

Contents

Introduction	1
Prerequisites	1
General restrictions and guidelines	1
Example: Configuring autoLearn mode	2
Network configuration	2
Applicable hardware and software versions.....	2
Restrictions and guidelines	4
Procedures	4
Verifying the configuration	5
Configuration files	6
Example: Configuring userLoginWithOUI mode	7
Network configuration	7
Applicable hardware and software versions.....	7
Procedures	9
Configuring the RADIUS server.....	9
Configuring the device.....	12
Verifying the configuration	13
Configuration files	16
Example: Configuring macAddressElseUserLoginSecure mode	17
Network configuration	17
Applicable hardware and software versions.....	18
Procedures	20
Configuring the RADIUS server.....	20
Configuring the device.....	22
Verifying the configuration	23
Configuration files	27
Example: Configuring port security to support redirect URL assignment by a ClearPass RADIUS server	28
Network configuration	28
Applicable hardware and software versions.....	28
Prerequisites	30
Procedures	31
Configuring the ClearPass RADIUS server.....	31
Configuring the device.....	32
Verifying the configuration	33
Configuration files	37

Introduction

This document provides port security configuration examples.

Port security combines and extends 802.1X and MAC authentication to provide MAC-based network access control. The feature 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.

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.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of port security.

General restrictions and guidelines

When you configure port security, follow these restrictions and guidelines:

- Disable global 802.1X and MAC authentications before you enable port security on a port.
- Port security automatically modifies the following 802.1X or MAC authentication settings for different security modes:
 - The status of 802.1X and MAC authentication.
 - The 802.1X access control method.
 - The 802.1X port authorization state.
- Disabling port security on a port will log off all online users on that port.
- Port security modes are mutually exclusive with link aggregation and service loopback group.
- 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.

- To change the security mode of a port security-enabled port, you must use the **undo port-security port-mode** command to set the port in noRestrictions mode first.

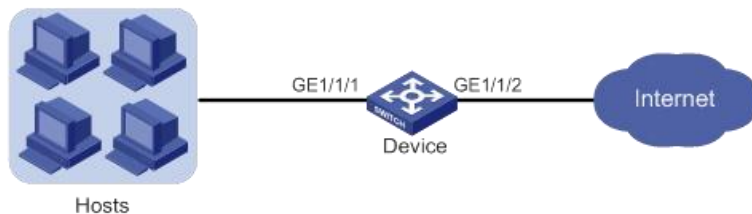
Example: Configuring autoLearn mode

Network configuration

As shown in [Figure 1](#):

- Configure port security mode **autoLearn** on GigabitEthernet 1/0/1 to allow users to access the network without authentication.
- Configure the port to accept a maximum of 64 users (secure MAC addresses) to access the network. After the number of secure MAC addresses reaches 64, the port stops learning secure MAC addresses and no new user can access the network.
- To prevent inactive users from using secure MAC address entries, configure a secure MAC address aging timer.
- Configure GigabitEthernet 1/0/1 to shut down temporarily for 30 seconds when a new user accesses the network after the number of secure MAC addresses reaches 64.

Figure 1 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
SC 3570 switch series	Release 11xx
SC 5525 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
SC 5520 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
SC 3170 switch series	Release 11xx
SC 3130 switch series	Release 63xx

Restrictions and guidelines

Before you enable the autoLearn mode, you must set the maximum number of secure MAC addresses that port security allows on the port (by using the `port-security max-mac-count` command). You cannot change the setting after the port is set to the **autoLearn** mode.

Procedures

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 GigabitEthernet 1/0/1.
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port-security max-mac-count 64
# Set the port security mode to autoLearn.
[Device-GigabitEthernet1/0/1] port-security port-mode autolearn
# Specify the intrusion protection action as disableport-temporarily.
[Device-GigabitEthernet1/0/1] port-security intrusion-mode disableport-temporarily
[Device-GigabitEthernet1/0/1] quit
# Configure the port to be silent for 30 seconds after the intrusion protection feature is triggered.
[Device] port-security timer disableport 30
```

Verifying the configuration

Verify that port security is correctly configured.

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

Global port security parameters:

```
Port security           : Enabled
AutoLearn aging time    : 30 min
Disableport timeout     : 30 s
Blockmac timeout        : 180 s
MAC move                 : Denied
Authorization fail       : Online
NAS-ID profile           : 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
Open authentication     : Disabled
Traffic-statistics      : Disabled
OUI value list          :
```

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            : Not configured
Free VLANs               : Not configured
Open authentication       : Disabled
MAC-move VLAN check bypass : Disabled
```

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

Display information about the learned MAC addresses.

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

```
[Device-GigabitEthernet1/0/1] display this
```

```
#
```

```
interface GigabitEthernet1/0/1
```

```
port link-mode bridge
```

```

port-security intrusion-mode disableport-temporarily
port-security max-mac-count 64
port-security port-mode autolearn
port-security mac-address security sticky 00e0-fc00-5920 vlan 1
port-security mac-address security sticky 00e0-fc00-592a vlan 1
port-security mac-address security sticky 00e0-fc00-592b vlan 1
port-security mac-address security sticky 00e0-fc00-592c vlan 1
port-security mac-address security sticky 00e0-fc00-592d vlan 1
#
# 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 gigabitethernet 1/0/1
# Verify that the port is disabled after it receives a frame with an unknown MAC address.
[Device] display interface gigabitethernet 1/0/1
# Verify that the interface is re-enabled after 30 seconds.
[Device] display interface gigabitethernet 1/0/1
# Delete several secure MAC addresses.
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] undo port-security mac-address security sticky
00e0-fc00-5920 vlan 1
[Device-GigabitEthernet1/0/1] undo port-security mac-address security sticky
00e0-fc00-592a vlan 1
...
# Verify that the port security mode changes to autoLearn and the port can learn MAC addresses
again. (Details not shown.)

```

Configuration files

IMPORTANT:

Support for the **port link-mode bridge** command depends on the device model.

```

#
port-security enable
port-security timer disableport 30
port-security timer autolearn aging 30
#
interface GigabitEthernet1/0/1
port link-mode bridge
port-security intrusion-mode disableport-temporarily
port-security max-mac-count 64
port-security port-mode autolearn
#

```

Example: Configuring userLoginWithOUI mode

Network configuration

As shown in [Figure 2](#):

- An 802.1X user on a host and a printer are attached to port GigabitEthernet 1/0/1 on the device.
- The device uses a RADIUS server (INC in this example) to perform authentication, authorization, and accounting for all users in ISP domain **sun**.
- The device and the server use the shared key **expert** for secure RADIUS communication.

