

Parameter	Description
	<ul style="list-style-type: none"> • IPv4: Internet Protocol version 4, which is the first widely used protocol version and is at the core of standards-based Internet technology. • AppleTalk: A proprietary suite of protocols developed by Apple Inc. to provide communication services for Apple computers, such as file transfer, printing, email, and other network services. • IPX: Internet Packet Exchange (IPX) protocol stack, which is supported by Novell's NetWare operating system. • NetBEUI: Network Basic Input/Output System (NetBIOS) Extended User Interface, which is a non-routable protocol developed for the IBM to transfer NetBIOS messages. • IGMP: Internet Group Management Protocol, which is used by hosts and neighboring routers on IP networks to establish multicast group memberships.
Destination MAC Address	Indicates the destination MAC address. For example, value 00:01:6C:4C:58:FE indicates that the ADSL port filters data frames whose destination MAC addresses are 00:01:6C:4C:58:FE. If this parameter is left blank, the ADSL port filters the destination MAC addresses for all data frames.
Source MAC Address	Indicates the source MAC address. For example, value 90:FB:A6:14:9E:5A indicates that the ADSL port filters data frames whose source MAC addresses are 90:FB:A6:14:9E:5A. If this parameter is left blank, the ADSL port filters the source MAC addresses for all data frames.
Frame Direction	Indicates the direction in which a data frame is transmitted. The options are as follows: <ul style="list-style-type: none"> • LAN<=>WAN: The ADSL port filters the MAC addresses for data frames that are transmitted mutually between the LAN and WAN ports. • WAN=>LAN: The ADSL port filters the MAC addresses for data frames that are transmitted from the WAN ports to the LAN ports. • LAN=>WAN: The ADSL port filters the MAC addresses for data frames that are transmitted from the LAN ports to the WAN ports.


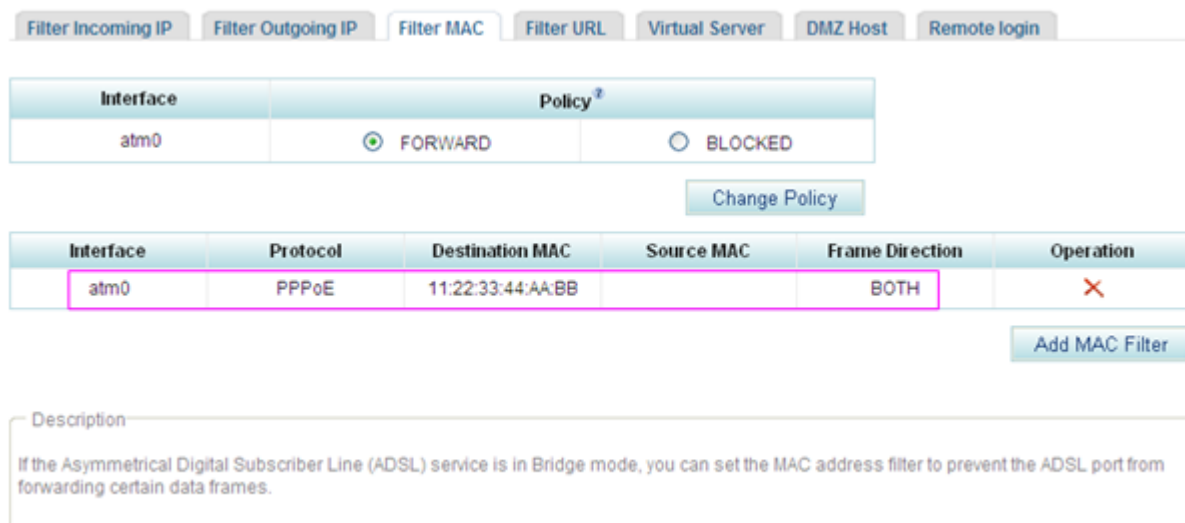
5. Click  to save the settings.
Figure 7-260 shows the configuration result.

Figure 7-260 Configuration result



Value **BOTH** indicates that the ADSL port filters the MAC addresses for data frames that are transmitted from the LAN port to the WAN port and from the WAN port to the LAN port.

----End

7.6.5 URL Filter

Using the URL filtering feature, an enterprise or a family can prevent its members from visiting certain websites.

Description

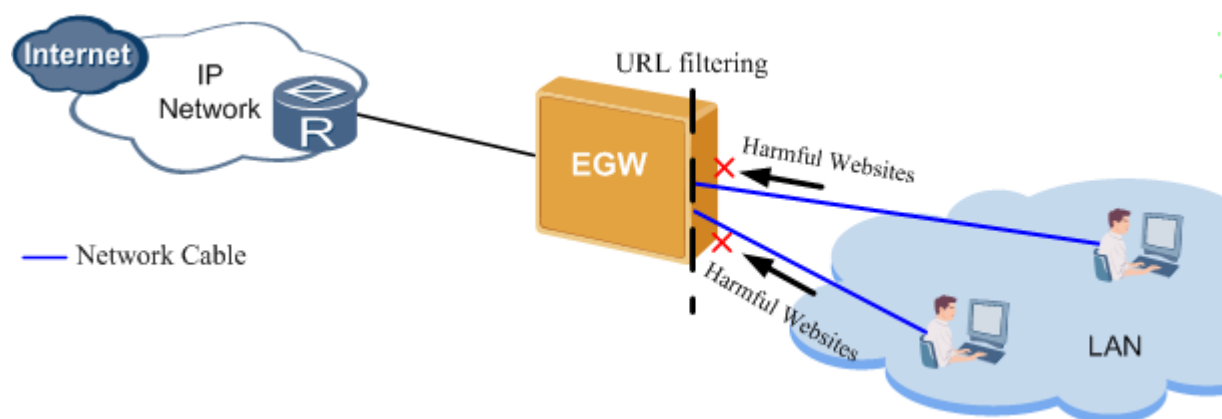
Principle

At present, contents at many websites are illegal or improper because they are not effectively supervised or restricted. Therefore, more and more enterprises use the URL access control function to ensure information security and restrict URL access.

As shown in [Figure 7-261](#), URL filtering is used to:

- Control access to websites containing content including pornography, terrorism, violence, gambling, or illegal information.
- Shield phishing websites to protect employees' privacy.
- Shield malicious websites to protect the enterprise's private network from attack.
- Provide customized services for enterprises, for example, allow employees to access specified websites.

Figure 7-261 URL filtering



Implementation

The EGW1520 provides the following URL filter modes:

- Include
URLs in the whitelist can be accessed.
- Exclude
URLs in the blacklist cannot be accessed.

NOTE

Use either whitelist or blacklist mode.

EGW1520 can filter the whole URL (for example, <http://www.example.com>) or the keyword in the URL (for example, [example.com](http://www.example.com)).

Specification

- Maximum number of URLs to be filtered at the same time: 100
- Maximum length of each URL: 128 bytes
- Full match and partial match

Limitation

Wildcards, for example, using * for full match, are not allowed in filtering rules.

Configuration

Prerequisite

You have logged in to the web management system. For details, see [7.7.1 Web Management](#).

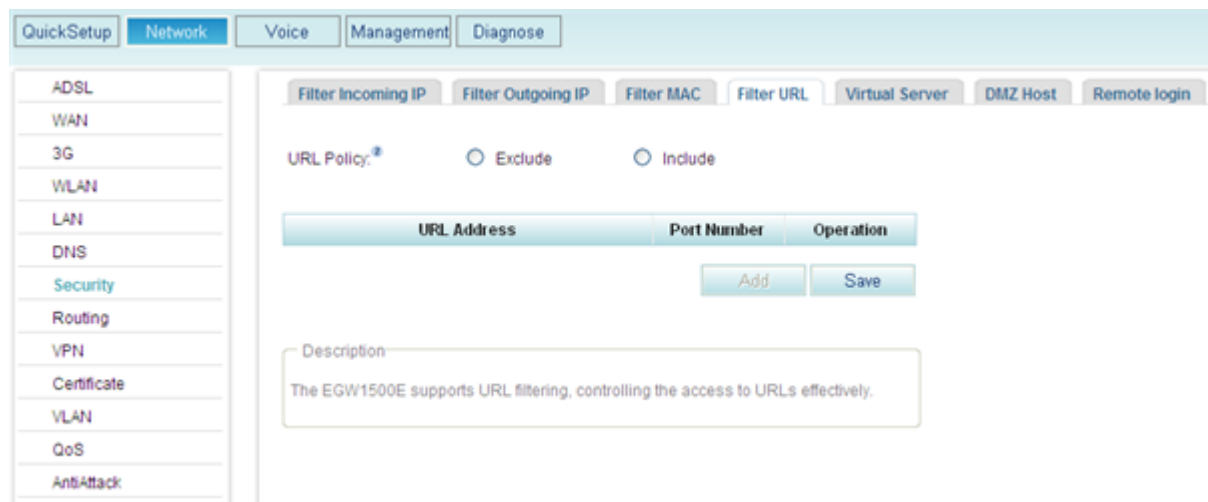
Procedure

Step 1 On the web management system, choose **Network** > **Security** from the navigation tree.

Step 2 Click the **Filter URL** tab.

The page shown in [Figure 7-262](#) is displayed.

Figure 7-262 Configuring the URL filter (1)



Step 3 Select a URL filter mode, for example, **Exclude**.

- Include
URLs in the whitelist can be accessed.
- Exclude
URLs in the blacklist cannot be accessed.

Step 4 Click  to save the filter mode.

The page shown in [Figure 7-263](#) is displayed.

Figure 7-263 Configuring the URL filter (2)



Step 5 Click  to add a URL to be filtered.

The page shown in [Figure 7-264](#) is displayed.

Figure 7-264 Configuring the URL filter (3)

Filter Incoming IP | Filter Outgoing IP | Filter MAC | Filter URL | Virtual Server | DMZ Host | Remote login

URL Address:

Port Number:

Back Save

Step 6 Enter the URL to be filtered (a complete URL or keywords) and the port number. The default port number is 80.

Step 7 Click  to save the settings.

[Figure 7-265](#) shows the configuration result.

Figure 7-265 Configuring the URL filter (4)

Filter Incoming IP | Filter Outgoing IP | Filter MAC | Filter URL | Virtual Server | DMZ Host | Remote login

URL Policy: Exclude Include

URL Address	Port Number	Operation
example.com	80	X

Add Save

Description

The EGW1500E supports URL filtering, controlling the access to URLs effectively.

----End

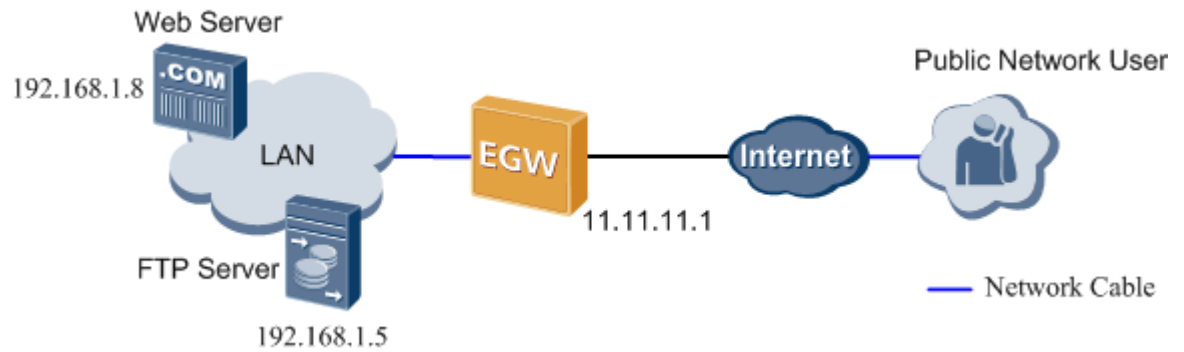
7.6.6 Virtual Server

After configuring the virtual server, users can access to servers in the private network, and enable services, such as web browsing and FTP download.

Description

A virtual server functions as a public server in the private network. Users in the external network can use services that the virtual server provides (such as web and FTP download services) after accessing the external address obtained from the EGW1520. [Figure 7-266](#) shows the typical network.

Figure 7-266 Typical virtual server network



Configuration

Prerequisites

- You have logged in to the web management system. For details, see [7.7.1 Web Management](#).
- The EGW1520 has been connected to [the upstream network](#) and the NAT function has been enabled.
- Required services and port numbers have been enabled on the private network.

Procedure

Step 1 On the web management system, choose **Network** > **Security** from the navigation tree.

Step 2 Click the **Virtual Server** tab.

The page shown in [Figure 7-267](#) is displayed.

Figure 7-267 Configuring a virtual server (1)



Step 3 Click  to add a virtual server.

The page shown in [Figure 7-268](#) is displayed.

Figure 7-268 Configuring a virtual server (2)

Service Name:

Select a Service:

Custom Service:

Virtual Server IP Address:

External Port Start	External Port End	Protocol	Type	Internal Port Start	Internal Port End
<input type="text"/>	<input type="text"/>	TCP	Single	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	Single	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	Single	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	Single	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	Single	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	Single	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	Single	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	Single	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	Single	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	Single	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	Single	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	Single	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	Single	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	Single	<input type="text"/>	<input type="text"/>

Step 4 Set parameters according to [Table 7-68](#).

Table 7-68 Parameter description

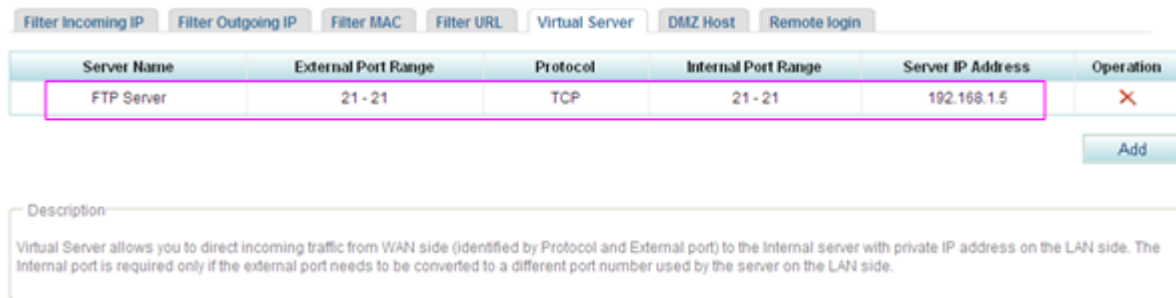
Parameter	Description
Select a Service	Indicates the service that is provided by the virtual server, such as the web, mail, and FTP services. The service must be enabled on the internal server(Multiple services can be enabled on a server in the internal network).
Custom Service	Allows you to define a service different from options in the Select a Service drop-down list box. The service that you define must be enabled on the internal server.
Virtual Server IP Address	Indicates the IP address of the internal server, for example, 192.168.1.5.
External Port Start	Indicates the start and end port numbers that the virtual server provides for external users. External users can use the port numbers between the start and end port numbers to access the virtual server. You are advised to use the default value.
External Port End	
Protocol	Indicates the transfer protocol used by the virtual server, for example, TCP for the web server.
Type	Indicates the port count used by the internal server.

Parameter	Description
	<ul style="list-style-type: none"> • Single: The internal server uses only one port. • Range: The internal server uses multiple ports. Port numbers on the internal server must be the same as those provided by the virtual server for external access, and you cannot change them.
Internal Port Start	Indicates the start and end port numbers that the internal server provides for external users, which must be the same as the start and end port numbers that the virtual server provides for external users.
Internal Port End	

Step 5 Click  to save the settings.

Figure 7-269 shows the configuration result.

Figure 7-269 Configuring a virtual server (3)



After the configuration is successful, external users can access the internal server through the EGW1520 WAN port or the ADSL IP address and port number.

----End

Typical Configuration Example

Network Requirements

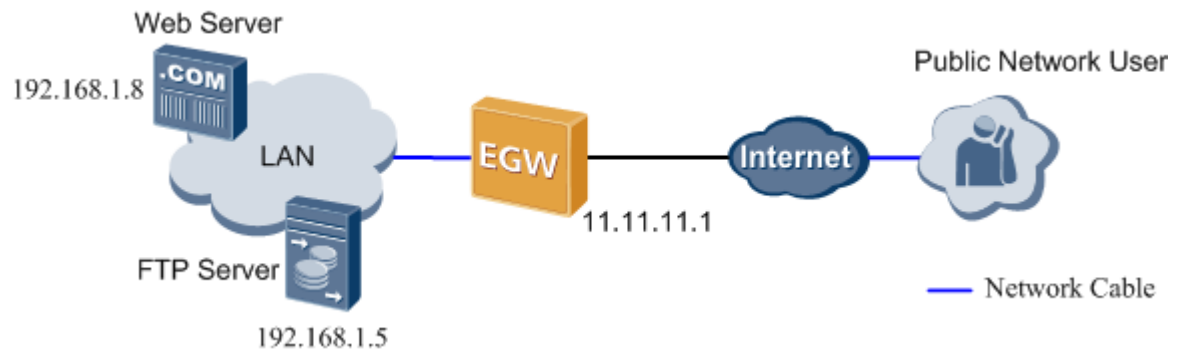
Users access the Internet through EGW1520 and want to configure a web server and an FTP server on the private network to provide web and FTP download services for external users. The network requirements are as follows:

- Connect EGW1520 to the Internet through the WAN port whose IP address is 11.11.11.1.
- Configure a web server and an FTP server on the private network, whose IP addresses are 192.168.1.8 and 192.168.1.5 respectively.
- After the configuration is complete, external systems can access the internal web server and FTP server.

Typical Network

Figure 7-270 shows the typical network diagram of the virtual server.

Figure 7-270 Typical network



Procedure

NOTE

- For details on how to configure the web and FTP servers, see the relevant documents.
 - For details on how to add a virtual server, see [Adding a virtual server](#).
1. Configure the web server software on the server whose IP address is 192.168.1.8 and enable the port number 80. Configure the FTP server software on the server whose IP address is 192.168.1.5 and enable the port number 21.
For details, see the related user guide.
 2. On the web management system, add a virtual server.
[Figure 7-271](#) shows the configuration result.

Figure 7-271 Configuration result

Server Name	External Port Range	Protocol	Internal Port Range	Server IP Address	Operation
FTP Server	21 - 21	TCP	21 - 21	192.168.1.5	✗
Web Server (HTTP)	80 - 80	TCP	80 - 80	192.168.1.8	✗

Add

Description

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side.

Verification

- If an external user enters **http://11.11.11.1** in the address box of the Internet Explorer and accesses the web server successfully, the web server is configured successfully. Otherwise, verify the configurations of the web server software and the EGW1520 virtual server.
- If an external user enters **ftp://11.11.11.1** in the address box of the Internet Explorer and accesses the FTP server successfully, the FTP server is configured successfully. Otherwise, verify the configurations of the FTP server software and the EGW1520 virtual server.



CAUTION

An external user must use the IP address that EGW1520 provides for external users (WAN port IP address **11.11.11.1** in this example) to access the internal server.

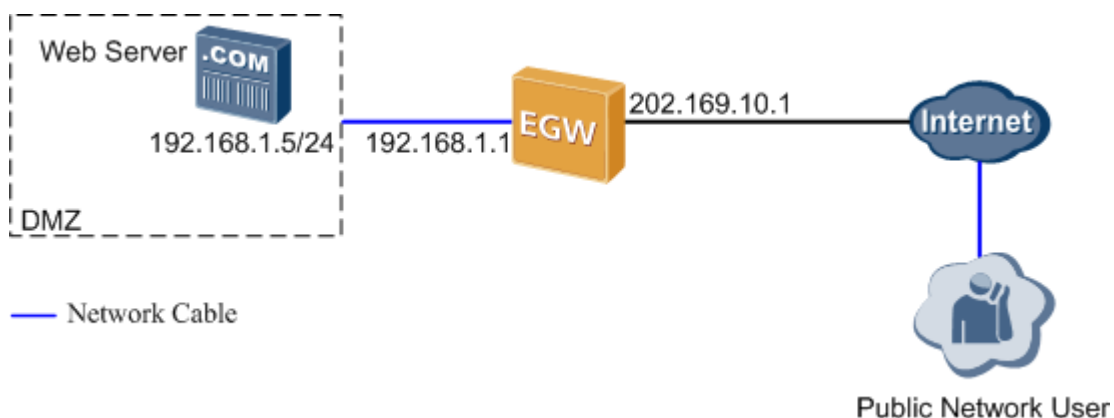
7.6.7 DMZ

A virtual server enables external users to access internal servers on the private network. When multiple services are running on internal servers, several virtual servers must be configured. This makes the configuration complicated. To simplify the configuration, configure only the IP addresses for internal servers in the Demilitarized Zone (DMZ). External users can access only the internal servers (such as the WWW and FTP servers) in the DMZ but cannot use the other internal resources. This protects the internal network against illegal access.

Description

The DMZ is deployed between a public network and an enterprise's private network. Some public servers (such as the web server and FTP server) are deployed in the DMZ, as shown in [Figure 7-272](#). The EGW1520 forwards all access requests from the public network (excluding those meeting NAT requirements) to the DMZ. This protects the internal network.

Figure 7-272 DMZ implementation



The following uses a web server in the DMZ as an example to describe the DMZ implementation.

1. After receiving external HTTP packets, the EGW1520 checks the packets. If the packets do not meet NAT requirement, EGW1520 forwards the packets to the DMZ.
2. EGW1520 converts the destination address of request packets to the DMZ web server's preset IP address, and sends the packets to the DMZ web server.
3. After receiving the request packets, the web server sends response packets to the computer on the public network. Then NAT is performed.

Configuration

Prerequisites

- You have logged in to the web management system. For details, see [7.7.1 Web Management](#).
- You have connected to the upstream network and the NAT function has been enabled. For details on how to connect to the upstream network, see [7.2 Connection Modes](#).

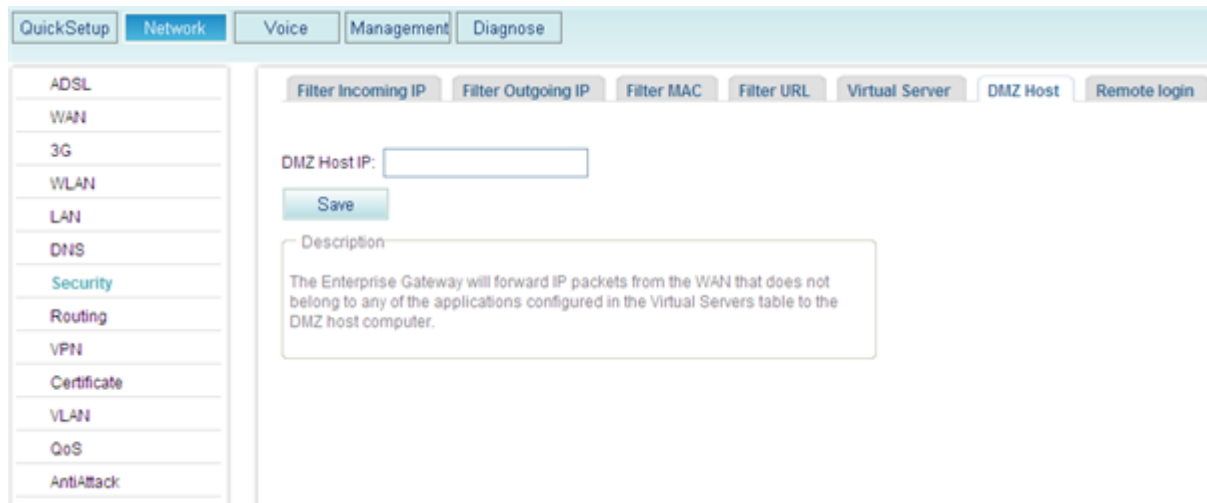
Procedure

Step 1 On the web management system, choose **Network > Security** from the navigation tree.

Step 2 Click the **DMZ Host** tab.

The page shown in [Figure 7-273](#) is displayed.

Figure 7-273 Configuring the DMZ (1)



Step 3 Enter the DMZ host IP address, for example, **192.168.1.5**.

Step 4 Click  to save the settings.

[Figure 7-274](#) shows the configuration result.

Figure 7-274 Configuring the DMZ (2)



----End

Typical Example

Networking Requirements

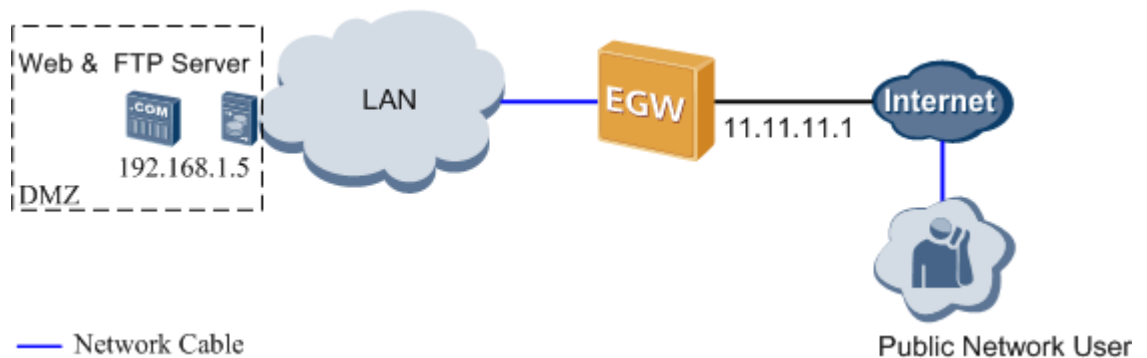
Assume that a user who uses the EGW1520 to connect to the Internet wants to deploy a web server and an FTP server on the intranet to provide website services and FTP resource download services for users on the external network. The network requirements are as follows:

- The EGW1520 uses a WAN port to connect to the Internet. The IP address of the WAN port is **11.11.11.1**.
- Deploy a web server and an FTP server on the same computer on the EGW1520's intranet. The IP address is **192.168.1.5**.
- Configure the DMZ to enable users on the external network to access the web server and FTP server.

Typical Network

Figure 7-275 shows the typical network.

Figure 7-275 DMZ typical network



Configuration Procedure

NOTE

- For details on how to configure the web and FTP servers, see the relevant documents.
- For details on how to configure the DMZ, see [Configuration](#).

1. On the computer whose IP address is **192.168.1.5**, configure the web server and the FTP server.
For details, see the related user guide.
2. Configure the DMZ on the web management system.

Figure 7-276 shows the configuration result.

Figure 7-276 Configuration result

Filter Incoming IP Filter Outgoing IP Filter MAC Filter URL Virtual Server **DMZ Host** Remote login

DMZ Host IP:

Save

Description

The Enterprise Gateway will forward IP packets from the WAN that does not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Verification

- Start the Internet Explorer and enter **http://11.11.11.1** in the address box as a user on the external network. If the web server is connected, the configuration is successful. If the web server is not connected, check the IP address setting of the DMZ host on the web server and EGW1520.
- Start the Internet Explorer and enter **ftp://11.11.11.1** in the address box as a user on the external network. If the FTP server is connected, the configuration is successful. If the FTP server is not connected, check the IP address setting of the DMZ host on the FTP server and EGW1520.



CAUTION

An external user must use EGW1520 external IP address (in this topic, it is the IP address of the WAN port **11.11.11.1**) to access internal servers.

7.6.8 Remote Login

This topic describes how to remotely configure and maintain the EGW1520 by connecting to uplink ports (WAN, ADSL, or 3G port).

The EGW1520 provides a public IP address for remote maintenance.

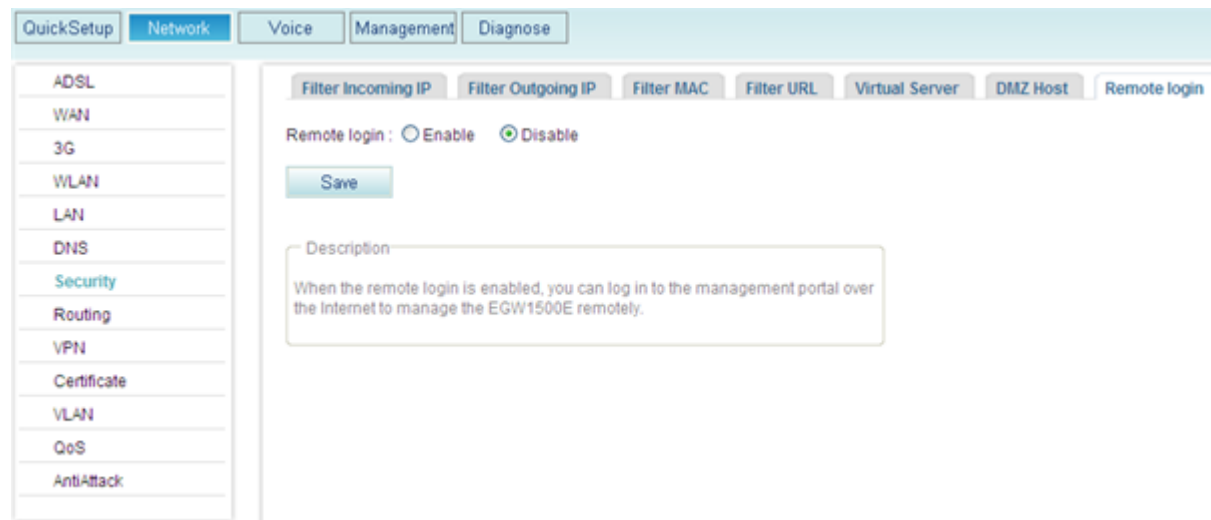
Enabling Remote Login

Step 1 On the web management system, choose **Network > Security** from the navigation tree.

Step 2 Click the **Remote login** tab.

The page shown in [Figure 7-277](#) is displayed.

Figure 7-277 Configuring remote login



Step 3 Select **Enable**.

Step 4 Click  to save the settings.

