

System Configuration

1. Configuring Command Line Interface
1. Configuring Basic Management
2. Configuring Lines
3. Configuring Time Range
4. Configuring HTTP
5. Configuring Syslog
6. Configuring ZAM
7. Configuring MONITOR

1 Configuring CLI

1.1 Overview

The command line interface (CLI) is a window used for text command interaction between users and network devices. You can enter commands in the CLI window to configure and manage network devices.

Protocols and Standards

N/A

1.2 Applications

Application	Description
Configuring and Managing Network Devices Through CLI	You can enter commands in the CLI window to configure and manage network devices

1.2.1 Configuring and Managing Network Devices Through CLI

Scenario

As shown in Figure 1-1, a user accesses network device A using a PC, and enter commands in the CLI window to configure and manage the network device.

Figure 1-1



Remarks	A is the network device to be managed. PC is a terminal.
----------------	---

1.3 Features

Overview

Feature	Description
---------	-------------

Accessing CLI	You can log in to a network device for configuration and management.
Command Modes	The CLI provides several command modes. Commands that can be used vary according to command modes.
System Help	You can obtain the help information of the system during CLI configuration.
Abbreviated Commands	If the entered string is sufficient to identify a unique command, you do not need to enter the full string of the command.
No and Default Options of Commands	You can use the no option of a command to disable a function or perform the operation opposite to the command, or use the default option of the command to restore default settings.
Prompts Indicating Incorrect Commands	An error prompt will be displayed if an incorrect command is entered.
History Commands	You can use short-cut keys to display or call history commands.
Featured Editing	The system provides short-cut keys for editing commands.
Searching and Filtering of the Show Command Output	You can run the show command to search or filter specified commands.
Command Alias	You can configure alias of a command to replace the command.

1.3.1 Accessing CLI

Before using the CLI, you need to connect a terminal or PC to a network device. You can use the CLI after starting the network device and finishing hardware and software initialization. When used for the first time, the network device can be connected only through the console port, which is called out band management. After performing relevant configuration, you can connect and manage the network device through Telnet.

1.3.2 Command Modes

Due to the large number of commands, these commands are classified by function to facilitate the use of commands. The CLI provides several commands modes, and all commands are registered in one or several command modes. You must first enter the command mode of a command before using this command. Different command modes are related with each other while distinguished from each other.

As soon as a new session is set up with the network device management interface, you enter User EXEC mode. In this mode, you can use only a small number of commands and the command functions are limited, such as the **show** commands. Execution results of commands in User EXEC mode are not saved.

To use more commands, you must first enter Privileged EXEC mode. Generally, you must enter a password to enter Privileged EXEC mode. In Privileged EXEC mode, you can use all commands registered in this command mode, and further enter global configuration mode.

Using commands of a certain configuration mode (such as global configuration mode and interface configuration mode) will affect configuration in use. If you save the configuration, these commands will be saved and executed next time the system is restarted. You must enter global configuration mode before entering another configuration mode, such as interface configuration mode.

The following table summarizes the command modes by assuming that the name of the network device is "Orion Alpha A28X".

Command Mode	Access Method	Prompt	Exit or Entering Another Mode	About
User EXEC (User EXEC mode)	Enter User EXEC mode by default when accessing a network device.	Orion Alpha A28X>	Run the exit command to exit User EXEC mode. Run the enable command to enter Privileged EXEC mode.	Use this command mode to conduct basic tests or display system information.
Privileged EXEC (Privileged EXEC mode)	In User EXEC mode, run the enable command to enter Privileged EXEC mode.	Orion Alpha A28X#	Run the disable command to return to User EXEC mode. Run the configure command to enter global configuration mode.	Use this command mode to check whether the configuration takes effect. This mode is password protected.
Global configuration (Global configuration mode)	In Privileged EXEC mode, run the configure command to enter global configuration mode.	Orion Alpha A28X(config)#	Run the exit or end command, or press Ctrl+C to return to Privileged EXEC mode. Run the interface command to enter interface configuration mode. When using the interface command, you must specify the interface. Run the vlan <i>vlan_id</i> command to enter VLAN configuration mode.	Using commands in this mode will affect the global parameters of the network device.
Interface configuration (Interface configuration mode)	In global configuration mode, run the interface command to enter interface configuration mode.	Orion Alpha A28X(config-if)#	Run the end command, or press Ctrl+C to return to Privileged EXEC mode. Run the exit command to return to global configuration mode. When using the interface command, you must specify the interface.	Use this configuration mode to configure various interfaces of the network device.
Config-vlan (VLAN configuration mode)	In global configuration mode, run the vlan <i>vlan_id</i> command to enter VLAN configuration mode.	Orion Alpha A28X(config-vlan)#	Run the end command, or press Ctrl+C to return to the Privileged EXEC mode. Run the exit command to return to global configuration mode.	Use this configuration mode to configure VLAN parameters.

1.3.3 System Help

When entering commands in the CLI window, you can obtain the help information using the following methods:

1. At the command prompt in any mode, enter a question mark (?) to list the commands supported by the current command mode and related command description.

For example

```
Orion Alpha A28X>?
```

```
Exec commands:
```


```
<1-99>      Session number to resume
disable     Turn off privileged commands
disconnect  Disconnect an existing network connection
enable      Turn on privileged commands
exit        Exit from the EXEC
help        Description of the interactive help system
lock        Lock the terminal
ping        Send echo messages
show        Show running system information
telnet      Open a telnet connection
traceroute  Trace route to destination
```

2. Enter a space and a question mark (?) after a keyword of a command to list the next keyword or variable associated with the keyword.

For example

```
Orion Alpha A28X(config)#interface ?
```

```
Aggregateport  Aggregate port interface
Dialer          Dialer interface
GigabitEthernet Gigabit Ethernet interface
Loopback        Loopback interface
Multilink       Multilink-group interface
Null            Null interface
Tunnel          Tunnel interface
Virtual-ppp     Virtual PPP interface
Virtual-template Virtual Template interface
Vlan            Vlan interface
range           Interface range command
```

-  If the keyword is followed by a parameter value, the value range and description of this parameter are displayed as follows:

```
Orion Alpha A28X(config)#interface vlan ?
<1-4094> Vlan port number
```

3. Enter a question mark (?) after an incomplete string of a command keyword to list all command keywords starting with the string.

For example

```
Orion Alpha A28X#d?
debug delete diagnostic dir disable disconnect
```

4. After an incomplete command keyword is entered, if the suffix of this keyword is unique, press the **Tab** key to display the complete keyword.

For example

```
Orion Alpha A28X# show conf<Tab>
Orion Alpha A28X# show configuration
```

5. In any command mode, run the **help** command to obtain brief description about the help system.

For example

```
Orion Alpha A28X(config)#help
Help may be requested at any point in a command by entering
a question mark '?'. If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
```

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show ?') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (e.g. 'show pr?'.)

1.3.4 Abbreviated Commands

If a command is long, you can enter a part of the command that is sufficient to identify the command keyword.

For example, to run the **interface** *gigabitEthernet 0/1* command in GigabitEthernet 0/1 interface configuration mode, enter the abbreviated command as follows:

```
Orion Alpha A28X(config)#int g0/1
```

1.3.5 No and Default Options of Commands

Most commands have the **no** option. Generally, the **no** option is used to disable a feature or function, or perform the operation opposite to the command. For example, run the **no shutdown** command to perform the operation opposite to the **shutdown** command, that is, enabling the interface. The keyword without the **no** option is used to enable a disabled feature or a feature that is disabled by default.

Most configuration commands have the **default** option. The **default** option is used to restore default settings of the command. Default values of most commands are used to disable related functions. Therefore, the function of the **default** option is the same as that of the **no** option in most cases. For some commands, however, the default values are used to enable related functions. In this case, the function of the **default** option is opposite to that of the **no** option. At this time, the **default** option is used to enable the related function and set the variables to default values.

 For specific function of the **no** or **default** option of each command, see the command reference.

1.3.6 Prompts Indicating Incorrect Commands

When you enter an incorrect command, an error prompt is displayed.

The following table lists the common CLI error messages.

Error Message	Meaning	How to Obtain Help
% Ambiguous command: "show c"	The characters entered are insufficient for identifying a unique command.	Re-enter the command, and enter a question mark after the word that is ambiguous. All the possible keywords will be displayed.
% Incomplete command.	The mandatory keyword or variable is not entered in the command.	Re-enter the command, and enter a space and a question mark. All the possible keywords or variables will be displayed.
% Invalid input detected at '^' marker.	An incorrect command is entered. The sign (^) indicates the position of the word that causes the error.	At the current command mode prompt, enter a question mark. All the command keywords allowed in this command mode will be displayed.

1.3.7 History Commands

The system automatically saves commands that are entered recently. You can use short-cut keys to display or call history commands.

The methods are described in the following table.

Operation	Result
Ctrl+P or the UP key	Display the previous command in the history command list. Starting from the latest record, you can repeatedly perform this operation to query earlier records.
Ctrl+N or the DOWN key	After pressing Ctrl+N or the DOWN key, you can return to a command that is recently executed in the history command list. You can repeatedly perform this operation to query recently executed commands.

 The standard terminals, such as the VT100 series, support the direction keys.

1.3.8 Featured Editing

When editing the command line, you can use the keys or short-cut keys listed in the following table:

Function	Key or Short-Cut Key	Description
Move the cursor on the editing line.	Left key or Ctrl+B	Move the cursor to the previous character.
	Right key or Ctrl+B	Move the cursor to the next character.
	Ctrl+A	Move the cursor to the head of the command line.
	Ctrl+E	Move the cursor to the end of the command line.
Delete an entered character.	Backspace key	Delete one character to the left of the cursor.
	Delete key	Delete one character to the right of the cursor.
Move the output by one line or one page.	Return key	When displaying contents, press the Return key to move the output one line upward and display the next line. This operation is performed when the output does not end yet.
	Space key	When displaying contents, press the Space key to page down and display the next page. This operation is performed when the output does not end yet.

When the editing cursor is close to the right boundary, the entire command line will move to the left by 20 characters, and the hidden front part is replaced by the dollar (\$) signs. You can use the related keys or short-cut keys to move the cursor to the characters in the front or return to the head of the command line.

For example, the whole **access-list** may exceed the screen width. When the cursor is close to the end of the command line for the first time, the entire command line moves to the left by 20 characters, and the hidden front part is replaced by the dollar signs (\$). Each time the cursor is close to the right boundary, the entire command line moves to the left by 20 characters.

```
access-list 199 permit ip host 192.168.180.220 host
$ost 192.168.180.220 host 202.101.99.12
$.220 host 202.101.99.12 time-range tr
```

Press **Ctrl+A** to return to the head of the command line. At this time, the hidden tail part of the command line is replaced by the dollar signs (\$).

```
access-list 199 permit ip host 192.168.180.220 host 202.101.99.$
```

 The default screen width is 80 characters.

1.3.9 Searching and Filtering of the Show Command Output

To search specified contents from the output of the **show** command, run the following command:

Command	Description
show <i>any-command</i> begin <i>regular-expression</i>	Searches specified contents from the output of the show command. The first line containing the contents and all information that follows this line will be output.

 The **show** command can be executed in any mode.

 Searched contents are case sensitive.

To filter specified contents from the output of the **show** command, run the following commands:

Command	Description
show <i>any-command</i> exclude <i>regular-expression</i>	Filters the output of the show command. Except those containing the specified contents, all lines will be output.
show <i>any-command</i> include <i>regular-expression</i>	Filters the output of the show command. Only the lines containing the specified contents will be output.

To search or filter the output of the **show** command, you must enter a vertical line (|). After the vertical line, select the searching or filtering rules and contents (character or string). Searched and filtered contents are case sensitive.

```
Orion Alpha A28X#show running-config | include interface
interface GigabitEthernet 0/0
interface GigabitEthernet 0/1
interface GigabitEthernet 0/2
interface GigabitEthernet 0/3
interface GigabitEthernet 0/4
interface GigabitEthernet 0/5
interface GigabitEthernet 0/6
interface GigabitEthernet 0/7
interface Mgmt 0
```

1.3.10 Command Alias

You can configure any word as the alias of a command to simplify the command input.

Configuration Effect

1. Replace a command with a word.

For example, configure "mygateway" as the alias of the **ip route 0.0.0.0 0.0.0.0 192.1.1.1** command. To run this command, you only need to enter "mygateway".

6. Replace the front part of a command with a word, and enter the later part.

For example, configure "ia" as the alias of the **ip address** command. To run this command, you need to enter "ia" and then the specified IP address and subnet mask.

Configuration Steps

📌 Displaying Default Alias

In User EXEC or Privileged EXEC mode, default alias are available for some commands. You can run the **show aliases** command to display these default aliases.

```
Orion Alpha A28X(config)#show aliases
Exec mode alias:
```

h	help
p	ping
s	show
u	undebug
un	undebug

 These default aliases cannot be deleted.

↘ Configuring a Command Alias

Command	alias <i>mode command-alias original-command</i>
Parameter	<i>mode</i> : indicates the command mode of the command represented by the alias.
Description	<i>command-alias</i> : indicates the command alias. <i>original-command</i> : indicates the command represented by the alias.
Command Mode	Global configuration mode
Usage Guide	In global configuration mode, run the alias ? command to list all command modes that can be configured with aliases.

↘ Displaying Settings of Command Aliases

Run the **show aliases** command to display alias settings in the system.

Notes

- The command replaced by an alias must start from the first character of the command line.
- The command replaced by an alias must be complete.
- The entire alias must be entered when the alias is used; otherwise, the alias cannot be identified.

Configuration Example

↘ Defining an Alias to Replace the Entire Command

Configuration Steps	In global configuration mode, configure the alias "ir" to represent the default route configuration command ip route 0.0.0.0 0.0.0.0 192.168.1.1 .
	<pre>Orion Alpha A28X#configure terminal Orion Alpha A28X(config)#alias config ir ip route 0.0.0.0 0.0.0.0 192.168.1.1</pre>
Verification	<ul style="list-style-type: none"> ● Run the show alias command to check whether the alias is configured successfully. <pre>Orion Alpha A28X(config)#show alias Exec mode alias: h help p ping s show</pre>

	<pre> u undebug un undebug Global configuration mode alias: ir ip route 0.0.0.0 0.0.0.0 192.168.1.1 </pre>
	<ul style="list-style-type: none"> ● Use the configured alias to run the command, and run the show running-config command to check whether the alias is configured successfully.
	<pre> Orion Alpha A28X(config)#ir Orion Alpha A28X(config)#show running-config Building configuration... ! alias config ir ip route 0.0.0.0 0.0.0.0 192.168.1.1 //Configuring an alias ... ip route 0.0.0.0 0.0.0.0 192.168.1.1 //Configuration result after the alias "ir" is entered ! </pre>

📌 Defining an Alias to Replace the Front Part of a Command

Configuration Steps	In global configuration mode, configure the alias "ir" to represent the front part "ip route" of the default route configuration command.
	<pre> Orion Alpha A28X#configure terminal Orion Alpha A28X(config)#alias config ir ip route </pre>
Verification	<ul style="list-style-type: none"> ● Run the show alias command to check whether the alias is configured successfully. <pre> Orion Alpha A28X(config)#show alias Exec mode alias: h help p ping s show u undebug un undebug Global configuration mode alias: ir ip route </pre>
	<ul style="list-style-type: none"> ● Enter the alias "ir" and then the later part of the command "0.0.0.0 0.0.0.0 192.168.1.1". ● Run the show ap-config running command to check whether the configuration is successful.

```

Orion Alpha A28X(config)#ir 0.0.0.0 0.0.0.0 192.168.1.1

Orion Alpha A28X(config)#show running

Building configuration...

!

alias config ir ip route //Configuring an alias

!

ip route 0.0.0.0 0.0.0.0 192.168.1.1 //Configuration result after the alias "ir" and the later
part of the command are entered

!

```

System Help

7. The system provides help information for command alias. An asterisk (*) will be displayed in front of an alias. The format is as follows:

```
*command-alias=original-command
```

For example, in Privileged EXEC mode, the default command alias "s" represents the **show** keyword. If you enter "s?", the keywords starting by "s" and alias information are displayed.

```
Orion Alpha A28X#s?
```

```
*s=show show start-chat start-terminal-service
```

8. If the command represented by an alias contains more than one word, the command is displayed in a pair of quotation marks.

For example, in Privileged EXEC mode, configure the alias "sv" to replace the **show version** command. If you enter "s?", the keywords starting by "s" and alias information are displayed.

```
Orion Alpha A28X#s?
```

```
*s=show *sv=" show version" show start-chat
```

```
start-terminal-service
```

9. You can use the alias to obtain help information about the command represented by the alias.

For example, configure the alias "ia" to represent the **ip address** command in interface configuration mode. If you enter "ia?" in interface configuration mode, the help information on "ip address?" is displayed, and the alias is replaced by the command.

```
Orion Alpha A28X(config-if)#ia ?
```

```
A.B.C.D IP address
```

```
dhcp IP Address via DHCP
```

```
Orion Alpha A28X(config-if)#ip address
```



If you enter a space in front of a command, the command represented by this alias will not be displayed.

2 Basic Management

2.1 Overview

This document is a getting started guide to network device management. It describes how to manage, monitor, and maintain network devices.

2.2 Applications

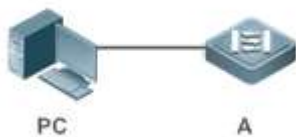
Application	Description
Network Device Management	A user logs in to a network device from a terminal and runs commands on a command line interface (CLI) to manage device configurations.

2.2.1 Network Device Management

Scenario

Network device management described in this document is performed through the CLI. A user logs in to Network Device A from a terminal and runs commands on the CLI to manage device configurations. See Figure 2-2.

Figure 2-2



2.3 Features

Basic Concepts

↘ TFTP

Trivial File Transfer Protocol (TFTP) is a TCP/IP protocol which allows a client to transfer a file to a server or get a file from a server.

↘ AAA

AAA is short for Authentication, Authorization and Accounting.

Authentication refers to the verification of user identities and the related network services.

Authorization refers to the granting of network services to users according to authentication results.

Accounting refers to the tracking of network service consumption by users. A billing system charges users based on consumption records.

AAA provides effective means of network management and security protection.

➤ RADIUS

Remote Authentication Dial In User Service (RADIUS) is the most widely used AAA protocol at present.

➤ Telnet

Telnet is a terminal emulation protocol in the TCP/IP protocol stack which provides access to a remote host through a virtual terminal connection. It is a standard protocol located at Layer 7 (application layer) of the Open System Interconnection (OSI) model and used on the internet for remote login. Telnet sets up a connection between the local PC and a remote host.

➤ System Information

System information includes the system description, power-on time, 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 slot and module information. 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), and actual and maximum number of physical ports.

Overview

Feature	Description
User Access Control	Controls the terminal access to network devices on the internet based on passwords and privileges.
Login Authentication Control	Performs username-password authentication to grant access to network devices when AAA is enabled. (Authentication is performed by a dedicated server.)
Basic System Parameters	Refer to the parameters of a system, such as the clock, banner, and Console baud rate.
Displaying Configurations	Displays the system configurations, including the configurations that the system is currently running and the device configurations stored in the nonvolatile random access memory (NVRAM).
Multiple-configuration Booting	Allows users to modify the path for saving startup configurations of the device and the corresponding file name.
Zero Configuration	Allows automatic service delivery and configuration maintenance for remote devices after device power-on, without requiring manual operation of network administrators.
Telnet	Telnet is an application-layer protocol in the TCP/IP protocol stack. It provides the standard governing remote login and virtual terminal communication on the internet.
Restart	Introduces system restart.
Running Batch File Commands	Runs commands in a file.

2.3.1 User Access Control

User access control refers to the control of terminal access to network devices on the internet based on passwords and privileges.

Working Principle

▾ Privilege Level

16 privilege levels are defined ranging from 0 to 15 for CLI on network devices to grant users access to different commands. Level 0 is the lowest level granting access to just a few commands, whereas level 15 is the highest level granting access to all commands. Levels 0 and 1 are common user levels without the device configuration permission (users are not allowed to enter global configuration mode by default). Levels 2–15 are privileged user levels with the device configuration permission.

▾ Password Classification

Passwords are classified into two types: password and security. The first type refers to simple encrypted passwords at level 15. The second type refers to secure encrypted passwords at levels 0–15. If a level is configured with both simple and secure encrypted passwords, the simple encrypted password will not take effect. If you configure a non-15 level simple encrypted password, a warning is displayed and the password is automatically converted into a secure encrypted password. If you configure the same simple encrypted password and secure encrypted password at level 15, a warning is displayed.

▾ Password Protection

Each privilege level on a network device has a password. An increase in privilege level requires the input of the target level password, whereas a reduction in privilege level does not require password input.

By default, only two privilege levels are password-protected, namely, level 1 (common user level) and level 15 (privileged user level). Sixteen privilege levels with password protection can be assigned to the commands in each mode to grant access to different commands.

If no password is configured for a privileged user level, access to this level does not require password input. It is recommended that a password be configured for security purposes.

▾ Command Authorization

Each command has its lowest execution level. A user with a privilege level lower than this level is not allowed to run the command. After the command is assigned a privilege level, users at this level and higher have access to the command.

Related Configuration

▾ Configuring a Simple Encrypted Password

- Run the **enable password** command.

▾ Configuring a Secure Encrypted Password

- Run the **enable secret** command.
- A secure encrypted password is used to control the switching between user levels. It has the same function as a simple encrypted password but uses an enhanced password encryption algorithm. Therefore, secure encrypted passwords are recommended out of security consideration.

↘ Configuring Command Privilege Levels

- Run the **privilege** command to assign a privilege level to a command.
- A command at a lower level is accessible by more users than a command at a higher level.

↘ Raising/Lowering a User Privilege Level

- Run the **enable** command or the **disable** command to raise or lower a user privilege level respectively.
- After logging in to a network device, the user can change his/her level to obtain access to commands at different privilege levels.
- To enable level increase logging, run the **login privilege log** command.

↘ Enabling Line Password Protection

- Line password protection is required for remote login (such as login through Telnet).
- Run the **password[0 | 7] line** command to configure a line password, and then run the **login** command to enable password protection.
- By default, terminals do not support the **lock** command.

2.3.2 Login Authentication Control

In login authentication with AAA disabled, the password entered by a user is checked against the configured line password. If they are consistent, the user can access the network device. In local authentication, 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 network device with proper management permissions.

In AAA, the username and password entered by a user are authenticated by a server. If authentication is successful, the user can access the network device and enjoy certain management permissions.

For example, a RADIUS server can be used to authenticate usernames and passwords and control users' management permissions on network devices. Network devices no longer store users' passwords, but send encrypted user information to the RADIUS server, including usernames, passwords, shared passwords, and access policies. This provides a convenient way to manage and control user access and improve user information security.

Working Principle

↘ Line Password

If AAA is disabled, you can configure a line password used to verify user identities during login. After AAA is enabled, line password verification does not take effect.

↘ Local Authentication

If AAA is disabled, you can configure local authentication to verify user identities and control management permissions by using the local user database. After AAA is enabled, local authentication does not take effect.

↘ AAA

AAA provides three independent security functions, namely, Authentication, Authorization and Accounting. A server (or the local user database) is used to perform authentication based on the configured login authentication method list and control users' management permissions. For details about AAA, see *Configuring AAA*.

Related Configuration

▾ [Configuring Local User Information](#)

- Run the **username** command to configure the account used for local identity authentication and authorization, including usernames, passwords, and optional authorization information.

▾ [Configuring Local Authentication for Line-Based Login](#)

- Run the **login local** command (in the case that AAA is disabled).
- Perform this configuration on every device.

▾ [Configuring AAA Authentication for Line-Based Login](#)

- The default authentication method is used after AAA is enabled.
- Run the **login authentication** command to configure a login authentication method list for a line.
- Perform this configuration when the local AAA authentication is required.

▾ [Configuring Non-AAA Authentication for Line-Based Login When AAA Is Enabled](#)

- Run the **login access non-aaa** command in global configuration mode.
- Perform this configuration on every device.

▾ [Configuring the Connection Timeout Time](#)

- The default connection timeout time is 10 minutes.
- Run the **exec-timeout** command to change the default connection timeout time. An established connection will be closed if no output is detected during the timeout time.
- Perform this configuration when you need to increase or reduce the connection timeout time.

▾ [Configuring the Session Timeout Time](#)

- The default session timeout time is 0 minutes, indicating no timeout.
- Run the **session-timeout** command to change the default session timeout time.
- The session established to a remote host through a line will be disconnected if no output is detected during the timeout time. Then the remote host is restored to Idle. Perform this configuration when you need to increase or reduce the session timeout time.

▾ [Locking a Session](#)

- By default, terminals do not support the **lock** command.
- Run the **lockable** command to lock the terminals connected to the current line.
- To lock a session, first enable terminal lock in line configuration mode, and then run the **lock** command in terminal EXEC mode to lock the terminal.

2.3.3 Basic System Parameters

System Time

The network device system clock records the time of events on the device. For example, the time shown in system logs is obtained from the system clock. Time is recorded in the format of *year-month-day, hour.minute:second, day of the week*.

When you use a network device for the first time, set its system clock to the current date and time manually.

Configuring a System Name and Command Prompt

You can configure a system name to identify a network device. The default system name is **Orion Alpha A28X**. A name with more than 32 characters will be truncated to keep only the first 32 characters. The command prompt keeps consistent with the system name.

Banner

A banner is used to display login prompt information. There are two types of banner: Daily notification and login banner.

- Daily notification is displayed on all terminals connected to network devices soon after login. Urgent messages (such as immediate system shutdown) can be delivered to users through daily notification.
- A login banner appears after daily notification to display login information.

Configuring the Console Baud Rate

You can manage network device through a Console port. The first configuration on the network device must be performed through the Console port. The serial port baud rate can be changed based on actual requirements. Note that the management terminal must have consistent baud rate setting with the device console.

Configuring the Connection Timeout Time

The connection timeout time is used to control device connections (including established connections and sessions established to remote hosts). A connection will be closed when no input is detected during the timeout time.

Related Configuration

Configuring the System Date and Clock

- Run the **clock set** command to configure the system time of a network device manually. The device clock starts from the configured time and keeps running even when the device is powered off.

Updating the Hardware Clock

- If the hardware clock and software clock are not synchronized, run the **clock update-calendar** command to copy the date and time of the software clock to the hardware clock.

Configuring a System Name

- Run the **hostname** command to change the default system name.
- The default host name is **Orion Alpha A28X**.