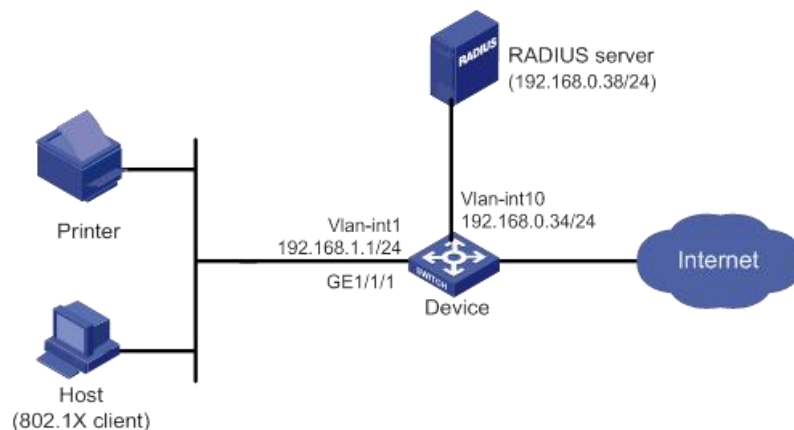
Configure port security mode **userLoginWithOUI** on port GigabitEthernet 1/0/1 to meet the following requirements:

- Permit only one 802.1X user to pass authentication.
- Permit the printer to access the Internet.

For the printer to pass authentication, add its OUI to the OUI list of port security.

Configure the **blockmac** intrusion protection action on GigabitEthernet 1/0/1, so the device adds the source MAC addresses of illegal frames to the blocked MAC address list. The device discards all frames sourced from the blocked MAC addresses.

Figure 2 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
SC 3570 switch series	Release 11xx
SC 5525 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
SC 5520 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
SC 3170 switch series	Release 11xx
SC 3130 switch series	Release 63xx

Procedures

Configuring the RADIUS server

This example uses INC PLAT 7.0 (E0201) and INC UAM 7.0 (E0201) to describe the procedure.

1. Add the device to INC as an access device:
 - a. Click the **User** tab.
 - b. From the navigation tree, select **User Access Policy > Access Device Management > Access Device**.
 - c. Click **Add**.
The **Add Access Device** page opens.

- d. In the **Access Configuration** area, configure the following parameters:
 - Enter **1812** in the **Authentication Port** field, and enter **1813** in the **Accounting Port** field.
 - Select **LAN Access Service** from the **Service Type** list.
 - Select **HP(Comware)** from the **Access Device Type** list.
 - Enter **expert** in the **Shared Key** and **Confirm Shared Key** field.
 - Use the default values for other parameters.
- e. In the **Device List** area, click **Select** or **Add Manually** to add the device at **192.168.0.34** as an access device.
 You must specify the source IP address of outgoing RADIUS packets on the device as the IP address of the access device on the server.
 On the device, the source IP address is configured by using the **nas-ip** or **radius nas-ip** command. The IP address configured by using the **nas-ip** command has a higher priority than the IP address configured by using the **radius nas-ip** command. If no IP address is specified as the source IP address, the IP address of the packet outbound interface is used as the source IP address. In this example, the IP address of the packet outbound interface is used, which is 192.168.0.34.
- f. Click **OK**.

Figure 3 Adding the device as an access device

User > User Access Policy > Access Device Management > Access Device > Add Access Device ? Help

Access Configuration

Authentication Port * <input type="text" value="1812"/>	Accounting Port * <input type="text" value="1813"/>
RADIUS Accounting <input type="text" value="Fully Supported"/>	Service Type <input type="text" value="LAN Access Service"/>
Access Device Type <input type="text" value="HP(Comware)"/>	Access Device Group <input type="text" value="--"/>
Shared Key * <input type="text" value="*****"/>	Confirm Shared Key * <input type="text" value="*****"/>
Service Group <input type="text" value="Ungrouped"/>	

Device List

Select
Add Manually
Clear All

Device Name	Device IP	Device Model	Comments	Delete
	192.168.0.34			

Total Items: 1.

OK
Cancel

2. Add an access policy:
 - a. Click the **User** tab.
 - b. From the navigation tree, select **User Access Policy > Access Policy**.
 - c. Click **Add**.
 - d. On the page that opens, configure the following parameters, as shown in [Figure 4](#):
 - Enter **802.1X-auth** in the **Access Policy Name** field.
 - Use the default values for other parameters.

Figure 4 Adding an access policy

User > User Access Policy > Access Policy > Add Access Policy

Basic Information

Access Policy Name * 802.1X-auth

Service Group * Ungrouped

Description

Authorization Information

Access Period None

Allocate IP * No

Downstream Rate(Kbps)

Upstream Rate(Kbps)

Priority

☐ RSA Authentication

Certificate Authentication ☒ None ☐ EAP

Certificate Type EAP-TLS AuthN

Deploy VLAN

☐ Deploy User Profile

☐ Deploy ACL

Deploy User Group

- e. Click **OK**.
3. Add an access service:
 - a. Click the **User** tab.
 - b. From the navigation tree, select **User Access Policy > Access Service**.
 - c. Click **Add**.
 - d. On the page that opens, configure the following parameters, as shown in Figure 5:
 - Enter **802.1X-auth** in the **Service Name** field.
 - Select **802.1X-auth** from the **Default Access Policy** list.

Figure 5 Adding an access service

User > User Access Policy > Access Service > Add Access Service

Basic Information

Service Name * 802.1X-auth

Service Suffix

Service Group * Ungrouped

Default Access Policy * 802.1X-auth

Default Proprietary Attribute Assignment Policy * Do not use

Default BYOD Page * PC - Default Page

Description

☒ Available

☐ Transparent Authentication on Portal Endpoints

Access Scenario List

Add

Access Scenario	Access Policy	Proprietary Attribute Assignment Policy	BYOD Page	Priority	Modify	Delete
No match found.						

OK Cancel

- e. Click **OK**.
4. Add an access user:
 - a. Click the **User** tab.
 - b. From the navigation tree, select **Access User Management > All Access Users**.
 - c. Click **Add**.
 - d. On the **Add Access User** page, configure the following parameters, as shown in Figure 6:
 - Click **Select** or **Add User** to associate the user with INC Platform user **hello**.
 - Enter **802.1X** in the **Account Name** field.
 - Enter **123456TESTplat&!** in the **Password** and **Confirm Password** fields.

- Configure other parameters in the **Access Information** area as needed.
- Select **802.1X-auth** from the **Access Service** list.