----End

Obtaining the Public IP Address of EGW1520

Step 1 On the web management system, choose **Management** > **Status** from the navigation tree.

Step 2 Click the **Network** tab.

The page shown in [Figure 7-278](#) is displayed.

Figure 7-278 Obtaining the IP address of EGW1520



Step 3 View the IP address of EGW1520. The IP address in [Figure 7-278](#) is the public IP address of EGW1520.

----End

Logging In to EGW1520 Remotely

Step 1 Use the Internet Explorer (6.0 or a later version) on your computer to access the public IP address of EGW1520.

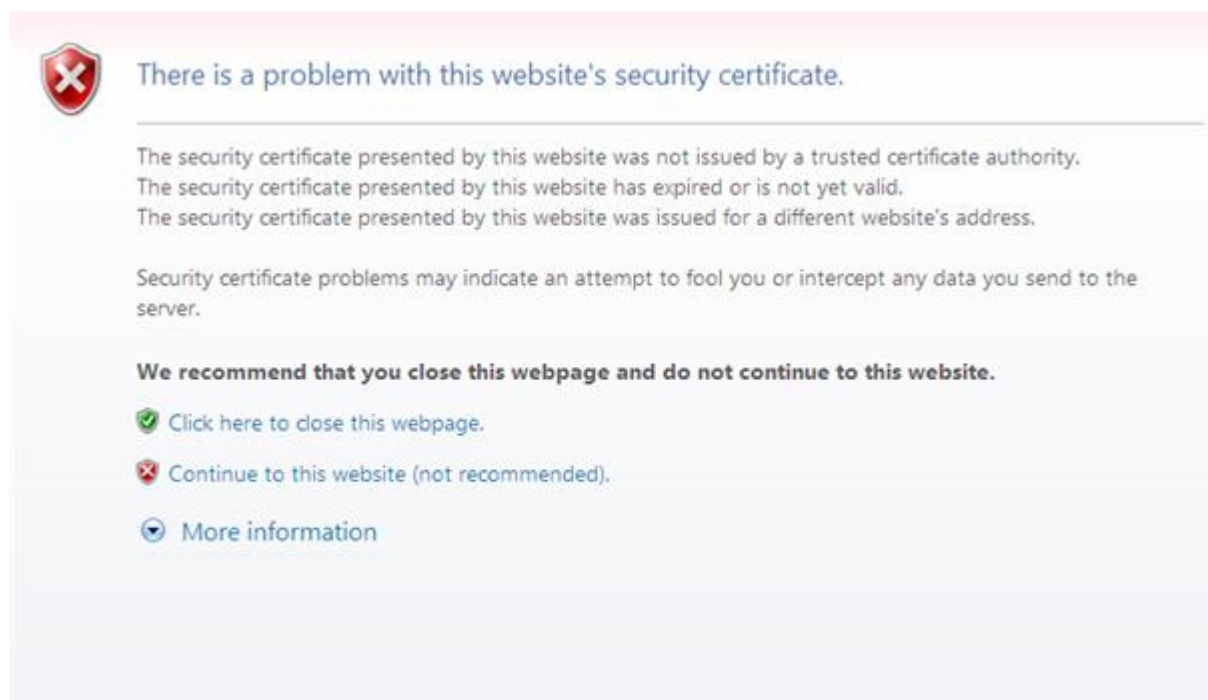


NOTE

When you log in to the EGW1520 using HTTP, the EGW1520 automatically changes your login mode to HTTPS to ensure communication security.

If the security level of your browser is not set properly, the system notifies you that the certificate is incorrect, as shown in [Figure 7-279](#).

Figure 7-279 Prompt information




Click  to continue your operation.

The page shown in [Figure 7-280](#) is displayed.

Figure 7-280 Logging in to the EGW1520



Step 2 Enter the user name (initial user name is **admin**) and password (initial password is **Admin@123**) and click .

----End

7.7 Operations and Maintenance

The EGW1520 can be managed on web pages or in TR-069 mode.

7.7.1 Web Management

The web management system allows users to set parameters, detect faults, and upgrade devices.



NOTE

The EGW1520 also supports remote login, from which you can remotely configure and maintain the EGW1520. For details about how to remotely log in to the EGW1520, see [7.6.8 Remote Login](#).

Prerequisite

Before logging in to the web management system, ensure that the configuration environment is ready.

1. Prepare a PC (maintenance terminal).
The PC must meet the following requirements:
 - Has the Ethernet adapter installed, supporting TCP/IP.
 - Has Windows XP or later operating system installed.

- Has Microsoft Internet Explorer 6.0 or later version without configuring the proxy server.
 - Supports the resolution 1024 x 768 or above.
2. The console cables have been connected.
- You can connect cables by using either of the following methods according to the network:
- Use the straight-through cable to connect the EGW1520 LAN port to the PC network port.
 - Use the straight-through cable to connect the EGW1520 LAN port to the PC network port through the switch or hub.
3. The PC IP address has been set.
- The IP addresses of the PC and EGW1520 must be on the same network segment. For example, if IP address of the EGW1520 is **192.168.1.1** (default value), the PC IP address can be set to **192.168.1.x**, where **x** ranges from **2** to **254**.

 **NOTE**

By default, DHCP is enabled on an EGW1520. The PC can use the automatic mode to obtain the IP address.

Background

Users can access the web management system in the following two modes:

- **HTTPS**
The web browser interacts with the EGW1520 using HTTPS, which ensures user information security.
- **HTTP**
The web browser interacts with the EGW1520 using HTTP.

 **NOTE**

- Only HTTPS access mode is enabled on EGW1520 by default. The HTTP access mode can be enabled on the page for configuring the LAN. For details, see [Configuring the LAN](#).
- HTTP transmits plain text. Use HTTP to perform web management only in trusted networks.
- If only the HTTPS mode is enabled, the system switches to the HTTPS mode automatically when you access the EGW1520 in HTTP mode.

Procedure

Step 1 Log in to the EGW1520 using Internet Explorer 6.0 or later. The default URL is **https://192.168.1.1**.

The page shown in [Figure 7-281](#) is displayed.

Figure 7-281 Logging in to the web management system (1)



 **NOTE**

- The default IP address of the EGW1520, login user name, and password can be obtained from the label at the bottom of the EGW1520.
- After logging in to the web management system, you can change IP address of the EGW1520. For details, see [Configuring the LAN](#).

Step 2 Enter the user name and password, and click **Log In**.

- Administrator: The user name is **admin** and the password is **Admin@123**.
- Common user: Both the initial user name and password are the internal number of a common user.

 **NOTE**

- Choose **Management > Password** to change the password after the initial login.
- Make a note of your password and keep it in a safe place. Do not share your password with anyone. If you forget your password, press and hold the **RESET** button on EGW1520 for more than six seconds, and log in to the web management system using the default password **Admin@123**. The configuration is restored to factory settings.
- If you fail to log in to the web management system for 5 consecutive times in 10 minutes, the system locks your PC IP address for 30 minutes.
- If you do not perform any operation in 10 minutes after logging in to the web management system, the login times out and the system requires re-login to ensure security.

----End

7.7.2 TR-069

The Technical Report 069 (TR-069) is a DSL forum (which was later renamed as broadband forum) technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices.

Description

This topic describes the principle, implementation, specification, and limitation of the TR-069.

Principle

The Technical Report 069 (TR-069) is a DSL forum (which was later renamed as broadband forum) technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices. As a bidirectional SOAP/HTTP-based protocol, it provides the communication between customer premises equipment (CPE) and Auto Configuration Servers (ACS). It includes both a safe auto configuration and the control of other CPE management functions within an integrated framework.

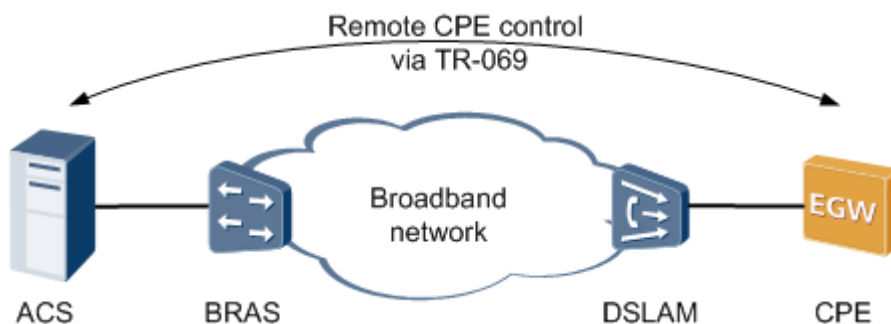
Customer premises equipment, such as gateways and set top boxes (STBs) are scattered on the user side. Maintenance personnel need to provide on-site services when configuration modification or troubleshooting is required, which increases management difficulty. TR-069 enables you to manage and maintain user's devices remotely on the network side. Details about the functions that TR-069 provides are as follows:

- Configuration management
Installs CPE without configurations and modifies parameter settings remotely.
- Version management
Manages CPE software and firmware, for example, download the software version, and back up and restore the configuration file.
- Remote monitoring
Monitors the CPE status and performance, and queries the CPE status.
- GUI-based management
Manages NEs on the EMS in GUI mode.
- Alarm management
Reports alarms to the EMS and instructs the EMS to delete an alarm in time once the alarm is cleared.

Implementation

As a CPE, EGW1520 supports TR-069, [Figure 7-282](#) shows TR-069 network.

Figure 7-282 TR-069 network diagram



ACS	Auto-Configuration Server
BRAS	Broadband Remote Access Server
DSLAM	Digital Subscriber Line Access Multiplexer
CPE	Customer Premises Equipment

NOTE

EGW1520 uses the ADSL port or WAN port to connect to ACS. The preceding figure uses the ADSL port as an example.

Specification

- TR-069
- TR-098
- TR-104

Limitation

N/A

Setting TR-069 Parameters on the ACS

This topic describes how to set TR-069 parameters on the ACS.

TR-069 Connection Parameters

For details about configurations on the ACS, see the related ACS configuration guide. This topic only lists TR-069 parameters for the ACS to connect to EGW1520, as shown in [Table 7-69](#).

Table 7-69 TR-069 connection parameters

Parameter	Description
ACS URL	Indicates the ACS URL. For example, http://www.acs.com .
ACS User Name	Indicates the user name for the ACS to authenticate the TR-069 client, which must be the same as the user name on the ACS.
ACS Password	Indicates the password for the ACS to authenticate the TR-069 client, which must be the same as the user name on the ACS.
Connection Request User Name	Indicates the user name for the TR-069 client to authenticate the ACS, which must be the same as the user name on the TR-069 client.
Connection Request Password	Indicates the password for the TR-069 client to authenticate the ACS, which must be the same as the user name on the TR-069 client.
Connection Request URL	Indicates the URL of the TR-069 client. For example, http://192.168.1.1:8081/CPE . 192.168.1.1 is the IP address of the EGW1520 local area network (LAN) gateway.

Setting TR-069 Parameters on the CPE

This topic describes how to set TR-069 parameters on the EGW1520.

Prerequisites

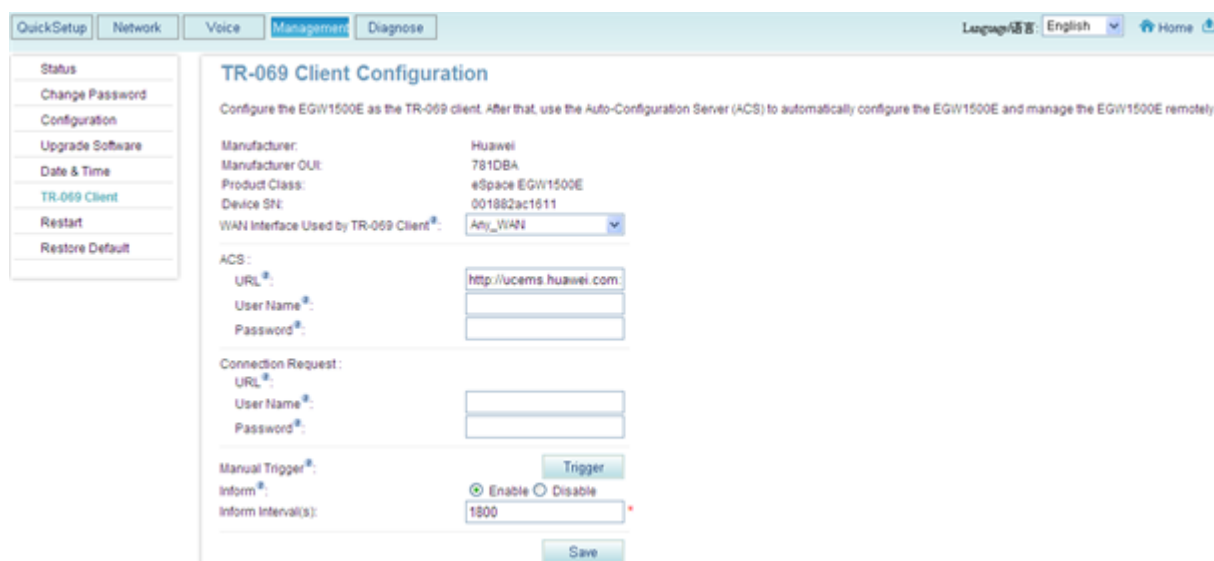
You have logged in to the web management system. For details, see [7.7.1 Web Management](#).

Procedure

- Step 1** On the web management system, choose **Management > TR-069 Client** from the navigation tree.

The page shown in [Figure 7-283](#) is displayed.

Figure 7-283 TR-069 client configuration




Step 2 Set parameters according to [Table 7-70](#).

Table 7-70 Parameter description

Parameter	Description
Manufacturer	Indicates the device manufacturer.
Manufacturer OUI	Indicates the organizationally Unique Identifier (OUI) of the manufacturer.
Product Class	Indicates the device model.
Device SN	Indicates the device sequence number.
WAN Interface Used by TR-069 Client	Indicates the WAN port on the TR-069 client connected to the ACS.
ACS URL	Indicates the ACS URL. For example, http://www.acs.com.
ACS User Name	Indicates the user name for the ACS to authenticate the TR-069 client, which must be the same as the user name on the ACS.
ACS Password	Indicates the password for the ACS to authenticate the TR-069 client, which must be the same as the user name on the ACS.
Connection Request URL	Indicates the URL of the TR-069 client.
Connection Request User Name	Indicates the user name for the TR-069 client to authenticate the ACS, which must be the same as the user name on the TR-069 client.
Connection Request Password	Indicates the password for the TR-069 client to authenticate the ACS, which must be the same as the

Parameter	Description
	user name on the TR-069 client.
Manual Trigger	Initiates the session to the ACS manually by clicking Trigger .
Inform	Indicates whether to initiate a session to the ACS periodically.
Inform Interval(Sec)	Indicates the interval to initiate a session to the ACS, in seconds. The default value is 1800.

Step 3 Click  to save the settings.

----End

Result

After the EGW1520 is connected to the ACS by using TR-069, use ACS to configure and manage the EGW1520. [TR-069 parameters reference](#) lists parameters in the TR-069 data model.

8 Diagnosis Mode

About This Chapter

This topic describes diagnosis modes for the EGW1520.

[8.1 Enabling the Debug Log](#)

This topic describes how to enable the debug log for each process. The system can generate the debug logs for different processes.

[8.2 Configuring Traffic Mirroring](#)

This section describes how to configure traffic mirroring to capture packets. Traffic mirroring allows you to use a packet capture tool on the mirroring port to obtain information about packets entering or leaving the monitored port.

[8.3 Downloading Black Box Files](#)

This topic describes how to download black box files.

[8.4 Pinging IP Addresses](#)

This topic describes how to ping an IP address. Using the ping function, you can ping the peer device of the EGW1520 to check the connection between them.

8.1 Enabling the Debug Log

This topic describes how to enable the debug log for each process. The system can generate the debug logs for different processes.

Large amounts of logs are generated during the EGW1520 running process.

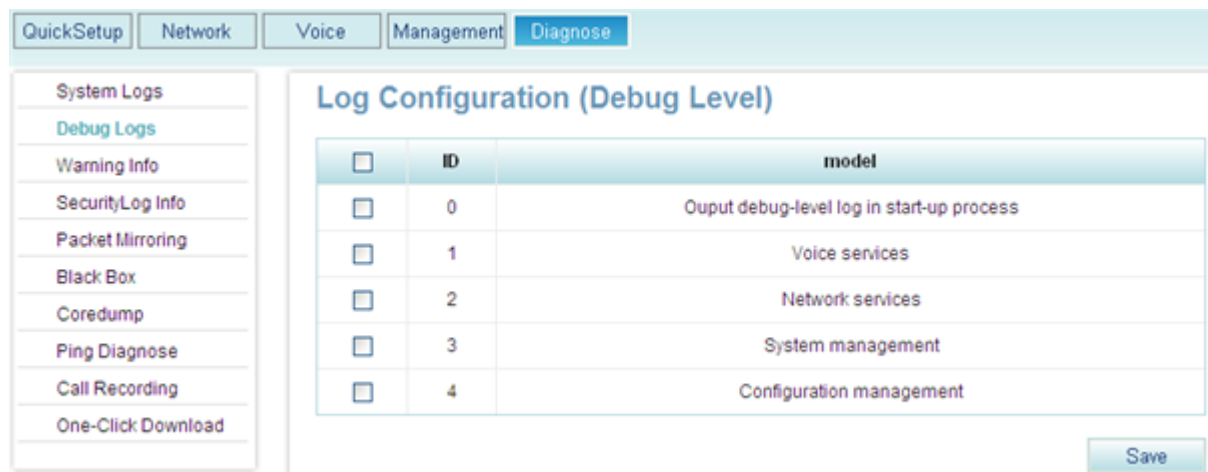
By default, the system does not generate the debug logs. To generate the debug logs, enable the debug log and log generation function, set the log level to debug, and configure the log saving mode. For details, see [9.4 Managing System Logs](#).

Procedure

Step 1 On the web management system, choose **Diagnose > Debug Logs** from the navigation tree.

The page shown in [Figure 8-1](#) is displayed.


Figure 8-1 Enabling the debug logs for each module



Step 2 Enable the debug logs for modules according to [Table 8-1](#).

Table 8-1 Parameter description

Parameter	Description
Output debug-level log in start-up process	Debug logs are generated when the system starts. For example, when you want to debug the system during system startup, enable this function.
Voice services	Debug logs for voice services are generated. For example, when the synchronization server cannot synchronize service data, enable this function.
Network services	Debug logs for network services are generated. For example, when you want to view the IP address obtained by EGW1520 that functions as a client, enable this function.
System management	Debug logs for system management are generated. For example, when you want to view message sending and receiving information in the system, enable this function.
Configuration management	Debug logs for configuration management are generated. For example, when you want to monitor network time synchronization, enable this function.

Step 3 Click  to save the settings.

----End

8.2 Configuring Traffic Mirroring

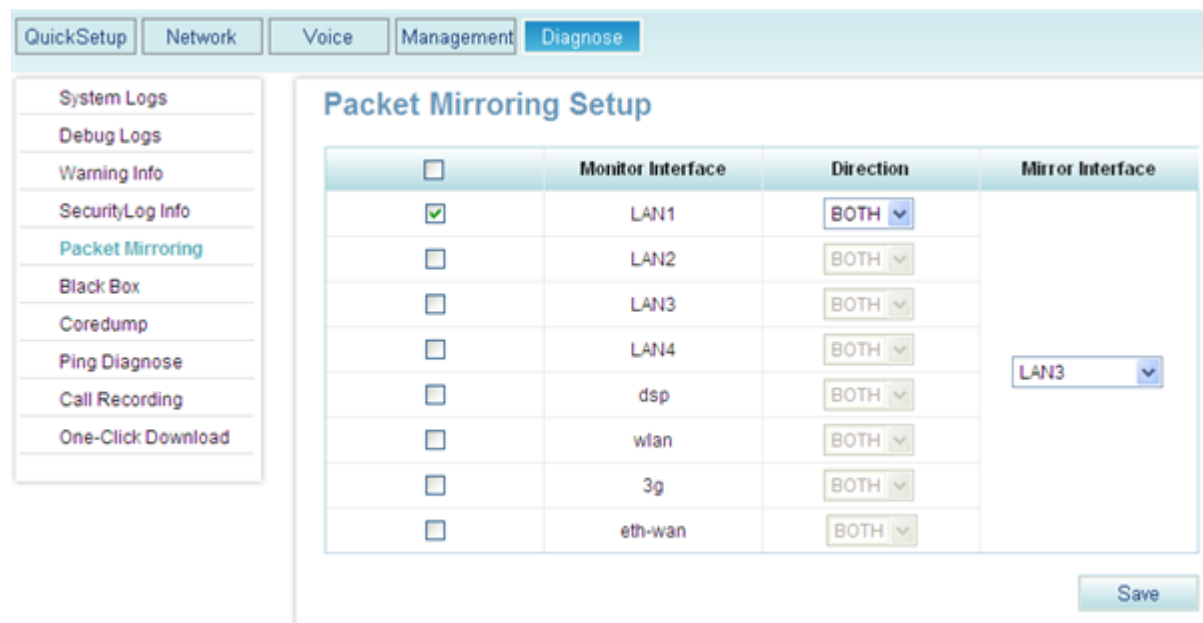
This section describes how to configure traffic mirroring to capture packets. Traffic mirroring allows you to use a packet capture tool on the mirroring port to obtain information about packets entering or leaving the monitored port.

Procedure

Step 1 On the web management system, choose **Diagnose** > **Packet Mirroring** from the navigation tree.

The page shown in [Figure 8-2](#) is displayed.

Figure 8-2 Traffic mirroring




Step 2 Set parameters according to [Table 8-2](#).

Table 8-2 Parameters

Item	Description
Monitored port	Port that the mirroring port monitors.
Direction	Direction in which packets are monitored: <ul style="list-style-type: none"> IN: Only the packets that the EGW1520 receives on the monitored port are monitored. OUT: Only the packets that the EGW1520 sends from the monitored port are monitored. BOTH: The packets that the monitored port receives and sends out are monitored.
Mirroring port	Port that captures packets from the monitored port. As shown in Figure

Item	Description
	8-2, interface LAN3 captures the incoming and outgoing packets on interface LAN1. NOTE Manage the captured packets carefully.

Step 3 Click  to save the settings.
----End

8.3 Downloading Black Box Files

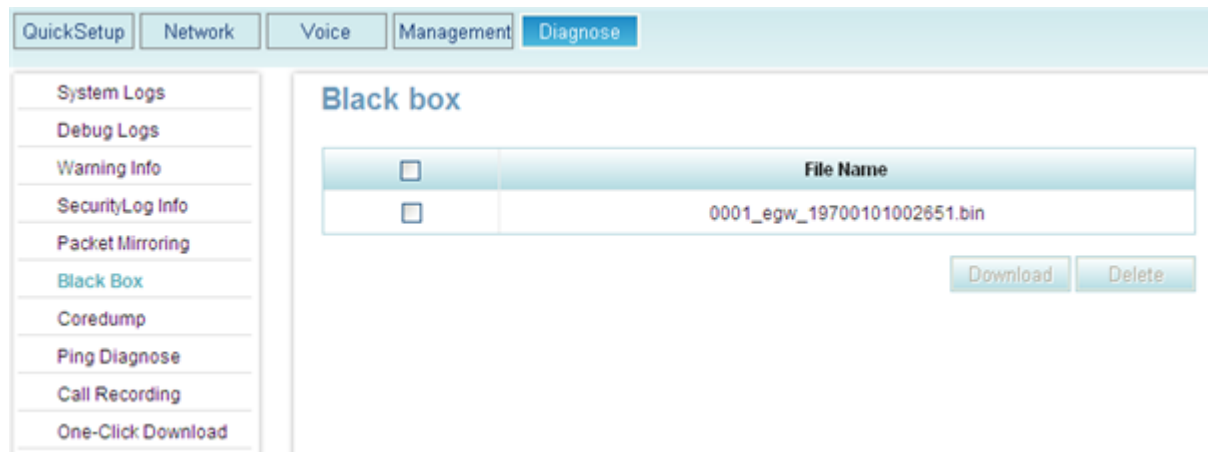
This topic describes how to download black box files.

Critical or minor defects that occur during the EGW1520 running process are recorded in black box files. You can view black box files to analyze system exceptions.


Procedure

Step 1 On the web management system, choose **Diagnose** > **Black Box** from the navigation tree.
The page shown in [Figure 8-3](#) is displayed.

Figure 8-3 Downloading black box files



Step 2 Select a black box file to download.

Step 3 Click  to save the file to the local host or other hosts on the network as prompted.

 **NOTE**

To delete a black box file, select the file and click



----End

8.4 Pinging IP Addresses

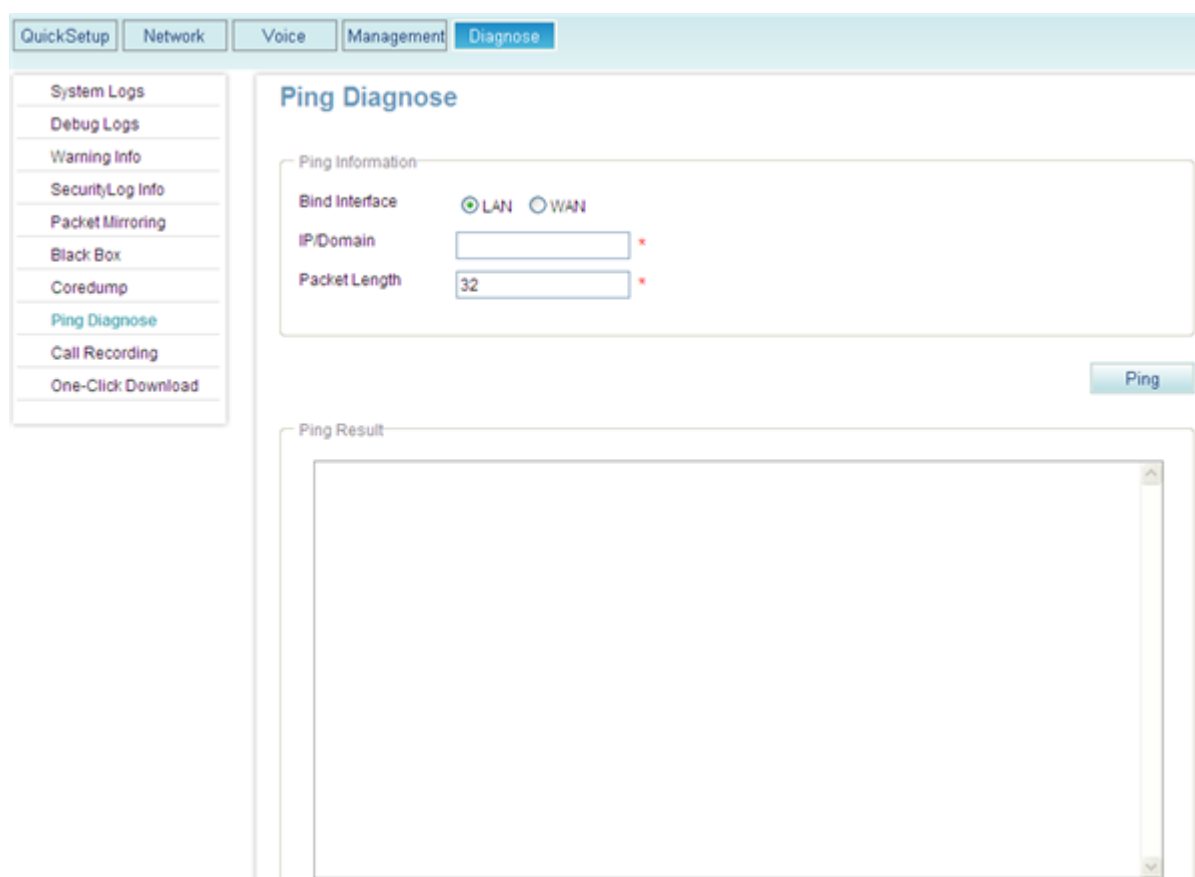
This topic describes how to ping an IP address. Using the ping function, you can ping the peer device of the EGW1520 to check the connection between them.

Procedure

Step 1 On the web management system, choose **Diagnose** > **Ping Diagnose** from the navigation tree.

The page shown in [Figure 8-4](#) is displayed.

Figure 8-4 IPPing Diagnose page



Step 2 Select **Bind Interface**.

Step 3 Set parameters according to [Table 8-3](#).

