Contents

1 Configuring MAC Address

1.1 Introduction

A Media Access Control (MAC) address is used to identify the position of a device in a network. Generally, a MAC address consists of 12 hexadecimals and contains a total of 48 bits (six bytes). The first 24 bits are applied for by vendors from The Internet Engineering Task Force (IETF) and used to identify a network device manufacturer. The last 24 bits are assigned by the vendors and used to identify network cards produced by the manufacturers.

1.1.1 MAC Address Table

A MAC address table records mappings of MAC addresses and interfaces to virtual local area networks (VLANs). A device queries the MAC address table based on the destination MAC address in a received packet. If the device finds an entry that is consistent with the destination MAC Address in the packet, the device forwards the packet through the interface corresponding to the entry in unicast mode. If the device does not find such an entry, it forwards the packet through all interfaces other than the receiving interface in broadcast mode.

Note

This section describes static, dynamic, and filtering MAC address entries. For more information about multicast MAC address entries and specific configurations, see "IGMP" in *Multicast Configuration Guide*.

1.1.2 Classification of MAC Address Entries

MAC address entries are classified into the following types:

- Static MAC address entries: Manually configured by the administrator. Packets whose destination MAC address matches the one in such an entry are forwarded through the correct interface. This type of entries does not age.
- Dynamic MAC address entries: Automatically generated by devices. Packets whose destination MAC address matches the one in such an entry are forwarded through the correct interface. This type of entries ages.
- Filtering MAC address entries: Manually configured by the administrator. Packets whose source or destination MAC address matches the one in such an entry are discarded. This type of entries does not age.

The priorities of these types of MAC address entries are ranked in descending order as follows: Filtering MAC address entries > Static MAC address entries > Dynamic MAC address entries. If two entries have the same MAC address and VLAN, the higher-priority entry can overwrite the lower-priority one, and entries with the same priority can overwrite each other.

1.1.3 Generation of MAC Address Entries

A MAC address entry can be automatically learned or manually configured.

1. Automatic learning

A device automatically generates a MAC address entry based on the source MAC address in a received packet. The learning procedure is as follows:

(1) Initially, the MAC address table of Device A is empty. To send a packet to User C, User A sends the packet to the interface GigabitEthernet 0/1 of Device A. Upon receiving the packet, Device A generates a MAC address entry, with the MAC address being MAC A and the interface being GigabitEthernet 0/1.

(2) As Device A does not have an entry corresponding to MAC A, it forwards the packet through all interfaces other than GigabitEthernet 0/1 in broadcast mode. In this case, other users also receive the packet that User A sends to User C.

(3) User C sends a reply packet destined for User A to Device A through the interface GigabitEthernet 0/3. Upon receiving the packet, Device A generates a MAC address entry, with the MAC address being MAC C and the interface being GigabitEthernet 0/3. Meanwhile, Device A finds an entry corresponding to MAC A and then forwards the packet to User A through GigabitEthernet 0/1 in unicast mode.

(4) After the communication between User A and User C is complete, Device A learns two MAC address entries. Later, packets are forwarded between User A and User C in unicast mode and other users do not receive packets destined for these two users.

