Contents

1 Configuring Basic Management

1.1 Overview

Basic management refers to a series of basic network device management functions, including monitoring and maintenance. This document describes the principles, configuration methods, and configuration examples of these basic management functions.

1.2 Basic Concepts

Table 1-1Basic Concepts

Concept	Description
TFTP	The Trivial File Transfer Protocol (TFTP) is a protocol used for simple file transfer between a client and a server in the Transmission Control Protocol (TCP)/Internet Protocol (IP) suite.
AAA	Authentication, Authorization and Accounting (AAA), including: ● Authentication: Verifies user identities and available network services. ● Authorization: Grants network services to users according to authentication results. ● Accounting: Records the network service consumption of users and to send the records to the billing system. After the AAA mode is enabled, some servers (or the local user database) are used to authenticate users' management permissions according to their usernames and password at terminal login and the configured AAA login authentication method list. For details about AAA, see "Configuring AAA" in the *Security Configuration Guide*.
RADIUS	The Remote Authentication Dial In User Service (RADIUS) is the most widely used AAA protocol.
Telnet	Telnet is a terminal emulation protocol in the TCP/IP protocol suite which provides a connection to a remote host by creating a virtual terminal. It is a standard protocol at Layer 7 (application layer) of the Open System Interconnection (OSI) model and is used on the Internet for remote login. During remote login through telnet, users must enter the usernames and passwords for authentication. Telnet sets up a connection between the local personal computer (PC) and a remote host.
System information	System information includes the system description, system power-on time, system hardware and software versions, control-layer software version, and boot-layer software version.
Hardware information	Hardware information includes the physical device information as well as information

Concept	Description
	about pluggable modules on the device. ● The device information includes the device description and slot quantity. ● The slot information includes the slot ID, module description (which is empty if a slot does not have a module), number of physical ports on a module inserted into a slot, and maximum number of ports supported by a slot.
System configurations	System configurations include: ● Running configurations: Configurations running on all component modules of the system. ● Startup configurations: Configurations stored in the non-volatile random-access memory (NVRAM) of the system.

1.3 Configuration Task Summary

All the following configuration tasks are optional and may be selected as needed.

- Configuring Passwords and Privilege Levels
- Configuring Login and Authentication
- Configuring Basic System Parameters
- Enabling or Disabling a Specific Service
- Rolling Back System Configurations
- Configuring Multiple-configuration Booting
- Configuring a Restart Policy
- Running Batch File Commands
- Configuring the Telnet Service
- Configuring Automatic Configuration File Backup to a Remote Server

1.4 Configuring Passwords and Privilege Levels

1. Overview

Passwords and privilege levels can be configured to control network terminals' access to network devices.

16 privilege levels from 0 to 15 are defined for users in the command line interface (CLI) of network devices. Users of various privilege levels can run different commands. A smaller value indicates a lower privilege level. Level 0 is the lowest level and users of this level can run only a few commands, whereas level 15 is the highest level and users of this level can run all commands. Levels 0 and 1 are common user levels without the device configuration permission (users are not allowed to enter the global configuration mode). Levels 2 to 15 are privileged user levels with the device configuration permission.

Password protection is configured for each privilege level on the device so that users of different levels can use different command collections. An increase in privilege level requires the input of the correct password of the target privilege level, whereas a reduction in privilege level does not require password input.

Passwords fall into two types: passwords and secrets.

- Passwords are simple encrypted passwords. You can set them for privilege levels 1 to 15.
- Secrets are secure encrypted passwords. You can set them for privilege levels 1 to 15.

Passwords must be stored in encryption mode. Passwords use simple encryption, and secrets use secure encryption.

Caution

- If a privilege level is configured with both a password and a secret, the password does not take effect.
- If no password is configured for a privileged user level, you do not need to input a password to enter this level. For security purposes, it is recommended that a password be configured for privileged user levels.

