

Contents

Configuring the MAC address table	1
About the MAC address table	1
How a MAC address entry is created.....	1
Types of MAC address entries.....	1
MAC address table tasks at a glance.....	2
Configuring MAC address entries	2
About MAC address entry-based frame forwarding	2
Restrictions and guidelines for MAC address entry configuration.....	3
Prerequisites for MAC address entry configuration.....	3
Adding or modifying a static or dynamic MAC address entry.....	3
Adding or modifying a blackhole MAC address entry	4
Adding or modifying a multiport unicast MAC address entry	4
Setting the aging timer for dynamic MAC address entries	5
Enabling MAC address learning at the ingress.....	6
Disabling MAC address learning.....	6
About disabling MAC address learning	6
Disabling global MAC address learning	6
Disabling MAC address learning on an interface	6
Configuring MAC address move notifications and suppression.....	7
Enabling ARP fast update for MAC address moves	8
Configuring the base MAC address	9
Enabling SNMP notifications for the MAC address table	9
Display and maintenance commands for MAC address table	10
MAC address table configuration examples.....	10
Example: Configuring the MAC address table	10
Configuring MAC Information.....	12
About MAC Information.....	12
Enabling MAC Information	12
Configuring the MAC Information mode.....	12
Setting the MAC change notification interval	13
Setting the MAC Information queue length	13
MAC Information configuration examples	14
Example: Configuring MAC Information.....	14

Configuring the MAC address table

About the MAC address table

An Ethernet device uses a MAC address table to forward frames. A MAC address entry includes a destination MAC address, an outgoing interface, and a VLAN ID. When the device receives a frame, it uses the destination MAC address of the frame to look for a match in the MAC address table.

- The device forwards the frame out of the outgoing interface in the matching entry if a match is found.
- The device floods the frame in the VLAN of the frame if no match is found.

How a MAC address entry is created

The entries in the MAC address table include entries automatically learned by the device and entries manually added.

MAC address learning

The device can automatically populate its MAC address table by learning the source MAC addresses of incoming frames on each interface.

The device performs the following operations to learn the source MAC address of incoming packets:

1. Checks the source MAC address (for example, MAC-SOURCE) of the frame.
2. Looks up the source MAC address in the MAC address table.
 - The device updates the entry if an entry is found.
 - The device adds an entry for MAC-SOURCE and the incoming port if no entry is found.

When the device receives a frame destined for MAC-SOURCE after learning this source MAC address, the device performs the following operations:

1. Finds the MAC-SOURCE entry in the MAC address table.
2. Forwards the frame out of the port in the entry.

The device performs the learning process for each incoming frame with an unknown source MAC address until the table is fully populated.

Manually configuring MAC address entries

Dynamic MAC address learning does not distinguish between illegitimate and legitimate frames, which can invite security hazards. When Host A is connected to Port A, a MAC address entry will be learned for the MAC address of Host A (for example, MAC A). When an illegal user sends frames with MAC A as the source MAC address to Port B, the device performs the following operations:

1. Learns a new MAC address entry with Port B as the outgoing interface and overwrites the old entry for MAC A.
2. Forwards frames destined for MAC A out of Port B to the illegal user.

As a result, the illegal user obtains the data of Host A. To improve the security for Host A, manually configure a static entry to bind Host A to Port A. Then, the frames destined for Host A are always sent out of Port A. Other hosts using the forged MAC address of Host A cannot obtain the frames destined for Host A.

Types of MAC address entries

A MAC address table can contain the following types of entries:

- **Static entries**—A static entry is manually added to forward frames with a specific destination MAC address out of the associated interface, and it never ages out. A static entry has higher priority than a dynamically learned one.
- **Dynamic entries**—A dynamic entry can be manually configured or dynamically learned to forward frames with a specific destination MAC address out of the associated interface. A dynamic entry might age out. A manually configured dynamic entry has the same priority as a dynamically learned one.
- **Blackhole entries**—A blackhole entry is manually configured and never ages out. A blackhole entry is configured for filtering out frames with a specific source or destination MAC address. For example, to block all frames destined for or sourced from a user, you can configure the MAC address of the user as a blackhole MAC address entry. A blackhole entry has higher priority than a dynamically learned one.
- **Multipoint unicast entries**—A multipoint unicast entry is manually added to send frames with a specific unicast destination MAC address out of multiple ports, and it never ages out. A multipoint unicast entry has higher priority than a dynamically learned one.