Figure 1-1 Automatically Learning MAC Address Entry I

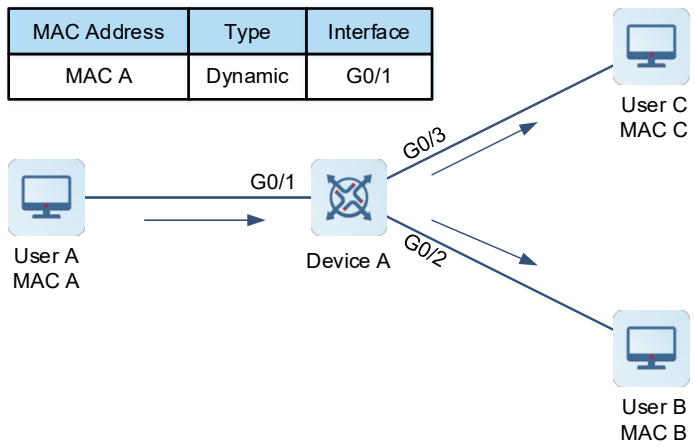
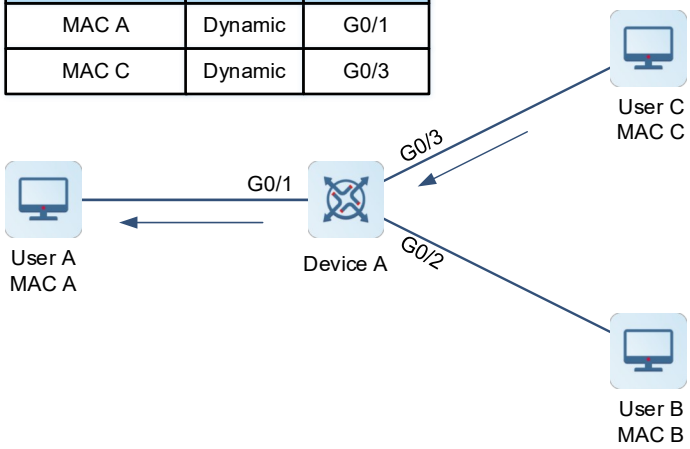


Figure 1-2 Automatically Learning MAC Address Entry II

MAC Address	Type	Interface
MAC A	Dynamic	G0/1
MAC C	Dynamic	G0/3



2. Manual configuration

If the device forwards packets based on automatically generated MAC address entries, security risks exist. For example, if an attacker forges a packet by using a MAC address of a valid user and sends the packet to another interface of the device, the device automatically updates the corresponding MAC address entry and sends subsequent packets destined for the user to the attacker. To improve network security, the network administrator can add a specified MAC address entry to bind the MAC address of the valid user to a device interface. The static MAC address entry configured in this way is not updated due to packet forwarding. If a packet whose source MAC address is the MAC address of the valid user is received from another user, the device directly discards this packet.

1.1.4 Update and Aging of MAC Address Entries

Static and filtering MAC address entries do not automatically update or age. Dynamic MAC address entries are updated and age in the following scenarios:

(1) When the device learns a new dynamic MAC address entry, the device sets the age flag bit of this entry to 1.

(2) If the source MAC address in a received packet already exists in the MAC address table, the device updates the entry and sets the age flag bit to 1.

(3) The device checks the age flag bit of a dynamic MAC address entry at the interval of the aging time. For entries whose flag bit is 1, the device sets the flag bit to 0. For entries whose flag bit is 0, the device deletes the entries.

Therefore, the actual aging time of a dynamic MAC address entry ranges between the specified age value and two times the age value.

1.1.5 Protocols and Standards

- IEEE 802.3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications
- IEEE 802.1Q: Virtual Bridged Local Area Networks

1.2 Restrictions and Guidelines

If an L2 interface has subinterfaces, running the **default interface** command in global configuration mode does not affect configurations related to the MAC address learning function, the upper limit of learned MAC addresses, the forwarding rule to be used after the upper limit of learned MAC addresses is reached, and the MAC address flapping protection policy.

1.3 Configuration Task Summary

All the following configuration tasks are optional and may be selected as needed.

- Configuring Static MAC Address Entries
- Configuring Filtering MAC Address Entries
- Disabling Dynamic MAC Address Learning
  - Disabling MAC Address Learning in Global Configuration Mode
  - Disabling MAC Address Learning for an Interface
- Configuring Upper Limit of Learned MAC Addresses
  - Configuring Upper Limit of MAC Addresses Learned from a VLAN
  - Configuring Upper Limit of MAC Addresses Learned from an Interface
- Configuring Aging Time of Dynamic MAC Address Entries
- Enabling MAC Address Flapping Detection and Protection
- Configuring Reporting Interval of MAC Address Table Usage Alarms and MAC Address Table Usage Threshold
- Configuring the Function of MAC Address Entry Change Notification

1.4 Configuring Static MAC Address Entries

1.4.1 Overview

You can manually configure static MAC address entries to bind MAC addresses to device interfaces.

