneously, and uses the same CHADDR value as the MAC address each time. In this way, the consistency check between the source MAC address and the CHADDR can be avoided.

Man-in-the-Middle Attacks

- An attacker uses the ARP mechanism to enable a client to learn the mapping between the DHCP server's IP address and attacker's MAC address, and enable the server to learn the mapping between the client's IP address and attacker's MAC address. In this way, all IP packets exchanged between the client and server traverse the attacker's device.
- Vulnerability analysis: The man-in-the-middle attack is a spoofing IP/MAC attack. This attack uses the mapping between the forged IP address and MAC address to deceive the DHCP client and server.

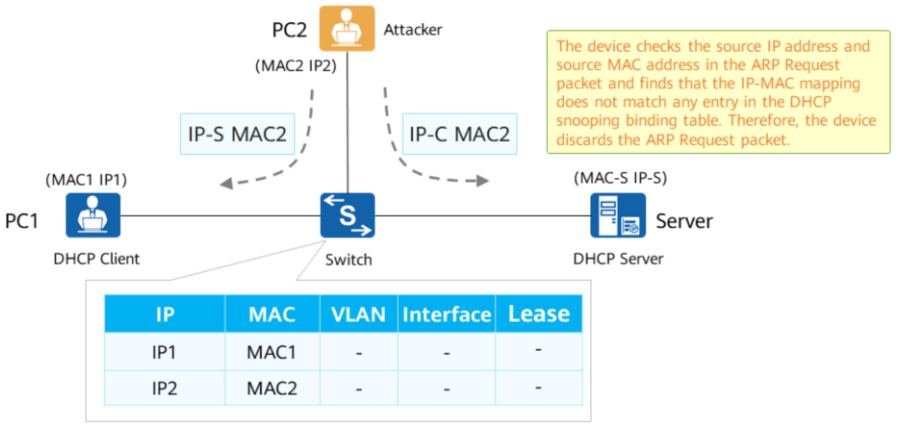


 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- As shown in the figure, the attacker uses the ARP mechanism to enable PC1 to learn the mapping between IP-S and MAC2 and enable the server to learn the mapping between IP1 and MAC2. When PC1 sends an IP packet to the DHCP server, the destination IP address is IP-S and the source IP address is IP1. The destination MAC address of the frame in which the IP packet is encapsulated is MAC2 and the source MAC address is MAC1, so the frame reaches PC2 first. After receiving the frame, the attacker changes the destination MAC address to MAC-S and the source MAC address to MAC2, and then sends the frame to the server. When the DHCP server sends an IP packet to PC1, the destination IP address is IP1 and the source IP address is IP-S. The destination MAC address of the frame in which the IP packet is encapsulated is MAC2 and the source MAC address is MAC-S, so the frame reaches PC2 first. After receiving the frame, the attacker changes the destination MAC address to MAC1 and the source MAC address to MAC2, and then sends the frame to PC1.
- The IP packets transmitted between PC1 and the DHCP server traverse the attacker's device (man-in-the-middle). Therefore, the attacker can easily obtain some information in the IP packets and use the information to perform other damage operations. The attacker can easily tamper with the DHCP messages transmitted between PC1 and the DHCP server. These messages are encapsulated in UDP packets, and UDP packets are encapsulated in IP packets. In this way, the attacker can directly attack the DHCP server.

Defense Against DHCP Man-in-the-Middle Attacks

Solution: To defend against man-in-the-middle attacks and IP/MAC spoofing attacks, configure the DHCP snooping binding table. When an interface receives an ARP or IP packet, the interface matches the source IP address and source MAC address in the ARP or IP packet against the DHCP snooping binding table. Packets that match entries are forwarded, whereas packets that do not match entries are discarded.



