System Management Configuration, Cisco Catalyst PON Series Switches

First Published: 2020-11-09

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **GPON System Parameters** 1

About GPON System Parameters 1

GPON System Optical Parameter Detection (SFP) 1

GPON Port Optical Threshold Alarm 1

GPON Uplink FEC 1

Optical link protection (not supported yet) 1

How to Configure GPON System Parameters 2

Configuring GPON Uplink FEC 2

Monitoring GPON Port Optical Parameter Diagnosis Information 3

Monitoring GPON System Performance Statistics 3

Configuration Examples for GPON System Parameters 3

Example: Viewing the GPON Port Optical Parameter Diagnosis Information 3

Example: Viewing the GPON System Performance Statistics 4

Example: Configuring the GPON Uplink FEC 6

CHAPTER 2 **System Maintenance** 7

Monitoring the System Status 7

Configuring The System Clock 8

Testing the Network Connection 9

Perform Route Tracking 9

Configuring a Banner 10

CHAPTER 3 **Configuring File Upload and File Download** 13

File Upload Overview 13

File Download Overview 13

How to Configure File Upload and File Download 14

Configuring File Upload 14
Configuring File Download 16
Configuration Examples for File Upload and File Download 18
Configuration Example for File Upload 18
Configuration Example for File Download 19

CHAPTER 4 Decompilation Configuration 21
Decompilation Configuration Overview 21
Basic Commands for Decompilation 21
Configuring the Switchover of File Execution Mode 22
Configuration Examples for Decompilation 23

CHAPTER 5 Configuring the Utilization Alarm 25
Utilization Alarm Overview 25
How to Configure the Utilization Alarm 26
Configuring the Port Utilization Alarm 26
Configuring the CPU Utilization Alarm 27
Configuration Examples for Utilization Alarm 27

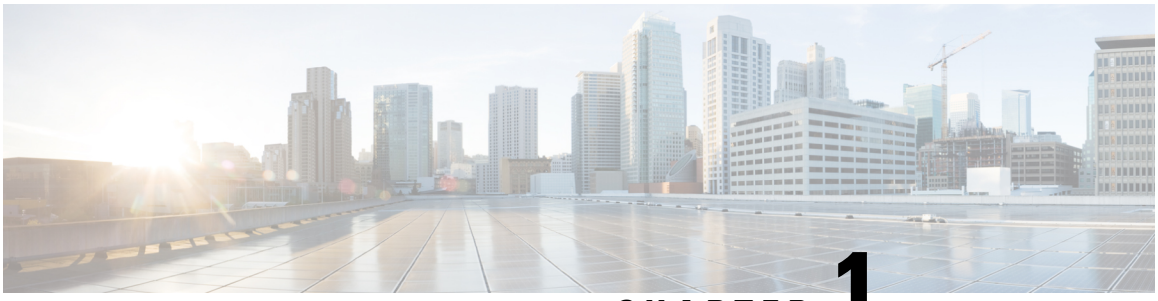
CHAPTER 6 System Log 29
System Log Overview 29
System Log Configuration 29
Enabling Syslog 29
Configuring the Log Serial Number 30
Configuring the Timestamp 31
Configuring the Log to Output to the Terminal 32
Configuring the Log to Output to the Buffer 33
Configuring the Log to Output to the Flash 34
Configuring the Log to Output to the External Server 35
Configuring the Log to Output to the SNMP Agent 36
Monitoring the System Log 37
Example: Syslog Configuration 38

CHAPTER 7 Configuring the System Clock 39

Overview for System Clock 39
Configuring the System Clock 39
Example: Configuring the System Clock 40

CHAPTER 8 Configuring SNTP Client 41
Simple Network Time Protocol Client 41
How to Configure SNTP Client 41
Enabling SNTP Client 41
Configuring the SNTP Client Mode 42
Configuring the SNTP Server Address 43
Configuring the Broadcast Transmission Delay 44
Configuring the Polling Interval 45
Configuring Timeout Retransmission 45
Configuring Legacy Server List 46
Configuring Authentication 47
Configuring System Clock Manually 48
Configuration Examples for SNTP Client 50

CHAPTER 9 Configuring Network Time Protocol 51
Information About Network Time Protocol 51
NTP Work Mode 52
How to Configure NTP 52
Enabling NTP 52
Configuring Reference Clocks 53
Configuring Client Mode 53
Configuring Peer Mode 54
Configuring Broadcast Mode 55
Configuring Multicast Mode 56
Configuring Access Control 57
Configuring Authentication 58
Disabling Incoming Packets 59
Configuring Maximum Number of Dynamic Sessions 59
Monitoring NTP 60
Example: Enabling Authentication and Configuring Broadcast Mode 61



CHAPTER 1

GPON System Parameters

- About GPON System Parameters, on page 1
- How to Configure GPON System Parameters, on page 2
- Configuration Examples for GPON System Parameters, on page 3

About GPON System Parameters

The PON system parameters allow you to to configure and manage the PON system.

GPON System Optical Parameter Detection (SFP)

GPON System Optical Parameter Detection provides information about optical parameter diagnosis and the GPON port optical parameter threshold. It is mainly used to query the alarm monitoring of GPON optical module parameters and optical module parameters in real time. When the optical line problem occurs in the GPON system, these functions can be used to confirm whether the GPON optical module works normally.

GPON Port Optical Threshold Alarm

GPON Port Optical Threshold Alarm allows you to configure the GPON port to receive and send optical parameter alarm thresholds. When the receiving and transmitting optical power of the GPON optical module is not within the threshold, an optical power alarm will be generated.

GPON Uplink FEC

By configuring the GPON Uplink FEC function, FEC is performed on data frames to increase the reliability of data transmission.

Optical link protection (not supported yet)

The optical line protection system is an automatic monitoring and protection system that is completely independent of the communication transmission system and is completely established on the physical link of the optical cable. When the working optical fiber loss increases and the communication quality is degraded or the working optical fiber is blocked, the system can automatically switch the optical communication transmission system from the working optical fiber to the standby optical fiber in real time, restore communication, and realize synchronous switching protection of the optical cable line, thereby greatly

improving The availability of fiber optic cable lines enhances the reliability of communication systems and guarantees service quality.

How to Configure GPON System Parameters

Configuring GPON Uplink FEC

To configure GPON uplink FEC, perform this procedure.

Before you begin

Modifying and activating the line profile entry will cause the ONT that is associated with the profile offline and online.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**deploy profile line** **Example:** `Device(config)# deploy profile line`	Enters line profile configuration mode.
Step 4	**aim** {*index_num* [**name** *name*] | **name** *name*} **Example:** `Device(deploy-profile-line)# aim 5`	Creates the line profile.
Step 5	[**no**] **local fec** **Example:** `Device(deploy-profile-line-5)# local fec`	Enables the ONT uplink FEC. Use the **no local fec** command to disable the ONT uplink FEC.
Step 6	**active** **Example:** `Device(deploy-profile-line-5)# active`	Activates the rule.

Monitoring GPON Port Optical Parameter Diagnosis Information

The commands in the following table can be used to monitor GPON port optical parameter diagnosis information.

Table 1: GPON Port Optical Parameter Diagnosis Information

Command	Purpose
show interface sfp [**gpon** *port_id*]	Displays information about GPON port optical parameter for real-time detection of SFP parameters, such as temperature, VCC, Tx bias Current, and Tx power, Rx power. *port_id*: The PON port ID .

Monitoring GPON System Performance Statistics

The commands in the following table can be used to monitor GPON system performance statistics.

Table 2: GPON Port System Performance Statistics

Command	Purpose
show ont statistics *ont_id* **traffic**	Displays information about ONT uplink and downlink data frame statistics
show ont statistics *ont_id* [**port** *port_id*]	Displays information about Ethernet port data frame statistics *port_id*: The ONT ethernet Port ID. The range is from 1 to 24. *ont_id*: The ONT ID.
show ont statistics *ont_id* [**gem** {**broadcast** | **multicast** | **unicast**}] *GEM port index*	Displays information about GEM port data frame statistics

Configuration Examples for GPON System Parameters

Example: Viewing the GPON Port Optical Parameter Diagnosis Information

The following example shows how to view the GPON port optical parameter diagnosis information.

```
Device> enable
Device# configure terminal
Device(config)# show interface sfp gpon 0/1
Port g0/1 :
Common information:
  Optical Module status         :Online
```

```
  Port state                    :On
  Transceiver Type              :SFP
  Module type                   :GPON
  Module sub-type               :Class B+
  Used type                     :ONT
  Connector Type                :SC
  WaveLength(nm)                :1490
  Transfer Distance(m)          :20000(9um)
  Digital Diagnostic Monitoring :YES
  VendorName                    :WTD
Manufacture information:
  Manu. Serial Number           :BP132701660779
  Manufacturing Date            :2013-07-09
  VendorName                    :WTD
  Vendor PN                     :RTXM167-522
  Vendor Revision               :1.0
Diagnostic information:
  Temperature( )                :31
  Voltage(V)                    :3.24
  Bias Current(mA)              :5.75
  Bias High Threshold(mA)       :70.00
  Bias Low  Threshold(mA)       :0.00
  RX Power(dBm)                 :-
  RX Power High Threshold(dBm)  :-10.0
  RX Power Low  Threshold(dBm)  :-27.9
  TX Power(dBm)                 :3.81
  TX Power High Threshold(dBm)  :5.00
  TX Power Low  Threshold(dBm)  :0.999
```

Example: Viewing the GPON System Performance Statistics

The following example shows the statistics of ONT uplink and downlink data frames.

```
Device> enable
Device# configure terminal
Device(config)# show ont statistics 0/1/1 traffic

Upstream frames          :   0
Upstream bytes           :   0
Downstream frames        :   0
Downstream bytes         :   0
Up traffic (kbps)        :   0
Down traffic (kbps)      :   0
```