Figure 6 Adding an access user account

User > All Access Users > Add Access User

Access account

Access Information

User Name *

Account Name *

☐ Trial Account ☐ Default BYOD User ☐ Computer User ☐ Fast Access User

Password * Confirm Password *

☒ Allow User to Change Password ☐ Enable Password Strategy ☐ Modify Password at Next Login

Inspiration Time Expiration Time

Max. Idle Time(Minutes) Max. Concurrent Logins

Max. Smart Device Bindings for Portal

Login Message

Access Service

Service Name	Service Suffix	Status	Allocate IP
<input checked="" type="checkbox"/> 802.1X-auth		Available	

- e. Click **OK**.

Configuring the device

The following procedure contains RADIUS commands. For more information about RADIUS commands, see AAA commands in the security command reference for the device.

1. Assign an IP address to each interface, as shown in [Figure 2](#). Make sure the host, printer, device, and RADIUS server can reach each other. (Details not shown.)
2. Configure the RADIUS scheme:

Create RADIUS scheme **radsum**.

```
<Device> system-view
[Device] radius scheme radsum
New RADIUS scheme.
```

Specify the server at 192.168.0.38 as the primary RADIUS authentication server.

```
[Device-radius-radsun] primary authentication 192.168.0.38
```

Specify the server at 192.168.0.38 as the primary RADIUS accounting server.

```
[Device-radius-radsun] primary accounting 192.168.0.38
```

Set the authentication shared key to **expert** in plain text for secure communication between the device and the RADIUS server.

```
[Device-radius-radsun] key authentication simple expert
```

Set the accounting shared key to **expert** in plain text for secure communication between the device and the RADIUS server.

```
[Device-radius-radsun] key accounting simple expert
```

Set the response timeout time of the RADIUS server to 5 seconds.

```
[Device-radius-radsun] timer response-timeout 5
```

Set the maximum number of RADIUS packet retransmission attempts to 5.

```
[Device-radius-radsun] retry 5
```

Set the real-time accounting interval to 15 minutes.

```
[Device-radius-radsun] timer realtime-accounting 15
```

- ```
Exclude domain names from the usernames sent to the RADIUS server.
[Device-radius-radsun] user-name-format without-domain
[Device-radius-radsun] quit

Create ISP domain sun and enter ISP domain view.
[Device] domain sun

Configure ISP domain sun to use RADIUS scheme radsun for authentication, authorization,
and accounting of all LAN users.
[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

Configure domain sun as the default domain.
[Device] domain default enable sun
```
3. Set the 802.1X authentication method to CHAP. By default, the authentication method for 802.1X is CHAP.
- ```
[Device] dot1x authentication-method chap
```
4. Configure port security:
- ```
Add five OUI values, including the OUI of the printer. You can add a maximum of 16 OUI
values. If the MAC address of a user matches one of the OUIs, the device will allow the user to
pass authentication. Each port can permit only one OUI user 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 gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port-security port-mode userlogin-withoui

Configure port GigabitEthernet 1/0/1 to perform the blockmac intrusion protection action.
[Device-GigabitEthernet1/0/1] port-security intrusion-mode blockmac
[Device-GigabitEthernet1/0/1] quit

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

## Verifying the configuration

# Display RADIUS scheme **radsun**.

In Release 63xx:

```
[Device] display radius scheme radsun
Total 1 RADIUS schemes
```

```

RADIUS scheme name: radsun
Index: 0
Primary authentication server:
Host name: Not configured
IP : 192.168.0.38 Port: 1812
VPN : Not configured
```

```

State: Active
Test profile: Not configured
Weight: 0
Primary accounting server:
 Host name: Not configured
 IP : 192.168.0.38 Port: 1813
 VPN : Not configured
 State: Active
 Weight: 0
Accounting-On function : Disabled
 extended 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(seconds) : 900
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
Attribute 25 : Standard
Attribute Remanent-Volume unit : Kilo
server-load-sharing : Disabled
Attribute 31 MAC format : HH-HH-HH-HH-HH-HH
Stop-accounting-packet send-force : Disabled
Reauthentication server selection : Reselect

```

---

### In Release 65xx:

```

[Device] display radius scheme radsun
Total 1 RADIUS schemes

```

---

```

RADIUS scheme name: radsun

```

```

Index: 0
Primary authentication server:
 Host name: Not configured
 IP : 192.168.0.38 Port: 1812
 VPN : Not configured
 State: Active
 Test profile: Not configured
 Weight: 0
Primary accounting server:

```

```

Host name: Not configured
IP : 192.168.0.38 Port: 1813
VPN : Not configured
State: Active
Weight: 0
Accounting-On function : Disabled
 extended 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(seconds) : 900
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
Attribute 25 : Standard
Attribute Remanent-Volume unit : Kilo
server-load-sharing : Disabled
Attribute 30 format : HH-HH-HH-HH-HH-HH:SSID
Attribute 30 MAC format : HH-HH-HH-HH-HH-HH
Attribute 31 MAC format : HH-HH-HH-HH-HH-HH
Stop-accounting-packet send-force : Disabled
Reauthentication server selection : Reselect
Attribute 218 of vendor ID 25506 : DHCP-Option 61
 Format 1 (1-byte Type field)

```

#### # Display the port security configuration on GigabitEthernet 1/0/1.

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

```
Global port security parameters:
```

```

Port security : Enabled
AutoLearn aging time : 0 min
Disableport timeout : 20 s
Blockmac timeout : 180 s
MAC move : Denied
Authorization fail : Online
NAS-ID profile : 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
Open authentication : Disabled
Traffic-statistics : Disabled
OUI value list :
 Index : 1 Value : 123401
 Index : 2 Value : 123402
 Index : 3 Value : 123403
 Index : 4 Value : 123404
 Index : 5 Value : 123405

```

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 : 0
Authorization : Permitted
NAS-ID profile : Not configured
Free VLANs : Not configured
Open authentication : Disabled
MAC-move VLAN check bypass : Disabled

```

After the 802.1X user comes online, the number of secure MAC addresses on the port is 1.

# Display 802.1X information.

```
[Device] display dot1x interface gigabitethernet 1/0/1
```

# Verify that GigabitEthernet 1/0/1 allows a user whose MAC address has an OUI from the specified OUIs to pass authentication.

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

| MAC Address    | VLAN ID | State   | Port/NickName | Aging |
|----------------|---------|---------|---------------|-------|
| 1234-0300-0011 | 1       | Learned | XGE1/0/1      | Y     |

## Configuration files

I

### IMPORTANT:

Support for the **port link-mode bridge** command depends on the device model.