2. Restrictions and Guidelines

- When a password or secret is configured for the first time and the plaintext string is less than eight characters or contains only one type of characters, the system prompts you that it is a weak password.
- After logging in to a device, a user can run the **enable** command to raise his/her privilege level to access commands at different privilege levels. An increase in privilege level requires the input of the correct password of the target privilege level by default.
- You can specify the **level** keyword in the password configuration command to configure a password for a specific privilege level. After you set a password for a specific privilege level, the password works for the users who need to access commands of this level.
- The **enable** commands include **enable** (for role switching), **enable password**, and **enable secret**. If no role is specified, these three commands are used to set the role configured by running the **enable** command.
- **enable password**
  - This command is used to configure passwords only for level 15 and takes effect only when no secret is configured. If you use this command to configure a password for a non-15 level, the system displays a warning and the password is automatically converted into a secret.
  - If the password and secret set for level 15 are the same, the system displays a warning.
  - If you specify an encryption type but enter a plaintext password during password configuration, you cannot enter the privileged EXEC mode again.
- To enable logging for level increase or role switching, run the **login privilege log** command.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) (Optional) Display help information.

help

(3) Raise the privilege level.

enable { [*privilege-level*] | [**role** *role-name*] }

When the role-based access control (RBAC) function is enabled, this command can be used to switch the terminal role. If no role is specified, the system switches to role **network-admin** by default.

(4) Enter the global configuration mode.

configure terminal

(5) Configure a password.

enable password { [**level** *password-level*] | [**role** *role-name*] } { *password* | [**0** | **7**] *encrypted-password* }

Preamble spaces are allowed in front of the password but the spaces are ignored. Intermediate and trailing spaces are recognized.

(6) Configure a secret.

enable secret { [**level** *secret-level*] | [**role** *role-name*] } { [**0**] *password* | **5** *encrypted-secret* }

When the RBAC function is enabled and no role is specified, this command is used to set a password for role **network-admin** by default.

(7) ((Optional) Configure the role for running the **enable** commands.

enable default role *role-name*

The default role for running **enable** commands is **network-admin**.

Only when the RBAC function is enabled, this command is available.

(8) Enable level increase logging.

login privilege log

The level increase or role switching logging function is disabled by default.

(9) Configure command privilege levels.

privilege *mode* { **all** | **level** *level* | **reset** } *command-string*

(10) (Optional) Enter the line configuration mode.

line [**console** | **vty**] *first-line* [*last-line*]

(11) Configure a password for line-based login.

password { [**0**] *password* | **7** *encrypted-password* }

(12) Verify the password for line-based login.

login

The verification function of simple login passwords is disabled for the console line and enabled for the virtual terminal lines by default.

1.5 Configuring Login and Authentication

1.5.1 Configuration Tasks

Login and authentication configuration includes the following tasks:

- Configuring Local User Authentication and Line-based Login Authentication
- Configuring Telnet Login

1.5.2 Configuring Local User Authentication and Line-based Login Authentication

1. Overview

When AAA is disabled, you can configure a line password or local user authentication to control users to log in to and manage the device. When login authentication (via the **login** command) is configured for a line, only users who pass the line password verification are allowed to log in. When local user authentication (via the **login local** command) is configured for a line, the username and password entered by a user are checked against those stored in the local user database. If they are matched, the user can access the device with proper management permissions.

When AAA is enabled, some servers can be used to authenticate users' management permissions by their usernames and passwords at their login. Only authenticated users are allowed to log in. For example, a RADIUS server can authenticate usernames and passwords and control users' permissions to manage the device. Thus, instead of using locally stored password information for authentication, the device sends encrypted user information to the RADIUS server for verification. The server configures unified usernames, passwords, shared passwords, and access policies of users to manage and control user access and improve the security of user information.

Caution

After AAA is enabled, line password verification and local user authentication do not take effect.

