

Contents

Introduction	1
Prerequisites	1
Example: Configuring HWTACACS authentication and authorization in ACS for Telnet users	1
Network configuration	1
Analysis	1
Applicable hardware and software versions	2
Procedures	4
Configuring the HWTACACS server	4
Configuring the device	7
Verifying the configuration	8
Configuration files	8
Example: Configuring RADIUS authentication and authorization in INC for SSH users	9
Network configuration	9
Analysis	10
Applicable hardware and software versions	10
Restrictions and guidelines	12
Procedures	12
Configuring RADIUS servers	12
Configuring the device	14
Verifying the configuration	16
Configuration files	20
Example: Configuring RADIUS authentication and authorization in ACS for SSH users	21
Network configuration	21
Analysis	21
Applicable hardware and software versions	22
Restrictions and guidelines	24
Procedures	24
Configuring the RADIUS server	24
Configuring the device	27
Verifying the configuration	28
Configuration files	30
Example: Configuring HWTACACS authentication and authorization in ACS for SSH users	31
Network configuration	31
Analysis	32
Applicable hardware and software versions	32
Restrictions and guidelines	34
Procedures	34
Configuring the HWTACACS server	34
Configuring the device	37
Verifying the configuration	39
Configuration files	41

Introduction

This document provides AAA configuration examples for Telnet and SSH users.

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 AAA.

Example: Configuring HWTACACS authentication and authorization in ACS for Telnet users

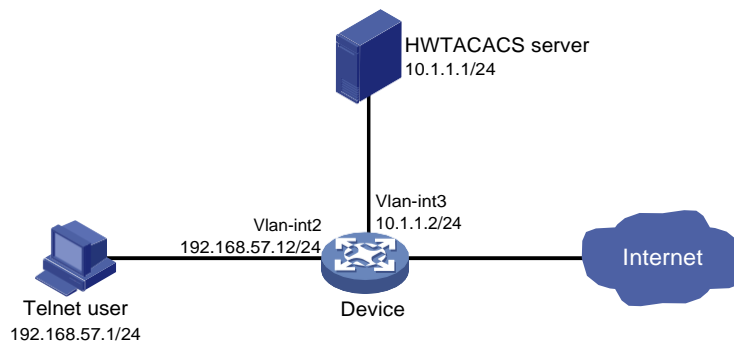
Network configuration

As shown in [Figure 1](#), configure the device to meet the following requirements:

- The HWTACACS server is used to provide authentication and authorization services for Telnet users.
- The authenticated users are permitted to execute the **display** commands of all system features and resources.

Add a user account with username **user@bbb** and password **123456TESTplat&!** on the HWTACACS server.

Figure 1 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- Configure the Telnet username and password on the HWTACACS server to identify valid users.
- For Telnet users to perform AAA, set the authentication mode to **scheme** on VTY userlines.

- Configure the same shared key on the device and the HWTACACS server to secure HWTACACS communication. When the shared key is configured, the device and the HWTACACS server transfer passwords safely and the device can verify the integrity of each HWTACACS response.
- Configure HWTACACS authentication and authorization by performing the following tasks on the device:
 - Create an HWTACACS scheme.
 - Specify the authentication and authorization servers.
 - Apply the HWTACACS scheme to the ISP domain to which the Telnet users belong on the device.
- Configure the HWTACACS server to assign the **network-operator** user role to the users, so the users can use all **display** commands.

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 HWTACACS server

In this example, the server runs ACS 4.0.

Adding a user

1. In the navigation tree, click **User Setup**.
2. Enter **user@bbb** in the **User** field and click **Add/Edit**, as shown in [Figure 2](#).

Figure 2 Adding a user

Select

User:

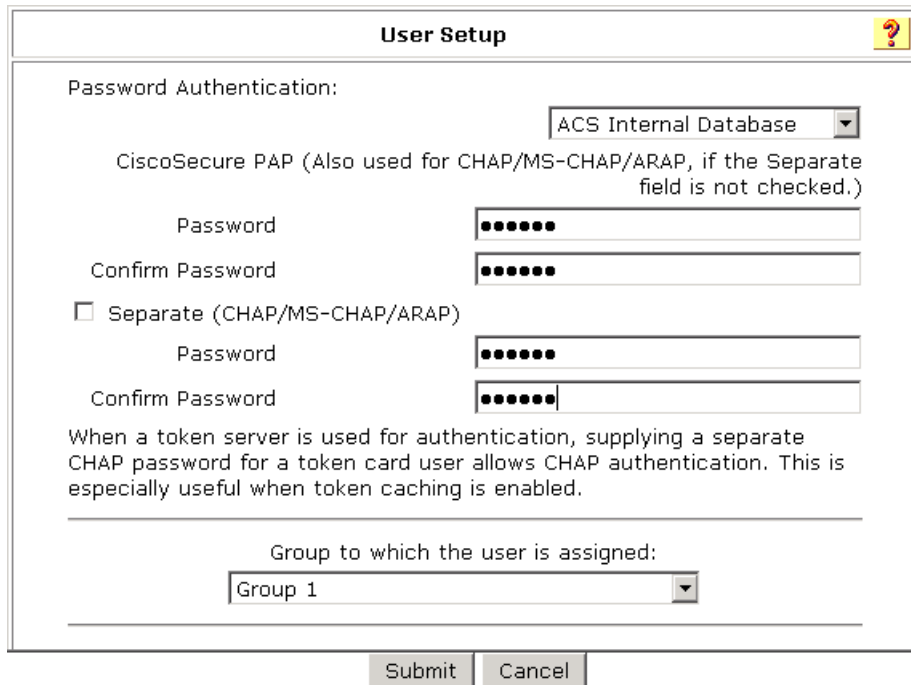
List users beginning with letter/number:

<u>A</u>	<u>B</u>	<u>C</u>	<u>D</u>	<u>E</u>	<u>F</u>	<u>G</u>	<u>H</u>	<u>I</u>	<u>J</u>	<u>K</u>	<u>L</u>	<u>M</u>
<u>N</u>	<u>O</u>	<u>P</u>	<u>Q</u>	<u>R</u>	<u>S</u>	<u>T</u>	<u>U</u>	<u>V</u>	<u>W</u>	<u>X</u>	<u>Y</u>	<u>Z</u>
<u>0</u>	<u>1</u>	<u>2</u>	<u>3</u>	<u>4</u>	<u>5</u>	<u>6</u>	<u>7</u>	<u>8</u>	<u>9</u>			

Configuring the user

1. On the **User Setup** page, configure the following parameters, as shown in [Figure 3](#):
 - Enter **123456TESTplat&!** in the **Password** and **Confirm Password** fields.
 - Assign the user to user group **Group 1**.

Figure 3 Configuring the user password



The 'User Setup' dialog box is shown. It has a title bar with a question mark icon. The main content area is titled 'Password Authentication:'. It contains a dropdown menu set to 'ACS Internal Database'. Below this is a note: 'CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)'. There are two sets of password fields. The first set has 'Password' and 'Confirm Password' fields, both containing six dots. The second set is preceded by an unchecked checkbox labeled 'Separate (CHAP/MS-CHAP/ARAP)', and also has 'Password' and 'Confirm Password' fields with six dots. Below these fields is a paragraph: 'When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.' At the bottom, there is a label 'Group to which the user is assigned:' followed by a dropdown menu set to 'Group 1'. At the very bottom of the dialog are 'Submit' and 'Cancel' buttons.

