

# Contents

Introduction .....	1
Prerequisites .....	1
Example: Configuring console login .....	1
Network configuration .....	1
Analysis .....	1
Applicable hardware and software versions.....	1
Restrictions and guidelines .....	3
Procedures .....	3
Verifying the configuration .....	4
Configuration files .....	5
Example: Configuring user-role based Telnet login.....	5
Network configuration .....	5
Analysis .....	6
Applicable hardware and software versions.....	6
Procedures .....	8
Verifying the configuration .....	9
Configuration files .....	10
Example: Configuring login user command authorization and accounting ...	11
Network configuration .....	11
Analysis .....	12
Applicable hardware and software versions.....	12
Restrictions and guidelines .....	14
Procedures .....	14
Configuring the HWTACACS server.....	14
Configuring the device.....	17
Verifying the configuration .....	19
Configuration files .....	21
Example: Configuring Telnet login .....	21
Network configuration .....	21
Analysis .....	22
Applicable hardware and software versions.....	22
Procedures .....	24
Verifying the configuration .....	25
Configuration files .....	25
Example: Telnetting from the device to another device.....	26
Network configuration .....	26
Analysis .....	26
Applicable hardware and software versions.....	27
Procedures .....	29
Configuring Device A .....	29
Configuring Device B .....	30
Verifying the configuration .....	30
Configuration files .....	31

# Introduction

This document provides login configuration examples. It also provides examples for implementing user access control by using command authorization and command accounting.

## 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 login management.

## Example: Configuring console login

### Network configuration

Configure console login so users must pass local authentication to log in to the device through the console port.

### Analysis

The port properties for the terminal emulation program must match the console port's default settings.

By default, a local user is assigned the user role **network-operator** and is not assigned any service type. To enable the user to log in through the console port, you must assign the **terminal** service type to the user. To enable the user to manage the device, you must assign the **network-admin** user role to the user.

### 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

For successful console port login, follow these restrictions and guidelines:

- Identify the console port carefully to make sure you are connecting to the correct port.
- Prepare a console terminal, for example, a PC. Make sure the console terminal has a terminal emulation program, such as HyperTerminal or PuTTY. For information about how to use terminal emulation programs, see the programs' user guides.

## Procedures

1. Turn off the PC if the PC is on.
2. Connect the DB-9 female connector of the console cable to the serial port of the PC.
3. Identify the console port of the device carefully and connect the RJ-45 connector of the console cable to the console port.

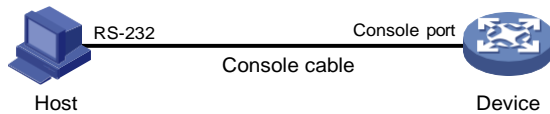
---

**ⓘ IMPORTANT:**

The serial ports on PCs do not support hot swapping. To connect a PC to an operating switch, first connect the PC end. To disconnect a PC from an operating device, first disconnect the device end.

---

**Figure 1 Connecting a configuration terminal to the console port**



4. Turn on the PC.
5. On the PC, launch the terminal emulation program, and create a connection that uses the serial port connected to the device. Set the port properties so the port properties match the following console port default settings:
  - o **Bits per second**—9600 bps.
  - o **Flow control**—None.
  - o **Parity**—None.
  - o **Stop bits**—1.
  - o **Data bits**—8.

6. Power on the device and press **Enter** as prompted.  
The user view prompt appears. You can enter commands to configure or manage the device. To get help, enter ?.

7. Configure AUX line 0:

# Enter AUX line view.

```
<Sysname> system-view
```

```
[Sysname] line aux 0
```

# Enable scheme authentication to use AAA to authenticate the console login user.

```
[Sysname-line-aux0] authentication-mode scheme
```

```
[Sysname-line-aux0] quit
```

# Create the local user **admin**.

```
[Sysname] local-user admin class manage
```

New local user added.

# Set the password to **hello12345** (plain text) for the local user.

```
[Sysname-luser-manage-admin] password simple hello12345
```

# Assign the **terminal** service type and the **network-admin** user role to the user. Reclaim the default user role.

```
[Sysname-luser-manage-admin] service-type terminal
```

```
[Sysname-luser-manage-admin] authorization-attribute user-role network-admin
```

```
[Sysname-luser-manage-admin] undo authorization-attribute user-role  
network-operator
```

```
[Sysname-luser-manage-admin] quit
```

## Verifying the configuration

Log in to the device through the console port again, and press **Enter** and enter the username **admin** and password **hello12345** as prompted.

Line aux0 is available.

Press ENTER to get started.