2. Restrictions and Guidelines

- In the enabled AAA authentication mode, set line-based login for this authentication, and use the AAA authentication methods, including RADIUS authentication, local authentication, and no authentication.
- In the enabled AAA security service, to perform non-AAA authentication for a line run the **login access non-aaa** command. The configuration is valid for all terminals.
- The **username** command is used to create a local user database for authentication. The encryption type **7** needs to be specified only when encrypted passwords are copied and pasted. If the value **7** is specified as the encryption type, the entered ciphertext string must consist of an even number of characters. The login user cannot delete his/her account.
- To lock a session, enable locking on the terminal connected to a line in line configuration mode, and run the **lock** command in the EXEC mode of the terminal to lock the terminal. When a user enters any character on the locked terminal, the password prompt is displayed. The terminal will be automatically unlocked if the entered password is correct.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a local user account and optional authorization information.

username *username* [**login mode** { **console** | **ssh** | **telnet** | **ftp** }] [**online amount** *amount-number*] [**permission** *oper-mode path*] { [**privilege** *privilege-level*] | [**role** *text-string*] } [**reject remote-login**] [**web-auth**] [**pwd-modify**] [**nopassword** | **password** [**0** | **7**] *text-string* | **secret** [**0** | **5** | **8**] *text-string*]

No local user account or authorization information is configured by default.

(4) (Optional) Import user information from a file.

username import *filename*

(5) (Optional) Export user information to a file.

username export *filename*

(6) (Optional) Enter the line configuration mode.

line [**console** | **vty**] *first-line* [*last-line*]

(7) Configure the connection timeout time.

exec-timeout *exec-timeout-minutes* [*exec-timeout-seconds*]

The default connection timeout time is 10 minutes.

If there is no input information during the specified time, the server interrupts the established connection.

(8) Configure the session timeout time.

session-timeout *session-timeout-time* [**output**]

The default session timeout time is 0 minute for remote terminals. That is, the sessions never time out. If there is no input information during the specified time, the device closes sessions established to a remote terminal on the current line and restores the terminal to the idle state.

(9) Configure local authentication for line-based login.

login local

When AAA is disabled, no local user authentication is configured for lines by default.

(10) (Optional) Configure non-AAA authentication for line-based login when AAA is enabled.

login access non-aaa

When AAA is enabled, non-AAA authentication is disabled by default.

(11) (Optional) Enable locking on a terminal connected to a line.

lockable

The function of locking terminals connected to the current line is disabled by default.

(12) Return to the privileged EXEC mode.

end

(13) Lock the terminal connected to the current line.

lock

1.5.3 Configuring Telnet Login

1. Overview

As an application-layer protocol in the TCP/IP protocol suite, telnet provides the standard for remote login and virtual terminal communication on the Internet. The telnet client service allows a local or remote login user of the device to access other remote system resources on the Internet.

2. Restrictions and Guidelines

If you have run the **telnet** command to initiate a telnet client session, you can press **Ctrl+Shift+6+X** (press **Ctrl+Shift+6**, release the buttons, and then press **X**) to temporarily exit the session. To restore this session, run the **<1–99>** command. To display information about established sessions, run the **show sessions** command.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Run the **telnet** command to log in to the telnet server.

telnet [**oob**] { *hostname* | *ipv4-address* | *ipv6-address* } [*port-number*] [**/source** { **ip** *ipv4-address* | **ipv6** *ipv6-address* | **interface** *interface-type interface-name* }] [**via** *mgmt-name*]

(3) Run the **do telnet** command to log in to the telnet server.

do telnet [**oob**] { *hostname* | *ipv4-address* | *ipv6-address* } [*port-number*] [**/source** { **ip** *ipv4-address* | **ipv6** *ipv6-address* | **interface** *interface-type interface-name* }] [**via** *mgmt-name*]

(4) (Optional) Restore the established telnet client session.

1–99

(5) (Optional) Disconnect a suspended telnet client session.

disconnect *session-id*

(6) Enter the global configuration mode.

configure terminal

(7) Enable the telnet server service.

enable service telnet-server

1.6 Configuring Basic System Parameters

1.6.1 Configuration Tasks

Basic system parameter configuration includes the following tasks:

- Configuring the System Clock
- Configuring a System Name and Command Prompt
- Configuring System Notifications

1.6.2 Configuring the System Clock

1. Overview

The system clock includes the date (year, month, and day), time (hour, minute, and second), and week information. This function is used to record event occurrence time, such as the system logging. When you use a device for the first time, set its system time to the current date and time manually.