#

```

port-security enable
port-security oui index 1 mac-address 1234-0100-0000
port-security oui index 2 mac-address 1234-0200-0000
port-security oui index 3 mac-address 1234-0300-0000
port-security oui index 4 mac-address 1234-0400-0000
port-security oui index 5 mac-address 1234-0500-0000

```

```
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port-security port-mode userlogin-withoutui
 port-security intrusion-mode blockmac
#
radius scheme radsun
 primary authentication 192.168.0.38
 primary accounting 192.168.0.38
 key authentication cipher c3$s9TAYm34R8sS5k/Cylg2sDm69ZRupMvGJg==
 key accounting cipher c3$UaUPGk8AfZAQLHF1bKNcEoM2HXGiuWowBQ==
 retry 5
 timer response-timeout 5
 timer realtime-accounting 15
 user-name-format without-domain
#
domain sun
 authentication lan-access radius-scheme radsun
 authorization lan-access radius-scheme radsun
 accounting lan-access radius-scheme radsun
#
domain default enable sun
#
```

## Example: Configuring macAddressElseUserLoginSecure mode

### Network configuration

As shown in [Figure 7](#):

- Users on hosts are attached to port GigabitEthernet 1/0/1 on the device.
- All MAC authentication users use a shared user account with username **aaa** and password **123456TESTplat&!**.
- The device uses a RADIUS server (INC in this example) to perform authentication, authorization, and accounting for all users in domain **sun**.
- The device and the server use shared key **expert** for secure RADIUS communication.

Configure port security mode **macAddressElseUserLoginSecure** on port GigabitEthernet 1/0/1 to meet the following requirements:

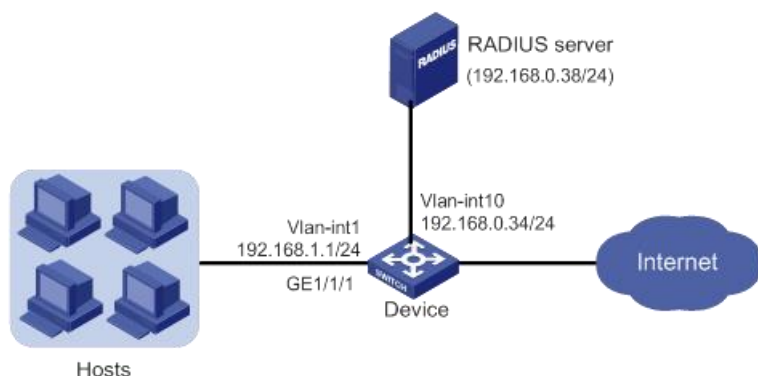
- Allow only one 802.1X user to pass authentication, and allow multiple MAC authentication users to pass authentication.
- MAC authentication has a higher priority than 802.1X authentication. For an 802.1X user, the device initiates MAC authentication first, and then 802.1X authentication if the user fails MAC authentication. For a MAC authentication user, the device initiates only MAC authentication.

Configure port GigabitEthernet 1/0/1 to accept a maximum of 64 authenticated users.

Set the NTK mode to **ntkonly** mode on port GigabitEthernet 1/0/1 to prevent outbound frames from being sent to unknown MAC addresses.



**Figure 7 Network diagram**



## Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

| Hardware              | Software version                                             |
|-----------------------|--------------------------------------------------------------|
| SC 3570 switch series | Release 11xx                                                 |
| SC 5525 switch series | Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx |
| SC 5520 switch series | Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx |
| SC 3170 switch series | Release 11xx                                                 |
| SC 3130 switch series | Release 63xx                                                 |

# Procedures

## Configuring the RADIUS server

This example uses INC PLAT 7.0 (E0201) and INC UAM 7.0 (E0201) to describe the procedure.

1. Add the device to INC as an access device in the same way the device is added to INC in "[Example: Configuring userLoginWithOUI mode.](#)"
2. Add an access policy, an access service, and an access user for 802.1X authentication in the same way they are added in "[Example: Configuring userLoginWithOUI mode.](#)"
3. Add an access policy for MAC authentication:
  - a. Click the **User** tab.
  - b. From the navigation tree, select **User Access Policy > Access Policy**.
  - c. Click **Add**.
  - d. On the page that opens, configure the following parameters, as shown in [Figure 8](#):
    - Enter **MAC-auth** in the **Access Policy Name** field.
    - Use the default values for other parameters.

**Figure 8 Adding an access policy**

User > User Access Policy > Access Policy > Add Access Policy

| Basic Information    |           |
|----------------------|-----------|
| Access Policy Name * | MAC-auth  |
| Service Group *      | Ungrouped |
| Description          |           |

| Authorization Information                    |                                                                 |                                             |    |
|----------------------------------------------|-----------------------------------------------------------------|---------------------------------------------|----|
| Access Period                                | None ?                                                          | Allocate IP *                               | No |
| Downstream Rate(Kbps)                        |                                                                 | Upstream Rate(Kbps)                         |    |
| Priority                                     |                                                                 | <input type="checkbox"/> RSA Authentication |    |
| Certificate Authentication                   | <input checked="" type="radio"/> None <input type="radio"/> EAP |                                             |    |
| Certificate Type                             | EAP-TLS AuthN                                                   |                                             |    |
| Deploy VLAN                                  |                                                                 |                                             |    |
| <input type="checkbox"/> Deploy User Profile |                                                                 | Deploy User Group                           | ?  |
| <input type="checkbox"/> Deploy ACL          |                                                                 |                                             |    |

- e. Click **OK**.
4. Add an access service for MAC authentication:

- a. Click the **User** tab.
- b. From the navigation tree, select **User Access Policy > Access Service**.
- c. Click **Add**.
- d. On the page that opens, configure the following parameters, as shown in [Figure 9](#):
  - Enter **MAC-auth** in the **Service Name** field.
  - Select **MAC-auth** from the **Default Access Policy** list.

**Figure 9 Adding an access service**

The screenshot displays the 'Add Access Service' configuration interface. The 'Basic Information' section includes the following fields and values:

- Service Name \***: MAC-auth
- Service Suffix**: (empty)
- Service Group \***: Ungrouped
- Default Access Policy**: MAC-auth
- Default Proprietary Attribute Assignment Policy \***: Do not use
- Default BYOD Page \***: PC - Default Page
- Description**: (empty)
- Available**: ☒
- Transparent Authentication on Portal Endpoints**: ☐

The 'Access Scenario List' section features an 'Add' button and a table with the following columns: Access Scenario, Access Policy, Proprietary Attribute Assignment Policy, BYOD Page, Priority, Modify, and Delete. The table currently contains the text 'No match found.' At the bottom of the form are 'OK' and 'Cancel' buttons.