A static, blackhole, or multipoint unicast MAC address entry can overwrite a dynamic MAC address entry, but not vice versa. A static entry, a blackhole entry, and a multipoint unicast entry cannot overwrite one another.

This document does not cover the configuration of static multicast MAC address entries. For more information about configuring static multicast MAC address entries, see IGMP snooping in *IP Multicast Configuration Guide*.

MAC address table tasks at a glance

All MAC address table configuration tasks are optional..

To configure the MAC address table, perform the following tasks:

- [Configuring MAC address entries](#)
 - [Adding or modifying a static or dynamic MAC address entry](#)
 - [Adding or modifying a blackhole MAC address entry](#)
 - [Adding or modifying a multipoint unicast MAC address entry](#)
- [Setting the aging timer for dynamic MAC address entries](#)
- [Configuring MAC address learning](#)
 - [Enabling MAC address learning at the ingress](#)
 - [Disabling MAC address learning](#)
- [Configuring MAC address move notifications and suppression](#)
- [Enabling ARP fast update for MAC address moves](#)
- [Configuring the base MAC address](#)
- [Enabling SNMP notifications for the MAC address table](#)

Configuring MAC address entries

About MAC address entry-based frame forwarding

A frame whose source MAC address matches different types of MAC address entries is processed differently.

Type	Description
Static MAC address entry	Forwards the frame according to the destination MAC address regardless of whether the frame's ingress interface is the same as that in the entry.
Multipoint unicast MAC address entry	<ul style="list-style-type: none"> Learns the MAC address of the frame and generates a dynamic MAC address entry, but the generated dynamic MAC address entry does not take effect. Forwards the frame based on the multipoint unicast MAC address entry.
Blackhole MAC address entry	Drops the frame.
Dynamic MAC address entry	<ul style="list-style-type: none"> Learns the MAC address of the frames received on a different interface from that in the entry and overwrites the original entry. Forwards the frame received on the same interface as that in the entry and updates the aging timer for the entry.

Restrictions and guidelines for MAC address entry configuration

A manually configured dynamic MAC address entry will overwrite a learned entry that already exists with a different outgoing interface for the MAC address.

The manually configured static, blackhole, and multipoint unicast MAC address entries cannot survive a reboot if you do not save the configuration. The manually configured dynamic MAC address entries are lost upon reboot whether or not you save the configuration.

Prerequisites for MAC address entry configuration

Before manually configuring a MAC address entry for an interface, make sure the VLAN in the entry has been created.

Adding or modifying a static or dynamic MAC address entry

Adding or modifying a static or dynamic MAC address entry globally

1. Enter system view.
system-view
2. Add or modify a static or dynamic MAC address entry.
mac-address { dynamic | static } mac-address interface interface-type interface-number vlan vlan-id

By default, no MAC address entry is configured globally.

Make sure you have assigned the interface to the VLAN.

Adding or modifying a static or dynamic MAC address entry on an interface

1. Enter system view.
system-view
2. Enter interface view.
 - o Enter Layer 2 Ethernet interface view.
interface interface-type interface-number
 - o Enter Layer 2 aggregate interface view.
interface bridge-aggregation interface-number

3. Add or modify a static or dynamic MAC address entry.

```
mac-address { dynamic | static } mac-address vlan vlan-id
```

By default, no MAC address entry is configured on an interface.

Make sure you have assigned the interface to the VLAN.

Adding or modifying a blackhole MAC address entry

1. Enter system view.

```
system-view
```

2. Add or modify a blackhole MAC address entry.

```
mac-address blackhole mac-address vlan vlan-id
```

By default, no blackhole MAC address entry is configured.

