Contents

Configuring port security

Overview

Port security combines and extends 802.1X and MAC authentication to provide MAC-based network access control. This feature applies to networks, such as a WLAN, that require different authentication methods for different users on a port.

Port security provides the following functions:

- Prevents unauthorized access to a network by checking the source MAC address of inbound traffic.
- Prevents access to unauthorized devices or hosts by checking the destination MAC address of outbound traffic.
- Controls MAC address learning and authentication on a port to make sure the port learns only source trusted MAC addresses.

A frame is illegal if its source MAC address cannot be learned in a port security mode or it is from a client that has failed 802.1X or MAC authentication. The port security feature automatically takes a predefined action on illegal frames. This automatic mechanism enhances network security and reduces human intervention.

NOTE:

As a best practice, use the 802.1X authentication or MAC authentication feature rather than port security for scenarios that require only 802.1X authentication or MAC authentication. For more information about 802.1X and MAC authentication, see "Configuring 802.1X" and "Configuring MAC authentication."

Port security features

NTK

The need to know (NTK) feature prevents traffic interception by checking the destination MAC address in the outbound frames. The feature ensures that frames are sent only to the following hosts:

- Hosts that have passed authentication.
- Hosts whose MAC addresses have been learned or configured on the access device.

Intrusion protection

The intrusion protection feature checks the source MAC address in inbound frames for illegal frames, and takes a predefined action on each detected illegal frame. The action can be disabling the port temporarily, disabling the port permanently, or blocking frames from the illegal MAC address for 3 minutes (not user configurable).

Port security modes

Port security supports the following categories of security modes:

- **MAC learning control**—Includes two modes: autoLearn and secure. MAC address learning is permitted on a port in autoLearn mode and disabled in secure mode.
- **Authentication**—Security modes in this category implement MAC authentication, 802.1X authentication, or a combination of these two authentication methods.

Upon receiving a frame, the port in a security mode searches the MAC address table for the source MAC address. If a match is found, the port forwards the frame. If no match is found, the port learns the MAC address or performs authentication, depending on the security mode. If the frame is illegal, the port takes the predefined NTK or intrusion protection action, or sends SNMP notifications. Outgoing frames are not restricted by port security's NTK action unless they trigger the NTK feature.

The maximum number of users a port supports equals the smaller value from the following values:

- The maximum number of secure MAC addresses that port security allows.
- The maximum number of concurrent users the authentication mode in use allows.

For example, if 802.1X allows more concurrent users than port security's limit on the number of MAC addresses on the port in userLoginSecureExt mode, port security's limit takes effect.

Table 1 describes the port security modes and the security features.

Table 1 Port security modes

Purpose	Security mode		Features that can be triggered
Turning off the port security feature	noRestrictions (the default mode) In this mode, port security is disabled on the port and access to the port is not restricted.		N/A
Controlling MAC address learning	autoLearn		NTK/intrusion protection
	secure		
Performing 802.1X authentication	userLogin		N/A
	userLoginSecure		NTK/intrusion protection
	userLoginSecureExt		
	userLoginWithOUI		
Performing MAC authentication	macAddressWithRadius		NTK/intrusion protection
Performing a combination of MAC authentication and 802.1X authentication	Or	macAddressOrUserLoginSecure	NTK/intrusion protection
		macAddressOrUserLoginSecureExt	
	Else	macAddressElseUserLoginSecure	
		macAddressElseUserLoginSecureExt	

TIP:

- **userLogin** specifies 802.1X authentication and port-based access control. **userLogin** with **Secure** specifies 802.1X authentication and MAC-based access control. **Ext** indicates allowing multiple 802.1X users to be authenticated and serviced at the same time. A security mode without **Ext** allows only one user to pass 802.1X authentication.
- **macAddress** specifies MAC authentication.
- **Else** specifies that the authentication method before **Else** is applied first. If the authentication fails, whether to turn to the authentication method following **Else** depends on the protocol type of the authentication request.
- In a security mode with **Or**, the authentication method to be used depends on the protocol type of the authentication request.

Controlling MAC address learning

- autoLearn.

A port in this mode can learn MAC addresses. The automatically learned MAC addresses are not added to the MAC address table as dynamic MAC address. Instead, these MAC addresses are added to the secure MAC address table as secure MAC addresses. You can also configure secure MAC addresses by using the **port-security mac-address security** command.

A port in autoLearn mode allows frames sourced from the following MAC addresses to pass:

- Secure MAC addresses.
- MAC addresses configured by using the **mac-address dynamic** and **mac-address static** commands.

When the number of secure MAC addresses reaches the upper limit, the port transitions to secure mode.

- secure.

  MAC address learning is disabled on a port in secure mode. You configure MAC addresses by using the **mac-address static** and **mac-address dynamic** commands. For more information about configuring MAC address table entries, see *Layer 2—LAN Switching Configuration Guide*.

  A port in secure mode allows only frames sourced from the following MAC addresses to pass:

  - Secure MAC addresses.
  - MAC addresses configured by using the **mac-address dynamic** and **mac-address static** commands.

Performing 802.1X authentication

- userLogin.

  A port in this mode performs 802.1X authentication and implements port-based access control. The port can service multiple 802.1X users. Once an 802.1X user passes authentication on the port, any subsequent 802.1X users can access the network through the port without authentication.