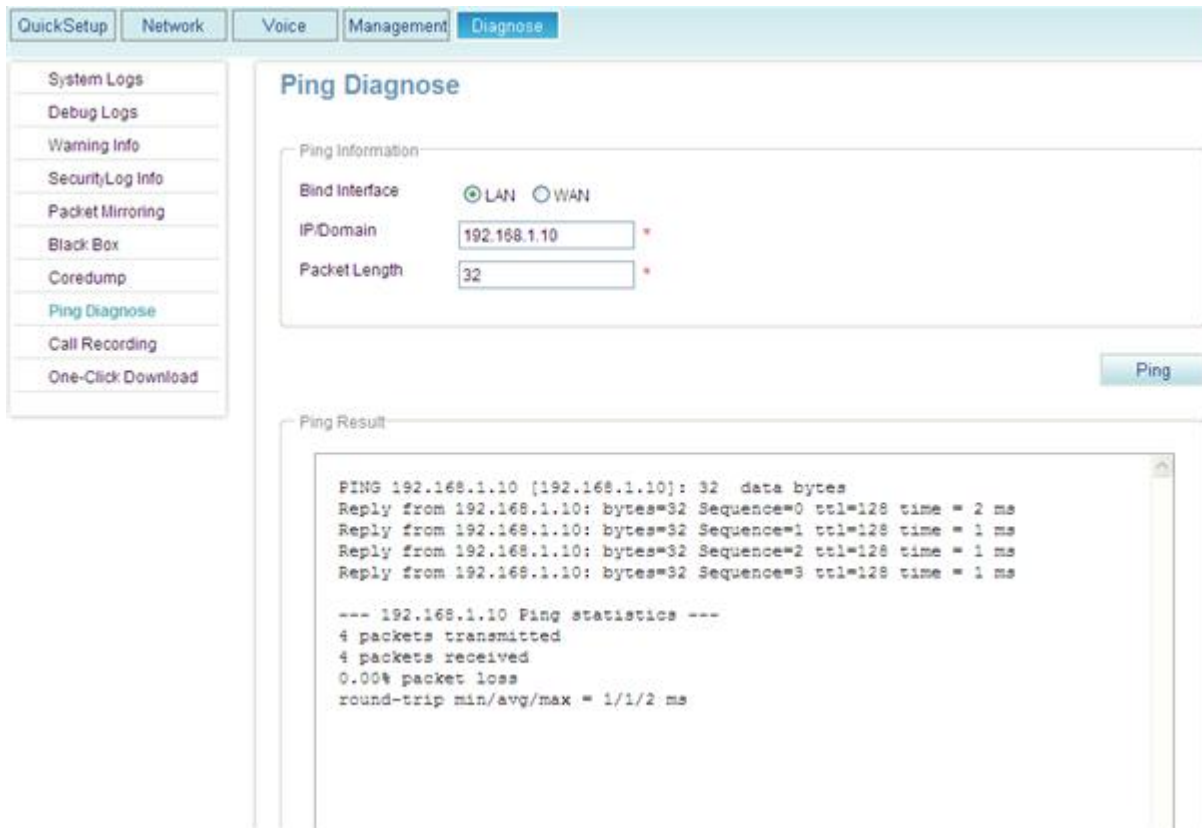
Table 8-3 Parameter settings

Parameter	Description
IP/Domain	The IP address that will be pinged.
Packet Length	Size of packets that are sent during the ping operation. The packet size ranges from 20 bytes to 1500 bytes.

Step 4 Click .

The page shown in [Figure 8-5](#) is displayed.

Figure 8-5 Diagnosis result



----End

9 System Management

About This Chapter

This topic describes how to manage and maintain the EGW1520 in different modes.

[9.1 Configuring the System Time](#)

This topic describes how to configure the system time manually and how to synchronize the NTP server time.

[9.2 Managing the Configuration File](#)

This topic describes how to back up and load the configuration file.

[9.3 Restoring Factory Settings](#)

This topic describes how to restore factory settings.

[9.4 Managing System Logs](#)

This topic describes how to manage system logs.

[9.5 Viewing Alarms](#)

This topic describes how to view alarms. You can analyze the exceptions occur during system running according to the alarms.

[9.6 Viewing Security Logs](#)

This topic describes how to view security logs to query the recent operations.

[9.7 Viewing Electronic Labels](#)

You can learn about the device information based on its electronic label.

[9.8 Downloading Call Records](#)

This topic describes how to back up call records on the local computer.

[9.9 One-Click Download](#)

This topic describes how to use the one-click download function to collect system information. If the system is faulty, you can download system information and send it to the maintenance personnel for fault location.

[9.10 Changing the Password](#)

This topic describes how to change the password for logging in to the EGW1520.

9.11 Upgrading Host Software

This topic describes how to upgrade host software.

9.12 Uploading Voice Files

This topic describes how to upload voice files.

9.13 Restarting the EGW1520

This topic describes how to restart the EGW1520.

9.1 Configuring the System Time

This topic describes how to configure the system time manually and how to synchronize the NTP server time.

The EGW1520 requires correct time to report alarms, trace malicious calls, and generate logs. The EGW1520 allows you to configure the system time in either of the following modes:

- Configure time manually on the local computer. For details, see [Configuring Local Time](#).
 - Sets system time on the web management system.
 - Supports setting time zones and daylight saving time (DST).
- Synchronize time automatically by using the NTP server. For details, see [Configuring NTP Time](#).

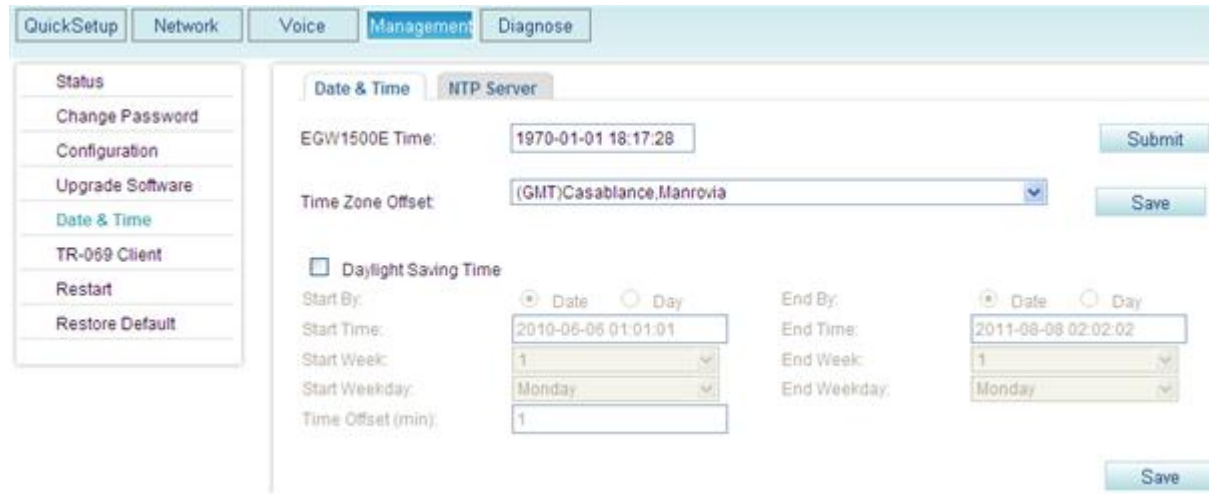
NTP functions at the application layer. Based on the IP and the User Datagram Format (UDP), the NTP is used to synchronize the time between distributed time servers and clients. As the EGW1520 supports the NTP protocol, it can function as an NTP client to synchronize time with the NTP server.

Configuring Local Time

- Step 1** On the web management system, choose **Management > Date & Time** from the navigation tree.

The page shown in [Figure 9-1](#) is displayed.

Figure 9-1 Date & Time tab page (1)



Step 2 Set EGW1520 Time as required.

Step 3 Click  to save the settings.

 **NOTE**

When the EGW1520 restarts, the system time that you configure is restored to the default setting (such as 1970-01-01 00:00:00).

Step 4 (Optional) Configure the time zone.

1. Set parameters according to [Table 9-1](#).

Table 9-1 Parameter description (1)

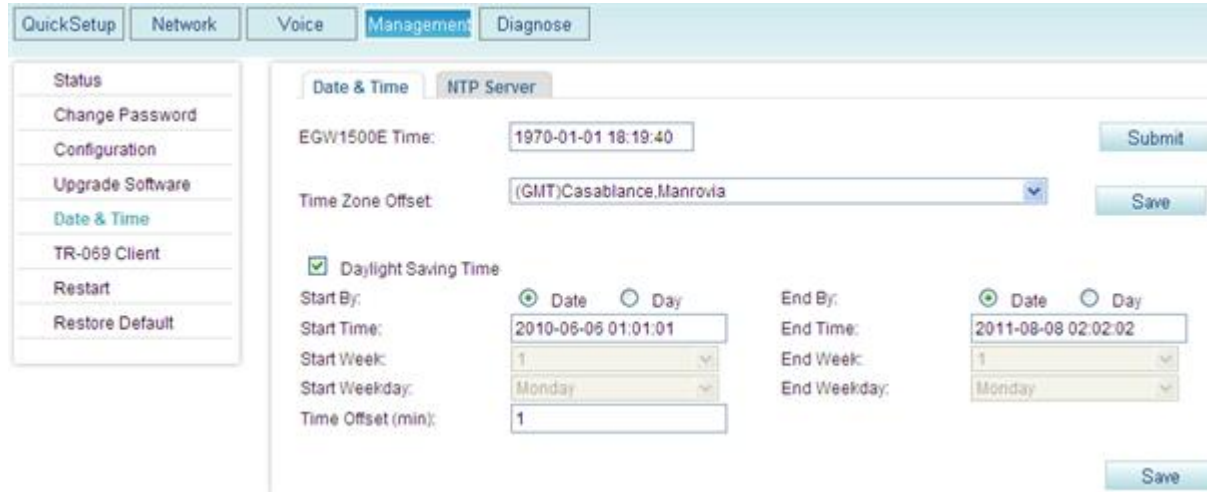
Parameter	Description
Time zone Offset	Set the time zone. <ul style="list-style-type: none"> • GMT+: east of GMT • GMT-: west of GMT For example, set this parameter to GMT+ and 08:00 (GMT+8 time zone).

2. Click  to save the settings.

Step 5 (Optional) Configure the DST.

1. Click **Daylight Saving Time**.
The page shown in [Figure 9-2](#) is displayed.

Figure 9-2 Configuring the DST



2. Set parameters according to [Table 9-2](#).

Table 9-2 Parameter description (2)

Parameter	Description
Start By	Start type of the DST. <ul style="list-style-type: none"> • Date: The start time is a date. • Day: The start time is a day in a week.
End By	End type of the DST. <ul style="list-style-type: none"> • Date: The end time is a date. • Day: The end time is a day in a week.
Start Time	DST start time.
End Time	DST end time.
Start Week	Week counting from the start time. This parameter is valid when Type is set to Start Day .
End Week	Week counting from the end time. This parameter is valid when Type is set to End Day .
Start Weekday	Day in a week counting from the start time. This parameter is valid when Type is set to Start Day .
End Weekday	Day in a week counting backward from the end time. This parameter is valid when Type is set to End Day .
Time Offset (min)	DST offset. If the DST function is enabled, the system time is the original time plus the offset within the validity period of the DST.

3. Click  to save the settings.

----End

Configuring NTP Time

- Step 1** On the web management system, choose **Management > Date & Time** from the navigation tree.
- Step 2** Click the **NTP Server** tab.
- Step 3** Click **Network Time Synchronization Service**.

The page shown in [Figure 9-3](#) is displayed.

Figure 9-3 Configuring the NTP server

- Step 4** Set parameters according to [Table 9-3](#).

Table 9-3 Parameter description (3)

Parameter	Description
Main NTP Server	IP address or domain name of the active NTP server.
Sub NTP Server	IP address or domain name of the standby NTP server.
Synchronization Interval	Period of synchronizing the NTP server time.

Parameter	Description
(s)	
Synchronization Status	Status of NTP server time synchronization.
Encryption Type	The value is the same as that of the NTP server.
Authentication Key ID	The value is the same as that of the NTP server.
Password	The value is the same as that of the NTP server.

Step 5 Click  to save the settings.

 **NOTE**

Check whether the NTP server time is the same as the EGW1520 time on the **Date & Time** tab page. If yes, the NTP server time synchronization is successful.

----End

9.2 Managing the Configuration File

This topic describes how to back up and load the configuration file.

During routine maintenance, configuration data may be missing due to abnormal device restart or upgrade failure. Therefore, you are advised to back up the configuration file periodically.

After backup is complete, you can load the configuration file as required to recover data.

The EGW1520 allows you to back up and load the configuration file in web mode. You can:

- Back up the configuration file, which contains all the configurable data and can be encrypted. For details, see [Backing Up the Configuration File](#).
- Load the configuration file in HTTP mode. For details, see [Loading the Configuration File \(HTTP\)](#).
- Load the configuration file in FTP mode. For details, see [Loading the Configuration File \(FTP\)](#).
- Load the configuration file in TFTP mode. For details, see [Loading the Configuration File \(TFTP\)](#).
- Load the configuration file in FTPS mode. For details, see [Loading the Configuration File \(FTPS\)](#).

 **NOTE**

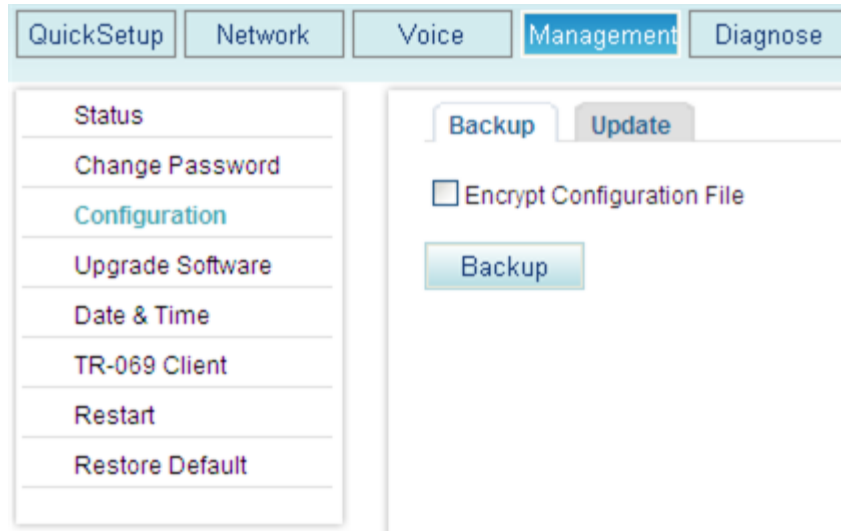
In FTP mode, data is transmitted in plain text. Load configuration files in FTP mode on trusted networks.

Backing Up the Configuration File


Step 1 On the web management system, choose **Management > Configuration** from the navigation tree.

The page shown in [Figure 9-4](#) is displayed.

Figure 9-4 Backing up the configuration file



Step 2 (Optional) Select **Encrypt Configuration File** to encrypt the configuration file.

Step 3 Click  to back up the configuration file to the local host or other hosts on the network as prompted.

NOTE

The configuration file is in .xml format. The default file name is in **CFG+WAN port's MAC address.xml**, for example, CFG001882ab2415.xml. You can also change the file name.

----End

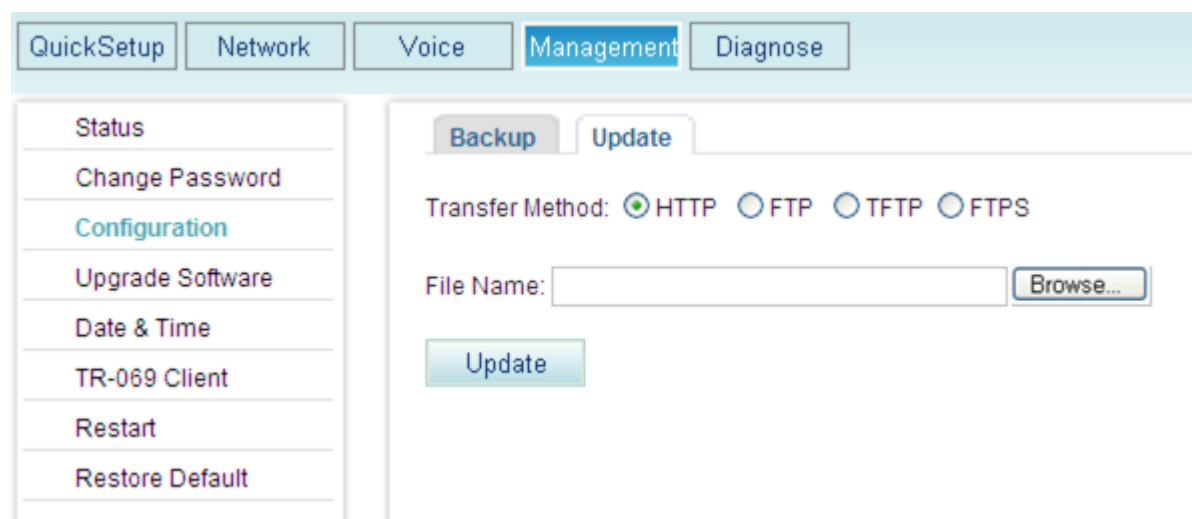
Loading the Configuration File (HTTP)

Step 1 On the web management system, choose **Management > Configuration** from the navigation tree.

Step 2 Click the **Update** tab.


The page shown in [Figure 9-5](#) is displayed.

Figure 9-5 Loading the configuration file (HTTP)



Step 3 Click **Browse** and select a configuration file.

Set the file path, which can be a local path, for example, **D:\CFG001882ab2415.xml**, or a network path, for example, **\\10.168.10.111\CFG001882ab2415.xml**.

Step 4 Click  and proceed as prompted.

After loading is successful, the EGW1520 automatically restarts. After the restart is complete, you can log in to the EGW1520 web management system.

 **NOTE**

- The restart takes 2 to 3 minutes depending on the device configuration. If the configuration data is more, the startup time is longer.
- If the uploading fails, the configuration data on the EGW1520 remains. You can reload the configuration file.
- After the LAN port restarts, the management IP address changes to the imported IP address.

----End

Loading the Configuration File (FTP)

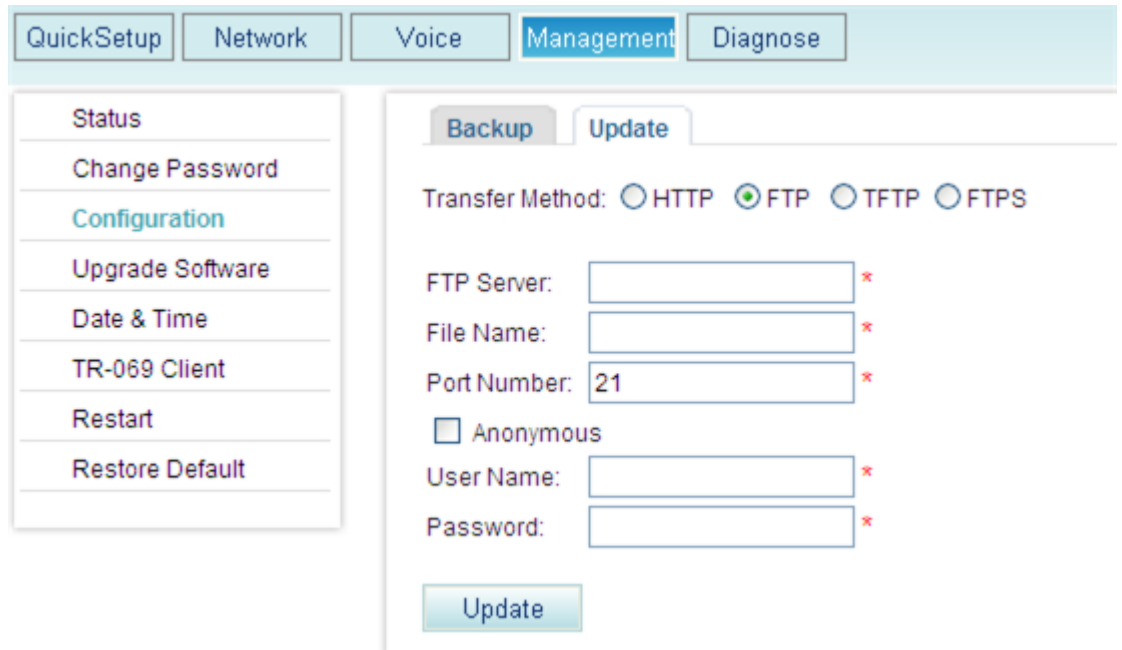
Step 1 On the web management system, choose **Management > Configuration** from the navigation tree.

Step 2 Click the **Update** tab.

Step 3 Click **FTP**.

The page shown in [Figure 9-6](#) is displayed.

Figure 9-6 Loading the configuration file (FTP)



Step 4 Set parameters according to [Table 9-4](#).

Table 9-4 FTP parameters

Parameter	Description
FTP Server	IP address of the FTP server. NOTE Ensure that the FTP service is enabled when configuration files are loaded and that the FTP server connects to the EGW1520 properly.
File Name	Relative path of the file to be uploaded. If the configuration file is stored in C:/ftp/egw/CFG001882ab2415.xml and the access path that is set on the FTP server is C:/ftp , set the relative path to egw/CFG001882ab2415.xml .
Port Number	Port number of the FTP server, which is 21 by default.
Anonymous	If you select Anonymous , the EGW1520 connects to the FTP server as an anonymous user that is the default user on the FTP server.
User Name	User name for logging in to the FTP server. This parameter is configured on the FTP server.
Password	Password for logging in to the FTP server. This parameter is configured on the FTP server.

Step 5 Click  and proceed as prompted.

After loading is successful, the EGW1520 automatically restarts. After the restart is complete, you can log in to the EGW1520 web management system.

 **NOTE**

- The restart takes 2 to 3 minutes depending on the device configuration. If the configuration data is more, the startup time is longer.
- If the uploading fails, the configuration data on the EGW1520 remains. You can reload the configuration file.
- After the LAN port restarts, the management IP address changes to the imported IP address.

----End

Loading the Configuration File (TFTP)

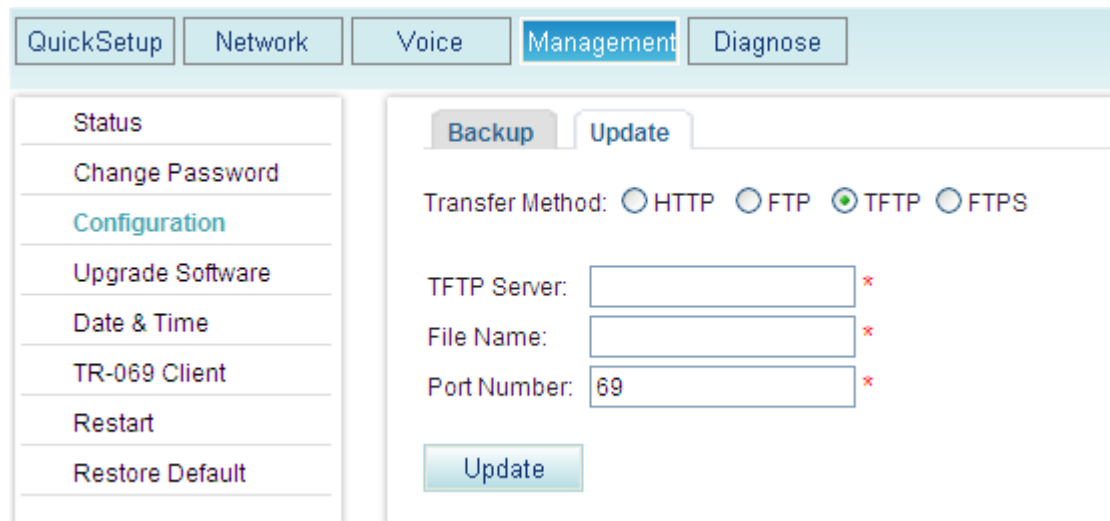
Step 1 On the web management system, choose **Management > Configuration** from the navigation tree.

Step 2 Click the **Update** tab.

Step 3 Click **TFTP**.

The page shown in [Figure 9-7](#) is displayed.

Figure 9-7 Loading the configuration file (TFTP)



The screenshot shows the web management interface with the following elements:

- Navigation tabs: QuickSetup, Network, Voice, **Management**, Diagnose.
- Left sidebar menu: Status, Change Password, **Configuration**, Upgrade Software, Date & Time, TR-069 Client, Restart, Restore Default.
- Right panel tabs: **Backup**, Update.
- Transfer Method: HTTP FTP TFTP FTPS
- TFTP Server: *
- File Name: *
- Port Number: *
- Update button:

Step 4 Set parameters according to [Table 9-5](#).

Table 9-5 TFTP parameters

Parameter	Description
TFTP Server	IP address of the TFTP server. NOTE

Parameter	Description
	Ensure that the TFTP service is enabled when configuration files are loaded and that the TFTP server connects to the EGW1520 properly.
File Name	Relative path of the file to be uploaded. If the configuration file is stored in C:/tftp/egw/CFG001882ab2415.xml and the access path that is set on the TFTP server is C:/tftp , set the relative path to egw/CFG001882ab2415.xml .
Port Number	Port number of the TFTP server, which is 69 by default.

Step 5 Click  and proceed as prompted.

After loading is successful, the EGW1520 automatically restarts. After the restart is complete, you can log in to the EGW1520 web management system.

 **NOTE**

- The restart takes 2 to 3 minutes depending on the device configuration. If the configuration data is more, the startup time is longer.
- If the uploading fails, the configuration data on the EGW1520 remains. You can reload the configuration file.
- After the LAN port restarts, the management IP address changes to the imported IP address.

----End

Loading the Configuration File (FTPS)

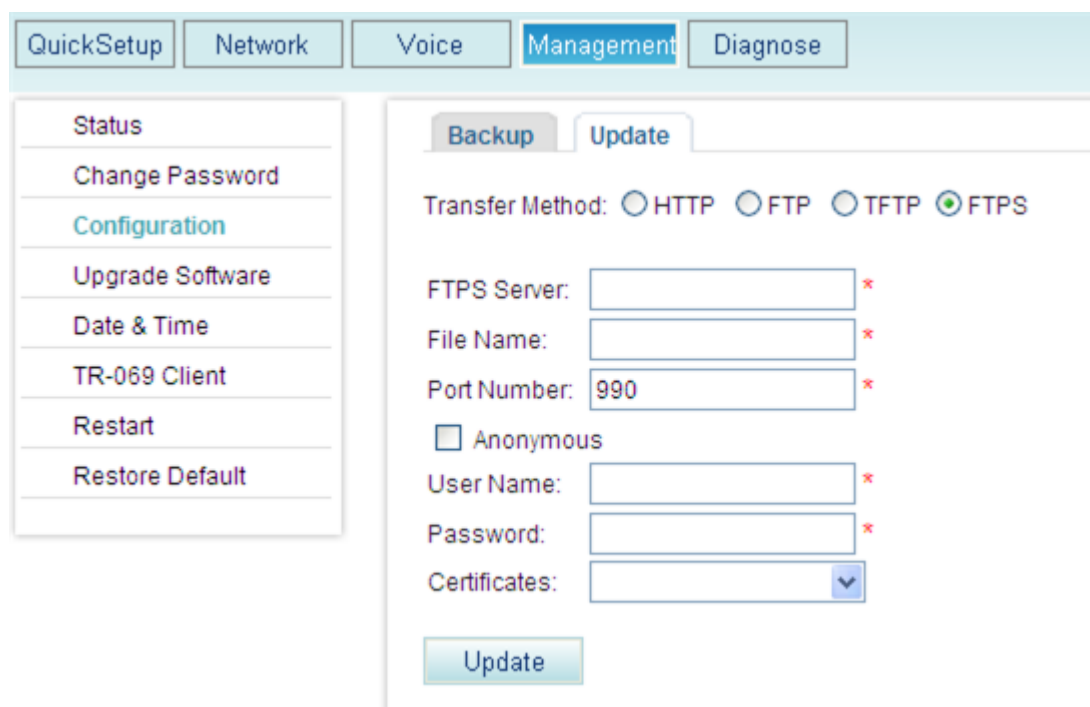
Step 1 On the web management system, choose **Management > Configuration** from the navigation tree.

Step 2 Click the **Update** tab.

Step 3 Click **FTPS**.

The page shown in [Figure 9-8](#) is displayed.

Figure 9-8 Loading the configuration file (FTPS)



Step 4 Set parameters according to [Table 9-6](#).

Table 9-6 FTPS parameters

Parameter	Description
FTPS Server	IP address of the FTPS server. NOTE Ensure that the FTPS service is enabled when configuration files are loaded and that the TFTP server connects to the EGW1520 properly.
File Name	Relative path of the file to be uploaded. If the configuration file is stored in C:/ftps/egw/CFG001882ab2415.xml and the access path that is set on the FTP server is C:/ftps , set the relative path to egw/CFG001882ab2415.xml .
Port Number	Port number of the FTPS server. The default port number is 990.
Anonymous	If Anonymous is selected, the EGW1520 connects to the FTPS server as an anonymous user.
User Name	User name for logging in to the FTPS server. This parameter is configured on the FTPS server.
Password	Password for logging in to the FTPS server. This parameter is configured on the FTPS server.
Certificates	Certificate for authenticate logins. NOTE Before using the certificate to authenticate logins, configure the certificate by

Parameter	Description
	referring to 7.5.7 Certificate .

Step 5 Click  and proceed as prompted.

After loading is successful, the EGW1520 automatically restarts. After the restart is complete, you can log in to the EGW1520 web management system.

 **NOTE**

- The restart takes 2 to 3 minutes depending on the device configuration. If the configuration data is more, the startup time is longer.
- If the uploading fails, the configuration data on the EGW1520 remains. You can reload the configuration file.
- After the LAN port restarts, the management IP address changes to the imported IP address.

----End

9.3 Restoring Factory Settings

This topic describes how to restore factory settings.

Before restoring factory settings, refer [9.2 Managing the Configuration File](#) to back up the configuration information of the current version.

After restoration, the EGW1520 restarts automatically to make the factory settings take effect. To view factory settings, log in to the web management system again.

To restore factory settings, press the **RESET** button on the device or perform operations on the web page.

RESET Button

Press **RESET** on the EGW1520 for longer than six seconds.


Web Mode

Step 1 On the web, choose **Management** > **Restore Default** from the navigation tree.

The page shown in [Figure 9-9](#) is displayed.

Figure 9-9 Restore page



Step 2 Click  and proceed as prompted.

 **NOTE**

After the EGW1520 restarts, the configuration data changes to factory settings. Use the IP address **192.168.1.1**, the user name **admin** and the password **Admin@123** to log in to the web management system again, see [7.7.1 Web Management](#).

----End

9.4 Managing System Logs

This topic describes how to manage system logs.

During the EGW1520 running, a large number of logs are generated and sent to the syslog management module. You can send the log file to the Huawei technical support for faults analysis. The EGW1520 provides the following log functions:

- Backs up the log file remotely.
If the remote backup function is configured, the syslog management module sends the log file to the log server for your remote maintenance. For details, see [Backing Up Log Files Remotely](#).
- Backs up the log file locally.
If the local backup function is configured, the log file is saved in the local flash memory. The EGW1520 allows you to download the latest log files from the flash memory on a web page. For details, see [Backing Up the Log File Locally](#).