Adding or modifying a multiport unicast MAC address entry

About multiport unicast MAC address entry configuration

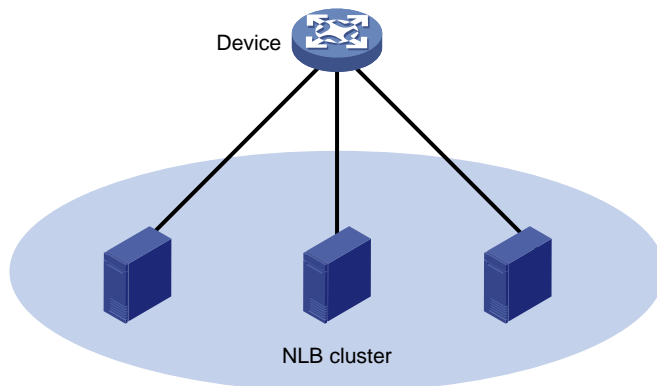
You can configure a multiport unicast MAC address entry to associate a unicast destination MAC address with multiple ports. The frame with a destination MAC address matching the entry is sent out of multiple ports.

For example, in NLB unicast mode (see [Figure 1](#)):

- All servers within a cluster use the cluster's MAC address as their own address.
- Frames destined for the cluster are forwarded to every server in the group.

In this case, you can configure a multiport unicast MAC address entry on the device connected to the server group. Then, the device forwards the frame destined for the server group to every server through all ports connected to the servers within the cluster.

Figure 1 NLB cluster



You can configure a multiport unicast MAC address entry globally or on an interface.

Configuring a multiport unicast MAC address entry globally

1. Enter system view.

```
system-view
```

2. Add or modify a multiport unicast MAC address entry.

```
mac-address multiport mac-address interface interface-list vlan vlan-id
```

By default, no multiport unicast MAC address entry is configured globally.

Make sure you have assigned the interface to the VLAN.

Configuring a multiport unicast MAC address entry on an interface

1. Enter system view.

```
system-view
```

2. Enter interface view.

- o Enter Layer 2 Ethernet interface view.

```
interface interface-type interface-number
```

- o Enter Layer 2 aggregate interface view.

```
interface bridge-aggregation interface-number
```

3. Add the interface to a multiport unicast MAC address entry.

```
mac-address multiport mac-address vlan vlan-id
```

By default, no multiport unicast MAC address entry is configured on an interface.

Make sure you have assigned the interface to the VLAN.

Setting the aging timer for dynamic MAC address entries

About aging timer for dynamic MAC address entries

For security and efficient use of table space, the MAC address table uses an aging timer for each dynamic MAC address entry. If a dynamic MAC address entry is not updated before the aging timer expires, the device deletes the entry. This aging mechanism ensures that the MAC address table can promptly update to accommodate latest network topology changes.

A stable network requires a longer aging interval, and an unstable network requires a shorter aging interval.

An aging interval that is too long might cause the MAC address table to retain outdated entries. As a result, the MAC address table resources might be exhausted, and the MAC address table might fail to update its entries to accommodate the latest network changes.

An interval that is too short might result in removal of valid entries, which would cause unnecessary floods and possibly affect the device performance.

To reduce floods on a stable network, set a long aging timer or disable the timer to prevent dynamic entries from unnecessarily aging out. Reducing floods improves the network performance. Reducing flooding also improves the security because it reduces the chances for a data frame to reach unintended destinations.

Procedure

1. Enter system view.

```
system-view
```

2. Set the aging timer for dynamic MAC address entries.

```
mac-address timer { aging seconds | no-aging }
```

The default setting is 300 seconds.

Enabling MAC address learning at the ingress

About MAC address learning at the ingress

The device can learn the source MAC address of a packet when it receives the packet or when it sends out the packet.

Enable ingress MAC address learning if the device is on a CFD network. In a CFD environment, egress MAC address learning might cause unnecessary broadcasts.

For more information about CFD, see *High Availability Configuration Guide*.

Procedure

1. Enter system view.

```
system-view
```

2. Enable MAC address learning at the ingress.

```
mac-address mac-learning ingress
```

By default, the device learns MAC addresses at the egress.

Disabling MAC address learning

About disabling MAC address learning

MAC address learning is enabled by default. To prevent the MAC address table from being saturated when the device is experiencing attacks, disable MAC address learning. For example, you can disable MAC address learning to prevent the device from being attacked by a large amount of frames with different source MAC addresses.