- userLoginSecure.

  A port in this mode performs 802.1X authentication and implements MAC-based access control. The port services only one user passing 802.1X authentication.

- userLoginSecureExt.

  This mode is similar to the userLoginSecure mode except that this mode supports multiple online 802.1X users.

- userLoginWithOUI.

  This mode is similar to the userLoginSecure mode. The difference is that a port in this mode also permits frames from one user whose MAC address contains a specific OUI.

  In this mode, the port performs OUI check first. If the OUI check fails, the port performs 802.1X authentication. The port permits frames that pass OUI check or 802.1X authentication.

NOTE:

An OUI is a 24-bit number that uniquely identifies a vendor, manufacturer, or organization. In MAC addresses, the first three octets are the OUI.

Performing MAC authentication

macAddressWithRadius: A port in this mode performs MAC authentication, and services multiple users.

Performing a combination of MAC authentication and 802.1X authentication

- macAddressOrUserLoginSecure.

  This mode is the combination of the macAddressWithRadius and userLoginSecure modes. The mode allows one 802.1X authentication user and multiple MAC authentication users to log in.

In this mode, the port performs 802.1X authentication first. If 802.1X authentication fails, MAC authentication is performed.

- macAddressOrUserLoginSecureExt.

  This mode is similar to the macAddressOrUserLoginSecure mode, except that this mode supports multiple 802.1X and MAC authentication users.

- macAddressElseUserLoginSecure.

  This mode is the combination of the macAddressWithRadius and userLoginSecure modes, with MAC authentication having a higher priority as the **Else** keyword implies. The mode allows one 802.1X authentication user and multiple MAC authentication users to log in.

  The port performs MAC authentication upon receiving non-802.1X frames. Upon receiving 802.1X frames, the port performs MAC authentication and then, if the authentication fails, 802.1X authentication.

- macAddressElseUserLoginSecureExt.

  This mode is similar to the macAddressElseUserLoginSecure mode except that this mode supports multiple 802.1X and MAC authentication users as the **Ext** keyword implies.

Configuration task list

Tasks at a glance	Remarks
(Required.) Enabling port security	N/A
(Optional.) Setting port security's limit on the number of secure MAC addresses on a port	N/A
(Required.) Setting the port security mode	N/A
(Required.) Configuring port security features: • Configuring NTK • Configuring intrusion protection	Configure one or more port security features according to the network requirements.
(Optional.) Configuring secure MAC addresses	N/A
(Optional.) Ignoring authorization information from the server	N/A
(Optional.) Enabling MAC move	N/A
(Optional.) Applying NAS-ID profile to port security	N/A
(Optional.) Enabling the authorization-fail-offline feature	N/A
(Optional.) Enabling SNMP notifications for port security	N/A

Enabling port security

Before you enable port security, disable 802.1X and MAC authentication globally.

When port security is enabled, you cannot enable 802.1X or MAC authentication, or change the access control mode or port authorization state. Port security automatically modifies these settings in different security modes.

To enable port security:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Enable port security.	**port-security enable**	By default, port security is disabled.

You can use the **undo port-security enable** command to disable port security. Because the command logs off the online users, make sure no online users are present.

Enabling or disabling port security resets the following security settings to the default:

- 802.1X access control mode is MAC based.
- 802.1X port authorization state is auto.

For more information about 802.1X authentication and MAC authentication configuration, see "Configuring 802.1X" and "Configuring MAC authentication."

Setting port security's limit on the number of secure MAC addresses on a port

You can set the maximum number of secure MAC addresses that port security allows on a port for the following purposes:

- Controlling the number of concurrent users on the port.

  For a port operating in a security mode (except for autoLearn and secure), the upper limit equals the smaller of the following values:

  - The limit of the secure MAC addresses that port security allows.
  - The limit of concurrent users allowed by the authentication mode in use.
- Controlling the number of secure MAC addresses on the port in autoLearn mode.

The port security's limit on the number of secure MAC addresses on a port is independent of the MAC learning limit described in MAC address table configuration. For more information about MAC address table configuration, see *Layer 2—LAN Switching Configuration Guide*.

To set the maximum number of secure MAC addresses allowed on a port:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Set the maximum number of secure MAC addresses allowed on a port.	**port-security max-mac-count** *count-value*	By default, port security does not limit the number of secure MAC addresses on a port.

Setting the port security mode

Before you set a port security mode for a port, complete the following tasks:

- Disable 802.1X and MAC authentication.
- Verify that the port does not belong to a link aggregation group.
- If you are configuring the autoLearn mode, set port security's limit on the number of secure MAC addresses. You cannot change the setting when the port is operating in autoLearn mode.

When you set the port security mode, follow these guidelines:

- You can specify a port security mode when port security is disabled, but your configuration cannot take effect.
- Changing the port security mode of a port logs off the online users of the port.
- Do not enable 802.1X authentication or MAC authentication on a port where port security is configured.
- The device supports the URL attribute assigned by a RADIUS server in the following port security modes:
  - **mac-authentication**.
  - **mac-else-userlogin-secure.**
  - **mac-else-userlogin-secure-ext**.
  - **userlogin-secure.**
  - **userlogin-secure-ext**.
  - **userlogin-secure-or-mac.**
  - **userlogin-secure-or-mac-ext**.
  - **userlogin-withoui**.