1.4.2 Restrictions and Guidelines

- Interfaces in the MAC address entries can be specified as L2 Ethernet interfaces or L2 aggregation ports (APs).
- If a MAC address is bound to different interfaces in the same VLAN, the last configuration prevails.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a static MAC address.

mac-address-table static *mac-address* **vlan** *vlan-id* **interface** *interface-type interface-number*

No static MAC address entry exists by default.

1.5 Configuring Filtering MAC Address Entries

1.5.1 Overview

To prohibit a user from sending and receiving packets in certain scenarios, you can add the MAC address of the user to a filtering MAC address entry. After the entry is configured, packets whose source or destination MAC address matches the MAC address in the filtering MAC address entry are directly discarded.

1.5.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a filtering MAC address.

mac-address-table filtering *mac-address* **vlan** *vlan-id*

No filtering MAC address entry exists by default.

1.6 Disabling Dynamic MAC Address Learning

1.6.1 Overview

MAC address learning is enabled by default. A device automatically generates a dynamic MAC address entry based on the source MAC address in a received packet. The device queries the MAC address table to perform unicast forwarding, which reduces broadcast frequency and therefore reduces the network traffic. The device learns or updates the MAC address entry each time it receives a packet, which results in low security. An attacker may forge and send a large number of packets with different source MAC addresses to the device to use up the MAC address entry resources. Consequently, the device cannot update the MAC address entries in time. You can disable dynamic MAC address learning if required.

1.6.2 Disabling MAC Address Learning in Global Configuration Mode

1. Overview

If you disable MAC address learning in global configuration mode, the device does not learn MAC addresses.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Disable MAC address learning in global configuration mode.

mac-address-learning disable

MAC address learning is enabled in global configuration mode by default.

1.6.3 Disabling MAC Address Learning for an Interface

1. Overview

If MAC address learning is enabled in global configuration mode, you can disable this function for a specific interface.

2. Restrictions and Guidelines

- If 802.1X, IP Source Guard, or the port security function is configured on an interface, MAC address learning must be disabled for this interface. For more information about 802.1X, IP Source Guard, or the port security function, see sections "802.1X", "IP Source Guard", or "Port Security" in *Security Configuration Guide*.
- This function can be enabled on L2 Ethernet interfaces and L2 APs only.

3. Procedure

(1) Enter the privileged EXEC mode.
enable

(1) Enter the global configuration mode.

configure terminal

(2) Enter the interface configuration mode.

interface *interface-type interface-number*

(3) Disable MAC address learning for an interface.

no mac-address-learning

No MAC address learning is enabled for an interface by default.

1.7 Configuring Upper Limit of Learned MAC Addresses

1.7.1 Overview

The number of MAC address entries on the device is limited. Packets can be forwarded only in broadcast mode in order to prevent the device from learning a large number of dynamic MAC address entries from an interface or a VLAN (for example, when it is attacked by packets with different source addresses) and prevent MAC address learning failures on other interfaces and VLANs. In this case, you can configure the upper limit of MAC addresses learned from each interface or VLAN based on actual network plans. When the number of MAC addresses reaches the upper limit, the device stops learning MAC addresses from the corresponding interface or VLAN. You can also configure a forwarding rule to be used after the number of learned MAC addresses reaches the upper limit, to determine whether to forward packets whose source MAC address is not in the MAC address table. With this function, you can save MAC address entry resources and enhance network security.

This function is available only to dynamic MAC address entries.

1.7.2 Configuring Upper Limit of MAC Addresses Learned from a VLAN

1. Overview

You can configure the upper limit of MAC addresses learned from a VLAN and the packet forwarding rule to be used after the number of learned MAC addresses reaches the upper limit.

2. Restrictions and Guidelines

- If the number of MAC addresses learned from a VLAN is greater than the upper limit, the device stops learning MAC addresses from the VLAN, and starts learning again only after the number drops below the upper limit as aged address entries are deleted.
- This function does not limit replication of MAC address entries to a VLAN whose number of learned MAC address entries reaches the upper limit.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a VLAN and enter the VLAN configuration mode.

vlan *vlan-id*

(4) Configure the upper limit of dynamic MAC addresses learned from a VLAN.

max-dynamic-mac-count *count*

No upper limit of learned MAC addresses is configured for a VLAN by default.