2. Click **Submit**.

Configuring the network settings

1. In the navigation tree, click **Network Configuration**.
2. On the **Add AAA Client** page, configure the following parameters, as shown in [Figure 4](#):
 - o Enter an AAA client hostname in the **AAA Client Hostname** field. This example uses **Device**.
 - o Enter **10.1.1.2** in the **AAA Client IP Address** field.
The IP address is the source IP address for outgoing HWTACACS packets on the device.
 - o Enter **expert** in the **Key** field.
The key configured here is the same as the authentication, authorization, and accounting keys configured on the device for secure HWTACACS communication.
 - o Select **TACACS+ (Cisco IOS)** from the **Authenticate Using** list.

Figure 4 Configuring the network settings

Add AAA Client

AAA Client Hostname: Device

AAA Client IP Address: 10.1.1.2

Key: expert

Network Device Group: (Not Assigned)

Authenticate Using: TACACS+ (Cisco IOS)

☐ Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

☐ Log Update/Watchdog Packets from this AAA Client

☐ Log RADIUS Tunneling Packets from this AAA Client

☐ Replace RADIUS Port info with Username from this AAA Client

Submit Submit + Apply Cancel

3. Click **Submit + Apply**.

Configuring the user group

1. In the navigation tree, click **Group Setup**.
2. Select **1: Group 1 (29 users)** from the **Group** list and click **Edit Settings**, as shown in [Figure 5](#).

Figure 5 Selecting a user group

Group Setup

Group Setup

Select

Group : 1: Group 1 (29 users)

Users in Group Edit Settings Rename Group

3. On the **TACACS+ Settings** page, configure the following parameters, as shown in [Figure 6](#):
 - o Select **Shell(exec)**, which enables command execution for all users in the group.
 - o Select **Custom attributes**, and enter **roles=\\network-operator** in the **Custom attributes** field.
 - o Configure other settings as needed.

Figure 6 Configuring the user group

TACACS+ Settings

☐ **PPP IP**

☐ In access control list

☐ Out access control list

☐ Route

☐ Routing

☐ Custom attributes

Note: PPP LCP will be automatically enabled if this service is enabled

☒ **Shell (exec)**

☐ Access control list

☐ Auto command

☐ Callback line

☐ Callback rotary

☐ Idle time

☐ No callback verify

☐ No escape

☐ No hangup

☐ Privilege level

☐ Timeout

☒ Custom attributes

Submit Cancel

4. Click **Submit**.

Configuring the device

Create VLAN 2 and assign GigabitEthernet 1/0/2 to the VLAN.

```
<Device> system-view
[Device] vlan 2
[Device-vlan2] port gigabitethernet 1/0/2
[Device-vlan2] quit
```

Assign an IP address to VLAN-interface 2.

```
[Device] interface vlan-interface 2
[Device-Vlan-interface2] ip address 192.168.57.12 255.255.255.0
[Device-Vlan-interface2] quit
```

Create VLAN 3 and assign GigabitEthernet 1/0/1 to the VLAN.

```
[Device] vlan 3
[Device-vlan3] port gigabitethernet 1/0/1
[Device-vlan3] quit
```

Assign an IP address to VLAN-interface 3.

```
[Device] interface vlan-interface 3
[Device-Vlan-interface3] ip address 10.1.1.2 255.255.255.0
[Device-Vlan-interface3] quit
```

Enable the Telnet server feature.

```
[Device] telnet server enable
```

Enable scheme authentication on VTY user lines 0 through 63.

```
[Device] line vty 0 63
[Device-line-vty0-63] authentication-mode scheme
[Device-line-vty0-63] quit
```

Create an HWTACACS scheme named **hwtac**.

```
[Device] hwtacacs scheme hwtac
```

Specify the primary HWTACACS server with the IP address 10.1.1.1 and port number 49.

```
[Device-hwtacacs-hwtac] primary authentication 10.1.1.1 49
[Device-hwtacacs-hwtac] primary authorization 10.1.1.1 49
[Device-hwtacacs-hwtac] primary accounting 10.1.1.1 49
```

Specify the shared key as **expert** for secure HWTACACS communication between the device and HWTACACS server.

```
[Device-hwtacacs-hwtac] key authentication simple expert
[Device-hwtacacs-hwtac] key authorization simple expert
[Device-hwtacacs-hwtac] key accounting simple expert
[Device-hwtacacs-hwtac] quit
```

Create an ISP domain named **bbb**, and specify the domain to use HWTACACS scheme **hwtac** as the AAA methods of login users.

```
[Device] domain bbb
[Device-isp-bbb] authentication login hwtacacs-scheme hwtac
[Device-isp-bbb] authorization login hwtacacs-scheme hwtac
[Device-isp-bbb] accounting login hwtacacs-scheme hwtac
[Device-isp-bbb] quit
```

Verifying the configuration

Telnet to the device, and enter username **user@bbb** and password **123456TESTplat&!**. The user logs into the device. (Details not shown.)

Verify that the user can use the **display** commands of all system features and resources. (Details not shown.)

Configuration files

❗ IMPORTANT:

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

```
#
telnet server enable
#
vlan 2 to 3
#
interface Vlan-interface2
ip address 192.168.57.12 255.255.255.0
#
interface Vlan-interface3
ip address 10.1.1.2 255.255.255.0
#
```



```

interface GigabitEthernet1/0/2
  port link-mode bridge
  port access vlan 2
#
interface GigabitEthernet1/0/1
  port link-mode bridge
  port access vlan 3
#
line vty 0 63
  authentication-mode scheme
  user-role network-operator
#
hwtacacs scheme hwtac
  primary authentication 10.1.1.1
  primary authorization 10.1.1.1
  primary accounting 10.1.1.1
  key authentication cipher $c$3$X3oR/wjLFjDqIyjdAmvjwAhiuqewGABglQ==
  key authorization cipher $c$3$5pmuq0RJ9UWMWDkRNNERX6HFM0aRv5txFg==
  key accounting cipher $c$3$FSdSiBY1u+ZNkAYYlPw9YkGxJA4iR8MDjw==
#
domain bbb
  authentication login hwtacacs-scheme hwtac
  authorization login hwtacacs-scheme hwtac
  accounting login hwtacacs-scheme hwtac
#

```

Example: Configuring RADIUS authentication and authorization in INC for SSH users

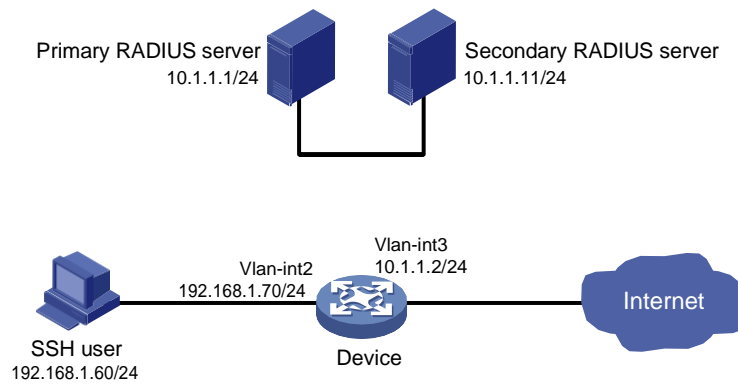
Network configuration

As shown in [Figure 7](#), configure the device to meet the following requirements:

- The RADIUS servers are used to provide authentication and authorization services for SSH users. One server acts as the primary server and the other acts as the secondary server.
- Domain names are included in the usernames sent to the RADIUS servers.
- The authenticated users are permitted to use the **display** commands of all system features and resources.

The RADIUS servers run INC. Add a user account with username **hello@bbb** and password **123456TESTplat&!** on each RADIUS server.