  During authentication, a user is redirected to the Web interface specified by the server-assigned URL attribute. After the user passes the Web authentication, the RADIUS server records the MAC address of the Web user and uses a DM (Disconnect Message) to log off the Web user. When the user initiates 802.1X or MAC authentication again, it will pass the authentication and come online successfully.

To enable a port security mode:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. (Optional.) Set an OUI value for user authentication.	**port-security oui index** *index-value* **mac-address** *oui-value*	By default, no OUI value is configured for user authentication. This command is required for the **userlogin-withoui** mode. You can set multiple OUIs, but when the port security mode is **userlogin-withoui**, the port allows one 802.1X user and only one user that matches one of the specified OUIs.
3. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
4. Set the port security mode.	**port-security port-mode** { **autolearn** | **mac-authentication** | **mac-else-userlogin-secure** | **mac-else-userlogin-secure-ext** | **secure** | **userlogin** | **userlogin-secure** | **userlogin-secure-ext** | **userlogin-secure-or-mac** | **userlogin-secure-or-mac-ext** | **userlogin-withoui** }	By default, a port operates in noRestrictions mode. After enabling port security, you can change the port security mode of a port only when the port is operating in noRestrictions (the default) mode. To change the port security mode for a port in any other mode, first use the **undo port-security port-mode** command to restore the default port security mode.

Configuring port security features

Configuring NTK

The NTK feature checks the destination MAC addresses in outbound frames to make sure frames are forwarded only to authenticated devices.

The NTK feature supports the following modes:

- **ntkonly**—Forwards only unicast frames with authenticated destination MAC addresses.
- **ntk-withbroadcasts**—Forwards only broadcast frames and unicast frames with authenticated destination MAC addresses.
- **ntk-withmulticasts**—Forwards only broadcast frames, multicast frames, and unicast frames with authenticated destination MAC addresses.

The NTK feature drops any unicast frame with an unknown destination MAC address. Not all port security modes support triggering the NTK feature. For more information, see Table 1.

To configure the NTK feature:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Configure the NTK feature.	**port-security ntk-mode** { **ntk-withbroadcasts** | **ntk-withmulticasts** | **ntkonly** }	By default, NTK is disabled on a port and all frames are allowed to be sent.

Configuring intrusion protection

Intrusion protection enables a device to take one of the following actions in response to illegal frames:

- **blockmac**—Adds the source MAC addresses of illegal frames to the blocked MAC address list and discards the frames. All subsequent frames sourced from a blocked MAC address are dropped. A blocked MAC address is restored to normal state after being blocked for 3 minutes. The interval is fixed and cannot be changed.
- **disableport**—Disables the port until you bring it up manually.
- **disableport-temporarily**—Disables the port for a period of time. The period can be configured with the **port-security timer disableport** command.

To configure the intrusion protection feature:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Configure the intrusion protection feature.	**port-security intrusion-mode** { **blockmac** | **disableport** | **disableport-temporarily** }	By default, intrusion protection is disabled.
4. Return to system view.	**quit**	N/A

Step	Command	Remarks
5. (Optional.) Set the silence timeout period during which a port remains disabled.	**port-security timer disableport** *time-value*	By default, the port silence timeout is 20 seconds.

NOTE:

On a port operating in either macAddressElseUserLoginSecure mode or macAddressElseUserLoginSecureExt mode, intrusion protection is triggered only after both MAC authentication and 802.1X authentication fail for the same frame.

Configuring secure MAC addresses

Secure MAC addresses are configured or learned in autoLearn mode. If the secure MAC addresses are saved, they can survive a device reboot. You can bind a secure MAC address only to one port in a VLAN.

When the maximum number of secure MAC address entries is reached, the port changes to secure mode. In secure mode, the port cannot add or learn any more secure MAC addresses. The port allows only frames sourced from secure MAC addresses or MAC addresses configured by using the **mac-address dynamic** or **mac-address static** command to pass through.

Secure MAC addresses include static, sticky, and dynamic secure MAC addresses.

Table 2 A comparison of static, sticky, and dynamic secure MAC addresses

Type	Address sources	Aging mechanism	Can be saved and survive a device reboot?
Static	Manually added (by using the **port-security mac-address security** command without the **sticky** keyword).	Not available. The static addresses never age out unless you perform any of the following tasks: • Manually remove these MAC addresses. • Change the port security mode. • Disable the port security feature.	Yes.
Sticky	• Manually added (by using the **port-security mac-address security** command with the **sticky** keyword). • Converted from dynamic secure MAC addresses. • Automatically learned when the dynamic secure MAC feature (**port-security mac-address dynamic**) is disabled.	By default, sticky MAC addresses do not age out. However, you can configure an aging timer or use the aging timer together with the inactivity aging feature to delete old sticky MAC addresses. • If only the aging timer is configured, the aging timer counts up regardless of whether traffic data has been sent from the sticky MAC address. • If both the aging timer and the inactivity aging feature are configured, the aging timer restarts once traffic data is detected from the sticky MAC address.	Yes. The secure MAC aging timer restarts at a reboot.
Dynamic	• Converted from sticky MAC addresses. • Automatically learned after the dynamic secure MAC feature is enabled.	Same as sticky MAC addresses.	No. All dynamic secure MAC addresses are lost at reboot.