(5) (Optional) Configure a forwarding rule to be used after the number of dynamic MAC addresses learned from a VLAN reaches the upper limit.

max-dynamic-mac-count exceed-action { **forward** | **discard** }

By default, after the number of MAC addresses learned from a VLAN reaches the upper limit, the device continues forwarding packets whose source MAC address is not learned.

1.7.3 Configuring Upper Limit of MAC Addresses Learned from an Interface

1. Overview

You can configure the upper limit of MAC addresses learned from an interface and the packet forwarding rule to be used after the number of learned MAC addresses reaches the upper limit.

2. Restrictions and Guidelines

If the number of MAC addresses learned from an interface is greater than the upper limit, the device stops learning MAC addresses from the interface, and starts learning again only after the number drops below the upper limit as aged MAC address entries are deleted.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the upper limit of dynamic MAC addresses learned from an interface.

max-dynamic-mac-count *count*

No upper limit of learned MAC addresses is configured for an interface by default.

(5) (Optional) Configure a forwarding rule to be used after the number of dynamic MAC addresses learned from an interface reaches the upper limit.

max-dynamic-mac-count exceed-action { **forward** | **discard** }

By default, after the number of MAC addresses learned from an interface reaches the upper limit, the device continues forwarding packets whose source MAC address is not learned.

1.8 Configuring Aging Time of Dynamic MAC Address Entries

1. Overview

The device deletes useless dynamic MAC address entries based on the aging time to save entry resources on the device. An overly long aging time may lead to untimely deletion of useless entries, whereas an overly short aging time may lead to deletion of some valid entries and repeated learning of MAC addresses by the device, which increases the packet broadcast frequency. Therefore, you are advised to configure a proper aging time of dynamic MAC address entries as required to save device resources without affecting network stability.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the aging time of dynamic MAC addresses.

mac-address-table aging-time *time*

The aging time of dynamic MAC addresses is 300s by default.

1.9 Enabling MAC Address Flapping Detection and Protection

1.9.1 Overview

If a MAC address is learned from different interfaces in the same VLAN, MAC address flapping occurs. If MAC address flapping occurs frequently between two specific interfaces, a network loop is formed. In this case, packets with the same source MAC address are received from different interfaces, and the MAC address entry is updated frequently. By enabling MAC address flapping detection, you can effectively monitor MAC address flapping events on the L2 network. Each time a MAC address flapping event occurs, the device reports a log alarm message. You can configure the MAC address flapping protection policy on the interfaces. When the

device detects that MAC address flapping occurs between two interfaces with different priorities, the device reports an alarm message and disables the lower-priority interface.

1.9.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure MAC address flapping detection.

mac-address-table flapping-logging

MAC address flapping detection is disabled by default.

(4) Enter the interface configuration mode.

interface *interface-type interface-number*

(5) (Optional) Configure a MAC address flapping protection policy.

mac-address-table flapping action { **error-down** | **priority** *priority* }

No MAC address flapping protection policy is configured by default.

The MAC address flapping protection policy is available only for an interface with MAC address flapping detection enabled.

1.10 Configuring Reporting Interval of MAC Address Table Usage Alarms and MAC Address Table Usage Threshold

1.10.1 Overview

When the usage of a MAC address table of a device exceeds the upper or lower limit, the device reports an alarm message. With this function, you can adjust the reporting interval of MAC address table usage alarms and MAC address table usage threshold (in percentage).

When the usage of a MAC address table is higher than the upper limit, the device reports an alarm message at the specified interval. After the usage drops below the upper limit, the device reports a restoration message and stops reporting the alarm message. When the usage of a MAC address table is lower than the lower limit, the device reports an alarm message at the specified interval. After the usage rises above the lower limit, the device reports a restoration message and stops reporting the alarm message.

1.10.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a reporting interval of the MAC address table usage alarms.

mac-address-table warning-interval *interval*

The reporting interval of the MAC address table usage alarms is 3600s by default.

If you set the interval to 0s, MAC address table usage alarm reporting is disabled.