 **NOTE**

The EGW1520 writes the flash memory when a 512 KB log is generated. When the size of generated logs reaches 2 MB, the earliest logs are overwritten by the latest ones.

- Sets the log level.

- Deletes the log file.
You can delete the log file in the local flash memory in web mode. For details, see [Deleting Logs](#).

Configuring Logs

Prerequisite

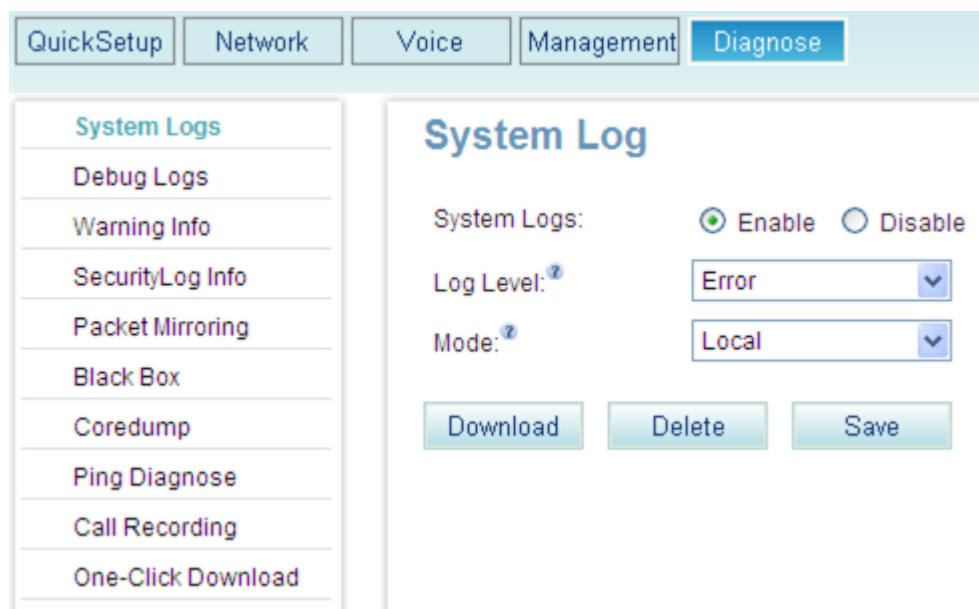
The log service has been started on the log server. The log path and log file name have been set.

Configuration Procedure

Step 1 On the web management system, choose **Diagnose** > **System Logs** from the navigation tree.

The page shown in [Figure 9-10](#) is displayed.

Figure 9-10 Enabling the function of generating logs



Step 2 Set log levels according to [Table 9-7](#).


Table 9-7 Log level

Parameter	Description
Log Level	<p>The options are as follows:</p> <ul style="list-style-type: none"> • Emergency: Error log, which indicates that a critical fault occurs and the system cannot be recovered. • Alert: Error log, which indicates that a severe fault occurs and must be rectified immediately. • Critical: Error log, which indicates that a major fault occurs. • Error: Error log, which indicates that a minor fault occurs. • Warning: Warning log, which indicates that certain functions are

Parameter	Description
	<p>unavailable.</p> <ul style="list-style-type: none">• Notice: Notification log, which indicates that a major event occurs.• Informational: Informational log, which indicates common events and status information• Debugging: Debug log, which records information about system internal debugging. <p>NOTE To generate debug logs, set the log level to Debugging and enable the debug log for each module. For details, see 8.1 Enabling the Debug Log.</p>

 **NOTE**

The EGW1520 only sends log information whose level is equal to or higher than that you set to the log server. The highest level is **Emergency** and the lowest level is **Debugging**.

Step 3 Click  to save the settings.

----End

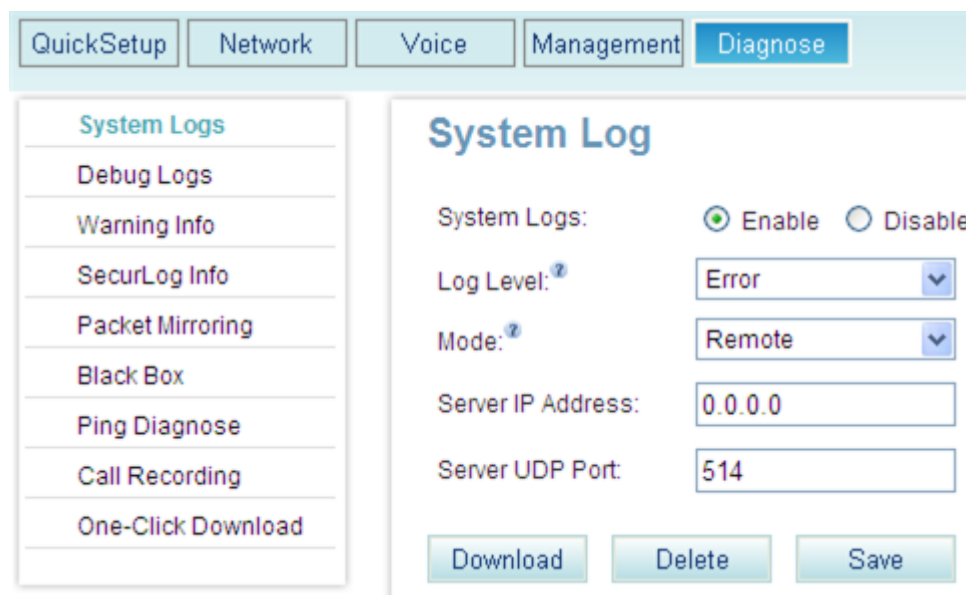
Backing Up Log Files Remotely

Step 1 Enable the function of generating logs. For details, see [Configuring Logs](#).

Step 2 Set **Mode** to **Remote**.

The page shown in [Figure 9-11](#) is displayed.


Figure 9-11 Remote backup



Step 3 Set parameters according to [Table 9-8](#).

Table 9-8 Parameter description

Parameter	Description
Mode	Log backup mode. The options are as follows: <ul style="list-style-type: none"> Local: Saves the log file to the local computer. Remote: Sends the log file to the remote log server. Both: Sends the log file to the local computer and the remote log server.
Server IP Address	IP address of the log server. Set this parameter when Mode is set to Remote or Both .
Server UDP Port	Port number of the log server. Set this parameter when Mode is set to Remote or Both . The default value is 514 .

Step 4 Click  to save the settings.

The log file is automatically sent to the log server.

----End

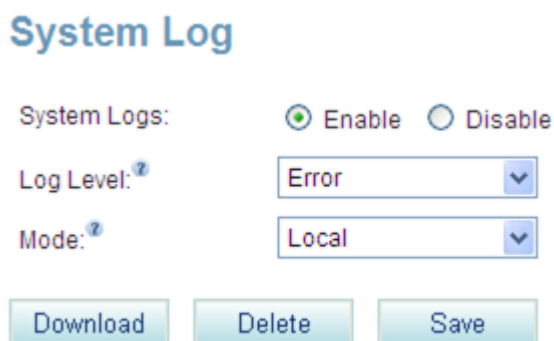
Backing Up the Log File Locally

Step 1 Enable the function of generating logs. For details, see [Configuring Logs](#).

Step 2 Set **Mode** to **Local**.

The page shown in [Figure 9-12](#) is displayed.

Figure 9-12 Local backup



The screenshot shows the 'System Log' configuration interface. At the top, the title 'System Log' is displayed in blue. Below it, there are three rows of configuration options: 'System Logs:' with radio buttons for 'Enable' (selected) and 'Disable'; 'Log Level:' with a dropdown menu set to 'Error'; and 'Mode:' with a dropdown menu set to 'Local'. At the bottom, there are three buttons: 'Download', 'Delete', and 'Save'.

Step 3 Click  to save the settings.

The log file will be automatically saved to the local flash memory.

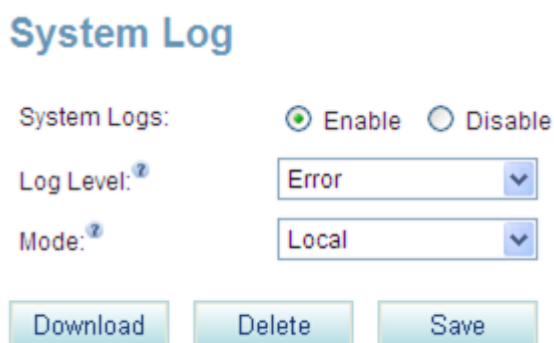
----End

Downloading Logs


Step 1 Enable the function of generating logs. For details, see [Configuring Logs](#).

The page shown in [Figure 9-13](#) is displayed.

Figure 9-13 Downloading logs



The screenshot shows the 'System Log' configuration interface, identical to Figure 9-12. It displays the 'System Log' title, 'System Logs' (Enable selected), 'Log Level' (Error), and 'Mode' (Local). The 'Download' button is highlighted with a light blue background.

Step 2 Click , and back up log files to the local host or other hosts on the network as prompted.

 **NOTE**

- The log file is in .log format. The default file name is in **Log+Current EGW1520 system date.log** format, for example, **Log20100101.log**. You can also change the file name.
- After downloading the log file, you can delete the log file from the flash memory according to [Deleting Logs](#).

----End

Deleting Logs

You can delete old logs from the flash memory.

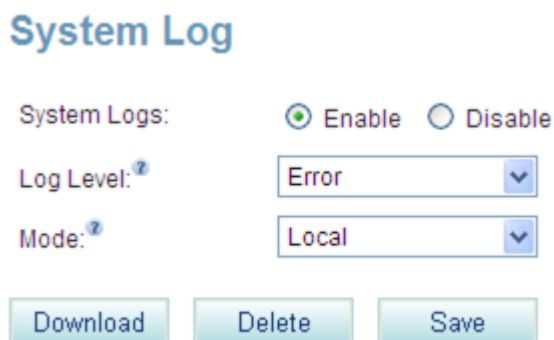
 **NOTE**

Log information that is sent to the log server is not affected.

Step 1 Enable the function of generating logs. For details, see [Configuring Logs](#).

The page shown in [Figure 9-14](#) is displayed.

Figure 9-14 Deleting logs



Step 2 Click  and proceed as prompted.

----End

9.5 Viewing Alarms

This topic describes how to view alarms. You can analyze the exceptions occur during system running according to the alarms.


Procedure

Step 1 On the web management system, choose **Diagnose > Warning Info** from the navigation tree.


The page shown in [Figure 9-15](#) is displayed.

Figure 9-15 Alarms

ID	Level	Time	Warning Info
1	Minor	1970-01-03 03:03:03	the admin username or password may be wrong
2	Minor	1970-01-03 03:03:04	the admin username or password may be wrong
3	Minor	1970-01-01 00:01:33	System reboot completed, Upgrade image.
4	Minor	1970-01-01 00:01:35	System reboot completed, Upgrade image.
5	Minor	1970-01-01 00:02:34	the conf username or password may be wrong
6	Minor	1970-01-01 15:52:03	ppp connection down,layer 3 is deleted
7	Minor	1970-01-01 00:01:43	System reboot completed, Restore config.
8	Minor	1970-01-01 00:01:44	System reboot completed, Restore config.
9	Minor	1970-01-01 00:23:19	IP connection down,layer 3 is deleted
10	Minor	1970-01-02 14:32:26	the admin username or password may be wrong
11	Minor	1970-01-01 00:01:45	System reboot completed, Restore config.
12	Minor	1970-01-01 00:01:32	System reboot completed, Unknown 0xd8cf.
13	Major	1970-01-01 00:00:42	lan4 link up
14	Major	1970-01-01 00:00:43	lan2 link up
15	Minor	1970-01-01 00:01:33	System reboot completed, Unknown 0xf9cf.
16	Major	1970-01-01 09:47:40	lan3 link up
17	Major	1970-01-01 09:47:59	lan3 link down
18	Major	1970-01-01 09:48:02	lan3 link up
19	Major	1970-01-01 09:51:00	lan2 link down
20	Major	1970-01-01 09:51:02	lan2 link up

Step 2 Click  to save the file to the local host or other hosts on the network as prompted.

 **NOTE**

To delete all alarms, click .

----End

9.6 Viewing Security Logs

This topic describes how to view security logs to query the recent operations.



NOTE

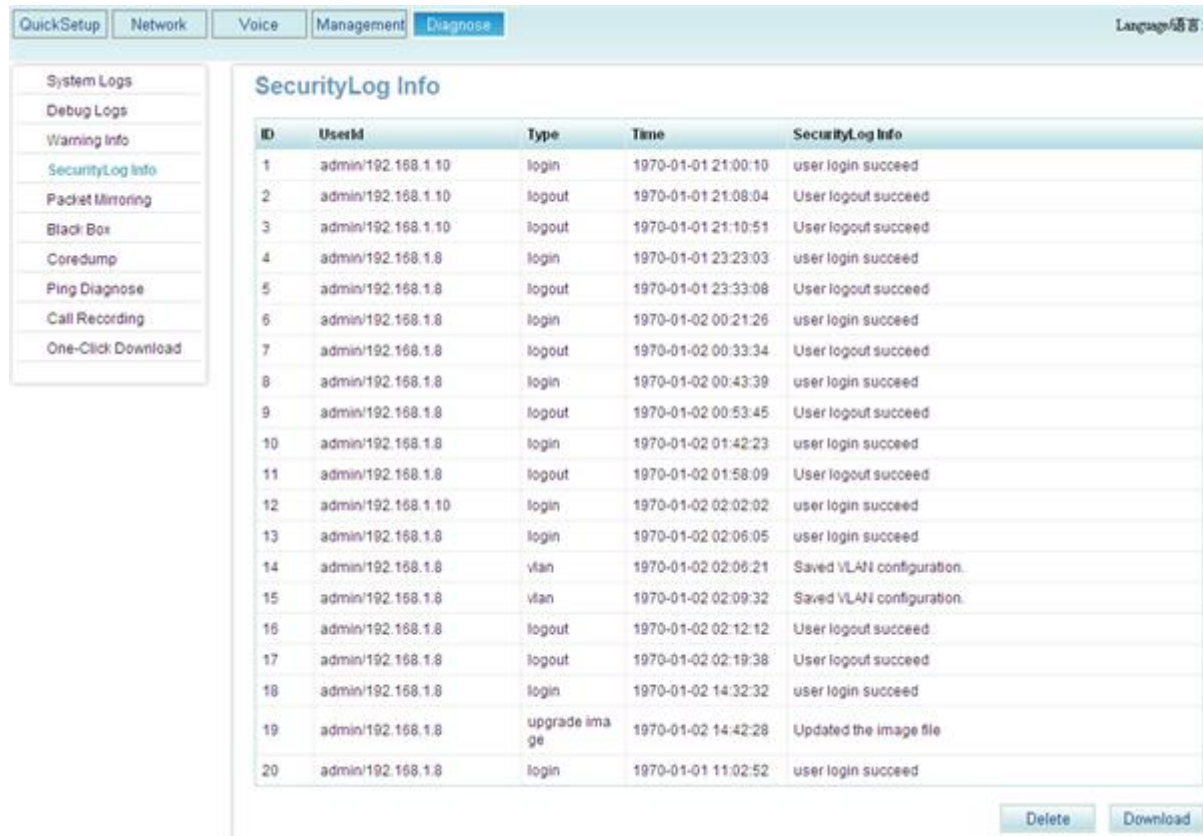
When automatic software upgrade is configured, the system generates security logs only for the first upgrade.


Procedure

Step 1 Choose **Diagnose > SecurityLog Info** from the navigation tree.

A page shown in [Figure 9-16](#) is displayed.


Figure 9-16 Viewing security logs



Step 2 Click  and back up log files to the local host or other hosts on the network as prompted.



NOTE

To delete all security logs, click .

. Only network administrators can delete all security logs.

Log sample

A log sample is as follows:

- User ID: 192.168.1.8
- Log type: alarmlog
- Time: 1970-01-01 01:28:30

- Log information: Downloaded alarm logs succeed

The following is a detailed description of the preceding log sample:

- admin/192.168.1.8: The user name is **admin** and the user ID is **192.168.1.8**.
- alarmlog: This log is an alarm log.
- 1970-01-01 01:28:30: Time when this operation is performed.
- Downloaded alarm logs succeed: This alarm log is downloaded successfully.

For details about the security log information, see [12.2 Security Log Information](#).

----End

9.7 Viewing Electronic Labels

You can learn about the device information based on its electronic label.

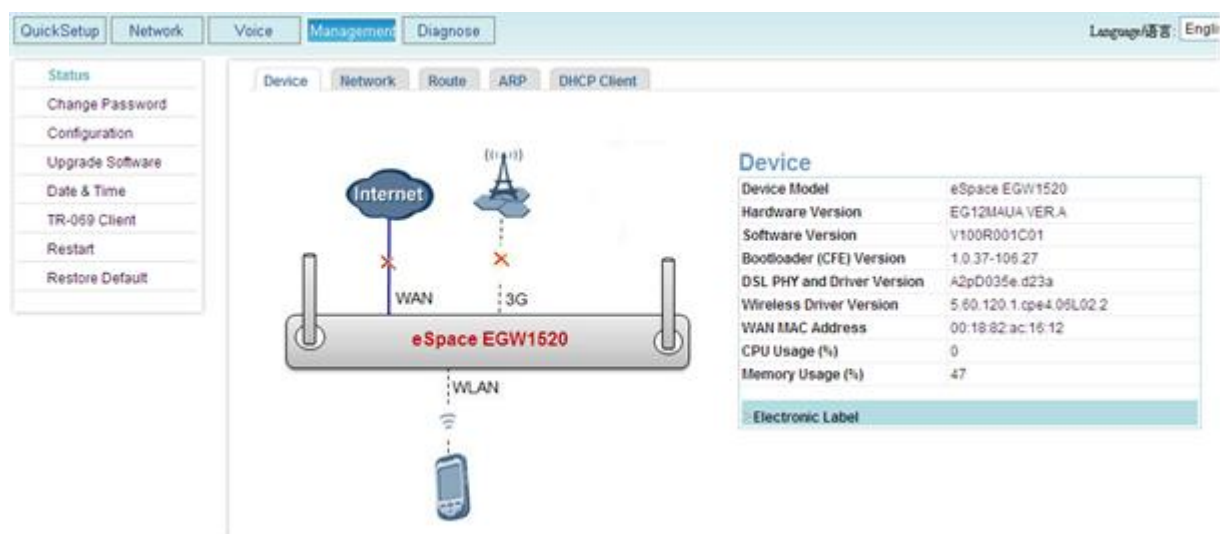
To view the electronic label of a device, perform the following operations:

Step 1 You have logged in to the web management system. For details, see [7.7.1 Web Management](#)

Step 2 Choose **Management > Status >** from the navigation tree.

The system displays a page, as shown in [Figure 9-17](#).

Figure 9-17 Electronic label (1)



Step 3 Click **Electronic Label** .

The system displays a page, as shown in [Figure 9-18](#).

Figure 9-18 Electronic label (2)

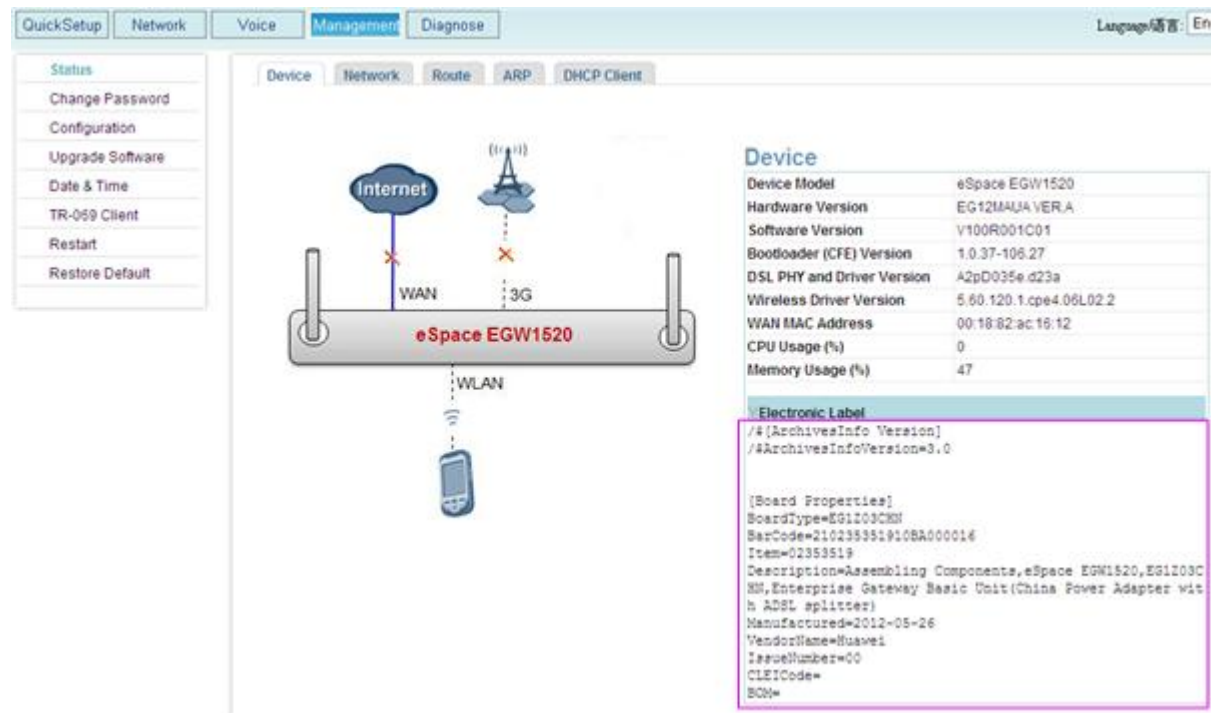


Table 9-9 describes the parameters in the electronic label information.

Table 9-9 Description of electronic label parameters

Parameter	Meaning
BoardType	Model of the field replaceable unit (FRU).
BarCode	Bar code of the FRU, which is the same as the device bar code.
Item	BBOM code of the FRU.
Description	Description of the FRU.
Manufactured	Manufacture date of the FRU.
VendorName	Vendor name of the FRU.
IssueNumber	Issue number of the FRU.
CLEICode	CLEI code of the FRU.
BOM	Specific item code of the FRU.

NOTE

The physical label is affixed to the bottom of the device.

----End

9.8 Downloading Call Records

This topic describes how to back up call records on the local computer.

The call record backup function has the following features:

- Saves the latest 5000 records. When the number of saved call records reaches 5,000, the system overwrites the earliest call records to save the latest ones.
- Saves 40 call records each time. If the number of latest call records is smaller than 40, the system saves call records at an interval of four hours.
- Saves the call start and end time, and the calling and called numbers.

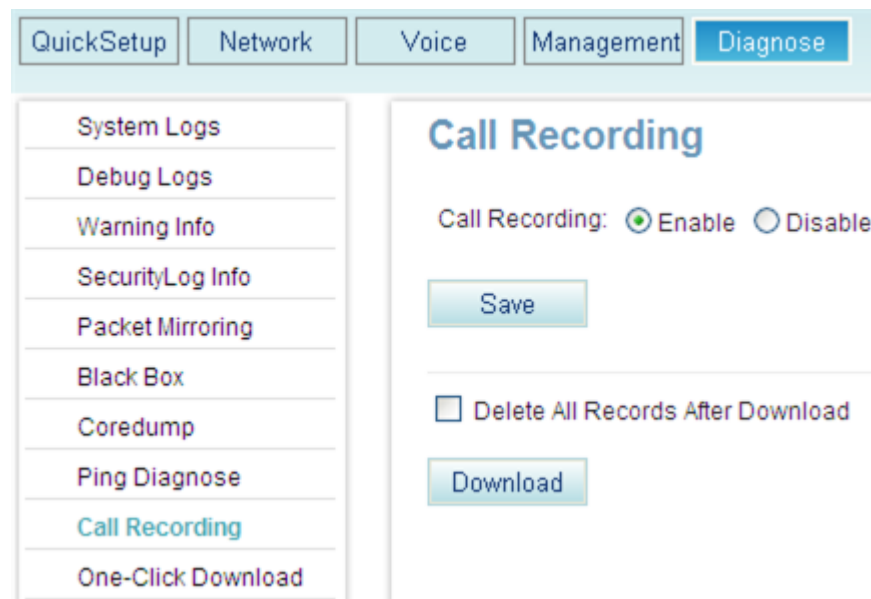
Configuration procedure

Step 1 On the web management system, choose **Diagnose** > **Call Recording** from the navigation tree.

Step 2 Set **Call Recording** to **Enable**.

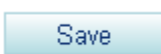
The page shown in [Figure 9-19](#) is displayed.


Figure 9-19 Downloading call records



NOTE

By default, the system disables the call record backup function.

Step 3 Click  to save the settings.

Step 4 Click  to download call records that are saved. Download call records to a local host or other hosts on the network.

 **NOTE**

- The call record file must be in the .txt format. The default file name is in **CDR+Current EGW1520 system date.txt** format, for example, **CDR20110101.txt**. You can also change the file name.
- Click the **Delete All Records After Download** option button. Then the web management system will delete call records after the downloading is complete.

----End

9.9 One-Click Download

This topic describes how to use the one-click download function to collect system information. If the system is faulty, you can download system information and send it to the maintenance personnel for fault location.

The EGW1520 provides the one-click download function for you to collect the following information:

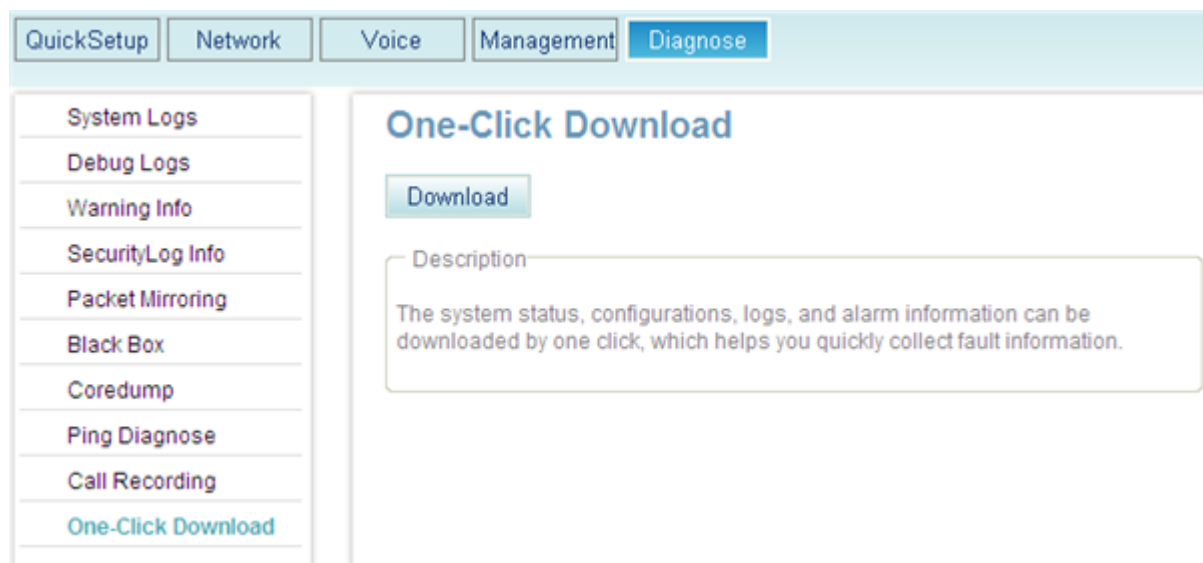
- System configurations (device model, hardware version, software version, MAC address on WAN port, IP address on WAN port, and IP address on LAN port)
- System logs
- Alarm information


Procedure

- Step 1** On the web management system, choose **Diagnose > One-Click Download** from the navigation tree.

The page shown in [Figure 9-20](#) is displayed.

Figure 9-20 One-click download



Step 2 Click  to download information.

----End

9.10 Changing the Password

This topic describes how to change the password for logging in to the EGW1520.

The EGW1520 allows a maximum of 10 users to log in at the same time.

The new password takes effect upon the next login. When a user changes the password, other users who have logged in are not affected.

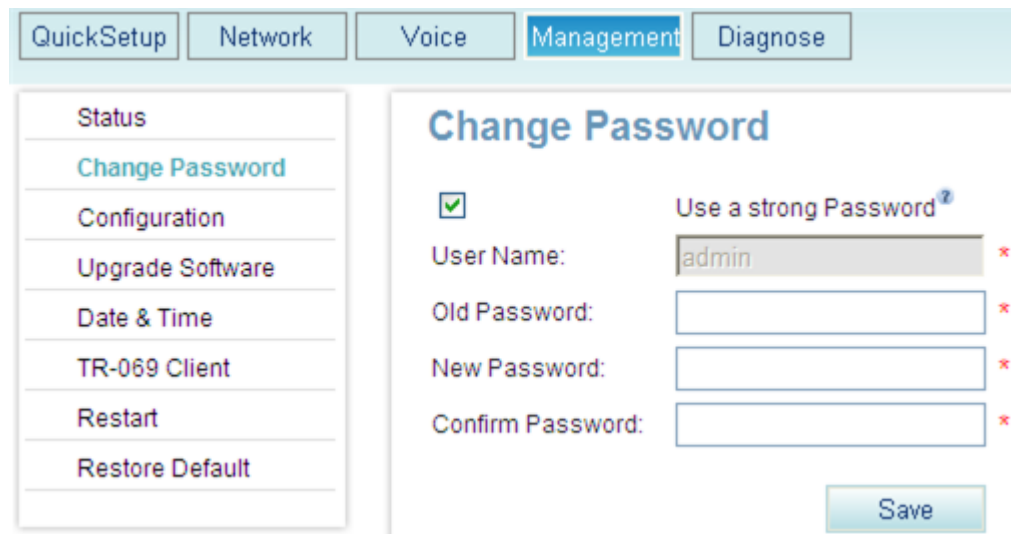
If you forget the password, you can only restore the password to the default factory setting. As a result, the configuration data is lost.