Configuring a Command Prompt

- Run the **prompt** command.

↘ **Configuring Daily Notification**

- By default, no daily notification is configured.
- Run the **banner motd** command to configure daily notification.
- Daily notification is displayed on all terminals connected to network devices soon after login. Urgent messages (such as immediate system shutdown) can be delivered to users through daily notification.

↘ **Configuring a Login Banner**

- By default, no login banner is configured.
- Run the **banner login** command to configure a login banner to display login information.

↘ **Configuring the Console Baud Rate**

- Run the **speed** command.
- The default baud rate is 9,600 bps.

2.3.4 Displaying Configurations

Displays the system configurations, including the configurations that the system is currently running and the device configurations stored in the NVRAM.

Working Principle

↘ **Running Configurations**

Running configurations, namely, running-config, are the configurations that individual component modules run in real time. A request can be made to all running components to collect configurations, which will be orchestrated before being displayed to users. Only running components may provide real-time configurations, whereas unloaded components do not display configurations. In the case that the system is started, a component process is restarted, and a hot patch is executed, the configurations collected during this period may be inaccurate due to the component unstable state. For example, the configurations of a component may not be missing initially but can be displayed later.

↘ **Startup Configurations**

The configurations stored in the NVRAM, namely, startup-config, are the configurations executed during device startup. When the system is restarted, startup-config is loaded to become new running-config. To display permanent configurations, the system needs to read the **startup-config** file in the NVRAM.

Related Configuration

↘ **Displaying Running Configurations**

Run the **show running-config [interface *interface*]** command to display the configurations that the system is currently running or the configurations on an interface.

↘ **Displaying Startup Configurations**

Run the **show startup-config** command.

📌 Storing Startup Configurations

Run the **write** or **copy running-config startup-config** command to store the current running configurations as new startup configurations.


2.3.5 Multiple-configuration Booting

Multiple-configuration booting allows users to modify the path for saving startup configurations of the device and the corresponding file name. At present, configurations can be saved to an extended flash memory.

Working Principle

- By default, the startup configuration file of a device is saved in **Flash:/config.text** and named **config.text**. Use this command to modify the path for saving startup configurations of the device and the corresponding file name.

 The startup configuration file name follows a slash "/", for example, **flash:/Orion Alpha A28X.text**.

 The startup configuration file name consists of a path and a file name. The path is mandatory. Otherwise, configurations cannot be saved by using the **write** command. Take **Flash:/Orion Alpha A28X/Orion Alpha A28X.text** as examples, where the **Flash:/Orion Alpha A28X** folder must exist. In master-slave mode, all device paths are required.

Related Configuration

📌 Modifying the Path for Saving Startup Configurations and the Corresponding File Name

Run the **boot config { flash:filename }** command to modify the path for saving startup configurations and the corresponding file name.

📌 Displaying the Path for Saving Startup Configurations and the Corresponding File Name


Run the **show boot config** command to display the path for saving startup configurations and the corresponding file name.


2.3.6 Zero Configuration


The zero configuration function allows automatic service delivery and configuration maintenance for remote devices after device power-on, without requiring manual operation of network administrators.

Working Principle

The zero configuration function involves the following process: A device with default configurations is powered on, obtains a device management address from the DHCP server of the ACS, and sends the SNMP INFORM message to the ACS; after receiving the SNMP INFORM message, the ACS delivers startup configurations of the device, and immediately validates the configurations.

 The zero configuration function is applicable to the ACS solution only.

 The zero configuration function is applicable to standalone systems only.

 With the zero configuration function, DHCP Snooping Trust is enabled only on the last two electrical ports and all SFP ports of the device by default, regardless of whether the device supports the MGMT port.



Enabling and disabling the zero configuration function will delete the startup configuration file of the device and trigger device restart.

Related Configuration

Enabling and Disabling the Zero Configuration Function

Run the **zcm** { **enable** | **disable** } command to enable or disable the zero configuration function.

2.3.7 Telnet

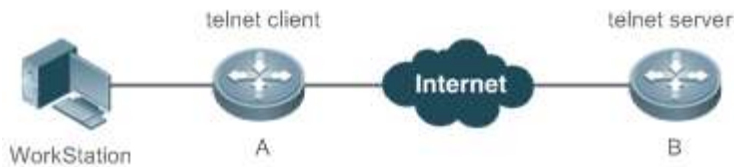
Working Principle

Telnet is an application-layer protocol in the TCP/IP protocol stack. It provides the standard governing remote login and virtual terminal communication on the internet.

The Telnet Client service allows a local or remote user who has logged in to a network device to use its Telnet Client program to access other remote system resources on the internet. In Figure 2-3, a user with a PC connects to Network Device A by using the terminal emulation or Telnet program and then logs in to Network Device B by using the **telnet** command to perform configuration management.

Orion Alpha A28X Telnet program supports the use of IPv4 and IPv6 addresses. A Telnet server accepts Telnet connection requests that carry IPv4 and IPv6 addresses. A Telnet client can send connection requests to hosts identified by IPv4 and IPv6 addresses.

Figure 2-3



Related Configuration

Enabling the Telnet Client Service

- Run the **telnet** command to log in to a remote device.

Enabling the DoTelnet Client Service

- Run the **do telnet** command to log in to a remote device.

Restoring a Telnet Client Session

- Run the **<1-99>** command.

Disconnecting a Suspended Telnet Client Session

- Run the **disconnect session-id** command.


Enabling the Telnet Server Service


- Run the **enable service telnet-server** command.
- Perform this configuration when you need to enable Telnet login.

2.3.8 Restart

The timed restart feature makes user operation easier in some scenarios (such as tests).

- If you configure a time interval, the system will restart after the interval. The interval is in the format of *mmm* or *hh:mm*, in the unit of minutes. You can specify the interval name to reflect the restart purpose.
- If you define a future time, the system will restart when the time is reached.

 The clock feature must be supported by the system if you want to use the **at** option. It is recommended that you configure the system clock in advance. A new restart plan will overwrite the existing one. A restart plan will be invalid if the system is restarted before the plan takes effect.

 The span between the restart time and current time must not exceed 31 days, and the restart time must be later than the current system time. After you configure a restart plan, do not to change the system clock; otherwise, the plan may fail (for example, the system time is changed to a time after the restart time.)


Related Configuration


↳ **Configuring Restart**

- Run the **reload** command to configure a restart policy.
- Perform this configuration when you need to restart a device at a specific time.

2.3.9 Running Batch File Commands

In system management, sometimes it takes a long time to enter many commands on the CLI to manage a function. This process is prone to errors and omissions. You can put the commands to a batch file according to configuration steps and execute the file to complete related configuration.

 You can specify the name and content of the batch file on your PC and transfer the file to the device flash memory through TFTP. The batch processing content simulates user input. Therefore, you need to edit the batch file content according to the CLI command configuration sequence. In addition, you need to write the responses to interactive commands to the batch file to ensure normal command execution.





 The batch file size must not exceed 128 KB; otherwise, it will fail to be executed. You can divide a large batch file into multiple parts not larger than 128 KB each.





Related Configuration

↳ **Batch-Running Commands**

- Run **execute** to run the commands in batches.
- This command provides a convenient way to run multiple commands at a time.

2.4 Configuration

Configuring Passwords and Privileges	 (Optional) It is used to configure passwords and command privilege levels.	
	enable password	Configures a simple encrypted password.
	enable secret	Configures a secure encrypted password.
	enable	Raises a user privilege level.
	login privilege log	Outputs log information of user privilege level increase.
	disable	Lowers a user privilege level.
	privilege	Configures command privilege levels.
	password	Specifies a line password.
	login	Enables line password protection.
Configuring Login and Authentication	 (Optional) It is used to configure different login modes and authentication methods.	
	username	Configures local user account information and optional authorization information.
	login local	Configures local authentication for line-based login.
	login access non-aaa	Configures non-AAA authentication for line-based login when AAA is enabled.
	login authentication	Configures AAA authentication for line-based login.
	telnet	Enables the Telnet Client service.
	do telenet	Enables the DoTelnet Client service.
	enable service telnet-server	Enables the Telnet Server service.
	exec-timeout	Configures the connection timeout time.
	session-timeout	Configures the session timeout time.
	lockable	Enables line-based terminal lock.
	lock	Locks a terminal connected to the current line.
Configuring Basic System Parameters	 (Optional) It is used to configure basic system parameters.	
	clock set	Configures the system date and clock.
	clock update-calendar	Updates the hardware clock.
	hostname	Configures a system name.
	prompt	Configures a command prompt.
	banner motd	Configures daily notification.
	bannerlogin	Configures a login banner.
	speed	Configures the Console baud rate.
Enabling and Disabling a	 (Optional) It is used to enable and disable a specific service.	

Specific Service	enable service	Enables a service.
	 (Optional) It is used to modify the startup configuration file.	
Configuring Multiple-configuration Booting	boot config { flash: <i>filename</i> }	Modifies the path for saving startup configurations and the corresponding file name.
	 (Optional) It is used to enable or disable the zero configuration function.	
Configuring the Zero Configuration Function	zcm { enable disable }	Enables or disables the zero configuration function.
	 (Optional) It is used to configure a system restart policy.	
Configuring a Restart Policy	reload	Restarts a device.
	 (Optional) It is used to run the commands in batches.	
Running Batch File Commands	execute { [flash:] <i>filename</i> }	Runs the commands in batches.

2.4.1 Configuring Passwords and Privileges

Configuration Effect

- Configure passwords to control users' access to network devices.
- Assign a privilege level to a command to grant the command access to only the users at or higher than the level.
- Lower the command privilege level to grant more users access to the command.
- Raise the command privilege level to limit the command access to a few users.

Notes

- You can use the password configuration command with the **level** option to configure a password for a specific privilege level. After you specify the level and the password, the password works for the users who need to access this level.
- By default, no password is configured for any level. The default level is 15.
- If you configure a simple encrypted password with a non-15 level, a warning is displayed and the password is automatically converted into a secure encrypted password.
- The system chooses the secure encrypted password over the simple encrypted password if both of them are configured.

Configuration Steps

▾ Configuring a Simple Encrypted Password

- (Optional) Perform this configuration when you need to establish simple encrypted password verification when users switch between different privilege levels.
- Run the **enable password** command to configure a simple encrypted password.

▾ Configuring a Secure Encrypted Password

- (Optional) Perform this configuration when you need to establish secure encrypted password verification when users switch between different privilege levels.
- Run the **enable secret** command to configure a secure encrypted password.
- A secure encrypted password has the same function as a simple encrypted password but uses an enhanced password encryption algorithm. Therefore, secure encrypted passwords are recommended out of security consideration.

▾ Configuring Command Privilege Levels


- Optional.
- A command at a lower level is accessible by more users than a command at a higher level.

▾ Raising/Lowering a User Privilege Level

- After logging in to a network device, the user can change his/her level to obtain access to commands at different privilege levels.
- Run the **enable** command or the **disable** command to raise or lower a user privilege level respectively.
- To enable level increase logging, run the **login privilege log** command.

▾ Enabling Line Password Protection

- (Optional) Line password protection is required for remote login (such as login through Telnet).
- Run the **password [0 | 7] line** command to configure a line password, and then run the **login** command to enable login authentication.


 If a line password is configured but login authentication is not configured, the system does not display password prompt.


Verification

- Run the **show privilege** command to display the current user level.
- Run the **show running-config** command to display the configuration.

Related Commands

▾ Configuring a Simple Encrypted Password

Command	enable password [level level] { password [0 7] encrypted-password }
Parameter	<i>level</i> : Indicates a specific user level.
Description	<p><i>password</i>: Indicates the password used to enter privileged EXEC mode.</p> <p><i>0</i>: Indicates that the password is entered in plaintext.</p> <p><i>7</i>: Indicates that the password is entered in cyphertext.</p> <p><i>encrypted-password</i>: Indicates the password text, which must contain case-sensitive English letters and digits.</p> <hr/> <p> Leading spaces are allowed, but will be ignored. However, intermediate and trailing spaces are recognized.</p>
Command	Global configuration mode

Mode	
Usage Guide	<p>Currently, simple encrypted passwords can be configured with only level 15 and take effect only when no secure encrypted password is configured.</p> <p>If you configure a simple encrypted password with a non-15 level, a warning is displayed and the password is automatically converted into a secure encrypted password.</p> <p>If the level 15 simple encrypted password and secure encrypted password are configured the same, a warning is displayed.</p> <hr/> <p> If you specify an encryption type and enter a password in plaintext, you cannot re-enter privileged EXEC mode. An encrypted password cannot be retrieved once lost. You have to configure a new password.</p>


↘ Configuring a Secure Encrypted Password

Command	enable secret [level <i>level</i>] { <i>secret</i> [0 5] <i>encrypted-secret</i> }
Parameter	<i>level</i> : Indicates a specific user level.
Description	<p><i>secret</i>: Indicates the password used to enter privileged EXEC mode.</p> <p>0 5: Indicates the password encryption type. 0 indicates no encryption, and 5 indicates secure encryption.</p> <p><i>encrypted-password</i>: Indicates the password text.</p>
Command Mode	Global configuration mode
Usage Guide	Use this command to configure passwords for different privilege levels.

↘ Raising a User Privilege Level

Command	enable [<i>privilege-level</i>]
Parameter	<i>privilege-level</i> : Indicates a specific privilege level.
Description	
Command Mode	Privileged EXEC mode
Usage Guide	An increase in privilege level requires the input of the target level password.

↘ Lowering a User Privilege Level

Command	disable [<i>privilege-level</i>]
Parameter	<i>privilege-level</i> : Indicates a specific privilege level.
Description	
Command Mode	Privileged EXEC mode
Usage Guide	<p>A reduction in privilege level does not require password input.</p> <p>Use this command to exit Privileged EXEC mode and return to user EXEC mode. If <i>privilege-level</i> is specified, the current privilege level is reduced to the specified level.</p> <hr/> <p> <i>privilege-level</i> must be lower than the current level.</p>

↘ Enabling Level Increase Logging

Command	login privilege log
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command to enable logging of privilege level increase. The configuration takes effect for all terminals.

↘ Configuring Command Privilege Levels

Command	privilege mode [all] { level level reset } command-string
Parameter Description	<p><i>mode</i>: Indicates the CLI mode of the command. For example, config indicates the global configuration mode, EXEC indicates the privileged command mode, and interface indicates the interface configuration mode.</p> <p>all: Changes the subcommand privilege levels of a specific command to the same level.</p> <p>level level: Indicates a privilege level, ranging from 0 to 15.</p> <p>reset: Restores the command privilege level to the default.</p> <p><i>command-string</i>: Indicates the command to be assigned a privilege level.</p>
Command Mode	Global configuration mode
Usage Guide	To restore a command privilege level, run the no privilege mode [all] level level command command in global configuration mode.

↘ Specifying a Line Password

Command	password[0 7] line
Parameter Description	<p>0: Indicates to configure a password in plaintext.</p> <p>7: Indicates to configure a password in cyphertext.</p> <p><i>line</i>: Indicates the password string.</p>
Command Mode	Line configuration mode
Usage Guide	N/A

↘ Enabling Line Password Protection

Command	login
Parameter Description	N/A
Command Mode	Line configuration mode
Usage Guide	N/A

Configuration Example

↘ Configuring Command Authorization

Scenario	Assign privilege level 1 to the reload command and its subcommands and configure level 1 as the valid
-----------------	--

	level (by configuring the test password).
Configuration Steps	<ul style="list-style-type: none"> Assign privilege level 1 to the reload command and its subcommands. <pre> Orion Alpha A28X# configure terminal Orion Alpha A28X(config)# privilege exec all level 1 reload Orion Alpha A28X(config)# enable secret level 1 0 test Orion Alpha A28X(config)# end </pre>
Verification	<ul style="list-style-type: none"> Check whether the reload command and its subcommands are accessible at level 1. <pre> Orion Alpha A28X# disable 1 Orion Alpha A28X> reload ? at reload at<cr> </pre>

2.4.2 Configuring Login and Authentication

Configuration Effect

- Establish line-based login identity authentication.
- Run the **telnet** command on a network device to log in to a remote device.
- Close an established connection if no output is detected during the timeout time.
- Disconnect an established session connecting to a remote host and restore the host to Idle if no output is detected during the timeout time.
- Lock a terminal to deny access. 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.

Configuration Steps

▾ Configuring Local User Information

- Mandatory.
- Run the **username** command to configure the account used for local identity authentication and authorization, including usernames, passwords, and optional authorization information.
- Perform this configuration on every device.

▾ Configuring Local Authentication for Line-Based Login

- Mandatory.
- Configure local authentication for line-based login in the case that AAA is disabled.
- Perform this configuration on every device.

▾ Configuring AAA Authentication for Line-Based Login

- (Optional) Perform this configuration to configure AAA authentication for line-based login.
- Configure AAA authentication for line-based login in the case that AAA is enabled.
- Perform this configuration on every device.

↘ **Configuring Non-AAA Authentication for Line-Based Login When AAA Is Enabled**

- Optional.
- Run the **login access non-aaa** command in global configuration mode to authenticate line-based login in non-AAA mode in the case that AAA is enabled.
- Perform this configuration on every device.

↘ **Enabling the Telnet Client Service**

- Run the **telnet** command to log in to a remote device.

↘ **Enabling the DoTelnet Client Service**

- Run the **do telnet** command to log in to a remote device.

↘ **Restoring a Telnet Client Connection**

- (Optional) Perform this configuration to restore the connection on a Telnet client.

↘ **Closing a Suspended Telnet Client Connection**

- (Optional) Perform this configuration to close the suspended connection on a Telnet client.

↘ **Enabling the Telnet Server Service**

- Optional.
- Enable the Telnet Server service when you need to enable Telnet login.

↘ **Configuring the Connection Timeout Time**

- Optional.
- An established connection will be closed if no output is detected during the timeout time.
- Perform this configuration when you need to increase or reduce the connection timeout time.

↘ **Configuring the Session Timeout Time**

- Optional.
- The session connecting to a remote host will be disconnected and the host be restored to Idle if no output is detected during the timeout time.
- Perform this configuration when you need to increase or reduce the session timeout time.

↘ **Locking a Session**

- (Optional) Perform this configuration when you need to temporarily exit a session on a device.

- To lock a session, first enable terminal lock in line configuration mode, and then run the **lock** command to lock the terminal.

Verification

- Run the **show running-config** command to display the configuration.
- In the case that AAA is disabled, after local user information and line-based local authentication are configured, check whether users are prompted for username and password input for access to the CLI.
- In the case that AAA is enabled, after local user information and local AAA authentication are configured, check whether users are prompted for username and password input for access to the CLI.
- Run the **show user** command to display the information about the users who have logged in to the CLI.
- Telnet clients can connect to devices enabled with the Telnet Server service.
- When a user presses **Enter** on a locked CLI, the user is prompted for password input. The session is unlocked only when the entered password is the same as the configured one.
- Run the **show sessions** command to display every established Telnet client instance.

Related Commands

📌 Configuring Local User Information

Command	username <i>name</i> [login mode { aux console ssh telnet }] [online amount <i>number</i>] [permission <i>oper-mode path</i>] [privilege <i>privilege-level</i>] [reject remote-login] [web-auth] [pwd-modify] [nopassword password [0 7] <i>text-string</i> secret [0 5] <i>text-string</i>]
Parameter Description	<p><i>name</i>: Indicates a user name.</p> <p>login mode: Indicates the login mode.</p> <p>aux: Sets the login mode to AUX.</p> <p>console: Sets the login mode to Console.</p> <p>ssh: Sets the login mode to SSH.</p> <p>telnet: Sets the login mode to Telnet.</p> <p>online amount <i>number</i>: Indicates the maximum number of online accounts.</p> <p>permission <i>oper-mode path</i>: Configures the file operation permission. <i>op-mode</i> indicates the operation mode, and <i>path</i> indicates the directory or path of a specific file.</p> <p>privilege <i>privilege-level</i>: Indicates the account privilege level, ranging from 0 to 15.</p> <p>reject remote-login: Rejects remote login by using the account.</p> <p>web-auth: Allows only Web authentication for the account.</p> <p>pwd-modify: Allows the account owner to change the password. This option is available only when web-auth is configured.</p> <p>nopassword: Indicates that no password is configured for the account.</p> <p>password [0 7] <i>text-string</i>: Indicates the password configured for the account. 0 indicates that the password is input in plaintext, and 7 indicates that the password is input in cyphertext. The default is plaintext.</p> <p>secret [0 5] <i>text-string</i>: If the password type is 0, the password is in plain text. If the type is 5, the password is encrypted. The password is in plain text by default.</p>

Command Mode	Global configuration mode
Usage Guide	Use this command to create a local user database to be used by authentication. If the value 7 is selected for the encryption type, the entered cyphertext string must consist of an even number of characters. This setting is applicable to the scenario where encrypted passwords may be copied and pasted. In other cases, the value 7 is not selected.

↘ [Configuring Local Authentication for Line-Based Login](#)

Command	login local
Parameter Description	N/A
Command Mode	Line configuration mode
Usage Guide	Use this command to configure local authentication for line-based login in the case that AAA is disabled. Local user information is configured by using the username command.

↘ [Configuring AAA Authentication for Line-Based Login](#)

Command	login authentication { default list-name }
Parameter Description	default: Indicates the default authentication method list name. <i>list-name:</i> Indicates the optional method list name.
Command Mode	Line configuration mode
Usage Guide	Use this command to configure AAA authentication for line-based login in the case that AAA is enabled. The AAA authentication methods, including RADIUS authentication, local authentication, and no authentication, are used during the authentication process.

↘ [Configuring Non-AAA Authentication for Line-Based Login When AAA Is Enabled](#)

Command	login access non-aaa
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command when you need to perform non-AAA authentication on line-based login in the case that AAA is enabled. The configuration takes effect for all terminals.

↘ [Enabling the Telnet Client Service](#)

Command	telnet host [port] [/source { ip A.B.C.D ipv6 X:X:X:X interface interface-name }]
Parameter Description	<i>host:</i> Indicates the IPv4 address, IPv6 address, or host name of the Telnet server. <i>port:</i> Indicates the TCP port number of the Telnet server. The default value is 23. /source: Indicates the source IP address or source port used by a Telnet client. ip A.B.C.D: Indicates the source IPv4 address used by the Telnet client. ipv6 X:X:X:X: Indicates the source IPv6 address used by the Telnet client.

	interface <i>interface-name</i> : Indicates the source port used by the Telnet client.
Command Mode	Privileged EXEC mode
Usage Guide	A user can telnet to a remote device identified by an IPv4 host name, IPv6 host name, IPv4 address, or IPv6 address.

📌 Enabling the DoTelnet Client Service

Command	do telnet <i>host</i> [<i>port</i>] [/ source { ip <i>A.B.C.D</i> ipv6 <i>X:X:X::X</i> interface <i>interface-name</i> }]
Parameter Description	<i>host</i> : Indicates the IPv4 address, IPv6 address, or host name of the Telnet server. <i>port</i> : Indicates the TCP port number of the Telnet server. The default value is 23. /source : Indicates the source IP address or source port used by a Telnet client. ip <i>A.B.C.D</i> : Indicates the source IPv4 address used by the Telnet client. ipv6 <i>X:X:X::X</i> : Indicates the source IPv6 address used by the Telnet client. interface <i>interface-name</i> : Indicates the source port used by the Telnet client.
Command Mode	Privileged EXEC mode/configuration mode/interface configuration mode
Usage Guide	A user can telnet to a remote device identified by an IPv4 host name, IPv6 host name, IPv4 address, or IPv6 address.

📌 Restoring a Telnet Client Session

Command	<1-99>
Parameter Description	N/A
Command Mode	User EXEC mode
Usage Guide	Use this command to restore a Telnet client session. A user can press the shortcut key Ctrl+Shift+6 X to temporarily exit the Telnet client session that is established using the telnet command, run the <1-99> command to restore the session, and run the show sessions command to display the session information.

📌 Closing a Suspended Telnet Client Connection

Command	disconnect <i>session-id</i>
Parameter Description	<i>session-id</i> : Indicates the suspended Telnet client session ID.
Command Mode	User EXEC mode
Usage Guide	Use this command to close a specific Telnet client session by entering the session ID.

📌 Enabling the Telnet Server Service

Command	enable service telnet-server
Parameter Description	N/A
Command Mode	Global configuration mode

Usage Guide	Use this command to enable the Telnet Server service. The IPv4 and IPv6 services are also enabled after the command is executed.
--------------------	--

↘ Configuring the Connection Timeout Time

Command	exec-timeout <i>minutes</i> [<i>seconds</i>]
Parameter	<i>minutes</i> : Indicates the connection timeout time in the unit of minutes.
Description	<i>seconds</i> : Indicates the connection timeout time in the unit of seconds.
Command Mode	Line configuration mode
Usage Guide	Use this command to configure the timeout time for the established connections on a line. A connection will be closed when no input is detected during the timeout time. To remove the connection timeout configuration, run the no exec-timeout command in line configuration mode.

↘ Configuring the Session Timeout Time

Command	session-timeout <i>minutes</i> [output]
Parameter	<i>minutes</i> : Indicates the session timeout time in the unit of minutes.
Description	output : Indicates whether to add data output as a timeout criterion.
Command Mode	Line configuration mode
Usage Guide	Use this command to configure the timeout time for the remote host sessions on a line. A session will be disconnected when no input is detected during the timeout time. To cancel the session timeout time, run the no session-timeout command in line configuration mode.

↘ Enabling Line-Based Terminal Lock

Command	lockable
Parameter	N/A
Description	
Command Mode	Line configuration mode
Usage Guide	N/A

↘ Locking a Terminal Connected to the Current Line

Command	lock
Parameter	N/A
Description	
Command Mode	Line configuration mode
Usage Guide	N/A

Configuration Example

↘ Establishing a Telnet Session to a Remote Network Device

Configuration Steps	<ul style="list-style-type: none"> ● Establish a Telnet session to a remote network device with the IP address 192.168.65.119. ● Establish a Telnet session to a remote network device with the IPv6 address 2AAA:BBBB::CCCC. ● Run the telnet command in privileged EXEC mode, and run the do telnet command in privileged EXEC mode/configuration mode/interface configuration mode.
	<pre>Orion Alpha A28X# telnet 192.168.65.119 Trying 192.168.65.119 ... Open User Access Verification Password:</pre>
	<pre>Orion Alpha A28X# telnet 2AAA:BBBB::CCCC Trying 2AAA:BBBB::CCCC ... Open User Access Verification Password: Orion Alpha A28X(config)# do telnet 2AAA:BBBB::CCCC Trying 2AAA:BBBB::CCCC ... Open User Access Verification Password:</pre>
Verification	<ul style="list-style-type: none"> ● Check whether the Telnet sessions are established to the remote network devices.