IP	MAC	VLAN	Interface	Lease
IP1	MAC1	-	-	-
IP2	MAC2	-	-	-

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- A DHCP man-in-the-middle attack is a spoofing IP/MAC attack. Preventing DHCP man-in-the-middle attacks is equivalent to preventing spoofing IP/MAC attacks.
- The switch running DHCP snooping listens to DHCP messages exchanged between the client and the DHCP server, and obtains the MAC address of the client from the DHCP messages. The MAC address (value of the CHADDR field in the DHCP messages, client's IP address (IP address allocated by the DHCP server to the corresponding CHADDR), and other information are stored in a database, which is also called the DHCP snooping binding table. The switch running DHCP snooping creates and dynamically maintains the DHCP snooping binding table. The binding table contains the MAC address, IP address, IP address lease, and VLAN ID of each client.
- As shown in the figure, if the DHCP server assigns IP address IP1 to PC1 and IP address IP2 to PC2, IP1 is bound to MAC1 and IP2 is bound to MAC2. These bindings are stored in the DHCP snooping binding table. To enable the server to learn the mapping between IP1 and MAC2, the attacker sends an ARP Request packet in which the source IP address is set to IP1 and the source MAC address is set to MAC2. After receiving the ARP Request packet, the switch checks the source IP address and source MAC address in the packet and finds that the IP-MAC (IP1-MAC2) mapping does not match any entry in the DHCP snooping binding table. Therefore, the switch discards the ARP Request packet, this effectively prevents spoofing IP/MAC attacks.
- To prevent IP/MAC spoofing attacks, run the **arp dhcp-snooping-detect enable** command in the system view of the switch.

DHCP Snooping Configuration Commands (1)

1. Enable DHCP snooping globally.

   [Huawei] **dhcp snooping enable** [**ipv4** | **ipv6**]

2. Enable DHCP snooping in the VLAN view.

   [Huawei-vlan2] **dhcp snooping enable**

   If you run this command in the VLAN view, the command takes effect for all DHCP messages in a specified VLAN received by all the interfaces on the device.

3. Configure an interface as the trusted interface in the VLAN view.

   [Huawei-vlan2] **dhcp snooping trusted interface** *interface-type interface-number*

   If you run this command in the VLAN view, the command takes effect only for the DHCP messages received by the interface in the VLAN that the interface belongs to.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

DHCP Snooping Configuration Commands (2)

4. Enable DHCP snooping in the interface view.

```
[Huawei-GigabitEthernet0/0/1] dhcp snooping enable
```

5. Configure an interface as the trusted interface in the interface view.

```
[Huawei-GigabitEthernet0/0/1] dhcp snooping trusted
```

By default, all interfaces are untrusted interfaces.

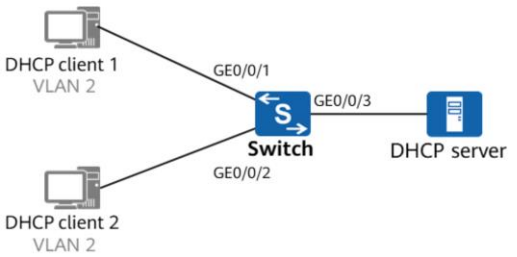
6. (Optional) Configure the device to discard DHCP Request messages with non-0 GIADDR field.

```
[Huawei] dhcp snooping check dhcp-giaddr enable vlan { vlan-id1 [ to vlan-id2 ] }
```

Enable the device to check whether the GIADDR field in a DHCP Request message is 0. This command can be run in both the VLAN view and interface view.
If you run this command in the VLAN view, the command configuration takes effect for the DHCP messages received by all interfaces on the device from the specified VLAN. If you run this command in the interface view, the command configuration takes effect for all DHCP messages on the specified interface.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Examples for Configuring DHCP Snooping



As shown in the figure, basic DHCP and VLAN configurations are complete, and DHCP snooping is configured on the switch.

Method 1: Interface view

```
[Switch] dhcp snooping enable ipv4
[Switch] interface GigabitEthernet 0/0/1
[Switch-GigabitEthernet0/0/1] dhcp snooping enable
[Switch] interface GigabitEthernet 0/0/2
[Switch-GigabitEthernet0/0/2] dhcp snooping enable
[Switch] interface GigabitEthernet 0/0/3
[Switch-GigabitEthernet0/0/3] dhcp snooping enable
[Switch-GigabitEthernet0/0/3] dhcp snooping trusted
```

Method 2: VLAN view

```
[Switch] dhcp snooping enable ipv4
[Switch] vlan 2
[Switch-vlan2] dhcp snooping enable
[Switch] interface GigabitEthernet 0/0/3
[Switch-GigabitEthernet0/0/3] dhcp snooping trusted
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Verifying the Configuration

Run the **display dhcp snooping interface** command to check DHCP snooping information on an interface.