Procedure

Step 1 On the web management system, choose **Management > Change Password** from the navigation tree.

The page shown in [Figure 9-21](#) is displayed.

Figure 9-21 Change Password page

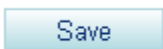


Step 2 Set parameters according to [Table 9-10](#).

Table 9-10 Parameter description

Parameter	Description
Use a strong Password	Indicates whether to set a complicated password. If this parameter is enabled, the password must contain special characters, such as @, # and %.

Parameter	Description
User Name	Indicates the user name. The user name is admin and cannot be changed.
Old Password	Indicates the current password.
New Password	Indicates the new password to be set. The password consists of 6 to 16 characters.
Confirm Password	Indicates that the user enters the new password again.

Step 3 Click  to save the settings.

----End

9.11 Upgrading Host Software

This topic describes how to upgrade host software.

The EGW1520 allows you to upgrade the host software on a web page. The following modes are provided:

- HTTP mode
- FTP mode
- TFTP mode
- FTPS mode

Upgrade procedures vary according to version. For details on the host software storage path and upgrade methods, see the *eSpace EGW1520 Upgrade Guide*.



CAUTION

If the device is powered off or network communication is interrupted during software upgrade, the device may crash or the configuration file may be lost.

9.12 Uploading Voice Files

This topic describes how to upload voice files.

Voice files can be uploaded to the EGW1520 to play announcements for users.

The EGW1520E allows you to upload voice files in .pcm format or compressed voice file packages in .zip format on a web page. The following modes are provided:

- [HTTP Mode](#)
- [FTP Mode](#)

- [TFTP Mode](#)
- [FTPS Mode](#)

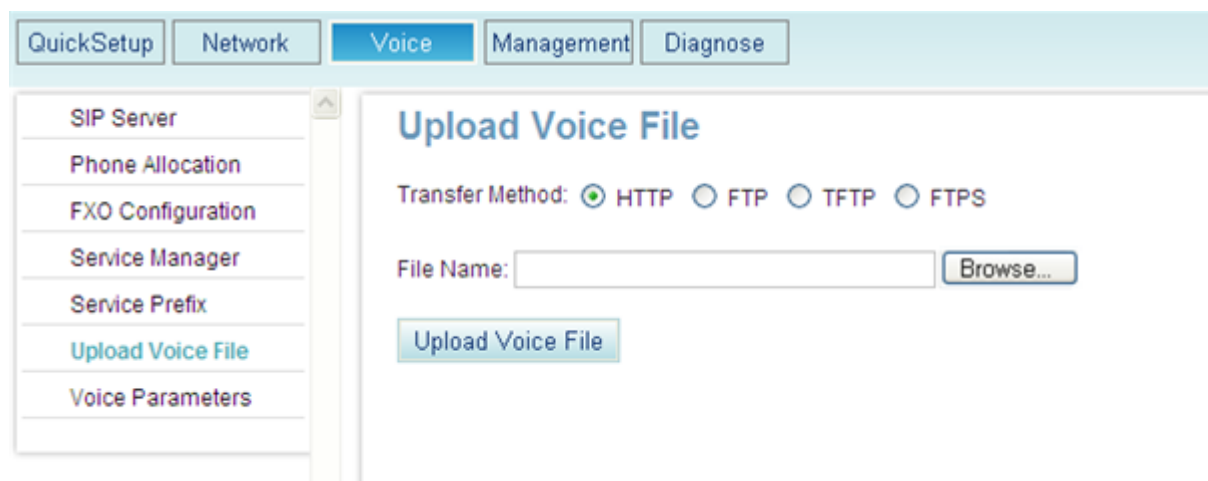
 **NOTE**

- By default, Chinese voice files are loaded on the EGW1520. You can choose **Voice > Upload Voice File** to change the language.
- When uploading a voice file in .pcm format, ensure that the file size is not greater than 1 MB. When uploading a voice file in .zip format, ensure that the file size is not greater than 30 MB.
- In FTP mode, data is transmitted in plain text. Load configuration files in FTP mode on trusted networks.

HTTP Mode

- Step 1** On the web management system, choose **Voice > Upload Voice File** from the navigation tree. The page shown in [Figure 9-22](#) is displayed.

Figure 9-22 Upload Voice File page (HTTP)



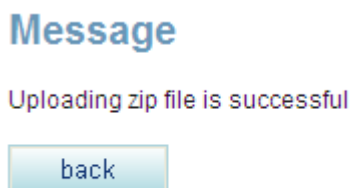
- Step 2** Click **Browse** and select the voice file to be uploaded.

The voice file path can be a local path, for example, **D:\english.zip**, or a network path, for example, **\\10.168.10.111\english.zip**.

- Step 3** Click  and proceed as prompted.

After the loading is successful, the **Message** page is displayed, as shown in [Figure 9-23](#).

Figure 9-23 Success message



 **NOTE**

If the loading fails, the voice file on the EGW1520 remains. You can reload the voice file.

----End

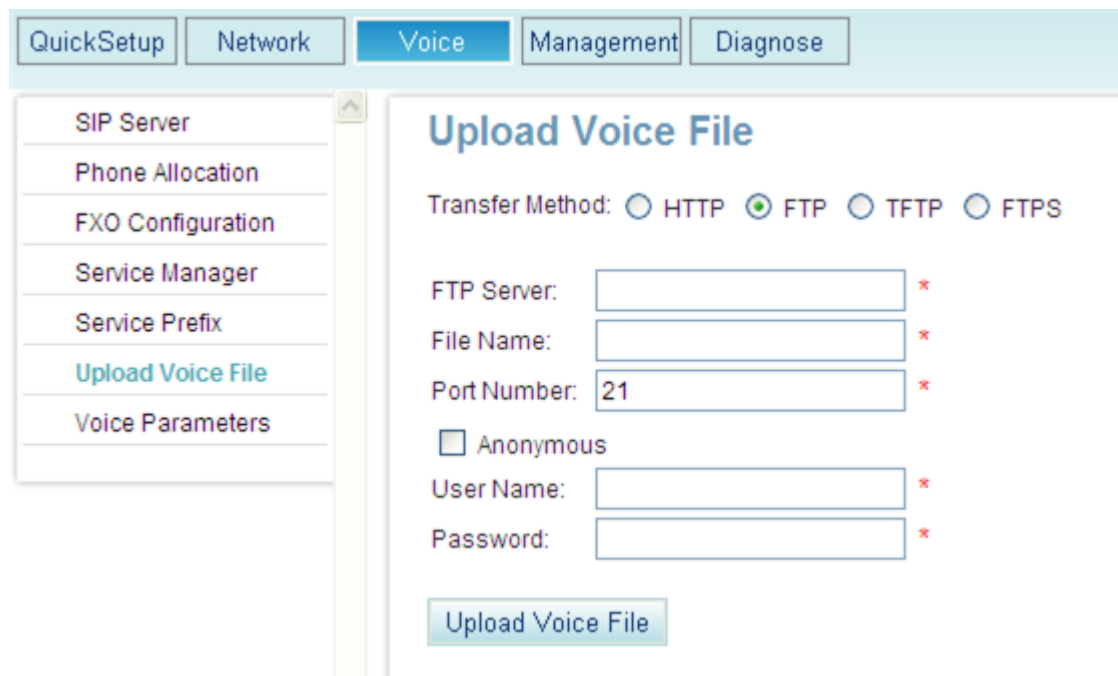
FTP Mode

Step 1 On the web management system, choose **Voice > Upload Voice File** from the navigation tree.

Step 2 Click **FTP**.

The page shown in [Figure 9-24](#) is displayed.

Figure 9-24 Upload Voice File page (FTP)



Step 3 Set parameters according to [Table 9-11](#).

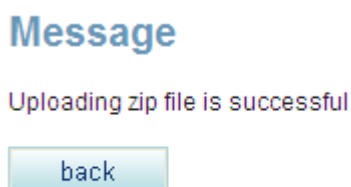
Table 9-11 FTP parameters

Parameter	Description
FTP Server	Indicates the IP address of the FTP server. NOTE Ensure that the FTP service is enabled when configuration files are loaded and that the FTP server connects to the EGW1520 properly.
File Name	Indicates the relative path of the file to be uploaded. If the file to be uploaded is stored in C:/ftp/egw/voice.zip and the access path that is set on the FTP server is C:/ftp , set the relative path to egw/voice.zip .
Port Number	Indicates the port number of the FTP server. The default value is 21 .
Anonymous	If you select Anonymous , the EGW1520 connects to the FTP server as an anonymous user that is the default user on the FTP server.
User Name	Indicates the user name for logging in to the FTP server. This parameter is configured on the FTP server.
Password	Indicates the password for logging in to the FTP server. This parameter is configured on the FTP server.

Step 4 Click  and proceed as prompted.

After the loading is successful, the **Message** page is displayed, as shown in [Figure 9-25](#).

Figure 9-25 Success message



 **NOTE**

If the loading fails, the voice file on the EGW1520 remains. You can reload the voice file.

----End

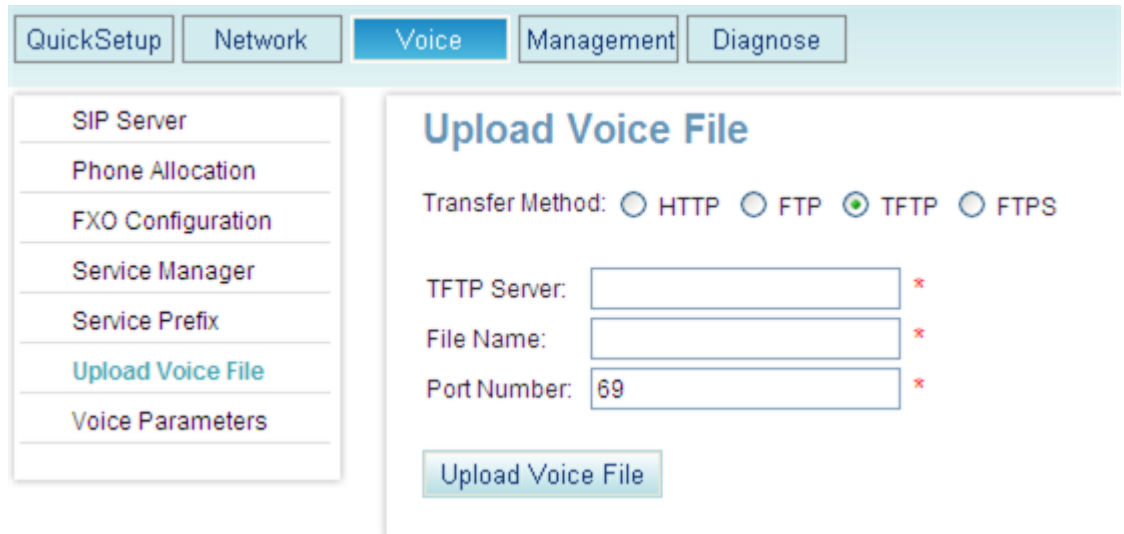
TFTP Mode

Step 1 On the web page's navigation bar, choose **Voice > Upload Voice File**.

Step 2 Click **TFTP**.

The page shown in [Figure 9-26](#) is displayed.

Figure 9-26 Upload Voice File page (TFTP)



Step 3 Set parameters according to [Table 9-12](#).

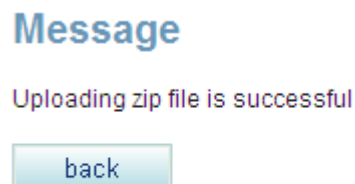
Table 9-12 TFTP parameters

Parameter	Description
TFTP Server	Indicates the IP address of the TFTP server. NOTE Ensure that the TFTP service is enabled when configuration files are loaded and that the TFTP server connects to the EGW1520 properly.
File Name	Indicates the relative path of the file to be uploaded. If the file to be uploaded is stored in C:/tftp/egw/voice.zip and the access path that is set on the FTP server is C:/tftp , set the relative path to egw/voice.zip .
Port Number	Indicates the port number of the TFTP server, which is 69 by default.

Step 4 Click [Upload Voice File](#) and proceed as prompted.

After the loading is successful, the **Message** page is displayed, as shown in [Figure 9-27](#).

Figure 9-27 Success message



 **NOTE**

If the loading fails, the voice file on the EGW1520 remains. You can reload the voice file.

----End

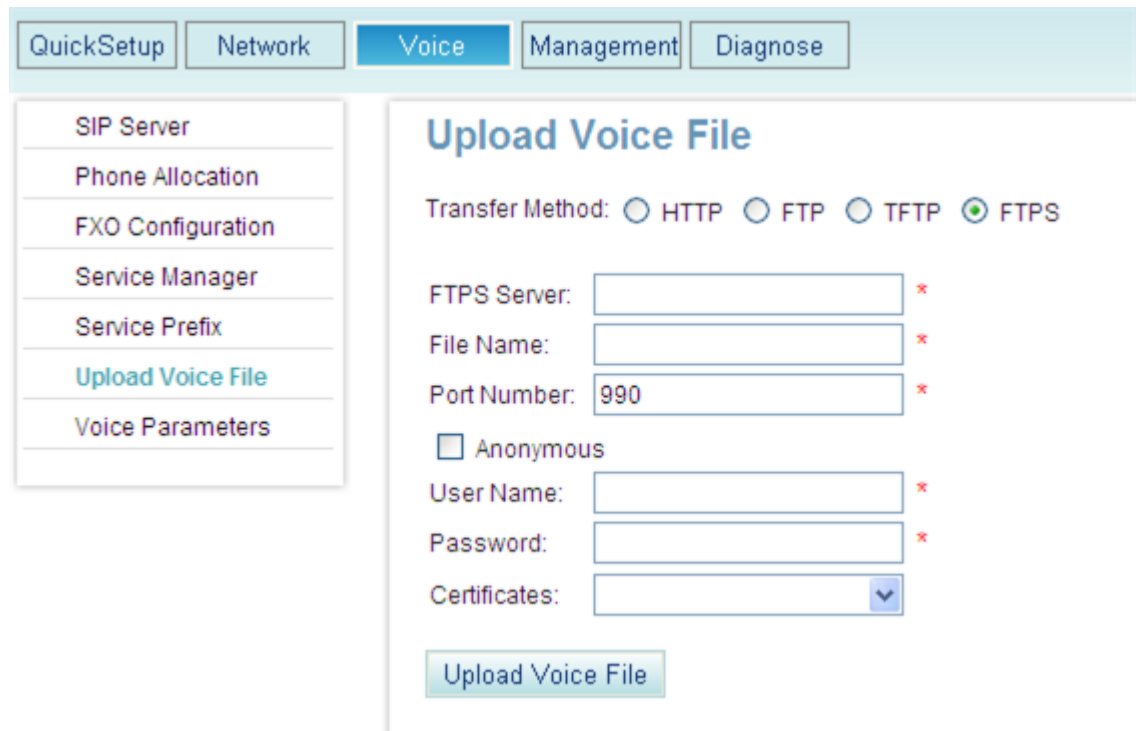
FTPS Mode

Step 1 On the web page's navigation bar, choose **Voice > Upload Voice File**.

Step 2 Click **FTPS**.

The page shown in [Figure 9-28](#) is displayed.

Figure 9-28 Upload Voice File page (FTPS)



Step 3 Set parameters according to [Table 9-13](#).

Table 9-13 FTPS parameters

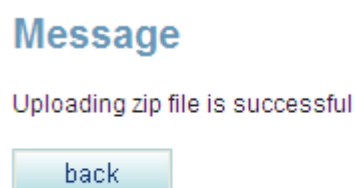
Parameter	Description
FTPS Server	IP address of the FTPS server. NOTE Ensure that the FTPS service is enabled when configuration files are loaded and that the TFTP server connects to the EGW1520 properly.
File Name	Indicates the relative path of the file to be uploaded. If the file to be uploaded is stored in C:/ftps/egw/voice.zip and the access path that is

Parameter	Description
	set on the FTPS server is C:/ftps , set the relative path to egw/voice.zip .
Port Number	Port number of the FTPS server. The default port number is 990.
Anonymous	If Anonymous is selected, the EGW1520 connects to the FTPS server as an anonymous user.
User Name	Indicates the user name for logging in to the FTPS server. This parameter is configured on the FTPS server.
Password	Indicates the password for logging in to the FTPS server. This parameter is configured on the FTPS server.
Certificates	Certificate for authenticate logins. NOTE Before using the certificate to authenticate logins, configure the certificate by referring to 7.5.7 Certificate .

Step 4 Click  and proceed as prompted.

After the loading is successful, the **Message** page is displayed, as shown in [Figure 9-29](#).

Figure 9-29 Success message



 **NOTE**

If the loading fails, the voice file on the EGW1520 remains. You can reload the voice file.

----End

9.13 Restarting the EGW1520

This topic describes how to restart the EGW1520.

You can restart the EGW1520 on the web page or pressing the RESET button on the device.

RESET Button

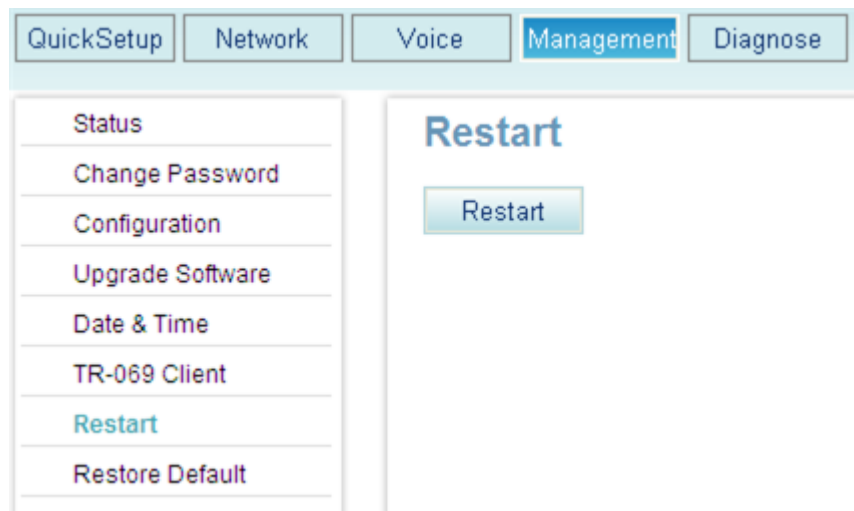
Press **RESET** on the EGW1520 for six seconds or shorter.

Web Mode

Step 1 On the web management system, choose **Management > Restart** from the navigation tree.

The page shown in [Figure 9-30](#) is displayed.

Figure 9-30 Restart page



Step 2 Click  and proceed as prompted.

The restart takes 2 to 3 minutes depending on the device configuration. More configurations indicate a longer restart duration. Access the web management system to check whether the restart is complete. The restart is complete if you can access the page.

----End

10 Security Maintenance

About This Chapter

This topic describes the concept and methods for maintaining the EGW1520.

- [10.1 Overview](#)
- [10.2 Application Layer Security](#)
- [10.3 System Layer Security](#)
- [10.4 Network Layer Security](#)
- [10.5 Management Layer Security](#)
- [10.6 Appendix](#)

10.1 Overview

10.1.1 Objectives

Application systems are facing growing security threats. If a security problem occurs, services will be interrupted, profits will decrease, and the system may break down. To detect potential security problems and resolve them in time, users need to establish an all-round protection system and execute maintenance tasks with a hierarchical approach.

As new security threats emerge continuously, technical methods are insufficient to ensure the security of application systems. Therefore, users also need to develop a security management system based on the suggestions given on problems found in routine security maintenance, which ensures proper running of the applications.

10.1.2 Layered Security Maintenance

Based on the security maintenance objects and objectives, security maintenance on service systems must be conducted at different layers.

Application Layer

The security maintenance at this layer is conducted to ensure that the EGW1520 and related web management system run properly and provide services correctly.

System layer

Security maintenance at this layer is conducted to ensure that the operating system runs properly, ensuring the proper running of applications at the application layer.

At the system layer, security maintenance is conducted using the maintenance terminals or tools corresponding to the maintenance objects.

Network Layer

Security maintenance at this layer is conducted to ensure the proper running of switches, routers, and firewalls and to ensure the application of security policies at this layer.

At the network layer, security maintenance is conducted using the maintenance terminals or tools of the maintenance objects.

Management layer

Security maintenance at this layer is conducted to enhance manual management and maintenance to prevent potential risks. The preceding layers are involved in management-layer security maintenance.

10.1.3 EGW1520 Security Overview

This topic describes the EGW1520 security solution.

Security is essential to communications products and systems. The EGW1520 security solution contains the following layers:

- The security at the management layer ensures the system maintenance, running, security, and continuity.
- The security at the application layer protects all Huawei applications, including access, data, communication, and coding.
- Security at the system layer protects the operating systems, databases, and middleware used by applications.
- The security of the network layer protects the network devices and communication.

With the cooperation of the four layers, the EGW1520 security solution provides security protection for small-sized enterprises.

[Figure 10-1](#) shows the layered architecture of the EGW1520 security solution.

Figure 10-1 Layered architecture of the EGW1520 security solution

Layered Security	Risk	Solution
Management layer security	<ul style="list-style-type: none"> - Relevant personnel lack security consciousness - Untimely version/patch upgrade 	<ul style="list-style-type: none"> - Security documents - Version/patch management
Application layer security	<ul style="list-style-type: none"> - Violent crack - Unauthorized access - Wiretap and data tempering - Unauthorized process - Information leakage 	<ul style="list-style-type: none"> - User management - ID authentication - Transmission security - Session management - Log management
System layer security	<ul style="list-style-type: none"> - Track - Password cracking 	<ul style="list-style-type: none"> - Disabling unsecure ports - System enhancement
Network layer security	<ul style="list-style-type: none"> - Information collection - Sniffing and cheating - Session hijack 	<ul style="list-style-type: none"> - DMZ division - Firewall - VLAN division

10.2 Application Layer Security

10.2.1 Application Layer Account Management

Accounts at the application layer

Table 10-1 listed the accounts at the application layer.

Table 10-1 Accounts at the application layer

User Name	Default Password	Function	Remarks
admin	Admin@123	Account for logging in to the web management system.	The user name and password are both case sensitive. The user name and rights cannot be changed.

Password Principle

- The login password must contain at least six digits.

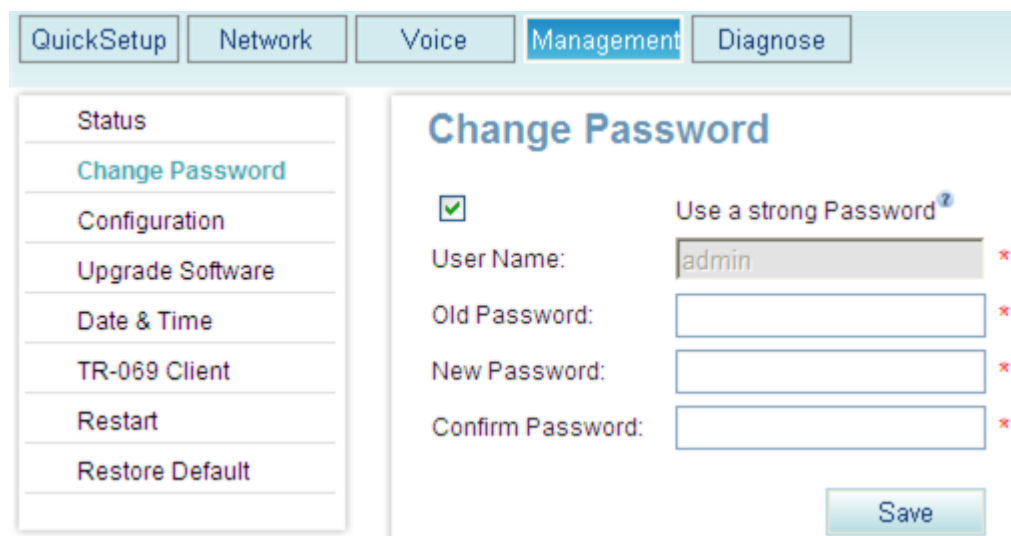
- The login password and service (for example, voice mailbox) password cannot be displayed on GUIs in clear text, and must be encrypted before they are stored.
- Before changing a password, you must enter the original password.

Changing a Password

Step 1 On the web management system, choose **Management > Change Password** from the navigation tree.


The page shown in [Figure 10-2](#) is displayed.

Figure 10-2 Change Password page



Step 2 (Optional) Enable the strong password. If this parameter is enabled, the password must contain special characters, such as @, #, %.

Step 3 Enter the original password, new password, and confirm password as prompted.

Step 4 Click  to save the settings.

----End

10.2.2 Web Access Control

Web access control methods of the EGW1520 are as follows:

- Combination of Session and Cookie
If you do not perform any operation in 10 minutes after logging in to the web management system, the login times out and the system requires re-login to ensure security.
- Logout request initiated by a client
After logging in to the web management system, click **Log Out** at the upper-right corner. The confirm dialog box is displayed. Click **OK**. The login dialog box is displayed.

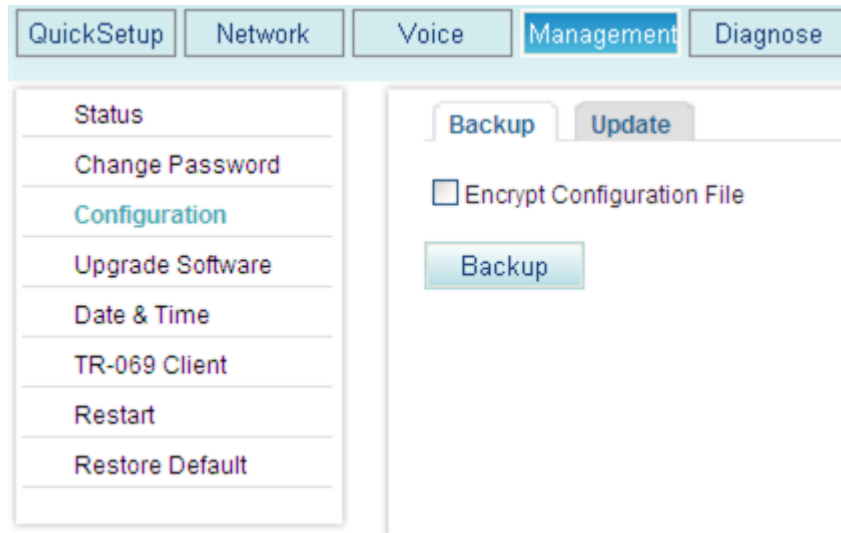
10.2.3 Application Data Protection

Encrypting a Configuration File


Step 1 On the web management system, choose **Management > Configuration** from the navigation tree.

The page shown in [Figure 10-3](#) is displayed.

Figure 10-3 Backing up the configuration file



Step 2 Select **Encrypt Configuration File** to encrypt the whole configuration file.

Step 3 Click  to save the configuration file to the local host or other hosts on the network as prompted.

----End

10.2.4 Application Layer Log Check

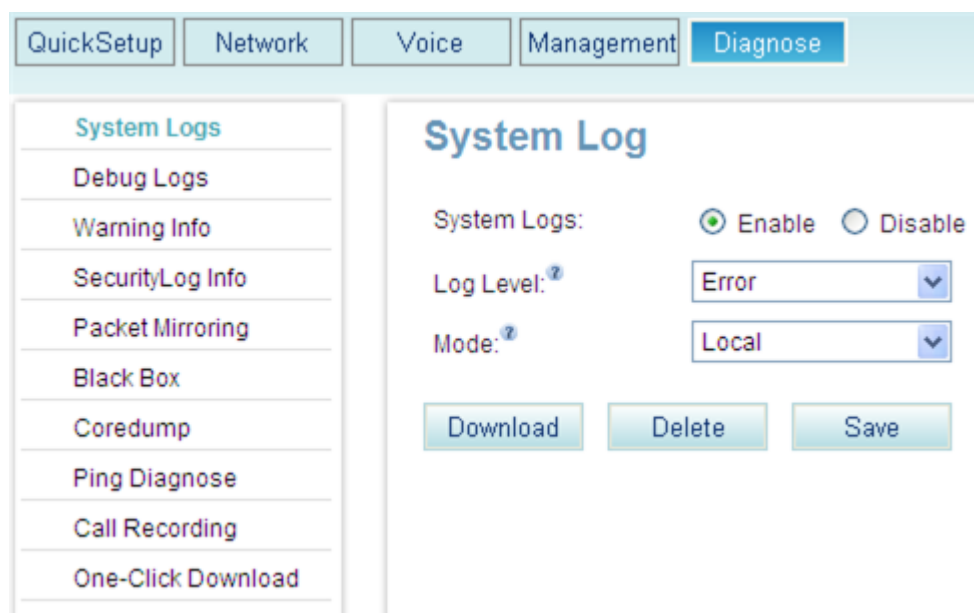
This topic describes how to check application layer logs. To ensure the application layer security, you must check the application layer logs periodically.


Checking the log function

Step 1 On the web management system, choose **Diagnose > System Logs** from the navigation tree.

The page shown in [Figure 10-4](#) is displayed.

Figure 10-4 Enabling the log function



Step 2 Click  to save the settings.

----End

Checking Log Generation

Step 1 Set **Mode** to **Local**.

Step 2 Click  to save the logs to the local host.

Step 3 Verify that log files are displayed on the local desktop.

NOTE

The log file is in .log format. The default file name is in **admin_Log+Current EGW1520 system date.log** format, for example, **Log20100101.log**.

Step 4 Open the local log files to view logs.