Figure 7 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- Configure the SSH username and password on the primary and secondary RADIUS servers to identify valid users.
- For SSH users to perform AAA, set the authentication mode to **scheme** on VTY userlines.
- Configure the same shared key on the device and the RADIUS servers to secure RADIUS communication. When the shared key is configured, the device and the RADIUS servers transfer passwords safely and the device can verify the integrity of each RADIUS response.
- Configure RADIUS authentication and authorization by performing the following tasks on the device:
 - Create a RADIUS scheme.
 - Specify the primary and secondary servers for authentication and authorization.
 - Apply the RADIUS scheme to the ISP domain to which the SSH users belong.
- Configure the RADIUS servers to assign the **network-operator** user role to the users, so the users can use all **display** commands.

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

When you configure RADIUS authentication and authorization for SSH users, follow these restrictions and guidelines:

- The Stelnet server supports only 256-bit and 384-bit ECDSA key pairs.
- Local DSA, ECDSA, and RSA key pairs for SSH use default names. You cannot assign names to the key pairs.

Procedures

Configuring RADIUS servers

In this example, RADIUS servers run INC PLAT 7.0 (E0102) and INC UAM 7.0 (E0201). This example describes the configuration of the primary RADIUS server. Configure the secondary

RADIUS server in the same way the primary RADIUS server is configured.

Adding the device to INC as an access device

1. Click the **User** tab.
2. From the navigation tree, select **User Access Policy > Access Device Management > Access Device**.
The access device list appears.
3. Click **Add**.
4. On the **Add Access Device** page, configure the following parameters, as shown in [Figure 8](#):
 - Enter **1812** and **1813** in the **Authentication Port** and **Accounting Port** fields, respectively.
 - Enter **expert** in the **Shared Key** and **Confirm Shared Key** fields.
 - Select **Device Management Service** from the **Service Type** list.
 - Select **INTELBRAS(General)** from the **Access Device Type** list.
 - Use the default values for other parameters in the **Access Configuration** area.
 - In the **Device List** area, click **Select** or **Add Manually** to add the device (10.1.1.2) to INC as an access device.

Figure 8 Adding an access device

User > User Access Policy > Access Device Management > Access Device > Add Access Device

Access Configuration

Authentication Port *	1812	Accounting Port *	1813
RADIUS Accounting	Fully Supported	Service Type	Device Management Service
Access Device Type	H3C(General)	Access Device Group	
Shared Key *	*****	Confirm Shared Key *	*****
Service Group	Ungrouped		

Device List

Select Add Manually Clear All

Device Name	Device IP	Device Model	Comments	Delete
	10.1.1.2			

Total Items: 1.

OK Cancel

5. Click **OK**.

Adding a device management user

1. Click the **User** tab.
2. From the navigation tree, select **Access User > Device User**.
The device management user list appears.
3. Click **Add**.
4. On the **Add Device User** page, configure the following parameters, as shown in [Figure 9](#):
 - Enter **hello@bbb** in the **Account Name** field.
 - Enter **aabbcc** in the **User Password** and **Confirm Password** fields.
 - Select **SSH** from the **Service Type** list.
 - Enter **network-operator** in the **Role Name** field.
The network-operator user role has access to the **display** commands of all system features and resources.
 - In the **IP Address List of Managed Devices** area, click **Add** to specify an IP segment (from 10.1.1.0 to 10.1.1.255) for management. The IP segment must contain the IP address of the access device.

Figure 9 Adding a device management user

User > Device User > Add Device User

Add Device User

Basic Information of Device User

Account Name * ?

User Password *

Confirm Password *

Service Type

EXEC Priority

Role Name

Tips

Note: If you enter multiple role names, enter one role name on each line. The sum of the total number of bytes occupied by the role names and the number of role names (excluding duplicate names) cannot exceed 234. For example, if you enter 10 role names, the number of bytes occupied by the role names cannot exceed 224.

Bound User IP List

Start IP	End IP	Delete
No match found.		

IP Address List of Managed Devices

Start IP	End IP	Delete
10.1.1.0	10.1.1.255	<input type="button" value="Delete"/>

5. Click **OK**.

Configuring the device

Create VLAN 2 and assign GigabitEthernet 1/0/2 to the VLAN.

```
<Device> system-view
[Device] vlan 2
[Device-vlan2] port gigabitethernet 1/0/2
[Device-vlan2] quit
```

Assign an IP address to VLAN-interface 2.

```
[Device] interface vlan-interface 2
[Device-Vlan-interface2] ip address 192.168.1.70 255.255.255.0
[Device-Vlan-interface2] quit
```

Create VLAN 3 and assign GigabitEthernet 1/0/1 to the VLAN.

```
[Device] vlan 3
[Device-vlan3] port gigabitethernet 1/0/1
[Device-vlan3] quit
```

Assign an IP address to VLAN-interface 3.

```
[Device] interface vlan-interface 3
[Device-Vlan-interface3] ip address 10.1.1.2 255.255.255.0
[Device-Vlan-interface3] quit
```

Create a local RSA key pair.

```
[Device] public-key local create rsa
```

The range of public key modulus is (512 ~ 4096).

If the key modulus is greater than 512, it will take a few minutes.

Press CTRL+C to abort.

```

Input the modulus length [default = 1024]:
Generating Keys...
.....
Create the key pair successfully.

# Create a local DSA key pair.
[Device] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....
Create the key pair successfully.

# Create a 256-bit ECDSA key pair.
[Device] public-key local create ecdsa secp256r1
Generating Keys...
Create the key pair successfully.

# Create a 384-bit ECDSA key pair.
[Device] public-key local create ecdsa secp384r1
Generating Keys...
.
Create the key pair successfully.

# Enable the Stelnet server.
[Device] ssh server enable

# Enable scheme authentication on VTY user lines 0 through 63.
[Device] line vty 0 63
[Device-line-vty0-63] authentication-mode scheme
[Device-line-vty0-63] quit

# Create a RADIUS scheme named rad.
[Device] radius scheme rad

# Specify the primary authentication RADIUS server with the IP address 10.1.1.1 and port number 1812.
[Device-radius-rad] primary authentication 10.1.1.1 1812

# Specify the secondary authentication RADIUS server with the IP address 10.1.1.11 and port number 1812.
[Device-radius-rad] secondary authentication 10.1.1.11 1812

# Specify the primary accounting RADIUS server with the IP address 10.1.1.1 and port number 1813.
[Device-radius-rad] primary accounting 10.1.1.1 1813

# Specify the secondary accounting RADIUS server with the IP address 10.1.1.11 and port number 1813.
[Device-radius-rad] secondary accounting 10.1.1.11 1813

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

```

Include domain names in the usernames sent to the RADIUS server.

```
[Device-radius-rad] user-name-format with-domain
[Device-radius-rad] quit
```

Create an ISP domain named **bbb**, and configure the ISP domain to use the RADIUS scheme **rad** as the AAA methods of login users.

```
[Device] domain bbb
[Device-isp-bbb] authentication login radius-scheme rad
[Device-isp-bbb] authorization login radius-scheme rad
[Device-isp-bbb] accounting login radius-scheme rad
[Device-isp-bbb] quit
```

Verifying the configuration

Initiate an SSH connection to the device, and enter username **hello@bbb** and password **123456TESTplat&!**. The user logs into the device. (Details not shown.)