```
[Switch]display dhcp snooping interface GigabitEthernet 0/0/3
 DHCP snooping running information for interface GigabitEthernet0/0/3 :
 DHCP snooping                    : Enable
 Trusted interface                : Yes
 Dhcp user max number               : 1024     (default)
 Current dhcp user number           : 0
 Check dhcp-giaddr                : Disable  (default)
 Check dhcp-chaddr                : Disable  (default)
 Alarm dhcp-chaddr                : Disable  (default)
 Check dhcp-request               : Disable  (default)
 Alarm dhcp-request               : Disable  (default)
----- more ------
```

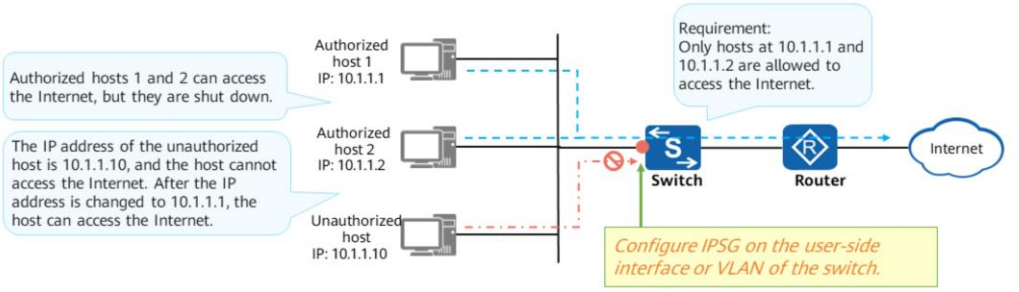

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Overview of IPSG

- Some attackers forge IP addresses of authorized users to obtain network access rights and access networks. As a result, authorized users are unable to access networks or sensitive information may be intercepted. IP source guard (IPSG) provides a mechanism to effectively defend against IP address spoofing attacks.
- IPSG is a Layer 2 interface-based source IP address filtering technology. It prevents unauthorized hosts from using IP addresses of authorized hosts or specified IP addresses to access or attack a network.



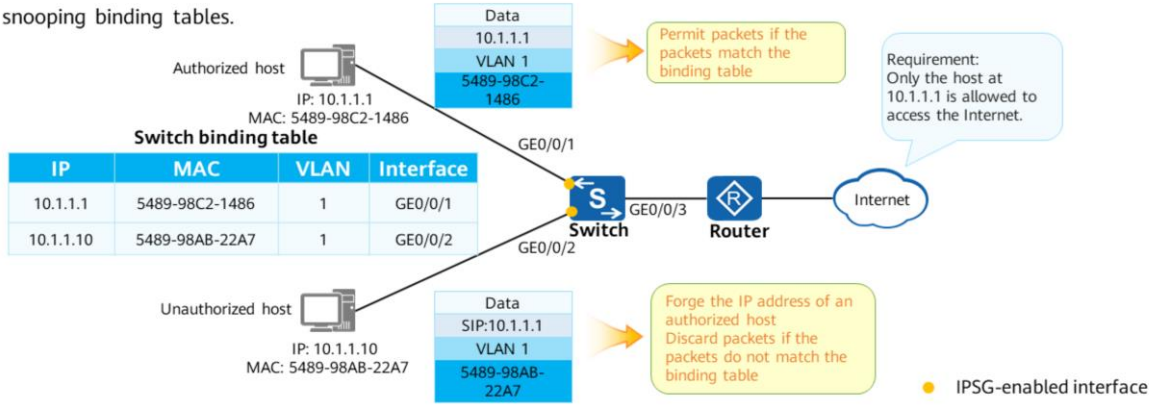
 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- If the unauthorized host forges the IP address of an authorized host to obtain network access rights, configure IPSG on the switch's user-side interface or VLAN. The switch then checks the IP packets received by the interface and discards the packets from unauthorized hosts to prevent IP address spoofing attacks.
- Generally, IPSG is configured on the interfaces or VLANs of the access device connected to users.

Working Mechanism of IPSG

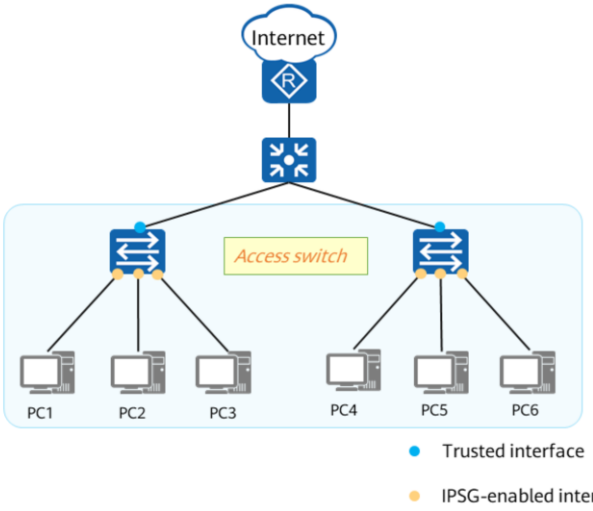
IPSG checks IP packets on Layer 2 interfaces against a binding table that contains the bindings of source IP addresses, source MAC addresses, VLAN IDs, and inbound interfaces. Only packets that match the binding table are forwarded, and packets that do not match the binding table are discarded. Binding tables include static and dynamic DHCP snooping binding tables.



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- After the binding table is generated, the IPSG-enabled device delivers ACL rules to the specified interface or VLAN according to the binding table, and then checks all IP packets against the ACL rules. The switch forwards the packets from hosts only when the packets match binding entries, and discards the packets that do not match binding entries. When the binding table is modified, the IPSG-enabled device delivers the ACL rules again.
- By default, if IPSG is enabled in the scenario where no binding table is generated, the switch rejects all IP packets except DHCP Request messages.