----End

Releasing the Log Storage Space

The EGW1520 writes the flash memory when a 512 KB log is generated. When the size of generated logs reaches 2 MB, the earliest logs are overwritten by the latest ones.

The administrator must download and delete logs in the log management module to release the log storage space periodically.

10.3 System Layer Security

Security maintenance at this layer is conducted to ensure that the operating system runs properly, ensuring the proper running of applications at the application layer.

The system layer security maintenance contains:

- System log function that can help checking system security. For details, see [10.2.4 Application Layer Log Check](#).
- Web management system function that supports the EGW1520 connecting to the client through HTTPS.

Logging In to the Web Management System

Step 1 On the maintenance terminal, open Internet Explorer, and enter **https://192.168.1.1** in the address box.



NOTE

- If errors about the security certificate occur during the login process, click **Yes** to go on.
- After logging in to the web management system, you can change IP address of the EGW1520. For details, see [Configuring the LAN](#).

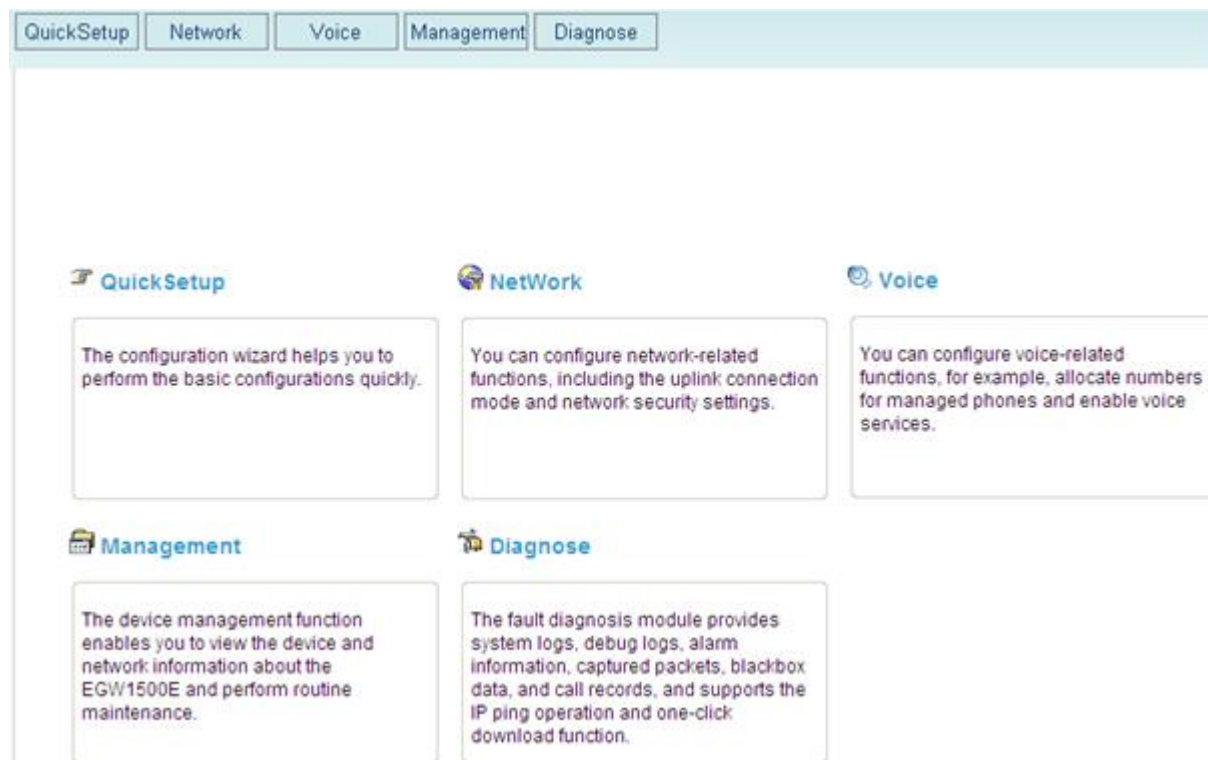
Step 2 Press **Enter**, and the page shown in [Figure 10-5](#) is displayed.

Figure 10-5 Logging in to the web management system (1)



Step 3 Enter the user name **admin** and default password **Admin@123**, and click **Log in**. The page shown in [Figure 10-6](#) is displayed.

Figure 10-6 Logging in to the web management system (2)



 **NOTE**

- Choose **Management > Change Password** to change the password after the initial login.
- Make a note of your password and keep it in a safe place. Do not share your password with anyone. If you forget your password, press and hold the **RESET** button on EGW1520 for more than six seconds, and log in to the web management system using the default password **Admin@123**. The configuration is restored to factory settings.
- If you fail to log in to the web management system for 5 consecutive times within 10 minutes, the system locks your PC IP address for 30 minutes.
- If you do not perform any operation in 10 minutes after logging in to the web management system, the login times out and the system requires re-login to ensure security.

----End

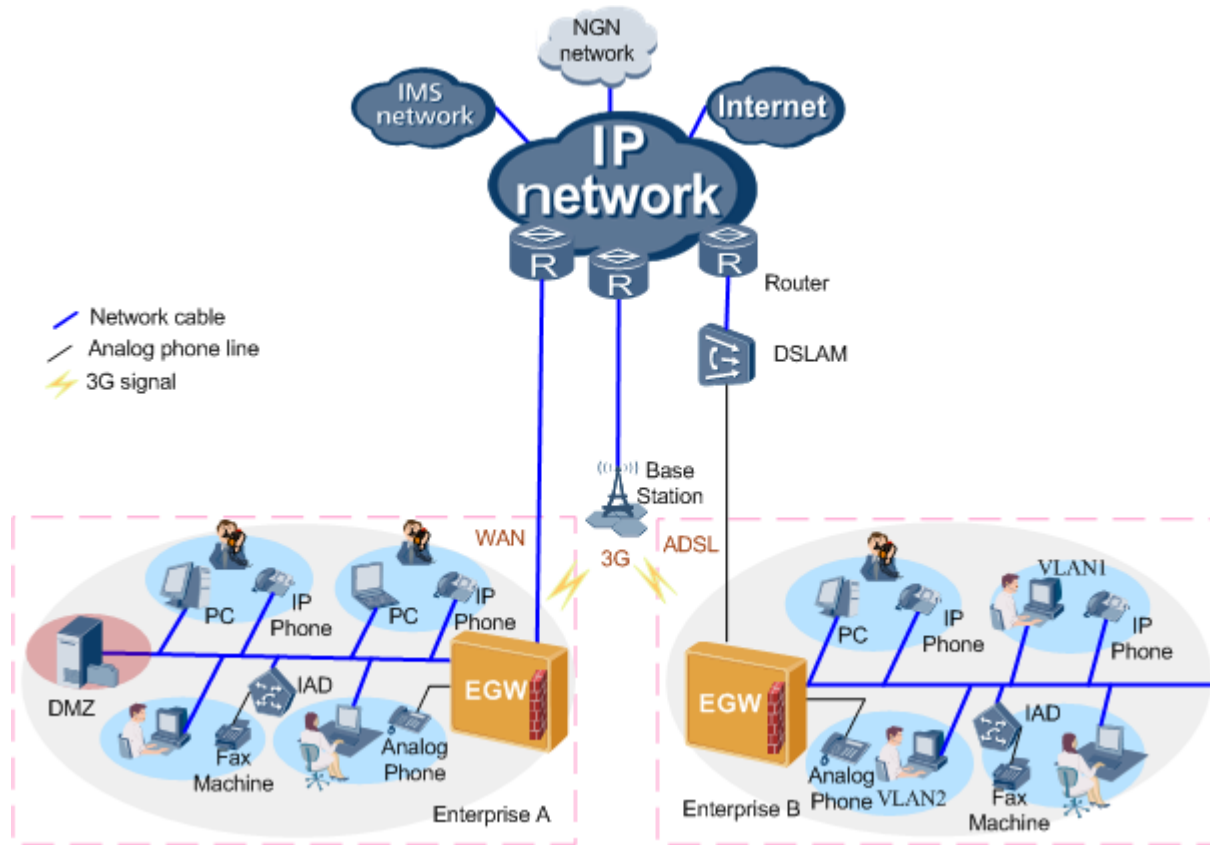
10.4 Network Layer Security

The network layer provides firewall, Demilitarized Zone (DMZ), and VLAN division functions.

10.4.1 Security Network

Figure 10-7 shows the security network of the EGW1520 solution.

Figure 10-7 EGW1520 security network



The EGW1520 security network:

- Is deployed at the entrance and exit of the enterprise network, which provides the firewall function to filter information and prevent unauthorized access.
- Provides the filtering function, which can configure Internet access policy and protect the network security.
- Provides the NAT ALG function based on the SIP protocol to ensure the voice communication security.
- Provides the DMZ function to protect the internal network. External users can access only internal servers in the DMZ.
- Provides the VLAN division function to separate different zones in the network.

10.4.2 Network Security Maintenance

Firewall Security Check on the WAN Side

The EGW1520 provides the firewall function to filter information and prevent unauthorized access.

Enabling the firewall

Step 1 On the web management system, choose **Network > WAN** from the navigation tree.

The page shown in [Figure 10-8](#) is displayed.

Figure 10-8 Enabling the firewall (1)



Step 2 Click  .

The page shown in [Figure 10-9](#) is displayed.

Figure 10-9 Enabling the firewall (2)

Service Configuration

Select Service Type:

- PPPoE
- IPoE

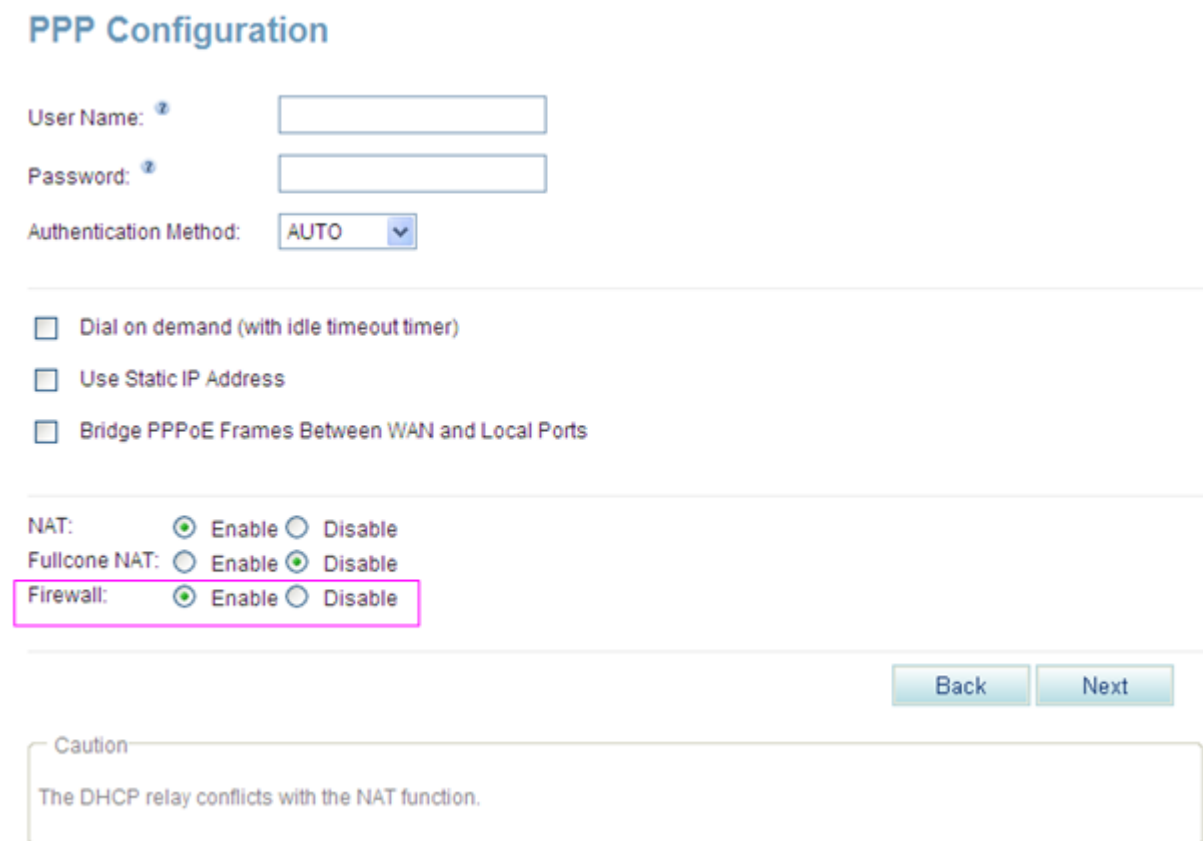
Enter Service Description:

Step 3 Click  .

The page shown in [Figure 10-10](#) is displayed.

Figure 10-10 Enabling the firewall (3)



PPP Configuration

User Name:

Password:

Authentication Method:

Dial on demand (with idle timeout timer)

Use Static IP Address

Bridge PPPoE Frames Between WAN and Local Ports

NAT: Enable Disable

Fullcone NAT: Enable Disable

Firewall: Enable Disable

Caution
The DHCP relay conflicts with the NAT function.

Step 4 Set **Firewall** to **Enable**.

----End

Checking the Firewall Function

If you enable the firewall on the WAN side, packets that are being sent to an EGW1520 or a downstream device will be blocked by the firewall on the WAN side.

NOTE

By configuring the incoming packet filter function, you can specify packets that can be sent through the firewall on the WAN side.

DMZ Security Check

External systems can use virtual servers to access the intranet server. When large amounts of services are running on the intranet server, multiple virtual servers must be configured. You can configure the DMZ to simplify the virtual server configuration process.

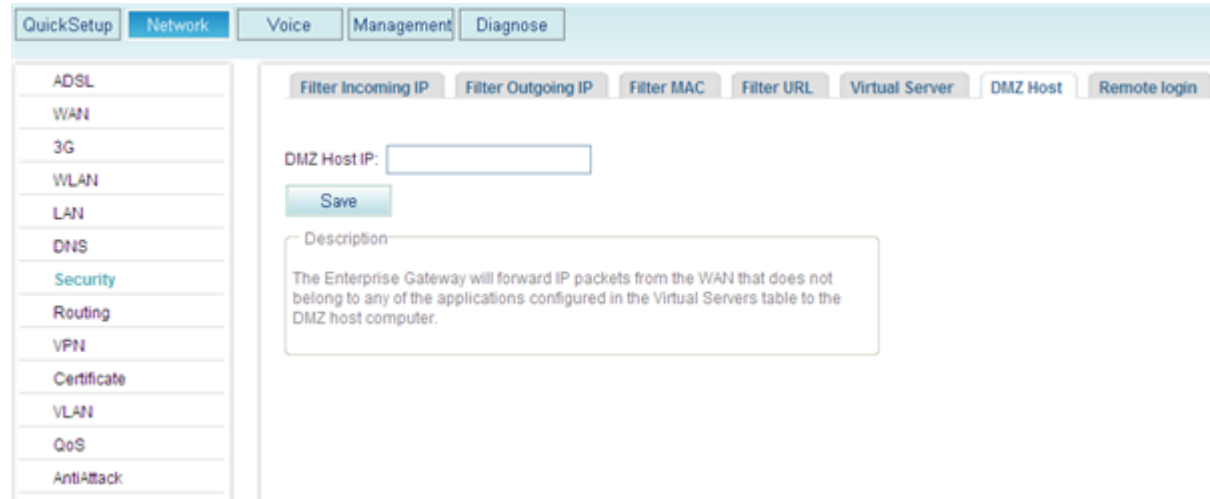
Enabling the DMZ Function

Step 1 On the web management system, choose **Network** > **Security** from the navigation tree.


Step 2 Click the **DMZ Host** tab.

The page shown in [Figure 10-11](#) is displayed.

Figure 10-11 Configuring the DMZ (1)



Step 3 Enter the DMZ Host IP address.

Step 4 Click  to save the settings.

----End

Checking the DMZ Function

Step 1 Connect the EGW1520 to the Internet through the WAN port as an internal user, and set the IP address to **11.11.11.1** for the WAN port.

Step 2 Set the DMZ Host IP address to **192.168.1.5** on the EGW1520.

Step 3 Configure the web and FTP servers on the server whose IP address is **192.168.1.5** as the internal user.

Step 4 Open Internet Explorer and enters **https://11.11.11.1** or **ftp://11.11.11.1** in the address box as an external user.

----End

If the external user can access the web or FTP server, the DMZ is configured successfully.

VLAN Security Check

VLANs are created on a physical LAN to separate the LAN into multiple broadcast domains. Hosts on a VLAN can communicate with each other, and hosts between VLANs cannot communicate with each other. That is, broadcast packets can be sent between hosts on the same VLAN, which improves network security.

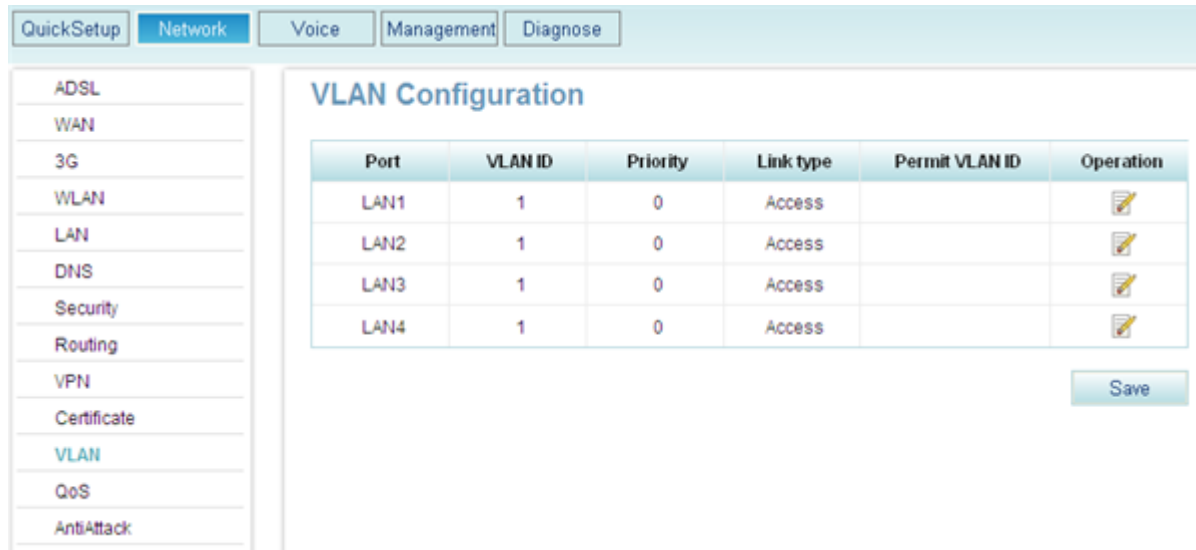
Configuring the VLAN

The EGW1520 supports port-based VLANs. LAN ports are added to different VLANs so that users are separated and virtual working groups are divided.

Step 1 On the web management system, choose **Network > VLAN** from the navigation tree.

The page shown in [Figure 10-12](#) is displayed.

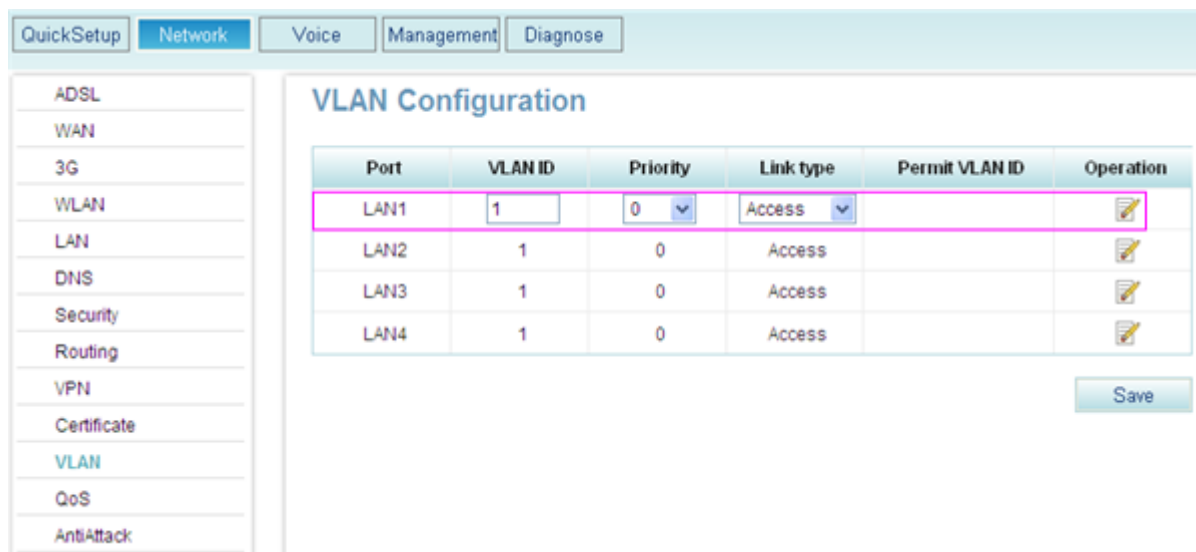
Figure 10-12 Configuring the VLAN (1)



Step 2 Click corresponding to the port to be configured in the **Operation** column.

The page shown in [Figure 10-13](#) is displayed.


Figure 10-13 Configuring the VLAN (2)



Step 3 Set parameters according to [Table 10-2](#).

Table 10-2 VLAN parameters

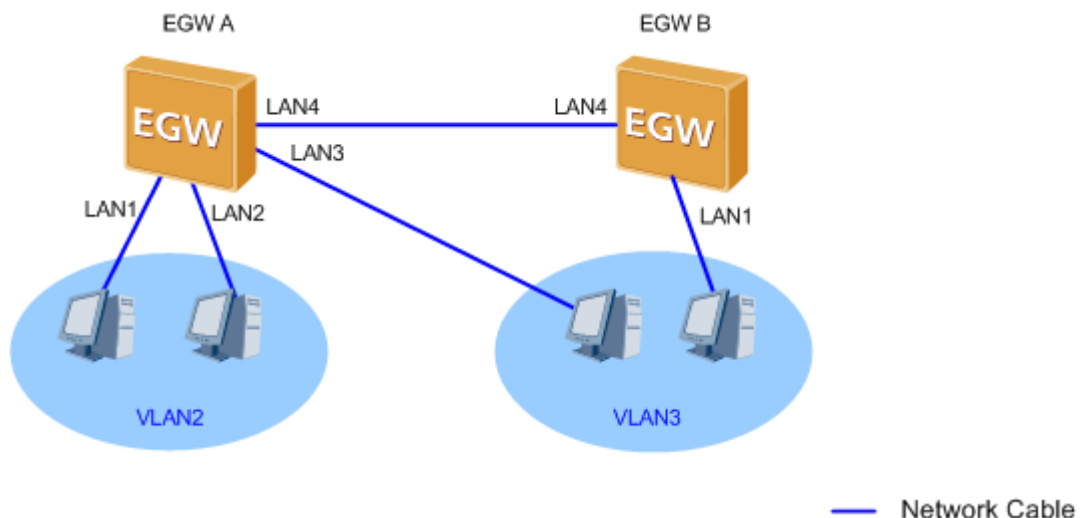
Parameter	Description
Port	Indicates the LAN port on the EGW1520. The EGW1520 provides four LAN ports (LAN1 to LAN4).
VLAN ID	Indicates the VLAN that port belongs to. The default value is 1 .
Priority	Indicates the 802.1p priority based on which devices that connect to the port (such as a switch) process packets. The value ranges from 0 to 3. A larger value indicates a higher priority.
Link type	The options are as follows: <ul style="list-style-type: none"> • Access: Ports of this type can be added to only one VLAN, and are always connected to PCs and switches. • Trunk: Ports of this type can be added to multiple VLAN, and can identify and transmit packets that belong to multiple VLANs based on the VLAN tag.
Permit VLAN ID	Indicates the VLAN ID that is allowed to pass through the port. This parameter is configurable only when Link type is set to Trunk .

Step 4 Click  to save the settings.
----End

Checking the VLAN Function

[Figure 10-14](#) shows the typical network.

Figure 10-14 Typical VLAN network



- Step 1** Change the VLAN IDs to **VLAN 2** for LAN1 and LAN2, and to **VLAN 3** for LAN3 on EGW1520 A. Set the connection type to **Access**
- Step 2** Change the connection type to **Trunk** for LAN4 on EGW1520 A, and set the VLAN changing range to 3.
- Step 3** Change the VLAN IDs to **VLAN 3** for LAN1 on EGW1520 B. Set the connection type to **Access**
- Step 4** Change the connection type to **Trunk** for LAN4 on EGW1520 B, and set the VLAN changing range to 3.
- End

After the configuration, hosts on the same VLAN can communicate with each other. Hosts on different VLANs cannot communicate with each other.

10.5 Management Layer Security

This topic describes general maintenance suggestions for routine security maintenance. Carriers can formulate security management regulations by referring to these suggestions and abide by these regulations to ensure system security.

10.5.1 Security Principles for System Maintenance

Minimum Principle

- Install only required services and components.
- The functions and roles of servers must be distinguished. Do not install unnecessary services and components.
- A service's internal components must be downsized according to the preceding principles.

Minimum Accounts

- Accounts must be managed strictly according to account policies.
- The addition, modification, and deletion of accounts in the system must be strictly controlled.

Minimum Rights

- Assign minimum rights to system services and accounts.
- Control right assignment strictly in the operating system.

Dedication

- A host must run only one type of service.
- Partitions where the operating system, applications, and data are located must be separated.

Audit

- Operations on the host must be logged and monitored in other feasible methods.
- Failures to access the system's important resources must be audited.
- Successes in accessing the system's key resources must be audited.
- Successes and failures to modify the access control policies must be audited.

10.5.2 Password Maintenance

Users need to be authenticated when they attempt to log in to the application system portal. The carrier can configure the account and password complexity, and password validity period based on security requirements.

During password maintenance, ensure that:

- The admin user's password is kept by a designate person.
- Passwords must be encrypted before transfer. Do not transfer passwords using emails.
- Huawei engineers need to request the customer to change passwords before system delivery.

10.5.3 Log Maintenance

The system administrator can detect potential risks according to logs.

Checking Logs Periodically

The maintenance personnel need to periodically check system logs. If any faults are detected, they must report them to the upper-level departments. If the causes cannot be located or the faults cannot be rectified, contact the local representative office or Huawei technical support center.

Backing Up Logs Periodically

The maintenance personnel need to periodically save log files to external storage media such as disks, tapes, and CD-ROMs for backup. After successful backup, the original log files need to be deleted to free up the space.

10.5.4 Security Evaluation

You are advised to find a qualified evaluation organization to evaluate the system security. When implementing security evaluation, contact Huawei technical support engineers.

10.5.5 Vulnerability Scanning

You are advised to use tools to scan vulnerabilities. To use Huawei vulnerability scanning tool, contact Huawei technical support engineers.

10.5.6 Data Backup

Based on security maintenance requirements, back up data in the following scenarios:

- Before and after security configuration, maintenance, and troubleshooting
- Upgrade

For details, see the *eSpace Upgrade Guide*.

10.5.7 Network Connection Change

When the network connection changes, you are advised to:

- Ensure that the new security policy cannot affect the original security policy.
- Analyze the network topology.

10.5.8 Defect Reporting

If the customer system is attacked, Huawei technical support engineers will solve this problem depending on whether any security accidents occur.

- If a security accident occurs, Huawei technical support engineers will provide remote or on-site support to mitigate the attack impact with the assistance of customer maintenance personnel and generate an accident handling report.
- If no security accident occurs, Huawei technical support engineers will record the problem information and forward it to the research and development (R&D) team to process. After the R&D team works out a solution, Huawei technical support engineers will analyze the solution impact on services and develop a feasible solution.

10.5.9 Emergency Response Mechanism

The customer must formulate the emergency response mechanism to deal with emergencies, recover the system, and minimize losses.

10.6 Appendix

The communication matrix must be customized based on the actual network. For details, see [Communication Matrix](#).

11 Troubleshooting

About This Chapter

This topic provides the method to use for troubleshooting when typical faults are found in the EGW1520.

11.1 Precautions

This topic describes the precautions for troubleshooting.

11.2 Troubleshooting Process

This topic describes the EGW1520 troubleshooting process.

11.3 Voice-Specific Faults

Voice-specific faults mainly refer to the faults that occur during user registration, call setup, and service invocation.

11.4 Network Faults

Network faults primarily include network port indicator fault and uplink network disconnection.

11.5 System Faults

System faults mainly include web management system fault and failure to obtain the system time from the NTP server.

11.1 Precautions

This topic describes the precautions for troubleshooting.

Before locating and troubleshooting faults, you must read and observe the following precautions:

- Strictly comply with the operation and industry rules and regulations to ensure safety of personnel and devices.
- Observe anti-static safety measures (for example, wear anti-static wrist straps).
- Record details about all the faults that occur during maintenance.

- Record all the important operations, for example, restarting a process and restoring factory settings. An important operation must be performed by qualified operators after the related data is backed up and proper measures are provided against security and emergency events.