- e. Click **OK**.
5. Add an access user for MAC authentication:
    - a. Click the **User** tab.
    - b. From the navigation tree, select **Access User Management > All Access Users**.
    - c. Click **Add**.
    - d. On the **Add Access User** page, configure the following parameters, as shown in [Figure 10](#):
      - Click **Select** or **Add User** to associate the user with INC Platform user **hello2**.
      - Enter **aaa** in the **Account Name** field.
      - Enter **123456TESTplat&!** in the **Password** and **Confirm Password** fields.
      - Configure other parameters in the **Access Information** area as needed.
      - Select **MAC-auth** from the **Access Service** list.

**Figure 10 Adding an access user account**

User > All Access Users > Add Access User

Access account

Access Information

User Name \*

Account Name \*

☐ Trial Account ☐ Default BYOD User ☐ Computer User ☐ Fast Access User

Password \*  Confirm Password \*

☒ Allow User to Change Password ☐ Enable Password Strategy ☐ Modify Password at Next Login

Inspiration Time   Expiration Time

Max. Idle Time(Minutes)  Max. Concurrent Logins

Max. Smart Device Bindings for Portal

Login Message

Access Service

| Service Name                                 | Service Suffix | Status    | Allocate IP |
|----------------------------------------------|----------------|-----------|-------------|
| <input type="checkbox"/> 802.1X-auth         |                | Available |             |
| <input checked="" type="checkbox"/> MAC-auth |                | Available |             |

e. Click **OK**.

## Configuring the device

1. Assign an IP address to each interface, as shown in [Figure 7](#). Make sure the hosts, device, and RADIUS server can reach each other. (Details not shown.)
2. Configure the RADIUS scheme:

# Create RADIUS scheme **radsun**.

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

```
[Device] radius scheme radsun
```

New RADIUS scheme.

# Specify the server at 192.168.0.38 as the primary RADIUS authentication server.

```
[Device-radius-radsun] primary authentication 192.168.0.38
```

# Specify the server at 192.168.0.38 as the primary RADIUS accounting server.

```
[Device-radius-radsun] primary accounting 192.168.0.38
```

# Set the authentication shared key to **expert** in plain text for secure communication between the device and the RADIUS server.

```
[Device-radius-radsun] key authentication simple expert
```

# Set the accounting shared key to **expert** in plain text for secure communication between the device and the RADIUS server.

```
[Device-radius-radsun] key accounting simple expert
```

# Set the response timeout time of the RADIUS server to 5 seconds.

```
[Device-radius-radsun] timer response-timeout 5
```

# Set the maximum number of RADIUS packet retransmission attempts to 5.

```
[Device-radius-radsun] retry 5
```

# Set the real-time accounting interval to 15 minutes.

```
[Device-radius-radsun] timer realtime-accounting 15
```

# Exclude domain names from the usernames sent to the RADIUS server.

```
[Device-radius-radsun] user-name-format without-domain
```

```
[Device-radius-radsun] quit
```

- ```
# Create ISP domain sun and enter ISP domain view.
[Device] domain sun

# Configure ISP domain sun to use RADIUS scheme radsun for authentication, authorization,
and accounting of all LAN users.
[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

# Specify ISP domain sun as the default domain.
[Device] domain default enable sun
```
3. Configure MAC authentication:
- ```
Configure a shared account for MAC authentication users, and set the username to aaa and
password to plaintext string of 123456TESTplat&!.
[Device] mac-authentication user-name-format fixed account aaa password simple
123456TESTplat&!

Specify domain sun as the global MAC authentication domain.
[Device] mac-authentication domain sun
```
4. Set the 802.1X authentication method to CHAP. By default, the authentication method for 802.1X is CHAP.
- ```
[Device] dot1x authentication-method chap
```
5. Configure port security:
- ```
Set port security's limit on the number of secure MAC addresses to 64 on GigabitEthernet
1/0/1.
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port-security max-mac-count 64

Set the port security mode to macAddressElseUserLoginSecure.
[Device-GigabitEthernet1/0/1] port-security port-mode mac-else-userlogin-secure

Set the NTK mode of the port to ntkonly.
[Device-GigabitEthernet1/0/1] port-security ntk-mode ntkonly
[Device-GigabitEthernet1/0/1] quit

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

## Verifying the configuration

```
Verify that port security is correctly configured.
[Device] display port-security interface gigabitethernet 1/0/1
Global port security parameters:
 Port security : Enabled
 AutoLearn aging time : 30 min
 Disableport timeout : 30 s
 Blockmac timeout : 180 s
 MAC move : Denied
 Authorization fail : Online
 NAS-ID profile : 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
Open authentication : Disabled
Traffic-statistics : Disabled
OUI value list :

```

GigabitEthernet1/0/1 is link-up

```

Port mode : macAddressElseUserLoginSecure
NeedToKnow mode : NeedToKnowOnly
Intrusion protection mode : DisablePortTemporarily
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 : Not configured
Free VLANs : Not configured
Open authentication : Disabled
MAC-move VLAN check bypass : Disabled

```

**# Verify that port GigabitEthernet 1/0/1 allows multiple MAC authentication users to be authenticated.**

[Device] display mac-authentication interface gigabitethernet 1/0/1

Global MAC authentication parameters:

```

MAC authentication : Enabled
Authentication method : PAP
Username format : Fixed account
 Username : aaa
 Password : *****
MAC range accounts 0
 MAC address Mask Username
Offline detect period : 300 s
Quiet period : 60 s
Server timeout : 100 s
Reauth period : 3600 s
User aging period for critical VLAN : 1000 s
User aging period for critical VSI : 1000 s
User aging period for guest VLAN : 1000 s
User aging period for guest VSI : 1000 s
Authentication domain : sun
HTTP proxy port list : Not configured
HTTPS proxy port list : Not configured
Online MAC-auth wired user : 3

```

Silent MAC users:

| MAC address | VLAN ID | From port | Port index |
|-------------|---------|-----------|------------|
|-------------|---------|-----------|------------|

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
Critical VLAN : Not configured
Critical voice VLAN : Disabled
Host mode : Single VLAN
Offline detection : Enabled
Authentication order : Default
User aging : Enabled
Server-recovery online-user-sync : Enabled

Guest VSI : Not configured
Guest VSI auth-period : 30 s
Critical VSI : Not configured
Auto-tag feature : Disabled
VLAN tag configuration ignoring : Disabled
Max online users : 4294967295
Authentication attempts : successful 0, failed 0
Current online users : 3

 MAC address Auth state
 1234-0300-0011 authenticated
 1234-0300-0012 authenticated
 1234-0300-0013 authenticated