Login: admin

Password:

```
*****
* Copyright (c) 2004-2021 Intelbras S.A, All rights reserved.*
* Without the owner's prior written consent, *
* no decompiling or reverse-engineering shall be allowed. *
*****
<Sysname>
```

## Configuration files

```
#
line aux 0
    authentication-mode scheme
    user-role network-admin
#
local-user admin class manage
    password hash $h$6$RgG+mm4RKXICN1tY$ld6pV+qB2a/BBFXVnqocFJjYgx/EKCYod9tHmGRP8AA
    1qnbeRcB6Bd4jW+cteG9aY2Gc+J8JqLHsWwvtnLyEAw==
    service-type terminal
    authorization-attribute user-role network-admin
#
```

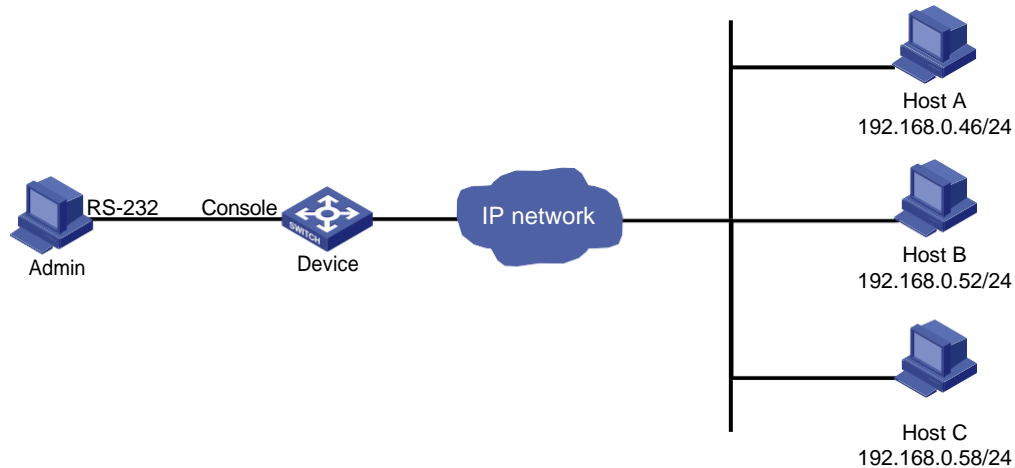
## Example: Configuring user-role based Telnet login

### Network configuration

As shown in [Figure 2](#), users need to log in to the device remotely to manage the device.

- Configure Telnet login to enable users to Telnet to the device.
- Configure Telnet user authentication so a Telnet user must provide the correct username and password at login.
- Configure access control so only Telnet users at 192.168.0.46/24 and 192.168.0.52/24 can Telnet to the device.
- Configure two local users.
  - One local user can manage the device.
  - One local user can use only the read commands of features.

Figure 2 Network diagram



## Analysis

Telnet service is disabled by default. To enable Telnet login, you must enable Telnet service.

To control Telnet login, configure an ACL to permit access only from the specified IP addresses.

By default, a local user is assigned the user role **network-operator**. To restrict a local user to read commands, you must create a user role that can access only read 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 3170 switch series	Release 11xx
SC 5520 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
SC 5525 switch series	Release 63xx, Release 65xx, Release 6615Pxx,
SC 3130 switch series	Release 63xx
SC 3570 switch series	Release 11xx

# Procedures

# Log in to the device through the console port. (Details not shown.)

# Enable Telnet service.

```
<Sysname> system-view
[Sysname] telnet server enable
```

# Enable scheme authentication to use AAA to authenticate the Telnet login user.

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

# Create the local user **userA**. Set the password to **hello12345** (plain text).

```
[Sysname] local-user userA class manage
New local user added.
[Sysname-luser-manage-userA] password simple hello12345
```

# Assign the Telnet service type and the **network-admin** user role to the user. Reclaim the default user role.

```
[Sysname-luser-manage-userA] authorization-attribute user-role network-admin
[Sysname-luser-manage-userA] service-type telnet
[Sysname-luser-manage-userA] undo authorization-attribute user-role network-operator
[Sysname-luser-manage-userA] quit
```

# Create user role **roleB**. Add rule 1 to permit the user role to access read commands of all features.

```
[Sysname] role name roleB
[Sysname-role-roleB] rule 1 permit read feature
[Sysname-role-roleB] quit
```

# Create the local user **userB**. Set the password to **hello12345** (plain text).

```
[Sysname] local-user userB class manage
```



New local user added.

```
[Sysname-luser-manage-userB] password simple hello12345
```

**# Assign the Telnet service type and the **roleB** user role to the user. Reclaim the default user role.**

```
[Sysname-luser-manage-userB] authorization-attribute user-role roleB
```

```
[Sysname-luser-manage-userB] service-type telnet
```

```
[Sysname-luser-manage-userB] undo authorization-attribute user-role network-operator
```

```
[Sysname-luser-manage-userB] quit
```

**# Create ACL 2000 and add rules to permit only access from 192.168.0.46 and 192.168.0.52.**

```
[Sysname] acl basic 2000
```

```
[Sysname-acl-ipv4-basic-2000] rule 1 permit source 192.168.0.46 0
```

```
[Sysname-acl-ipv4-basic-2000] rule 2 permit source 192.168.0.52 0
```

```
[Sysname-acl-ipv4-basic-2000] rule 3 deny source any
```

```
[Sysname-acl-ipv4-basic-2000] quit
```

**# Apply the ACL to filter Telnet logins.**

```
[Sysname] telnet server acl 2000
```

## Verifying the configuration

1. Telnet to the device from Host A, and enter the username **userA** and password **hello12345** as prompted.
2. Display the commands available in user view.