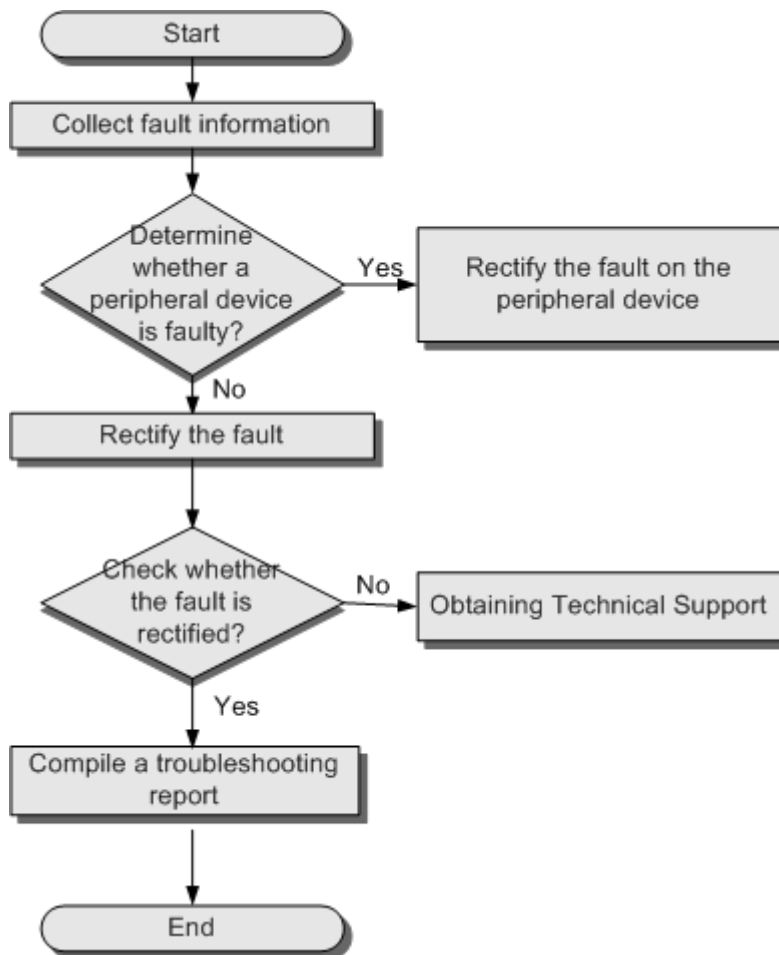
11.2 Troubleshooting Process

This topic describes the EGW1520 troubleshooting process.

The EGW1520 troubleshooting process involves collecting fault information, rectifying faults, verifying fault rectification, compiling troubleshooting reports, and obtaining Huawei technical support.

Figure 11-1 shows the troubleshooting flowchart.

Figure 11-1 Troubleshooting flowchart



11.2.1 Collecting Fault Information

Detailed fault description helps to quickly locate faults. The scenario information, networking information, and system information must be collected when a fault occurs.

Collecting Scenario Information

This topic describes the fault scenario information that must be collected immediately after a fault occurs.

Collect the following scenario information after a fault occurs:

- Fault occurrence time and place
- Fault symptom
- Operations that were performed before the fault occurred
- Measures that have been taken after the fault occurred and the results
- Services that were affected by the fault and the scope of the fault

Collecting Networking Information

Networking information helps maintenance personnel to simulate the fault scenario and locate the fault.

The maintenance personnel must document and save the following onsite information:

- Physical network, including physical connections and connection media.
- Device names and versions.
- Logical connections between devices.
- Device interconnection information, such as the VLAN, IP address, subnet, gateway or port of a device.

Collecting System Information

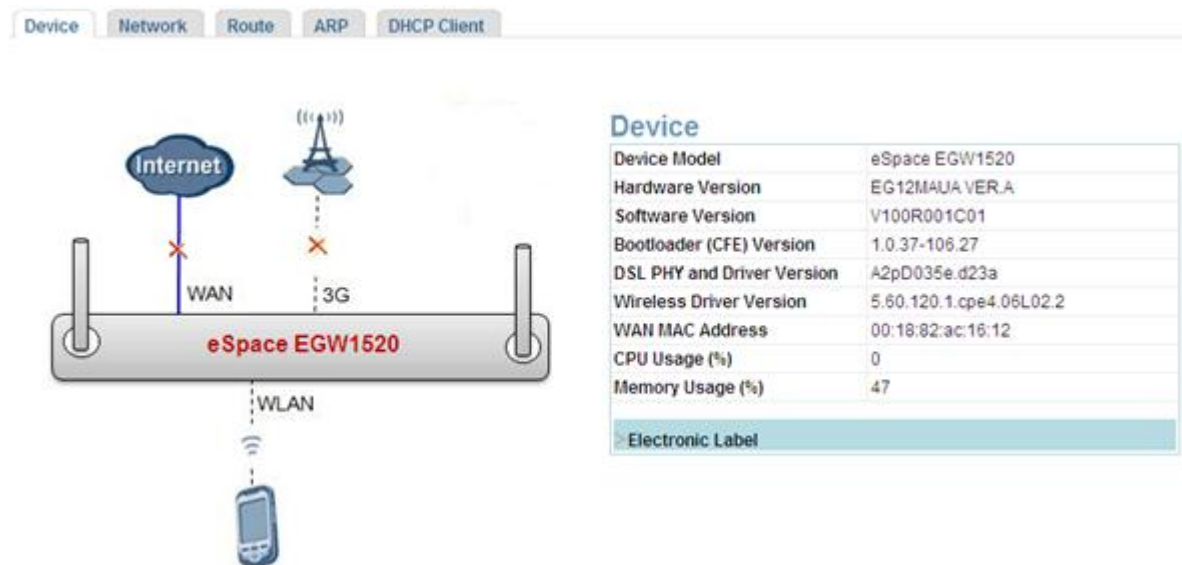
System information includes information about the device, network, route, Address Resolution Protocol (ARP), and Dynamic Host Configuration Protocol (DHCP). By collecting system information, you can learn about the software and hardware versions and detailed network information.

To collect the EGW1520 system information, perform the following operations:

1. Log in to the web management system. For details, see [7.7.1 Web Management](#).
2. Choose **Management** > **Status** from the navigation tree on the left.

The page shown in [Figure 11-2](#) is displayed.

Figure 11-2 Collecting system information



3. Select **Device**, **Network**, **Route**, **ARP**, and **DHCP Client** in turn to view and manually record system information.



NOTE

For the description of the parameters that are displayed when you select **Device**, **Network**, **Route**, **ARP**, or **DHCP Client**, see [Web Parameters Reference](#).

11.2.2 Rectifying Faults

After locating a fault, take proper measures to rectify the fault.

Take measures based on the fault symptom. For the troubleshooting cases, see [11.3 Voice-Specific Faults](#), [11.4 Network Faults](#), and [11.5 System Faults](#).

11.2.3 Verifying Fault Rectification

After taking measures to rectify a fault, verify that the fault is rectified.

If the fault is rectified, compile a troubleshooting report. If the fault is not rectified, [contact Huawei technical support engineers](#).

11.2.4 Compiling a Troubleshooting Report

After verifying that a fault is rectified, record the fault rectification process and compile a troubleshooting report for future reference.

The troubleshooting report should include: fault symptom, fault location, fault rectification, and preventive suggestions.

11.2.5 Obtaining Technical Support

Huawei Technologies Co., Ltd. provides customers with comprehensive technical support and service. Please feel free to contact our local office or company headquarters.

Huawei Technologies Co., Ltd.

Address: Administration Building, Huawei Technologies Co., Ltd., Bantian, Longgang District, Shenzhen, P. R. China

Postal Code: 518129

Website: <http://support.huawei.com>

Customer service telephone: 4008302118

Email: support@huawei.com

11.3 Voice-Specific Faults

Voice-specific faults mainly refer to the faults that occur during user registration, call setup, and service invocation.

11.3.1 Voice Service Users Cannot Register with the IMS/NGN Network

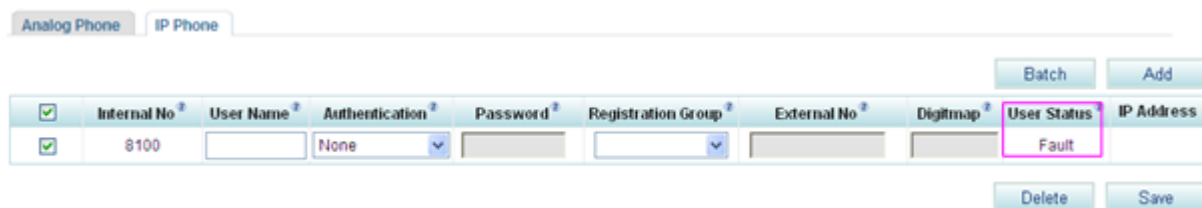
This topic provides the method to use for troubleshooting when voice service users cannot register with the IMS/NGN network.

Symptom

After network and voice data are configured on the EGW1520, EGW1520 voice service users cannot register with the IP Multimedia Subsystem (IMS) network or Next Generation Network (NGN), and the value of **User Status** is **Fault**.

The page shown in [Figure 11-3](#) is displayed.

Figure 11-3 Voice Service Users Cannot Register with the IMS/NGN Network



Possible Causes

- A network exception has occurred.
- The SIP server configuration is incorrect.
- The number configuration is incorrect.
- The Network Address Translation (NAT) function is disabled.

Troubleshooting Procedure

Step 1 Check the network connection.

Check the network connection in either of the following ways:

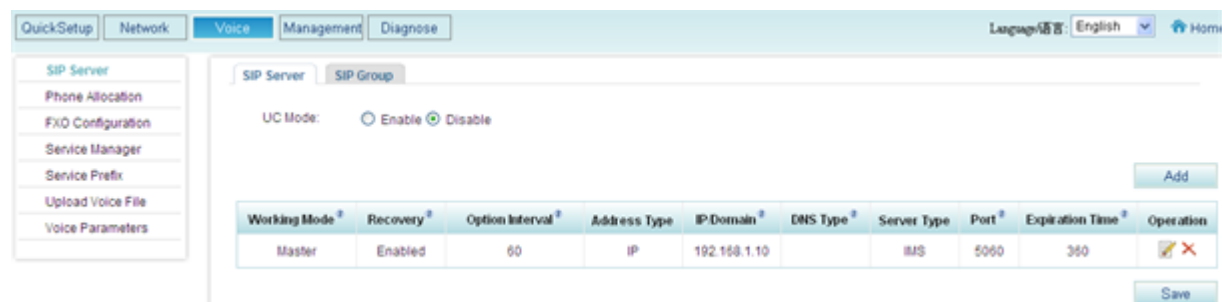
- Check whether the Internet indicator is on. If the indicator is on or blinks, the EGW1520 has been registered with the network service provider and the network connection is normal.
- Choose **Management** > **Status** from the navigation tree on the web management system, click the **Network** tab. If the value of **Status** is **Connected** on the **Network** page, the network connection is normal.

If the network connection is abnormal, see [Installation](#) to verify the cable connections and [7.2 Connection Modes](#) to verify the network configuration.

Step 2 Verify the SIP Server parameter settings.

1. Choose **Voice** > **SIP Server** from the navigation tree on the web management system. The page shown in [Figure 11-4](#) is displayed.

Figure 11-4 SIP Server page



2. Ensure that the parameters listed in [Table 11-1](#) are set correctly.

Table 11-1 SIP Server parameters

Parameter	Description
Working Mode	<ul style="list-style-type: none"> • Master: active SIP server • Slave: standby SIP server
Recovery	Indicates whether to enable the failback function. When the active server fails, resources and services will be automatically switched to the standby server. If this function is enabled, resources and services will be automatically switched back to the original active server after the original active server has been recovered.
Option Interval	Interval for sending option messages to the active server. Option messages are used to check whether the active server can be used. NOTE This parameter is valid only for the master server.
Address Type	The address can be an IP address or a domain name. The network carrier provides this value.

Parameter	Description
IP/Domain	IP address or domain name of the SIP server. The network carrier provides this value.
DNS Type	<p>Mode for the DNS server to parse the IP address. This parameter is valid when Address Type is set to Domain.</p> <ul style="list-style-type: none"> SRV: A domain name is configured to parse multiple IP address. The two IP addresses with the highest priorities are the IP addresses of the active SIP server and standby SIP server. <p>NOTE If you set DNS Type to SRV, you do not need to configure the standby SIP server.</p> <ul style="list-style-type: none"> HOST: One domain name corresponds to one IP address. To perform switchover between the active and standby servers, two SIP servers need to be configured.
Server Type	Select a server type according to the actual SIP network connected to the EGW1520.
Port	Port number of the SIP server. The network carrier provides this value. The default value 5060 is recommended.
Expiration Time	Timeout interval for the registration group to register with the SIP server, in seconds. The value ranges from 0 to 14400. The default value 360 is recommended.

Step 3 Choose **Voice > Phone Allocation** from the navigation tree on the web management system, and check the registration group and external number configuration for Analog Phone users and IP Phone users. The registration group and external number configuration must be consistent with the settings on the IMS/NGN side. If an external number is prefixed with a plus sign (+), change the plus sign to **00**.

Step 4 Check whether the NAT function is enabled.

Choose **Management > Status** from the navigation tree on the web management system, click the **Network** tab. If the value of **NAT** is not **Enabled** on the **Network** tab page, see [Configuring ADSL](#) or [Configuring WAN](#) to delete the Asymmetric Digital Subscriber Line (ADSL) or Wide Area Network (WAN) connection and add another ADSL or WAN connection to enable the NAT function.

Step 5 If the fault persists, see [Obtaining Huawei Technical Support](#).

----End

11.3.2 Failure to Make Outer-Office Calls

This topic provides the method to use for troubleshooting when outer-office calls cannot be made.

Symptom

- Intra-office users cannot make calls to outer-office users.

- When an intra-office user makes a call to an outer-office user, the first call attempt fails and the second succeeds.

Possible Causes

The dial on demand function is enabled on the EGW1520.

Troubleshooting Procedure

Step 1 Check whether the dial on demand function is enabled on the EGW1520.

1. Choose **Management** > **Status** from the navigation tree on the web management system.
2. Click the **Network** tab. Check the value of **Status**.

The page shown in [Figure 11-5](#) is displayed.

Figure 11-5 Value of Status

The screenshot shows the web management interface with the 'Management' tab selected. Under 'Status', the 'Network' sub-tab is active. A table displays the status of the 'atm0' interface, with the 'Status' column highlighted in pink and showing 'Idle'. Below this, another table shows ADSL line rates and LAN IP address.

Interface	Description	Type	NAT	Firewall	Status	IP Address	Subnet Mask	Default Gateway
atm0	ipoe_0_0_35	IPoE	Enabled	Enabled	Idle	0.0.0.0	0.0.0.0	0.0.0.0

ADSL Line Rate-UpStream (kbit/s)	ADSL Line Rate-DownStream (kbit/s)	LAN IP Address	Default Gateway	Primary DNS Server	Secondary DNS Server
0	0	192.168.1.1	-	0.0.0.0	0.0.0.0

- If the value of **Status** is **Idle**, the dial on demand function is enabled on the EGW1520. Then go to [2](#).
- If the value of **Status** is not **Idle**, go to [3](#).

Step 2 Disable the dial on demand function on the EGW1520.

The following describes how to disable the WAN dial on demand function. To disable the ADSL dial on demand function, see [ADSL Configuration](#).

1. Select **Network** > **WAN** from the navigation tree on the web management system. The page shown in [Figure 11-6](#) is displayed.

Figure 11-6 Configuring the WAN connection (1)




2. Click  .
The page shown in [Figure 11-7](#) is displayed.

Figure 11-7 Configuring the WAN connection (2)

Service Configuration

Select Service Type:

- PPPoE
 IPoE

Enter Service Description:


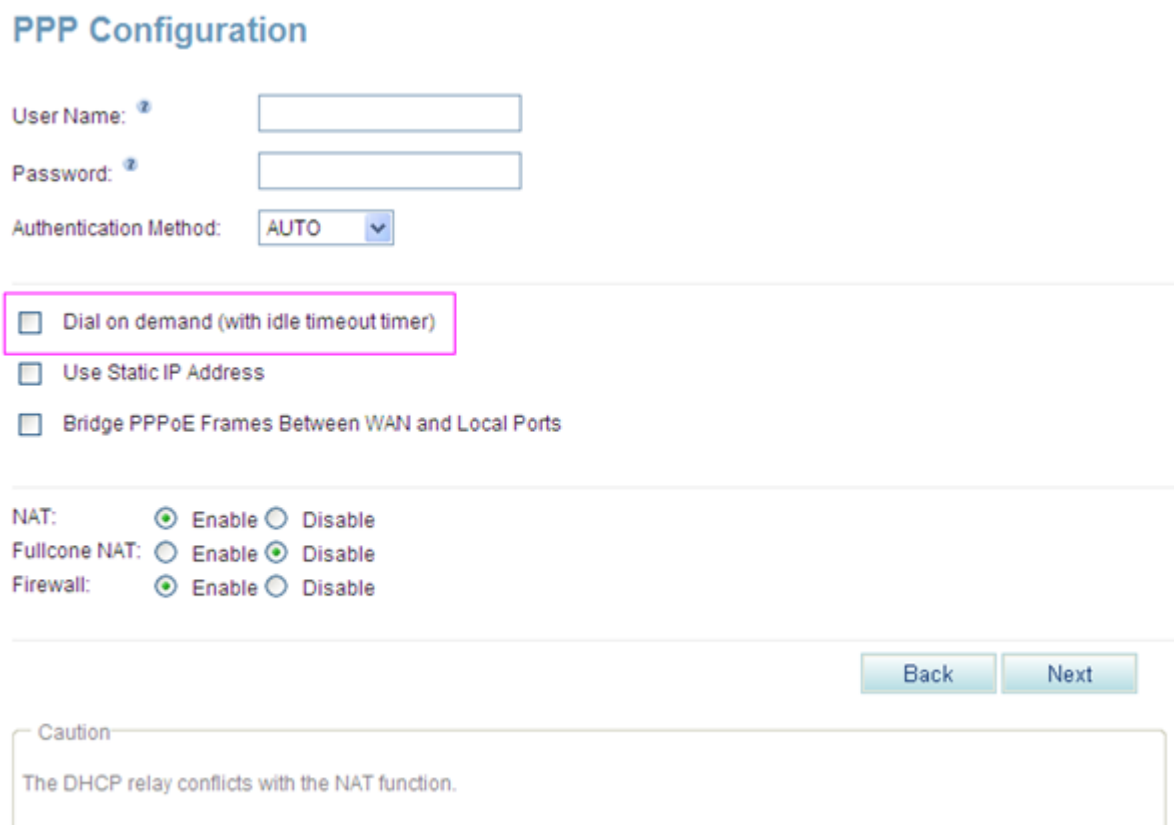
3. Click  .
The page shown in [Figure 11-8](#) is displayed.

Figure 11-8 Disabling the dial on demand function



PPP Configuration

User Name:

Password:

Authentication Method:

Dial on demand (with idle timeout timer)

Use Static IP Address

Bridge PPPoE Frames Between WAN and Local Ports

NAT: Enable Disable

Fullcone NAT: Enable Disable

Firewall: Enable Disable

Caution
The DHCP relay conflicts with the NAT function.

4. Deselect **Dial on demand (with idle timeout timer)** to disable the dial on demand function.

Step 3 If the fault persists, see [Obtaining Huawei Technical Support](#).

----End

11.3.3 Calls Cannot Be Set Up Between an IP Phone and an Analog Phone

This topic provides the method to use for troubleshooting when calls cannot be set up between an IP phone and an analog phone.

Symptom

Calls cannot be set up between an IP phone and an analog phone.

Possible Causes

- Cable connections are incorrect.
- One or both phones are faulty.
- The two phones use different codecs.
- The IP Phone gateway configuration is incorrect.

Troubleshooting Procedure

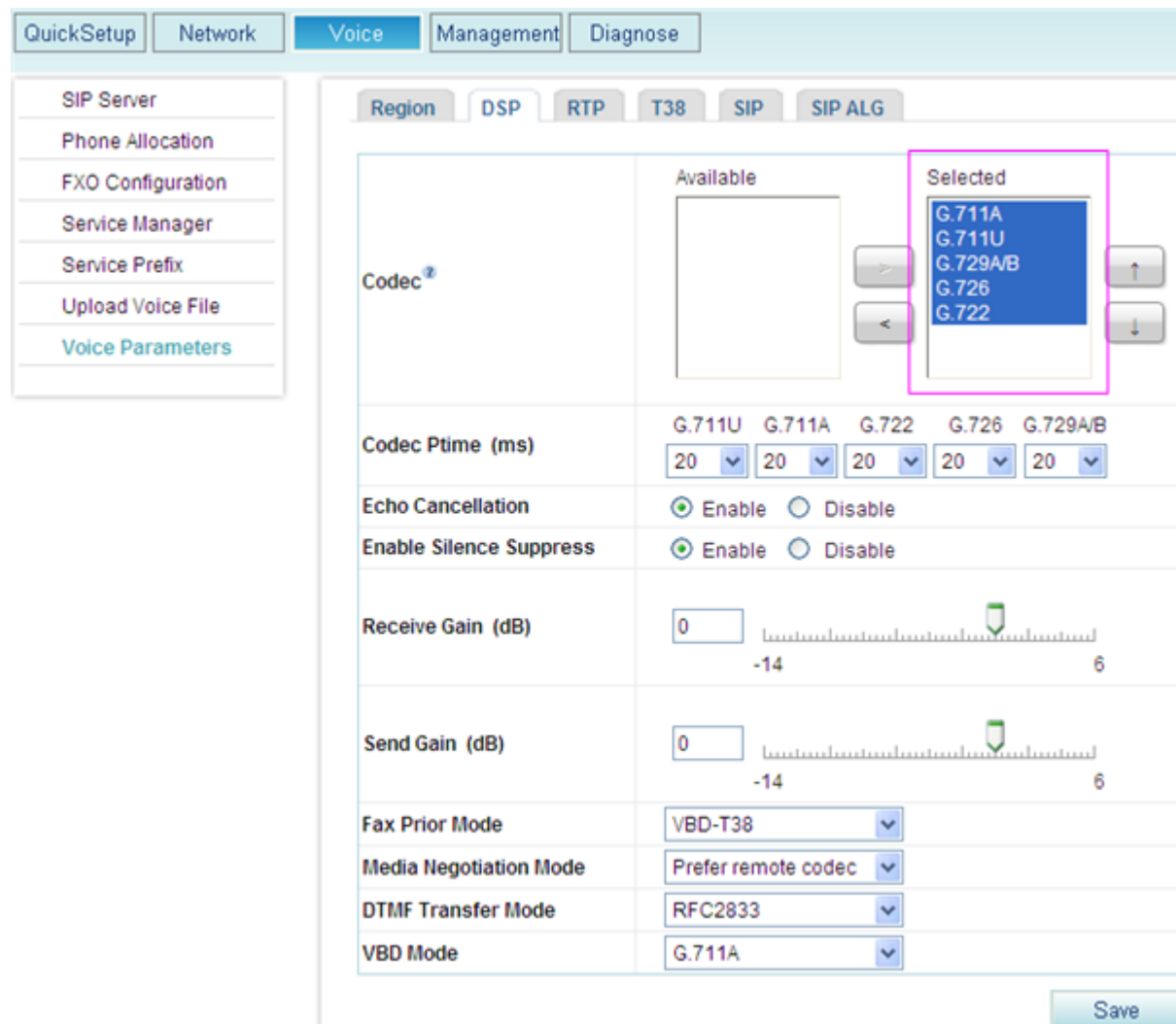
- Step 1** Check cable connections between the IP phone and an analog phone. If the cable is disconnected from either phone, reconnect it. Use a new cable if the original one is damaged.
- Step 2** Check the phones. If they are faulty, replace them.
- Step 3** Check the voice codecs configured on IP phones and EGW1520. Ensure that they share at least one voice codec.

To change the voice codec of the IP phone, see the IP phone user manual. The voice codec of the analog phone is determined by the voice codec of EGW1520. To change the voice codec of the analog phone, proceed as follows:

1. Choose **Voice > Voice Parameters** from the navigation tree on the web management system.
2. Click the **DSP** tab.

The page shown in [Figure 11-9](#) is displayed.

Figure 11-9 DSP tab page



3. Select available codec types and add them to the **Selected** box.

Step 4 Check the IP Phone gateway configuration. For details about how to configure the IP Phone gateway, see the IP Phone user manual.

Step 5 If the fault persists, see [11.2.5 Obtaining Technical Support](#).

----End

11.3.4 CCBS Service Is Unavailable

This topic provides the method to use for troubleshooting when the Call Completion on Busy Subscriber (CCBS) service is unavailable.

Symptom

The CCBS service is unavailable.

Possible Causes

- The CCBS service is disabled.
- The CCBS service is enabled for certain prefixes only.
- The CCBS service is enabled, but the calling party has enabled the calling line identification restriction (CLIR) function.
- The services that allow users to answer multiple calls simultaneously are disabled on the IMS or NGN server. These services include multiple call service and call waiting service.

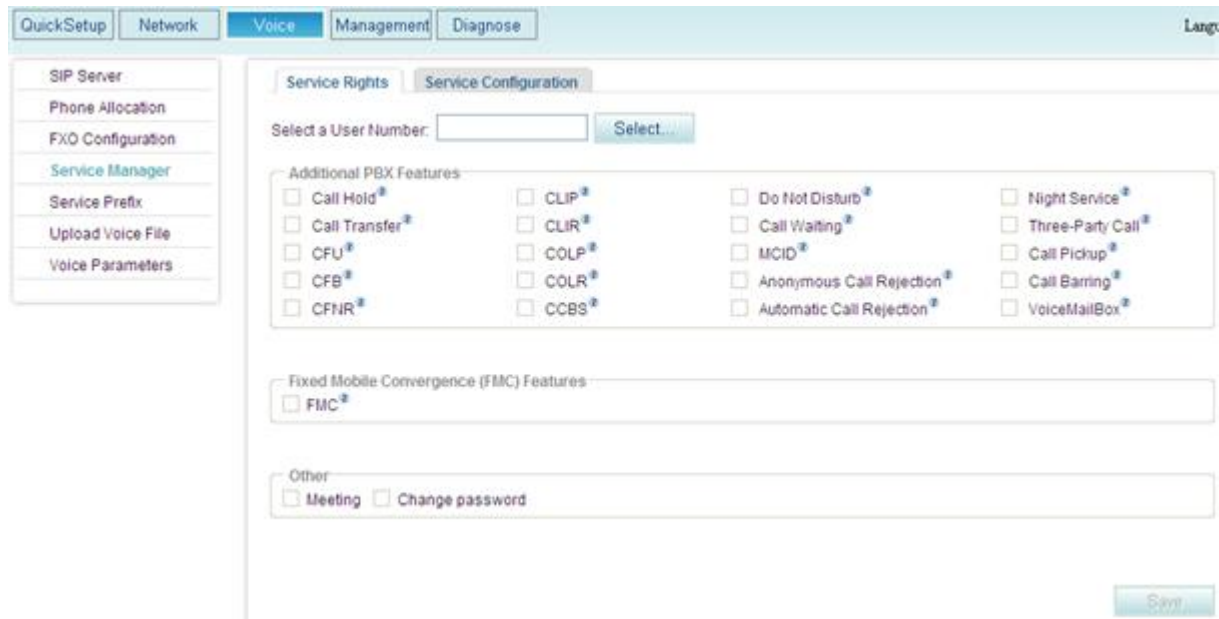
Troubleshooting Procedure

Step 1 Check whether the CCBS service is enabled.

1. Choose **Voice > Service Manager** from the navigation tree on the web management system.

The page shown in [Figure 11-10](#) is displayed.