Verify that the user can use the **display** commands of all system features and resources. (Details not shown.)

```
<Sysname> display radius scheme
Total 1 RADIUS schemes
```

RADIUS scheme name: rad

Index: 0

Primary authentication server:

Host name: Not Configured

IP : 10.1.1.1

Port: 1812

VPN : Not configured

State: Active (duration: 0 weeks, 0 days, 0 hours, 2 minutes, 2 seconds)

Test profile: Not configured

Weight: 0

Primary accounting server:

Host name: Not Configured

IP : 10.1.1.1

Port: 1813

VPN : Not configured

State: Active (duration: 0 weeks, 0 days, 0 hours, 1 minutes, 37 seconds)

Weight: 0

Second authentication server:

Host name: Not Configured

IP : 10.1.1.11

Port: 1812

VPN : Not configured

State: Active (duration: 0 weeks, 0 days, 0 hours, 1 minutes, 50 seconds)

Test profile: Not configured

Weight: 0

Second accounting server:

Host name: Not Configured

```

IP      : 10.1.1.11                               Port: 1813
VPN     : Not configured
State: Active (duration: 0 weeks, 0 days, 0 hours, 1 minutes, 23 seconds)
Weight: 0
Accounting-On function                : Disabled
    extended function                  : Disabled
    retransmission times               : 50
    retransmission interval(seconds)   : 3
Timeout Interval(seconds)             : 3
Retransmission Times                 : 3
Retransmission Times for Accounting Update : 5
Server Quiet Period(minutes)         : 5
Realtime Accounting Interval(seconds) : 720
Stop-accounting packets buffering     : Enabled
    Retransmission times              : 500
NAS IP Address                       : Not configured
VPN                                   : Not configured
User Name Format                      : with-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 packets send-force   : Disabled
Reauthentication server selection     : Inherit
Attribute 218 of vendor ID 25506     : DHCP-Option 61
                                         Format 1 (1-byte Type field)

```

(Release 63xx.) Display RADIUS scheme configuration.

```

<Sysname> display radius scheme
Total 1 RADIUS schemes

```

```

-----
RADIUS scheme name: rad
Index: 0
Primary authentication server:
    Host name: Not Configured
    IP      : 10.1.1.1                               Port: 1812
    VPN     : Not configured
    State: Active
    Test profile: Not configured
    Weight: 0
Primary accounting server:
    Host name: Not Configured
    IP      : 10.1.1.1                               Port: 1813
    VPN     : Not configured
    State: Active

```



```

    Weight: 0
Second authentication server:
    Host name: Not Configured
    IP   : 10.1.1.11                      Port: 1812
    VPN  : Not configured
    State: Active
    Test profile: Not configured
    Weight: 0
Second accounting server:
    Host name: Not Configured
    IP   : 10.1.1.11                      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)       : 3
Retransmission Times            : 3
Retransmission Times for Accounting Update : 5
Server Quiet Period(minutes)    : 5
Realtime Accounting Interval(seconds) : 720
Stop-accounting packets buffering : Enabled
    Retransmission times         : 500
NAS IP Address                   : Not configured
VPN                              : Not configured
User Name Format                  : with-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 packets send-force : Disabled
Reauthentication server selection : Inherit

```

(R65xx.) Display RADIUS scheme configuration.

```
<Sysname> display radius scheme
```

```
Total 1 RADIUS schemes
```

```
-----
RADIUS scheme name: rad
```

```
Index: 0
```

```
Primary authentication server:
```

```
Host name: Not Configured
```

```
IP   : 10.1.1.1
```

```
Port: 1812
```

```
VPN  : Not configured
```

```

State: Active
Test profile: Not configured
Weight: 0
Primary accounting server:
  Host name: Not Configured
  IP      : 10.1.1.1                      Port: 1813
  VPN     : Not configured
  State:   Active
  Weight:  0
Second authentication server:
  Host name: Not Configured
  IP      : 10.1.1.11                     Port: 1812
  VPN     : Not configured
  State:   Active
  Test profile: Not configured
  Weight:  0
Second accounting server:
  Host name: Not Configured
  IP      : 10.1.1.11                     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)       : 3
Retransmission Times            : 3
Retransmission Times for Accounting Update : 5
Server Quiet Period(minutes)    : 5
Realtime Accounting Interval(seconds) : 720
Stop-accounting packets buffering : Enabled
  Retransmission times          : 500
NAS IP Address                  : Not configured
VPN                             : Not configured
User Name Format                 : with-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 packets send-force : Disabled
Reauthentication server selection : Inherit
Attribute 218 of vendor ID 25506 : DHCP-Option 61

```

The output shows that the primary RADIUS server is in **Active** state.

Disconnect the device from the primary RADIUS server. (Details not shown.)

Verify that the primary RADIUS server has changed to the **Block** state in the RADIUS scheme. (Details not shown.)

Configuration files



IMPORTANT:

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

```
#
vlan 2 to 3
#
interface Vlan-interface2
 ip address 192.168.1.70 255.255.255.0
#
interface Vlan-interface3
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 3
#
line vty 0 63
 authentication-mode scheme
 user-role network-operator
#
 ssh server enable
#
radius scheme rad
 primary authentication 10.1.1.1
 primary accounting 10.1.1.1
 secondary authentication 10.1.1.11
 secondary accounting 10.1.1.11
 key authentication cipher $c$3$GBZ1jhslcGwSOpSejsESMnOr8Gb8SIT5ew==
 key accounting cipher $c$3$nGb/DWK8pxbHaLXQVc+xsmbUrletIZVd7Q==
#
domain bbb
 authentication login radius-scheme rad
 authorization login radius-scheme rad
 accounting login radius-scheme rad
#
```

Example: Configuring RADIUS authentication and authorization in ACS for SSH users

Network configuration

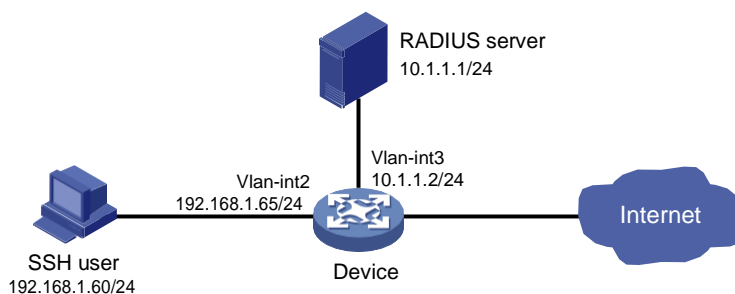
As shown in [Figure 10](#), configure the device to meet the following requirements:

- Act as the Stelnet server to provide RADIUS-based authentication and authorization services for the SSH user.
- Assign the highest level of privilege to the SSH user after the user passes authentication.

The RADIUS server runs Cisco ACS. Add a user account with username **manager@bbb** and password **1234ab##** on the RADIUS server.

The host runs Stelnet client software.

Figure 10 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- Configure the SSH username and password on the RADIUS server to identify valid users.
- For SSH users to perform AAA, set the authentication mode to **scheme** on VTY userlines.
- To support Stelnet clients that use different types of key pairs, generate DSA, ECDSA, and RSA key pairs on the Stelnet server.
- Configure RADIUS authentication and authorization by performing the following tasks on the device:
 - Create a RADIUS scheme.
 - Specify the authentication and authorization servers.
 - Apply the RADIUS scheme to the ISP domain to which the SSH users belong on the device.
- Enable the default user role feature and specify **network-admin** as the default user role, so the authenticated users can obtain the highest level of privilege.

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

When you configure RADIUS authentication and authorization for SSH users, follow these restrictions and guidelines:

- The Stelnet server supports only 256-bit and 384-bit ECDSA key pairs.
- Local DSA, ECDSA, and RSA key pairs for SSH use default names. You cannot assign names to the key pairs.