The commands for device configuration and management are included in the list.

Login: userA

Password:

```
*****
* Copyright (c) 2004-2021 Intelbras S.A, All rights reserved.*
* Without the owner's prior written consent,                      *
* no decompiling or reverse-engineering shall be allowed.         *
*****
```

<Sysname> ?

User view commands:

archive	Archive configuration
arp	Address Resolution Protocol (ARP) module
backup	Backup operation
boot-loader	Software image file management
bootrom	Update/read/backup/restore bootrom
cd	Change current directory
cfg	Connectivity Fault Detection (CFD) module
clock	Specify the system clock
copy	Copy a file
create	Create a file
debugging	Enable system debugging functions
delete	Delete a file
diagnostic-logfile	Diagnostic log file configuration
dir	Display files and directories on the storage media
display	Display current system information

```

erase          Alias for 'delete'
exception      Exception information configuration
exit          Alias for 'quit'
fdisk          Partition a storage medium
fixdisk        Check and repair a storage medium
format         Format a storage medium
free           Release a connection
ftp            Open an FTP connection

```

----- More -----

3. Telnet to the device from Host B, and enter the username **userB** and password **hello12345** as prompted.

4. Display the commands available in user view.

Only read commands are displayed.

Login: userB

Password:

```

*****
* Copyright (c) 2004-2021 Intelbras S.A, All rights reserved.*
* Without the owner's prior written consent,                      *
* no decompiling or reverse-engineering shall be allowed.         *
*****

```

<Sysname> ?

User view commands:

```

dir            Display files and directories on the storage media
display        Display current system information
erase          Alias for 'delete'
exit           Alias for 'quit'
md5sum         Compute the hash digest of a file using the MD5 algorithm
more           Display the contents of a file
no             Alias for 'undo'
pwd            Display current working directory
quit           Exit from current command view
sha256sum      Compute the hash digest of a file using the SHA256 algorithm
show           Alias for 'display'
system-view    Enter the System View
write          Alias for 'save'

```

<Sysname>

5. Telnet to the device from Host C.

Your access request is rejected.

## Configuration files

```

#
telnet server enable
telnet server acl 2000
#
acl basic 2000

```

```

rule 1 permit source 192.168.0.46 0
rule 2 permit source 192.168.0.52 0
rule 3 deny
#
line vty 0 63
 authentication-mode scheme
 user-role network-operator
#
local-user userA class manage
 password hash $h$6$I2Sg4LljlqVUWQZ3$JA6KkU3zfVVRg48MM92X6cVpdiqR2JF887PKi3GQMwn
XXXcsWBuz7GIeJZeeNFMmMBaV7DPkKblnb0sGT2axvg==
 service-type telnet
 authorization-attribute user-role network-admin
#
local-user userB class manage
 password hash $h$6$q+c3OcSxrPpDpsDf$BWkgfOyxBLyR5zyYgF/+VvN/lofy8lzoHDlFf800jDl
a6/EiSJbSBl33PeazilSkWSYcttkg5v5bGecB7oYwAw==
 service-type telnet
 authorization-attribute user-role roleB
#
role name roleB
 rule 1 permit read feature
#

```

## Example: Configuring login user command authorization and accounting

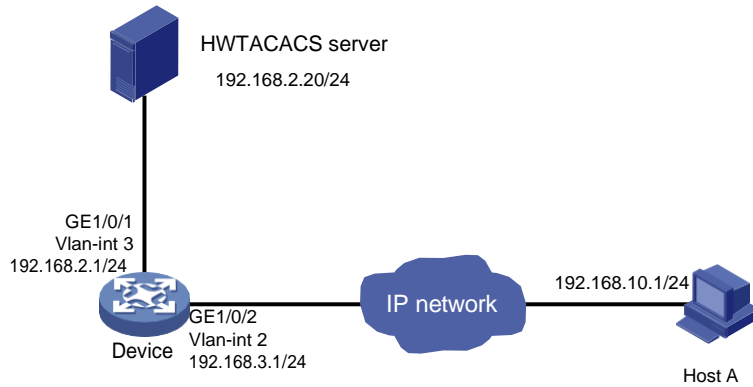
### Network configuration

As shown in [Figure 3](#), Host A needs to log in to the device to manage the device.

For device security purposes, configure the device to perform the following tasks:

- Allow Host A to Telnet in after authentication.
- Use the HWTACACS server to control the commands that the user can execute.
- Send commands executed by users to the HWTACACS server to monitor and control user operations on the device.

**Figure 3 Network diagram**



## Analysis

To implement command authorization and accounting, you must perform the following tasks:

- Enable scheme authentication and configure a HWTACACS scheme on the device.
- Configure an account on the HWTACACS server for the Telnet user and assign commands for the user to use.

## 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 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

The command authorization function takes effect immediately after you execute the **command authorization** command. Before executing this command, you must complete the following tasks:

- Configure a user account on the HWTACACS server and specify the commands for the user to use.
- Configure the required HWTACACS scheme on the device.