After MAC address learning is disabled, the device immediately deletes existing dynamic MAC address entries.

Disabling global MAC address learning

Restrictions and guidelines

After you disable global MAC address learning, the device cannot learn MAC addresses on any interfaces.

Global MAC address learning does not take effect on a VXLAN VSI. For information about VXLAN VSIs, see *VXLAN Configuration Guide*.

Procedure

1. Enter system view.

```
system-view
```

2. Disable global MAC address learning.

```
undo mac-address mac-learning enable
```

By default, global MAC address learning is enabled.

Disabling MAC address learning on an interface

About disabling MAC address learning on an interface

When global MAC address learning is enabled, you can disable MAC address learning on a single interface.

Procedure

1. Enter system view.
system-view
2. Enter interface view.
 - o Enter Layer 2 Ethernet interface view.
interface *interface-type* *interface-number*
 - o Enter Layer 2 aggregate interface view.
interface bridge-aggregation *interface-number*
3. Disable MAC address learning on the interface.
undo mac-address mac-learning enable
By default, MAC address learning is enabled on an interface.

Configuring MAC address move notifications and suppression

About MAC address move notifications and suppression

The outgoing interface for a MAC address entry learned on interface A is changed to interface B when the following conditions exist:

- Interface B receives a packet with the MAC address as the source MAC address.
- Interface B belongs to the same VLAN as interface A.

In this case, the MAC address is moved from interface A to interface B, and a MAC address move occurs.

The MAC address move notifications feature enables the device to output MAC address move logs when MAC address moves are detected.

If a MAC address is continuously moved between the two interfaces, Layer 2 loops might occur. To detect and locate loops, you can view the MAC address move information. To display the MAC address move records after the device is started, use the **display mac-address mac-move** command.

If the system detects that MAC address moves occur frequently on an interface, you can configure MAC address move suppression to shut the interface down. The interface automatically goes up after a suppression interval. Or, you can manually bring up the interface.

Restrictions and guidelines

After you configure MAC address move notifications, the system sends only log messages to the information center module. If the device is also configured with the **snmp-agent trap enable mac-address** command, the system also sends SNMP notifications to the SNMP module.

Procedure

1. Enter system view.
system-view
2. Enable MAC address move notifications and optionally specify a MAC move detection interval.
mac-address notification mac-move [interval *interval*]
By default, MAC address move notifications are disabled.
3. (Optional.) Set MAC address move suppression parameters.


```
mac-address notification mac-move suppression { interval interval | threshold threshold }
```

By default, the suppression interval is 30 seconds, and the suppression threshold is 3.

For the MAC address move suppression parameters to take effect, enable the MAC address move suppression on a port.

4. Enter interface view.

- o Enter Layer 2 Ethernet interface view.

```
interface interface-type interface-number
```

- o Enter Layer 2 aggregate interface view.

```
interface bridge-aggregation interface-number
```

5. Enable MAC address move suppression.

```
mac-address notification mac-move suppression
```

By default, MAC address move suppression is disabled.

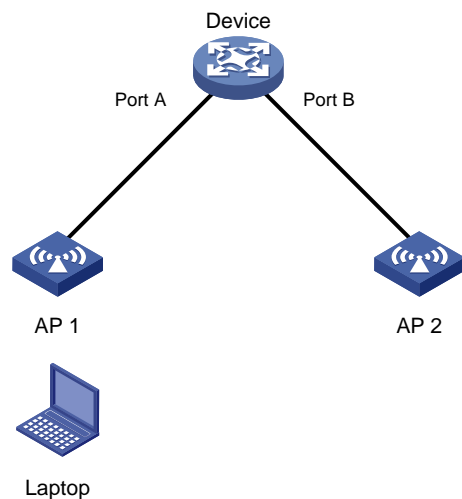
Enabling ARP fast update for MAC address moves

About ARP fast update for MAC address moves

ARP fast update for MAC address moves allows the device to update an ARP entry immediately after the outgoing interface for a MAC address changes. This feature ensures data connection without interruption.

As shown in [Figure 2](#), a mobile user laptop accesses the network by connecting to AP 1 or AP 2. When the AP to which the user connects changes, the device updates the ARP entry for the user immediately after it detects a MAC address move.