📌 Configuring the Connection Timeout Time

Configuration Steps	<ul style="list-style-type: none"> ● Set the connection timeout time to 20 minutes.
	<pre>Orion Alpha A28X# configure terminal//Enter global configuration mode. Orion Alpha A28X# line vty 0 //Enter line configuration mode. Orion Alpha A28X(config-line)#exec-timeout 20 //Set the connection timeout time to 20 minutes.</pre>
Verification	<ul style="list-style-type: none"> ● Check whether the connection between a terminal and the local device is closed when no input is detected during the timeout time.

📌 Configuring the Session Timeout Time

Configuration Steps	<ul style="list-style-type: none"> ● Set the session timeout time to 20 minutes.
	<pre>Orion Alpha A28X# configure terminal//Enter global configuration mode. Orion Alpha A28X(config)# line vty 0 //Enter line configuration mode. Orion Alpha A28X(config-line)#session-timeout 20//Set the session timeout time to 20 minutes.</pre>

Configuration Steps	<ul style="list-style-type: none"> ● Set the session timeout time to 20 minutes.
Verification	<ul style="list-style-type: none"> ● Check whether the session between a terminal and the local device is disconnected when no input is detected during the timeout time.

2.4.3 Configuring Basic System Parameters


Configuration Effect

- Configure basic system parameters.

Configuration Steps

▾ Configuring the System Date and Clock

- Mandatory.
- Configure the system time of a network device manually. The device clock starts from the configured time and keeps running even when the device is powered off.

 The time configuration is applied only to the software clock if the network device does not provide a hardware clock. The configuration will be invalid when the device is powered off.

▾ Updating the Hardware Clock

- Optional.
- Perform this configuration when you need to copy the date and time of the software clock to the hardware clock so that the hardware clock is synchronized with the software clock.

▾ Configuring a System Name

- (Optional) Perform this configuration to change the default system name.

▾ Configuring a Command Prompt

- (Optional) Perform this configuration to change the default command prompt.

▾ Configuring Daily Notification

- (Optional) Perform this configuration when you need to display important prompts or warnings to users.
- You can configure notification in one or multiple lines, which will be displayed to users after login.

▾ Configuring a Login Banner

- (Optional) Perform this configuration when you need to display important messages to users upon login or logout.

▾ Configuring the Console Baud Rate

- (Optional) Perform this configuration to change the default Console baud rate.

Verification

- Run the **show clock** command to display the system time.

- Check whether a login banner is displayed after login.
- Run the **show version** command to display the system information and version.

Related Commands

↘ Configuring the System Date and Clock

Command	clock set <i>hh:mm:ss month day year</i>
Parameter Description	<i>hh:mm:ss</i> : Indicates the current time, in the format of <i>hour</i> (24-hour format): <i>minute:second</i> . <i>day</i> : Indicates a day (1–31) of the month. <i>month</i> : Indicates a month (from January to December) of the year. <i>year</i> : Indicates a year, ranging from 1993 to 2035. Abbreviation is not supported.
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to configure the system time. If the device does not provide a hardware clock, the time configuration will be invalid when the device is powered off.

↘ Updating the Hardware Clock

Command	clock update-calendar
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	After the configuration, the time of the software clock will overwrite that of the hardware clock.

↘ Configuring a System Name

Command	hostname <i>name</i>
Parameter Description	<i>name</i> : Indicates the system name, which must consist of printable characters and must not exceed 63 bytes.
Command Mode	Global configuration mode
Usage Guide	To restore the system name to the default, run the no hostname command in global configuration mode.

↘ Configuring a Command Prompt

Command	prompt <i>string</i>
Parameter Description	<i>string</i> : Indicates the command prompt name. A name with more than 32 characters will be truncated to keep only the first 32 characters.
Command Mode	Privileged EXEC mode
Usage Guide	To restore the command prompt to the default settings, run the no prompt command in global configuration mode.

↘ Configuring Daily Notification

Command	banner motd <i>c message c</i>
Parameter Description	<i>c</i> : Indicates a delimiter, which can be any character, such as "&".
Command Mode	Global configuration mode
Usage Guide	A message must start and end with delimiter+carriage return respectively. Any characters following the ending delimiter will be dropped. Any letter contained in the message must not be used as the delimiter. The message must not exceed 255 bytes.

↘ [Configuring a Login Banner](#)

Command	banner login <i>c message c</i>
Parameter Description	<i>c</i> : Indicates a delimiter, which can be any character, such as "&".
Command Mode	Global configuration mode
Usage Guide	A message must start and end with delimiter+carriage return respectively. Any characters following the ending delimiter will be dropped. Any letter contained in the message must not be used as the delimiter. The message must not exceed 255 bytes. To remove the login banner configuration, run the no banner login command in global configuration mode.

↘ [Configuring the Console Baud Rate](#)

Command	speed <i>speed</i>
Parameter Description	<i>speed</i> : Indicates the console baud rate, in the unit of bps. The serial port baud rate can be set to 9,600 bps, 19,200 bps, 38,400 bps, 57,600 bps, or 115,200 bps. The default is 9,600 bps.
Command Mode	Line configuration mode
Usage Guide	You can configure the asynchronous line baud rate based on requirements. The speed command is used to configure receive and transmit rates for the asynchronous line.

Configuration Example

↘ [Configuring the System Time](#)

Configuration Steps	<ul style="list-style-type: none"> Change the system time to 2003-6-20, 10:10:12. <pre>Orion Alpha A28X# clock set 10:10:12 6 20 2003 //Configure the system time and date.</pre>
Verification	<ul style="list-style-type: none"> Run the show clock command in privileged EXEC mode to display the system time. <pre>Orion Alpha A28X# show clock //Confirm that the changed system time takes effect. clock: 2003-6-20 10:10:54</pre>

↘ [Configuring Daily Notification](#)

Configuration Steps	<ul style="list-style-type: none"> Configure the daily notification message "Notice: system will shutdown on July 6th." with the pound key (#) as the delimiter.
	<pre>Orion Alpha A28X(config)# banner motd #//Starting delimiter Enter TEXT message. End with the character '#''. Notice: system will shutdown on July 6th.# //Ending delimiter Orion Alpha A28X(config)#</pre>
Verification	<ul style="list-style-type: none"> Run the show running-config command to display the configuration. Connect to the local device through the Console, Telnet or SSH, and check whether daily notification is displayed before the CLI appears.
	<pre>C:\>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:</pre>

📌 Configuring a Login Banner

Configuration Steps	<ul style="list-style-type: none"> Configure the login banner message "Access for authorized users only. Please enter your password." with the pound key (#) as the delimiter.
	<pre>Orion Alpha A28X(config)# banner login #//Starting delimiter Enter TEXT message. End with the character '#''. Access for authorized users only. Please enter your password. # //Ending delimiter Orion Alpha A28X(config)#</pre>
Verification	<ul style="list-style-type: none"> Run the show running-config command to display the configuration. Connect to the local device through the Console, Telnet or SSH, and check whether the login banner is displayed before the CLI appears.
	<pre>C:\>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:</pre>

📌 Configuring the Serial Port Baud Rate

Configuration Steps	<ul style="list-style-type: none"> Set the serial port baud rate to 57,600 bps.
----------------------------	--

	<pre> Orion Alpha A28X# configure terminal //Enter global configuration mode. Orion Alpha A28X(config)# line console 0 //Enter console line configuration mode. Orion Alpha A28X(config-line)# speed 57600 //Set the console baud rate to 57,600 bps. Orion Alpha A28X(config-line)# end //Returns to privileged mode. </pre>
Verification	<ul style="list-style-type: none"> ● Run the show command to display the configuration.
	<pre> Orion Alpha A28X# show line console 0 //Displays the console configuration. 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 </pre>

2.4.4 Enabling and Disabling a Specific Service

Configuration Effect

- Dynamically adjust system services when the system is running, and enable and disable specific services (SNMP Agent, SSH Server, and Telnet Server).

Configuration Steps

📌 Enabling the SNMP Agent, SSH Server, and Telnet Server Services

- (Optional) Perform this configuration when you need to use these services.

Verification

- Run the **show running-config** command to display the configuration.
- Run the **show services** command to display the service Enabled/Disable state.

Related Commands

↳ Enabling the SSH Server, Telnet Server, and SNMP Agent Services

Command	<code>enable service { ssh-server telnet-server snmp-agent }</code>
Parameter Description	ssh-server: Enables or disables the SSH Server service. The IPv4 and IPv6 services are also enabled together with this service. telnet-server: Enables or disables the Telnet Server service. The IPv4 and IPv6 services are also enabled together with this service. snmp-agent: Enables or disables the SNMP Agent service. The IPv4 and IPv6 services are also enabled together with this service.
Command Mode	Global configuration mode
Usage Guide	Use this command to enable and disable specific services.

Configuration Example

↳ Enabling the SSH Server Service

Configuration Steps	<ul style="list-style-type: none">● Enable the SSH Server service.
	<pre>Orion Alpha A28X# configure terminal //Enter global configuration mode. Orion Alpha A28X(config)#enable service ssh-server //Enable the SSH Server service.</pre>
Verification	<ul style="list-style-type: none">● Run the show running-config command to display the configuration.● Run the show ip ssh command to display the configuration and running state of the SSH Server service.

2.4.5 Configuring Multiple-configuration Booting

Configuration Effect

- Modify the path for saving startup configurations and the corresponding file name.

Notes

- The startup configuration file name consists of a path and a file name. The path is mandatory. Otherwise, configurations cannot be saved by using the **write** command. Take **Flash:/Orion Alpha A28X/Orion Alpha A28X.text** as examples, where the **Flash:/Orion Alpha A28X** folder must exist. In master-slave mode, all device paths are required.

Configuration Steps

↳ Modifying the Path for Saving Startup Configurations and the Corresponding File Name

- (Optional) Perform this configuration when you need to modify the startup configuration file.

Verification

- Run the **show boot config** command to display the path for saving startup configurations and the corresponding file name.

Related Commands

↘ Modifying the Path for Saving Startup Configurations and the Corresponding File Name

Command	boot config { flash:filename }
Parameter Description	flash: Saves the startup configuration file in the extensible Flash.
Command Mode	Global configuration mode
Usage Guide	Use this command to modify the path for saving startup configurations and the corresponding file name.

Configuration Example

↘ Changing the Path of the Startup Configuration File to Flash:/Orion Alpha A28X.text

Configuration Steps	<ul style="list-style-type: none"> ● Change the startup configuration file path into Flash:/Orion Alpha A28X.text.
	<pre>Orion Alpha A28X# configure terminal //Enter global configuration mode. Orion Alpha A28X(config)# boot config flash:/Orion Alpha A28X.text//Change the path and file name into flash:/Orion Alpha A28X.text.</pre>
Verification	<ul style="list-style-type: none"> ● Run the show boot config command to display the path for saving startup configurations and the corresponding file name.

2.4.6 Configuring the Zero Configuration Function

Configuration Effect

- Enable or disable the zero configuration function.

Notes

- The zero configuration function is applicable to the ACS solution only.
- With the zero configuration function, DHCP Snooping Trust is enabled only on the last two electrical ports and all SFP ports of the device by default, regardless of whether the device supports the MGMT port.
- Enabling and disabling the zero configuration function will delete the startup configuration file of the device and trigger device restart.

Configuration Steps

↘ Enabling or Disabling the Zero Configuration Function

- (Optional) Perform this configuration when you need to enable or disable the zero configuration function.

Verification

- Run the **show zcm mod** command to check whether the zero configuration function is enabled.

Related Commands

↳ Enabling or Disabling the Zero Configuration Function

Command	zcm { enable disable }
Parameter	enable: Enables the zero configuration function.
Description	disable: Disables the zero configuration function.
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to enable and disable the zero configuration function.

Configuration Example

↳ Enabling the Zero Configuration Function

Configuration Steps	<ul style="list-style-type: none"> ● Enable the zero configuration function. <pre>Orion Alpha A28X# zcm enable //Enable the zero configuration function. %% Warning: After switching mode the device will automatically restart! % Do you want to switch to zero configuration mode? [yes/no]:y *Sep 29 12:36:20: %ZCM-5-MODE_SWITCH: The device is reloading due to zero or non-zero configuration mode switch.</pre>
Verification	<ul style="list-style-type: none"> ● Run the show zcm mode command to display whether the zero configuration function is enabled.

2.4.7 Configuring a Restart Policy

Configuration Effect

Configure a restart policy to restart a device as scheduled.

Configuration Steps


↳ Configuring Direct Restart


Run the **reload** command in privileged EXEC mode to restart the system immediately.

↳ Configuring Timed Restart

```
reload at hh:mm:ss month day year
```

If you configure a specific time, the system will restart at the time. The time must be a time in the future. The **month day year** parameter is optional. If it is not specified, the system clock time is used by default.

 The clock feature must be supported by the system if you want to use the **at** option. It is recommended that you configure the system clock in advance. A new restart plan will overwrite the existing one. A restart plan will be invalid if the system is restarted before the plan takes effect.

 The restart time must be later than the current system time. After you configure a restart plan, do not change the system clock; otherwise, the plan may fail (for example, the system time is changed to a time after the restart time.)

Related Commands

Restarting a Device

Command	<code>reload [at { <i>hh</i> [:<i>mm</i> [:<i>ss</i>]] } [<i>month</i> [<i>day</i> [<i>year</i>]]]]</code>
Parameter	at <i>hh:mm:ss</i> : Indicates the time when the system will restart.
Description	<i>month</i> : Indicates a month of the year, ranging from 1 to 12. <i>day</i> : Indicates a date, ranging from 1 to 31. <i>year</i> : Indicates a year, ranging from 1993 to 2035. Abbreviation is not supported.
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to enable a device to restart at a specific time.

2.4.8 Running Batch File Commands


Configuration Effect


Run the commands in batches.

Configuration Steps

Running the execute Command

Run the **execute** command, with the path set to the batch file to be executed.

 You can specify the name and content of the batch file on your PC and transfer the file to the device flash memory through TFTP. The batch processing content simulates user input. Therefore, you need to edit the batch file content according to the CLI command configuration sequence. In addition, you need to write the responses to interactive commands to the batch file to ensure normal command execution.

 The batch file size must not exceed 128 KB; otherwise, it will fail to be executed. You can divide a large batch file into multiple parts not larger than 128 KB each.

Related Commands

Command	<code>execute { [flash :] <i>filename</i> }</code>
Parameter	<i>filename</i> : Indicates the path for the batch file to be executed.
Description	
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to run the commands related to a function in batches.

2.5 Monitoring

Displaying

Description	Command
show boot config	Displays the path and filename of the startup configuration file.
show clock	Displays the current system time.
show line { aux <i>line-num</i> console <i>line-num</i> tty <i>line-num</i> vty <i>line-num</i> <i>line-num</i> }	Displays line configurations.
show reload	Displays system restart settings.
show running-config [interface <i>interface</i>]	Displays the current running configurations of the device or the configurations on an interface.
show startup-config	Displays the device configurations stored in the NVRAM.
show this	Displays the current system configurations.
show version [devices module slots]	Displays system information.
show sessions	Displays the information of each established Telnet client instance.

3 Configuring Lines

3.1 Overview

There are various types of terminal lines on network devices. You can manage terminal lines in groups based on their types. Configurations on these terminal lines are called line configurations. On network devices, terminal lines are classified into multiple types such as CTY, TTY, AUX, and VTY.

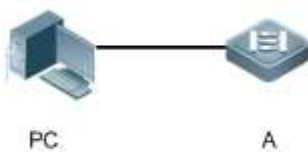
3.2 Applications

Application	Description
Accessing a Device Through Console	Enter the command-line interface (CLI) of a network device through the Console.
Accessing a Device Through VTY	Enter the CLI of a network device through Telnet or SSH.

3.2.1 Accessing a Device Through Console

Scenario

Figure 3-4



Remarks	A is a network device to be managed. PC is a network management station.
----------------	---

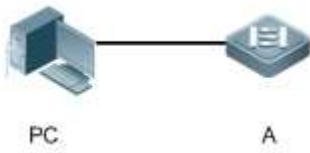
Deployment

The network management station connects to the Console port of a network device through a serial cable. Using the Console software (Hyper Terminal or other terminal simulation software) on the network management station, you can access the Console of the network device and enter the CLI to configure and manage the network device.

3.2.2 Accessing a Device Through VTY

Scenario

Figure 3-5



Remarks	A is a network device to be managed. PC is a network management station.
----------------	---

Deployment

The network management station connects to a network device through the network. Using a VTY client (such as Putty) on the network management station, you can access the network device through Telnet or SSH and enter the CLI to configure and manage the network device.

3.3 Features

Basic Concepts

↳ CTY

The CTY line refers to the line connected to the Console port. Most network devices have a Console port. You can access the local system through the Console port.

↳ VTY

The VTY line is a virtual terminal line that does not correspond to any hardware. It is used for Telnet or SSH connection.

Overview

Feature	Description
Basic Features	Configures a terminal, displays and clears terminal connection information.

3.3.1 Basic Features

Related Configuration

↳ Configuring Terminal Lines

Run the **line** command in global configuration mode to enter the configuration mode of a specified line.

Configure the line attributes.

↳ Clearing Terminal Connections


When a terminal connects to the network device, the corresponding terminal line is occupied. Run the **show user** command to display the connection status of these terminal lines. If you want to disconnect the terminal from the network device, run the **clear line** command to clear the terminal line. After the terminal lines are cleared, the related connections (such as Telnet and SSH) are interrupted, the CLI exits, and the terminal lines restore to the unoccupied status. Users can re-establish connections.

📌 Specifying the Number of VTY Terminals

Run the **line vty** command to enter the VTY line configuration mode and specify the number of VTY terminals.

By default, there are 5 VTY terminals, numbered from 0 to 4. You can increase the number of VTY terminals to 36, with new ones numbered from 5 to 35. Only new terminals can be removed.

3.4 Configuration

Configuration	Description and Command	
Entering Line Configuration Mode	 (Mandatory) It is used to enter the line configuration mode.	
	line [console vty] first-line [last-line]	Enters the specified line configuration mode.
	line vty line-number	Increases or reduces the number of available VTY lines.

3.4.1 Entering Line Configuration Mode

Configuration Effect

Enter line configuration mode to configure other functions.

Configuration Steps

📌 Entering Line Configuration Mode

- Mandatory.
- Unless otherwise specified, enter line configuration mode on each device to configure line attributes.

📌 Increasing/Reducing the Number of VTY Lines

- Optional.
- Run the **(no) line vty line-number** command to increase or reduce the number of VTY lines.

Verification

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

Related Commands

📌 Entering Line Configuration Mode

Command	line [console vty] first-line [last-line]
Parameter	console: Indicates the Console port.
Description	vtty: Indicates a virtual terminal line, which supports Telnet or SSH. <i>first-line:</i> Indicates the number of the first line. <i>last-line:</i> Indicates the number of the last line.
Command	Global configuration mode

Mode	
Usage Guide	N/A

↘ Increasing/Reducing the Number of VTY Lines


Command	<code>line vty line-number</code>
Parameter Description	<i>line-number</i> : Indicates the number of VTY lines. The value ranges from 0 to 35.
Command Mode	Global configuration mode
Usage Guide	Run the no line vty line-number command to reduce the number of available VTY lines.

↘ Displaying Line Configuration

Command	<code>show line {console line-num vty line-num line-num }</code>
Parameter Description	console : Indicates the Console port. vty : Indicates a virtual terminal line, which supports Telnet or SSH. <i>line-num</i> : Indicates the line to be displayed.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuration Example



Scenario Figure 3-6	 <p>The diagram shows a PC on the left connected by a line to a network device labeled 'A' on the right.</p>
Configuration Steps	<ul style="list-style-type: none"> ● Connect the PC to network device A through the Console line and enter the CLI on the PC. ● Run the show user command to display the connection status of the terminal line. ● Run the show line console 0 command to display the status of the Console line. ● Enter global configuration mode and run the line vty command to increase the number of VTY terminals to 36.
A	<pre>Orion Alpha A28X#show user Line User Host(s) Idle Location ----- * 0 con 0 --- idle 00:00:00 --- Orion Alpha A28X#show line console 0</pre>

```

CON      Type      speed  Overruns
* 0      CON      9600   0

Line 0, Location: "", Type: "vt100"

Length: 24 lines, Width: 79 columns

Special Chars: Escape Disconnect Activation
                ^x      ^D      ^M

Timeouts:      Idle EXEC      Idle Session
                00:10:00      never

History is enabled, history size is 10.

Total input: 490 bytes
Total output: 59366 bytes
Data overflow: 0 bytes
stop rx interrupt: 0 times

Orion Alpha A28X#show line vty ?
<0-5>      Line number

Orion Alpha A28X#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Orion Alpha A28X(config)#line vty 35

Orion Alpha A28X(config-line)#

*Oct 31 18:56:43: %SYS-5-CONFIG_I: Configured from console by console

```

Verification

- After running the **show line** command, you can find that the number of terminals increases.
- Run the **show running-config** command to display the configuration.

A

```

Orion Alpha A28X#show line vty ?
<0-35>      Line number

Orion Alpha A28X#show running-config

Building configuration...

Current configuration : 761 bytes

```

```
version 11.0(1C2B1) (10/16/13 04:23:54 CST -ngcf78)

ip tcp not-send-rst

vlan 1
!
interface GigabitEthernet 0/0
!
interface GigabitEthernet 0/1
  ip address 192.168.23.164 255.255.255.0
!
interface GigabitEthernet 0/2
!
interface GigabitEthernet 0/3
!
interface GigabitEthernet 0/4
!
interface GigabitEthernet 0/5
!
interface GigabitEthernet 0/6
!
interface GigabitEthernet 0/7
!
interface Mgmt 0
!
line con 0
line vty 0 35
  login
!
end
```

3.4.2 Configuring Line Attributes

Configuration Effect

Configure line attributes in line configuration mode.

Configuration Steps

↳ Configuring the Absolute Timeout for Line Disconnection

- Optional.
- Run the **absolute-timeout** command to ensure that a line is disconnected after the specified time.

↳ Configuring the Character You Enter at a Vacant Terminal to Begin a Terminal Session

- Optional.
- Run the **activation-character** command in line configuration mode to configure a character to activate a terminal.

↳ Enabling Automatic Command Execution

- Optional.
- Run the **autocommand** command in line configuration mode to enable automatic command execution on terminals with asynchronous ports.

↳ Configuring the Number of Data Bits per Character for Physical Terminal Connections

- Optional.
- Run the **databits** command in line configuration mode.

↳ Configuring the EXEC Character Width for Physical Terminal Connections

- Optional.
- Run the **exec-character-bits** command in line configuration mode.

↳ Configuring Flow Control Mode for Physical Terminal Connections

- Optional.
- Run the **flowcontrol** command in line configuration mode.

↳ Configuring the Parity Bit for Physical Terminal Connections

- Optional.
- Run the **parity** command in line configuration mode.

↳ Configuring the Start Character of Software Flow Control for Physical Terminal Connections

- Optional.
- Run the **start-character** command in line configuration mode.

↳ Configuring the Stop Character of Software Flow Control for Physical Terminal Connections

- Optional.
- Run the **stop-character** command in line configuration mode.

↳ Configuring the Number of Stop Bits per Byte for Physical Terminal Connections

- Optional.
- Run the **stopbits** command in line configuration mode.

↘ [Configuring the Type of Terminal Connected to a Line](#)

- Optional.
- Run the **terminal-type** command in line configuration mode.

Verification

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

Related Commands

↘ [Configuring the Absolute Timeout for Line Disconnection](#)

Command	absolute-timeout <i>minutes</i>
Parameter Description	<i>minutes</i> : Indicates the absolute timeout of the current line in minutes. The value ranges from 0 to 60.
Command Mode	Line configuration mode
Usage Guide	Configure the absolute timeout for line disconnection. As long as the specified time expires, the line is disconnected no matter whether you are on the operating terminal or not. Before the line is disconnected, the system displays the remaining time after which the terminal will exit: <pre>Terminal will be login out after 20 second</pre>

↘ [Configuring the Character You Enter at a Vacant Terminal to Begin a Terminal Session](#)

Command	activation-character <i>ascii-value</i>
Parameter Description	<i>ascii-value</i> : Indicates the ASCII value of the hotkey character for beginning a terminal session. The value ranges from 0 to 127.
Command Mode	Line configuration mode
Usage Guide	If auto-selection is enabled for the current line, the hotkey character for beginning a terminal session must be set to the default value.

↘ [Enabling Automatic Command Execution](#)

Command	autocommand <i>autocommand-string</i>
Parameter Description	<i>autocommand-string</i> : Indicates the command line to be automatically executed.
Command Mode	Line configuration mode
Usage Guide	In most cases, after a user acts as a dumb terminal to connect to a router through an asynchronous serial port, the user can remotely log in to the specified host through Telnet or obtain the specified application-based terminal service with the autocommand command.

▾ Configuring the Number of Data Bits per Character for Physical Terminal Connections

Command	databits <i>bit</i>
Parameter Description	<i>bit</i> : Indicates the number of data bits per character. The value ranges from 5 to 8.
Command Mode	Line configuration mode
Usage Guide	The asynchronous hardware (such as an asynchronous serial port and AUX port) of a router generates seven data bits with parity in flow communication mode. If parity is being generated, specify 7 data bits per character. If no parity is being generated, specify 8 data bits per character. Only early devices support 5 or 6 data bits, which are seldom used.

▾ Configuring the EXEC Character Width for Physical Terminal Connections

Command	exec-character-bits { 7 8 }
Parameter Description	7 : Selects the 7-bit ASCII character set. 8 : Selects the 8-bit ASCII character set.
Command Mode	Line configuration mode
Usage Guide	If you need to enter Chinese characters or display Chinese characters, images, or other international characters in the command line, run the exec-character-bits 8 command.