## Procedures

### Configuring the HWTACACS server

In this example, the HWTACACS server runs on INC PLAT 7.1 (E0302) and INC INC - EIA 7.1 (E0301).

1. Add a device area:
  - a. Log in to INC.
  - b. Click the **User** tab.
  - c. From the navigation tree, select **Device User Policy > Authorization Conditions > Device Areas**.
  - d. Click **Add**.
  - e. Set the area name to **system** and click **OK**.

**Figure 4 Adding a device area**

User > Device User Policy > Authorization Conditions > Device Areas > Add Device Area [? Help](#)

Device Area Details	
Area Name *	system ?
Parent Area Name	--
Description	

OK Cancel

2. Add a device:
  - a. From the navigation tree, select **Device User Policy > Device Management**.
  - b. Click **Add**.
  - c. Enter **expert** for both **Shared Key** and **Confirm Shared Key**.
  - d. Set the authentication port to **49**.
  - e. Select the device area **system**.
  - f. Select **Not Supported** for **Single Connection** to disable establishing multiple sessions over a single TCP connection.
  - g. Select **Not Supported** for **Watchdog** to disable the device from sending watchdog packets while the user is online.
  - h. In the **Device Management** area, click **Add Manually**.
  - i. Enter the IP address **192.168.2.1** and click **OK**.
  - j. Click **OK**.

**Figure 5 Adding a device**

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

**Device Configuration**

Shared Key \*

.....

?

Confirm Shared Key \*

.....

?



Authentication Port \*

49



?

Device Area

system

Device Type

Single Connection \*

Not Supported

Watchdog \*

Not Supported

Description

**Device Management**

Select

Add Manually

Clear All

Device Name	Device IP	Device Model	Delete
	192.168.2.1		

Total Items: 1.

OK

Cancel

3. Add a shell profile:
  - a. From the navigation tree, select **Device User Policy > Authorization Command > Shell Profiles**.
  - b. Click **Add**.
  - c. Enter the profile name **Shell Profile1**.
  - d. Select the privilege Level **1**.
  - e. Click **OK**.

**Figure 6 Adding a shell profile**

User > Device User Policy > Authorization Command > Shell Profiles > Add Shell Profile ? Help

Add Shell Profile

Shell Profile Name \*

Shell Profile1

ACL

?

Privilege Level

1

Idle Time

Minutes

Session Lifetime

Minutes

Auto Run

Custom Attribute

Add Attribute

?

Description

OK

Cancel

4. Add an authorization policy:
  - a. From the navigation tree, select **Device User Policy > Authorization Policies**.
  - b. Click **Add**.
  - c. Enter the policy name **tac**.
  - d. In the **Access Authorization Info** area, click **Add** to configure access authorization information.
  - e. Select **system** for **Device Area**, **Unlimited** for **Device Type** and **Authorized Time Range**.
  - f. Select the shell profile **Shell Profile1**.
  - g. Select **Unlimited** for **Authorization Command Set** and click **OK**.
  - h. Click **OK**.

**Figure 7 Configuring access authorization information**

Access Authorization

Device Area

system

Device Type

Unlimited

Authorized Time Range

Unlimited

Shell Profile

Shell Profile1

Authorization Command Set

Unlimited

OK

Cancel

**Figure 8 Adding an authorization policy**

User > Device User Policy > Authorization Policies > Add Authorization Policy Help

Authorization Policy Info

**Basic Information**

Authorization Policy Name \*  ?

Description

☐ Enable RSA

**Access Authorization Info**

Device Area	Device Type	Authorized Time F	Shell Profile	Authorization C	Priority	Modify	Delete
system	Unlimited	Unlimited	Shell Profile1	Unlimited	↑↓	✎	🗑
Unlimited	Unlimited	Unlimited	Deny	Forbid		✎	

5. Add a device user:
  - a. From the navigation tree, select **Device User > All Device Users**.
  - b. Click **Add**.
  - c. Enter the account name **monitor** and username **telnet-user**.
  - d. Enter the login password **hello12345** and confirm the password.
  - e. Select the user authorization policy **tac**.
  - f. Enter **5** for **Max. Online Users** to limit the number of online users that use the account.
  - g. Click **OK**.

**Figure 9 Adding a device user**

User > Device User > All Device Users > Add Device User Help

Add Device User

Account Name \*  ? User Name

Login Password \*  Confirm Login Password \*

Device User Group \*

Group Authorization Policy  User Authorization Policy

Max. Online Users  Expiration Date

☐ Enable Privilege-Increase Password ☐ Enable Password Strategy

**Tips**  
Login the TAM Self-Service Center , device users go to address <http://IMC primary server address:port/imc/noAuth/tam/login.jsf>

## Configuring the device

# Assign IP addresses to relevant interfaces. Make sure the device and the HWTACACS server can reach each other, and the device and Host A can reach each other. (Details not shown.)