Configuration prerequisites

Before you configure secure MAC addresses, complete the following tasks:

- Enable port security.
- Set port security's limit on the number of MAC addresses on the port. Perform this task before you enable autoLearn mode.
- Set the port security mode to autoLearn.
- Configure the port to permit packets of the specified VLAN to pass or add the port to the VLAN. Make sure the VLAN already exists.

Configuration procedure

To configure a secure MAC address:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. (Optional.) Set the secure MAC aging timer.	**port-security timer autolearn aging** *time-value*	By default, secure MAC addresses do not age out.
3. Configure a secure MAC address.	• In system view: **port-security mac-address security** [**sticky**] *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id* • In Layer 2 Ethernet interface view: **a.** **interface** *interface-type interface-number* **b.** **port-security mac-address security** [**sticky**] *mac-address* **vlan** *vlan-id* **c.** **quit**	By default, no secure MAC address exists. In the same VLAN, a MAC address cannot be specified as both a static secure MAC address and a sticky MAC address.
4. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
5. (Optional.) Enable inactivity aging.	**port-security mac-address aging-type inactivity**	By default, the inactivity aging feature is disabled.
6. (Optional.) Enable the dynamic secure MAC feature.	**port-security mac-address dynamic**	By default, the dynamic secure MAC feature is disabled. Sticky MAC addresses can be saved to the configuration file. Once saved, they can survive a device reboot.

Ignoring authorization information from the server

You can configure a port to ignore the authorization information received from the server (local or remote) after an 802.1X or MAC authentication user passes authentication.

To configure a port to ignore authorization information from the server:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Ignore the authorization information received from the authentication server.	**port-security authorization ignore**	By default, a port uses the authorization information received from the authentication server.

Enabling MAC move

MAC move allows 802.1X or MAC authenticated users to move between ports on a device. For example, if an authenticated 802.1X user moves to another 802.1X-enabled port on the device, the authentication session is deleted from the first port. The user is reauthenticated on the new port.

If MAC move is disabled, 802.1X or MAC users authenticated on one port cannot pass authentication after they move to another port.

As a best practice, enable MAC move for users that roam between ports to access the network.

To enable MAC move:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable MAC move.	**port-security mac-move permit**	By default, MAC move is disabled.

Applying NAS-ID profile to port security

By default, the device sends its device name in the NAS-Identifier attribute of any RADIUS requests.

A NAS-ID profile enables you to send different NAS-Identifier attribute strings in RADIUS requests from different VLANs. The strings can be organization names, service names, or any user categorization criteria, depending on the administrative requirements.

For example, map the NAS-ID **companyA** to all VLANs of company A. The device will send **companyA** in the NAS-Identifier attribute for the RADIUS server to identify requests from any Company A users.

You can apply a NAS-ID profile to port security globally or on a port. On a port, the device selects a NAS-ID profile in the following order:

1. The port-specific NAS-ID profile.

2. The NAS-ID profile applied globally.

If no NAS-ID profile is applied or no matching binding is found in the selected profile, the device uses the device name as the NAS-ID.

For more information about the NAS-ID profile configuration, see "Configuring AAA."

To apply a NAS-ID profile to port security:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Apply a NAS-ID profile.	• In system view: **port-security nas-id-profile** *profile-name* • In Layer 2 Ethernet interface view: **a.** **interface** *interface-type interface-number* **b.** **port-security nas-id-profile** *profile-name*	By default, no NAS-ID profile is applied in system view or in Layer 2 Ethernet interface view.

Enabling the authorization-fail-offline feature

The authorization-fail-offline feature logs off port security users that fail ACL or user profile authorization.

A user fails ACL or user profile authorization in the following situations:

- The device fails to authorize the specified ACL or user profile to the user.
- The server assigns a nonexistent ACL or user profile to the user.

This feature does not apply to VLAN authorization failure. The device logs off these users directly.

To enable the authorization-fail-offline feature:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable the authorization-fail-offline feature.	**port-security authorization-fail offline**	By default, this feature is disabled, and the device does not log off users that fail ACL or user profile authorization.

Enabling SNMP notifications for port security

Use this feature to report critical port security events to an NMS. For port security event notifications to be sent correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see *Network Management and Monitoring Configuration Guide*.

This feature takes effect only when intrusion protection feature is configured.

To enable SNMP notifications for port security:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable SNMP notifications for port security.	**snmp-agent trap enable port-security** [**address-learned** | **dot1x-failure** | **dot1x-logoff** | **dot1x-logon** | **intrusion** | **mac-auth-failure** | **mac-auth-logoff** | **mac-auth-logon**] *	By default, SNMP notifications are disabled for port security.