▾ Configuring Flow Control Mode for Physical Terminal Connections

Command	flowcontrol { hardware none software }
Parameter Description	hardware : Configures hardware flow control. none : Configures no flow control. software : Configures software flow control.
Command Mode	Line configuration mode
Usage Guide	By running this command, you can specify the flow control mode to keep the Tx rate of one end the same as the Rx rate of the peer end. Since terminals cannot receive data while sending data, flow control serves to prevent data loss. When high-data-rate devices communicate with low-rate-data devices (e.g., a printer communicates with a network port), you also need to enable flow control to prevent data loss. Orion Alpha A28X general operating system provides two flow control modes: software flow control (controlled with control keys) and hardware flow control (controlled by hardware). The default stop character and start character for software flow control are respectively Ctrl+S (XOFF, with the ASCII value 19) and Ctrl+Q (XON, with the ASCII value 17). You can also run the stop-character and start-character commands to configure them.

▾ Configuring the Parity Bit for Physical Terminal Connections

Command	parity { even none odd }
Parameter Description	even : Indicates the even parity check. none : Indicates no parity check. odd : Indicates the odd parity check.

Command Mode	Line configuration mode
Usage Guide	When using certain hardware (such as an asynchronous serial port and Console port) for communication, you are usually required to configure a parity bit.

↘ Configuring the Start Character of Software Flow Control for Physical Terminal Connections

Command	start-character <i>ascii-value</i>
Parameter Description	<i>ascii-value</i> : Indicates the ASCII value of the start character of software flow control for physical terminal connections. The value ranges from 0 to 255.
Command Mode	Line configuration mode
Usage Guide	After software flow control is enabled, the start character for software flow control indicates the start of data transmission.

↘ Configuring the Stop Character of Software Flow Control for Physical Terminal Connections

Command	stop-character <i>ascii-value</i>
Parameter Description	<i>ascii-value</i> : Indicates the ASCII value of the stop character of software flow control for physical terminal connections. The value ranges from 0 to 255.
Command Mode	Line configuration mode
Usage Guide	After software flow control is enabled, the stop character for software flow control indicates the end of data transmission.

↘ Configuring the Number of Stop Bits per Byte for Physical Terminal Connections


Command	stopbits { 1 2 }
Parameter Description	1: Indicates one stop bit. 2: Indicates two stop bits.
Command Mode	Line configuration mode
Usage Guide	You should configure the stop bits for communication between the asynchronous line and the connected network device (such as a conventional numb terminal and modem).

↘ Configuring the Type of Terminal Connected to a Line

Command	terminal-type <i>terminal-type-string</i>
Parameter Description	<i>terminal-type-string</i> : Indicates the description of the terminal type, such as vt100 and ansi.
Command Mode	Line configuration mode
Usage Guide	You can run the terminal-type vt100 command to restore the default terminal type or run the terminal-type command to configure the type of terminal connected to a line as required. Upon Telnet connection, one end negotiates with the other end about the terminal type based on its terminal type configuration (Telnet ID: 0x18). For details, see RFC 854.

Configuration Example

Configuring the Baud Rate, Data Bits, Parity Bits, and Stop Bits

Scenario Figure 3-7	 <p>The diagram shows a laptop labeled 'PC' on the left and a network device labeled 'A' on the right. A black line representing a console cable connects the two devices.</p>
Configuration Steps	<ul style="list-style-type: none">● Connect the PC to network device A through the Console line and enter the CLI on the PC.● Configure the baud rate, data bits, parity bit, and stop bits in global configuration mode.● Run the show line console 0 command to display the status of the Console line.
A	<pre>Orion Alpha A28X#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Orion Alpha A28X(config)#line console 0 Orion Alpha A28X(config-line)#speed 115200 Orion Alpha A28X(config-line)#databits 8 Orion Alpha A28X(config-line)#parity even Orion Alpha A28X(config-line)#stopbits 1 Orion Alpha A28X#show line console 0 CON Type speed Overruns * 0 CON 115200 0 Line 0, Location: "", Type: "vt100" Length: 24 lines, Width: 79 columns Special Chars: Escape Disconnect Activation ^^x none Timeouts: Idle EXEC Idle Session 00:10:00 never History is enabled, history size is 10. Total input: 636 bytes Total output: 30498 bytes Data overflow: 0 bytes stop rx interrupt: 0 times</pre>
Verification	<ul style="list-style-type: none">● Run the show running-config command to display the configuration.
A	<pre>Orion Alpha A28X#show line vty ?</pre>

<0-35> Line number

Orion Alpha A28X#show running-config

Building configuration...

Current configuration : 761 bytes

version 11.0(1C2B1) (10/16/13 04:23:54 CST -ngcf78)

ip tcp not-send-rst

vlan 1

!

interface GigabitEthernet 0/0

!

interface GigabitEthernet 0/1

ip address 192.168.23.164 255.255.255.0

!

interface GigabitEthernet 0/2

!

interface GigabitEthernet 0/3

!

interface GigabitEthernet 0/4

!

interface GigabitEthernet 0/5

!

interface GigabitEthernet 0/6

!

interface GigabitEthernet 0/7

!

line con 0

parity even

stopbits 1

speed 115200

line vty 0 35

```
login
!  
end
```

3.4.3 Configuring Terminal Attributes

Configuration Effect

Configure terminal attributes in privileged EXEC mode of a terminal.

Configuration Steps

▾ Configuring the Number of Data Bits per Character for the Current Session

- Optional.
- Run the **terminal databits** command on the terminal.

▾ Configuring the EXEC Character Width for the Current Session

- Optional.
- Run the **terminal exec-character-bits** command on the terminal.

▾ Configuring Flow Control Mode for the Current Session

- Optional.
- Run the **terminal flowcontrol** command on the terminal.

▾ Configuring the Parity Bits for the Current Session

- Optional.
- Run the **terminal parity** command on the terminal.

▾ Configuring the Start Character of Software Flow Control for the Current Session

- Optional.
- Run the **terminal start-character** command on the terminal.

▾ Configuring the Stop Character of Software Flow Control for the Current Session

- Optional.
- Run the **terminal stop-character** command on the terminal.

▾ Configuring the Number of Stop Bits in Each Byte for the Current Session

- Optional.
- Run the **terminal stopbits** command on the terminal.

▾ Configuring the Type of Terminal Connected to the Current Line for the Current Session

- Optional.
- Run the [terminal terminal-type](#) command on the terminal.

Verification

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

Related Commands

▾ Configuring the Number of Data Bits per Character for the Current Session

Command	terminal databits <i>bit</i>
Parameter Description	<i>bit</i> : Indicates the number of data bits per character, ranging from 5 to 8.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

▾ Configuring the EXEC Character Width for the Current Session

Command	terminal exec-character-bits { 7 8 }
Parameter Description	7: Selects the 7-bit ASCII character set. 8: Selects the full 8-bit ASCII character set.
Command Mode	Privileged EXEC mode
Usage Guide	If you need to enter Chinese characters or display Chinese characters, images, or other international characters in the command line, run the terminal exec-character-bits 8 command.

▾ Configuring Flow Control Mode for the Current Session

Command	terminal flowcontrol { hardware none software }
Parameter Description	hardware : Configures hardware flow control. none : Configures no flow control. software : Configures software flow control.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

▾ Configuring the Parity Bit of the Asynchronous Line for the Current Session

Command	terminal parity { even none odd }
Parameter Description	even : Indicates the even parity check. none : Indicates no parity check. odd : Indicates the odd parity check.
Command Mode	Line configuration mode

Usage Guide	When using certain hardware (such as an asynchronous serial port and Console port) for communication, you are usually required to configure a parity bit.
--------------------	---

↘ Configuring the Start Character of Software Flow Control for the Current Session

Command	terminal start-character <i>ascii-value</i>
Parameter Description	<i>ascii-value</i> : Indicates the ASCII value of the start character of software flow control for the current session. The value ranges from 0 to 255.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

↘ Configuring the Stop Character of Software Flow Control for the Current Session

Command	terminal stop-character <i>ascii-value</i>
Parameter Description	<i>ascii-value</i> : Indicates the ASCII value of the stop character of for the current session. The value ranges from 0 to 255.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

↘ Configuring the Number of Stop Bits for the Current Session


Command	terminal stopbits { 1 2 }
Parameter Description	1: Indicates one stop bit. 2: Indicates two stop bits.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

↘ Configuring the Type of Terminal Connected to the Current Line for the Current Session

Command	terminal terminal-type <i>terminal-type-string</i>
Parameter Description	<i>terminal-type-string</i> : Indicates the description of the terminal type, such as vt100 and ansi.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuration Example

↘ Configuring the Terminal Type and Baud Rate of a Terminal

Scenario Figure 3-8	 <p>The diagram illustrates a connection between a PC and a terminal device. On the left, there is an icon of a laptop labeled 'PC'. A horizontal line connects it to a terminal device icon on the right, which is labeled 'A'.</p>
-------------------------------	---

Configuration Steps	<ul style="list-style-type: none"> ● Connect the PC to network device A through the Console line and enter the CLI on the PC. ● Configure the terminal type and baud rate of the terminal in privileged EXEC mode.
A	<pre>Orion Alpha A28X#terminal terminal-type ansi Orion Alpha A28X#terminal speed 115200</pre>
Verification	<ul style="list-style-type: none"> ● Run the show line console 0 command to display the status of the Console line.
A	<pre>Orion Alpha A28X#show line console 0 CON Type speed Overruns * 0 CON 115200 0 Line 0, Location: "", Type: "ansi" Length: 24 lines, Width: 79 columns Special Chars: Escape Disconnect Activation ^x none Timeouts: Idle EXEC Idle Session 00:10:00 never History is enabled, history size is 10. Total input: 858 bytes Total output: 57371 bytes Data overflow: 0 bytes stop rx interrupt: 0 times</pre>

3.5 Monitoring

Clearing



Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears the line connection status.	clear line { console <i>line-num</i> vty <i>line-num</i> <i>line-num</i> }

Displaying

Description	Command
Displays the line configuration.	show line { console <i>line-num</i> vty <i>line-num</i> <i>line-num</i> }
Displays historical records of a line.	show history
Displays the privilege level of a line.	show privilege
Displays users on a line.	show user [all]

4 Configuring Time Range

4.1 Overview

Time Range is a time-based control service that provides some applications with time control. For example, you can configure a time range and associate it with an access control list (ACL) so that the ACL takes effect within certain time periods of a week.

4.2 Applications

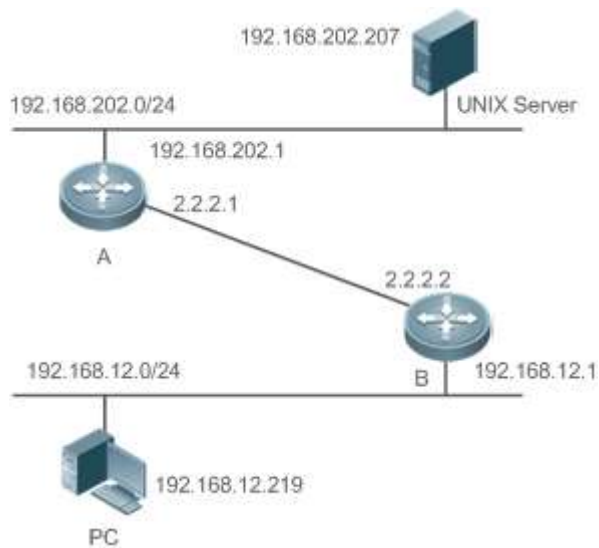
Typical Application	Scenario
Applying Time Range to an ACL	Apply a time range to an ACL module so that the time-based ACL takes effect

4.2.1 Applying Time Range to an ACL

Application Scenario

An organization allows users to access the Telnet service on a remote Unix host during working hours only, as shown in Figure 4-9.

Figure 4-9



Remarks	Configure an ACL on device B to implement the following security function: Hosts in network segment 192.168.12.0/24 can access the Telnet service on a remote Unix host during normal working hours only.
---------	--

Functional Deployment

- On device B, apply an ACL to control Telnet service access of users in network segment 192.168.12.0/24. Associate the ACL with a time range, so that the users' access to the Unix host is allowed only during working hours.

4.3 Features

Basic Concepts

↳ Absolute Time Range

The absolute time range is a time period between a start time and an end time. For example, [12:00 January 1 2000, 12:00 January 1 2001] is a typical absolute time range. When an application based on a time range is associated with the time range, a certain function can be effective within this time range.

↳ Periodic Time

Periodic time refers to a periodical interval in the time range. For example, "from 8:00 every Monday to 17:00 every Friday" is a typical periodic time interval. When a time-based application is associated with the time range, a certain function can be effective periodically from every Monday to Friday.

Features

Feature	Function
Using Absolute Time Range	Sets an absolute time range for a time-based application, so that a certain function takes effect within the absolute time range.
Using Periodic Time	Sets periodic time or a time-based application, so that a certain function takes effect within the periodic time.

4.3.1 Using Absolute Time Range

Working Principle

When a time-based application enables a certain function, it determines whether current time is within the absolute time range. If yes, the function is effective or ineffective at the current time depending on specific configuration.



4.3.2 [Using Periodic Time](#)

Working Principle

When a time-based application enables a certain function, it determines whether current time is within the period time. If yes, the function is effective or ineffective at the current time depending on specific configuration.

4.4 Configuration Details

Configuration	Description and Command
---------------	-------------------------

Configuring Time Range	 Mandatory configuration. Time range configuration is required so as to use the time range function.	
	time-range <i>time-range-name</i>	Configures a time range.
	 Optional configuration. You can configure various parameters as necessary.	
	absolute { [<i>start time date</i>] [<i>end time date</i>] }	Configures an absolute time range.
	periodic <i>day-of-the-week time to</i> [<i>day-of-the-week</i>] <i>time</i>	Configures periodic time.

4.4.1 Configuring Time Range

Configuration Effect

- Configure a time range, which may be an absolute time range or a periodic time interval, so that a time-range-based application can enable a certain function within the time range.

Configuration Method

▾ Configuring Time Range

- Mandatory configuration.
- Perform the configuration on a device to which a time range applies.

▾ Configuring Absolute Time Range

- Optional configuration.

▾ Configuring Periodic Time

- Optional configuration.

Verification

- Use the **show time-range** [*time-range-name*] command to check time range configuration information.

Related Commands

▾ Configuring Time Range

Command Syntax	time-range <i>time-range-name</i>
Parameter Description	<i>time-range-name</i> : name of the time range to be created.
Command Mode	Global configuration mode
Usage Guide	Some applications (such as ACL) may run based on time. For example, an ACL can be effective within certain time ranges of a week. To this end, first you must configure a time range, then you can configure relevant time control in time range configuration mode.

↘ Configuring Absolute Time Range

Command Syntax	absolute { [<i>start time date</i>] [<i>end time date</i>] }
Parameter Description	start time date : start time of the range. end time date : end time of the range.
Command Mode	Time range configuration mode
Usage Guide	Use the absolute command to configure a time absolute time range between a start time and an end time to allow a certain function to take effect within the absolute time range.

↘ Configuring Periodic Time

Command Syntax	periodic <i>day-of-the-week time to</i> [<i>day-of-the-week</i>] <i>time</i>
Parameter Description	<i>day-of-the-week</i> : the week day when the periodic time starts or ends <i>time</i> : the exact time when the periodic time starts or ends
Command Mode	Time range configuration mode
Usage Guide	Use the periodic command to configure a periodic time interval to allow a certain function to take effect within the periodic time.

4.5 Monitoring

Displaying

Function	Command
Displays time range configuration.	show time-range [<i>time-range-name</i>]

5 Configuring HTTP Service

5.1 Overview

Hypertext Transfer Protocol (HTTP) is used to transmit Web page information on the Internet. It is at the application layer of the TCP/IP protocol stack. The transport layer adopts connection-oriented Transmission Control Protocol (TCP).

Hypertext Transfer Protocol Secure (HTTPS) is an HTTP supporting the Secure Sockets Layer (SSL) protocol. HTTPS is mainly used to create a secure channel on an insecure network, ensure that information can hardly be intercepted, and provide certain reasonable protection against man-in-the-middle attacks. At present, HTTPS is widely used for secure and sensitive communication on the Internet, for example, electronic transactions.

Protocols and Standards

- RFC1945: Hypertext Transfer Protocol -- HTTP/1.0
- RFC2616: Hypertext Transfer Protocol -- HTTP/1.1
- RFC2818: Hypertext Transfer Protocol Over TLS -- HTTPS

5.2 Applications

Application	Description
HTTP Application Service	Users manage devices based on Web.

5.2.1 HTTP Application Service

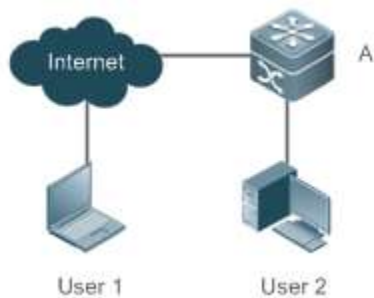
Scenario

After the HTTP service is enabled, users can access the Web management page after passing authentication by only entering **http://IP address of a device** in the browser of a PC. On the Web page, users you can monitor the device status, configure devices, upload and download files.

Take the following figure as an example to describe Web management.

- Users can remotely access devices on the Internet or configure and manage devices on the Local Area Network (LAN) by logging in to the Web server.
- According to actual conditions, users can choose to enable the HTTPS or HTTP service or enable the HTTPS and HTTP services at the same time.
- Users can also access the HTTP service of devices by setting and using HTTP/1.0 or HTTP/1.1 in the browser.

Figure 5-10



Remarks	A is a Orion Alpha A28X device. User 1 accesses the device through the Internet. User 2 accesses the device through a LAN.
----------------	--

Deployment

- When a device runs HTTP, users can access the device by entering <http://IP address of the device> in the browser of a PC.
- When a device runs HTTPS, users can access the device by entering <https://IP address of the device> in the browser of a PC.

5.3 Features

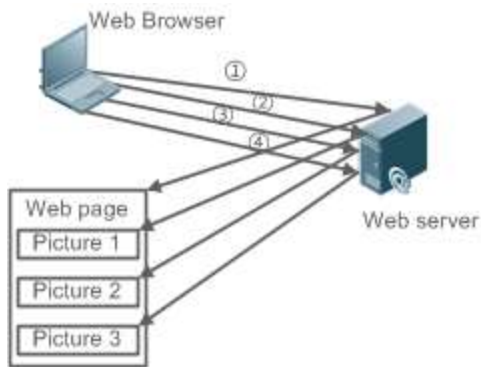
Basic Concepts

HTTP Service

The HTTP service refers to transmission of Web page information on the Internet by using HTTP. HTTP/1.0 is currently an HTTP version that is the most widely used. As one Web server may receive thousands or even millions of access requests, HTTP/1.0 adopts the short connection mode to facilitate connection management. One TCP connection is established for each request. After a request is completed, the TCP connection is released. The server does not need to record or trace previous requests. Although HTTP/1.0 simplifies connection management, HTTP/1.0 introduces performance defects.

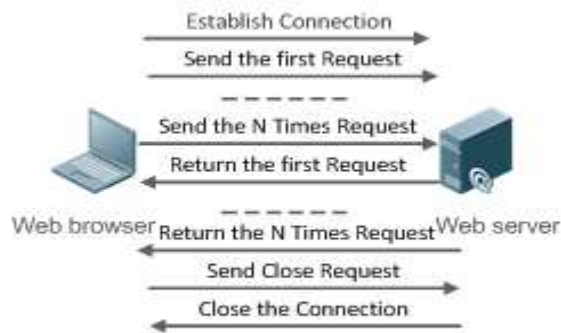
For example, a web page may need lots of pictures. However, the web page contains not real picture contents but URL connection addresses of the pictures. In this case, the browser sends multiple requests during access. Each request requires establishing an independent connection and each connection is completely isolated. Establishing and releasing connections is a relatively troublesome process, which severely affects the performance of the client and server, as shown in the following figure:

Figure 5-2



HTTP/1.1 overcomes the defect. It supports persistent connection, that is, one connection can be used to transmit multiple requests and response messages. In this way, a client can send a second request without waiting for completion of the previous request. This reduces network delay and improves performance. See the following figure:

Figure 5-3



At present, Orion Alpha A28X devices support both HTTP/1.0 and HTTP/1.1.

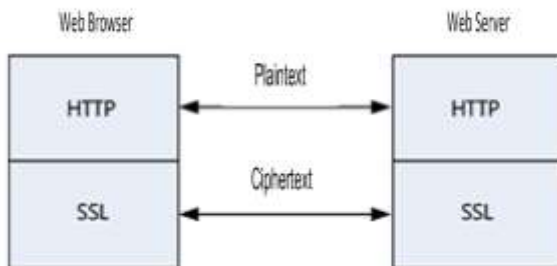
i Which HTTP version will be used by a device is decided by the Web browser.

↳ HTTPS Service

The HTTPS service adds the SSL based on the HTTP service. Its security basis is the SSL. To run HTTPS properly, a server must have a Public Key Infrastructure (PKI) certificate while a client may not necessarily need one. The SSL protocol provides the following services:

- Authenticating users and servers and ensuring that data is sent to the correct client and server.
- Encrypting data to prevent data from being stolen midway.
- Maintaining data integrity and ensuring that data is not changed during transmission.

Figure 5-4



- During a local upgrade, a device serves as an HTTP server. Users can log in to the device through a Web browser and upload upgrade files to the device to realize file upgrade on the device.

Features

Feature	Description
HTTP Service	Users log in to devices through Web pages to configure and manage devices.
Local HTTP Upgrade Service	Upgrade files are uploaded to a device to realize file upgrade on the device.

5.3.1 HTTP Service

HTTP is a service provided for Web management. Users log in to devices through Web pages to configure and manage devices.

Working Principle

Web management covers Web clients and Web servers. Similarly, the HTTP service also adopts the client/server mode. The HTTP client is embedded in the Web browser of the Web management client. It can send HTTP packets and receive HTTP response packets. The Web server (namely HTTP server) is embedded in devices. The information exchange between the client and the server is as follows:

- A TCP connection is established between the client and the server. The default port ID of the HTTP service is 80 and the default port ID of the HTTPS service is 443.
- The client sends a request message to the server.
- The server resolves the request message sent by the client. The request content includes obtaining a Web page, executing a CLI command, and uploading a file.
- After executing the request content, the server sends a response message to the client.

Related Configuration

📄 Enabling the HTTP Service

By default, the HTTP service is disabled.

The **enable service web-server** command can be used to enable HTTP service functions, including the HTTP service and HTTPS service.

The HTTP service must be enabled so that users can log in to devices through Web pages to configure and manage devices.

📌 **Configuring HTTP Authentication Information**

By default, the system creates the **admin** account. The account cannot be deleted and only the password of the account can be changed. The administrator account is the admin account, which corresponds to the level 0 permission. The administrator account owns all permissions on the Web client and can edit other management accounts and authorize the accounts to access pages. The new accounts that are added correspond to the level 1 permission.

The **webmaster level** command can be used to configure an authenticated user name and a password.

After this command is run, you need to enter the configured user name and password to log in to the Web page.

📌 **Configuring an HTTP Service Port**

By default, the HTTP service port ID is 80.

The **http port** command can be used to configure an HTTP service port ID. The value range of the port ID is 80 and 1025 to 65535.

By configuring an HTTP service port ID, you can reduce the number of attacks initiated by illegal users on the HTTP service.

📌 **Configuring an HTTPS Service Port**

By default, the HTTPS service port ID is 443.

The **http secure-port** command can be used to configure an HTTPS service port ID. The value range of the port ID is 443 and 1025 to 65535.

By configuring an HTTPS service port ID, you can reduce the number of attacks initiated by illegal users on the HTTPS service.

5.3.2 Local HTTP Upgrade Service

When a device serves as the HTTP server, users can log in to the device through a Web browser and upload upgrade files (including component package and Web package) to the device or directly upload files to the device through Trivial File Transfer Protocol (TFTP).

Working Principle

- A component package or Web package is uploaded through the local upgrade function provided by Web.
- After successfully receiving a file, the device checks the version for its validity.
- After the file check is successful, if the file is a Web package, perform the upgrade directly; if the file is a component package, decide whether to perform the upgrade in the browser by restarting the device.

Related Configuration

↘ Updating a Web Package

Run the **upgrade web download** command to download a Web package from the TFTP server.

After the command is run, download a Web package from the TFTP server. After the package passes the validity check, directly use the Web package for upgrade without restarting the device.



You can also run the **upgrade web** command to directly upgrade a Web package stored locally.

↘ Updating a Subsystem Component

By default, a device does not upgrade subsystem components uploaded through a browser or TFTP.

To upgrade a subsystem component, you must restart the device.

5.4 Configuration

Configuration	Description and Command	
Configuring the HTTP Service	 (Mandatory) It is used to enable the HTTP service.	
	enable service web-server	Enables the HTTP service.
	webmaster level	Configures HTTP authentication information.
	http port	Configures an HTTP service port.
	http secure-port	Configures an HTTPS service port.
Configuring a Local HTTP Upgrade	 (Mandatory) It is used to realize a local HTTP upgrade.	
	upgrade web	Upgrades a Web package stored on a device.
	upgrade web download	Automatically downloads a Web package from a server and automatically upgrades the package.

5.4.1 Configuring the HTTP Service

Configuration Effect

After the HTTP service is enabled on a device, users can log in to the Web management page after passing authentication and monitor the device status, configure devices, upload and download files.

Configuration Steps

↘ Enabling the HTTP Service

- Mandatory
- If there is no special requirement, enable the HTTP service on Orion Alpha A28X devices. Otherwise, the Web service is inaccessible.

↘ Configuring HTTP Authentication Information

- By default, the user name **admin** and the password **admin** are configured.
- If there is no special requirement, you can log in to the Web page by using the default user name and directly update authentication information through the Web browser. If you always use the default account, security risks may exist because unauthorized personnel can obtain device configuration information once the IP address is disclosed.

↘ **Configuring an HTTP Service Port**

- If an HTTP service port needs to be changed, the HTTP service port must be configured.
- If there is no special requirement, the default HTTP service port 80 can be used for access.

↘ **Configuring an HTTPS Service Port**

- If an HTTPS service port needs to be changed, the HTTPS service port must be configured.
- If there is no special requirement, the default HTTPS service port 443 can be used for access.

Verification

- Enter **http://IP address of the device: service port** to check whether the browser skips to the authentication page.
- Enter **https://IP address of the device: service port** to check whether the browser skips to the authentication page.