Figure 2 ARP fast update application scenario



Procedure

1. Enter system view.

```
system-view
```

2. Enable ARP fast update for MAC address moves.

```
mac-address mac-move fast-update
```

By default, ARP fast update for MAC address moves is disabled.

Configuring the base MAC address

About the base MAC address

The base MAC address is the start MAC address of the 128 consecutive MAC addresses that are reserved for system use.

The base MAC address determines the higher 36 bits of the reserved MAC addresses and the MAC addresses that can be assigned to Layer 3 interfaces.

Restrictions and guidelines

When you configure the base MAC address, make sure the base MAC address plus 128 (decimal) produces a MAC address that has the same higher 36 bits.

After you configure the base MAC address, you cannot modify or delete the base MAC address setting within 30 seconds.

When you assign a MAC address to a Layer 3 interface, make sure the following requirements are met:

- The MAC address must have the same higher 36 bits as the base MAC address.
- The MAC address must be no lower than the base MAC address plus 128 (decimal).

Procedure

1. Enter system view.
system-view
2. Configure the base MAC address.
routing-interface base-mac *mac-address*
By default, no base MAC address exists.

Enabling SNMP notifications for the MAC address table

About SNMP notifications for the MAC address table

To report critical MAC address move events to an NMS, enable SNMP notifications for the MAC address table. For MAC address move event notifications to be sent correctly, you must also configure SNMP on the device.

When SNMP notifications are disabled for the MAC address table, the device sends the generated logs to the information center. To display the logs, configure the log destination and output rule configuration in the information center.

For more information about SNMP and information center configuration, see the network management and monitoring configuration guide for the device.

Procedure

1. Enter system view.
system-view
2. Enable SNMP notifications for the MAC address table.
snmp-agent trap enable mac-address [mac-move]

By default, SNMP notifications are enabled for the MAC address table.

When SNMP notifications are disabled for the MAC address table, syslog messages are sent to notify important events on the MAC address table module.

Display and maintenance commands for MAC address table

Execute **display** commands in any view.

Task	Command
Display MAC address table information.	display mac-address [<i>mac-address</i> [vlan <i>vlan-id</i>] [[dynamic static] [interface <i>interface-type interface-number</i>] blackhole multiport] [vlan <i>vlan-id</i>] [count] nickname <i>nickname</i>]
Display the aging timer for dynamic MAC address entries.	display mac-address aging-time
Display the system or interface MAC address learning state.	display mac-address mac-learning [interface <i>interface-type interface-number</i>]
Display the MAC address move records.	display mac-address mac-move [slot <i>slot-number</i>]
Display MAC address statistics.	display mac-address statistics

MAC address table configuration examples

Example: Configuring the MAC address table

Network configuration

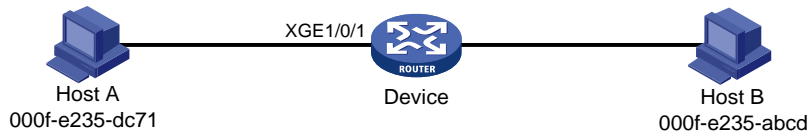
As shown in [Figure 3](#):

- Host A at MAC address 000f-e235-dc71 is connected to Ten-GigabitEthernet 1/0/1 of Device and belongs to VLAN 1.
- Host B at MAC address 000f-e235-abcd, which behaved suspiciously on the network, also belongs to VLAN 1.

Configure the MAC address table as follows:

- To prevent MAC address spoofing, add a static entry for Host A in the MAC address table of Device.
- To drop all frames destined for Host B, add a blackhole MAC address entry for Host B.
- Set the aging timer to 500 seconds for dynamic MAC address entries.

Figure 3 Network diagram



Procedure

⚠ IMPORTANT:

By default, interfaces on the device are disabled (in **ADM** or **Administratively Down** state). To have an interface operate, you must use the **undo shutdown** command to enable that interface.