Procedures

Configuring the RADIUS server

In this example, the server runs ACS 4.2. Before you perform the following tasks, make sure the host, the device, and the RADIUS server can reach each other.

1. Enter the username and password, and click **Login**, as shown in [Figure 11](#).

Figure 11 Logging into ACS



2. Add the device to ACS as an AAA client:
 - a. In the navigation tree, click **Network Configuration**.
 - b. Click **Add Entry**, as shown in [Figure 12](#).

Figure 12 Adding an AAA client

The screenshot shows the 'Network Configuration' page with a sidebar on the left containing links to User Setup, Group Setup, Shared Profile Components, Network Configuration (highlighted), System Configuration, and Interface Configuration. The main content area has a 'Select' header and a table titled 'AAA Clients'. The table has three columns: 'AAA Client Hostname', 'AAA Client IP Address', and 'Authenticate Using'. The table is currently empty, showing 'None Defined'. Below the table are 'Add Entry' and 'Search' buttons.

- c. On the **Add AAA Client** page, configure the following parameters, as shown in [Figure 13](#):
- Enter an AAA client hostname in the **AAA Client Hostname** field. This example uses **Device**.
 - Enter **10.1.1.2** in the **AAA Client IP Address** field.
The IP address is the source IP address for outgoing RADIUS packets on the device.
 - Enter **expert** in the **Shared Secret** field.
The shared secret must be the same as the authentication and accounting keys configured on the device for secure RADIUS communication.
 - Select **RADIUS (IETF)** from the **Authenticate Using** list.

Figure 13 Configuring the AAA client

The screenshot shows the 'Add AAA Client' configuration page. The sidebar on the left is the same as in Figure 12, with 'Network Configuration' highlighted. The main content area has an 'Edit' header and a title 'Add AAA Client'. The form contains the following fields and options:

- AAA Client Hostname**: Device
- AAA Client IP Address**: 10.1.1.2
- Shared Secret**: expert
- RADIUS Key Wrap**
 - Key Encryption Key**: (empty field)
 - Message Authenticator Code Key**: (empty field)
 - Key Input Format**: ☐ ASCII ☒ Hexadecimal
- Authenticate Using**: RADIUS (IETF) (dropdown menu)
- ☐ Single Connect TACACS+ AAA Client (Record stop in accounting on failure)
- ☐ Log Update/Watchdog Packets from this AAA Client
- ☐ Log RADIUS Tunneling Packets from this AAA Client
- ☐ Replace RADIUS Port info with Username from this AAA Client
- ☐ Match Framed-IP-Address with user IP address for accounting packets from this AAA Client

At the bottom are 'Submit', 'Submit + Apply', and 'Cancel' buttons.

- d. Click **Submit + Apply**.
3. Add a user:

- a. In the navigation tree, click **User Setup**.
- b. On the **User Setup** page, enter **manager** in the **User** field and click **Add/Edit**, as shown in Figure 14.

Figure 14 Adding a user

User Setup

Select

User: manager

Find Add/Edit

List users beginning with letter/number:

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9			

List all users

Remove Dynamic Users

- c. Configure parameters for the user, including the user password and user group, as shown in Figure 15.

This example uses the default user group.

Figure 15 Configuring the user manager

User Setup

Edit

User: manager (New User)

☐ Account Disabled

Supplementary User Info

Real Name: admin

Description: network administrator

User Setup

Password Authentication:

ACS Internal Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password:

Confirm Password:

☒ Separate (CHAP/MS-CHAP/ARAP)

Password:

Confirm Password:

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:

Submit Cancel

- d. Click **Submit**.

Configuring the device

Create VLAN 2 and assign GigabitEthernet 1/0/2 to the VLAN.

```
<Device> system-view
[Device] vlan 2
[Device-vlan2] port gigabitethernet 1/0/2
[Device-vlan2] quit
```

Assign an IP address to VLAN-interface 2.

```
[Device] interface vlan-interface 2
[Device-Vlan-interface2] ip address 192.168.1.65 255.255.255.0
[Device-Vlan-interface2] quit
```

Create VLAN 3 and assign GigabitEthernet 1/0/1 to the VLAN.

```
[Device] vlan 3
[Device-vlan3] port gigabitethernet 1/0/1
[Device-vlan3] quit
```

Assign an IP address to VLAN-interface 3.

```
[Device] interface vlan-interface 3
[Device-Vlan-interface3] ip address 10.1.1.2 255.255.255.0
[Device-Vlan-interface3] quit
```

Create a local RSA key pair.

```
[Device] public-key local create rsa
The range of public key modulus is (512 ~ 4096).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
...
Create the key pair successfully.
```

Create a local DSA key pair.

```
[Device] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....
Create the key pair successfully.
```

Create a local 256-bit ECDSA key pair.

```
[Device] public-key local create ecdsa secp256r1
Generating Keys...
Create the key pair successfully.
```

Create a local 384-bit ECDSA key pair.

```
[Device] public-key local create ecdsa secp384r1
Generating Keys...
.
Create the key pair successfully.
```

Enable the Stelnet server.

```
[Device] ssh server enable
```

Enable scheme authentication on VTY user lines 0 through 63.

```
[Device] line vty 0 63
```

```
[Device-line-vty0-63] authentication-mode scheme
```

```
[Device-line-vty0-63] quit
```

Enable the default user role feature and specify **network-admin** as the default user role.

```
[Device] role default-role enable network-admin
```

Create a RADIUS scheme named **rad**.

```
[Device] radius scheme rad
```

Specify the primary RADIUS authentication server with the IP address 10.1.1.1 and port number 1812.

```
[Device-radius-rad] primary authentication 10.1.1.1 1812
```

Specify the shared key as **expert** for secure RADIUS communication between the device and RADIUS server.

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

Remove the domain name from usernames sent to the RADIUS server.

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

```
[Device-radius-rad] quit
```

Create an ISP domain named **bbb**, and specify the domain to use RADIUS scheme **rad** as the authentication and authorization methods of login users.

```
[Device] domain bbb
```

```
[Device-isp-bbb] authentication login radius-scheme rad
```

```
[Device-isp-bbb] authorization login radius-scheme rad
```

```
[Device-isp-bbb] accounting login none
```

```
[Device-isp-bbb] quit
```