The following example shows the Ethernet port data frame statistics.

```
Device> enable
Device# configure terminal
Device(config)# show ont statistics 0/1/1 port 1

Received frames                    :   0
Received unicast frames            :   0
Received multicast frames          :   0
Received broadcast frames          :   0

Received 64-byte frames            :   0
Received 65~127-byte frames        :   0
Received 128~255-byte frames       :   0
Received 256~511-byte frames       :   0
```

```
Received 512~1023-byte frames       :   0
Received 1024~1518-byte frames      :   0
Received undersize frames           :   0
Received oversize frames            :   0
Received fragments                  :   0
Received jabbers                    :   0
Received FCS error frames           :   0
Discard frames                      :   0
Received alignment error frames     :   0
MAC sub-layer received error frames :   0
PPPOE filtered frames               :   0
Buffer overflows on receive         :   0
Received bytes                      :   0

Sent frames                         :   0
Sent unicast frames                 :   0
Sent multicast frames               :   0
Sent broadcast frames               :   0

Carrier sense error frames          :   0
SQE test error messages             :   0
Sent single collision frames        :   0
Sent multiple collision frames      :   0
Sent excessive collision frames     :   0
Late collision frames               :   0
MAC sub-layer sent error frames     :   0
Buffer overflows on transmit        :   0
Sent bytes                          :   0
```

The following example shows the GEM Port data frame statistics.

```
Device> enable
Device# configure terminal
Device(config)# show ont statistics 0/1/1 gem unicast 1
Lost of frames        :   0
Received frames       :   0
Received blocks       :   0
Sent frames           :   0
Sent blocks           :   0
```

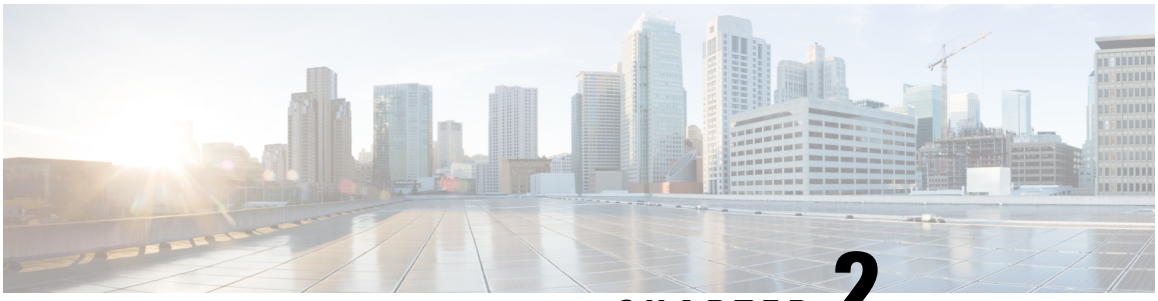
The following example shows the ONT data frame statistics

```
Device> enable
Device# configure terminal
Device(config)# show ont statistics overall 0/1/1
Received bytes              :   1759
Received Discard frames     :   0
Received error frames       :   0

Sent bytes                  :   0
Sent Discard frames         :   0
Sent error frames           :   0
Up rate (pps)               :   0
Down rate (pps)             :   0
Up traffic (kbps)           :   0
Down traffic (kbps)         :   0
Up bandwidth throughput     :   0%
Down bandwidth throughput   :   0%
```