# Enable Telnet service.

```
<Sysname> system-view
```



```
[Sysname] telnet server enable
```

**# Create the HWTACACS scheme **tac**.**

```
[Sysname] hwtacacs scheme tac
Create a new HWTACACS scheme.
```

**# Configure the scheme to use the HWTACACS server at 192.168.2.20:49 for authentication, authorization, and accounting.**

```
[Sysname-hwtacacs-tac] primary authentication 192.168.2.20 49
[Sysname-hwtacacs-tac] primary authorization 192.168.2.20 49
[Sysname-hwtacacs-tac] primary accounting 192.168.2.20 49
```

**# Set the shared keys to **expert**.**

```
[Sysname-hwtacacs-tac] key authentication simple expert
[Sysname-hwtacacs-tac] key authorization simple expert
[Sysname-hwtacacs-tac] key accounting simple expert
```

**# Remove domain names from usernames sent to the HWTACACS server.**

```
[Sysname-hwtacacs-tac] user-name-format without-domain
[Sysname-hwtacacs-tac] quit
```

**# Configure the system-predefined domain **system**.**

```
[Sysname] domain system
```

**# Use the HWTACACS scheme **tac** for login user authentication, authorization, and accounting. Use local authentication, authorization, and accounting as the backup method.**

```
[Sysname-isp-system] authentication login hwtacacs-scheme tac local
[Sysname-isp-system] authorization login hwtacacs-scheme tac local
[Sysname-isp-system] accounting login hwtacacs-scheme tac local
```

**# Use the HWTACACS scheme **tac** for command authorization and accounting. Use local authorization as the backup command authorization method.**

```
[Sysname-isp-system] authorization command hwtacacs-scheme tac local
[Sysname-isp-system] accounting command hwtacacs-scheme tac
[Sysname-isp-system] quit
```

**# Create the local user **monitor**. Set the password to **hello12345** (plain text).**

```
[Sysname] local-user monitor class manage
New local user added.
[Sysname-luser-manage-monitor] password simple hello12345
```

**# Assign the Telnet service type and the **level-1** user role to the user. Reclaim the default user role.**

```
[Sysname-luser-manage-monitor] service-type telnet
[Sysname-luser-manage-monitor] authorization-attribute user-role level-1
[Sysname-luser-manage-monitor] undo authorization-attribute user-role network-operator
[Sysname-luser-manage-monitor] quit
```

**# Enable scheme authentication to use AAA to authenticate the Telnet login user.**

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

**# Enable command authorization and command accounting.**

```
[Sysname-line-vty0-63] command authorization
[Sysname-line-vty0-63] command accounting
[Sysname-line-vty0-63] quit
```

# Verifying the configuration

## 1. Verify the command authorization feature:

# Telnet to the device, and enter the username **monitor** and password **hello12345**.

```
C:\Documents and Settings\Administrator> telnet 192.168.2.1
```

```
Login: monitor
```

```
Password:
```

```
*****
* Copyright (c) 2004-2021 Intelbras S.A, All rights reserved.*
* Without the owner's prior written consent,                      *
* no decompiling or reverse-engineering shall be allowed.         *
*****
```

# Display commands available in user view and system view. Only commands permitted by the level-1 user role are displayed.

```
<Sysname> ?
```

User view commands:

display	Display current system information
erase	Alias for 'delete'
exit	Alias for 'quit'
mtrace	Configure the multicast traceroute
no	Alias for 'undo'
ping	Ping function
quit	Exit from current command view
show	Alias for 'display'
ssh2	Establish an Stelnet connection to an Stelnet server
super	Switch to a user role
system-view	Enter the System View
telnet	Establish a telnet connection
tracert	Tracert function
write	Alias for 'save'

```
<Sysname> system-view
```

```
[Sysname] ?
```

System view commands:

access-list	Alias for 'acl'
display	Display current system information
end	Alias for 'return'
erase	Alias for 'delete'
exit	Alias for 'quit'
hostname	Alias for 'sysname'
logging	Alias for 'info-center'
mtrace	Configure the multicast traceroute
no	Alias for 'undo'
ping	Ping function
quit	Exit from current command view
return	Exit to User View
show	Alias for 'display'

tracert            Tracert function  
write            Alias for 'save'

2. Verify the command accounting feature:

- a. Log in to INC.
- b. Click the **User** tab.
- c. From the navigation tree, select **Device User > Log Management > Audit Logs**.
- d. In the **Query Audit Logs** area, enter the account name **monitor**, select the audit time range, and click **Query**.

A log for user **monitor** shows that the user executed the **system-view** command.

**Figure 10 Querying audit logs**

User > Device User > Log Management > Audit Logs

★ Add to My Favorites ? Help

Query Audit Logs Advanced Query

Account Name  Audit Type

Audit Time From  To

Audit Log List

Login Name	Account Name	CLI	Audit Type	Audit Time	Device IP	Details
monitor	monitor	system-view	Enter Command At CLI	2014-08-06 20:10:29	192.168.2.1	
monitor	monitor		Start	2014-08-06 20:10:26	192.168.2.1	

1-2 of 2. Page 1 of 1.

- e. Click the **Details** icon for the log of the **Start** audit type.