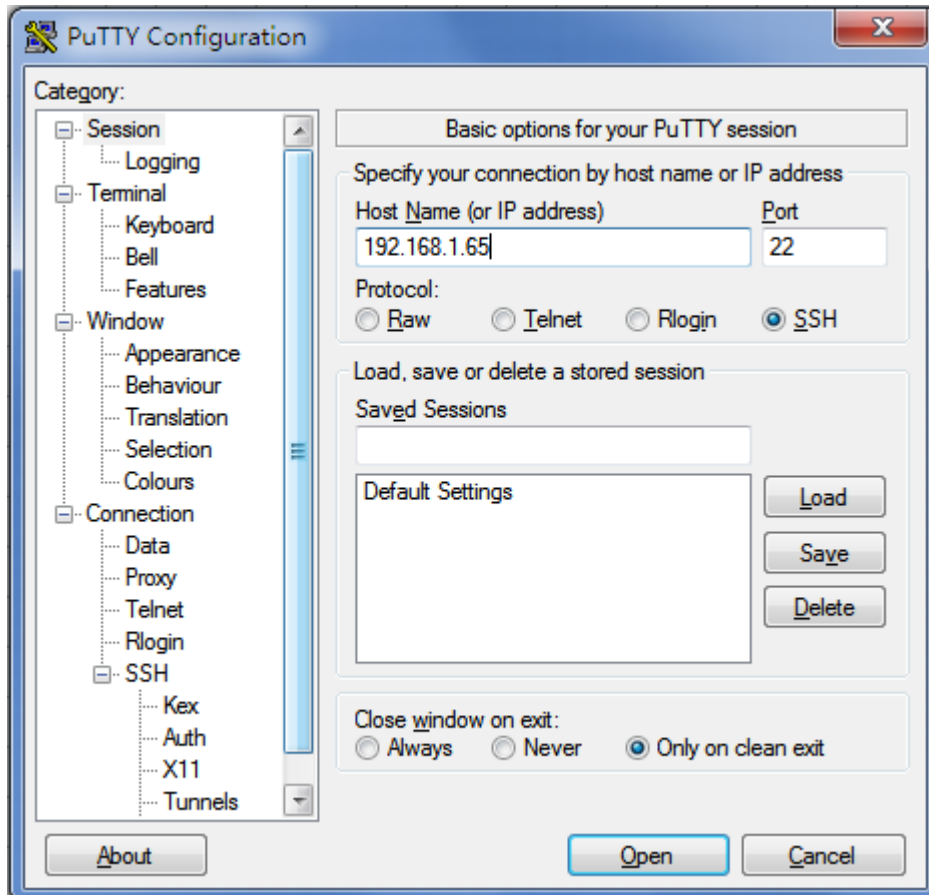
Verifying the configuration

Stelnet client software includes PuTTY and OpenSSH. This example uses an Stelnet client that runs PuTTY 0.58.

To verify that you can log into the Stelnet server from the Stelnet client:

1. Launch PuTTY.
2. From the navigation tree, click **Session**.
The **PuTTY Configuration** page appears.
3. Configure the following parameters, as shown in [Figure 16](#):
 - a. Enter **192.168.1.65** in the **Host Name (or IP address)** field.
 - b. Enter **22** in the **Port** field.
 - c. Select **SSH** for **Protocol**.

Figure 16 Specifying basic connection parameters



4. Click **Open**.

The system might display a security alert dialog box, as shown in [Figure 17](#).

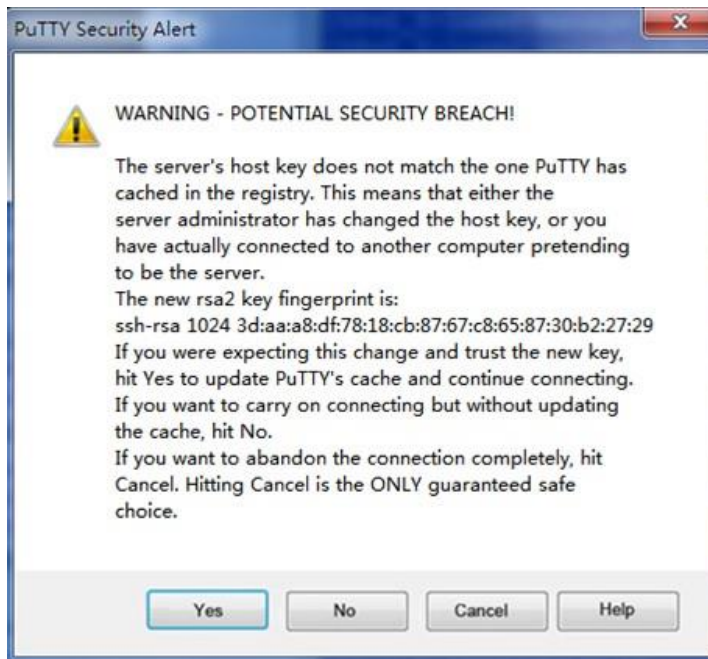
Figure 17 PuTTY Security Alert dialog box (1)



5. Click **Yes** or **No** to continue the connection.

The system might display another security alert dialog box, as shown in [Figure 18](#).

Figure 18 PuTTY Security Alert dialog box (2)



6. Click **Yes** or **No** to continue the connection.
7. Enter username **manager@bbb** and password **1234ab##** to log into the Stelnet server.

login as: manager@bbb

manager@bbb@192.168.1.65's password:

```
*****
* Copyright (c) 2004-2019 New INTELBRAS Technologies Co., Ltd. All rights
* reserved.*
* Without the owner's prior written consent,                               *
* no decompiling or reverse-engineering shall be allowed.                  *
*****
```

<Device>

Configuration files

⚠ IMPORTANT:

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

```
#
vlan 2 to 3
#
interface Vlan-interface2
 ip address 192.168.1.65 255.255.255.0
#
interface Vlan-interface3
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/2
```

```

port link-mode bridge
port access vlan 2
#
interface GigabitEthernet1/0/1
port link-mode bridge
port access vlan 3
#
line vty 0 63
authentication-mode scheme
user-role network-operator
#
ssh server enable
#
radius scheme rad
primary authentication 10.1.1.1
key authentication cipher $c$3$+zkawxNT2KQ1IhixdPDszSvNAH5b+yFMIQ==
user-name-format without-domain
#
domain bbb
authentication login radius-scheme rad
authorization login radius-scheme rad
accounting login none
#
role default-role enable network-admin
#

```

Example: Configuring HWTACACS authentication and authorization in ACS for SSH users

Network configuration

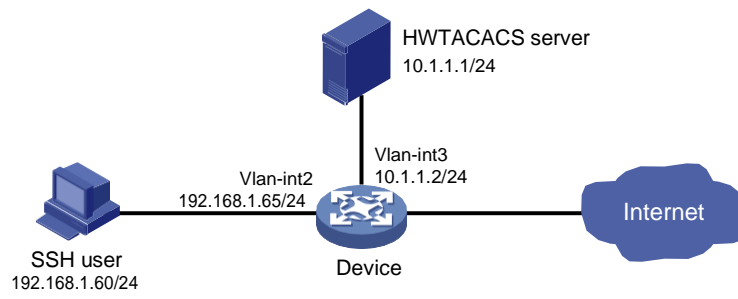
As shown in [Figure 19](#), configure the device to meet the following requirements:

- Act as the Stelnet server to provide HWTACACS-based authentication and authorization services for the SSH user.
- Assign the highest level of privilege to the SSH user after the user passes authentication.

The HWTACACS server runs Cisco ACS. Add a user account with username **manager@bbb** and password **1234ab##** on the HWTACACS server.

The host runs Stelnet client software.

Figure 19 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- Configure the SSH username and password on the HWTACACS server to identify valid users.
- For SSH users to perform AAA, set the authentication mode to **scheme** on VTY userlines.
- To support Stelnet clients that use different types of key pairs, generate DSA, ECDSA, and RSA key pairs on the Stelnet server.
- Configure HWTACACS authentication and authorization by performing the following tasks on the device:
 - Create an HWTACACS scheme.
 - Specify the authentication and authorization servers.
 - Apply the HWTACACS scheme to the ISP domain to which the SSH users belong on the device.
- Enable the default user role feature and specify **network-admin** as the default user role, so the authenticated users can have the highest level of privilege.

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

When you configure HWTACACS authentication and authorization for SSH users, follow these restrictions and guidelines:

- The Stelnet server supports only 256-bit and 384-bit ECDSA key pairs.
- Local DSA, ECDSA, and RSA key pairs for SSH use default names. You cannot assign names to the key pairs.

Procedures

Configuring the HWTACACS server

In this example, the server runs ACS 4.2. Before you perform the following tasks, make sure the host, the device, and the HWTACACS server can reach each other.