Displaying and maintaining port security

Execute **display** commands in any view:

Task	Command
Display the port security configuration, operation information, and statistics.	**display port-security** [**interface** *interface-type interface-number*]
Display information about secure MAC addresses.	**display port-security mac-address security** [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**]
Display information about blocked MAC addresses.	**display port-security mac-address block** [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**]

Port security configuration examples

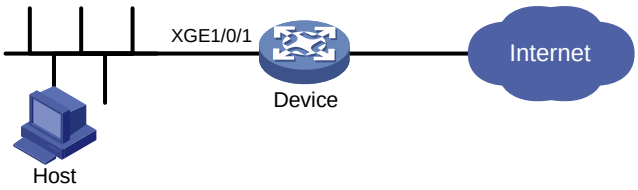
autoLearn configuration example

Network requirements

As shown in Figure 1, configure port Ten-GigabitEthernet 1/0/1 on the device to meet the following requirements:

- Accept up to 64 users without authentication.
- Be permitted to learn and add MAC addresses as sticky MAC addresses, and set the secure MAC aging timer to 30 minutes.
- Stop learning MAC addresses after the number of secure MAC addresses reaches 64. If any frame with an unknown MAC address arrives, intrusion protection starts, and the port shuts down and stays silent for 30 seconds.

Figure 1 Network diagram



Configuration procedure

Enable port security.

```
<Device> system-view
[Device] port-security enable
```

Set the secure MAC aging timer to 30 minutes.

```
[Device] port-security timer autolearn aging 30
```

Set port security's limit on the number of secure MAC addresses to 64 on port Ten-GigabitEthernet 1/0/1.

```
[Device] interface ten-gigabitethernet 1/0/1
[Device-Ten-GigabitEthernet1/0/1] port-security max-mac-count 64
```

Set the port security mode to autoLearn.

```
[Device-Ten-GigabitEthernet1/0/1] port-security port-mode autolearn
```

Configure the port to be silent for 30 seconds after the intrusion protection feature is triggered.

```
[Device-Ten-GigabitEthernet1/0/1] port-security intrusion-mode disableport-temporarily
[Device-Ten-GigabitEthernet1/0/1] quit
[Device] port-security timer disableport 30
```

Verifying the configuration

Verify the port security configuration.

```
[Device] display port-security interface ten-gigabitethernet 1/0/1
Port security parameters:
   Port security          : Enabled
   AutoLearn aging time   : 30 min
   Disableport timeout    : 30 s
   MAC move               : Denied
   Authorization fail     : Online
 NAS-ID profile is not configured
   Dot1x-failure trap     : Disabled
   Dot1x-logon trap       : Disabled
   Dot1x-logoff trap      : Disabled
   Intrusion trap         : Disabled
   Address-learned trap   : Disabled
   Mac-auth-failure trap  : Disabled
   Mac-auth-logon trap    : Disabled
   Mac-auth-logoff trap   : Disabled
   OUI value list         :

 Ten-GigabitEthernet1/0/1 is link-up
   Port mode                      : autoLearn
   NeedToKnow mode                : Disabled
   Intrusion protection mode      : DisablePortTemporarily
   Security MAC address attribute
       Learning mode              : Sticky
       Aging type                 : Periodical
   Max secure MAC addresses       : 64
   Current secure MAC addresses   : 5
   Authorization                  : Permitted
   NAS-ID profile is not configured
```

The output shows the following information:

- The port security's limit on the number of secure MAC addresses on the port is 64.
- The port security mode is autoLearn.
- The intrusion protection action is disabling the port (DisablePortTemporarily) for 30 seconds.

The port allows for MAC address learning, and you can display the number of learned MAC addresses in the **Current secure MAC addresses** field.

Display additional information about the learned MAC addresses.

```
[Device] interface ten-gigabitethernet 1/0/1
[Device-Ten-GigabitEthernet1/0/1] display this
#
interface Ten-GigabitEthernet1/0/1
 port-security max-mac-count 64
 port-security port-mode autolearn
```

```
 port-security mac-address security sticky 0002-0000-0015 vlan 1
 port-security mac-address security sticky 0002-0000-0014 vlan 1
 port-security mac-address security sticky 0002-0000-0013 vlan 1
 port-security mac-address security sticky 0002-0000-0012 vlan 1
 port-security mac-address security sticky 0002-0000-0011 vlan 1
#
[Device-Ten-GigabitEthernet1/0/1] quit
```

Verify that the port security mode changes to **secure** after the number of MAC addresses learned by the port reaches 64.

```
[Device] display port-security interface ten-gigabitethernet 1/0/1
```

Verify that the port will be disabled for 30 seconds after it receives a frame with an unknown MAC address. (Details not shown.)

After the port is re-enabled, delete several secure MAC addresses.

```
[Device] undo port-security mac-address security sticky 0002-0000-0015 vlan 1
[Device] undo port-security mac-address security sticky 0002-0000-0014 vlan 1
```

Verify that the port security mode of the port changes to **autoLearn**, and the port can learn MAC addresses again. (Details not shown.)

userLoginWithOUI configuration example

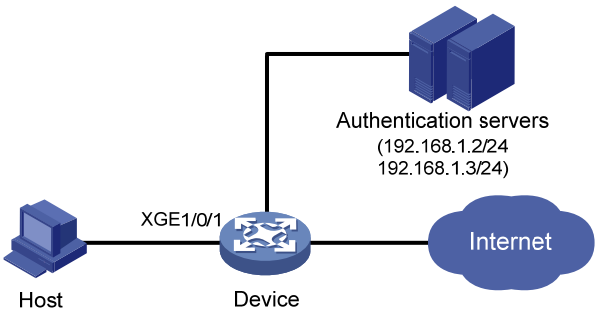
Network requirements

As shown in Figure 2, a client is connected to the device through port Ten-GigabitEthernet 1/0/1. The device authenticates the client with a RADIUS server. If the authentication succeeds, the client is authorized to access the Internet.