**Figure 11 Displaying details about the log of the Start audit type**

User > Device User > Log Management > Audit Logs > Audit Log Details

Audit Log Details

Login Name monitor

Account Name monitor

Device User Group Ungrouped

Privilege Level 1

CLI system-view

Task ID 0

Audit Time 2014-08-06 20:10:26

Audit Type Start

Device IP 192.168.2.1

User IP 192.168.10.1

Terminal vty0

Session ID 89715277

Serial Number 1

- f. Click the **Details** icon for the log of the **Enter Command At CLI** audit type.

**Figure 12 Displaying details about the log of the Enter Command At CLI audit type**

User > Device User > Log Management > Audit Logs > Audit Log Details

Audit Log Details

Login Name monitor

Account Name monitor

Device User Group Ungrouped

Privilege Level 1

CLI system-view

Task ID 0

Audit Time 2014-08-06 20:10:29

Audit Type Enter Command At CLI

Device IP 192.168.2.1

User IP 0.0.0.0

Terminal vty0

Session ID 1674910879

Serial Number 1

# Configuration files

```
#
telnet server enable
#
hwtacacs scheme tac
primary authentication 192.168.2.20
primary authorization 192.168.2.20
primary accounting 192.168.2.20
key authentication cipher $c$3$F1lMn3wBsh+vH6otPvoz+AdE7VaNS3c0Pw==
key authorization cipher $c$3$2x6XI5xU7UGX6VqWFXNp2n3FG07uTNjiQw==
key accounting cipher $c$3$2oKsuCOAZXl+3ibvTPxnJlYvJlMHqv73Lw==
user-name-format without-domain
#
domain system
authentication login hwtacacs-scheme tac local
authorization login hwtacacs-scheme tac local
accounting login hwtacacs-scheme tac local
authorization command hwtacacs-scheme tac local
accounting command hwtacacs-scheme tac
#
local-user monitor class manage
password hash $h$6$5BqWnAJTpBbU5NbY$PbdgF+43eE5WMvj2iHPySfd5nGqj5AhDCDOXTiUMJvR
FFVsZaF8EWltgpsQPRSq7SDKaGqwHTy9nsabAoGNaYg==
service-type telnet
authorization-attribute user-role level-1
#
line vty 0 63
authentication-mode scheme
user-role network-operator
idle-timeout 0 0
command authorization
command accounting
#
```

## Example: Configuring Telnet login

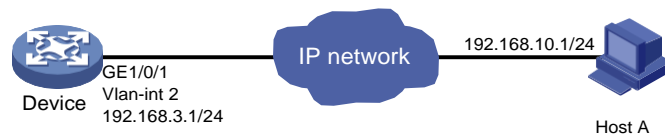
### Network configuration

As shown in [Figure 13](#), users need to log in to the device remotely to manage the device.

- Configure Telnet login to enable users to Telnet to the device.
- Configure Telnet user authentication so a Telnet user must provide the correct username and password at login.
- Configure the device to send up to 20 lines to the configuration terminal at a time.
- Set the command history buffer size to 100.

- Set the maximum number of concurrent Telnet users to 10.
- Set the session idle timeout to 20 minutes.

**Figure 13 Network diagram**



## Analysis

Telnet service is disabled by default. To enable Telnet login, you must enable Telnet service.

By default, a local user is assigned the user role **network-operator**. To allow the user to use all commands on the device, assign the user role **network-admin** to the user.

## 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 3170 switch series	Release 11xx
SC 3130 switch series	Release 63xx
SC 5525 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
SC 5520 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx



# Procedures

# Log in to the device through the console port. (Details not shown.)

# Change the device name and enable Telnet service.

```
<Sysname> system-view
[Sysname] sysname Device
[Device] telnet server enable
```

# Assign IP addresses to interfaces.

```
[Device] vlan 2
[Device-vlan2] port gigabitethernet 1/0/1
[Device-vlan2] quit
[Device] interface vlan-interface 2
[Device-Vlan-interface2] ip address 192.168.3.1 24
[Device-Vlan-interface2] quit
```

# Enable scheme authentication to use AAA to authenticate the Telnet login user.

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

# Configure common VTY line settings.

```
[Device-line-vty0-63] screen-length 20
[Device-line-vty0-63] history-command max-size 100
[Device-line-vty0-63] idle-timeout 20
[Device-line-vty0-63] quit
```

# Set the maximum number of concurrent Telnet users to 10.

```
[Device] aaa session-limit telnet 10
```

# Create the local user **test**. Set the password to **hello12345** (plain text).

```
[Device] local-user test class manage
New local user added.
[Device-luser-manage-test] password simple hello12345
```

# Assign the Telnet service type and the **network-admin** user role to the user. Reclaim the default user role.

```
[Device-luser-manage-test] service-type telnet
[Device-luser-manage-test] authorization-attribute user-role network-admin
[Device-luser-manage-test] undo authorization-attribute user-role network-operator
[Device-luser-manage-test] quit
```