```

**# Verify that GigabitEthernet 1/0/1 allows only one 802.1X user to be authenticated.**

[Device] display dot1x interface gigabitethernet 1/0/1

Global 802.1X parameters:

```

802.1X authentication : Enabled
CHAP authentication : Enabled
Max-tx period : 30 s
Handshake period : 15 s
Offline detect period : 300 s
Quiet timer : Disabled
 Quiet period : 60 s
Supp timeout : 30 s
Server timeout : 100 s
Reauth period : 3600 s
Max auth requests : 2
User aging period for Auth-Fail VLAN : 1000 s
User aging period for Auth-Fail VSI : 1000 s
User aging period for critical VLAN : 1000 s

```

```

User aging period for critical VSI : 1000 s
User aging period for guest VLAN : 1000 s
User aging period for guest VSI : 1000 s
EAD assistant function : Disabled
 EAD timeout : 30 min
Domain delimiter : @
Online 802.1X wired users : 1

```

GigabitEthernet1/0/1 is link-up

```

802.1X authentication : Enabled
Handshake : Enabled
Handshake reply : Disabled
Handshake security : Disabled
Offline detection : 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
Add Guest VLAN delay : Disabled
Re-auth server-unreachable : Logoff
Max online users : 4294967295
User IP freezing : Disabled
Reauth period : 0 s
Send Packets Without Tag : Disabled
Max Attempts Fail Number : 0
Guest VSI : Not configured
Auth-Fail VSI : Not configured
Critical VSI : Not configured
Add Guest VSI delay : Disabled
User aging : Enabled
Server-recovery online-user-sync : Enabled
Auth-Fail EAPOL : Disabled
Critical EAPOL : Disabled

```

EAPOL packets: Tx 0, Rx 0

Sent EAP Request/Identity packets : 0

EAP Request/Challenge packets: 0

EAP Success packets: 0

EAP Failure packets: 0

Received EAPOL Start packets : 0

EAPOL LogOff packets: 0



```
EAP Response/Identity packets : 0
EAP Response/Challenge packets: 0
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.)
```

## Configuration files

---

### IMPORTANT:

Support for the **port link-mode bridge** command depends on the device model.

---

```
#
mac-authentication domain sun
mac-authentication user-name-format fixed account aaa password cipher c3$HAlQ
nyXOWZXTgiOBPd7+kSPClKm7JbZlRw==
#
port-security enable
#
interface GigabitEthernet1/0/1
port link-mode bridge
port-security ntk-mode ntkonly
port-security max-mac-count 64
port-security port-mode mac-else-userlogin-secure
#
radius scheme radsun
primary authentication 192.168.0.38
primary accounting 192.168.0.38
key authentication cipher c3$s9TAYm34R8sS5k/Cylg2sDm69ZRupMvGJg==
key accounting cipher c3$UaUPGk8AfZAQLHFlbKNcEoM2HXGiuWowBQ==
retry 5
timer response-timeout 5
timer realtime-accounting 15
user-name-format without-domain
#
domain sun
authentication lan-access radius-scheme radsun
authorization lan-access radius-scheme radsun
accounting lan-access radius-scheme radsun
#
domain default enable sun
#
```

# Example: Configuring port security to support redirect URL assignment by a ClearPass RADIUS server

## Network configuration

As shown in [Figure 11](#):

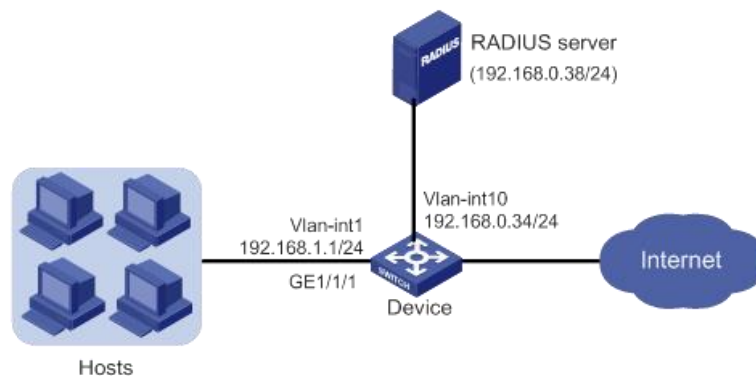
- Users on hosts are attached to port GigabitEthernet 1/0/1 on the device. All MAC authentication users use a shared user account with username **dot1x** and password **Abc123!**.
- The device acts as the NAS and a ClearPass RADIUS server performs remote authentication, authorization, and accounting for all users in domain **sun**. If a user passes authentication, the ClearPass server assigns a redirect URL to that user for Web authentication.

Configure port security mode **macAddressElseUserLoginSecureExt** on port GigabitEthernet 1/0/1 to meet the following requirements:

- Allow multiple 802.1X users and MAC authentication users to pass authentication.
- MAC authentication has a higher priority than 802.1X authentication. For an 802.1X user, the device initiates MAC authentication first, and then 802.1X authentication if the user fails MAC authentication. For a MAC authentication user, the device initiates only MAC authentication.

Set the NTK mode to **ntkonly** mode on GigabitEthernet 1/0/1 to prevent outbound frames from being sent to unknown MAC addresses.

**Figure 11 Network diagram**



## Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

| Hardware              | Software version                                             |
|-----------------------|--------------------------------------------------------------|
| SC 3570 switch series | Release 11xx                                                 |
| SC 5525 switch series | Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx |
| SC 5520 switch series | Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx |
| SC 3170 switch series | Release 11xx                                                 |
| SC 3130 switch series | Release 63xx                                                 |

## Prerequisites

Install ClearPass Policy Manager on an ESX/ESXi Virtual Machine and set up the ClearPass server, including: importing CPPM-VM-x86\_64-6.5.0.71095-ESX-CP-VA-500-ovf, adding resources to VMs, configuring the ClearPass management IP address (192.168.0.38 in this example), and setting the system time zone.

For more information about ClearPass server configuration, see the manual for the server.

# Procedures

## Configuring the ClearPass RADIUS server

The ClearPass server in this example runs CPPM-VM-x86\_64-6.5.0.71095-ESX-CP-VA-500-ovf.