Example: Configuring the GPON Uplink FEC

The following example shows how to configure the GPON uplink FEC.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile line
Device(deploy-profile-line)# aim 1
Device(deploy-profile-line-1)# local fec
Device(deploy-profile-line-1)# active
```



CHAPTER 2

System Maintenance

- Monitoring the System Status, on page 7
- Configuring The System Clock, on page 8
- Testing the Network Connection, on page 9
- Perform Route Tracking, on page 9
- Configuring a Banner, on page 10

Monitoring the System Status

Use the following commands in privileged EXEC mode to monitor the system status.

Note Forwarding database table is an Address Resolution Protocol (ARP) table which is issued to the three-tier switching chip, that is a hardware ARP table. The Layer 2 device does not have this entry.

Command	Purpose
show version	Displays version information.
show system	Displays system information.
show memory	Displays memory information.
show cpu-utilization	Displays CPU utilization.
show cpu-statistics ethernet *port-num*	Displays the statistics of CPU packets, according to port statistics.
show cpu-classification interface ethernet *port-num*	Displays the statistics of CPU packet types.
show username	Displays the information of the administrator who can log in to the system.
show users	Displays the information of the administrator who has logged in to the system.
show clock	Displays the system clock.

Command	Purpose
show ip fdb	Displays all forwarding database tables.
show ip fdb *ip*	Displays the forwarding database table of the specified IP address.
show ip fdb *ip mask*	Displays the forwarding database table of the specified IP address segment.

Configuring The System Clock

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **hostname** *host-name*
4. **no hostname** *host-name*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**hostname** *host-name* **Example:** `Device(config)# hostname host1`	Sets the system command line interface prompt.
Step 4	**no hostname** *host-name* **Example:** `Device(config)# no hostname host1`	(Optional) Cancels the system command line interface prompt.
Step 5	**end** **Example:** `Device(config)# end`	(Optional) Exits the global configuration mode and returns to privileged EXEC mode.

Testing the Network Connection

SUMMARY STEPS

1. **enable**
2. **ping** {**-i** *ttl* | **-l** *packet length* | **-n** *packet number* | **-s** *source ip* | **-t** *timeout*} *ip_host_address*
3. **ping6** {**-a** *ipv6 source address* | **-c** *count* | **-h** *hop limit* | **-s** *packet length* | **-t** | **-w** *time out*} *ipv6_host_address*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**ping** {**-i** *ttl* | **-l** *packet length* | **-n** *packet number* | **-s** *source ip* | **-t** *timeout*} *ip_host_address* **Example:** `Device# ping 10.1.1.10`	Runs the ping command. • **-i** *ttl*: TTL value to be sent. • **-l** *packet length*: Length of the sent packet, in bytes. • **-n** *packet number*: Number of sent packets. • **-s** *source ip*: Source IP address of the sent packet. • **-t** *timeout*: The timeout to wait for the response after sending the packet, in seconds.
Step 3	**ping6** {**-a** *ipv6 source address* | **-c** *count* | **-h** *hop limit* | **-s** *packet length* | **-t** | **-w** *time out*} *ipv6_host_address* **Example:** `Device# ping6 2001:DB8::10`	Runs the ping command. • **-a** *ipv6 source address*: The source IPV6 address to be sent. • **-c** *count*: Number of sent packets. • **-h** *hop limit*: Hop limit. • **-s** *packet length*: Length of the sent packet, in bytes. • **-w** *time out*: The timeout to wait for the response after sending the packet, in seconds.

Perform Route Tracking

Tracert is mainly used for route tracking and checking network connections. Run the following configurations in privileged EXEC user mode.

SUMMARY STEPS

1. **enable**

2. **tracert** {**-u** | **-c**} {**-p** *udpport* | **-f** *first_ttl* | **-h** *maximum_hops* | **-w** *time_out* | **-t** *timeout*} *ip_host_address*
3. **tracert6** {**-c** | **-h** *maximum_hops* | **-w** *time_out* } *ipv6_host_address*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**tracert** {**-u**	**-c**} {**-p** *udpport*	**-f** *first_ttl*	**-h** *maximum_hops*	**-w** *time_out*	**-t** *timeout*} *ip_host_address* **Example:** `Device# tracert -c 10.1.1.10`	Performs IPv4 route tracking. • **-u**: Sends UDP packets. • **-c**: Sends ICMP echo packets. This is the default. • **-p** *udpport*: Destination port address for sending UDP packets. It ranges from 1 to 65535. The default port is 62929. • **-f** *first_ttl*: Initial TTL value of the sent packets, in the range of 1 to 255. The default is 1. • **-h** *maximum_hops*: Maximum TTL value of the sent packets, in the range of 1 to 255. The default is 30. • **-w** *time_out*: The timeout to wait for the response after sending the packet, in the range of 10 to 60, in seconds. The default value is 10 seconds. • *ip_host_address*: Destination IP host address.
Step 3	**tracert6** {**-c**	**-h** *maximum_hops*	**-w** *time_out* } *ipv6_host_address* **Example:** `Device# tracert6 -c 333 -h 33 -w 22 2001:DB8::1`	Performs IPv6 route tracking. • **-c**: Sends ICMP echo packets. This is the default. • **-f** *first_ttl*: Initial TTL value of the sent packets, in the range of 1 to 255. The default is 1. • **-w** *time_out*: The timeout to wait for the response after sending the packet, in the range of 10 to 60, in seconds. The default value is 10 seconds. • *ip6_host_address*: Destination IPv6 host address.

Configuring a Banner

After setting the banner, the manufacturer information will appear when the device is logged in.

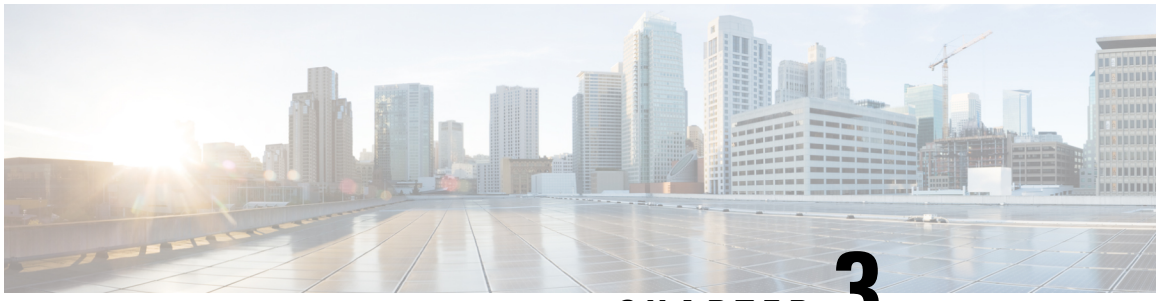
SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **banner** {**line1** | **line2** | **line3** | **line4**} *banner_string*
4. **screen-rows per-page** *number*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**banner** {**line1**	**line2**	**line3**	**line4**} *banner_string* **Example:** `Device(config)# banner line3 hello`	Customizes the selected line of the banner. The banner string ranges from 1 to 78.
Step 4	**screen-rows per-page** *number* **Example:** `Device(config)# screen-rows per-page 20`	(Optional) Enables the banner function and displays device information. You can display up to 25 lines of information at one time by default when viewing device information. The range of per-page is 0 to 256, and 0 means that all information is displayed.
Step 5	**end** **Example:** `Device(config)# end`	(Optional) Exits the global configuration mode and returns to privileged EXEC mode.



CHAPTER 3

Configuring File Upload and File Download

- File Upload Overview, on page 13
- File Download Overview, on page 13
- How to Configure File Upload and File Download, on page 14
- Configuration Examples for File Upload and File Download, on page 18

File Upload Overview

File uploading refers to uploading files in DUT flash to external file servers, such as host files, configuration files, SSH key files, and log files in the upgrade file for analysis, backup, or migration to other compatible devices.

It is recommended that the uploaded file name is the same suffix as the file download:

File Type	Suffix
Host File	.arj
Bootrom file	.bin
Configuration file	.txt
SSH key file	.txt

The following upload tools are supported: tftp and ftp.

File Download Overview

File download is to download files from the external to the DUT's flash, such as the upgrade files (host file, bootrom file), the configuration file, and the SSH key file.

The suffix of the files must be the following:

File Type	Suffix
Host File	.arj
Bootrom file	.bin

File Type	Suffix
Configuration file	.txt
SSH key file	.txt

The following download tools are supported: xmodem, tftp, and ftp.

When using the xmodem tool, after entering the command, select **Send** -> **Send File** in the **HyperTerminal** menu. In the **Send File** dialog box, enter the full path and file name of the file in the **File Name** field. Select **Xmodem** from the **Protocol** drop-down list, and then click **Send**.

When an external file is downloaded to the DUT, it is saved in the flash memory and does not take effect immediately. You must use the related configuration commands. After upgrading the host and bootrom, restart the DUT. When you download the configuration file, it will overwrite the original configuration file in flash. You must use the downloaded configuration file in the privileged EXEC mode with the **copy startup-config running-config**.

Refer to the SSH module user manual for key usage.

How to Configure File Upload and File Download

Configuring File Upload

To upload a file, perform the following steps:

SUMMARY STEPS

1. **enable**
2. Use either ftp: or tftp: to upload a file:
   - **upload application ftp** { **inet** | **inet6** }*ftp-server-ip-address file-name ftp-username ftp-password*
   - **upload application tftp** { **inet** | **inet6** }*tftp-server-ip-address file-name*
3. Use either ftp: or tftp: to upload a file:
   - **upload logging ftp** { **inet** | **inet6** }*ftp-server-ip-address file-name ftp-username ftp-password*
   - **upload logging tftp** { **inet** | **inet6** }*tftp-server-ip-address file-name*
4. **copy running-config startup-config**
5. Use either ftp: or tftp: to upload a file:
   - **upload configuration ftp** { **inet** | **inet6** }*ftp-server-ip-address file-name ftp-username ftp-password*
   - **upload configuration tftp** { **inet** | **inet6** }*tftp-server-ip-address file-name*
6. Use either ftp: or tftp: to upload a file:
   - **upload automatically configuration ftp** { **inet** | **inet6** }*ftp-server-ip-address file-name ftp-username ftp-password* **per hours** *hours* **minutes** *minutes*
   - **upload automatically configuration tftp** { **inet** | **inet6** }*tftp-server-ip-address file-name* **per hours** *hours* **minutes** *minutes*
7. Use either ftp: or tftp: to upload a file:

- **upload keyfile** { **private** | **public** }**ftp**{ **inet** | **inet6** }*ftp-server-ip-address file-name ftp-username ftp-password*
- **upload keyfile** { **private** | **public** }**tftp**{ **inet** | **inet6** }*tftp-server-ip-address file-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	Use either ftp: or tftp: to upload a file: • **upload application ftp** { **inet** | **inet6** }*ftp-server-ip-address file-name ftp-username ftp-password* • **upload application tftp** { **inet** | **inet6** }*tftp-server-ip-address file-name* **Example:** `Device# upload application tftp inet 10.23.13.1 host.arj`	Uploads the host file.
Step 3	Use either ftp: or tftp: to upload a file: • **upload logging ftp** { **inet** | **inet6** }*ftp-server-ip-address file-name ftp-username ftp-password* • **upload logging tftp** { **inet** | **inet6** }*tftp-server-ip-address file-name* **Example:** `Device# upload logging tftp inet 10.23.13.1 log.arj`	Uploads the log file.
Step 4	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves the current configuration to flash.
Step 5	Use either ftp: or tftp: to upload a file: • **upload configuration ftp** { **inet** | **inet6** }*ftp-server-ip-address file-name ftp-username ftp-password* • **upload configuration tftp** { **inet** | **inet6** }*tftp-server-ip-address file-name* **Example:** `Device# upload configuration tftp inet 10.23.13.1 config.txt`	Uploads the configuration file.

	Command or Action	Purpose
Step 6	Use either ftp: or tftp: to upload a file: • **upload automatically configuration ftp { inet | inet6 }***ftp-server-ip-address file-name ftp-username ftp-password* **per hours** *hours* **minutes** *minutes* • **upload automatically configuration tftp { inet | inet6 }***tftp-server-ip-address file-name* **per hours** *hours* **minutes** *minutes* **Example:** `Device# upload automatically configuration tftp inet 10.23.13.1 config2.txt per hours 20 minutes 30`	Automatically uploads the configuration file.
Step 7	Use either ftp: or tftp: to upload a file: • **upload keyfile { private | public }ftp{ inet | inet6 }***ftp-server-ip-address file-name ftp-username ftp-password* • **upload keyfile { private | public }tftp{ inet | inet6 }***tftp-server-ip-address file-name* **Example:** `Device# upload keyfile public tftp inet 10.23.13.1 ssh.txt`	Uploads the SSH key file.

Configuring File Download

To download a file, perform the following steps:

SUMMARY STEPS

1. **enable**
2. Use either ftp:, tftp:, or xmodem: to download a file:
   - **load application ftp { inet | inet6 }***ftp-server-ip-address file-name ftp-username ftp-password*
   - **load application tftp { inet | inet6 }***tftp-server-ip-address file-name*
   - **load application xmodem**
3. Use either ftp:, tftp:, or xmodem: to download a file:
   - **load whole-bootrom ftp { inet | inet6 }***ftp-server-ip-address file-name ftp-username ftp-password*
   - **load whole-bootrom tftp { inet | inet6 }***tftp-server-ip-address file-name*
   - **load whole-bootrom xmodem**
4. Use either ftp: or tftp: to download a file:
   - **load ont-image ftp { inet | inet6 }***ftp-server-ip-address file-name ftp-username ftp-password*
   - **load ont-image tftp { inet | inet6 }***tftp-server-ip-address file-name*
5. **load epld ftp { inet | inet6 }***ftp-server-ip-address file-name ftp-username ftp-password*
6. Use either ftp:, tftp:, or xmodem: to download a file:

- **load configuration ftp { inet | inet6 }***ftp-server-ip-address file-name ftp-username ftp-password*
- **load configuration tftp { inet | inet6 }***tftp-server-ip-address file-name*
- **load configuration xmodem**

7. Use either ftp: or tftp: to download a file:
   - **load keyfile { private | public }ftp{ inet | inet6 }***ftp-server-ip-address file-name ftp-username ftp-password*
   - **load keyfile { private | public }tftp{ inet | inet6 }***tftp-server-ip-address file-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	Use either ftp:, tftp:, or xmodem: to download a file: • **load application ftp { inet | inet6 }***ftp-server-ip-address file-name ftp-username ftp-password* • **load application tftp { inet | inet6 }***tftp-server-ip-address file-name* • **load application xmodem** **Example:** `Device# load application tftp inet 10.23.13.1 host.arj`	Upgrades the host file.
Step 3	Use either ftp:, tftp:, or xmodem: to download a file: • **load whole-bootrom ftp { inet | inet6 }***ftp-server-ip-address file-name ftp-username ftp-password* • **load whole-bootrom tftp { inet | inet6 }***tftp-server-ip-address file-name* • **load whole-bootrom xmodem** **Example:** `Device# load whole-bootrom tftp inet 10.23.13.1 bootrom1.bin`	Upgrades the bootrom file.
Step 4	Use either ftp: or tftp: to download a file: • **load ont-image ftp { inet | inet6 }***ftp-server-ip-address file-name ftp-username ftp-password* • **load ont-image tftp { inet | inet6 }***tftp-server-ip-address file-name* **Example:**	Upgrades the ont-image file.

	Command or Action	Purpose
	`Device# load ont-image tftp inet 10.23.13.1 ont1.image`	
Step 5	**load epld ftp** { **inet** | **inet6** }*ftp-server-ip-address file-name ftp-username ftp-password* **Example:** `Device# load epld tftp inet 10.23.13.1 epld1.epld`	Upgrades the epld file.
Step 6	Use either ftp:, tftp:, or xmodem: to download a file: • **load configuration ftp** { **inet** | **inet6** }*ftp-server-ip-address file-name ftp-username ftp-password* • **load configuration tftp** { **inet** | **inet6** }*tftp-server-ip-address file-name* • **load configuration xmodem** **Example:** `Device# load configuration tftp inet 10.23.13.1 config.txt`	Downloads the configuration file.
Step 7	Use either ftp: or tftp: to download a file: • **load keyfile** { **private** | **public** }**ftp**{ **inet** | **inet6** }*ftp-server-ip-address file-name ftp-username ftp-password* • **load keyfile** { **private** | **public** }**tftp**{ **inet** | **inet6** }*tftp-server-ip-address file-name* **Example:** `Device# load keyfile public tftp inet 10.23.13.1 ssh.txt`	Downloads the SSH key file.

Configuration Examples for File Upload and File Download

Configuration Example for File Upload

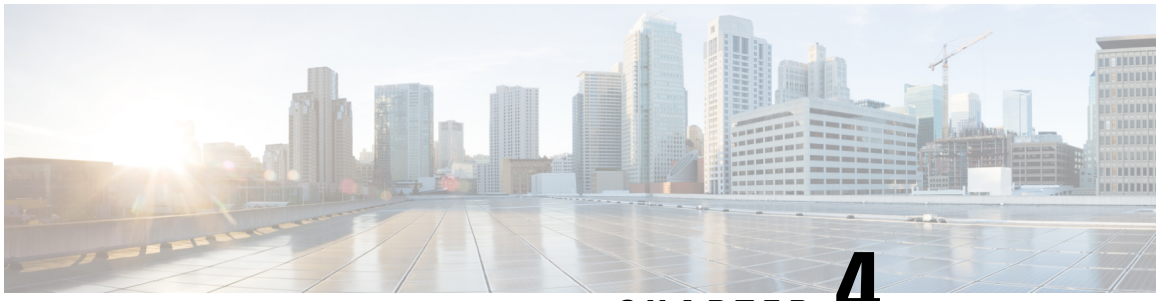
The following example shows how to upload the host file and the configuration file:

```
Device# upload application tftp 192.168.1.99 host.arj
Uploading APP file via TFTP...
Upload APP file via TFTP successfully.

Device# upload configuration tftp 192.168.1.99 text.txt
Uploading config file via TFTP...
Upload config file via TFTP successfully.
```

Configuration Example for File Download

The following example shows how to download the host file and the bootrom file:

```
Device# load application tftp 192.168.1.99 host.arj
Downloading application via TFTP...
Download application via TFTP successfully.

Device# load whole-bootrom tftp 192.168.1.99 bootrom_rom.bin
```



CHAPTER 4

Decompilation Configuration

- Decompilation Configuration Overview, on page 21
- Basic Commands for Decompilation, on page 21
- Configuring the Switchover of File Execution Mode, on page 22
- Configuration Examples for Decompilation, on page 23

Decompilation Configuration Overview

Device configuration can be performed in two ways. The first is called the default configuration, that does not require user configuration. After the DUT is powered on for the first time, or after the startup configuration is cleared, the existing configurations, such as the admin user, ensure that the DUT satisfies the simple usage environment. The second configuration is to increase or modify the configuration, such as creating vlan 2, modifying pvid = 2.

Device configuration can be classified into three types based on the method of saving:

- Temporary Cache Configuration - Also called Current Running configuration, this configuration does not exist after the DUT restarts.
- Startup Configuration - This configuration can be loaded either automatically or manually after the DUT is restarted.
- Flash Configuration - In this configuration, a small number of particularly important configurations will be saved directly to the flash: such as stacking configuration, user name configuration; stacking configuration will not enter the decompilation, that is, it will not be displayed in the **show running-config** command output, it can only be displayed by the **show module** command. User name configuration will enter the decompilation, that is, it will be displayed in the **show running-config** command output, as well as by the **show module** command. The configuration in flash is permanent and does not need to be saved with commands. To delete the flash configuration, use the **no** form of the corresponding command in the module.

Basic Commands for Decompilation

Command	Description
show running-config [*module* | **interface ethernet** *port-num*]	Displays the decompilation of the current configuration.

Command	Description
show startup-config [*module*]	Displays the startup configuration.
copy running-config startup-config	Saves the current configuration to the startup configuration.
copy startup-config running-config	Loads the boot configuration at the command line.
clear startup-config	Clears the startup configuration.

- Loading the startup configuration at reboot:

  During the restart process, the default is to load the configuration automatically after 6 seconds. Press **Enter** according to the prompt message to load immediately.

  To not load the startup configuration at reboot, press **Ctrl + C** according to the prompt message during the restart process.

Configuring the Switchover of File Execution Mode

You can change the execution mode of the configuration file through the command line interface. The system-saved configuration file can be executed in both interruptible and non-interruptible modes. When an error is encountered while executing the configuration file, execution in the interruptible mode stops immediately and echoes the error. In non-interruptible mode, execution is not stopped, the error is echoed, and the configuration file continues execution. The default is non-interruptible mode.

To configure the file execution mode switchover, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **buildrun mode stop**
3. **buildrun mode continue**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**buildrun mode stop** **Example:** `Device# buildrun mode stop`	Sets the execution mode to interruptible.
Step 3	**buildrun mode continue** **Example:** `Device# buildrun mode continue`	Sets the execution mode to non-interruptible.

Configuration Examples for Decompilation

The following example shows how to view the decompilation of the current configuration:

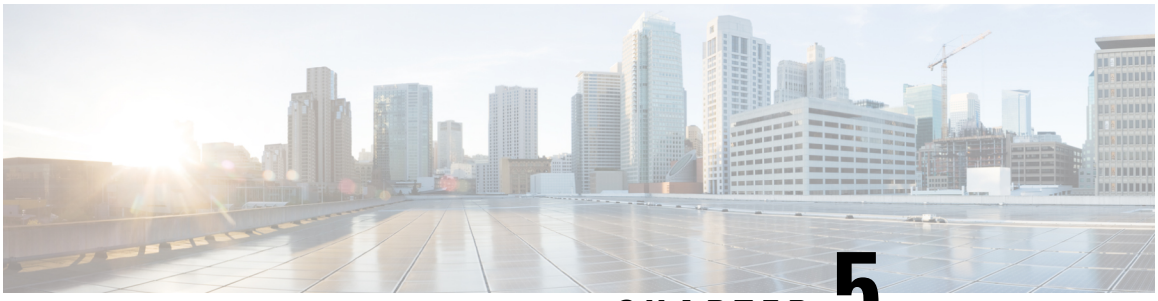
```
Device# show running-config
!LanSwitch BuildRun
enable
configure terminal
![DEVICE]
interface ethernet 0/1
exit
interface ethernet 0/2
exit
interface ethernet 0/3
exit
interface ethernet 0/4
exit
interface ethernet 0/5
exit
interface ethernet 0/6
exit
interface ethernet 0/7
exit
interface ethernet 0/8
exit
.....
```

The following example shows how to save the current configuration to the startup configuration:

```
Device# copy running-config startup-config
Startup config in flash will be updated, are you sure(y/n)? [n]y
Building, please wait...
Update startup config successfully.
```

The following example shows how to use the startup configuration:

```
Device# copy startup-config running-config
Running config will be updated, are you sure(y/n)? [n]y
Start to load startup-config, please wait for a while ...
Load successfully.
```



CHAPTER 5

Configuring the Utilization Alarm

- Utilization Alarm Overview, on page 25
- How to Configure the Utilization Alarm, on page 26
- Configuration Examples for Utilization Alarm, on page 27

Utilization Alarm Overview

The device utilization alarm function is used to monitor the bandwidth of the device, CPU resource consumption, and generate alarm notification in the event of congestion, so that the administrator can keep abreast of the network and equipment running.

The port utilization alarm function can set two trigger alarm thresholds:

- Exceed: When the port bandwidth utilization equals or exceeds the **exceed value**, a congestion alarm is triggered.
- Normal: When the port bandwidth utilization falls below the **normal value**, the recovered alarm is triggered.

The CPU utilization alarm function can also set two trigger alarm thresholds:

- Busy: When the CPU utilization equals or exceeds the **busy value**, an alarm is triggered, indicating that the CPU is busy.
- Unbusy: When the CPU utilization is equal to or lower than the **unbusy value**, an alarm is triggered, indicating that the CPU is idle.

Note The alarm information is moved as output to the Syslog by default. To show output in the terminal, enable the command.

How to Configure the Utilization Alarm

Configuring the Port Utilization Alarm

To configure the port utilization alarm, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **alarm all-packets**
4. **interface** *port-number*
5. **alarm all-packets**
6. **alarm all-packets threshold exceed** *exceed-value* **normal** *normal-value*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**alarm all-packets** **Example:** `Device(config)# alarm all-packets`	Enables alarms on all ports. Use the **no** form of the command to disable alarms on all ports.
Step 4	**interface** *port-number* **Example:** `Device(config)# interface gpon 0/1`	Enters the port configuration mode.
Step 5	**alarm all-packets** **Example:** `Device(config-if-gpon-0/1)# alarm all-packets`	Enables port alarm. Use the **no** form of the command to disable port alarm.
Step 6	**alarm all-packets threshold exceed** *exceed-value* **normal** *normal-value* **Example:** `Device(config-if-gpon-0/1)# alarm all-packets threshold exceed 34 normal 4`	Configures port threshold information.

Configuring the CPU Utilization Alarm

To configure the CPU utilization alarm, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **alarm cpu**
4. **alarm cpu threshold** {[**busy** *busy-value*] | [**unbusy***unbusy-value*]}
5. **show alarm cpu**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**alarm cpu** **Example:** `Device(config)# alarm all-packets`	Enables CPU alarm. Use the **no** form of the command to disable CPU alarm.
Step 4	**alarm cpu threshold** {[**busy** *busy-value*]	[**unbusy***unbusy-value*]} **Example:** `Device(config)# alarm cpu threshold busy 63 normal 20`	Configures port threshold information.
Step 5	**show alarm cpu** **Example:** `Device(config)# show alarm cpu`	(Optional) Displays the CPU alarm information.

Configuration Examples for Utilization Alarm

The following example shows how to configure the port alarm:

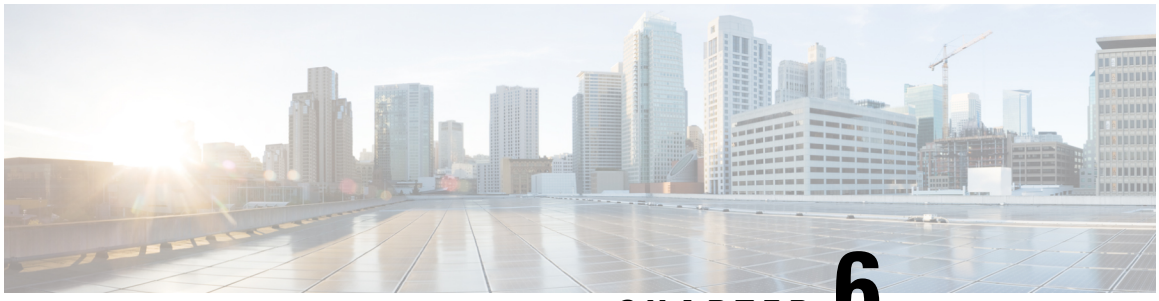
```
Device> enable
Device# configure terminal
Device(config)# alarm all-packets
Device(config)# interface ethernet 1/2
Device(config-if-ethernet-1/2)# alarm all-packets
Device(config-if-ethernet-1/2)# alarm all-packets threshold exceed 50 normal 40
```

The following example shows how to configure the CPU alarm:

```
Device> enable
Device# configure terminal
Device(config)# alarm cpu
Device(config)# alarm cpu threshold busy 90 unbusy 85
```

The following is a sample output of the **show alarm cpu** command:

```
Device(config)# show alarm cpu
CPU status alarm        : enable
CPU busy threshold(%)   : 90
CPU unbusy threshold(%) : 85
CPU status              : unbusy
```



CHAPTER 6

System Log

- System Log Overview, on page 29
- System Log Configuration, on page 29
- Monitoring the System Log, on page 37
- Example: Syslog Configuration, on page 38

System Log Overview

Syslog is the system information center, to complete the unified processing and output of information.

The other modules in the system will send the output information to Syslog. Syslog determines the output format of the information according to the configuration of the user and outputs the information to the specified display device according to the information switching and filtering rules of each output direction configured by the user.

With the Syslog information producer, which is each module of output information, you do not need to export information to the console, Telnet terminal, or log host (Syslog server). You only need to output the information to Syslog. By configuring the appropriate filtering rules, information consumers, which are console, Telnet terminal, history buffer, log host and SNMP agent, a user can choose the desired information and discard unwanted information.

System Log Configuration

Enabling Syslog

Note The logging function is enabled by default and stored in the buffer.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **logging**

4. **show logging**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**logging** **Example:** `Device(config)# logging`	Enables log function.
Step 4	**show logging** **Example:** `Device(config)# show logging`	(Optional) Displays the configuration information.
Step 5	**end** **Example:** `Device(config)# end`	(Optional) Exits the global configuration mode and returns to privileged EXEC mode.

Configuring the Log Serial Number

Note The logging function is enabled by default.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **logging sequence-numbers**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**logging sequence-numbers** **Example:** `Device(config)# logging sequence-numbers`	Enables the log serial number.
Step 4	**end** **Example:** `Device(config)# end`	(Optional) Exits the global configuration mode and returns to privileged EXEC mode.

Configuring the Timestamp

Note There is no separate timestamp switch. There are three timestamp types:

- notime: do not show the time
- uptime: show the boot time
- datetime: show the date and time

The default is uptime.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **logging timestamps** {**notime** | **uptime** | **datetime**}
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**logging timestamps** {**notime** | **uptime** | **datetime**} **Example:** `Device(config)# logging timestamps datetime`	Configures the timestamp type.
Step 4	**end** **Example:** `Device(config)# end`	(Optional) Exits the global configuration mode and returns to privileged EXEC mode.

Configuring the Log to Output to the Terminal

In privileged EXEC mode, configure the log to output to the terminal device. In global configuration mode, you can configure information display and filtering rules. By default, the device logs do not output to the terminal, but output to the buffer. There is a slight difference between the command for the serial terminal and the Telnet or SSH terminal.

Note

- Log output to the terminal: In the serial console, the default configuration is terminal monitor; in other terminal console, the default is no terminal monitor.
- Log information display: In the non-console terminal configuration, only affect this landing of the current terminal, the other terminals, the next landing of the current terminal is invalid.
- *monitor-num* is 0 for the console, and 1 to 5 for Telnet and SSH terminals.
- Output log default rule: All modules, log level 0-5,7. Deleting the filtering rule restores the default rule.

SUMMARY STEPS

1. **enable**
2. **terminal monitor**
3. **configure terminal**
4. **logging monitor** {**all** | *monitor-num*} [*level_value* | **level-list** *level_value* | **none**]
5. **show logging filter monitor** *monitor-num*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**terminal monitor** **Example:**	Enables output to the terminal.

	Command or Action	Purpose
	`Device# terminal monitor`	
Step 3	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 4	**logging monitor** {**all** | *monitor-num*} [*level_value* | **level-list** *level_value* | **none**] **Example:** `Device(config)# logging monitor all 3`	(Optional) Enables log display and configures the filtering rules.
Step 5	**show logging filter monitor** *monitor-num* **Example:** `Device(config)# show logging filter monitor 3`	(Optional) Displays the filtering rules.
Step 6	**end** **Example:** `Device(config)# end`	(Optional) Exits the global configuration mode and returns to privileged EXEC mode.

Configuring the Log to Output to the Buffer

Note The default is log output to buffer. The default rule is to output all modules and logs at the level 0-6. Deleting the filtering rule restores the default rule.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **logging buffered** [*level_value* | **level-list** *level_value* | **none**]
4. **show logging filter buffered**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**logging buffered** [*level_value* | **level-list** *level_value* | **none**] **Example:** `Device(config)# logging buffered 3`	Enables output to buffer and configures the filtering rules.
Step 4	**show logging filter buffered** **Example:** `Device(config)# show logging filter buffered`	(Optional) Displays the filtering rules.
Step 5	**end** **Example:** `Device(config)# end`	(Optional) Exits the global configuration mode and returns to privileged EXEC mode.

Configuring the Log to Output to the Flash

In global configuration mode, you can configure Syslog to save to Flash, which is not saved in flash memory by default.

Note

- When the log is output to flash, the default rule is to output all modules and the log level is 0-5. Deleting the filtering rule restores the default rules.
- When the log is output to flash, the default cycle is 30M. By default, 100 logs are saved at one time.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **logging flash** [*level_value* | **interval** *interval-value* | **level-list** *level_value* | **msg-number** *msg-num-value* | **none**]
4. **show logging filter flash**
5. **show logging flash**[[*level_value* | **count** | **level-list** *level_value*] **module** *module-name*]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**logging flash** [*level_value* | **interval** *interval-value* | **level-list** *level_value* | **msg-number** *msg-num-value* | **none**] **Example:** `Device(config)# logging flash msg-number 220`	Enables output to flash and configures the filtering rules.
Step 4	**show logging filter flash** **Example:** `Device(config)# show logging filter flash`	(Optional) Displays the filtering rules.
Step 5	**show logging flash**[[*level_value* | **count** | **level-list** *level_value*] **module** *module-name*] **Example:** `Device(config)# show logging flash`	(Optional) Displays the log information in the flash.
Step 6	**end** **Example:** `Device(config)# end`	(Optional) Exits the global configuration mode and returns to privileged EXEC mode.

Configuring the Log to Output to the External Server

Configure the specified server address for log output, information output switch, filtering rule, and logging tool and source address in global configuration mode.

Note

- The sip of log messages must be the interface of the device. The Layer 3 device uses the IP address of the corresponding interface of the log server by default. The Layer 2 device automatically uses the system IP and does not need to be configured.
- The default logging tool name uses localuse7.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **logging** *ip-address*
4. **logging host** {*ip-address* | **all**} [*level_value* | **level-list** *level_value* | **none**]
5. **logging facility** {**clock1** | **clock2** | **ftp** | **kernel** | **lineprinter** | **localuse0** | **localuse1** | **localuse2** | **localuse3** | **localuse4** | **localuse5** | **localuse6** | **localuse7** | **logalert** | **logaudit** | **mail** | **networknews** | **ntp** | **security1** | **security2** | **syslogd** | **system** | **userlevel** | **uucp**}
6. **logging source** *ip-address*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**logging** *ip-address* **Example:** `Device(config)# logging 10.1.1.10`	Configures the log server.
Step 4	**logging host** {*ip-address* | **all**} [*level_value* | **level-list** *level_value* | **none**] **Example:** `Device(config)# logging host all`	Enables the log server and configures the filtering rules.
Step 5	**logging facility** {**clock1** | **clock2** | **ftp** | **kernel** | **lineprinter** | **localuse0** | **localuse1** | **localuse2** | **localuse3** | **localuse4** | **localuse5** | **localuse6** | **localuse7** | **logalert** | **logaudit** | **mail** | **networknews** | **ntp** | **security1** | **security2** | **syslogd** | **system** | **userlevel** | **uucp**} **Example:** `Device(config)# logging facility log1`	(Optional) Configures the logging tool name.
Step 6	**logging source** *ip-address* **Example:** `Device(config)# logging source 10.1.1.11`	(Optional) Configures the sip for log packet.
Step 7	**end** **Example:** `Device(config)# end`	(Optional) Exits the global configuration mode and returns to privileged EXEC mode.

Configuring the Log to Output to the SNMP Agent

Configure Syslog output to the SNMP agent in global configuration mode. To send Syslog messages to SNMP Workstation in trap messages, you must also configure the Trap host address. Refer to the SNMP configuration instructions.

By default, logs are not set to output to the SNMP agent.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **logging snmp-agent**
4. **logging snmp-agent** {*level_value* | **level-list** *level_value* | **none**]
5. **show logging filter snmp-agent**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**logging snmp-agent** **Example:** `Device(config)# logging 10.1.1.10`	Enables log output to the SNMP agent.
Step 4	**logging snmp-agent** {*level_value* | **level-list** *level_value* | **none**] **Example:** `Device(config)# logging snmp-agent none`	(Optional) Configures the filtering rules.
Step 5	**show logging filter snmp-agent** **Example:** `Device(config)# show logging filter snmp-agent`	(Optional) Displays the filtering rules.
Step 6	**end** **Example:** `Device(config)# end`	(Optional) Exits the global configuration mode and returns to privileged EXEC mode.

Monitoring the System Log

In the global configuration mode, you can configure the debugging function to print the debugging information of the corresponding module. By default, debugging information of all modules is disabled.

Command	Purpose
debug {**all** | *module_name*}	Enables debugging function.
show debug	Displays the configuration information.

Example: Syslog Configuration

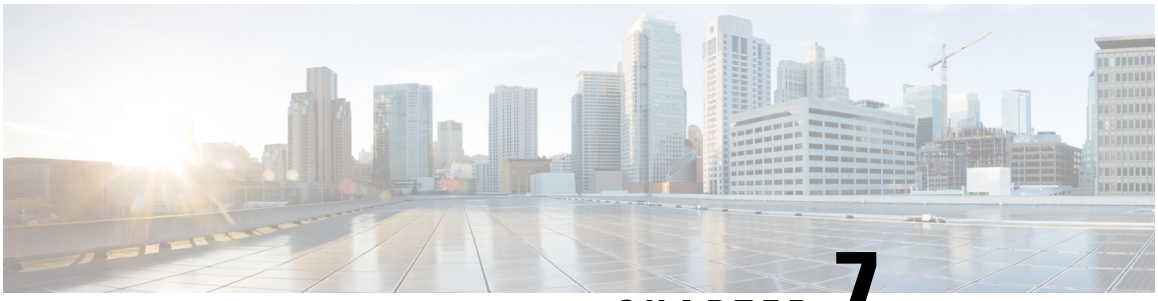
This example shows how to output the logs of the STP module and the device module at levels 0-4 to the console terminal: turn on the serial number display, use timestamp datetime, log output to the flash memory, log information of level 3 and 4 to output to buffer, output logs to external server 10.1.1.3, and open ARP debugging information.

The following example shows the system log configuration.