(4) Configure the upper and lower limits of the MAC address table usage.

mac-address-table warning-threshold upper-limit *upper-limit-threshold* **lower-limit** *lower-limit-threshold*

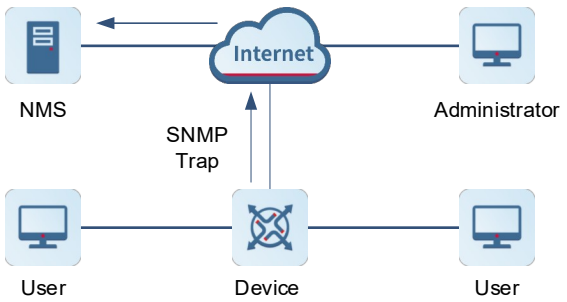
By default, the upper and lower limits for reporting MAC address table usage alarms are 80% and 70%, respectively.

1.11 Configuring the Function of MAC Address Entry Change Notification

1.11.1 Overview

After the function of MAC address entry change notification is configured on a device, the device generates a notification message for a MAC address entry change when the device learns a new MAC address or has aged a learned MAC address. In addition, the device sends the notification message in SNMP Trap mode to a specified Network Management Station (NMS). This function helps the network administrator monitor user change of network devices.

Figure 1-1 Application Scenario of the Function of MAC Address Entry Change Notification



As shown in Figure 1-1, when the device generates a notification for an added MAC address, a new user identified by the MAC address starts to use the network. When the device generates a notification for a deleted MAC address, the corresponding user does not send packets in the address aging time. In this case, it is considered that the user stops using the network. When the device is accessed by a large number of users, the device may generate a large number of MAC address entry change notifications in a short time, and the traffic increases.

To reduce traffic, you can configure an interval for sending MAC address entry change notifications. When the configured interval arrives, the system sends all notifications in a period of time at a time. This helps reduce the network traffic. Each notification message contains information about several MAC address changes.

A generated notification is stored in a history table for MAC address entry change notifications. The administrator may know recent MAC address changes by checking the history table even without NMS.

1.11.2 Restrictions and Guidelines

A MAC address entry change notification is generated only for a dynamic MAC address entry.

1.11.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an NMS host address for receiving MAC address entry change notifications.

snmp-server host { *ipv4-address* | **ipv6** *ipv6-address* } **traps** [**version** { **1** | **2c** | **3** [**auth** | **noauth** | **priv**] }] *community-string*

No NMS host address is configured for receiving MAC address entry change notifications by default.

(4) Enable sending of MAC address entry change notifications in Trap messages.

snmp-server enable traps

Sending Trap messages to the NMS host is forbidden by default.

(5) Enable the function of MAC address entry change notification in global configuration mode.

mac-address-table notification

The function of MAC address entry change notification is disabled in global configuration mode by default.

(6) (Optional) Configure an interval for sending MAC address entry change notifications.

mac-address-table notification interval *interval*

The device sends MAC address entry change notifications at an interval of 1s by default.

(7) (Optional) Configure the size of a history table for MAC address entry change notifications.

mac-address-table notification history-size *size*

The size of the history table for MAC address entry change notifications is 50 by default.

(8) Enter the interface configuration mode.

interface *interface-type interface-number*

(9) Enable the function of MAC address entry change notification for an interface.

snmp trap mac-notification { **added** | **removed** }

The function of MAC address entry change notification is disabled for an interface by default.

1.12 Monitoring

This section describes the **show** commands used for checking the running status of a configured function to verify the configuration effect.

You can run the **clear** commands to clear information.

⚠ Caution

Running the **clear** commands may lose vital information and thus interrupt services.