2. Restrictions and Guidelines

- The device clock starts from the configured time and keeps running even when the device is powered off.
- If a device has no hardware clock, the manually configured time becomes invalid when the device is powered off.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Configure the system date and clock.

clock set *hh:mm*:*ss* [*MM* [*DD* [*YY*]]]

(3) (Optional) Update the hardware clock.

clock update-calendar

(4) (Optional) Synchronize the software clock with the hardware time.

clock read-calendar

(5) (Optional) Configure the summer time.

clock summer-time *summer-time-zone* **start** *start-month* [*week* | **last**] *start-date hh:mm* **end** *end-month* [*week* | **last**] *end-date hh:mm* [**ahead** *hours-offset* [*minutes-offset*]]

(6) (Optional) Configure the time zone.

clock timezone *timezone hours-offset* [*minutes-offset*]

1.6.3 Configuring a System Name and Command Prompt

1. Overview

To facilitate management, you can configure a system name for each device to identify the device. The default system name is **orion_B26Q**, and acts as the default command prompt. The command prompt changes with the system name. A system name longer than 32 characters is truncated to keep only the first 32 characters.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a system name.

hostname *hostname*

The default host name is **orion_B26Q**.

(4) Configure a command prompt.

prompt *prompt-string*

No CLI prompt is configured by default, and the system name is used as the command prompt.

1.6.4 Configuring System Notifications

1. Overview

System notifications are prompts displayed after user login and are classified into the following two types:

- Message of the day (MOTD): Sends urgent messages to users. MOTD information is displayed on the terminal after a user logs in to the device.
- Login banner: Provides some common login prompts and appears after MOTD information.

2. Restrictions and Guidelines

After entering a delimiter and pressing **Enter**, you can enter text, and then enter a delimiter and press **Enter** again to stop entering the text. Any characters following the ending delimiter are dropped. Text in the notification information must not contain the delimiter letter.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure MOTD information.

banner motd *c message c*

No MOTD information is configured by default.

(4) Configure login banner information.

banner login *c message c*

No login banner information is configured by default.

(5) Configure a prompt indicating the establishment of a reverse telnet connection.

banner incoming *c message c*

No prompt for the establishment of a reverse telnet connection is configured by default.

(6) Configure a prompt for the access to the privileged EXEC mode.

banner privilege-mode *c message c*

No prompt for the access to the privileged EXEC mode is configured by default.

(7) Configure a prompt for SLIP/PPP line connection.

banner slip-ppp *c message c*

No prompt for SLIP/PPP line connection is configured by default.

(8) Configure a prompt for user login authentication timeout.

banner prompt-timeout *c message c*

No prompt for user login authentication timeout is configured by default.

(9) (Optional) Enter the line configuration mode.

line [**console** | **vty**] *first-line* [*last-line*]

(10) Configure a welcome prompt indicating that a user has entered the user EXEC mode of a line.

banner exec *c message c*

No welcome prompt indicating that a user has entered the user EXEC mode of a line is configured by default.

(11) (Optional) Configure a prompt indicating that the function of displaying EXEC prompt information is activated again for a specific line.

banner exec-banner *c message c*

The function of displaying EXEC prompt information is activated for all lines by default.

1.7 Enabling or Disabling a Specific Service

1. Overview

When the system is running, you can dynamically adjust system services and enable or disable specific services (SSH server service, telnet server service, SNMP agent service, and Web server service).

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable a specific service.

enable service { **ssh-server** | **telnet-server** | **snmp-agent** | **web-server** }

The Simple Network Management Protocol (SNMP) agent service is enabled and the telnet server, Secure Shell (SSH) server, and Web server services are disabled by default.

(4) (Optional) Save system configurations (**running-config**) to a specific position.

write [**auto-save interval** *interval-time* | **memory** [**auto-save interval** *interval-time*] | **terminal**]

1.8 Rolling Back System Configurations

1. Overview

Rollback configuration allows you to make a snapshot for the current configurations, that is, a copy or checkpoint of the current configurations, and apply the checkpoint configurations to the device without restarting the device. This function applies to the following scenarios:

- When current system configurations contain too many errors to locate or roll back one by one, you must roll back the current configurations to a previous correct state.
- When the device application environment changes and the device needs to run the configurations in a

configuration file, you can roll back the current configurations to the specified configuration file state without restarting the device.