Add a static MAC address entry for MAC address 000f-e235-dc71 on Ten-GigabitEthernet 1/0/1 that belongs to VLAN 1.

```
<Device> system-view
```

```
[Device] mac-address static 000f-e235-dc71 interface ten-gigabitethernet 1/0/1 vlan 1
```

Add a blackhole MAC address entry for MAC address 000f-e235-abcd that belongs to VLAN 1.

```
[Device] mac-address blackhole 000f-e235-abcd vlan 1
```

Set the aging timer to 500 seconds for dynamic MAC address entries.

```
[Device] mac-address timer aging 500
```

Verifying the configuration

Display the static MAC address entries for Ten-GigabitEthernet 1/0/1.

```
[Device] display mac-address static interface ten-gigabitethernet 1/0/1
```

MAC Address	VLAN ID	State	Port/Nickname	Aging
000f-e235-dc71	1	Static	XGE1/0/1	N

Display the blackhole MAC address entries.

```
[Device] display mac-address blackhole
```

MAC Address	VLAN ID	State	Port/Nickname	Aging
000f-e235-abcd	1	Blackhole	N/A	N

Display the aging time of dynamic MAC address entries.

```
[Device] display mac-address aging-time
```

```
MAC address aging time: 500s.
```

Configuring MAC Information

About MAC Information

The MAC Information feature can generate syslog messages or SNMP notifications when MAC address entries are learned or deleted. You can use these messages to monitor user's leaving or joining the network and analyze network traffic.

The MAC Information feature buffers the MAC change syslog messages or SNMP notifications in a queue. The device overwrites the oldest MAC address change written into the queue with the most recent MAC address change when the following conditions exist:

- The MAC change notification interval does not expire.
- The queue has been exhausted.

To send a syslog message or SNMP notification immediately after it is created, set the queue length to zero.

Enabling MAC Information

Restrictions and guidelines

For MAC Information to take effect, you must enable MAC Information both globally and on interfaces.

Procedure

1. Enter system view.
`system-view`
2. Enable MAC Information globally.
`mac-address information enable`
By default, MAC Information is globally disabled.
3. Enter Layer 2 Ethernet interface view.
`interface interface-type interface-number`
4. Enable MAC Information on the interface.
`mac-address information enable { added | deleted }`
By default, MAC Information is disabled on an interface.

Configuring the MAC Information mode

About MAC Information modes

The following MAC Information modes are available for sending MAC address changes:

- **Syslog**—The device sends syslog messages to notify MAC address changes. The device sends syslog messages to the information center, which then outputs them to the monitoring terminal. For more information about information center, see *Network Management and Monitoring Configuration Guide*.
- **Trap**—The device sends SNMP notifications to notify MAC address changes. The device sends SNMP notifications to the NMS. For more information about SNMP, see *Network Management and Monitoring Configuration Guide*.

Procedure

1. Enter system view.
`system-view`
2. Configure the MAC Information mode.
`mac-address information mode { syslog | trap }`
The default setting is **trap**.

Setting the MAC change notification interval

About the MAC change notification interval

To prevent syslog messages or SNMP notifications from being sent too frequently, you can set the MAC change notification interval to a larger value.

Procedure

1. Enter system view.
`system-view`
2. Set the MAC change notification interval.
`mac-address information interval interval`
The default setting is 1 second.

Setting the MAC Information queue length

About the MAC Information queue length

If the MAC Information queue length is 0, the device sends a syslog message or SNMP notification immediately after learning or deleting a MAC address.

If the MAC Information queue length is not 0, the device stores MAC changes in the queue:

- The device overwrites the oldest MAC change written into the queue with the most recent MAC change when the following conditions exist:
 - The MAC change notification interval does not expire.
 - The queue has been exhausted.
- The device sends syslog messages or SNMP notifications only if the MAC change notification interval expires.

Procedure

1. Enter system view.
`system-view`
2. Set the MAC Information queue length.
`mac-address information queue-length value`
The default setting is 50.