- A static binding entry contains the MAC address, IP address, VLAN ID, and inbound interface. IPSG checks received packets against all options in a static binding entry.
- A dynamic binding entry contains the MAC address, IP address, VLAN ID, and inbound interface. You can specify the options to be checked, and IPSG filters the packets received by interfaces according to the specified options. By default, the IPSG-enabled device checks packets against all the four options.
    - Common check items:
        - Source IP address
        - Source MAC address
        - Source IP address + Source MAC address
        - Source IP address + Source MAC address + Interface
        - Source IP address + Source MAC address + Interface + VLAN

Application of IPSG



- IPSG prevents PCs from changing their own IP addresses.
  - PCs can only use the IP addresses allocated by the DHCP server or static IP addresses configured by an administrator to access the network. If a PC changes its IP address without permission, the PC cannot access the network. This prevents PCs from obtaining network rights without permission.
- If IP addresses on a small-scale network are statically allocated, IPSG can be used to prevent unauthorized PCs from accessing the network.
  - Users cannot access the intranet with their own computers. This prevents intranet resource leaks.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

IPSG Configuration Commands

1. Configure a static binding table.

   [Huawei] **user-bind static { { { ip-address | ipv6-address } { *start-ip* [**to** *end-ip*] } &<1-10> | ipv6-prefix** *prefix/prefix-length* **} | mac-address** *mac-address* **} * [interface** *interface-type interface-number* **] [vlan** *vlan-id* **[ce-vlan** *ce-vlan-id* **]]**

   The IPSG-enabled device matches packets against the static binding table.

2. Enable IPSG.

   [Huawei-GigabitEthernet0/0/1] **ip source check user-bind enable**

   The configuration of IP packet check in the VLAN view is the same as that in the interface view.

3. Enable the alarm function of IP packet check.

   [Huawei-GigabitEthernet0/0/1] **ip source check user-bind alarm enable**

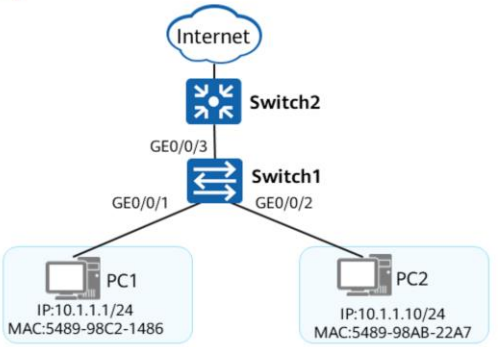
4. Set the alarm threshold for IP packet check.

   [Huawei-GigabitEthernet0/0/1] **ip source check user-bind alarm threshold** *threshold*

   After this alarm function is configured, the switch generates an alarm if the number of discarded IP packets exceeds the threshold.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Example for Configuring IPSG



- As shown in the figure, PCs are configured with static IP addresses for unified management. IPSG is configured on the access switch to prevent hosts from changing their own IP addresses to access the network.
  - Configure a static binding table.
  - Enable IPSG and configure the alarm function.

Switch1 configuration:

```
# Configure a static binding table on the access switch.
[Switch1] user-bind static ip-address 10.1.1.1 mac-address 5489-98C2-1486
[Switch1] user-bind static ip-address 10.1.1.10 mac-address 5489-98AB-22A7
# Enable IPSG and configure the alarm function of IP packet check on GE0/0/1.
[Switch1] interface GigabitEthernet 0/0/1
[Switch1-GigabitEthernet0/0/1] ip source check user-bind enable
[Switch1-GigabitEthernet0/0/1] ip source check user-bind alarm enable
[Switch1-GigabitEthernet0/0/1] ip source check user-bind alarm threshold 100
# The configuration of GE0/0/2 is similar to that of GE0/0/1.
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

Verifying the Configuration

- Run the **display dhcp static user-bind all** command on the switch to check the static binding table.
- PC1 and PC2 can access the Internet using statically configured IP addresses, and cannot access the Internet after changing their IP addresses.

```
[Switch1] display dhcp static user-bind all
DHCP static Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
IP Address                MAC Address               VSI/VLAN(O/I/P) Interface
--------------------------------------------------------------------------------
10.1.1.1                  5489-98C2-1486            --  /--  /--    --
10.1.1.10                 5489-98AB-22A7            --  /--  /--    --
--------------------------------------------------------------------------------
Print count:        2       Total count:        2
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Quiz

1. (Multiple) Which of the following attacks can DHCP snooping defend against?
   A. Starvation attacks by changing the CHADDR field
   B. Bogus DHCP server attacks
   C. TCP flag attacks
   D. Man-in-the-middle attacks and IP/MAC spoofing attacks

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

1. ABD

Summary

- Port isolation can isolate interfaces in a VLAN. Two port isolation modes are available: Layer 2 isolation and Layer 3 interworking, and Layer 2 and Layer 3 isolation.
- MAC address entries of a switch are classified into static, blackhole, and dynamic MAC address entries.
- Port security enables a switch to convert dynamic MAC addresses learned by an interface into secure MAC addresses. Secure MAC addresses are usually used together with security protection actions.
- Enabling MAC address flapping detection on a switch helps engineers quickly troubleshoot loops on the switch.
- MACsec defines a method for secure data communication based on Ethernet and ensures data transmission security through hop-by-hop data encryption between devices.
- The difference between traffic suppression and storm control is that traffic suppression only limits the rate of various packets and discards excess packets, whereas storm control takes different actions, such as shutting down an interface or blocking packets based on the packet rate.
- DHCP snooping plays an important role in preventing network attacks on terminals that automatically obtain IP addresses on the Ethernet. You can configure the DHCP snooping trusted interface and DHCP snooping binding table to prevent DHCP-based network attacks.
- The IPSG-enabled switch checks packets against the binding table to prevent IP address spoofing attacks and prevent unauthorized users from using forged IP addresses of authorized users to attack a network.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.


Thank You
www.huawei.com