Related Commands

↘ **Enabling the HTTP Service**

Command	enable service web-server [http https all]
Parameter Description	http https all : Enables the corresponding service. http indicates enabling the HTTP service, https indicates enabling the HTTPS service, and all indicates enabling the HTTP and HTTPS services at the same time. By default, the HTTP and HTTPS services are enabled at the same time.
Command Mode	Global configuration mode.
Usage Guide	If no key word or all is put at the end of the command when the command is run, the HTTP and HTTPS services are enabled at the same time. If the key word http is put at the end of the command, only the HTTP service is enabled; if the key word https is put at the end of the command, only the HTTPS service is enabled. The no enable service web-server or default enable service web-server command is used to disable the corresponding HTTP service. If no key word is put at the end of the no enable service web-server or default enable service web-server command, the HTTP and HTTPS services are disabled.

↘ **Configuring HTTP Authentication Information.**

Command	webmaster level <i>privilege-level</i> username <i>name</i> password { <i>password</i> [0 7] <i>encrypted-password</i> }
Parameter Description	<i>privilege-level</i> : Permission level bound to a user. <i>name</i> : User name. <i>password</i> : User password. 0 7 : Password encryption type. 0: no encryption; 7: simple encryption. The default value is 0 . <i>encrypted-password</i> : Password text.
Command	Global configuration mode.

Mode	
Usage Guide	<p>When the HTTP server is used, you need to be authenticated before logging in to the Web page. The webmaster level command is used to configure a user name and a password for logging in to the Web page.</p> <p>Run the no webmaster level <i>privilege-level</i> command to delete all user names and passwords of the specified permission level.</p> <p>Run the no webmaster level <i>privilege-level</i> username <i>name</i> command to delete the specified user name and password.</p> <hr/> <p> User names and passwords involve three permission levels: Up to 10 user names and passwords can be configured for each permission level.</p> <p> By default, the system creates the admin account. The account cannot be deleted and only the password of the account can be changed. The administrator account is the admin account, which corresponds to the level 0 permission. The administrator account owns all permissions on the Web client and can edit other management accounts and authorize the accounts to access pages. The new accounts that are added correspond to the level 1 permission.</p>

📌 [Configuring an HTTP Service Port](#)

Command	http port <i>port-number</i>
Parameter Description	<i>port-number</i> : Configures an HTTP service port. The value range is 80 and 1025 to 65535.
Command Mode	Global configuration mode.
Usage Guide	Run the command to set an HTTP service port.


📌 [Configuring an HTTPS Service Port](#)

Command	http secure-port <i>port-number</i>
Parameter Description	<i>port-number</i> : Configures an HTTPS service port. The value range is 443 and 1025 to 65535.
Command Mode	Global configuration mode.
Usage Guide	Run the command to set an HTTPS service port.

Configuration Example

📌 [Managing one Orion Alpha A28X Device by Using Web and Logging in to the Device through a Web Browser to Configure Related Functions](#)

- Log in to the device by using the **admin** account configured by default.
- To improve security, the Web browser is required to support both HTTP and HTTPS for access.
- The user is required to configure an HTTP service port to reduce the number of attacks initiated by illegal users on HTTP.

Scenario Figure 5-5	
Configuration Steps	<ul style="list-style-type: none"> ● Enable the HTTP and HTTPS services at the same time. ● Set the HTTP service port ID to 8080 and the HTTPS service port ID to 4430.
A	<pre>A#configure terminal A(config)# enable service web-server A(config)# http port 8080 A(config)# http secure-port 4430</pre>
Verification	Check HTTP configurations.
A	<pre>A# show web-server status http server status: enabled http server port: 8080 https server status:enabled https server port: 4430</pre>

Common Errors

- If the HTTP service port is not the default port 80 or 443, you must enter a specific configured service port in the browser. Otherwise, you cannot access devices on the Web client.

5.4.2 Configuring a Local HTTP Upgrade

Configuration Effect

Perform an HTTP upgrade through the browser or the **upgrade web** command.

Notes

- So long as a Web package is uploaded successfully and passes the version check, the device directly performs an upgrade based on the latest Web package.
- The **upgrade web download** command is used to automatically download files from the TFTP server and automatically perform an upgrade.
- The **upgrade web** command is used to automatically upgrade the Web package in the local file system.

Configuration Steps

N/A

Verification

- Access and view the latest Web page through the browser.

Related Commands

Downloading a Web Package from the TFTP Server


Command	upgrade download tftp: <i>path</i>
Parameter Description	tftp: Connects the TFTP server through a common data port and downloads a Web package. path: Path of a Web package on the TFTP server.
Command Mode	Privileged EXEC mode
Usage Guide	This command is used to download a Web package from the TFTP server and automatically perform an upgrade.

Upgrading a Web Package Stored on a Local Device


Command	upgrade web <i>uri</i>
Parameter Description	uri: Local path for storing a Web package.
Command Mode	Privileged EXEC mode
Usage Guide	This command is used to upgrade a Web package stored on a device and automatically perform an upgrade.

Configuration Example


Obtaining the Latest Web Package from the Official Website and Running the Web Package

Scenario Figure 5-6	
Configuration Steps	<ul style="list-style-type: none"> ● Connect to a local PC whose IP address is 10.10.10.13 and assign an IP address 10.10.10.131 in the same network segment to the device. ● Log in to the device through Web and upload the latest Web package to the device.
A	<pre>A#configure terminal A(config)# vlan 1 A(config-vlan)# exit A(config)# interface vlan 1 A(config-VLAN 1)# ip address 10.10.10.131 255.255.255.0 A(config-VLAN 1)# exit A(config)# enable service web-server</pre>
	On a PC, use the local upgrade function on the Web page to upload a Web package for upgrade.
Verification	On the PC, log in to the device through Web again and check whether the latest Web page is displayed.

↘ Upgrading a Web Package by Running the upgrade web download Command

Scenario Figure 5-7	
Configuration Steps	<ul style="list-style-type: none"> ● Connect to a local PC whose IP address is 10.10.10.13 and assign an IP address 10.10.10.131 in the same network segment to the device. ● Start the TFTP server.
A	<pre>A#configure terminal A(config)# vlan 1 A(config-vlan)# exit A(config)# interface vlan 1 A(config-VLAN 1)# ip address 10.10.10.131 255.255.255.0 A(config-VLAN 1)# end A#upgrade web download tftp:// 10.10.10.13/web.upd Press Ctrl+C to quit !!!!!!!!!! download 3896704 bytes Begin to upgrade the web package... Web package upgrade successfully.</pre>
Verification	<p>On the PC, log in to the device through Web again and check whether the latest Web page is displayed.</p>

↘ Upgrading a Web Package by Running the upgrade web Command

Scenario Figure 5-8	
Configuration Steps	<ul style="list-style-type: none"> ● Connect to a local PC whose IP address is 10.10.10.13 and assign an IP address 10.10.10.131 in the same network segment to the device. ● Start the TFTP server.
A	<pre>A#configure terminal A(config)# vlan 1 A(config-vlan)# exit A(config)# interface vlan 1 A(config-VLAN 1)# ip address 10.10.10.131 255.255.255.0 A(config-VLAN 1)# end</pre>

	<pre> A#copy tftp://10.10.10.13/web.upd flash:/web.upd Press Ctrl+C to quit !!!!!!! Accessing tftp:// 10.10.10.13/web.upd finished, 3896704 bytes prepared Flushing data to flash:/web.upd.. Flush data done A #upgrade web flash:/web.upd Web package upgrade successfully. A # </pre>
Verification	On the PC, log in to the device through Web again and check whether the latest Web page is displayed.

Common Errors

- Access to the web page through the browser shows that the web page is not updated based on the latest Web package. This is possibly because the local browser has a cache. Clear the cache of the local browser and access the Web page again.

5.5 Monitoring

Displaying

Description	Command
Displays the configuration and status of the Web service.	show web-server status

6 Configuring Syslog

6.1 Overview

Status changes (such as link up and down) or abnormal events may occur anytime. Orion Alpha A28X products provide the syslog mechanism to automatically generate messages (log packets) in fixed format upon status changes or occurrence of events. These messages are displayed on the related windows such as the Console or monitoring terminal, recorded on media such as the memory buffer or log files, or sent to a group of log servers on the network so that the administrator can analyze network performance and identify faults based on these log packets. Log packets can be added with the timestamps and sequence numbers and classified by severity level so that the administrator can conveniently read and manage log packets.

Protocols and Standards

- RFC3164: The BSD syslog Protocol
- RFC5424: The_Syslog_Protocol

6.2 Applications

Application	Description
Sending Syslogs to the Console	Monitor syslogs through the Console.
Sending Syslogs to the Log Server	Monitor syslogs through the server.

6.2.1 Sending Syslogs to the Console

Scenario

Send syslogs to the Console to facilitate the administrator to monitor the performance of the system. The requirements are as follows:

1. Send logs of Level 6 or higher to the Console.
2. Send logs of only the ARP and IP modules to the Console.

Figure 6-11 shows the network topology.

Figure 6-11 Network topology



Deployment

Configure the device as follows:

1. Set the level of logs that can be sent to the Console to informational (Level 6).
2. Set the filtering direction of logs to terminal.
3. Set log filtering mode of logs to contains-only.
4. Set the filtering rule of logs to single-match. The module name contains only ARP or IP.

6.2.2 Sending Syslogs to the Log Server

Scenario

Send syslogs to the log server to facilitate the administrator to monitor the logs of devices on the server. The requirements are as follows:

1. Send syslogs to the log server 10.1.1.1.
2. Send logs of Level 7 or higher to the log server.
3. Send syslogs from the source interface Loopback 0 to the log server.

Figure 6-12 shows the network topology.

Figure 6-12 Network topology



Deployment

Configure the device as follows:

1. Set the IPv4 address of the server to 10.1.1.1.
2. Set the level of logs that can be sent to the log server to debugging (Level 7).
3. Set the source interface of logs sent to the log server to Loopback 0.

6.3 Features

Basic Concepts

↘ Classification of Syslogs

Syslogs can be classified into two types:

- Log type
- Debug type

↘ Levels of Syslogs

Eight severity levels of syslogs are defined in descending order, including emergency, alert, critical, error, warning, notification, informational, and debugging. These levels correspond to eight numerical values from 0 to 7. A smaller value indicates a higher level.

Only logs with a level equaling to or higher than the specified level can be output. For example, if the level of logs is set to informational (Level 6), logs of Level 6 or higher will be output.

The following table describes the log levels.

Level	Numerical Value	Description
emergencies	0	Indicates that the system cannot run normally.
alerts	1	Indicates that the measures must be taken immediately.
critical	2	Indicates a critical condition.
errors	3	Indicates an error.
warnings	4	Indicates a warning.
notifications	5	Indicates a notification message that requires attention.
informational	6	Indicates an informational message.
debugging	7	Indicates a debugging message.

↘ Output Direction of Syslogs

Output directions of syslogs include Console, monitor, server, buffer, and file. The default level and type of logs vary with the output direction. You can customize filtering rules for different output directions.

The following table describes output directions of syslogs.

Output Direction	Description	Default Output Level	Description
Console	Console	Debugging (Level 7)	Logs and debugging information are output.
monitor	Monitoring terminal	Debugging (Level 7)	Logs and debugging information are output.
server	Log server	Informational (Level 6)	Logs and debugging information are output.
buffer	Log buffer	Debugging (Level 7)	Logs and debugging information are output. The log buffer is used to store syslogs.
file	Log file	Informational (Level 6)	Logs and debugging information are output. Logs in the log buffer are periodically written into files.

↘ RFC3164 Log Format

Formats of syslogs may vary with the syslog output direction.

- If the output direction is the Console, monitor, buffer, or file, the syslog format is as follows:

```
seq no: *timestamp: sysname %module-level-mnemonic: content
```

For example, if you exit configuration mode, the following log is displayed on the Console:

```
001233: *May 22 09:44:36: Orion Alpha A28X %SYS-5-CONFIG_I: Configured from console by console
```

- If the output direction is the log server, the syslog format is as follows:

```
<priority>seq no: *timestamp: sysname %module-level-mnemonic: content
```

For example, if you exit configuration mode, the following log is displayed on the log server:

<189>001233: *May 22 09:44:36: Orion Alpha A28X %SYS-5-CONFIG_I: Configured from console by console

The following describes each field in the log in details:

10. Priority

This field is valid only when logs are sent to the log server.

The priority is calculated using the following formula: Facility x 8 + Level. Level indicates the numerical code of the log level and Facility indicates the numerical code of the facility. The default facility value is local7 (23). The following table lists the value range of the facility.


Numerical Code	Facility Keyword	Facility Description
0	kern	kernel messages
1	user	user-level messages
2	mail	mail system
3	daemon	system daemons
4	auth1	security/authorization messages
5	syslog	messages generated internally by syslogs
6	lpr	line printer subsystem
7	news	network news subsystem
8	uucp	UUCP subsystem
9	clock1	clock daemon
10	auth2	security/authorization messages
11	ftp	FTP daemon
12	ntp	NTP subsystem
13	logaudit	log audit
14	logalert	log alert
15	clock2	clock daemon
16	local0	local use 0 (local0)
17	local1	local use 1 (local1)
18	local2	local use 2 (local2)
19	local3	local use 3 (local3)
20	local4	local use 4 (local4)
21	local5	local use 5 (local5)
22	local6	local use 6 (local6)
23	local7	local use 7 (local7)

11. Sequence Number

The sequence number of a syslog is a 6-digit integer, and increases sequentially. By default, the sequence number is not displayed. You can run a command to display or hide this field.

12. Timestamp

The timestamp records the time when a syslog is generated so that you can display and check the system event conveniently. Orion Alpha A28X devices support two syslog timestamp formats: datetime and uptime.

 If the device does not have the real time clock (RTC), which is used to record the system absolute time, the device uses its startup time (uptime) as the syslog timestamp by default. If the device has the RTC, the device uses its absolute time (datetime) as the syslog timestamp by default.

The two timestamp formats are described as follows:

- Datetime format

The datetime format is as follows:

```
Mmm dd yyyy hh:mm:ss.msec
```

The following table describes each parameter of the datetime.

Timestamp Parameter	Parameter Name	Description
Mmm	Month	Mmm refers to abbreviation of the current month. The 12 months in a year are written as Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec.
dd	Day	dd indicates the current date.
yyyy	Year	yyyy indicates the current year, and is not displayed by default.
hh	Hour	hh indicates the current hour.
mm	Minute	mm indicates the current minute.
ss	Second	ss indicates the current second.
msec	Millisecond	msec indicates the current millisecond.

By default, the datetime timestamp displayed in the syslog does not contain the year and millisecond. You can run a command to display or hide the year and millisecond of the datetime timestamp.

- Uptime format

The uptime format is as follows:

```
dd:hh:mm:ss
```

The timestamp string indicates the accumulated days, hours, minutes, and seconds since the system is started.

13. Sysname

This field indicates the name of the device that generates the log so that the log server can identify the host that sends the log. By default, this field is not displayed. You can run a command to display or hide this field.

14. Module

This field indicates the name of the module that generates the log. The module name is an upper-case string of 2 to 20 characters, which contain upper-case letters, digits, or underscores. The module field is mandatory in the log-type information, and optional in the debug-type information.

15. Level

Eight syslog levels from 0 to 7 are defined. The level of syslogs generated by each module is fixed and cannot be modified.

16. Mnemonic

This field indicates the brief information about the log. The mnemonic is an upper-case string of 4 to 32 characters, which may include upper-case letters, digits, or underscore. The mnemonic field is mandatory in the log-type information, and optional in the debug-type information.

17. Content

This field indicates the detailed content of the syslog.

📄 RFC5424 Log Format

The syslog format in the output direction is as follows:

```
<priority>version timestamp sysname MODULE LEVEL MNEMONIC [structured-data] description
```

For example, if you exit configuration mode, the following log is displayed on the Console:

```
<133>1 2013-07-24T12:19:33.130290Z Orion Alpha A28X SYS 5 CONFIG - Configured from console by console
```

The following describes each field in the log in details:

18. Priority

The priority is calculated using the following formula: Facility x 8 + Level. Level indicates the numerical code of the log level and Facility indicates the numerical code of the facility. When the RFC5424 format is enabled, the default value of the facility field is local0 (16).

19. Version

According to RFC5424, the version is always 1.

20. Timestamp

The timestamp records the time when a syslog is generated so that you can display and check the system event conveniently. Orion Alpha A28X devices use the following uniformed timestamp format when the RFC5424 logging function is enabled:

```
YYYY-MM-DDTHH:MM:SS.SECFRACZ
```

The following table describes each parameter of the timestamp.

Timestamp Parameter	Description	Remark
YYYY	Year	YYYY indicates the current year.
MM	Month	MM indicates the current month.
DD	Day	DD indicates the current date.
T	Separator	The date must end with "T".
HH	Hour	HH indicates the current hour.
MM	Minute	MM indicates the current minute.
SS	Second	SS indicates the current second.
SECFRAC	Millisecond	SECFRAC indicates the current millisecond (1–6 digits).
Z	End mark	The time must end with "Z".

21. Sysname

This field indicates the name of the device that generates the log so that the log server can identify the host that sends the log.

22. Module

This field indicates the name of the module that generates the log. The module name is an upper-case string of 2 to 20 characters, which contain upper-case letters, digits, or underscores. The module field is mandatory in the log-type information, and optional in the debug-type information.

23. Level

Eight syslog levels from 0 to 7 are defined. The level of syslogs generated by each module is fixed and cannot be modified.

24. Mnemonic

This field indicates the brief information about the log. The mnemonic is an upper-case string of 4 to 32 characters, which contain upper-case letters, digits, or underscores. The Mnemonic field is mandatory in the log-type information, and optional in the debug-type information.

25. Structured-Data

Structured-data introduced in RFC5424 is parsed as a whole string containing parameter information. Each log may contain 0 or multiple parameters. If a parameter is null, replace this parameter with a placeholder (-). The format of this field is as follows:

```
[SD_ID@enterpriseID PARAM-NAME=PARAM-VALUE]
```

The following table describes each parameter of the structured-data field.

Parameter in structured-data	Description	Remarks
SD_ID	Parameter information name	The parameter information name is capitalized, and must be unique in a log.
@	Separator	"@enterpriseID" is added only to the customized parameter information, not to the parameter information defined in RFC5424.
enterpriseID	Enterprise ID	The enterprise ID is maintained by the Internet Assigned Numbers Authority (IANA). Orion Alpha A28X Networks' enterprise ID is 4881. You can query the enterprise ID on the official website of IANA. http://www.iana.org/assignments/enterprise-numbers
PARAM-NAME	Parameter name	The parameter name is capitalized, and must be unique in the structured-data of a log.
PARAM-VALUE	Parameter value	The parameter value must be enclosed in double quotation marks. Values of the IP address or MAC address must be capitalized, and other types of values are capitalized as required.

26. description

This field indicates the content of the syslog.

Overview

Feature	Description
Logging	Enable or disable the system logging functions.
Syslog Format	Configure the syslog format.

Logging Direction	Configure the parameters to send syslogs in different directions.
Syslog Filtering	Configure parameters of the syslog filtering function.
Featured Logging	Configure parameters of the featured logging function.
Syslog Monitoring	Configure parameters of the syslog monitoring function.

6.3.1 Logging

Enable or disable the logging, log redirection, and log statistics functions.

Related Configuration

↘ Enable Logging

By default, logging is enabled.

Run the **logging on** command to enable logging in global configuration mode. After logging is enabled, logs generated by the system are sent in various directions for the administrator to monitor the performance of the system.

↘ Enabling Log Redirection

By default, log redirection is enabled on the Virtual Switching Unit (VSU).

Run the **logging rd on** command to enable log redirection in global configuration mode. After log redirection is enabled, logs generated by the standby device or standby supervisor module are redirected to the active device or active supervisor module on the VSU to facilitate the administrator to manage logs.

↘ Enabling Log Statistics

By default, log statistics is disabled.

Run the **logging count** command to enable log statistics in global configuration mode. After log statistics is enabled, the system records the number of times a log is generated and the last time when the log is generated.

6.3.2 Syslog Format

Configure the syslog format, including the RFC5424 log format, timestamp format, sysname, and sequence number.

Related Configuration

↘ Enabling the RFC5424 Log Format

By default, the RFC5424 log format is disabled.

After the new format (RFC5424 log format) is enabled, the **service sequence-numbers**, **service sysname**, **service timestamps**, **service private-syslog**, and **service standard-syslog** that are applicable only to the old format (RFC3164 log format) lose effect and are hidden.

After the old format (RFC3164 log format) is enabled, the **logging delay-send**, **logging policy**, and **logging statistic** commands that are applicable only to the RFC5424 log format lose effect and are hidden.

After log format switchover, the outputs of the **show logging** and **show logging config** commands change accordingly.

↘ Configuring the Timestamp Format

By default, the syslog uses the datetime timestamp format, and the timestamp does not contain the year and millisecond.

Run the **service timestamps** command in global configuration mode to use the datetime timestamp format that contains the year and millisecond in the syslog, or change the datetime format to the uptime format.

↘ Adding Sysname to the Syslog

By default, the syslog does not contain sysname.

Run the **service sysname** command in global configuration mode to add sysname to the syslog.

↘ Adding the Sequence Number to the Syslog

By default, the syslog does not contain the sequence number.

Run the **service sequence-numbers** command in global configuration mode to add the sequence number to the syslog.

↘ Enabling the Standard Log Format

By default, logs are displayed in the following format:

```
*timestamp: %module-level-mnemonic: content
```

Run the **service standard-syslog** command in global configuration mode to enable the standard log format and logs are displayed in the following format:

```
timestamp %module-level-mnemonic: content
```

Compared with the default log format, an asterisk (*) is missing in front of the timestamp, and a colon (:) is missing at the end of the timestamp in the standard log format.

↘ Enabling the Private Log Format

By default, logs are displayed in the following format:

```
*timestamp: %module-level-mnemonic: content
```

Run the **service private-syslog** command in global configuration mode to enable the private log format and logs are displayed in the following format:

```
timestamp module-level-mnemonic: content
```

Compared with the default log format, an asterisk (*) is missing in front of the timestamp, a colon (:) is missing at the end of the timestamp, and a percent sign (%) is missing at the end of the module name in the private log format.

6.3.3 Logging Direction

Configure parameters for sending syslogs in different directions, including the Console, monitor terminal, buffer, the log server, and log files.

Related Configuration

↘ Synchronizing User Input with Log Output

By default, this function is disabled.

Run the **logging synchronous** command in line configuration mode to synchronize user input with log output. After this function is enabled, user input will not be interrupted.

↘ **Configuring the Log Rate Limit**

By default, no log rate limit is configured.

Run the **logging rate-limit** { *number* | **all** *number* | **console** {*number* | **all** *number* } } [**except** [*severity*]] command in global configuration mode to configure the log rate limit.

↘ **Configuring the Log Redirection Rate Limit**

By default, a maximum of 200 logs are redirected from the standby device to the active device of VSU per second.

Run the **logging rd rate-limit** *number* [**except** *severity*] command in global configuration mode to configure the log redirection rate limit, that is, the maximum number of logs that are redirected from the standby device to the active device or from the standby supervisor module to the active supervisor module per second.

↘ **Configuring the Level of Logs Sent to the Console**

By default, the level of logs sent to the Console is debugging (Level 7).

Run the **logging console** [*level*] command in global configuration mode to configure the level of logs that can be sent to the Console.

↘ **Sending Logs to the Monitor Terminal**

By default, it is not allowed to send logs to the monitor terminal.

Run the **terminal monitor** command in the privileged EXEC mode to send logs to the monitor terminal.

↘ **Configuring the Level of Logs Sent to the Monitor Terminal**

By default, the level of logs sent to the monitor terminal is debugging (Level 7).

Run the **logging monitor** [*level*] command in global configuration mode to configure the level of logs that can be sent to the monitor terminal.

↘ **Writing Logs into the Memory Buffer**

By default, logs are written into the memory buffer, and the default level of logs is debugging (Level 7).

Run the **logging buffered** [*buffer-size*] [*level*] command in global configuration mode to configure parameters for writing logs into the memory buffer, including the buffer size and log level.

↘ **Sending Logs to the Log Server**

By default, logs are not sent to the log server.

Run the **logging server** { *ip-address* | **ipv6** *ipv6-address* } [**udp-port** *port*] command in global configuration mode to send logs to a specified log server.

↘ **Configuring the Level of Logs Sent to the Log Server**

By default, the level of logs sent to the log server is informational (Level 6).

Run the **logging trap** [*level*] command in global configuration mode to configure the level of logs that can be sent to the log server.

↘ **Configuring the Facility Value of Logs Sent to the Log Server**

If the RFC5424 log format is disabled, the facility value of logs sent to the log server is local7 (23) by default. If the RFC5424 log format is enabled, the facility value of logs sent to the log server is local0 (16) by default.

Run the **logging facility** *facility-type* command in global configuration mode to configure the facility value of logs sent to the log server.

↘ **Configuring the Source Address of Logs Sent to the Log Server**

By default, the source address of logs sent to the log server is the IP address of the interface sending logs.

Run the **logging source** [**interface**] *interface-type interface-number* command to configure the source interface of logs. If this source interface is not configured, or the IP address is not configured for this source interface, the source address of logs is the IP address of the interface sending logs.

Run the **logging source** { **ip** *ip-address* | **ipv6** *ipv6-address* } command to configure the source IP address of logs. If this IP address is not configured on the device, the source address of logs is the IP address of the interface sending logs.

↘ **Writing Logs into Log Files**

By default, logs are not written into log files. After the function of writing logs into log files is enabled, the level of logs written into log files is informational (Level 6) by default.

Run the **logging file** {**flash:filename** } [*max-file-size*] [*level*] command in global configuration mode to configure parameters for writing logs into log files, including the type of device where the file is stored, file name, file size, and log level.

↘ **Configuring the Number of Log Files**

By default, the number of log files is 16.

Run the **logging file numbers** *numbers* command in global configuration mode to configure the number of log files.

↘ **Configuring the Interval at Which Logs Are Written into Log Files**

By default, logs are written into log files at the interval of 3600s (one hour).

Run the **logging flash interval** *seconds* command in global configuration mode to configure the interval at which logs are written into log files.

↘ **Configuring the Storage Time of Log Files**

By default, the storage time is not configured.

Run the **logging life-time level** *level days* command in global configuration mode to configure the storage time of logs. The administrator can specify different storage days for logs of different levels.

↘ **Immediately Writing Logs in the Buffer into Log Files**

By default, syslogs are stored in the syslog buffer and then written into log files periodically or when the buffer is full.

Run the **logging flash flush** command in global configuration mode to immediately write logs in the buffer into log files so that you can collect logs conveniently.

6.3.4 Syslog Filtering

By default, logs generated by the system are sent in all directions.