Table 1-1 Monitoring

Command	Purpose
clear mac-address-table dynamic [**address** *mac-address*] [**interface** *interface-type interface-number*] [**vlan** *vlan-id*]	Clears the dynamic MAC address entries.
clear mac-address-table flapping record	Clears the MAC address flapping records.
show mac-address-table { **dynamic** | **static** | **filter** } [**address** *mac-address*] [**vlan** *vlan-id*] [**interface** *interface-id*]	Displays the MAC address table.
show mac-address-table { **evpn** | **mlag** }	Displays the EVPN or MLAG address table.
show mac-address-table address *mac-address* [**vsi** *vsi-id*] [**vni** *vni-id*]	Displays the specific EVPN or MAC address table.
show mac-address-table [**vsi** *vsi-id*] [**vni** *vni-id*]	Displays the specific VNI or VSI address table.
show mac-address-table all	Displays all types of addresses.
show mac-address-table aging-time	Displays the aging time for dynamic MAC addresses.
show mac-address-table max-dynamic-mac-count	Displays the maximum number of dynamic MAC addresses.
show mac-address-table notification [**interface** [*interface-type interface-number*] **| history**]	Displays the configurations and history table for MAC address entry change notifications.
show mac-address-table flapping record	Displays the dynamic MAC address flapping records.

1.13 Configuration Examples

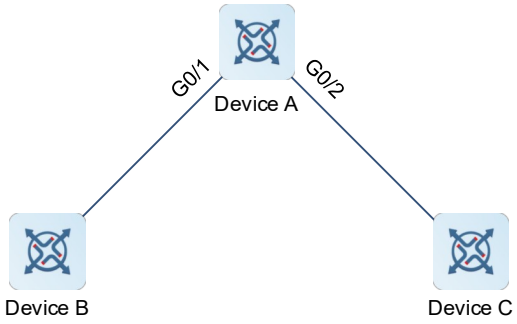
1.13.1 Configuring MAC Address Flapping Detection

1. Requirements

As shown in Figure 1-1, an L2 loop may occur between Device B and Device C due to misoperation. After you enable MAC address flapping detection and configure a protection policy, the device can report alarms upon loops, and disable the faulty interface based on the protection policy.

2. Topology

Figure 1-1 MAC Address Flapping Detection



3. Notes

- Enable MAC address flapping detection on Device A.
- Configure a MAC address flapping protection policy on the interfaces of Device A.
- Set the priority of GigabitEthernet 0/1 to be higher than that of GigabitEthernet 0/2 on Device A.

4. Procedure

Enable MAC address flapping detection.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# mac-address-table flapping-logging
```

Configure a protection policy to disable GigabitEthernet 0/1 upon MAC address flapping and set the priority of this interface to **5**.

```
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config)# (config-if-GigabitEthernet 0/1)# mac-address-table flapping
action error-down
DeviceA(config)# (config-if-GigabitEthernet 0/1)# mac-address-table flapping
action priority 5
DeviceA(config)# (config-if-GigabitEthernet 0/1)# exit
```

Configure a protection policy to disable GigabitEthernet 0/2 upon MAC address flapping and set the priority of this interface to **1**.

```
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config)# (config-if-GigabitEthernet 0/2)# mac-address-table flapping
action error-down
DeviceA(config)# (config-if-GigabitEthernet 0/2)# mac-address-table flapping
action priority 1
```

5. Verification

After the preceding configuration, the device generates an alarm message when MAC address flapping from GigabitEthernet 0/1 to GigabitEthernet 0/2 occurs. Run the **show mac-address-table flapping record** command to display the dynamic MAC address flapping records.

View the records on Device A after MAC address flapping is detected.

```
DeviceA# show mac-address-table flapping record
 Mac address flapping detect status       : on
 Mac address flapping detect interval     : 1s
 Mac address flapping syslog supress time : 1800s
 Mac address flapping record max count    : 300
 Mac address flapping record total count  : 2

 Move-Time           VLAN  MAC-Address    Original-Port   Move-Ports   Status
 ------------------- ----- -------------- --------------- ------------ --------
 2020.11.14 12:10:46 1     0001.1111.1111 ge0/1           ge0/2        Normal
 2020.11.14 12:10:58 1     0001.1111.1111 ge0/2           ge0/1        ERR-DOWN
```

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
mac-address-table flapping-logging
!
!
interface gigabitEthernet 0/1
mac-address-table flapping action error-down
mac-address-table flapping action priority 5
!
!
interface gigabitEthernet 0/2
mac-address-table flapping action error-down
mac-address-table flapping action priority 1
!
```