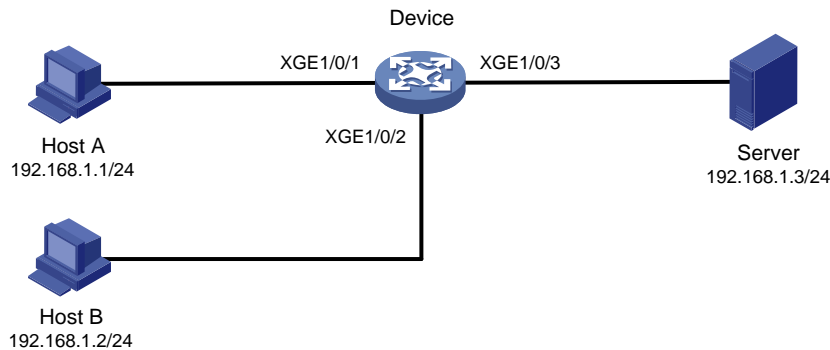
MAC Information configuration examples

Example: Configuring MAC Information

Network configuration

Enable MAC Information on Ten-GigabitEthernet 1/0/1 on Device in [Figure 4](#) to send MAC address changes in syslog messages to the log host, Host B, through interface Ten-GigabitEthernet 1/0/2.

Figure 4 Network diagram



Restrictions and guidelines

When you edit file `/etc/syslog.conf`, follow these restrictions and guidelines:

- Comments must be on a separate line and must begin with a pound sign (#).
- No redundant spaces are allowed after the file name.

The logging facility name and the severity level specified in the `/etc/syslog.conf` file must be the same as those configured on the device. Otherwise, the log information might not be output correctly to the log host. The logging facility name and the severity level are configured by using the `info-center loghost` and `info-center source` commands, respectively.

Procedure

ⓘ IMPORTANT:

By default, interfaces on the device are disabled (in **ADM** or **Administratively Down** state). To have an interface operate, you must use the `undo shutdown` command to enable that interface.

1. Configure Device to send syslog messages to Host B:

Enable the information center.

```
<Device> system-view
```

```
[Device] info-center enable
```

Specify the log host 192.168.1.2/24 and specify **local4** as the logging facility.

```
[Device] info-center loghost 192.168.1.2 facility local4
```

Disable log output to the log host.

```
[Device] info-center source default loghost deny
```

To avoid output of unnecessary information, disable all modules from outputting logs to the specified destination (**loghost**, in this example) before you configure an output rule.

Configure an output rule to output to the log host MAC address logs that have a severity level no lower than **informational**.

```
[Device] info-center source mac loghost level informational
```

2. Configure the log host, Host B:

Configure Solaris as follows. Configure other UNIX operating systems in the same way Solaris is configured.

a. Log in to the log host as a root user.

b. Create a subdirectory named **Device** in directory **/var/log/**.

```
# mkdir /var/log/Device
```

c. Create file **info.log** in the **Device** directory to save logs from **Device**.

```
# touch /var/log/Device/info.log
```

d. Edit the file **syslog.conf** in directory **/etc/** and add the following contents:

```
# Device configuration messages
local4.info /var/log/Device/info.log
```

In this configuration, **local4** is the name of the logging facility that the log host uses to receive logs, and **info** is the informational level. The UNIX system records the log information that has a severity level no lower than **informational** to file **/var/log/Device/info.log**.

e. Display the process ID of **syslogd**, end the **syslogd** process, and then restart **syslogd** using the **-r** option to make the new configuration take effect.

```
# ps -ae | grep syslogd
147
# kill -HUP 147
# syslogd -r &
```

The device can output MAC address logs to the log host, which stores the logs to the specified file.

3. Enable MAC Information on Device:

Enable MAC Information globally.

```
[Device] mac-address information enable
```

Configure the MAC Information mode as syslog.

```
[Device] mac-address information mode syslog
```

Enable MAC Information on Ten-GigabitEthernet 1/0/1 to enable the port to record MAC address change information when the interface performs either of the following operations:

- o Learns a new MAC address.
- o Deletes an existing MAC address.

```
[Device] interface ten-gigabitethernet 1/0/1
```

```
[Device-Ten-GigabitEthernet1/0/1] mac-address information enable added
```

```
[Device-Ten-GigabitEthernet1/0/1] mac-address information enable deleted
```

```
[Device-Ten-GigabitEthernet1/0/1] quit
```

Set the MAC Information queue length to 100.

```
[Device] mac-address information queue-length 100
```

Set the MAC change notification interval to 20 seconds.

```
[Device] mac-address information interval 20
```