Working Principle

↘ Filtering Direction

Five log filtering directions are defined:

- **buffer**: Filters out logs sent to the log buffer, that is, logs displayed by the **show logging** command.
- **file**: Filters out logs written into log files.
- **server**: Filters out logs sent to the log server.
- **terminal**: Filters out logs sent to the Console and monitor terminal (including Telnet and SSH).

The four filtering directions can be used either in combinations to filter out logs sent in various directions, or separately to filter out logs sent in a single direction.

↘ Filtering Mode

Two filtering modes are available:

- **contains-only**: Indicates that only logs that contain keywords specified in the filtering rules are output. You may be interested in only a specified type of logs. In this case, you can apply the contains-only mode on the device to display only logs that match filtering rules on the terminal, helping you check whether any event occurs.
- **filter-only**: Indicates that logs that contain keywords specified in the filtering rules are filtered out and will not be output. If a module generates too many logs, spamming may occur on the terminal interface. If you do not care about this type of logs, you can apply the filter-only mode and configure related filtering rules to filter out logs that may cause spamming.

The two filtering modes are mutually exclusive, that is, you can configure only one filtering mode at a time.

↘ Filter Rule

Two filtering rules are available:

- **exact-match**: If exact-match is selected, you must select all the three filtering options (module, level, and mnemonic). If you want to filter out a specified log, use the exact-match filtering rule.
- **single-match**: If exact-match is selected, you only need to select one of the three filtering options (module, level, and mnemonic). If you want to filter out a specified type of logs, use the single-match filtering rule.

If the same module, level, or mnemonic is configured in both the single-match and exact-match rules, the single-match rule prevails over the exact-match rule.

Related Configuration

↘ Configuring the Log Filtering Direction

By default, the log filtering direction is all, that is, logs sent in all directions are filtered.

Run the **logging filter direction { all | buffer | file | server | terminal }** command in global configuration mode to configure the log filtering direction to filter out logs in the specified directions.

↘ Configuring the Log Filtering Mode

By default, the log filtering mode is filter-only.

Run the **logging filter type** { **contains-only** | **filter-only** } command in global configuration mode to configure the log filtering mode.

↘ Configuring the Log Filtering Rule

By default, no log filtering rule is configured on a device, that is, logs are not filtered out.

Run the **logging filter rule exact-match module** *module-name mnemonic mnemonic-name level level* command in global configuration mode to configure the exact-match rule.

Run the **logging filter rule single-match** { **level** *level* | **mnemonic** *mnemonic-name* | **module** *module-name* } command in global configuration mode to configure the single-match rule.

6.3.5 Featured Logging

The featured logging functions include level-based logging, delayed logging, and periodical logging. If the RFC5424 log format is enabled, logs can be sent in all directions, delayed logging is enabled, and periodical logging is disabled by default. If the RFC5424 log format is disabled, level-based logging, delayed logging, and periodical logging are disabled.

Working Principle

↘ Level-based Logging

You can use the level-based logging function to send syslogs to different destinations based on different module and severity level. For example, you can configure commands to send WLAN module logs of Level 4 or lower to the log server, and WLAN module logs of Level 5 or higher to local log files.

↘ Delayed Logging

After generated, logs are not directly sent to the log server, and instead they are buffered in the log file. The device sends the log file to the syslog server through FTP at a certain interval. This function is called delayed logging.

If the device generates too many logs, sending all logs to the server in real time may deteriorate the performance of the device and the syslog server, and increase the burden of the network. In this case, the delayed logging function can be used to reduce the packet interaction.

By default, the log file sent to the remote server is named **File size_Device IP address_Index.txt**. If the prefix of the log file name is modified, the log file sent to the remote server is named **Configured file name prefix_File size_Device IP address_Index.txt**. The file stored on the local Flash of the device is named **Configured file name prefix_Index.txt**. By default, the file name prefix is `syslog_ftp_server`, the delayed logging interval is 3600s (one hour), and the log file size is 128 KB.

The maximum value of the delayed logging interval is 65535s, that is, 18 hours. If you set the delayed logging interval to the maximum value, the amount of logs generated in this period may exceed the file size (128 KB). To prevent loss of logs, logs will be written into a new log file, and the index increases by 1. When the timer expires, all log files buffered in this period will be sent to the FTP or TFTP server at a time.

The Flash on the device that is used to buffer the local log files is limited in size. A maximum of eight log files can be buffered on the device. If the number of local log files exceeds eight before the timer expires, all log files that are generated earlier will be sent to the FTP or TFTP server at a time.

↘ Periodical Logging

Logs about performance statistics are periodically sent. All periodical logging timers are managed by the syslog module. When the timer expires, the syslog module calls the log processing function registered with each module to output the performance statistic logs and send logs in real time to the remote syslog server. The server analyzes these logs to evaluate the device performance.

By default, the periodical logging interval is 15 minutes. To enable the server to collect all performance statistic logs at a time, you need to set the log periodical logging intervals of different statistic objects to a common multiple of them. Currently, the interval can be set to 0, 15, 30, 60, or 120. 0 indicates that periodical logging is disabled.

Related Configuration

↘ Configuring the Level-based Logging Policy

By default, device logs are sent in all directions.

Run the **logging policy module** *module-name* [**not-lesser-than**] *level* **direction** { **all** | **server** | **file** | **console** | **monitor** | **buffer** } command in global configuration mode to configure the level-based logging policy.

↘ Enabling Delayed Display of Logs on the Console and Remote Terminal

By default, delayed display of logs on the Console and remote terminal is disabled.

Run the **logging delay-send terminal** command in global configuration mode to enable delayed display of logs on the Console and remote terminal.

↘ Configuring the Name of the File for Delayed Logging

By default, the log file sent to the remote server is named **File size_Device IP address_Index.txt**. If the prefix of the log file name is modified, the log file sent to the remote server is named **Configured file name prefix_File size_Device IP address_Index.txt**. The file stored on the local Flash of the device is named **Configured file name prefix_Index.txt**. The default file name prefix is `syslog_ftp_server`.

Run the **logging delay-send file flash:filename** command in global configuration mode to configure the name of the log file that is buffered on the local device.

↘ Configuring the Delayed Logging Interval

By default, the delayed logging interval is 3600s (one hour).

Run the **logging delay-send interval seconds** command in global configuration mode to configure the delayed logging interval.

↘ Configuring the Server Address and Delayed Logging Mode

By default, logs are not sent to any FTP or TFTP server.

Run the **logging delay-send server** { *ip-address* | **ipv6** *ipv6-address* } **mode** { **ftp user** *username* **password** [**0** | **7**] *password* | **fttp** } command in global configuration mode to configure the server address and delayed logging mode.

↳ Enabling Periodical Logging

By default, periodical logging is disabled.

Run the **logging statistic enable** command in global configuration mode to enable periodical uploading of logs. After this function is enabled, the system outputs a series of performance statistics at a certain interval so that the log server can monitor the system performance.

↳ Enabling Periodical Display of Logs on the Console and Remote Terminal

By default, periodical display of logs on the Console and remote terminal is disabled.

Run the **logging statistic terminal** command in global configuration mode to enable periodical display of logs on the Console and remote terminal.

↳ Configuring the Periodical Logging Interval

By default, the periodical logging interval is 15 minutes.

Run the **logging statistic mnemonic *mnemonic* interval *minutes*** command in global configuration mode to configure the periodical logging interval.

6.3.6 Syslog Monitoring

After syslog monitoring is enabled, the system monitors the access attempts of users and generates the related logs.

Working Principle

After logging of login/exit attempts is enabled, the system records the access attempts of users. The log contains user name and source address.

After logging of operations is enabled, the system records changes in device configurations, The log contains user name, source address, and operation.

Related Configuration

↳ Enabling Logging of Login or Exit Attempts

By default, a device does not generate logs when users access or exit the device.






Run the **logging userinfo** command in global configuration mode to enable logging of login/exit attempts. After this function is enabled, the device displays logs when users access the devices through Telnet, SSH, or HTTP so that the administrator can monitor the device connections.






↳ Enabling Logging of Operations




By default, a device does not generate logs when users modify device configurations.

Run the **logging userinfo command-log** command in global configuration mode to enable logging of operations. After this function is enabled, the system displays related logs to notify the administrator of configuration changes.

6.4 Configuration

Configuration	Description and Command	
Configuring Syslog Format	 (Optional) It is used to configure the syslog format.	
	service timestamps [<i>message-type</i> [<i>uptime</i> <i>datetime</i> [<i>msec</i>] [<i>year</i>]]]	Configures the timestamp format of syslogs.
	service sysname	Adds the sysname to the syslog.
	service sequence-numbers	Adds the sequence number to the syslog.
	service standard-syslog	Enables the standard syslog format.
	service private-syslog	Enables the private syslog format.
	service log-format rfc5424	Enables the RFC5424 syslog format.
Sending Syslogs to the Console	 (Optional) It is used to configure parameters for sending syslogs to the Console.	
	logging on	Enables logging.
	logging count	Enables log statistics.
	logging console [<i>level</i>]	Configures the level of logs displayed on the Console.
	logging rate-limit { <i>number</i> all <i>number</i> console { <i>number</i> all <i>number</i> } } [except [<i>severity</i>]]	Configures the log rate limit.
Sending Syslogs to the Monitor Terminal	 (Optional) It is used to configure parameters for sending syslogs to the monitor terminal.	
	terminal monitor	Enables the monitor terminal to display logs.
	logging monitor [<i>level</i>]	Configures the level of logs displayed on the monitor terminal.
Writing Syslogs into the Memory Buffer	 (Optional) It is used to configure parameters for writing syslogs into the memory buffer.	
	logging buffered [<i>buffer-size</i>] [<i>level</i>]	Configures parameters for writing syslogs into the memory buffer, including the buffer size and log level.
Sending Syslogs to the Log Server	 (Optional) It is used to configure parameters for sending syslogs to the log server.	
	logging server { <i>ip-address</i> ipv6 <i>ipv6-address</i> } [udp-port <i>port</i>]	Sends logs to a specified log server.
	logging trap [<i>level</i>]	Configures the level of logs sent to the log server.
	logging facility <i>facility-type</i>	Configures the facility value of logs sent to the log server.
	logging source [interface] <i>interface-type</i> <i>interface-number</i>	Configures the source interface of logs sent to the log server.
logging source { ip <i>ip-address</i> ipv6 <i>ipv6-address</i> }	Configures the source address of logs sent to the log server.	

Configuration	Description and Command	
Writing Syslogs into Log Files	 (Optional) It is used to configure parameters for writing syslogs into a file.	
	logging file { flash:filename } [<i>max-file-size</i>] [<i>level</i>]	Configures parameters for writing syslogs into a file, including the file storage type, file name, file size, and log level.
	logging file numbers <i>numbers</i>	Configures the number of files which logs are written into. The default value is 16.
	logging flash interval <i>seconds</i>	Configures the interval at which logs are written into log files. The default value is 3600.
	logging life-time level <i>level days</i>	Configures the storage time of log files.
Configuring Syslog Filtering	 (Optional) It is used to enable the syslog filtering function.	
	logging filter direction { all buffer file server terminal }	Configures the log filtering direction.
	logging filter type { contains-only filter-only }	Configures the log filtering mode.
	logging filter rule exact-match module <i>module-name mnemonic mnemonic-name level level</i>	Configures the exact-match filtering rule.
	logging filter rule single-match { level <i>level</i> mnemonic <i>mnemonic-name</i> module <i>module-name</i> }	Configures the single-match filtering rule.
Configuring Level-based Logging	 (Optional) It is used to configure logging policies to send the syslogs based on module and severity level .	
	logging policy module <i>module-name</i> [not-lesser-than] <i>level</i> direction { all server file console monitor buffer }	Sends logs to different destinations by module and severity level
Configuring Delayed Logging	 (Optional) It is used to enable the delayed logging function.	
	logging delay-send terminal	Enables delayed display of logs on the Console and remote terminal.
	logging delay-send file flash:filename	Configures the name of the file on the local device where logs are buffered.
	logging delay-send interval <i>seconds</i>	Configures the interval at which logs are sent to the log server.
	logging delay-send server { <i>ip-address</i> ipv6 <i>ipv6-address</i> } mode { ftp user <i>username password</i> [0 7] <i>password</i> tftp }	Configures the server address and delayed logging mode.
Configuring Periodical	 (Optional) It is used to enable the periodical logging function.	

Configuration	Description and Command	
Logging	logging statistic enable	Enables the periodical logging function .
	logging statistic terminal	Enables periodical display of logs on the Console and remote terminal.
	logging statistic mnemonic <i>mnemonic</i> interval <i>minutes</i>	Configures the interval at which logs of a performance statistic object are sent to the server .
Configuring Syslog Redirection	 (Optional) It is used to enable the log redirection function.	
	logging rd on	Enables the log redirection function.
	logging rd rate-limit <i>number</i> [except severity]	Configures the log redirection rate limit.
Configuring Syslog Monitoring	 (Optional) It is used to configure parameters of the syslog monitoring function .	
	logging userinfo	Enables logging of login/exit attempts.
	logging userinfo command-log	Enables logging of operations.
Synchronizing User Input with Log Output	 (Optional) It is used to synchronize the user input with log output.	
	logging synchronous	Synchronizes user input with log output.

6.4.1 Configuring Syslog Format

Configuration Effect

- Configure the format of syslogs.

Notes

📄 RFC3164 Log Format

- If the device does not have the real time clock (RTC), which is used to record the system absolute time, the device uses its startup time (uptime) as the syslog timestamp by default. If the device has the RTC, the device uses its absolute time (datetime) as the syslog timestamp by default.
- The log sequence number is a 6-digit integer. Each time a log is generated, the sequence number increases by one. Each time the sequence number increases from 000000 to 1,000,000, or reaches 2^{32} , the sequence number starts from 000000 again.

📄 RFC5424 Log Format

- After the RFC5424 log format is enabled, the timestamp is uniform.
- In the RFC5424 log format, the timestamp may or may not contain the time zone. Currently, only the timestamp without the time zone is supported.

Configuration Steps

📄 Configuring the Timestamp Format of Syslogs

- (Optional) By default, the datetime timestamp format is used.

- Unless otherwise specified, perform this configuration on the device to configure the timestamp format.

▾ Adding the Sysname to the Syslog

- (Optional) By default, the syslog does not contain the sysname.
- Unless otherwise specified, perform this configuration on the device to add the sysname to the syslog.

▾ Adding the Sequence Number to the Syslog

- (Optional) By default, the syslog does not contain the sequence number.
- Unless otherwise specified, perform this configuration on the device to add the sequence number to the syslog.

▾ Enabling the Standard Log Format

- (Optional) By default, the default log format is used.
- Unless otherwise specified, perform this configuration on the device to enable the standard log format.

▾ Enabling the Private Log Format

- (Optional) By default, the default log format is used.
- Unless otherwise specified, perform this configuration on the device to enable the private log format.

▾ Enabling the RFC5424 Log Format

- (Optional) By default, the RFC5424 log format is disabled.
- Unless otherwise specified, perform this configuration on the device to enable the RFC5424 log format.

Verification

- Generate a syslog, and check the log format.

Related Commands

▾ Configuring the Timestamp Format of Syslogs

Command	service timestamps [<i>message-type</i> [uptime datetime [msec] [year]]]
Parameter Description	<p><i>message-type</i>: Indicates the log type. There are two log types: log and debug.</p> <p>uptime: Indicates the device startup time in the format of dd:hh:mm:ss, for example, 07:00:10:41.</p> <p>datetime: Indicates the current device time in the format of MM DD hh:mm:ss, for example, Jul 27 16:53:07.</p> <p>msec: Indicates that the current device time contains millisecond.</p> <p>year: Indicates that the current device time contains year.</p>
Command Mode	Global configuration mode
Configuration Usage	Two syslog timestamp formats are available, namely, uptime and datetime. You can select a timestamp format as required.

▾ Adding the Sysname to the Syslog

Command	service sysname
----------------	------------------------

Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	This command is used to add the sysname to the log to enable you to learn about the device that sends syslogs to the server.

▾ Adding the Sequence Number to the Syslog

Command	service sequence-numbers
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	This command is used to add the sequence number to the log. The sequence number starts from 1. After the sequence number is added, you can learn clearly whether any log is lost and the generation sequence of logs.

▾ Enabling the Standard Syslog Format

Command	service standard-syslog
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	<p>By default, logs are displayed in the following format (default format):</p> <pre>*timestamp: %module-level-mnemonic: content</pre> <p>If the standard syslog format is enabled, logs are displayed in the following format:</p> <pre>timestamp %module-level-mnemonic: content</pre> <p>Compared with the default format, an asterisk (*) is missing in front of the timestamp, and a colon (:) is missing at the end of the timestamp in the standard log format.</p>

▾ Enabling the Private Syslog Format

Command	service private-syslog
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	<p>By default, logs are displayed in the following format (default format):</p> <pre>*timestamp: %module-level-mnemonic: content</pre> <p>If the private syslog format is enabled, logs are displayed in the following format:</p> <pre>timestamp module-level-mnemonic: content</pre>

	Compared with the default format, an asterisk (*) is missing in front of the timestamp, a colon (:) is missing at the end of the timestamp, and a percent sign (%) is missing in front of the module name in the private log format.
--	--

↘ Enabling the RFC5424 Syslog Format

Command	<code>service log-format rfc5424</code>
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	<p>After the new format (RFC5424 log format) is enabled, the service sequence-numbers, service sysname, service timestamps, service private-syslog, and service standard-syslog commands that are applicable only to the old format (RFC3164 log format) loss effect and are hidden.</p> <p>After the old format (RFC3164 log format) is enabled, the logging delay-send, logging policy, and logging statistic commands that are applicable only to the RFC5424 log format loss effect and are hidden.</p> <p>After log format switchover, the outputs of the show logging and show logging config commands change accordingly.</p>

Configuration Example

↘ Enabling the RFC3164 Log Format

Scenario	<p>It is required to configure the timestamp format as follows:</p> <ol style="list-style-type: none"> 1. Enable the RFC3164 format. 2. Change the timestamp format to datetime and add the millisecond and year to the timestamp. 3. Add the sysname to the log. 4. Add the sequence number to the log.
Configuration Steps	<ul style="list-style-type: none"> ● Configure the syslog format.
	<pre>Orion Alpha A28X# configure terminal Orion Alpha A28X(config)# no service log-format rfc5424 Orion Alpha A28X(config)# service timestamps log datetime year msec Orion Alpha A28X(config)# service timestamps debug datetime year msec Orion Alpha A28X(config)# service sysname Orion Alpha A28X(config)# service sequence-numbers</pre>
Verification	<p>After the timestamp format is configured, verify that new syslogs are displayed in the RFC3164 format.</p> <ul style="list-style-type: none"> ● Run the show logging config command to display the configuration. ● Enter or exit global configuration mode to generate a new log, and check the format of the timestamp in the new log.
	<pre>Orion Alpha A28X(config)#exit</pre>

```

001302: *Jun 14 2013 19:01:40.293: Orion Alpha A28X %SYS-5-CONFIG_I: Configured from console by
admin on console

Orion Alpha A28X#show logging config

Syslog logging: enabled

  Console logging: level informational, 1306 messages logged

  Monitor logging: level informational, 0 messages logged

  Buffer logging: level informational, 1306 messages logged

  File logging: level informational, 121 messages logged

  File name:syslog_test.txt, size 128 Kbytes, have written 5 files

  Standard format:false

  Timestamp debug messages: datetime

  Timestamp log messages: datetime

  Sequence-number log messages: enable

  Sysname log messages: enable

  Count log messages: enable

  Trap logging: level informational, 121 message lines logged,0 fail

```

📌 Enabling the RFC5424 Log Format

Scenario	It is required to enable the RFC5424 format.
Configuration Steps	<ul style="list-style-type: none"> ● Configure the syslog format.
	<pre> Orion Alpha A28X# configure terminal Orion Alpha A28X(config)# service log-format rfc5424 </pre>
Verification	<p>Verify that new syslogs are displayed in the RFC5424 format.</p> <ul style="list-style-type: none"> ● Run the show logging config command to display the configuration. ● Enter or exit global configuration mode to generate a new log, and check the format of the new log.
	<pre> Orion Alpha A28X(config)#exit <133>1 2013-07-24T12:19:33.130290Z Orion Alpha A28X SYS 5 CONFIG - Configured from console by console Orion Alpha A28X#show logging config Syslog logging: enabled Console logging: level debugging, 4740 messages logged Monitor logging: level debugging, 0 messages logged Buffer logging: level debugging, 4745 messages logged </pre>

```
Statistic log messages: disable
Statistic log messages to terminal: disable
Delay-send file name:syslog_ftp_server, Current write index:3, Current send index:3, Cycle:10
seconds
Count log messages: enable
Trap logging: level informational, 2641 message lines logged,4155 fail
  logging to 192.168.23.89
  logging to 2000::1
Delay-send logging: 2641 message lines logged
  logging to 192.168.23.89 by tftp
```

6.4.2 Sending Syslogs to the Console

Configuration Effect

- Send syslogs to the Console to facilitate the administrator to monitor the performance of the system.

Notes

- If too many syslogs are generated, you can limit the log rate to reduce the number of logs displayed on the Console.

Configuration Steps

▾ Enabling Logging

- (Optional) By default, the logging function is enabled.

▾ Enabling Log Statistics

- (Optional) By default, log statistics is disabled.
- Unless otherwise specified, perform this configuration on the device to enable log statistics.

▾ Configuring the Level of Logs Displayed on the Console

- (Optional) By default, the level of logs displayed on the Console is debugging (Level 7).
- Unless otherwise specified, perform this configuration on the device to configure the level of logs displayed on the Console.

▾ Configuring the Log Rate Limit

- (Optional) By default, the no rate limit is configured.
- Unless otherwise specified, perform this configuration on the device to limit the log rate.

Verification

- Run the **show logging config** command to display the level of logs displayed on the Console.

Related Commands

↳ Enabling Logging

Command	logging on
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	By default, logging is enabled. Do not disable logging in general cases. If too many syslogs are generated, you can configure log levels to reduce the number of logs.

↳ Enabling Log Statistics

Command	logging count
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	By default, log statistics is disabled. If log statistics is enabled, syslogs will be classified and counted. The system records the number of times a log is generated and the last time when the log is generated.

↳ Configuring the Level of Logs Displayed on the Console

Command	logging console [level]
Parameter Description	<i>level</i> : Indicates the log level.
Command Mode	Global configuration mode
Configuration Usage	By default, the level of logs displayed on the Console is debugging (Level 7). You can run the show logging config command in privileged EXEC mode to display the level of logs displayed on the Console.

↳ Configuring the Log Rate Limit

Command	logging rate-limit { number all number console {number all number} } [except [severity]]
Parameter Description	<i>number</i> : Indicates the maximum number of logs processed per second. The value ranges from 1 to 10,000. all : Indicates that rate limit is applied to all logs ranging from Level 0 to Level 7. console : Indicates the number of logs displayed on the Console per second. except severity : Rate limit is not applied to logs with a level equaling to or lower than the specified severity level. By default, the severity level is error (Level 3), that is, rate limit is not applied to logs of Level 3 or lower.
Command Mode	Global configuration mode
Configuration Usage	By default, no rate limit is configured.

Configuration Example

📄 Sending Syslogs to the Console

Scenario	It is required to configure the function of displaying syslogs on the Console as follows: <ol style="list-style-type: none">1. Enable log statistics.2. Set the level of logs that can be displayed on the Console to informational (Level 6).3. Set the log rate limit to 50.
Configuration Steps	<ul style="list-style-type: none">● Configure parameters for displaying syslogs on the Console.
	<pre>Orion Alpha A28X# configure terminal Orion Alpha A28X(config)# logging count Orion Alpha A28X(config)# logging console informational Orion Alpha A28X(config)# logging rate-limit console 50</pre>
Verification	<ul style="list-style-type: none">● Run the show logging config command to display the configuration.
	<pre>Orion Alpha A28X(config)#show logging config Syslog logging: enabled Console logging: level informational, 1303 messages logged Monitor logging: level debugging, 0 messages logged Buffer logging: level debugging, 1303 messages logged File logging: level informational, 118 messages logged File name:syslog_test.txt, size 128 Kbytes, have written 5 files Standard format:false Timestamp debug messages: datetime Timestamp log messages: datetime Sequence-number log messages: enable Sysname log messages: enable Count log messages: enable Trap logging: level informational, 118 message lines logged,0 fail</pre>

6.4.3 Sending Syslogs to the Monitor Terminal

Configuration Effect

- Send syslogs to a remote monitor terminal to facilitate the administrator to monitor the performance of the system.

Notes

- If too many syslogs are generated, you can limit the log rate to reduce the number of logs displayed on the monitor terminal.

- By default, the current monitor terminal is not allowed to display logs after you access the device remotely. You need to manually run the **terminal monitor** command to allow the current monitor terminal to display logs.

Configuration Steps

▾ Allowing the Monitor Terminal to Display Logs

- (Mandatory) By default, the monitor terminal is not allowed to display logs.
- Unless otherwise specified, perform this operation on every monitor terminal connected to the device.

▾ Configuring the Level of Logs Displayed on the Monitor Terminal

- (Optional) By default, the level of logs displayed on the monitor terminal is debugging (Level 7).
- Unless otherwise specified, perform this configuration on the device to configure the level of logs displayed on the monitor terminal.

Verification

- Run the **show logging config** command to display the level of logs displayed on the monitor terminal.

Related Commands

▾ Allowing the Monitor Terminal to Display Logs

Command	terminal monitor
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Configuration Usage	By default, the current monitor terminal is not allowed to display logs after you access the device remotely. You need to manually run the terminal monitor command to allow the current monitor terminal to display logs.

▾ Configuring the Level of Logs Displayed on the Monitor Terminal

Command	logging monitor [level]
Parameter Description	<i>level</i> : Indicates the log level.
Command Mode	Global configuration mode
Configuration Usage	By default, the level of logs displayed on the monitor terminal is debugging (Level 7). You can run the show logging config command in privileged EXEC mode to display the level of logs displayed on the monitor terminal.