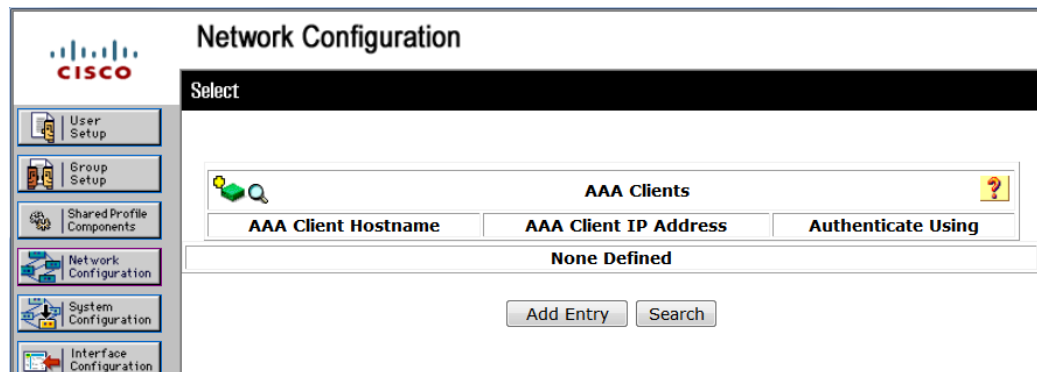
1. Enter the username and password, and click **Login**, as shown in [Figure 20](#).

Figure 20 Logging into ACS



2. Add the device to ACS as an AAA client:
 - a. In the navigation tree, click **Network Configuration**.
 - b. Click **Add Entry**, as shown in [Figure 21](#).

Figure 21 Adding an AAA client



- c. On the **Add AAA Client** page, configure the following parameters, as shown in [Figure 22](#):
 - Enter an AAA client hostname in the **AAA Client Hostname** field. This example uses **Device**.
 - Enter **10.1.1.2** in the **AAA Client IP Address** field.
The IP address is the source IP address for outgoing HWTACACS packets on the device.
 - Enter **expert** in the **Shared Secret** field.
The shared secret must be the same as the authentication, authorization, and accounting keys configured on the device for secure HWTACACS communication.
 - Select **TACACS+ (Cisco IOS)** from the **Authenticate Using** list.

Figure 22 Adding an AAA client

The screenshot shows the Cisco Network Configuration interface. On the left is a navigation tree with options: User Setup, Group Setup, Shared Profile Components, Network Configuration (highlighted), System Configuration, Interface Configuration, Administration Control, External User Databases, Posture Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main area is titled 'Network Configuration' with a sub-header 'Edit'. Below this is the 'Add AAA Client' form. The form contains the following fields and options:

- AAA Client Hostname: Device
- AAA Client IP Address: 10.1.1.2
- Shared Secret: expert
- RADIUS Key Wrap**
 - Key Encryption Key: [empty field]
 - Message Authenticator Code Key: [empty field]
 - Key Input Format: ☐ ASCII ☒ Hexadecimal
- Authenticate Using: TACACS+ (Cisco IOS) (dropdown menu)
- Single Connect TACACS+ AAA Client (Record stop in accounting on failure): ☐
- Log Update/Watchdog Packets from this AAA Client: ☐
- Log RADIUS Tunneling Packets from this AAA Client: ☐
- Replace RADIUS Port info with Username from this AAA Client: ☐
- Match Framed-IP-Address with user IP address for accounting packets from this AAA Client: ☐

At the bottom of the form are three buttons: Submit, Submit + Apply, and Cancel.

- d. Click **Submit + Apply**.
3. Add a user:
 - a. In the navigation tree, click **User Setup**.
 - b. On the **User Setup** page, enter **manager** in the **User** field and click **Add/Edit**, as shown in Figure 23.

Figure 23 Adding a user

The screenshot shows the Cisco User Setup interface. On the left is a navigation tree with options: User Setup (highlighted), Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Posture Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main area is titled 'User Setup' with a sub-header 'Select'. Below this is the 'Add/Edit' form. The form contains the following fields and options:

- User: manager
- Find: [button]
- Add/Edit: [button]
- List users beginning with letter/number:
 - A B C D E F G H I J K L M
 - N O P Q R S T U V W X Y Z
 - 0 1 2 3 4 5 6 7 8 9
- List all users: [button]
- Remove Dynamic Users: [button]

- c. Configure parameters for the user, including the user password and user group, as shown in Figure 24.

This example uses the default user group.

Figure 24 Configuring the user manager

The screenshot shows the Cisco User Setup web interface. On the left is a navigation menu with options: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Posture Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main content area is titled 'User Setup' and 'Edit'. Below this, it says 'User: manager (New User)'. There is a checkbox for 'Account Disabled'. A section titled 'Supplementary User Info' contains fields for 'Real Name' (admin) and 'Description' (network administrator). Another section titled 'User Setup' contains 'Password Authentication' options. It has a dropdown for 'ACS Internal Database' and a note about CiscoSecure PAP. There are fields for 'Password' and 'Confirm Password' (both masked with dots). A checkbox for 'Separate (CHAP/MS-CHAP/ARAP)' is present, followed by another set of 'Password' and 'Confirm Password' fields. A note explains that a separate CHAP password is useful for token card users. At the bottom, there is a field for 'Group to which the user is assigned:' and 'Submit' and 'Cancel' buttons.

- d. Click **Submit**.

Configuring the device

Create VLAN 2 and assign GigabitEthernet 1/0/2 to the VLAN.

```
<Device> system-view
[Device] vlan 2
[Device-vlan2] port gigabitethernet 1/0/2
[Device-vlan2] quit
```

Assign an IP address to VLAN-interface 2.

```
[Device] interface vlan-interface 2
[Device-Vlan-interface2] ip address 192.168.1.65 255.255.255.0
[Device-Vlan-interface2] quit
```

Create VLAN 3 and assign GigabitEthernet 1/0/1 to the VLAN.

```
[Device] vlan 3
[Device-vlan3] port gigabitethernet 1/0/1
[Device-vlan3] quit
```

Assign an IP address to VLAN-interface 3.

```
[Device] interface vlan-interface 3
[Device-Vlan-interface3] ip address 10.1.1.2 255.255.255.0
[Device-Vlan-interface3] quit
```

Create a local RSA key pair.

```
[Device] public-key local create rsa
The range of public key modulus is (512 ~ 4096).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
...
Create the key pair successfully.
```

Create a local DSA key pair.

```
[Device] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....
Create the key pair successfully.
```

Create a local 256-bit ECDSA key pair.

```
[Device] public-key local create ecdsa secp256r1
Generating Keys...
Create the key pair successfully.
```

Create a local 384-bit ECDSA key pair.

```
[Device] public-key local create ecdsa secp384r1
Generating Keys...
.
Create the key pair successfully.
```

Enable the Stelnet server.

```
[Device] ssh server enable
```

Enable scheme authentication on VTY user lines 0 through 63.

```
[Device] line vty 0 63
[Device-line-vty0-63] authentication-mode scheme
[Device-line-vty0-63] quit
```

Enable the default user role feature and specify **network-admin** as the default user role.

```
[Device] role default-role enable network-admin
```

Create an HWTACACS scheme named **tac**.

```
[Device] hwtacacs scheme tac
```

Specify the primary HWTACACS authentication server with the IP address 10.1.1.1 and port number 49.

```
[Device-hwtacacs-tac] primary authentication 10.1.1.1 49
```

Specify the shared key as **expert** for secure HWTACACS communication between the device and HWTACACS authentication server.

```
[Device-hwtacacs-tac] key authentication simple expert
```

Specify the primary HWTACACS authorization server with the IP address 10.1.1.1 and port number 49.

```
[Device-hwtacacs-tac] primary authorization 10.1.1.1 49
```