# Verifying the configuration

1. Telnet to the device from Host A, and enter the username **test** and password **hello12345**.

If the number of online Telnet users is less than 20, you are logged in to the system.

```
Login: test
```

```
Password:
```

```
*****
* Copyright (c) 2004-2021 Intelbras S.A, All rights reserved.*
* Without the owner's prior written consent,                      *
* no decompiling or reverse-engineering shall be allowed.         *
*****
```

```
<Device>
```

If the number of concurrent Telnet users has reached the maximum number, an error message is displayed.

```
C:\Users\zhangsan>telnet 192.168.3.1
```

```
Trying 192.168.3.1 ...
```

```
Press CTRL+K to abort
```

```
Connected to 192.168.3.1 ...
```

```
The connection was closed by the remote host!
```

2. After login, do not perform any operations within 20 minutes.

You are logged out.

```
Inactive timeout reached, logging out.
```

```
The connection was closed by the remote host!
```

## Configuration files



### IMPORTANT:

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

```
#
 sysname Device
#
telnet server enable
#
interface Vlan-interface2
 ip address 192.168.3.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
line vty 0 63
 authentication-mode scheme
 user-role network-operator
```



```

idle-timeout 20 0
screen-length 20
history-command max-size 100
#
aaa session-limit telnet 10
#
local-user test class manage
password hash $h$6$/Xa6qIOOrThQEVqbK$C00MPM5UaYoigaOfflWhpTskb/uB80yZ9006tpztnDe
vrFEHqkvxfkSb4hUadHuknPSnjLNQByztfr30cP/Hlg==
service-type telnet
authorization-attribute user-role network-admin
#

```

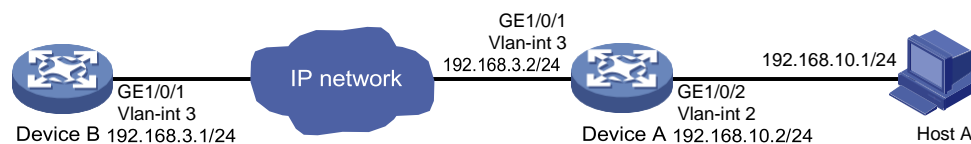
## Example: Telnetting from the device to another device

### Network configuration

As shown in [Figure 14](#), the user connected to Device A needs to Telnet to Device B to manage Device B.

- Configure Telnet login to enable users to Telnet to Device A and Device B.
- Configure Telnet user authentication on Device A so a Telnet user must provide the correct username and password to log in to Device A.
- Configure access control so only Telnet users at 192.168.10.1/24 can Telnet to Device A and only Device A can Telnet to Device B.
- Configure the devices to send up to 20 lines to the configuration terminal at a time.
- Set the command history buffer size to 100.
- Set the session idle timeout to 20 minutes.

**Figure 14 Network diagram**



### Analysis

Telnet service is disabled by default. To enable Telnet login, you must enable Telnet service.

By default, a local user is assigned the default user role **network-operator**. To allow the user to use all commands on the device, assign the user role **network-admin** to the user.

To control Telnet login, configure an ACL on each device to permit access only from the specified IP address.

# 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 Device A

# Log in to Device A through the console port. (Details not shown.)

# Change the device name and enable Telnet service.

```
<Sysname> system-view
[Sysname] sysname DeviceA
[DeviceA] telnet server enable
```

# Assign IP addresses to interfaces.

```
[DeviceA] vlan 3
[DeviceA-vlan3] port gigabitethernet 1/0/1
[DeviceA-vlan3] quit
[DeviceA] interface vlan-interface 3
[DeviceA-Vlan-interface3] ip address 192.168.3.2 24
[DeviceA-Vlan-interface3] quit
[DeviceA] vlan 2
[DeviceA-vlan2] port gigabitethernet 1/0/2
[DeviceA-vlan2] quit
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] ip address 192.168.10.2 24
[DeviceA-Vlan-interface2] quit
```

# Enable scheme authentication to use AAA to authenticate the Telnet login user.

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

# Configure common VTY line settings.

```
[DeviceA-line-vty0-63] screen-length 20
[DeviceA-line-vty0-63] history-command max-size 100
[DeviceA-line-vty0-63] idle-timeout 20
[DeviceA-line-vty0-63] protocol inbound telnet
[DeviceA-line-vty0-63] quit
```

# Create the local user **test**. Set the password to **hello12345** (plain text).

```
[DeviceA] local-user test class manage
New local user added.
[DeviceA-luser-manage-test] password simple hello12345
```

# Assign the Telnet service type and the **network-admin** user role to the user. Reclaim the default user role.

```
[DeviceA-luser-manage-test] service-type telnet
[DeviceA-luser-manage-test] authorization-attribute user-role network-admin
[DeviceA-luser-manage-test] undo authorization-attribute user-role network-operator
[DeviceA-luser-manage-test] quit
```

# Create ACL 2000 and add rules to permit only access from 192.168.10.1.

```
[DeviceA] acl basic 2000
[DeviceA-acl-ipv4-basic-2000] rule 1 permit source 192.168.10.1 0
[DeviceA-acl-ipv4-basic-2000] rule 2 deny source any
[DeviceA-acl-ipv4-basic-2000] quit
```