Configuration Example

▾ Sending Syslogs to the Monitor Terminal

Scenario	It is required to configure the function of displaying syslogs on the monitor terminal as follows: 1. Display logs on the monitor terminal. 2. Set the level of logs that can be displayed on the monitor terminal to informational (Level 6).
Configuration Steps	<ul style="list-style-type: none"> Configure parameters for displaying syslogs on the monitor terminal.
	<pre>Orion Alpha A28X# configure terminal Orion Alpha A28X(config)# logging monitor informational Orion Alpha A28X(config)# line vty 0 4 Orion Alpha A28X(config-line)# monitor</pre>
Verification	<ul style="list-style-type: none"> Run the show logging config command to display the configuration.
	<pre>Orion Alpha A28X#show logging config Syslog logging: enabled Console logging: level informational, 1304 messages logged Monitor logging: level informational, 0 messages logged Buffer logging: level debugging, 1304 messages logged File logging: level informational, 119 messages logged File name:syslog_test.txt, size 128 Kbytes, have written 5 files Standard format:false Timestamp debug messages: datetime Timestamp log messages: datetime Sequence-number log messages: enable Sysname log messages: enable Count log messages: enable Trap logging: level informational, 119 message lines logged,0 fail</pre>

Common Errors

- To disable this function, run the **terminal no monitor** command, instead of the **no terminal monitor** command.

6.4.4 Writing Syslogs into the Memory Buffer

Configuration Effect

- Write syslogs into the memory buffer so that the administrator can view recent syslogs by running the **show logging** command.

Notes

- If the buffer is full, old logs will be overwritten by new logs that are written into the memory buffer.

Configuration Steps

Writing Logs into the Memory Buffer

- (Optional) By default, the system writes logs into the memory buffer, and the default level of logs is debugging (Level 7).
- Unless otherwise specified, perform this configuration on the device to write logs into the memory buffer.

Verification

- Run the **show logging config** command to display the level of logs written into the memory buffer.
- Run the **show logging** command to display the level of logs written into the memory buffer.

Related Commands

Writing Logs into the Memory Buffer

Command	logging buffered [<i>buffer-size</i>] [<i>level</i>]
Parameter	<i>buffer-size</i> : Indicates the size of the memory buffer.
Description	<i>level</i> : Indicates the level of logs that can be written into the memory buffer.
Command Mode	Global configuration mode
Configuration Usage	By default, the level of logs written into the memory buffer is debugging (Level 7). Run the show logging command in privileged EXEC mode to display the level of logs written into the memory buffer and the buffer size.

Configuration Example

Writing Syslogs into the Memory Buffer

Scenario	It is required to configure the function of writing syslog messages into the memory buffer as follows: <ol style="list-style-type: none">1. Set the log buffer size to 128 KB (131,072 bytes).2. Set the information level of logs that can be written into the memory buffer to informational (Level 6).
Configuration Steps	<ul style="list-style-type: none">● Configure parameters for writing syslog messages into the memory buffer.
	<pre>Orion Alpha A28X# configure terminal Orion Alpha A28X(config)# logging buffered 131072 informational</pre>
Verification	<ul style="list-style-type: none">● Run the show logging config command to display the configuration and recent syslog messages.
	<pre>Orion Alpha A28X#show logging Syslog logging: enabled Console logging: level informational, 1306 messages logged Monitor logging: level informational, 0 messages logged Buffer logging: level informational, 1306 messages logged File logging: level informational, 121 messages logged</pre>

Scenario	It is required to configure the function of writing syslogs into the memory buffer as follows: 1. Set the log buffer size to 128 KB (131,072 bytes). 2. Set the information level of logs that can be written into the memory buffer to informational (Level 6).
Configuration Steps	<ul style="list-style-type: none"> ● Configure parameters for writing syslogs into the memory buffer.
	<pre>Orion Alpha A28X# configure terminal Orion Alpha A28X(config)# logging buffered 131072 informational</pre>
Verification	<ul style="list-style-type: none"> ● Run the show logging config command to display the configuration and recent syslogs.
	<pre>File name:syslog_test.txt, size 128 Kbytes, have written 5 files Standard format:false Timestamp debug messages: datetime Timestamp log messages: datetime Sequence-number log messages: enable Sysname log messages: enable Count log messages: enable Trap logging: level informational, 121 message lines logged,0 fail Log Buffer (Total 131072 Bytes): have written 4200 001301: *Jun 14 2013 19:01:09.488: Orion Alpha A28X %SYS-5-CONFIG_I: Configured from console by admin on console 001302: *Jun 14 2013 19:01:40.293: Orion Alpha A28X %SYS-5-CONFIG_I: Configured from console by admin on console //Logs displayed are subject to the actual output of the show logging command.</pre>

6.4.5 Sending Syslogs to the Log Server

Configuration Effect

- Send syslogs to the log server to facilitate the administrator to monitor logs on the server.

Notes

- To send logs to the log server, you must add the timestamp and sequence number to logs. Otherwise, the logs are not sent to the log server.

Configuration Steps

➤ Sending Logs to a Specified Log Server

- (Mandatory) By default, syslogs are not sent to any log server.
- Unless otherwise specified, perform this configuration on every device.

➤ Configuring the Level of Logs Sent to the Log Server

- (Optional) By default, the level of logs sent to the log server is informational (Level 6).
- Unless otherwise specified, perform this configuration on the device to configure the level of logs sent to the log server.

▾ Configuring the Facility Value of Logs Sent to the Log Server

- (Optional) If the RFC5424 format is disabled, the facility value of logs sent to the log server is local7 (23) by default. If the RFC5424 format is enabled, the facility value of logs sent to the log server is local0 (16) by default.
- Unless otherwise specified, perform this configuration on the device to configure the facility value of logs sent to the log server.

▾ Configuring the Source Interface of Logs Sent to the Log Server

- (Optional) By default, the source interface of logs sent to the log server is the interface sending the logs.
- Unless otherwise specified, perform this configuration on the device to configure the source interface of logs sent to the log server.

▾ Configuring the Source Address of Logs Sent to the Log Server


- (Optional) By default, the source address of logs sent to the log server is the IP address of the interface sending the logs.
- Unless otherwise specified, perform this configuration on the device to configure the source address of logs sent to the log server.

Verification

- Run the **show logging config** command to display the configurations related to the log server.

Related Commands

▾ Sending Logs to a Specified Log Server

Command	logging server { <i>ip-address</i> ipv6 <i>ipv6-address</i> } [udp-port <i>port</i>] Or logging { <i>ip-address</i> ipv6 <i>ipv6-address</i> } [udp-prot <i>port</i>]
Parameter Description	<i>ip-address</i> : Specifies the IP address of the host that receives logs. ipv6 <i>ipv6-address</i> : Specifies the IPv6 address of the host that receives logs. udp-port <i>port</i> : Specifies the port ID of the log server. The default port ID is 514.
Command Mode	Global configuration mode
Configuration Usage	This command is used to specify the address of the log server that receives logs. You can specify multiple log servers, and logs will be sent simultaneously to all these log servers.  You can configure up to five log servers on a Orion Alpha A28X product.

▾ Configuring the Level of Logs Sent to the Log Server

Command	logging trap [<i>level</i>]
Parameter	<i>level</i> : Indicates the log level.

Description	
Command Mode	Global configuration mode
Configuration Usage	By default, the level of logs sent to the log server is informational (Level 6). You can run the show logging config command in privileged EXEC mode to display the level of logs sent to the log server.

▾ Configuring the Facility Value of Logs Sent to the Log Server

Command	logging facility <i>facility-type</i>
Parameter Description	<i>facility-type</i> : Indicates the facility value of logs.
Command Mode	Global configuration mode
Configuration Usage	If the RFC5424 format is disabled, the facility value of logs sent to the server is local7 (23) by default. If the RFC5424 format is enabled, the facility value of logs sent to the server is local0 (16) by default.

▾ Configuring the Source Interface of Logs Sent to the Log Server

Command	logging source [interface] <i>interface-type interface-number</i>
Parameter Description	<i>interface-type</i> : Indicates the interface type. <i>interface-number</i> : Indicates the interface number.
Command Mode	Global configuration mode
Configuration Usage	By default, the source interface of logs sent to the log server is the interface sending the logs. To facilitate management, you can use this command to set the source interface of all logs to an interface so that the administrator can identify the device that sends the logs based on the unique address.

▾ Configuring the Source Address of Logs Sent to the Log Server

Command	logging source { ip ip-address ipv6 ipv6-address }
Parameter Description	ip ip-address : Specifies the source IPv4 address of logs sent to the IPv4 log server. ipv6 ipv6-address : Specifies the source IPv6 address of logs sent to the IPv6 log server.
Command Mode	Global configuration mode
Configuration Usage	By default, the source IP address of logs sent to the log server is the IP address of the interface sending the logs. To facilitate management, you can use this command to set the source IP address of all logs to the IP address of an interface so that the administrator can identify the device that sends the logs based on the unique address..

Configuration Example

▾ Sending Syslogs to the Log Server

Scenario	<p>It is required to configure the function of sending syslogs to the log server as follows:</p> <ol style="list-style-type: none"> 1. Set the IPv4 address of the log server to 10.1.1.100. 2. Set the level of logs that can be sent to the log server to debugging (Level 7). 3. Set the source interface to Loopback 0.
Configuration Steps	<ul style="list-style-type: none"> ● Configure parameters for sending syslogs to the log server.
	<pre>Orion Alpha A28X# configure terminal Orion Alpha A28X(config)# logging server 10.1.1.100 Orion Alpha A28X(config)# logging trap debugging Orion Alpha A28X(config)# logging source interface Loopback 0</pre>
Verification	<ul style="list-style-type: none"> ● Run the show logging config command to display the configuration.
	<pre>Orion Alpha A28X#show logging config Syslog logging: enabled Console logging: level informational, 1307 messages logged Monitor logging: level informational, 0 messages logged Buffer logging: level informational, 1307 messages logged File logging: level informational, 122 messages logged File name:syslog_test.txt, size 128 Kbytes, have written 5 files Standard format:false Timestamp debug messages: datetime Timestamp log messages: datetime Sequence-number log messages: enable Sysname log messages: enable Count log messages: enable Trap logging: level debugging, 122 message lines logged,0 fail logging to 10.1.1.100</pre>

6.4.6 Writing Syslogs into Log Files

Configuration Effect

- Write syslogs into log files at the specified interval so that the administrator can view history logs anytime on the local device.

Notes

- Syslogs are not immediately written into log files. They are first buffered in the memory buffer, and then written into log files either periodically (at the interval of one hour by default) or when the buffer is full.

Configuration Steps

Writing Logs into Log Files

- (Mandatory) By default, syslogs are not written to any log file.
- Unless otherwise specified, perform this configuration on every device.

Configuring the Number of Log Files

- (Optional) By default, syslogs are written to 16 log files.
- Unless otherwise specified, perform this configuration on the device to configure the number of files which logs are written into.

Configuring the Interval at Which Logs Are Written into Log Files

- (Optional) By default, syslogs are written to log files every hour.
- Unless otherwise specified, perform this configuration on the device to configure the interval at which logs are written into log files.

Configuring the Storage Time of Log Files

- (Optional) By default, no storage time is configured.
- Unless otherwise specified, perform this configuration on the device to configure the storage time of log files.

Immediately Writing Logs in the Buffer into Log Files

- (Optional) By default, syslogs are stored in the buffer and then written into log files periodically or when the buffer is full.
- Unless otherwise specified, perform this configuration to write logs in the buffer into log files immediately. This command takes effect only once after it is configured.

Verification

- Run the **show logging config** command to display the configurations related to the log server.

Related Commands

Writing Logs into Log Files

Command	logging file { flash:filename } [max-file-size] [level]
Parameter Description	flash: Indicates that log files will be stored on the extended Flash. filename: Indicates the log file name, which does not contain a file name extension. The file name extension is always txt. max-file-size: Indicates the maximum size of a log file. The value ranges from 128 KB to 6 MB. The default value is 128 KB. level: Indicates the level of logs that can be written into a log file.
Command Mode	Global configuration mode
Configuration	This command is used to create a log file with the specified file name on the specified file storage device.

Usage	<p>The file size increases with the amount of logs, but cannot exceed the configured maximum size. If not specified, the maximum size of a log file is 128 KB by default.</p> <p>After this command is configured, the system saves logs to log files. A log file name does not contain any file name extension. The file name extension is always txt, which cannot be changed.</p> <p>After this command is configured, logs will be written into log files every hour. If you run the logging file flash:syslog command, a total of 16 log files will be created, namely, syslog.txt, syslog_1.txt, syslog_2.txt, ..., syslog_14.txt, and syslog_15.txt. Logs are written into the 16 log files in sequence. For example, the system writes logs into syslog_1.txt after syslog.txt is full. When syslog_15.txt is full, logs are written into syslog.txt again,</p>
--------------	---

📌 Configuring the Number of Log Files

Command	logging file numbers <i>numbers</i>
Parameter Description	<i>numbers</i> : Indicates the number of log files. The value ranges from 2 to 32.
Command Mode	Global configuration mode
Configuration Usage	<p>This command is used to configure the number of log files.</p> <p>If the number of log files is modified, the system will not delete the log files that have been generated. Therefore, you need to manually delete the existing log files to save the space of the extended flash. (Before deleting existing log files, you can transfer these log files to an external server through TFTP.) For example, after the function of writing logs into log files is enabled, 16 log files will be created by default. If the device has generated 16 log files and you change the number of log files to 2, new logs will be written into syslog.txt and syslog_1.txt by turns. The existing log files from syslog_2.txt to syslog_15.txt will be preserved. You can manually delete these log files.</p>

📌 Configuring the Interval at Which Logs Are Written into Log Files


Command	logging flash interval <i>seconds</i>
Parameter Description	<i>seconds</i> : Indicates the interval at which logs are written into log files. The value ranges from 1s to 51,840s.
Command Mode	Global configuration mode
Configuration Usage	This command is used to configure the interval at which logs are written into log files. The countdown starts after the command is configured.

📌 Configuring the Storage Time of Log Files

Command	logging life-time level <i>level days</i>
Parameter Description	<p><i>level</i>: Indicates the log level.</p> <p><i>days</i>: Indicates the storage time of log files. The unit is day. The storage time is not less than seven days.</p>
Command Mode	Global configuration mode
Configuration Usage	After the log storage time is configured, the system writes logs of the same level that are generated in the same day into the same log file. The log file is named yyyy-mm-dd_filename_level.txt , where yyyy-mm-

	<p>dd is the absolute time of the day when the logs are generated, filename is the log file named configured by the logging file flash command, and level is the log level.</p> <p>After you specify the storage time for logs of a certain level, the system deletes the logs after the storage time expires. Currently, the storage time ranges from 7days to 365 days.</p> <p>If the log storage time is not configured, logs are stored based on the file size to ensure compatibility with old configuration commands.</p>
--	---

↳ Immediately Writing Logs in the Buffer into Log Files

Command	logging flash flush
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	<p>After this command is configured, syslog is stored in the buffer and then written into log files periodically or when the buffer is full. You can run this command to immediately write logs into log files.</p> <p> The logging flash flush command takes effect once after it is configured. That is, after this command is configured, logs in the buffer are immediately written to log files.</p>

Configuration Example

↳ Writing Syslogs into Log Files

Scenario	<p>It is required to configure the function of writing syslogs into log files as follows:</p> <ol style="list-style-type: none"> 1. Set the log file name to syslog. 2. Set the level of logs sent to the Console to debugging (Level 7). 3. Set the interval at which device logs are written into files to 10 minutes (600s).
Configuration Steps	<ul style="list-style-type: none"> ● Configure parameters for writing syslogs into log files. <pre>Orion Alpha A28X# configure terminal Orion Alpha A28X(config)# logging file flash:syslog debugging Orion Alpha A28X(config)# logging flash interval 600</pre>
Verification	<ul style="list-style-type: none"> ● Run the show logging config command to display the configuration. <pre>Orion Alpha A28X(config)#show logging config Syslog logging: enabled Console logging: level informational, 1307 messages logged Monitor logging: level informational, 0 messages logged Buffer logging: level informational, 1307 messages logged File logging: level debugging, 122 messages logged File name:syslog.txt, size 128 Kbytes, have written 1 files</pre>

Scenario	It is required to configure the function of writing syslogs into log files as follows: <ol style="list-style-type: none"> 1. Set the log file name to syslog. 2. Set the level of logs sent to the Console to debugging (Level 7). 3. Set the interval at which device logs are written into files to 10 minutes (600s).
Configuration Steps	<ul style="list-style-type: none"> ● Configure parameters for writing syslogs into log files.
	<pre>Orion Alpha A28X# configure terminal Orion Alpha A28X(config)# logging file flash:syslog debugging Orion Alpha A28X(config)# logging flash interval 600</pre>
Verification	<ul style="list-style-type: none"> ● Run the show logging config command to display the configuration.
	<pre>Standard format:false Timestamp debug messages: datetime Timestamp log messages: datetime Sequence-number log messages: enable Sysname log messages: enable Count log messages: enable Trap logging: level debugging, 122 message lines logged,0 fail logging to 10.1.1.100</pre>

6.4.7 Configuring Syslog Filtering

Configuration Effect

- Filter out a specified type of syslogs if the administrator does not want to display these syslogs.
- By default, logs generated by all modules are displayed on the Console or other terminals. You can configure log filtering rules to display only desired logs.

Notes

- Two filtering modes are available: contains-only and filter-only. You can configure only one filtering mode at a time.
- If the same module, level, or mnemonic is configured in both the single-match and exact-match rules, the single-match rule prevails over the exact-match rule.

Configuration Steps

↘ **Configuring the Log Filtering Direction**

- (Optional) By default, the filtering direction is all, that is, all logs are filtered out.
- Unless otherwise specified, perform this configuration on the device to configure the log filtering direction.

↘ **Configuring the Log Filtering Mode**

- (Optional) By default, the log filtering mode is filter-only.

- Unless otherwise specified, perform this configuration on the device to configure the log filtering mode.

↘ Configuring the Log Filtering Rule

- (Mandatory) By default, no filtering rule is configured.
- Unless otherwise specified, perform this configuration on the device to configure the log filtering rule.

Verification

- Run the **show running** command to display the configuration.

Related Commands

↘ Configuring the Log Filtering Direction

Command	logging filter direction { all buffer file server terminal }
Parameter Description	all : Filters out all logs. buffer : Filters out logs sent to the log buffer, that is, the logs displayed by the show logging command. file : Filters out logs written into log files. server : Filters out logs sent to the log server. terminal : Filters out logs sent to the Console and VTY terminal (including Telnet and SSH).
Command Mode	Global configuration mode
Configuration Usage	The default filtering direction is all , that is, all logs are filtered out. Run the default logging filter direction command to restore the default filtering direction.

↘ Configuring the Log Filtering Mode

Command	logging filter type { contains-only filter-only }
Parameter Description	contains-only : Indicates that only logs that contain keywords specified in the filtering rules are displayed. filter-only : Indicates that logs that contain keywords specified in the filtering rules are filtered out and will not be displayed.
Command Mode	Global configuration mode
Configuration Usage	Log filtering modes include contains-only and filter-only. The default filtering mode is filter-only.

↘ Configuring the Log Filtering Rule

Command	logging filter rule { exact-match module <i>module-name</i> mnemonic <i>mnemonic-name</i> level <i>level</i> single-match { level <i>level</i> mnemonic <i>mnemonic-name</i> module <i>module-name</i> } }
Parameter Description	exact-match : If exact-match is selected, you must specify all three filtering options. single-match : If single-match is selected, you may specify only one of the three filtering options. module <i>module-name</i> : Indicates the module name. Logs of this module will be filtered out. mnemonic <i>mnemonic-name</i> : Indicates the mnemonic. Logs with this mnemonic will be filtered out. level <i>level</i> : Indicates the log level. Logs of this level will be filtered out.
Command Mode	Global configuration mode

Configuration	Log filtering rules include exact-match and single-match.
Usage	<p>The no logging filter rule exact-match [module <i>module-name</i> mnemonic <i>mnemonic-name</i> level <i>level</i>] command is used to delete the exact-match filtering rules. You can delete all exact-match filtering rules at a time or one by one.</p> <p>The no logging filter rule single-match [level <i>level</i> mnemonic <i>mnemonic-name</i> module <i>module-name</i>] command is used to delete the single-match filtering rules. You can delete all single-match filtering rules at a time or one by one.</p>

Configuration Example

Configuring Syslog Filtering

Scenario	<p>It is required to configure the syslog filtering function as follows:</p> <ol style="list-style-type: none"> 1. Set the filtering directions of logs to terminal and server. 2. Set the log filtering mode to filter-only. 3. Set the log filtering rule to single-match to filter out logs that contain the module name "SYS".
Configuration Steps	<ul style="list-style-type: none"> ● Configure the syslog filtering function.
	<pre>Orion Alpha A28X# configure terminal Orion Alpha A28X(config)# logging filter direction server Orion Alpha A28X(config)# logging filter direction terminal Orion Alpha A28X(config)# logging filter type filter-only Orion Alpha A28X(config)# logging filter rule single-match module SYS</pre>
Verification	<ul style="list-style-type: none"> ● Run the show running-config include logging command to display the configuration. ● Enter and exit global configuration mode, and verify that the system displays logs accordingly.
	<pre>Orion Alpha A28X#configure Enter configuration commands, one per line. End with CNTL/Z. Orion Alpha A28X(config)#exit Orion Alpha A28X# Orion Alpha A28X#show running-config include logging logging filter direction server logging filter direction terminal logging filter rule single-match module SYS</pre>

6.4.8 Configuring Level-based Logging

Configuration Effect

- You can use the level-based logging function to send syslogs to **different destinations** based on different module and severity level. For example, you can configure a command to send WLAN module logs of Level 4 or lower to the log server, and WLAN module logs of Level 5 or higher to local log files.

Notes

- Level-based logging takes effect only when the RFC5424 format is enabled.

Configuration Steps

↳ Configuring Level-based Logging

- (Optional) By default, logs are sent in all directions.
- Unless otherwise specified, perform this configuration on the device to configure logging polices to send syslogs to different destinations based on module and severity level.

Verification

- Run the **show running** command to display the configuration.

Related Commands

↳ Configuring Level-based Logging

Command	logging policy module <i>module-name</i> [not-lesser-than] <i>level</i> direction { all server file console monitor buffer }
Parameter Description	module-name : Indicates the name of the module to which the logging policy is applied. not-lesser-than : If this option is specified, logs of the specified level or higher will be sent to the specified destination, and other logs will be filtered out. If this option is not specified, logs of the specified level or lower will be sent to the specified destination, and other logs will be filtered out. level : Indicates the level of logs for which the logging policy is configured. all : Indicates that the logging policy is applied to all logs. server : Indicates that the logging policy is applied only to logs sent to the log server. file : Indicates that the logging policy is applied only to logs written into log files. console : Indicates that the logging policy is applied only to logs sent to the Console. monitor : Indicates that the logging policy is applied only to logs sent to a remote terminal. buffer : Indicates that the logging policy is applied only to logs stored in the buffer.
Command Mode	Global configuration mode
Configuration Usage	This command is used to configure logging polices to send syslogs to different destinations based on module and severity level.

Configuration Example

↳ Configuring Level-based Logging

Scenario	It is required to configure the logging policies as follows: <ol style="list-style-type: none">1. Send logs of Level 5 or higher that are generated by the system to the Console.2. Send logs of Level 3 or lower that are generated by the system to the buffer.
Configuration Steps	<ul style="list-style-type: none">● Configure the logging policies.

	<pre>Orion Alpha A28X# configure terminal Orion Alpha A28X(config)# logging policy module SYS not-lesser-than 5 direction console Orion Alpha A28X(config)# logging policy module SYS 3 direction buffer</pre>
Verification	<ul style="list-style-type: none"> ● Run the show running-config include logging policy command to display the configuration. ● Exit and enter global configuration mode to generate a log containing module name "SYS". Verify that the log is sent to the destination as configured.
	<pre>Orion Alpha A28X#show running-config include logging policy logging policy module SYS not-lesser-than 5 direction console logging policy module SYS 3 direction buffer</pre>

6.4.9 Configuring Delayed Logging

Configuration Effect

- By default, delayed logging is enabled by default at the interval of 3600s (one hour). The name of the log file sent to the remote server is **File size_Device IP address_Index.txt**. Logs are not sent to the Console or remote terminal.
- You can configure the interval based on the frequency that the device generates logs for delayed uploading. This can reduce the burden on the device, syslog server, and network. In addition, you can configure the name of the log file as required.

Notes

- This function takes effect only when the RFC5424 format is enabled.
- It is recommended to disable the delayed display of logs on the Console and remote terminal. Otherwise, a large amount of logs will be displayed, increasing the burden on the device.
- The file name cannot contain any dot (.) because the system automatically adds the index and the file name extension (.txt) to the file name when generating a locally buffered file. The index increases each time a new file is generated. In addition, the file name cannot contain characters prohibited by your file system, such as \, /, :, *, ", <, >, and |. For example, the file name is log_server, the current file index is 5, the file size is 1000 bytes, and the source IP address is 10.2.3.5. The name of the log file sent to the remote server is **log_server_1000_10.2.3.5_5.txt** while the name of the log file stored on the device is **log_server_5.txt**. If the source IP address is an IPv6 address, the colon (:) in the IPv6 address must be replaced by the hyphen (-) because the colon (:) is prohibited by the file system. For example, the file name is log_server, the current file index is 6, the file size is 1000 bytes, and the source IPv6 address is 2001::1. The name of the log file sent to the remote server is **log_server_1000_2001-1_6.txt** while the name of the log file stored on the device is **log_server_6.txt**.
- If few logs are generated, you can set the interval to a large value so that many logs can be sent to the remote server at a time.

Configuration Steps

📌 Enabling Delayed Display of Logs on Console and Remote Terminal

- (Optional) By default, delayed display of logs on the Console and remote terminal is disabled.

- Unless otherwise specified, perform this configuration on the device to enable delayed display of logs on the Console and remote terminal.

↘ **Configuring the Name of the File for Delayed Logging**

- (Optional) By default, the name of the file for delayed logging is ***File size_Device IP address_Index.txt***.
- Unless otherwise specified, perform this configuration on the device to configure the name of the file for delayed logging.

↘ **Configuring the Delayed Logging Interval**

- (Optional) By default, the delayed logging interval is 3600s (one hour).
- Unless otherwise specified, perform this configuration on the device to configure the delayed logging interval.

↘ **Configuring the Server Address and Delayed Logging Mode**

- (Optional) By default, log files are not sent to any remote server.
- Unless otherwise specified, perform this configuration on the device to configure the server address and delayed logging mode

Verification

- Run the **show running** command to display the configuration.

Related Commands

↘ **Enabling Delayed Display of Logs on Console and Remote Terminal**

Command	logging delay-send terminal
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	N/A.