```
Device> enable
Device# terminal monitor
Device# configure terminal
Device(config)# logging
Device(config)# logging monitor all
Device(config)# logging monitor all level-list 0 to 4 module stp device
Device(config)# logging sequence-numbers
Device(config)# logging timestamps datetime
Device(config)# logging flash
Device(config)# logging buffered level-list 3 4
Device(config)# logging 10.1.1.3
Device(config)# logging host 10.1.1.3
Device(config)# logging facility ftp
Device(config)# debug ARP
Device(config)# logging flash
```

The following example shows the logging configuration information.

```
Device> enable
Device# configure terminal
Device(config)# show logging

state: on;
logging sequence-numbers: on;
logging timestamps: datetime;
logging language: english
logging monitor:
Console:   state: on;  display: off;  96 logged;  0 lost;  0 overflow.
logging buffered:  state: on;  249 logged;    0 lost;     0 overflow.
logging flash:  state: on;  37 logged;     0 lost;     0 overflow.
logging loghost:
logging facility: ftp;logging source: off
10.1.1.3:     state: on;  23 logged;     0 lost;     0 overflow.
logging SNMP Agent:  state: off;  0 logged;      0 lost;     0 overflow.
```



CHAPTER 7

Configuring the System Clock

- Overview for System Clock, on page 39
- Configuring the System Clock, on page 39
- Example: Configuring the System Clock, on page 40

Overview for System Clock

The system clock can be implemented in two ways. One is to automatically synchronize the time from the Simple Network Time Protocol (SNTP) server as the SNTP client, and the other can be configured by the administrator.

The system clock is divided into hardware clock and software clock. After configuring the system time manually, restart the device. If the default time is restored after restarting, it means that the hardware clock is not supported and only the software clock is supported.

Configuring the System Clock

SUMMARY STEPS

1. **enable**
2. **clock set** *HH:MM:SS YYYY/MM/DD*
3. **configure terminal**
4. **clock timezone** *zone-name hours- offset minutes-offset*
5. **clock summer-time** {**dayly** | **weekly**}
6. **show clock**

DETAILED STEPS

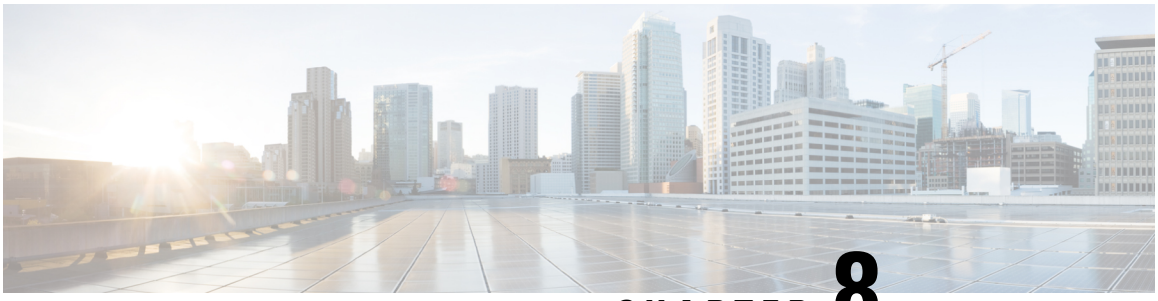
	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**clock set** *HH:MM:SS YYYY/MM/DD* **Example:** `Device# clock set 10:03:33`	Configures the system clock.
Step 3	**configure terminal** **Example:** `Device# configure terminal`	(Optional) Enters global configuration mode.
Step 4	**clock timezone** *zone-name hours- offset minutes-offset* **Example:** `Device(config)# configure terminal`	(Optional) Configures the system time zone.
Step 5	**clock summer-time** {**dayly** | **weekly**} **Example:** `Device(config)# clock summer-time dayly 00:00:00 2021/03/12 00:00:00 2021/11/0 5`	(Optional) Configures summer time.
Step 6	**show clock** **Example:** `Device(config)# show clock`	(Optional) Displays information about the system clock.

Example: Configuring the System Clock

The following example shows how to configure the system clock:

```
Device> enable
Device# clock set 17:50:50 2015/11/25

Set clock successfully.
Clock will be reset to 2013/01/01 00:00:00 after system rebooting because there
is no realtime clock chip.
```



CHAPTER 8

Configuring SNTP Client

- Simple Network Time Protocol Client, on page 41
- How to Configure SNTP Client, on page 41
- Configuration Examples for SNTP Client, on page 50

Simple Network Time Protocol Client

Switch system time can be achieved in two ways - the SNTP client where the SNTP server automatically synchronizes time; and the administrator's configuration.

The Simple Network Time Protocol (SNTP) is used for time synchronization between network devices. Normally, an SNTP server exists in the network and provides reference time for multiple SNTP clients. This way, time synchronization is achieved among all network devices.

SNTP can work in four modes: unicast, broadcast, multicast, and anycast.

- In the unicast mode, the client initiates a request to the server. After receiving the request, the server constructs a response message based on the local time and sends the response message back to the client.
- In the broadcast and multicast mode, the server periodically sends broadcast or multicast messages to the client, and the client receives the messages from the server.
- In the anycast mode, the client initiates a local broadcast address or a multicast address to send a request. In this case, the server in the network responds to the client. The client selects the server that receives the response message as the server, and discards the messages sent by the other server. After electing out of the server, the work pattern is same as unicast.

In all modes, the client receives a response message to parse the message to obtain the current standard time, and calculates the network transmission delay and local time compensation through a certain algorithm. The data is used to calibrate the current time.

How to Configure SNTP Client

Enabling SNTP Client

To enable or disable the SNTP client, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sntp client**
4. **show sntp client**
5. **show clock**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**sntp client** **Example:** `Device(config)# sntp client`	Enables the SNTP client. To disable the SNTP client, use the **no** form of this command. By default, the SNTP client is disabled.
Step 4	**show sntp client** **Example:** `Device(config)# show sntp client`	(Optional) Displays the SNTP client configuration.
Step 5	**show clock** **Example:** `Device(config)# show clock`	(Optional) Displays the system time.

Configuring the SNTP Client Mode

To configure the mode in which the SNTP client should function, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sntp client mode** { **anycast** [**key** *key-id*] | **broadcast** | **multicast** | **unicast** }
4. **show sntp client**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**sntp client mode** { **anycast** [**key** *key-id*] | **broadcast** | **multicast** | **unicast** } **Example:** `Device(config)# sntp client mode unicast`	Configures the work-mode of the SNTP client. By default, the SNTP client is set to broadcast mode.
Step 4	**show sntp client** **Example:** `Device(config)# show sntp client`	(Optional) Displays the SNTP client configuration.

Configuring the SNTP Server Address

When an SNTP client works in the unicast mode, you must configure the specified SNTP server.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sntp server** *ip-address*
4. **sntp server backup** *ip-address*
5. **show sntp client**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**sntp server** *ip-address* **Example:**	Configures the SNTP server address. Use the **no** form of the command to disable the SNTP server.

	Command or Action	Purpose
	`Device(config)# sntp server 122.2.2.1`	
Step 4	**sntp server backup** *ip-address* **Example:** `Device(config)# sntp server backup 112.1.1.1`	(Optional) Configures the SNTP backup server address. Use the **no** form of the command to disable the SNTP backup server.
Step 5	**show sntp client** **Example:** `Device(config)# show sntp client`	(Optional) Displays the SNTP client configuration.

Configuring the Broadcast Transmission Delay

When the SNTP client works in the broadcast or multicast mode, it is necessary to use the broadcast transmission delay parameter. In the broadcast mode, the local system time of the SNTP client is equal to the time taken from the server plus the transmission delay. You can modify the broadcast transmission delay based on the actual bandwidth of the network. To configure the broadcast transmission delay, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sntp client broadcastdelay** *time*
4. **show sntp client**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**sntp client broadcastdelay** *time* **Example:** `Device(config)# sntp client broadcastdelay 5`	Configures the broadcast propagation delay to the specified time in milliseconds. Use the **no** form of the command to disable broadcast propogation delay. By default, the broadcast propagation delay is 3 milliseconds.
Step 4	**show sntp client** **Example:** `Device(config)# show sntp client`	(Optional) Displays the SNTP client configuration.

Configuring the Polling Interval

When the SNTP client works in the unicast or anycast mode, you need to configure the polling interval. The SNTP client initiates a request to the server every other polling interval to calibrate the local system time. To configure the polling interval, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sntp client poll-interval** *time*
4. **show sntp client**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**sntp client poll-interval** *time* **Example:** `Device(config)# sntp client poll-interval 800`	Configures the polling interval to the specified time in seconds. Use the **no** form of the command to disable polling interval. By default, the polling interval is 1000 seconds.
Step 4	**show sntp client** **Example:** `Device(config)# show sntp client`	(Optional) Displays the SNTP client configuration.

Configuring Timeout Retransmission

When the SNTP request message is sent, there is no guarantee that the request message will reach the destination since it is a UDP message. In such cases, the timeout retransmission mechanism is adopted. When the client sends a request, if it does not receive a response within a certain period of time, it resends the request until the number of retransmissions exceeds the set value.

Note The configured timeout retransmission mechanism takes effect only when the SNTP client works in the unicast or anycast mode.

To configure the timeout retransmission attempts and the time interval, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sntp client retransmit-interval** *time*
4. **sntp client retransmit** *number*
5. **show sntp client**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**sntp client retransmit-interval** *time* **Example:** `Device(config)# sntp client retransmit-interval 20`	Configures the timeout retransmission interval. Use the **no** form of the command to disable retransmission interval. By default, the timeout retransmission interval is 5 seconds.
Step 4	**sntp client retransmit** *number* **Example:** `Device(config)# sntp client retransmit 8`	Sets the number of timeout retransmission attempts. By default, the number of timeout retransmission is set to 0.
Step 5	**show sntp client** **Example:** `Device(config)# show sntp client`	(Optional) Displays the SNTP client configuration.

Configuring Legacy Server List

When an SNTP client works in broadcast or multicast mode, it trusts and receives protocol messages from any SNTP server. If there is a malicious attack on the network server and it provides the wrong time, the local time cannot be synchronized to standard time.

When a list of valid servers is configured on the SNTP client, the client can only receive messages whose source addresses are in the legal server list.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sntp client valid-server** *ip-address wildcard*
4. **no sntp client valid-server** {**all** | *ip-address wildcard* }

5. **show sntp client**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**sntp client valid-server** *ip-address wildcard* **Example:** `Device(config)# sntp client valid-server 10.23.23.1 23.1.1.4`	Configures the legal server list.
Step 4	**no sntp client valid-server** {**all** | *ip-address wildcard* } **Example:** `Device(config)# sntp client valid-server all`	Deletes a legal server list.
Step 5	**show sntp client** **Example:** `Device(config)# show sntp client`	(Optional) Displays the SNTP client configuration.

Configuring Authentication

To further improve security, you can enable MD5 authentication between the SNTP server and the client. The SNTP client receives only authenticated messages.

To configure authentication, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sntp client authenticate**
4. **sntp client authentication-key** *key-number* **md5** *auth-key*
5. **sntp trusted-key** *key-number*
6. **sntp server key** *key-number*
7. **sntp client mode anycast key** *key-number*
8. **show sntp client**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**sntp client authenticate** **Example:** `Device(config)# sntp client authenticate`	Authenticates time sources. Use the **no** form of the command to disable authentication. By default, authentication is disabled.
Step 4	**sntp client authentication-key** *key-number* **md5** *auth-key* **Example:** `Device(config)# sntp client authentication-key 3 md5 5`	Configures the password for authentication for trusted time sources. Use the **no** form of the command to disable the authentication password.
Step 5	**sntp trusted-key** *key-number* **Example:** `Device(config)# sntp trusted-key 234586`	Configures a trusted password for multicast and broadcast modes. Use the **no** form of the command to disable the password.
Step 6	**sntp server key** *key-number* **Example:** `Device(config)# sntp server key 5`	Configures the password used by the server. This must be equal to the authentication-key Use the **no** form of the command to disable the password of the server.
Step 7	**sntp client mode anycast key** *key-number* **Example:** `Device(config)# sntp client mode anycast key 5`	Configures the password for anycast mode. This must be equal to the authentication-key.
Step 8	**show sntp client** **Example:** `Device(config)# show sntp client`	(Optional) Displays the SNTP client configuration.

Configuring System Clock Manually

The SNTP client can either automatically synchronize time from the SNTP server, or the administrator can perform manual calibration of the system clock.

Note If the switch has a built-in lithium battery, when the switch power is off, the system clock runs normally. If there is no built-in lithium battery and the switch power is off, the system clock stops running.

To manually calibrate the system clock, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **clock set** *HH:MM:SS YYYY/MM/DD*
3. **configure terminal**
4. **clock timezone** *time-zone-name hours-offset minutes-offset*
5. Use any of the following commands depending on the requirement:
   - **clock summer-time dayly** *start-time*
   - **clock summer-time weekly** *start-time*
6. **show clock**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**clock set** *HH:MM:SS YYYY/MM/DD* **Example:** `Device# clock set 22:22:13 2020/03/06`	
Step 3	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 4	**clock timezone** *time-zone-name hours-offset minutes-offset* **Example:** `Device(config)# clock timezone ch 3 43`	Configures the system time zone. Use the **no** form of the command to disable system time zone.
Step 5	Use any of the following commands depending on the requirement: • **clock summer-time dayly** *start-time* • **clock summer-time weekly** *start-time* **Example:** `Device(config)# clock summer-time dayly 00:00:00 2021/03/12 00:00:00 2021/11/05`	Configures daylight savings time. Use the **no** form of the command to disable daylight savings time.
Step 6	**show clock** **Example:** `Device(config)# show clock`	(Optional) Displays the system time.

Configuration Examples for SNTP Client

The following example shows how to configure the SNTP client in broadcast mode:

```
Device> enable
Device# configure terminal
Device(config)# sntp client mode broadcast
Device(config)# sntp client valid-server 192.168.1.99 0.0.0.0
Device(config)# sntp client authentication-key 1 md5 test
Device(config)# sntp trusted-key 1
Device(config)# sntp client authenticate
```

The following example shows how to configure the SNTP client in multicast mode:

```
Device> enable
Device# configure terminal
Device(config)# sntp client mode multicast
Device(config)# sntp client valid-server 192.168.1.99 0.0.0.0
Device(config)# sntp client authentication-key 1 md5 test
Device(config)# sntp trusted-key 1
Device(config)# sntp client authenticate
```

The following example shows how to configure the SNTP client in unicast mode:

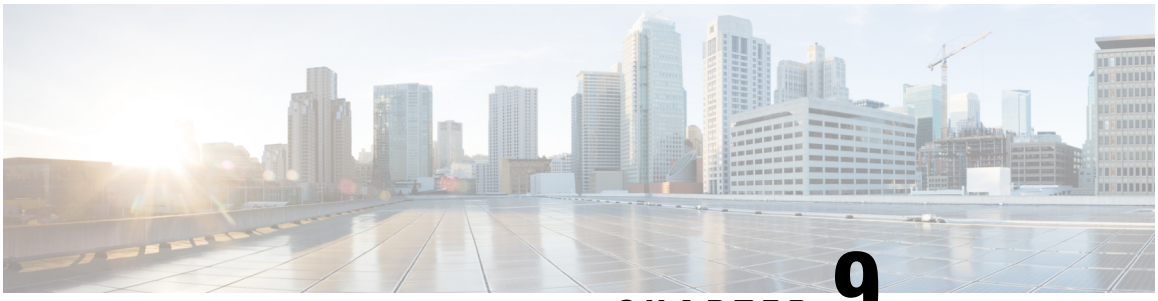
```
Device> enable
Device# configure terminal
Device(config)# sntp client
Device(config)# sntp client mode unicast
Device(config)# sntp server 192.168.1.99
Device(config)# sntp client authentication-key 1 md5 test
Device(config)# sntp server key 1
Device(config)# sntp client authenticate
```

The following example shows how to configure the SNTP client in anycast mode:

```
Device> enable
Device# configure terminal
Device(config)# sntp client mode anycast
Device(config)# sntp server 192.168.1.99
Device(config)# sntp client
Device(config)# sntp client authentication-key 1 md5 test
Device(config)# sntp client mode anycast key 1
Device(config)# sntp client authenticate
```

The following sample output displays time synchronization results:

```
Device(config)# show sntp client
Clock state  : synchronized    Current mode    : anycast
Use server   : 192.168.1.99    State           : idle
Server state : synchronized    Server stratum  : 1
Retrans-times: 3               Retrans-interval: 30s
Authenticate : enable          Authentication-key: 1
Poll interval   : 1000s
Last synchronized time: THU NOV 26 09:22:25 2015
Last received packet's originateTime: THU NOV 26 17:22:24 2015
Summer-time is not set.
```



CHAPTER 9

Configuring Network Time Protocol

- Information About Network Time Protocol, on page 51
- How to Configure NTP, on page 52
- Monitoring NTP, on page 60
- Example: Enabling Authentication and Configuring Broadcast Mode, on page 61

Information About Network Time Protocol

Network Time Protocol (NTP) synchronizes timekeeping among a set of distributed time servers and clients. With this synchronization, you can correlate events to the time that system logs were created and the time that other time-specific events occur. An NTP server must be accessible by the client switch.

An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock that is attached to a time server. NTP distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two machines to within a millisecond of one another.

NTP uses a stratum to describe how many NTP hops away a machine is from an authoritative time source. A stratum 1 time server has a radio or atomic clock that is directly attached, a stratum 2 time server receives its time from a stratum 1 time server, and so on. A machine running NTP automatically chooses as its time source the machine with the lowest stratum number that it is configured to communicate with through NTP. This strategy effectively builds a self-organizing tree of NTP speakers.

NTP has two ways to avoid synchronizing to a machine whose time might be ambiguous:

- NTP never synchronizes to a machine that is not synchronized itself.
- NTP compares the time that is reported by several machines and does not synchronize to a machine whose time is significantly different from the others, even if its stratum is lower.

The communications between machines running NTP, known as associations, are usually statically configured; each machine is given the IP addresses of all machines with which it should form associations. An associated pair of machines can keep accurate timekeeping by exchanging NTP messages between each other. However, in a LAN environment, you can configure NTP to use IP broadcast messages. With this alternative, you can configure the machine to send or receive broadcast messages, but the accuracy of timekeeping is marginally reduced because the information flow is one-way only.

NTP Work Mode

NTP supports 4 working modes for clock synchronization:

- Client Mode:

  In this mode, the OLT device or client sends regularly time-of day requests to a configured NTP server

- Peer Mode:

  In this mode, an NTP-configured device establishes an association with another peer device and synchronizes the time with each other.

- Broadcast Mode:

  In this mode, the NTP server sends the time information to all connected clients in the same subnet as the server.

- Multicast Mode:

  In this mode, the NTP server and clients have multicast configured and the NTP server sends the time information to only multcast-configured clients

How to Configure NTP

The following sections provide configurational information about NTP.

Enabling NTP

To enable or disable NTP, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. [**no**] **ntp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	[**no**] **ntp** **Example:**	Enables NTP. Use the **no** form of this command to disable NTP.

	Command or Action	Purpose
	`Device(config)# ntp`	

Configuring Reference Clocks

The device only supports local reference clock configurations. These configurations are generally only used for testing, and the purpose is to enable the device to perform synchronization testing as a server without other clock servers.

To configure reference clocks, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ntp reference-clock local**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**ntp reference-clock local** **Example:** `Device(config)# ntp reference-clock local`	Configures the local clock as reference clock. Use the **no** form of the command to remove the local clock as reference clock.

Configuring Client Mode

To configure client mode, perform the following steps:

Before you begin

- The NTP server can only be used as a time server to synchronize other devices after its own clock is synchronized.
- When the server is in an unsynchronized state or the clock level is greater than or equal to the client's clock level, it will not respond to the client's request.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **ntp unicast server** *ip_address* [**authentication-keyid** *key_id*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**ntp unicast server** *ip_address* [**authentication-keyid** *key_id*] **Example:** `Device(config)# ntp unicast server 192.168.0.11`	Configures synchronization to an NTP server. Use the **no** form of the command to disable the NTP server on the device.

Configuring Peer Mode

To configure synchronization to an NTP-configured peer device, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ntp unicast peer** *ip_address* [**authentication-keyid** *key_id*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**ntp unicast peer** *ip_address* [**authentication-keyid** *key_id*] **Example:** `Device(config)# ntp unicast peer 192.168.0.10`	Configures synchronization to an NTP-configured peer device. Use the **no** form of the command to remove synchronization to an NTP-configured peer device.

Configuring Broadcast Mode

In this mode, you need to enable the **ntp broadcast** command on the interface connecting the NTP server and the client device.

To configure broadcast mode, perform the following steps:

Before you begin

The NTP server clock must be synchronized before it can be used as a time server to synchronize client devices.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface vlan-interface** *vlan-id*
4. **ntp broadcast server** [**authentication-keyid** *key_id*]
5. **exit**
6. **interface vlan-interface** *vlan-id*
7. **ntp broadcast client**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**interface vlan-interface** *vlan-id* **Example:** `Device(config)# interface vlan-interface 1`	Creates a VLAN interface and enter interface configuration mode.
Step 4	**ntp broadcast server** [**authentication-keyid** *key_id*] **Example:** `Device(config-if-vlaninterface-1)# ntp broadcast server`	Enables NTP broadcast on the NTP server.
Step 5	**exit** **Example:** `Device(config-if-vlaninterface-1)# exit`	Enters global configuration mode.
Step 6	**interface vlan-interface** *vlan-id* **Example:**	Creates a VLAN interface and enter interface configuration mode.

	Command or Action	Purpose
	`Device(config)# interface vlan-interface 1`	
Step 7	**ntp broadcast client** **Example:** `Device(config-if-vlaninterface-1)# ntp broadcast client`	Enables NTP broadcast on the client device.

Configuring Multicast Mode

In this mode, you need to enable the **ntp multicast** command on the interface connecting the NTP server and the client device.

To configure multicast mode, perform the following steps:

Before you begin

The NTP server clock must be synchronized before it can be used as a time server to synchronize client devices.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface vlan-interface** *vlan-id*
4. **ntp multicast server** [**authentication-keyid** *key_id*]
5. **exit**
6. **ntp multicast client**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**interface vlan-interface** *vlan-id* **Example:** `Device(config)# interface vlan-interface 1`	Creates a VLAN interface and enter interface configuration mode.
Step 4	**ntp multicast server** [**authentication-keyid** *key_id*] **Example:**	Emables NTP multicast on the NTP server.

	Command or Action	Purpose
	`Device(config-if-vlaninterface-1)# ntp multicast server`	
Step 5	**exit** **Example:** `Device(config-if-vlaninterface-1)# exit`	Enters global configuration mode.
Step 6	**ntp multicast client** **Example:** `Device(config-if-vlaninterface-1)# ntp multicast client`	Emables NTP multicast on the client device.

Configuring Access Control

Through the access control configurations, you can specify the device's processing actions on the corresponding packets.

The supported actions are as follows:

- permit: Allow the continued processing of packets
- deny: Discard packets

You can configure multiple ACCESS control lists (ACLs). The lists are arranged in priority according to the maximum IP address and then the maximum mask. Packets are matched in sequence, and the first matching action shall prevail.

To configure access control for NTP services, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ntp access** *ip_address subnet_mask* {**permit** | **deny**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**ntp access** *ip_address subnet_mask* {**permit**	**deny**} **Example:**	Configures access control for NTP.

	Command or Action	Purpose
	`Device(config)# ntp access 192.168.0.10 255.255.255.0 permit`	Use the **no** form of the command to disable access control for NTP.

Configuring Authentication

To configure authentication, perform the following steps:

Before you begin

- The authentication will only take effect after the authentication is enabled.
- In addition to these authentication configurations, the mode configuration needs to specify which key to use in the corresponding command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ntp authentication**
4. **ntp authentication-keyid** *key_id* **md5** *string_value*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**ntp authentication** **Example:** `Device(config)# ntp authentication`	Enables NTP authentication. Use the **no** form of the command to disable authentication.
Step 4	**ntp authentication-keyid** *key_id* **md5** *string_value* **Example:** `Device(config)# ntp authentication-keyid 2 md5 cisco`	Configures the NTP authentication key. • *key_id* : The key ID. The value must be in the range of 1 to 65535. • *string_value*: The string value. The value must be alphanumeric and in the range of 1 to 64. Use the **no** form of the command to disable authentication key.

Disabling Incoming Packets

To disable incoming packets, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface vlan-interface** *vlan-id*
4. **ntp disable**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**interface vlan-interface** *vlan-id* **Example:** `Device(config)# interface vlan-interface 1`	Creates a VLAN interface and enter interface configuration mode.
Step 4	**ntp disable** **Example:** `Device(config-if-vlaninterface-1)# ntp disable`	Disables incoming packets.

Configuring Maximum Number of Dynamic Sessions

If the number of dynamic sessions exceeds this number, new dynamic sessions will not be created.

To configure maximum number of dynamic sessions, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ntp max-dynamic-sessions** *value*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. Enter your password, if prompted.

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**ntp max-dynamic-sessions** *value* **Example:** `Device(config)# ntp max-dynamic-sessions 20`	Configures the maximum number of dynamic sessions. The value must be in the range of 11 to 100. Use the **no** form of the command to remove the configured maximum number of dynamic sessions.

Monitoring NTP

Use the following commands to monitor NTP.

Table 3: Commands to Monitor NTP

Command	Purpose
show ntp reference-clock	Displays the reference clock configurations.
show ntp unicast server	Displays the unicast server configurations
show ntp unicast peer	Displays the unicast peer configurations.
show ntp broadcast server	Displays the broadcast server configurations
show ntp multicast server	Displays the multicast server configurations
show ntp access	Displays the access configurations.
show ntp authentication	Displays the authentication configurations.
show ntp disable	Displays the disable configurations.
show ntp max-dynamic-sessions	Displays the configured maximum number of dynamic sessions.
show ntp status	Displays the NTP status.
show ntp sessions	Displays the NTP session details.

Example: Enabling Authentication and Configuring Broadcast Mode

The following example shows how to enable authentication and broadcast mode on an NTP server:

```
Device> enable
Device# configure terminal
Device(config)# interface vlan-interface 1
Device(config-if-vlanInterface-1)# ntp broadcast server
```

The following example shows how to enable authentication and broadcast mode on a client device:

```
Device> enable
Device# configure terminal
Device(config)# ntp
Device(config)# ntp authentication
Device(config)# ntp authentication-keyid 1 md5 123ABC
Device(config)# interface vlan-interface 1
Device(config-if-vlanInterface-1)# ntp broadcast client
```