# Apply the ACL to filter Telnet logins.

```
[DeviceA] telnet server acl 2000
```

## Configuring Device B

# Log in to Device B through the console port. (Details not shown.)

# Change the device name and enable Telnet service.

```
<Sysname> system-view
```

```
[Sysname] sysname DeviceB
```

```
[DeviceB] telnet server enable
```

# Assign IP addresses to interfaces.

```
[DeviceB] vlan 3
```

```
[DeviceB-vlan3] port gigabitethernet 1/0/1
```

```
[DeviceB-vlan3] quit
```

```
[DeviceB] interface vlan-interface 3
```

```
[DeviceB-Vlan-interface3] ip address 192.168.3.1 24
```

```
[DeviceB-Vlan-interface3] quit
```

# Disable authentication for the Telnet login user.

```
[DeviceB] line vty 0 63
```

```
[DeviceB-line-vty0-63] authentication-mode none
```

# Configure common VTY line settings.

```
[DeviceB-line-vty0-63] screen-length 20
```

```
[DeviceB-line-vty0-63] history-command max-size 100
```

```
[DeviceB-line-vty0-63] idle-timeout 20
```

```
[DeviceB-line-vty0-63] protocol inbound telnet
```

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

# Create ACL 2000 and add rules to permit only access from 192.168.3.2.

```
[DeviceB] acl basic 2000
```

```
[DeviceB-acl-ipv4-basic-2000] rule 1 permit source 192.168.3.2 0
```

```
[DeviceB-acl-ipv4-basic-2000] rule 2 deny source any
```

```
[DeviceB-acl-ipv4-basic-2000] quit
```

# Apply the ACL to filter Telnet logins.

```
[DeviceB] telnet server acl 2000
```

## Verifying the configuration

1. Telnet to Device A from Host A and enter the username **test** and password **hello12345**. You are logged in to the system.

```
Login: test
```

```
Password:
```

```
*****
```

```
* Copyright (c) 2004-2021 Intelbras S.A, All rights reserved.*
```

```
* Without the owner's prior written consent, *
```

```
* no decompiling or reverse-engineering shall be allowed. *
```

```
*****
```

```
<DeviceA>
```

If you use another host to Telnet to Device A, your access request is rejected.

```
C:\Users\zhangsan>telnet 192.168.10.2
Trying 192.168.10.2 ...
Press CTRL+K to abort
Connected to 192.168.10.2 ...
Failed to connect to the remote host!
```

**2. After login, do not perform any operations in 20 minutes.**

You are logged out.

```
<DeviceA>
Inactive timeout reached, logging out.
```

The connection was closed by the remote host!

**3. Telnet from Device A to Device B.**

You are logged in to the system.

```
<DeviceA>telnet 192.168.3.1
Trying 192.168.3.1 ...
Press CTRL+K to abort
Connected to 192.168.3.1 ...
*****
* Copyright (c) 2004-2021 Intelbras S.A, All rights reserved.*
* Without the owner's prior written consent,                      *
* no decompiling or reverse-engineering shall be allowed.         *
*****
```

```
<DeviceB>
```

If you use another host or device to Telnet to Device B, your access request is rejected.

```
<Device> telnet 192.168.3.1
Trying 192.168.3.1 ...
Press CTRL+K to abort
Connected to 192.168.3.1 ...
Failed to connect to the remote host!
```

**4. After login, do not perform any operations within 20 minutes.**

You are logged out.

## Configuration files



**IMPORTANT:**

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

- Device A:

```
#
sysname DeviceA
#
telnet server enable
telnet server acl 2000
#
interface Vlan-interface2
```

```

ip address 192.168.10.2 255.255.255.0
#
interface Vlan-interface3
ip address 192.168.3.2 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-mode bridge
port access vlan 3
#
interface GigabitEthernet1/0/2
port link-mode bridge
port access vlan 2
#
line vty 0 63
authentication-mode scheme
user-role network-operator
protocol inbound telnet
idle-timeout 20 0
screen-length 20
history-command max-size 100
#
acl basic 2000
rule 1 permit source 192.168.10.1 0
rule 2 deny source any
#
local-user test class manage
password hash $h$6$V5dw8qzFDLAOmDzx$upf9K29n110G6OGdSXI0t69IoE5eot/Qh9Iuv/hptq6
2vxUq3867QbUBzmc6/hHwIfVQcDC8gVWpGvDQWXQTSQ==
service-type telnet
authorization-attribute user-role network-admin
#

```

- **Device B:**

```

#
sysname DeviceB
#
telnet server enable
telnet server acl 2000
#
interface Vlan-interface3
ip address 192.168.3.1 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-mode bridge
port access vlan 3
#
line vty 0 63
authentication-mode none
user-role network-operator

```

```
protocol inbound telnet
idle-timeout 20 0
screen-length 20
history-command max-size 100
#
acl basic 2000
rule 1 permit source 192.168.3.2 0
rule 2 deny source any
#
```