↘ **Configuring the Name of the File for Delayed Logging**

Command	logging delay-send file flash:filename
Parameter Description	flash:filename: Indicates the name of the file on the local device where logs are buffered.
Command Mode	Global configuration mode
Configuration Usage	This command is used to configure the name of the file on the local device where logs are buffered. The file name cannot contain any dot (.) because the system automatically adds the index and the file name extension (.txt) to the file name when generating a locally buffered file. The index increases each time a new file is generated. In addition, the file name cannot contain characters prohibited by your file

	<p>system, such as \, /, :, *, ", <, >, and .</p> <p>For example, the configured file name is log_server, the current file index is 5, the file size is 1000 bytes, and the source IP address is 10.2.3.5. The name of the log file sent to the remote server is log_server_1000_10.2.3.5_5.txt while the name of the log file stored on the device is log_server_5.txt.</p> <p>If the source IP address is an IPv6 address, the colon (:) in the IPv6 address must be replaced by the hyphen (-) because the colon (:) is prohibited by the file system.</p> <p>For example, the file name is log_server, the current file index is 6, the file size is 1000 bytes, and the source IPv6 address is 2001::1. The name of the log file sent to the remote server is log_server_1000_2001-1_6.txt while the name of the log file stored on the device is log_server_6.txt.</p>
--	---

↘ [Configuring the Delayed Logging Interval](#)

Command	logging delay-send interval <i>seconds</i>
Parameter Description	<i>seconds</i> : Indicates the delayed logging interval. The unit is second.
Command Mode	Global configuration mode
Configuration Usage	This command is used to configure the delayed logging interval. The value ranges from 600s to 65,535s.

↘ [Configuring the Server Address and Delayed Logging Mode](#)

Command	logging delay-send server { <i>ip-address</i> ipv6 <i>ipv6-address</i> } mode { ftp user <i>username password</i> [0 7] <i>password</i> tftp }
Parameter Description	<p><i>ip-address</i>: Indicates the IP address of the server that receives logs.</p> <p>ipv6 <i>ipv6-address</i>: Indicates the IPv6 address of the server that receives logs.</p> <p><i>username</i>: Specifies the user name of the FTP server.</p> <p><i>password</i>: Specifies the password of the FTP server.</p> <p>0: (Optional) Indicates that the following password is in plain text.</p> <p>7: Indicates that the following password is encrypted.</p>
Command Mode	Global configuration mode
Configuration Usage	This command is used to specify an FTP or a TFTP server for receiving the device logs. You can configure a total of five FTP or TFTP servers, but a server cannot be both an FTP and TFTP server.. Logs will be simultaneously sent to all FTP or TFTP servers.

[Configuration Example](#)

↘ [Configuring Delayed Logging](#)

Scenario	<p>It is required to configure the delayed logging function as follows:</p> <ol style="list-style-type: none"> 1. Enable the delayed display of logs on the Console and remote terminal. 2. Set the delayed logging interval to 7200s (two hours). 3. Set the name of the file for delayed logging to syslog_Orion Alpha A28X. 4. Set the IP address of the server to 192.168.23.12, user name to admin, password to admin, and logging mode to FTP.
Configuration Steps	<ul style="list-style-type: none"> ● Configure the delayed logging function.
	<pre>Orion Alpha A28X# configure terminal Orion Alpha A28X(config)# logging delay-send terminal Orion Alpha A28X(config)# logging delay-send interval 7200 Orion Alpha A28X(config)# logging delay-send file flash:syslog_Orion Alpha A28X Orion Alpha A28X(config)# logging delay-send server 192.168.23.12 mode ftp user admin password admin</pre>
Verification	<ul style="list-style-type: none"> ● Run the show running-config include logging delay-send command to display the configuration. ● Verify that logs are sent to the remote FTP server after the timer expires.
	<pre>Orion Alpha A28X#show running-config include logging delay-send logging delay-send terminal logging delay-send interval 7200 logging delay-send file flash:syslog_Orion Alpha A28X logging delay-send server 192.168.23.12 mode ftp user admin password admin</pre>

6.4.10 Configuring Periodical Logging

Configuration Effect

- By default, periodical logging is disabled. Periodical logging interval is 15 minutes. Periodical display of logs on the Console and remote terminal are disabled.
- You can modify the periodical logging interval. The server will collect all performance statistic logs at the time point that is the least common multiple of the intervals of all statistic objects.

Notes

- Periodical logging takes effect only when the RFC5424 format is enabled.
- The settings of the periodical logging interval and the function of displaying logs on the Console and remote terminal take effect only when the periodical logging function is enabled.
- It is recommended to disable periodical display of logs on the Console and remote terminal. Otherwise, a large amount of performance statistic logs will be displayed, increasing the burden on the device.
- To ensure the server can collect all performance statistic logs at the same time point, the timer will be restarted when you modify the periodical logging interval of a statistic object.

Configuration Steps

↳ Enabling Periodical Logging

- (Optional) By default, periodical logging is disabled.
- Unless otherwise specified, perform this configuration on the device to enable periodical logging.

↳ Enabling Periodical Display of Logs on Console and Remote Terminal

- (Optional) By default, periodical display of logs on the Console and remote terminal is disabled.
- Unless otherwise specified, perform this configuration on the device to enable periodical display of logs on the Console and remote terminal.

↳ Configuring the Periodical Logging Interval

- (Optional) By default, the periodical logging interval is 15 minutes.
- Unless otherwise specified, perform this configuration on the device to configure the interval at which logs of statistic objects are sent to the server.

Verification

- Run the **show running** command to display the configuration.

Related Commands

↳ Enabling Periodical Logging

Command	logging statistic enable
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	This command is used to enable periodical logging. After this function is enabled, the system outputs a series of performance statistics at a certain interval so that the log server can monitor the system performance.

↳ Enabling Periodical Display of Logs on Console and Remote Terminal

Command	logging statistic terminal
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	N/A

↳ Configuring the Periodical Logging Interval

Command	logging statistic mnemonic <i>mnemonic</i> interval <i>minutes</i>
----------------	---

Parameter	<i>mnemonic</i> : Identifies a performance statistic object.
Description	<i>minutes</i> : Indicates the periodical logging interval. The unit is minute.
Command Mode	Global configuration mode
Configuration Usage	This command is used to configure the periodical logging interval for a specified performance statistic object. The interval can be set to 0, 15, 30, 60, or 120 minutes. 0 indicates that periodical logging is disabled.

Configuration Example

📌 Configuring Periodical Logging

Scenario	It is required to configure the periodical logging function as follows: <ol style="list-style-type: none"> 1. Enable the periodical logging function. 2. Enable periodical display of logs on the Console and remote terminal. 3. Set the periodical logging interval of the statistic object TUNNEL_STAT to 30 minutes.
Configuration Steps	<ul style="list-style-type: none"> ● Configure the periodical logging function.
	<pre>Orion Alpha A28X# configure terminal Orion Alpha A28X(config)# logging statistic enable Orion Alpha A28X(config)# logging statistic terminal Orion Alpha A28X(config)# logging statistic mnemonic TUNNEL_STAT interval 30</pre>
Verification	<ul style="list-style-type: none"> ● Run the show running-config include logging statistic command to display the configuration. ● After the periodical logging timer expires, verify that logs of all performance statistic objects are generated at the time point that is the least common multiple of the intervals of all statistic objects.
	<pre>Orion Alpha A28X#show running-config include logging statistic logging statistic enable logging statistic terminal logging statistic mnemonic TUNNEL_STAT interval 30</pre>

6.4.11 Configuring Syslog Redirection

Configuration Effect

- On the VSU, logs on the secondary or standby device are displayed on its Console window, and redirected to the active device for display on the Console or VTY window, or stored in the memory buffer, extended flash, or syslog server.
- On a box-type VSU, after the log redirection function is enabled, logs on the secondary or standby device will be redirected to the active device, and the role flag (*device ID) will be added to each log to indicate that the log is redirected. Assume that four devices form a VSU. The ID of the active device is 1, the ID of the secondary device is 2, and the IDs of two standby devices are 3 and 4. The role flag is not added to logs generated by the active device. The

role flag (*2) is added to logs redirected from the secondary device to the active device. The role flags (*3) and (*4) are added respectively to logs redirected from the two standby devices to the active device.

- On a card-type VSU, after the log redirection function is enabled, logs on the secondary or standby supervisor module will be redirected to the active supervisor module, and the role flag "(device ID/supervisor module name)" will be added to each log to indicate that the log is redirected. If four supervisor modules form a VSU, the role flags are listed as follows: (*1/M1), (*1/M2), (*2/M1), and (*2/M2).

Notes

- The syslog redirection function takes effect only on the VSU.
- You can limit the rate of logs redirected to the active device to prevent generating a large amount of logs on the secondary or standby device.

Configuration Steps

▾ Enabling Log Redirection

- (Optional) By default, log redirection is enabled on the VSU.
- Unless otherwise specified, perform this configuration on the active device of VSU or active supervisor module.

▾ Configuring the Rate Limit

- (Optional) By default, a maximum of 200 logs can be redirected from the standby device to the active device of VSU per second.
- Unless otherwise specified, perform this configuration on the active device of VSU or active supervisor module.

Verification

- Run the **show running** command to display the configuration.

Related Commands

▾ Enabling Log Redirection

Command	logging rd on
Parameter	N/A
Description	
Command Mode	Global configuration mode
Configuration Usage	By default, log redirection is enabled on the VSU.

▾ Configuring the Rate Limit

Command	logging rd rate-limit <i>number</i> [except <i>level</i>]
Parameter Description	rate-limit <i>number</i> : Indicates the maximum number of logs redirected per second. The value ranges from 1 to 10,000. except <i>level</i> : Rate limit is not applied to logs with a level equaling to or lower than the specified severity

	level. By default, the severity level is error (Level 3), that is, rate limit is not applied to logs of Level 3 or lower.
Command Mode	Global configuration mode
Configuration Usage	By default, a maximum of 200 logs can be redirected from the standby device to the active device of VSU per second.

Configuration Example

↳ Configuring Syslog Redirection

Scenario	It is required to configure the syslog redirection function on the VSU as follows: <ol style="list-style-type: none"> 1. Enable the log redirection function. 2. Set the maximum number of logs with a level higher than critical (Level 2) that can be redirected per second to 100.
Configuration Steps	<ul style="list-style-type: none"> ● Configure the syslog redirection function.
	<pre>Orion Alpha A28X# configure terminal Orion Alpha A28X(config)# logging rd on Orion Alpha A28X(config)# logging rd rate-limit 100 except critical</pre>
Verification	<ul style="list-style-type: none"> ● Run the show running-config include logging command to display the configuration. ● Generate a log on the standby device, and verify that the log is redirected to and displayed on the active device.
	<pre>Orion Alpha A28X#show running-config include logging logging rd rate-limit 100 except critical</pre>

6.4.12 Configuring Syslog Monitoring

Configuration Effect

- Record login/exit attempts. After logging of login/exit attempts is enabled, the related logs are displayed on the device when users access the device through Telnet or SSH. This helps the administrator monitor the device connections.
- Record modification of device configurations. After logging of operations is enabled, the related logs are displayed on the device when users modify the device configurations. This helps the administrator monitor the changes in device configurations.

Notes

- If both the **logging userinfo** command and the **logging userinfo command-log** command are configured on the device, only the configuration result of the **logging userinfo command-log** command is displayed when you run the **show running-config** command.

Configuration Steps

↳ Enabling Logging of Login/Exit Attempts

- (Optional) By default, logging of login/exit attempts is disabled.
- Unless otherwise specified, perform this configuration on every line of the device to enable logging of login/exit attempts.

▾ Enabling logging of Operations

- (Optional) By default, logging of operations is disabled.
- Unless otherwise specified, perform this configuration on every line of the device to enable logging of operations.

Verification

- Run the **show running** command to display the configuration.

Related Commands

▾ Enabling Logging of Login/Exit Attempts

Command	logging userinfo
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	By default, a device does not generate related logs when users log into or exit the device.

▾ Enabling Logging of Operations

Command	logging userinfo command-log
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	The system generates related logs when users run configuration commands. By default, a device does not generate logs when users modify device configurations.

Configuration Example

▾ Configuring Syslog Monitoring

Scenario	It is required to configure the syslog monitoring function as follows: <ol style="list-style-type: none"> 1. Enable logging of login/exit attempts. 2. Enable logging of operations.
Configuration Steps	<ul style="list-style-type: none"> ● Configure the syslog monitoring function.

	<pre>Orion Alpha A28X# configure terminal Orion Alpha A28X(config)# logging userinfo Orion Alpha A28X(config)# logging userinfo command-log</pre>
Verification	<ul style="list-style-type: none"> ● Run the show running-config include logging command to display the configuration. ● Run a command in global configuration mode, and verify that the system generates a log.
	<pre>Orion Alpha A28X#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Orion Alpha A28X(config)#interface gigabitEthernet 0/0 *Jun 16 15:03:43: %CLI-5-EXEC_CMD: Configured from console by admin command: interface GigabitEthernet 0/0 Orion Alpha A28X#show running-config include logging logging userinfo command-log</pre>

6.4.13 Synchronizing User Input with Log Output

Configuration Effect

- By default, the user input is not synchronized with the log output. After this function is enabled, the content input during log output is displayed after log output is completed, ensuring integrity and continuity of the input.

Notes

- This command is executed in line configuration mode. You need to configure this command on every line as required.

Configuration Steps

📌 Synchronizing User Input with Log Output

- (Optional) By default, the synchronization function is disabled.
- Unless otherwise specified, perform this configuration on every line to synchronize user input with log output.

Verification

- Run the **show running** command to display the configuration.

Related Commands

📌 Synchronizing User Input with Log Output

Command	logging synchronous
Parameter Description	N/A
Command Mode	Line configuration mode
Configuration	This command is used to synchronize the user input with log output to prevent interrupting the user input.

Usage	
-------	--

Configuration Example

📄 Synchronizing User Input with Log Output

Scenario	It is required to synchronize the user input with log output as follows: 1. Enable the synchronization function.
Configuration Steps	<ul style="list-style-type: none"> Configure the synchronization function.
	<pre>Orion Alpha A28X# configure terminal Orion Alpha A28X(config)# line console 0 Orion Alpha A28X(config-line)# logging synchronous</pre>
Verification	<ul style="list-style-type: none"> Run the show running-config begin line command to display the configuration.
	<pre>Orion Alpha A28X#show running-config begin line line con 0 logging synchronous login local</pre> <p>As shown in the following output, when a user types in "vlan", the state of interface 0/1 changes and the related log is output. After log output is completed, the log module automatically displays the user input "vlan" so that the user can continue typing.</p> <pre>Orion Alpha A28X(config)#vlan *Aug 20 10:05:19: %LINK-5-CHANGED: Interface GigabitEthernet 0/1, changed state to up *Aug 20 10:05:19: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/1, changed state to up Orion Alpha A28X(config)#vlan</pre>

6.5 Monitoring

Clearing

 Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears logs in the memory buffer.	clear logging

Displaying

Description	Command
Displays log statistics and logs in the memory buffer based on the timestamp from oldest to latest.	show logging

Displays log statistics and logs in the memory buffer based on the timestamp from latest to oldest.	show logging reverse
Displays syslog configurations and statistics.	show logging config
Displays log statistics of each module in the system.	show logging count

7 Configuring ZAM

7.1 Overview

Manual deployment of all required devices for go-online on a network consumes a lot of labor and material resources, and has the following problems or defects:

- Manual deployment of a massive number of devices for go-online on a network imposes a high technical requirement on deployment personnel. It requires a long period, resulting in high labor and material costs.
- Manual deployment of a massive number of devices may cause fatigue, and consequently, may easily cause deployment inconsistency or errors, resulting in network malfunction.
- Manual deployment does not support control and unified management, easily causing difference and inconsistency.
- It is hard to track an event and network device deployment. The entire deployment process cannot be controlled and easily results in problems or missing.
- It is hard to manage device go-online in a unified manner. Online statuses of devices cannot be tracked and thus administrators cannot learn about the online and running statuses of the devices on the network.
- Device extensibility is poor. Automatic deployment of extensible devices and even the extensible network is not supported.

To address the preceding problems, Orion Alpha A28X launches the ZAM solution to enable zero configuration of network devices, support plug-and-play, and realize unified and automatic deployment. The ZAM solution imposes few technical requirement on deployment personnel and helps reduce workload and costs. It avoids inconsistent deployment, supports unified deployment and management, tracks online statuses of devices, and simplifies operation, maintenance, and deployment of a massive number of devices.

Protocols and Standards

- RFC1541: DHCP standard

7.2 Application

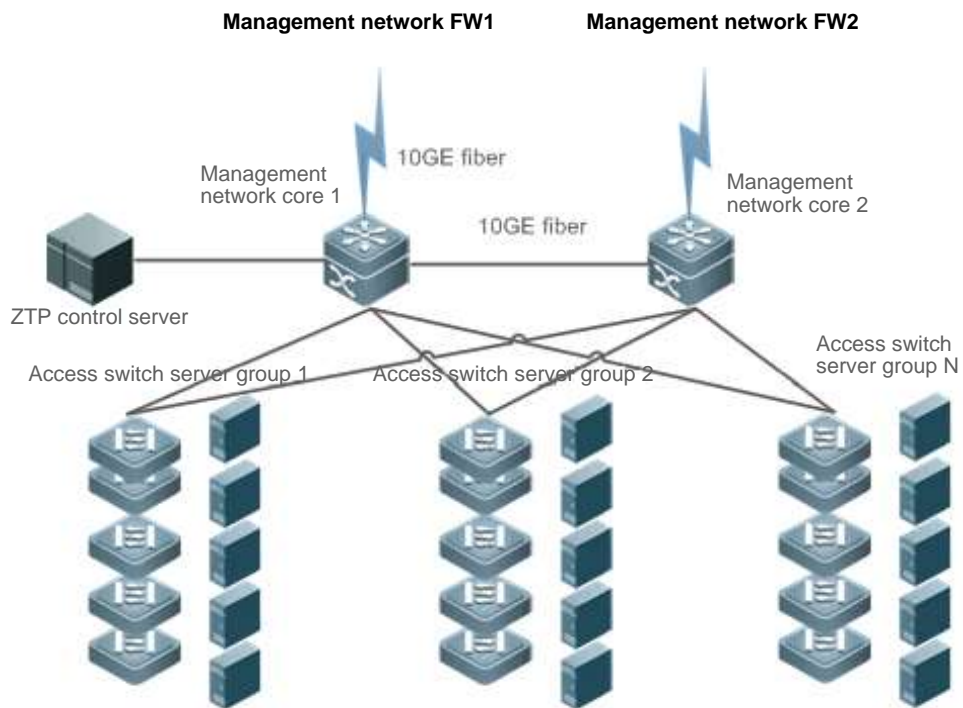
Application	Description
ZAM Automatic Deployment	Implements unified management on device deployment for go-online.

7.2.1 ZAM Automatic Deployment

Scenario

Figure 8-1 shows the network topology for ZAM solution. On the basis of the original network, a ZAM control server is added. DHCP and TFTP services are deployed on the ZAM server for managing and controlling device deployment in a unified manner for go-online, thus realizing unified management of all the deployed devices.

Figure 8-1



Deployment

- Deploy DHCP and TFTP services on the ZAM control server.
- Enable ZAM for access switch server groups 1, 2...N.

7.3 Features

Basic Concepts

↘ ZAM

Zero Automatic Manage

↘ IDC

Internet Data Center

↘ DHCP

Dynamic Host Configuration Protocol

↘ TFTP

Trivial File Transfer Protocol

Feature

Feature	Description
---------	-------------

Device Go-online via ZAM	Uses the ZAM solution to enable zero configuration of network devices.
--	--

7.3.1 Device Go-online via ZAM

The ZAM solution is implemented via three steps.

Step 1: A device without configurations accesses a network. The device applies for a fixed IP address from the ZAM control server via DHCP. The ZAM control server responds to the application by returning an IP address and the response also carries the TFTP server IP address and the configuration file name corresponding to the device. The device automatically applies the IP address, and resolves the TFTP server IP address and the configuration file name carried in the response.

Step 2: The device downloads the corresponding configuration file from the ZAM control server via TFTP (a TFTP server can be independently established).

Step 3: The device loads the configuration file.

The ZAM control server and device requiring go-online must meet the following requirements:

The ZAM control server must:

- Be capable of identifying a device requiring go-online, IP address of a specific device, the TFTP server IP address, and configuration file name of this device saved on the TFTP server.
- Be capable of allocating IP addresses to a device requiring go-online, that is, be capable of providing the DHCP service to pre-allocate an IP address, a TFTP server IP address, and a configuration file name, and enabling matching between the device and the preceding pre-allocated information.
- Provide the TFTP function and support configuration file download and storage if the TFTP function is deployed on the ZAM control server (recommended).

The device requiring go-online must:

- Be capable of automatically determining whether to go online via the ZAM solution after being powered on, that is, determining whether to go online without configuration via the ZAM solution.
- Be capable of applying to the DHCP server for an IP address, and obtaining the TFTP server IP address and configures file name.
- Be capable of downloading the specified configuration scripts from the TFTP server via TFTP.
- Be capable of automatically loading the configuration script.
- Provide a retry mechanism upon a ZAM deployment failure and provide a ZAM exit mechanism.

Working Principle

Device go-online via ZAM is divided into four stages:

↘ Initialization

At this stage, a device without configurations is powered on and accesses a network. After loading is completed, the device automatically pre-deploys the ZAM environment. The pre-deployment requirement is as follows:

- Use the MGMT port for ZTP management and retain all default configurations without extra operation.

↘ DHCP

After the pre-deployment, the device obtains the ZAM management IP address, TFTP server IP address, configuration file name of the device via DHCP. Requirements are as follows:

- On the MGMT port, enable DHCP.
- Trigger DHCP to obtain the ZAM management IP address. Add request identifiers of Option 67 (boot file name) and Option 150 (TFTP server IP address) to the requested parameter list.
- Resolve and deploy ZAM management IP address. Resolve Option 67 and Option 150 in the response.

↘ TFTP

Download the corresponding configuration script according to the configuration file name and TFTP server IP address obtained at the DHCP stage.

After the configuration script is downloaded successfully, execute the configuration script to download the corresponding configuration file or bin file from the TFTP server.

↘ Configuration loading

Load the configuration file or bin file obtained at the TFTP stage and restart the device.

Related Configuration


↘ Enabling ZAM

This function is enabled by default.

Run the ZAM command to enable or disable ZAM.

ZAM must be enabled on the device to implement automatic deployment via ZAM.

7.4 Configuration

Configuration	Description and Command
Configuring Device Go-online via ZAM	 (Mandatory) It is used to enable ZAM.
	<code>zam</code> Enables ZAM.

7.4.1 Configuring Device Go-online via ZAM

Configuration Effect

- Configure device go-online via ZAM, so that a device without configurations enters the go-online process and implements automatic deployment.

Notes

- Deploy a ZTP control server that supports device go-online via ZAM.

Configuration Steps

↳ Enabling ZAM

- Mandatory.
- Enable ZAM on each switch, unless otherwise specified.

Verification


Run the **show zam** command to check whether ZAM is enabled and to check configuration of the MGMT port.

Related Commands

↳ Enabling ZAM

Command	zam
Parameter	N/A
Description	
Command Mode	Global configuration mode
Usage Guide	Configure ZAM.

Configuration Example

 The following configuration example describes ZAM-related configuration only.

↳ Configuring Device Go-online via ZAM

Scenario	
Configuration Steps	Configure device go-online via ZAM as follows: <ul style="list-style-type: none">● Enable ZAM.
Online device via ZAM	<pre>A# configure terminal A(config)# zam A(config)# exit</pre>
Verification	<ul style="list-style-type: none">● Run the show zam command to display the current configuration and status of ZAM..
Orion Alpha A28X	<pre>Orion Alpha A28X#show zam ZTP state : disable ZTP status : Now is idle ZTP manage interface: Mgmt 0 Orion Alpha A28X#</pre>

Common Errors


- The network connection between a device requiring go-online and the ZAM control server is abnormal.
- The device requiring go-online is not in the zero-configuration state.

7.5 Monitoring

Displaying

Description	Command
Displays the current configuration and status of ZAM.	show zam

Debugging

 System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs the ZAM framework event.	debug zam

8 Configuring Monitoring

8.1 Overview

Intelligent monitoring is the intelligent hardware management of Orion Alpha A28X Network devices, including intelligent fan speed adjustment, and intelligent temperature monitoring. The intelligent monitoring performs the following tasks:

- Automatic fan speed adjustment based on ambient temperature changes
- Real-time temperature monitoring of boards to alert users

By default, the intelligent monitoring function is enabled after the device is powered on. It does not require any manual configuration.

Protocol Specification

N/A

8.2 Features

Basic Concepts

N/A

Features

Feature	Function
Intelligent Speed Adjustment of Fans	The rotating speed of fans is automatically adjusted as the temperature changes to address the heat dissipation needs of the system.
Intelligent Temperature Monitoring	The system automatically monitors the temperature. When the temperature exceeds a certain threshold, the system automatically generates an alarm.
Power monitoring	The system automatically monitors the power. When the power is insufficient or cannot be identified, the system automatically generates an alarm.

8.2.1 Intelligent Speed Adjustment of Fans

As the ambient temperature rises or drops, the fans automatically raise or reduce their rotating speed to dissipate heat and ensure that the noise is low.

Working Principle

The system automatically specifies default start rotating speed for the fans according to the current operating mode of the fans. As the ambient temperature rises or drops, the fans automatically raise or reduce their rotating speed to dissipate heat and ensure that the noise is low.

Verification

- Run the **show fan** command to display working status of all fans.
- Run the **show fan speed command** to display rotating speed.

8.2.2 Intelligent Temperature Monitoring

The system automatically monitors the temperature. When the temperature changes, the system automatically notifies users.

Working Principle

The system monitors the temperature once per minute. When the temperature exceeds a certain threshold, the system takes a certain action. The temperature and action vary with different devices.

Verification

Use the **show temperature** command to check the temperature thresholds and the current temperature of each line card.

8.2.3 Run the show temperature command to display system temperature. Power Monitoring

The system automatically monitors the power. When the power is insufficient or cannot be identified, the system automatically generates an alarm.

Working Principle

The system monitors the power once per minutes. If the system finds the power insufficient, the alarm LED becomes yellow and a Syslog message is generated. Once the alarm event is resolved, the system recovers. If the system cannot identify the inserted power, the alarm LED becomes yellow. After you remove the power, the system recovers.

Verification

Run the **show power** command to display power information.