During rollback, the system compares and handles the differences between the current configurations and checkpoint configurations.

- For the same commands in both configurations, the system does not process them.
- For the commands only in the current configurations, the system cancels them.
- For the commands only in the checkpoint configurations, the system runs them.
- For the different commands between both the current configurations and checkpoint configurations, the system cancels them, and then runs related commands in the checkpoint configurations.

2. Restrictions and Guidelines

- The checkpoint quantity is controlled using the internal function macro. For devices with a small flash memory, four checkpoints are supported. The default checkpoint quantity is **10**.
- Only one user can create checkpoints and configure rollback on a device at a time.
- It is recommended that you check the consistency of serial port baud rates between the current system configurations and checkpoint configurations before you perform rollback. If they are inconsistent, you are advised to change the serial port baud rate to that of the checkpoint configurations. Otherwise, a rate change will occur during rollback, causing a failure to display the rollback process information.
- During configuration rollback, do not hot-swap any supervisor module, line card, or service board and ensure that the device topology environment is the same as the environment of checkpoint creation. For example, if the device topology is a standalone environment during checkpoint creation but a virtual switching unit (VSU) environment during rollback, configuration rollback may fail.
- If an “Increased configuration:” message is displayed after rollback, configurations increase from the checkpoint configurations. This is because some commands cannot be reversed or fail to be reversed. For details, see the command manuals of specific functions, and manually reserve these commands.
- If a "Decreased configuration:" message is displayed after rollback, configurations decrease from the checkpoint configurations. This is because some commands fail to be executed during rollback. For details, see the command manuals of specific functions, and manually run these commands.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Create a checkpoint.

checkpoint [*checkpoint -name*] [**description** *description*]

No checkpoint is configured by default.

(3) Roll back configurations.

rollback running-config checkpoint *checkpoint -name* [**display-differences** | **ignore-results**]

(4) Clear the checkpoint data.

clear checkpoint database

1.9 Configuring Multiple-configuration Booting

1. Overview

Multiple-configuration booting allows users to modify the saving paths and names of startup configuration files of the device. This function saves configurations to an extended flash memory or an extended Universal Serial Bus (USB) flash drive of the device only. To save configurations to an extended USB flash drive, the device must support at least one USB port. If the device supports two or more USB ports, this function saves startup configurations to USB 0 only.

The startup configuration file of the device is saved in the flash memory and named **config.text** by default.

2. Restrictions and Guidelines

- The startup configuration file name can be an existing path. If the path does not exist, the **write** command fails to save the configurations. For example, if the startup configuration file name is set to **flash:/Hostname/Hostname.text** or **usb0:/Hostname/Hostname.text**, **flash:/Hostname** and **usb0:/Hostname** must exist. In master-slave mode, the paths must exist on all devices.
- To save the startup configuration file to a USB flash drive, the device must provide a USB port with a USB flash drive inserted. Otherwise, the **write** command will fail to save the configurations. In master-slave mode, all devices must have a USB flash drive inserted.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Modify the saving path and name of startup configuration file.

boot config { **flash:***filename* | **usb0:***filename* }

1.10 Configuring a Restart Policy

1.10.1 Configuration Tasks

The restart policy configuration includes the following tasks:

- Configuring Immediate Restart
- Configuring Scheduled Restart

1.10.2 Configuring Immediate Restart

1. Overview

Immediate restart applies when the device needs to be restarted immediately.

2. Restrictions and Guidelines

- A restart may interrupt services. Exercise caution.

- If the device to be restarted is being upgraded, it does not perform the restart.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Configure immediate device restart.

reload

1.10.3 Configuring Scheduled Restart

1. Overview

A restart policy enables the device to restart as scheduled. The following two scheduled restart functions are supported:

- Configure the system to restart after an interval. The interval is in the format of *mmm* or *hhh:mm*, in minutes. You can select either of the formats. You can specify an interval name to reflect the restart purpose.
- Configure the system to restart at a future time point.