- The RADIUS server at 192.168.1.2 functions as the primary authentication server and the secondary accounting server. The RADIUS server at 192.168.1.3 functions as the secondary authentication server and the primary accounting server. The shared key for authentication is **name**, and the shared key for accounting is **money**.
- All users use the authentication, authorization, and accounting methods of ISP domain **sun**.
- The RADIUS server response timeout time is 5 seconds. The maximum number of RADIUS packet retransmission attempts is five. The device sends real-time accounting packets to the RADIUS server at 15-minute intervals, and sends usernames without domain names to the RADIUS server.

Configure port Ten-GigabitEthernet 1/0/1 of the device to allow only one 802.1X user and a user that uses one of the specified OUI values to be authenticated.

Figure 2 Network diagram



Configuration procedure

The following configuration steps cover some AAA/RADIUS configuration commands. For more information about the commands, see *Security Command Reference*.

Make sure the host and the RADIUS server can reach each other.

1. Configure AAA:

Configure a RADIUS scheme named **radsun**.

```
<Device> system-view
[Device] radius scheme radsun
[Device-radius-radsun] primary authentication 192.168.1.2
[Device-radius-radsun] primary accounting 192.168.1.3
[Device-radius-radsun] secondary authentication 192.168.1.3
[Device-radius-radsun] secondary accounting 192.168.1.2
[Device-radius-radsun] key authentication simple name
[Device-radius-radsun] key accounting simple money
[Device-radius-radsun] timer response-timeout 5
[Device-radius-radsun] retry 5
[Device-radius-radsun] timer realtime-accounting 15
[Device-radius-radsun] user-name-format without-domain
[Device-radius-radsun] quit
```

Configure ISP domain **sun**.

```
[Device] domain sun
[Device-isp-sun] authentication lan-access radius-scheme radsun
[Device-isp-sun] authorization lan-access radius-scheme radsun
[Device-isp-sun] accounting lan-access radius-scheme radsun
[Device-isp-sun] quit
```

2. Set the 802.1X authentication method to CHAP. By default, the authentication method for 802.1X is CHAP.

```
[Device] dot1x authentication-method chap
```

3. Configure port security:

Enable port security.

```
[Device] port-security enable
```

Add five OUI values. (You can add up to 16 OUI values. The port permits only one user matching one of the OUIs to pass authentication.)

```
[Device] port-security oui index 1 mac-address 1234-0100-1111
[Device] port-security oui index 2 mac-address 1234-0200-1111
[Device] port-security oui index 3 mac-address 1234-0300-1111
[Device] port-security oui index 4 mac-address 1234-0400-1111
[Device] port-security oui index 5 mac-address 1234-0500-1111
```

Set the port security mode to userLoginWithOUI.

```
[Device] interface ten-gigabitethernet 1/0/1
[Device-Ten-GigabitEthernet1/0/1] port-security port-mode userlogin-withoui
[Device-Ten-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Verify the RADIUS scheme configuration.

```
[Device] display radius scheme radsun
RADIUS Scheme Name  : radsun
  Index : 0
```

```
  Primary Auth Server:
    Host name: Not configured
    IP  : 192.168.1.2                          Port: 1812   State: Active
    VPN : Not configured
  Primary Acct Server:
    Host name: Not configured
    IP  : 192.168.1.3                          Port: 1813   State: Active
    VPN : Not configured
  Second Auth Server:
    Host name: Not configured
    IP  : 192.168.1.3                          Port: 1812   State: Active
    VPN : Not configured
  Second Acct Server:
    Host name: Not configured
    IP  : 192.168.1.2                          Port: 1813   State: Active
    VPN : Not configured

  Accounting-On function                    : Disabled
    retransmission times                    : 50
    retransmission interval(seconds)        : 3
  Timeout Interval(seconds)                 : 5
  Retransmission Times                      : 5
  Retransmission Times for Accounting Update : 5
  Server Quiet Period(minutes)              : 5
  Realtime Accounting Interval(minutes)     : 15
  Stop-accounting packets buffering         : Enabled
    Retransmission Times                    : 500
  NAS IP Address                            : Not configured
  VPN                                       : Not configured
  User Name Format                          : without-domain
  Data flow unit                            : Byte
  Packet unit                               : one
  Attribute-15 check-mode                   : strict
```

After users pass authentication, display port security configuration. Verify that port Ten-GigabitEthernet 1/0/1 allows only one 802.1X user to be authenticated.