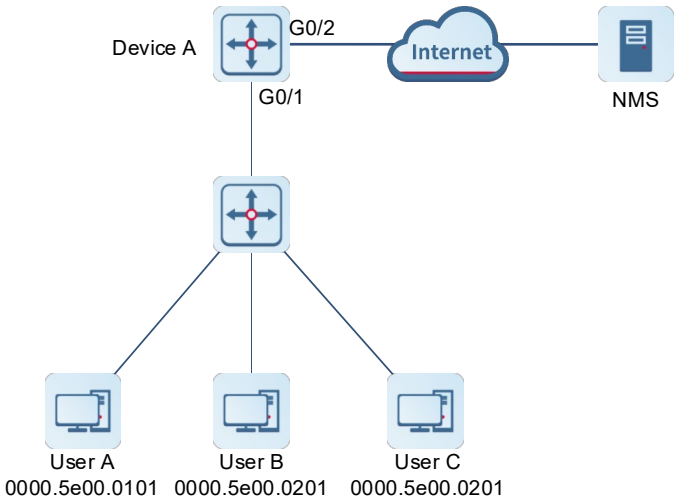
1.13.2 Configuring the Function of MAC Address Change Notification

1. Requirements

As shown in Figure 1-1, Device A is connected to devices of User A, User B, and User C, so that Device A records new MAC address entries learned from GigabitEthernet 0/1 and aged MAC address entries, sends MAC address entry change notifications to the specified NMS in SNMP Trap messages, and does not generate massive MAC address change information in a short time to prevent overusing network resources.

2. Topology

Figure 1-1 Function of MAC Address Entry Change Notification



3. Notes

- Enable the function of MAC address entry change notification in global configuration mode on Device A and configure an interval for sending MAC address Trap messages.
- Enable the function of MAC address entry change notification on GigabitEthernet 0/1 of Device A.
- Specify an SNMP host address and enable Trap notification of MAC address events.
- Ensure that the route between Device A and the NMS is reachable.

4. Procedure

Enable the function of MAC address entry change notification in global configuration mode on Device A and set the interval for sending MAC address Trap messages to 300s.

```
DeviceA# configure terminal
DeviceA(config)# mac-address-table notification
DeviceA(config)# mac-address-table notification interval 300
```

Enable the function of MAC address entry change notification on GigabitEthernet 0/1 and enable the function of sending Trap messages upon MAC address addition or deletion.

```
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/2)# snmp trap mac-notification added
DeviceA(config-if-GigabitEthernet 0/2)# snmp trap mac-notification removed
```

Set the SNMP host address to 192.168.1.1, SNMP version to SNMP v1 and community string to **123** to actively send MAC address Trap messages.

```
DeviceA(config-if-GigabitEthernet 0/2)# exit
DeviceA(config)# snmp-server host 192.168.1.10 traps version 2c 123 mac-
notification
```

Enable Trap notification of MAC address events.

```
DeviceA(config)# snmp-server enable traps
```

5. Verification

After the preceding configuration, run the **show mac-address-table notification** command to display the configuration status of the function of MAC address entry change notification in global configuration mode. Run the **show mac-address-table notification history** command to display the history table for MAC address entry change notifications.

Display the configuration status of the function of MAC address entry change notification in global configuration mode.

```
DeviceA# show mac-address-table notification
MAC Notification Feature : Enabled
Interval(Sec): 300
Maximum History Size : 50
Current History Size : 0
```

Display the history table for MAC address entry change notifications after the MAC address changes.

```
DeviceA# show mac-address-table notification history
History Index : 0
Entry Timestamp: 221683
MAC Changed Message :
Operation:ADD Vlan:1 MAC Addr: 0000.5e00.0201 GigabitEthernet 0/1
```

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
mac-address-table notification
mac-address-table notification interval 300
!
!
interface GigabitEthernet 0/1
 snmp trap mac-notification added
 snmp trap mac-notification removed
!
!
snmp-server host 192.168.1.10 traps version 2c 7 $10$135$2c+O$ mac-notification
snmp-server enable traps
!
```