2. Restrictions and Guidelines

- A restart may interrupt services. Exercise caution.
- If the device to be restarted is being upgraded, the system does not perform the restart.
- The restart time must be later than the current system time but cannot be more than 31 days later than the current system time. After you configure a restart schedule, do not change the system clock (for example, change the system time to a time after the restart time). Otherwise, the configuration may fail.
- To restart the system at a future time point, the system must support the clock function and the input time value must be a future time point. The **MM DD YY** parameter is optional. If it is not specified, the system clock time is used by default. A new restart schedule overwrites the existing one. If the system is restarted before a restart schedule takes effect, the schedule will be lost.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Configure scheduled device restart.

- Configure a scheduled restart schedule.

  reload at *hh*:*mm*:*ss* [*MM* [*DD* [*YY*]]]

- Configure a countdown restart schedule.

  reload in { [*hh* :] *mm*] }

  No restart function is configured by default.

(3) (Optional) Cancel the restart schedule.

reload cancel

1.11 Running Batch File Commands

1. Overview

To management system functions, it may take a long time to enter many commands on the CLI. This process is prone to errors and omissions. You can put the commands in a batch file according to configuration steps, and execute the file to complete related configurations.

2. Restrictions and Guidelines

- You can specify the name and content of the batch file on your PC and transfer the file to the flash memory of the device through TFTP. The content of the batch file simulates user input. Therefore, you must edit the content according to the configuration sequence of the CLI commands. For some interactive commands, you must write the responses in the batch file to ensure that the commands are normally run.
- The batch file must not exceed 128 KB in size; otherwise, it will fail to be executed. You can divide a large batch file into multiple files smaller than 128 KB in size each.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Run the **execute** command to execute the batch file.

execute { [**flash:**] *filename* }

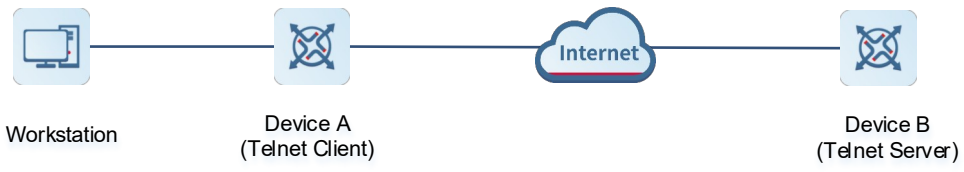
1.12 Configuring the Telnet Service

1. Overview

As an application-layer protocol in the TCP/IP protocol suite, telnet provides the standard for remote login and virtual terminal communication on the Internet.

The telnet client service allows a local or remote login user of the device to access other remote system resources on the Internet. As shown in the following figure, a user uses a PC to connect to device A by using the terminal emulation program or telnet program and then logs in to device B by running the **telnet** command to configure and manage device B.

Figure 1-1Telnet Service



The telnet program can use an IPv4

or IPv6

address for communication. The telnet server can accept

telnet connection requests from

IPv4 and IPv6 addresses. The telnet client can send connection requests

to hosts identified

by IPv4 and IPv6 addresses.

When the telnet server service is enabled on the device, you can use the telnet client to connect to the device and configure the following functions:

- Configure an access control list (ACL) for the telnet server.
- Disable the IP address blocking function of the telnet server.
- Configure the number of authentication failures, beyond which an IP address is blocked, and the time period for counting consecutive authentication failures on the telnet server.
- Configure the -period for awakening blocked IP addresses on the telnet server.
- Clear entries about blocking and authentication failures of all or specific IP addresses.