```
[Device] display port-security interface ten-gigabitethernet 1/0/1
Port security parameters:
   Port security          : Enabled
   AutoLearn aging time   : 0 min
   Disableport timeout    : 20 s
   MAC move               : Denied
   Authorization fail     : Online
 NAS-ID profile is not configured
   Dot1x-failure trap     : Disabled
   Dot1x-logon trap       : Disabled
   Dot1x-logoff trap      : Disabled
   Intrusion trap         : Disabled
   Address-learned trap   : Disabled
```

```
  Mac-auth-failure trap  : Disabled
  Mac-auth-logon trap    : Disabled
  Mac-auth-logoff trap   : Disabled
  OUI value list         :
    Index :  1         Value : 123401
    Index :  2         Value : 123402
    Index :  3,        Value : 123403
    Index :  4,        Value : 123404
    Index :  5,        Value : 123405

Ten-GigabitEthernet1/0/1 is link-up
  Port mode                     : userLoginWithOUI
  NeedToKnow mode               : Disabled
  Intrusion protection mode     : NoAction
  Security MAC address attribute
      Learning mode             : Sticky
      Aging type                : Periodical
  Max secure MAC addresses      : Not configured
  Current secure MAC addresses  : 1
  Authorization                 : Permitted
  NAS-ID profile is not configured
```

Display information about the online 802.1X user to verify 802.1X configuration.

```
[Device] display dot1x
```

Verify that the port also allows one user whose MAC address has an OUI among the specified OUIs to pass authentication.

```
[Device] display mac-address interface ten-gigabitethernet 1/0/1
MAC Address     VLAN ID   State          Port                              Aging
1234-0300-0011  1         Learned        Ten-GigabitEthernet1/0/1             Y
```

macAddressElseUserLoginSecure configuration example

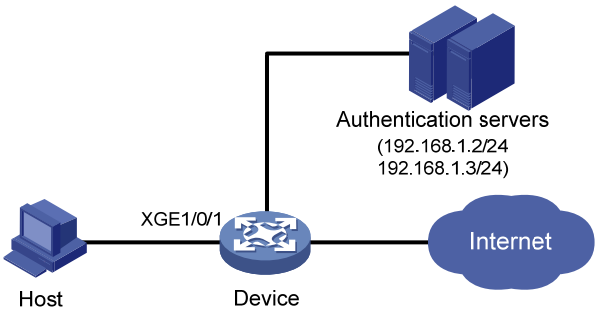
Network requirements

As shown in Figure 3, a client is connected to the device through Ten-GigabitEthernet 1/0/1. The device authenticates the client by a RADIUS server. If the authentication succeeds, the client is authorized to access the Internet.

Configure port Ten-GigabitEthernet 1/0/1 of the device to meet the following requirements:

- Allow more than one MAC authenticated user to log on.
- For 802.1X users, perform MAC authentication first and then, if MAC authentication fails, 802.1X authentication. Allow only one 802.1X user to log on.
- Use the MAC address of each user as the username and password for authentication. A MAC address is in the hexadecimal notation with hyphens, and letters are in upper case.
- Set the total number of MAC authenticated users and 802.1X authenticated users to 64.
- Enable NTK (**ntkonly** mode) to prevent frames from being sent to unknown MAC addresses.

Figure 3 Network diagram



Configuration procedure

Make sure the host and the RADIUS server can reach each other.

1. Configure RADIUS authentication/accounting and ISP domain settings. (See "userLoginWithOUI configuration example.")
2. Configure port security:

   # Enable port security.

   ```
   <Device> system-view
   [Device] port-security enable
   ```

   # Use MAC-based accounts for MAC authentication. Each MAC address must be in the hexadecimal notation with hyphens, and letters are in upper case.

   ```
   [Device] mac-authentication user-name-format mac-address with-hyphen uppercase
   ```

   # Specify the MAC authentication domain.

   ```
   [Device] mac-authentication domain sun
   ```

   # Set the 802.1X authentication method to CHAP. By default, the authentication method for 802.1X is CHAP.

   ```
   [Device] dot1x authentication-method chap
   ```

   # Set port security's limit on the number of MAC addresses to 64 on the port.

   ```
   [Device] interface ten-gigabitethernet 1/0/1
   [Device-Ten-GigabitEthernet1/0/1] port-security max-mac-count 64
   ```

   # Set the port security mode to macAddressElseUserLoginSecure.

   ```
   [Device-Ten-GigabitEthernet1/0/1] port-security port-mode
   mac-else-userlogin-secure
   ```

   # Set the NTK mode of the port to ntkonly.

   ```
   [Device-Ten-GigabitEthernet1/0/1] port-security ntk-mode ntkonly
   [Device-Ten-GigabitEthernet1/0/1] quit
   ```

Verifying the configuration

Verify the port security configuration.

```
[Device] display port-security interface ten-gigabitethernet 1/0/1
Port security parameters:
   Port security          : Enabled
   AutoLearn aging time   : 0 min
   Disableport timeout    : 20 s
   MAC move               : Denied
   Authorization fail     : Online
   Dot1x-failure trap     : Disabled
   Dot1x-logon trap       : Disabled
```

```
  Dot1x-logoff trap      : Disabled
  Intrusion trap         : Disabled
  Address-learned trap   : Disabled
  Mac-auth-failure trap  : Disabled
  Mac-auth-logon trap    : Disabled
  Mac-auth-logoff trap   : Disabled
NAS-ID profile is not configured
  OUI value list         :

Ten-GigabitEthernet1/0/1 is link-up
  Port mode                      : macAddressElseUserLoginSecure
  NeedToKnow mode                : NeedToKnowOnly
  Intrusion protection mode      : NoAction
  Security MAC address attribute
      Learning mode              : Sticky
      Aging type                 : Periodical
  Max secure MAC addresses       : 64
  Current secure MAC addresses   : 0
  Authorization                  : Permitted
  NAS-ID profile is not configured
```

After users pass authentication, display MAC authentication information. Verify that port Ten-GigabitEthernet 1/0/1 allows multiple MAC authentication users to be authenticated.