1. Log in to the ClearPass Policy Manager (CPPM).
2. On the **Configuration > Network > Devices** page, click **Add** at the top-right corner. On the page that opens, perform the following tasks:
  - a. Specify the IP address of the network access device (192.168.0.34 in this example).
  - b. Enter the RADIUS shared secret (also referred to as RADIUS shared key). In this example, the shared secret is **expert**.
  - c. Select the device vendor name.
  - d. Enable RADIUS CoA and use the default port number (3799) of RADIUS CoA.
  - e. Click **Add**.
3. On the **Configuration > Network > Device Groups** page, click **Add** at the top-right corner. On the page that opens, perform the following tasks:
  - a. Set the group name to **Group1**.
  - b. Add the IP address of the network access device (192.168.0.34 in this example) to the device group.
  - c. Click **Save**.
4. On the **Configuration > Identity > Local Users** page, click **Add** at the top-right corner. On the page that opens, perform the following tasks:
  - a. Set the user ID and name to **dot1x** and set the password to **Abc123!**,
  - b. Enable the user.
  - c. Select **Employee** as the user role.
  - d. Click **Add**.
5. On the **Configuration > Identity > Role Mappings** page, click **Add** at the top-right corner. On the page that opens, perform the following tasks:
  - a. Set the role mapping policy name to **dot1x-redirect-role-map**.
  - b. Select **Employee** as the default user role.
  - c. On the **Mapping Rules** tab, click **Add Rule**. On the page that opens, configure the parameters as follows:
    - Select **Radius:IETF** as the type.
    - Select **User-Name** as the name.
    - Select **EQUALS** as the operator.
    - Set the value to **dot1x**.
  - d. Click **Save**.
  - e. On the **Summary** tab, verify that the configuration is correct.
6. On the **Configuration > Enforcement > Profiles** page, click **Add** at the top-right corner. On the page that opens, perform the following tasks:
  - a. On the **Profile** tab, set the enforcement profile name to **dot1x** and select the device group that contains the network access device.
  - b. On the **Attributes** tab, configure the redirect URL and specify an ACL to permit traffic that requires URL redirection. You must configure ACL rules on the network access device for the ACL.

In this example, the redirect URL is the address of the ClearPass server. The following shows the values for the redirect URL and ACL in the enforcement profile on the server:

- url-redirect=https://192.168.0.38/guest/ciscowiredguest.php?mac=%{Connection:Client-Mac-Address-Colon}
- url-redirect-acl=3001

- c. Click **Save**.
  - d. On the **Summary** tab, verify that the configuration is correct.
7. On the **Configuration > Enforcement > Enforcement Policies** page, click **Add** at the top-right corner. On the page that opens, perform the following tasks:
    - a. On the **Enforcement** tab, set the enforcement policy name to **dot1x-redirect**, and select **dot1x** as the default profile. The enforcement type is RADIUS.
    - b. On the **Rules** tab, click **Add Rule**. On the page that opens, configure the parameters as follows.
      - Set the type to **Tips**.
      - Set the name to **Role**.
      - Set the operator to **EQUALS**.
      - Set the value to **Employee**.
      - Select **[RADIUS] dot1x** as the enforcement profile.
    - c. Click **Save**.
    - d. On the **Summary** tab, verify that the configuration is correct.
  8. On the **Configuration > Services** page, click **Add** at the top-right corner. On the page that opens, set the service name to **dot1x-wired-service**. Associate the service with other configuration items in different tabs and save the configuration.
    - o Select PAP as the authentication method.
    - o Add authentication source **[Guest User Repository] [Local SQL DB]**.
    - o Select **dot1x-redirect-role-map** as the role mapping policy.
    - o Select **dot1x-redirect** as the enforcement policy.
  9. On the **Summary** page, verify that the configuration is correct.

## Configuring the device

1. Assign an IP address to each interface, as shown in [Figure 11](#). Make sure the hosts, device, and RADIUS server can reach each other. (Details not shown.)
2. Configure the RADIUS scheme:
  - # Create RADIUS scheme **radsun**.

```
<Device> system-view
[Device] radius scheme radsun
New RADIUS scheme.
```
  - # Specify the server at 192.168.0.38 as the primary RADIUS authentication server.

```
[Device-radius-radsun] primary authentication 192.168.0.38
```
  - # Specify the server at 192.168.0.38 as the primary RADIUS accounting server.

```
[Device-radius-radsun] primary accounting 192.168.0.38
```
  - # Set the authentication shared key to **expert** in plain text for secure communication between the device and the RADIUS server.

```
[Device-radius-radsun] key authentication simple expert
```
  - # Set the accounting shared key to **expert** in plain text for secure communication between the device and the RADIUS server.

```

[Device-radius-radsun] key accounting simple expert
Exclude domain names from the usernames sent to the RADIUS server.
[Device-radius-radsun] user-name-format without-domain
Specify 192.168.0.34 as the source IP address of outgoing RADIUS packets.
[Device-radius-radsun] nas-ip 192.168.0.34
[Device-radius-radsun] quit

Create ISP domain sun and enter ISP domain view.
[Device] domain sun
Configure ISP domain sun to use RADIUS scheme radsun for authentication, authorization,
and accounting of all LAN users.
[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

Specify ISP domain sun as the default domain.
[Device] domain default enable sun

3. Configure port security:
Enable port security globally.
[Device] port-security enable

Set the port security mode to macAddressElseUserLoginSecureExt and set the NTK mode
to ntkonly on GigabitEthernet 1/0/1.
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port-security port-mode
mac-else-userlogin-secure-ext
[Device-GigabitEthernet1/0/1] port-security ntk-mode ntkonly
[Device-GigabitEthernet1/0/1] quit

Configure a shared account for MAC authentication users, and set the username to dot1x
and password to plaintext string of Abc123!.
[Device] mac-authentication user-name-format fixed account dot1x password simple
Abc123!

Enable the access device to terminate EAP packets and perform PAP authentication with the
RADIUS server.
[Device] dot1x authentication-method pap

4. Configure advanced ACL 3001 to permit traffic destined for the redirect URL. The redirect URL
is the address of the ClearPass server. Make sure the ACL number is the same as that
assigned by the ClearPass server.
[Device] acl advanced 3001
[Device-acl-ipv4-adv-3001] rule 0 permit ip destination 192.168.0.38 0
[Device-acl-ipv4-adv-3001] quit

```

## Verifying the configuration

```

Verify that port security is correctly configured.
[Device] display port-security interface gigabitethernet 1/0/1
Global port security parameters:
 Port security : Enabled
 AutoLearn aging time : 0 min
 Disableport timeout : 20 s