2. Restrictions and Guidelines

- When the number of authentication failures of telnet login meets the IP address blocking conditions in the authentication failure count period, the source IP address blocking is triggered. That is, the telnet client of this source IP address is not allowed to log in to the device to prevent the device from being attacked. The telnet client can log in to the device only after the IP address awakening period expires.
- In the enabled IP address blocking function, a user logs in to the device through telnet . When the number of consecutive authentication failures reaches the configured count within the authentication failure count period, source IP address blocking is triggered. When such number does not reach the configured count or one authentication operation is successful within the authentication failure count period, the authentication failures are cleared.
- After the time for awaking a blocked source IP address comes, entries about the IP address blocking are cleared. The blocked IP address is awakened immediately and can log in to the device through the telnet client.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an ACL for the telnet server.

ip telnet access-class { *acl-number* | *acl-name* }

(4) Disable the IP address blocking function of the telnet server.

ip telnet ip-block disable

The IP address blocking function of the telnet server is enabled by default.

(5) Configure the number of authentication failures, beyond which an IP address is blocked, and the -period for counting consecutive authentication failures on the telnet server.

ip telnet ip-block failed-times *failed-times* **period** *failed-period-time*

The allowed maximum number of authentication failures is 6, and the -period for counting consecutive authentication failures is 5 minutes by default.

(6) Configure the -period for awakening blocked IP addresses on the telnet server.

ip telnet ip-block reactive *reactive-period-time*

The default -period for awakening blocked IP addresses is 5 minutes.

(7) Configure the -period for awakening blocked IP addresses on the telnet server.

clear telnet ip-block { **all** | [*ipv4-address* | *ipv6-address*] }

1.13 Configuring Automatic Configuration File Backup to a Remote Server

1. Overview

By configuring the specific information and interval, you can automatically back up the configuration file of the device to the remote server.

2. Restrictions and Guidelines

- If no configuration file exists during command execution, an error is displayed.
- If the configuration file is deleted after the configuration command takes effect, the system stops backing up the configuration file to the remote server after the preset time expires.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure automatic backup of the configuration file backup to a remote server.

auto-backup configuration [**oob**] { **ftp** *server* [**port** *port-number*] **username** *username* **password** { [0] *password* | 7 *encrypted-password* } | **tftp** *server* } **interval** *interval-time* [**path** *folder*]] [**via** *mgmt_name*] [**vrf** *vrf_name*]

1.14 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Table 1-1Monitoring

Command	Purpose
show boot config	Displays the saving path and name of startup configuration file.
show checkpoint { checkpoint-name [**all**] | **summary** }	Displays all information about a checkpoint or a summary of all checkpoints.
show clock	Displays the current system time.

Command	Purpose
show line { **console** *line-number* **| vty** *line-number* **|** *line-number* }	Displays the line configurations.
show reload	Displays system restart settings.
show running-config [**interface** *interface*]	Displays the running configurations of the device system or configurations of an interface.
show startup-config	Displays the device configurations stored in the NVRAM.
show telnet ip-block { **all** | **list** }	Displays information about blocked IP addresses and authentication failures.
show this	Displays effective system configurations in current mode.
show version	Displays system information.
show service	Displays the service status (enabled/disabled).
show hostname	Displays the host name of the device.
show debugging	Displays information about enabled debugging functions.
show sessions	Displays information about established telnet client instances.
show language character-set	Displays the current character set encoding format of the device.
show calendar	Displays the hardware time.
show cpu	Displays the CPU information.
show memory [**history** | **low-watermark** | *process-id* | *process-name* | **slot** | **sorted total**]	Displays the memory information.
show memory vsd	Displays the memory information.
show pci-bus	Displays the PCI-mounted device information.
show processes cpu [**history** [**table**] | [**5sec** | **1min** | **5min** | **15min**] [**nonzero**]]	Displays the system task information.
show processes cpu detailed { *process-id* | *process*-name }	Displays the specified task information.
show usb-bus	Displays the USB-mounted device information.

1.15 Configuration Examples

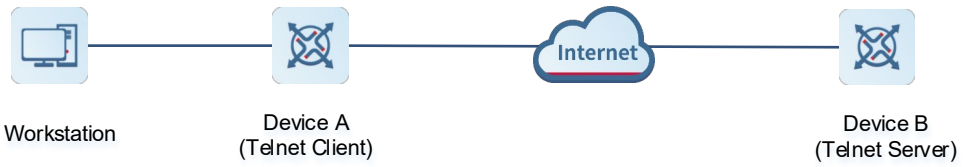
1.15.1 Configuring Login Authentication and Telnet Service

1. Requirements

- Establish a telnet session to a remote device.
- Complete login identity authentication.