```
[Device] display mac-authentication interface ten-gigabitethernet 1/0/1
Global MAC authentication parameters:
  MAC authentication     : Enabled
  User name format       : MAC address in uppercase(XX-XX-XX-XX-XX-XX)
          Username       : mac
          Password       : Not configured
  Offline detect period  : 60 s
  Quiet period           : 5 s
  Server timeout         : 100 s
  Reauth period          : 3600 s
  Authentication domain  : sun
Max MAC-auth users       : 4294967295 per slot
Online MAC-auth users    : 3

Silent MAC users:
         MAC address       VLAN ID  From port              Port index

Ten-GigabitEthernet1/0/1  is link-up
  MAC authentication         : Enabled
  Carry User-IP              : Disabled
  Authentication domain      : Not configured
  Auth-delay timer           : Disabled
  Periodic reauth            : Disabled
  Re-auth server-unreachable : Logoff
  Guest VLAN                 : Not configured
  Guest VLAN auth-period     : 30 s
```

```
   Critical VLAN              : Not configured
   Critical voice VLAN        : Disabled
   Host mode                  : Single VLAN
   Offline detection          : Enabled
   Authentication order       : Default

   Max online users           : 4294967295
   Authentication attempts    : successful 3, failed 7
   Current online users       : 3
          MAC address       Auth state
    1234-0300-0011   authenticated
    1234-0300-0012   authenticated
    1234-0300-0013   authenticated
```

Display 802.1X authentication information. Verify that Ten-GigabitEthernet 1/0/1 allows only one 802.1X user to be authenticated.

```
[Device] display dot1x interface ten-gigabitethernet 1/0/1
Global 802.1X parameters:
   802.1X authentication  : Enabled
   CHAP authentication    : Enabled
   Max-tx period          : 30 s
   Handshake period       : 15 s
   Quiet timer            : Disabled
       Quiet period       : 60 s
   Supp timeout           : 30 s
   Server timeout         : 100 s
   Reauth period          : 3600 s
   Max auth requests      : 2
   EAD assistant function : Disabled
       EAD timeout        : 30 min
   Domain delimiter       : @
 Max 802.1X users         : 4294967295 per slot
 Online 802.1X users      : 1

GigabitEthernet1/0/1  is link-up
   802.1X authentication      : Enabled
   Handshake                  : Enabled
   Handshake reply            : Disabled
   Handshake security         : Disabled
   Unicast trigger            : Disabled
   Periodic reauth            : Disabled
   Port role                  : Authenticator
   Authorization mode         : Auto
   Port access control        : MAC-based
   Multicast trigger          : Enabled
   Mandatory auth domain      : Not configured
   Guest VLAN                 : Not configured
   Auth-Fail VLAN             : Not configured
   Critical VLAN              : Not configured
```

```
Critical voice VLAN        : Disabled
Re-auth server-unreachable : Logoff
Max online users           : 4294967295
Send Packets Without Tag   : Disabled
Add Guest VLAN delay       : Disabled
Reauth period              : 3600 s

EAPOL packets: Tx 16331, Rx 102
Sent EAP Request/Identity packets : 16316
     EAP Request/Challenge packets: 6
     EAP Success packets: 4
     EAP Failure packets: 5
Received EAPOL Start packets : 6
         EAPOL LogOff packets: 2
         EAP Response/Identity packets : 80
         EAP Response/Challenge packets: 6
         Error packets: 0
Online 802.1X users: 1
```

Verify that frames with an unknown destination MAC address, multicast address, or broadcast address are discarded. (Details not shown.)

Troubleshooting port security

Cannot set the port security mode

Symptom

Cannot set the port security mode for a port.

Analysis

For a port operating in a port security mode other than noRestrictions, you cannot change the port security mode by using the **port-security port-mode** command.

Solution

To resolve the issue:

1. Set the port security mode to noRestrictions.
   ```
   [Device-Ten-GigabitEthernet1/0/1] undo port-security port-mode
   ```
2. Set a new port security mode for the port, for example, autoLearn.
   ```
   [Device-Ten-GigabitEthernet1/0/1] port-security port-mode autolearn
   ```
3. If the issue persists, contact H3C Support.

Cannot configure secure MAC addresses

Symptom

Cannot configure secure MAC addresses.

Analysis

No secure MAC address can be configured on a port operating in a port security mode other than autoLearn.

Solution

To resolve the issue:

1. Set the port security mode to autoLearn.

```
[Device-Ten-GigabitEthernet1/0/1] undo port-security port-mode
[Device-Ten-GigabitEthernet1/0/1] port-security max-mac-count 64
[Device-Ten-GigabitEthernet1/0/1] port-security port-mode autolearn
[Device-Ten-GigabitEthernet1/0/1] port-security mac-address security 1-1-2 vlan 1
```

2. If the issue persists, contact H3C Support.