Specify the shared key as **expert** for secure HWTACACS communication between the device and HWTACACS authorization server.

```
[Device-hwtacacs-tac] key authorization simple expert
```

Remove the domain name from usernames sent to the HWTACACS server.

```
[Device-hwtacacs-tac] user-name-format without-domain
```

```
[Device-hwtacacs-tac] quit
```

Create an ISP domain named **bbb**, and specify the domain to use HWTACACS scheme **tac** for authentication and authorization of login users.

```
[Device] domain bbb
```

```
[Device-isp-bbb] authentication login hwtacacs-scheme tac
```

```
[Device-isp-bbb] authorization login hwtacacs-scheme tac
```

```
[Device-isp-bbb] accounting login none
```

```
[Device-isp-bbb] quit
```

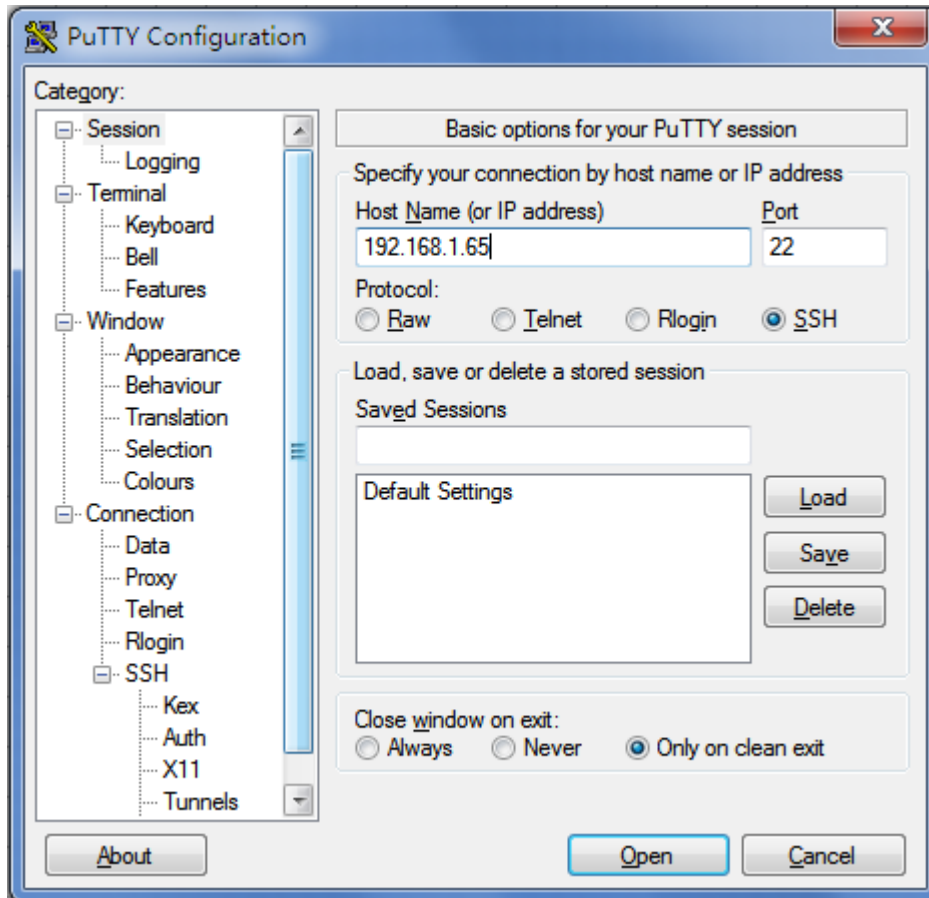
Verifying the configuration

Stelnet client software includes PuTTY and OpenSSH. This example uses an Stelnet client that runs PuTTY 0.58.

To verify that you can log into the Stelnet server from the Stelnet client:

1. Launch PuTTY.
2. From the navigation tree, click **Session**.
The **PuTTY Configuration** page appears.
3. Configure the following parameters, as shown in [Figure 25](#):
 - a. Enter **192.168.1.65** in the **Host Name (or IP address)** field.
 - b. Enter **22** in the **Port** field.
 - c. Select **SSH** for **Protocol**.

Figure 25 Specifying basic connection parameters



4. Click **Open**.

The system might display a security alert dialog box, as shown in [Figure 26](#).

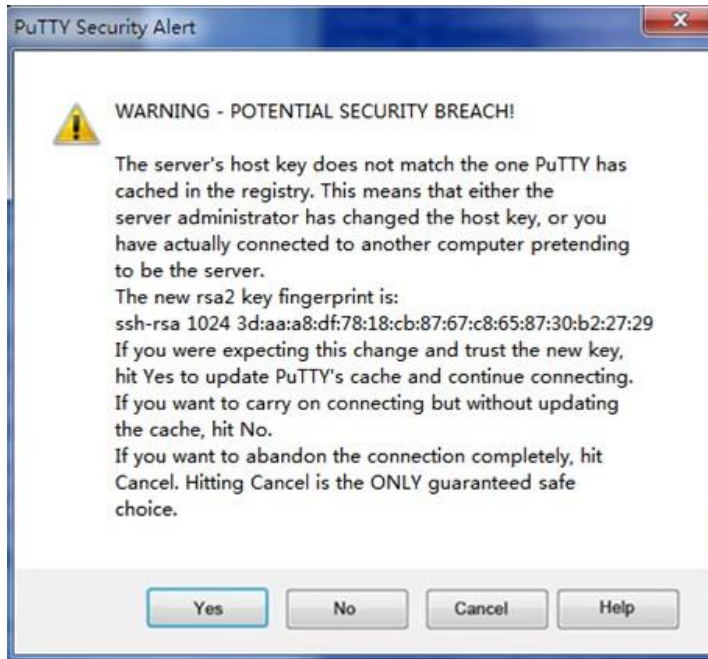
Figure 26 PuTTY Security Alert dialog box (1)



5. Click **Yes** or **No** to continue the connection.

The system might display another security alert dialog box, as shown in [Figure 27](#).

Figure 27 PuTTY Security Alert dialog box (2)



6. Click **Yes** or **No** to continue the connection.
7. Enter username **manager@bbb** and password **1234ab##** to log into the Stelnet server.

login as: manager@bbb

manager@bbb@192.168.1.65's password:

```
*****
* Copyright (c) 2004-2019 New INTELBRAS Technologies Co., Ltd. All rights
* reserved.*
* Without the owner's prior written consent,                               *
* no decompiling or reverse-engineering shall be allowed.                  *
*****
```

<Device>

Configuration files

⚠ IMPORTANT:

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

```
#
vlan 2 to 3
#
interface Vlan-interface2
 ip address 192.168.1.65 255.255.255.0
#
interface Vlan-interface3
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/2
```

```

port link-mode bridge
port access vlan 2
#
interface GigabitEthernet1/0/1
port link-mode bridge
port access vlan 3
#
line vty 0 63
authentication-mode scheme
user-role network-operator
#
ssh server enable
#
hwtacacs scheme tac
primary authentication 10.1.1.1
primary authorization 10.1.1.1
key authentication cipher $c$3$/9bCuPjMxjOtUvBx8NjtN+AnAsuLT2SrNA==
key authorization cipher $c$3$QF/fFJNv9IyKyFlsNOpeBYnDXArNhOvOdQ==
user-name-format without-domain
#
domain bbb
authentication login hwtacacs-scheme tac
authorization login hwtacacs-scheme tac
accounting login none
#
role default-role enable network-admin
#

```