```

```

Blockmac timeout : 180 s
MAC move : Denied
Authorization fail : Online
NAS-ID profile : 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
Open authentication : Disabled
Traffic-statistics : Disabled
OUI value list :

```

GigabitEthernet1/0/1 is link-up

```

Port mode : macAddressElseUserloginSecureExt
NeedToKnow mode : NeedToKnowOnly
Intrusion protection mode : NoAction
Security MAC address attribute
 Learning mode : Sticky
 Aging type : Periodical
Max secure MAC addresses : Not configured
Current secure MAC addresses : 0
Authorization : Permitted
NAS-ID profile : Not configured
Free VLANs : Not configured
Open authentication : Disabled
MAC-move VLAN check bypass : Disabled

```

#### # Display MAC authentication information on GigabitEthernet 1/0/1.

[Device] display mac-authentication interface gigabitethernet 1/0/1

Global MAC authentication parameters:

```

MAC authentication : Enabled
Authentication method : PAP
Username format : Fixed account
 Username : dot1x
 Password : *****
MAC range accounts : 0
 MAC address Mask Username
Offline detect period : 300 s
Quiet period : 60 s
Server timeout : 100 s
Reauth period : 3600 s
User aging period for critical VLAN : 1000 s
User aging period for critical VSI : 1000 s
User aging period for guest VLAN : 1000 s
User aging period for guest VSI : 1000 s

```

```

Authentication domain : sun
HTTP proxy port list : Not configured
HTTPS proxy port list : Not configured
Online MAC-auth wired user : 1

```

Silent MAC users:

| MAC address | VLAN ID | From port | Port index |
|-------------|---------|-----------|------------|
|-------------|---------|-----------|------------|

GigabitEthernet1/0/1 is link-up

```

MAC authentication : Enabled
Carry User-IP : Disabled
Authentication domain : sun
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
User aging : Enabled
Server-recovery online-user-sync : Enabled

Guest VSI : Not configured
Guest VSI auth-period : 30 s
Critical VSI : Not configured
Auto-tag feature : Disabled
VLAN tag configuration ignoring : Disabled
Max online users : 4294967295
Authentication attempts : successful 5, failed 38
Current online users : 1

```

| MAC address    | Auth state    |
|----------------|---------------|
| acf1-df6c-ff48 | Authenticated |

### # Display 802.1X information on GigabitEthernet 1/0/1.

[Device] display dot1x interface gigabitethernet 1/0/1

Global 802.1X parameters:

```

802.1X authentication : Enabled
PAP authentication : Enabled
Max-tx period : 30 s
Handshake period : 15 s
Offline detect period : 300 s
Quiet timer : Disabled
 Quiet period : 60 s
Supp timeout : 30 s
Server timeout : 100 s
Reauth period : 3600 s

```



```

Max auth requests : 2
User aging period for Auth-Fail VLAN : 1000 s
User aging period for Auth-Fail VSI : 1000 s
User aging period for critical VLAN : 1000 s
User aging period for critical VSI : 1000 s
User aging period for guest VLAN : 1000 s
User aging period for guest VSI : 1000 s
EAD assistant function : Disabled
 EAD timeout : 30 min
Domain delimiter : @
Online 802.1X wired users : 0

```

GigabitEthernet1/0/1 is link-up

```

802.1X authentication : Enabled
Handshake : Enabled
Handshake reply : Disabled
Handshake security : Disabled
Offline detection : 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
Add Guest VLAN delay : Disabled
Re-auth server-unreachable : Logoff
Max online users : 4294967295
User IP freezing : Disabled
Reauth period : 0 s
Send Packets Without Tag : Disabled
Max Attempts Fail Number : 0
Guest VSI : Not configured
Auth-Fail VSI : Not configured
Critical VSI : Not configured
Add Guest VSI delay : Disabled
User aging : Enabled
Server-recovery online-user-sync : Enabled
Auth-Fail EAPOL : Disabled
Critical EAPOL : Disabled

```

EAPOL packets: Tx 165, Rx 0

Sent EAP Request/Identity packets : 165

EAP Request/Challenge packets: 0

```

 EAP Success packets: 0
 EAP Failure packets: 0
 Received EAPOL Start packets : 0
 EAPOL LogOff packets: 0
 EAP Response/Identity packets : 0
 EAP Response/Challenge packets: 0
 Error packets: 0
 Online 802.1X users: 0

Display online user information after users pass authentication.
<Device> display mac-authentication connection
Total connections: 1
Slot ID: 2
User MAC address: acf1-df6c-ff48
Access interface: GigabitEthernet1/0/1
Username: dot1x
User access state: Successful
Authentication domain: sun
IPv4 address: 192.168.1.5
Initial VLAN: 4
Authorization untagged VLAN: N/A
Authorization tagged VLAN: N/A
Authorization VSI: N/A
Authorization ACL ID: 3001
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL:
https://192.168.0.38/guest/ciscowiredguest.php?mac=ac:f1:df:6c:ff:48
Termination action: Default
Session timeout period: N/A
Online from: 2018/03/02 12:52:17
Online duration: 0h 11m 12s

Verify that frames with an unknown destination MAC address, multicast address, or broadcast
address are discarded on GigabitEthernet 1/0/1. (Details not shown.)

```

## Configuration files

---

### IMPORTANT:

Support for the **port link-mode bridge** command depends on the device model.

---

```

#
 dot1x authentication-method pap
#
 mac-authentication user-name-format fixed account dot1x password cipher c3$HAlQ
nyXOWZXTgiOBPd7+kSPClKm7JbZ1Rw==
#
 port-security enable
#
 interface GigabitEthernet1/0/1

```

```

port link-mode bridge
port-security ntk-mode ntkonly
port-security port-mode mac-else-userlogin-secure-ext
#
acl advanced 3001
 rule 0 permit ip destination 192.168.0.38 0
#
radius scheme radsun
 primary authentication 192.168.0.38
 primary accounting 192.168.0.38
 key authentication cipher c3$s9TAYm34R8sS5k/Cylg2sDm69ZRupMvGJg==
 key accounting cipher c3$UaUPGk8AfZAQLHF1bKNcEoM2HXGiuWowBQ==
 retry 5
 user-name-format without-domain
 nas-ip 192.168.0.34
#
domain sun
 authentication lan-access radius-scheme radsun
 authorization lan-access radius-scheme radsun
 accounting lan-access radius-scheme radsun
#
domain default enable sun
#

```