2. Topology

Figure 1-1Configuring the Telnet Service



3. Notes

- Establish a telnet session to the remote device whose IP address is 192.168.65.119.
- Establish a telnet session to the remote device whose IPv6 address is 2AAA:BBBB::CCCC.

4. Procedure

(1) Configure user and authorization information.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line vty 0
Hostname(config-line)# password Guestuser
Hostname(config-line)# login
```

(2) Establish a telnet session to a remote device.

Run the **telnet** command in privileged EXEC mode, or run the **do telnet** command in privileged EXEC mode, user EXEC mode, or interface configuration mode.

```
Hostname# telnet 192.168.65.119
Trying 192.168.65.119 ... Open
User Access Verification
Password: Guestuser
Hostname# telnet 2AAA:BBBB::CCCC
Trying 2AAA:BBBB::CCCC ... Open
User Access Verification
Password:
Hostname(config)# do telnet 2AAA:BBBB::CCCC
Trying 2AAA:BBBB::CCCC ... Open
User Access Verification
Password: Guestuser
```

5. Verification

- Run the **ping** command to display the configurations. If the remote device can be pinged, the telnet service is configured.
- Verify the login identity. If the login is successful, login authentication is configured.

1.15.2 Configuring Basic System Parameters

1. Notes

- Configure the system time.
- Configure MOTD information.
- Configure login banner information.
- Set the serial port baud rate to 57,600 bps.

2. Procedure

(1) Configure the system time.

Set the system time to June 20, 2003, 10:10:12.

```
Hostname> enable
Hostname# clock set 10:10:12 6 20 2003
```

(2) Configure MOTD information.

Set the MOTD content to "Notice: system will shutdown on July 6th." with the pound key (#) as the delimiter.

```
Hostname# configure terminal
Hostname(config)# banner motd #
Enter TEXT message.  End with the character '#'.
Notice: system will shutdown on July 6th.#
Hostname(config)#
```

(3) Configure login banner information.

Set the login banner content to "Access for authorized users only. Please enter your password." with the pound key (#) as the delimiter.

```
Hostname(config)# banner login #
Enter TEXT message.  End with the character '#'.
Access for authorized users only. Please enter your password.
#
```

(4) Set the serial port baud rate to 57,600 bps.

```
Hostname# configure terminal
Hostname(config)# line console 0
Hostname(config-line)# speed 57600
Hostname(config-line)# end
```

3. Verification

- Verify the system time.

Run the **show clock** command in privileged EXEC mode to display the system time.

```
Hostname# show clock
clock: 2003-6-20 10:10:54
```

- Verify MOTD information.

  Connect to the local device through the console, telnet, or SSH, and check whether the MOTD information is displayed before the CLI appears.

```
Hostname# telnet 192.168.65.236
Notice:  system will shutdown on July 6th.
Access for authorized users only. Please enter your password.
 User Access Verification
Password:
```

- Verify login banner information.

  Connect to the local device through the console, telnet, or SSH, and check whether the login banner information is displayed before the CLI appears.

```
Hostname# telnet 192.168.65.236
Notice:  system will shutdown on July 6th.
Access for authorized users only. Please enter your password.
 User Access Verification
Password:
```

- Verify that the serial port baud rate is set to 57,600 bps.

  Run the **show line** command to display the configurations.

```
Hostname# show line console 0
CON     Type    speed   Overruns
* 0     CON     57600   0
Line 0, Location: "", Type: "vt100"
Length: 25 lines, Width: 80 columns
Special Chars: Escape  Disconnect  Activation
               ^^x     none        ^M
Timeouts:      Idle EXEC    Idle Session
               never        never
History is enabled, history size is 10.
Total input: 22 bytes
Total output:  115 bytes
Data overflow:  0 bytes
stop rx interrupt:  0 times
Modem: READY
```