Figure 11-10 Enabling the service right




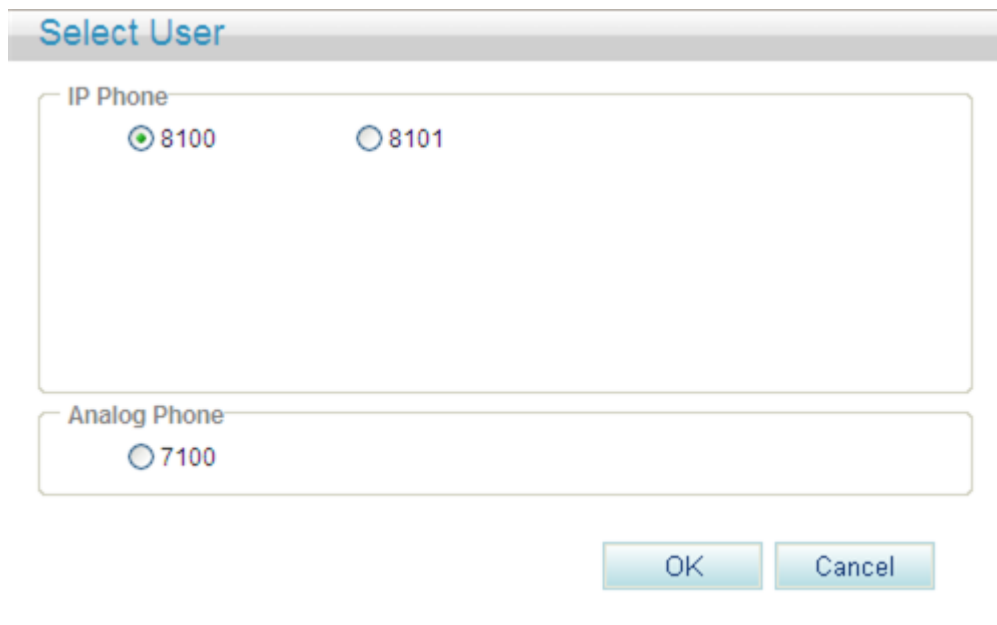

2. Click  .
The page shown in [Figure 11-11](#) is displayed.

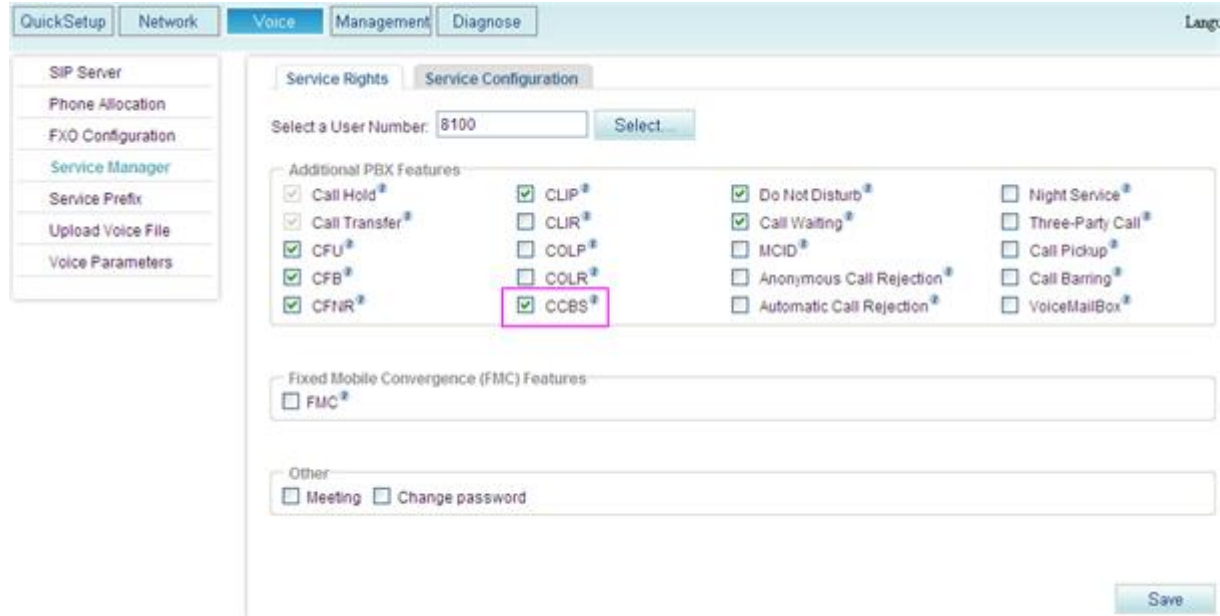
Figure 11-11 Selecting a user



3. Select the user whose voice services need to be enabled.
4. Click  .

5. Select the CCBS service to enable it.
The page shown in [Figure 11-12](#) is displayed.

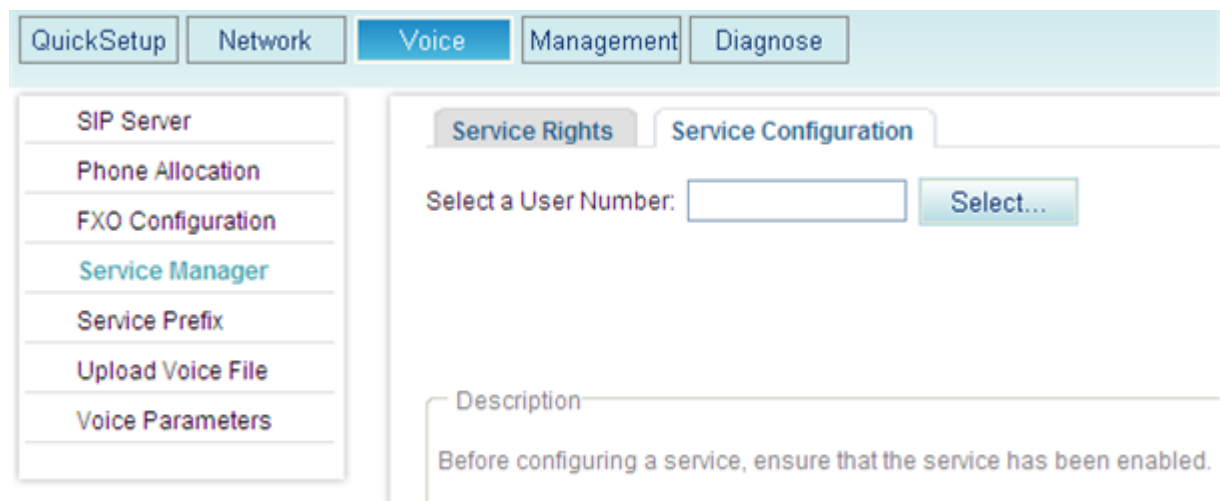
Figure 11-12 Enabling the CCBS service



Step 2 Check whether the CCBS service is enabled for certain prefixes only and the calling number starts with a different prefix.

1. Choose **Voice > Service Manager** from the navigation tree on the web management system.
2. Click the **Service Configure** tab.
The page shown in [Figure 11-13](#) is displayed.

Figure 11-13 Service Configure tab page




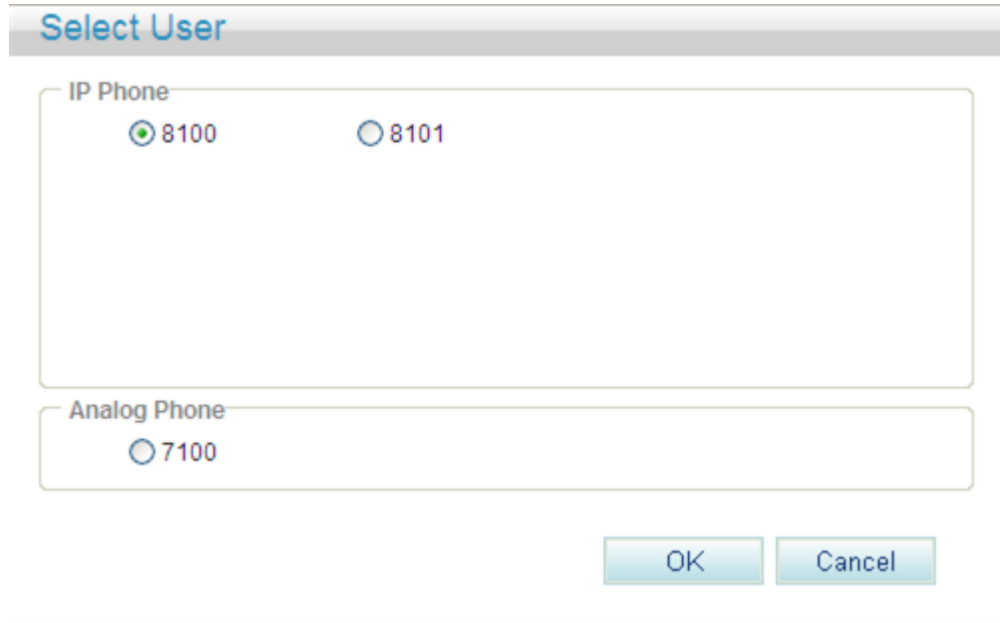
3. Click .
The page shown in [Figure 11-14](#) is displayed.

Figure 11-14 Selecting a user



The dialog box titled "Select User" contains two sections: "IP Phone" and "Analog Phone". The "IP Phone" section has two radio buttons, one selected for "8100" and one unselected for "8101". The "Analog Phone" section has one unselected radio button for "7100". At the bottom right, there are "OK" and "Cancel" buttons.


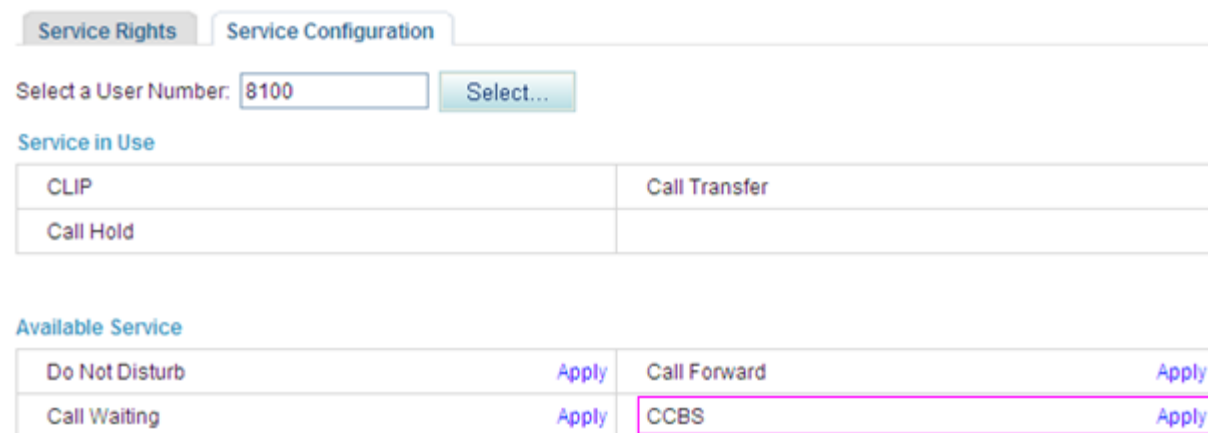
4. Select the user whose services need to be configured.
5. Click .
The page shown in [Figure 11-15](#) is displayed.

Figure 11-15 Configuring the CCBS service (1)



The "Service Configuration" page shows a "Service Rights" tab and a "Service Configuration" tab. Under "Service Configuration", there is a "Select a User Number:" field with "8100" entered and a "Select..." button. Below this are two tables: "Service in Use" and "Available Service".

Service in Use	
CLIP	Call Transfer
Call Hold	

Available Service	
Do Not Disturb	Apply
Call Forward	Apply
Call Waiting	Apply
CCBS	Apply

6. Click **Apply**.
The page shown in [Figure 11-16](#) is displayed.

Figure 11-16 Configuring the CCBS service (2)



If you do not specify the value of **Number**, all users can trigger the CCBS service when making calls. If you specify the value of **Number**, only users who have the preset user number or user number prefix can trigger the CCBS service.

- Step 3** Check whether the calling party has enabled the CLIR service. If the calling party has enabled the CLIR service, the called party cannot call back because the calling number cannot be obtained. If the calling party is an EGW1520 user, see [Calling Line Identity Restriction](#) to disable the CLIR service.
- Step 4** Enable the services that allow users to answer multiple calls simultaneously on the IMS or NGN server. If the calling party is a user on the IMS or NGN side and the call waiting service is disabled, the CCBS service is unavailable.
- Step 5** If the fault persists after you perform the preceding operations, see [Obtaining Huawei Technical Support](#).

----End

11.3.5 Failure to Synchronize Data in the UC Mode

This topic provides the method to use for troubleshooting when the EGW1520 cannot synchronize data in the UC mode.

Symptom

The EGW1520 failed to synchronize data when the UC mode is enabled.

Possible Causes

- Network faults occur.
- The data synchronization server is configured incorrectly.
- EGW1520 synchronization is not configured on the data synchronization server.

Troubleshooting Procedure

Step 1 Check whether the network is normal.

1. Check the network connection.

Choose **Management** > **Status** from the navigation tree on the web management page. Click the **Network** tab. If **Status** is set to **Connected** on the **Network** tab page, the network connection is normal.



NOTE

You can also check the Internet indicator. If the indicator is steady on or blinks, the network connection is normal.

If **Status** is set to other values, the network connection is abnormal. See [Installation](#) to verify cable connection and [7.2 Connection Modes](#) to verify network connection configurations.

2. Check the ADSL or WAN port configuration.

If the EGW1520 uplink mode is ADSL, choose **Network** > **ADSL** from the navigation tree on the web management page, and check the ADSL configuration.

If the EGW1520 uplink mode is WAN, choose **Network** > **WAN** from the navigation tree on the web management page, and check the WAN port configuration.

3. Ping the data synchronization server from the EGW1520. For details, see [8.4 Pinging IP Addresses](#).

If the data synchronization server fails to be pinged, contact the enterprise IT administrator to check whether the data synchronization server is faulty.

Step 2 Verify that the IP address, port, and synchronization key are correctly configured on the data synchronization server.

Choose **Voice** > **SIP Server** from the navigation tree on the web management page, and check the port and synchronization key configuration on the data synchronization server.



NOTE

The synchronization key of the data synchronization server on the EGW1520 side must be the same as that of the data synchronization server on the enterprise headquarters side.

Step 3 Contact the enterprise IT administrator to check whether EGW1520 synchronization is configured on the data synchronization server.

- If yes, ask the enterprise IT administrator to check whether the EGW1520 synchronization is correctly configured.
- If no, ask the enterprise IT administrator to add the EGW1520 synchronization to the data synchronization server.

Step 4 If the fault persists, see [11.2.5 Obtaining Technical Support](#).

----End

11.4 Network Faults

Network faults primarily include network port indicator fault and uplink network disconnection.

11.4.1 Network Port Indicator Fault

This topic provides the method to use for troubleshooting when the network port indicator is off while network cables are connected to the port.

Symptom

The LAN or WAN port indicator is off when network cables are connected to the port.

Possible Causes

- The device is powered off.
- The network cable is improperly connected to the port.
- The network cable is faulty.
- The network negotiation fails.

Troubleshooting Procedure

- Step 1** Ensure that the EGW1520 is powered on.
- Step 2** Ensure that the network cable is properly connected to the port.
- Step 3** Check the network cable. Insert the cable into another port. If the indicator is on, the cable is intact. If the indicator is off, the cable is damaged. In this case, replace the cable.
- Step 4** Ensure that the port connected to the EGW1520 is set to auto-negotiation mode. For details about how to set auto-negotiation mode, see the user manual for the peer device.
- Step 5** If the fault persists, see [Obtaining Huawei Technical Support](#).

----End

11.4.2 Failure to Access the IP Network Through ADSL

This topic provides the method to use for troubleshooting when the EGW1520 fails to access the IP network through the asymmetric digital subscriber line (ADSL).

Symptom

The ADSL is configured, but the EGW1520 fails to access the IP network through the ADSL.

[Figure 11-17](#) and [Figure 11-18](#) show the **Network** pages where the IP address is null and the value of **Status** is **Idle**.

Figure 11-17 Network page (null IP address)

The screenshot shows the Network page in the web management system. The 'Management' tab is selected. The 'Device' sub-tab is active, displaying a table of network interfaces. The 'ppp1' interface is highlighted with a pink box, showing a 'Status' of 'Unconfigured' and an 'IP Address' of '(null)'. Below this, another table shows ADSL line rates and LAN IP address (192.168.1.1).

Interface	Description	Type	NAT	Firewall	Status	IP Address	Subnet Mask	Default Gateway
ppp1	pppoe_0_0_35	PPPoE	Enabled	Enabled	Unconfigured	(null)	(null)	(null)

ADSL Line Rate-UpStream (kbit/s)	ADSL Line Rate-DownStream (kbit/s)	LAN IP Address	Default Gateway	Primary DNS Server	Secondary DNS Server
0	0	192.168.1.1	-	0.0.0.0	0.0.0.0

Figure 11-18 Network page (idle state)

The screenshot shows the Network page in the web management system. The 'Management' tab is selected. The 'Device' sub-tab is active, displaying a table of network interfaces. The 'atm0' interface is highlighted with a pink box, showing a 'Status' of 'idle' and an 'IP Address' of '0.0.0.0'. Below this, another table shows ADSL line rates and LAN IP address (192.168.1.1).

Interface	Description	Type	NAT	Firewall	Status	IP Address	Subnet Mask	Default Gateway
atm0	ipoe_0_0_35	IPoE	Enabled	Enabled	idle	0.0.0.0	0.0.0.0	0.0.0.0

ADSL Line Rate-UpStream (kbit/s)	ADSL Line Rate-DownStream (kbit/s)	LAN IP Address	Default Gateway	Primary DNS Server	Secondary DNS Server
0	0	192.168.1.1	-	0.0.0.0	0.0.0.0

Possible Causes

- The ADSL connection line is damaged.
- The ATM interface configuration is inconsistent with the configuration on the Digital Subscriber Line Access Multiplexer (DSLAM) side.
- A static IP address is configured and the Broadband Remote Access Server (BRAS) does not support static IP addresses.
- The Point-to-Point Protocol (PPP) authentication information is inconsistent with the corresponding information on the BARS side.
- The dial on demand function is enabled but no traffic flows through the uplink ADSL.

Troubleshooting Procedure

Step 1 Check the ADSL connection line.

Check the ADSL indicator on the front panel.

- If the indicator blinks, ADSL line training is being performed. Wait and re-access the IP network a few minutes later.
- If the indicator is off, ADSL line training fails. Ensure that the phone line is intact and inserted properly.
- If the indicator is steady on, the ADSL connection line is intact and inserted properly.

Step 2 Choose **Network** > **ADSL** from the navigation tree on the web management system.

The page shown in [Figure 11-19](#) is displayed.

Figure 11-19 ADSL configuration



Step 3 Ensure that the following configuration on the ADSL ATM interface is consistent with that on the DSLAM side:

- VPI and VCI
- DSL latency
- Encapsulation mode and service category
- DSL Link Type

For the PPPoE service, the value must be set to EoA on the ADSL ATM interface. For the PPPoA service, the value must be set to PPPoA on the DSL ATM interface.

Step 4 Ensure that the following configuration is consistent between the ADSL service side and the BRAS side:

- Static IP address: If a static IP address is configured on the ADSL service side, check whether the BRAS supports static IP addresses. If the BRAS does not support static IP addresses, do not use a static IP address. If the BRAS supports static IP addresses, check whether the static IP address is within the supported static IP address range.
- PPP authentication information, including the PPP user name, password, and authentication mode (the authentication mode can be set to **Auto**).
- Encapsulation mode and service category.

Step 5 If the dial on demand function is enabled, use a computer that is connected to the EGW1520 to access the Internet so that the traffic flows through uplink ADSL to trigger a network connection.

Step 6 If the fault persists, see [Obtaining Huawei Technical Support](#).

----End

11.4.3 Failure to Use 3G Data Card to Access a 3G Network

This topic provides the method to use for troubleshooting when the EGW1520 cannot access a 3G network with a 3G data card.

Symptom

Although a 3G data card is installed and configured, the EGW1520 cannot access a 3G network if the ADSL or WAN connection is unavailable.



NOTE

When **Backup Mode** is set to **Manual**, manual operations are required to enable the EGW1520 to access a 3G network.

Possible Causes

Possible causes are as follows:

- Parameter settings are incorrect.
- The 3G data card is faulty.
- No subscriber identity module (SIM) card is inserted in the 3G data card, or the 3G data card does not support the SIM card that is inserted.
- The SIM card is in arrears.
- The SIM card signals are poor.
- The data service has not been enabled.
- The personal identity number (PIN) lock function is enabled, but the SIM card is locked.

Troubleshooting Procedure

Step 1 Ensure that the model and version of the 3G data card is compatible to the EGW1520. The EGW1520 supports the following 3G data cards: Huawei ET302 with software version of 11.100.05.00.00, Huawei ET127 with software version of 11.101.01.36.00, Huawei K3765 with software version of 11.126.03.06.00, and Huawei E176G with software version of 11.126.03.02.00.

Step 2 Check the 3G data card indicator.

- If the indicator blinks, the 3G data card is connected properly.
- If the indicator is off, the physical connection is faulty between the 3G data card and the EGW1520 USB port. Ensure that the 3G data card is properly inserted and that the card is intact.

Step 3 Ensure that the SIM card is correctly inserted in the 3G data card.

Step 4 Ensure that the SIM card is in WCDMA mode, it has subscribed to the data service and has a sufficient account balance. For details, consult the carrier to whom the card belongs.


Step 5 Ensure that the SIM card is unlocked if the PIN lock function is enabled.

To unlock a SIM card, perform the following operations:

1. Choose **Network > 3G** from the navigation tree on the web management system.
The page shown in [Figure 11-20](#) is displayed.

Figure 11-20 Entering the PIN code



2. Enter the PIN code and click . If you forget the PIN code, contact the carrier.

 **NOTE**

- It takes about 15 seconds to unlock a SIM card.
- The SIM card will be locked by the PIN Unlocking Key (PUK) code if you enter incorrect PIN codes three consecutive times. When this occurs, contact the carrier.
- Disable the PIN lock function if **Backup Mode** is **Auto**, so that the EGW1520 can connect to the 3G network automatically when it is disconnected from the ADSL or WAN port.

- Step 6** Verify the 3G parameter values. To obtain the parameter values, contact the carrier. Use the default values if the carrier does not provide those values.

The page shown in [Figure 11-21](#) is displayed.

Figure 11-21 Verifying 3G parameter settings

3G Configuration

Backup Mode: Manual Auto

WCDMA

Dial String: *

Access Point Name:

TD SCDMA

Dial String: *

Access Point Name:

> SIM Configuration

Description

When the ADSL or WAN port is restored, EGW1500E connects to the ADSL or WAN port automatically.

Step 7 On the **3G Configuration** tab page, view the signal strength. Poor signals may disable the data service. Relocate the EGW1520 to improve the signal strength.

The page shown in [Figure 11-22](#) is displayed.

Figure 11-22 Viewing the signal strength



Step 8 If the fault persists, see [Obtaining Huawei Technical Support](#).

----End

11.4.4 Failure to Connect to the Wireless Network Client That Discovers an SSID

This topic provides the method to use for troubleshooting when the EGW1520 fails to connect to the wireless network client that discovers an SSID.

Symptom

A client discovers an SSID but fails to associate with the EGW1520 after you enter authentication information.

Possible Causes

- The authentication information is incorrect.
- The client and server use different authentication modes.
- The MAC address of the client is filtered out by the blacklist or whitelist configured on the server.

Troubleshooting Procedure

Step 1 Verify that you have entered the same authentication information (such as the WPS key) as that you have configured on the server.

Step 2 Ensure that the client and server use the same authentication mode.

Step 3 Check the settings of **MAC Filter** on the EGW1520. In the blacklist, add the MAC addresses of clients that are not allowed to connect to the EGW1520. In the whitelist, add the MAC addresses of clients that are allowed to connect to the EGW1520.

Step 4 If the fault persists, see [11.2.5 Obtaining Technical Support](#).

----End

11.4.5 Failure to Restrict the File Transfer Rate When Configuring QoS Policies

This topic provides the method to use for troubleshooting when users fail to restrict the file transfer rate when configuring QoS policies.

Symptom

Users fail to restrict the file transfer rate when configuring QoS policies.

Possible Causes

- The action interface is not enabled.
- An incorrect traffic classification or action interface is selected.
- Required parameters are not set or are incorrectly set.

Troubleshooting Procedure

Step 1 Check whether the indicator blinks on the action interface such as the WAN interface. If the indicator blinks, the action interface is enabled. Ensure that network parameters are set correctly. For example, WAN or ADSL connections are correctly added on the web management page.

Step 2 Verify that the traffic classification and action interfaces are valid.



NOTE

The selected interface must be a physical interface such as eth-wan, eth-lan, w10, or atm, not a logical interface such as WAN, LAN, or Local. In addition, traffic classification and action interfaces must be different. If the traffic classification interface is eth-lan, the action interface is eth-wan or atm.

The page shown in [Figure 11-23](#) is displayed.

Figure 11-23 QoS traffic classification and action interfaces

Step 3 Set **Ether Type** to **IP (0x800)** and configure the correct source or destination IP address. If the source or destination IP address is a QoS policy, do not configure the MAC address.

Step 4 If the fault persists, see [11.2.5 Obtaining Technical Support](#).

----End

11.4.6 Some Normal Data Packets Are Lost After the Flood Attack Defense Function Is Enabled

This topic provides the method to use for troubleshooting when some normal data packets are lost after the flood attack defense function is enabled.

Symptom

After the flood attack defense function is enabled, some normal data packets are discarded.

Possible Causes

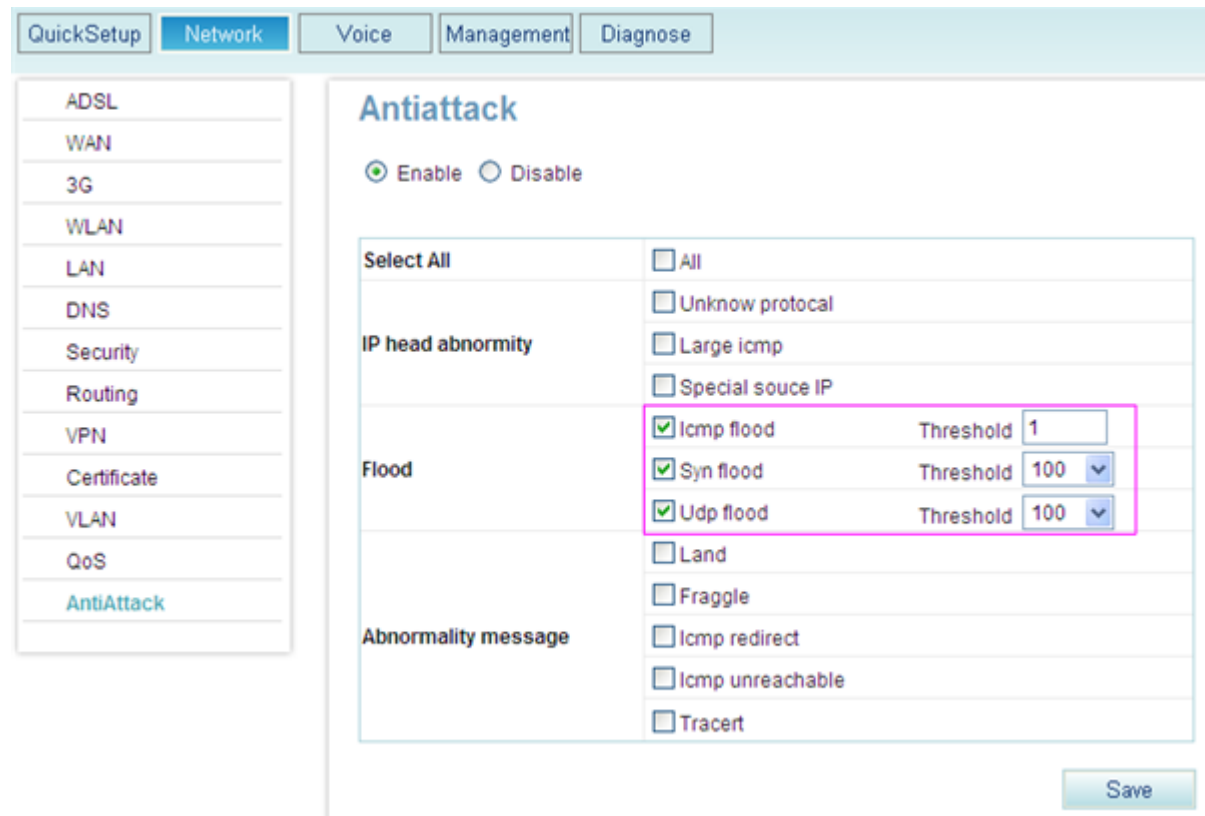
In the configuration of the flood attack defense function, the upper threshold of the data transmission rate is smaller than that is supported so that some normal data packets are discarded.

Troubleshooting Procedure

Step 1 Set the upper threshold of the data transmission rate to a value larger than that is supported. If the supported data transmission rate value is larger than the upper threshold value for a flood attack defense type, for example, 50 for ICMP flood attack defense and 1000 for SYN and UDP flood attack defense, disable flood attack defense for this type of data packets.

The page shown in [Figure 11-24](#) is displayed.

Figure 11-24 Configuring the flood attack defense



Step 2 If the fault persists, see [11.2.5 Obtaining Technical Support](#).

----End

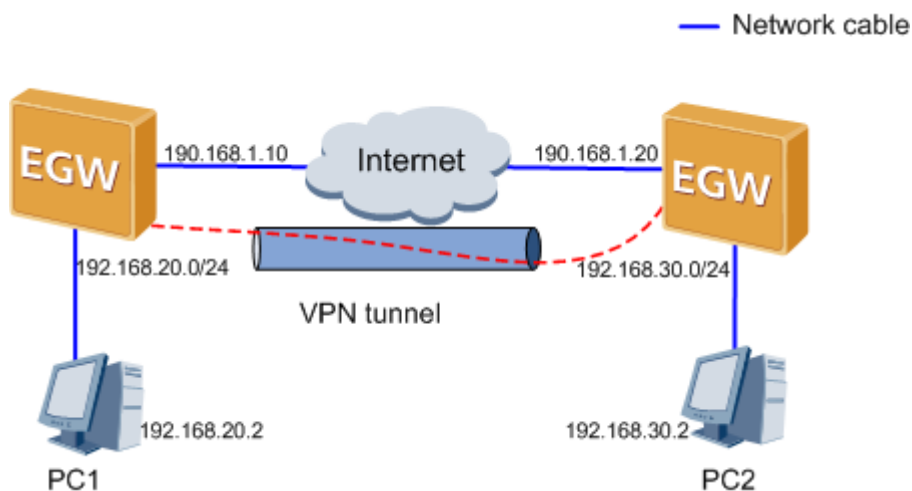
11.4.7 Signals Cannot Be Transmitted Through a VPN Tunnel

This topic provides the method to use for troubleshooting when signals cannot be transmitted through a VPN tunnel.

Symptom

The VPN tunnel is set up successfully while signals cannot be transmitted through it. For example, PC1 and PC2 cannot communicate, as shown in [Figure 11-25](#).

Figure 11-25 Typical network



Possible Causes

No route is configured between PCs.

Troubleshooting Procedure

Step 1 Check for the route between the PCs and add a route when necessary. For example, run the **route add 192.168.20.0 mask 255.255.255.0 192.168.30.1** command to add a route from PC1 to PC2, as shown in [Figure 11-25](#).

Step 2 If the fault persists, see [11.2.5 Obtaining Technical Support](#).

----End

11.4.8 IKE Negotiation Failure in the VPN Tunnel

This topic provides the method to use for troubleshooting when IKE negotiation fails in the VPN tunnel so that VPN servers at both ends of the VPN tunnel cannot set up a connection.

Symptom

The VPN server at one end of the VPN tunnel has the IKE negotiation information at the first stage, while the VPN server at the other end does not.

Possible Causes

The VPN server at one end of the VPN tunnel has saved the IKE negotiation information at the first stage during the previous IKE negotiation.

Troubleshooting Procedure

Step 1 Clear the IKE negotiation information from VPN servers at both ends and verify that both servers negotiate from the first stage.

 **NOTE**

Choose **VPN > IPSec Info** on the EGW1520. The **IPSec Info** page is displayed. Click **Clear SPI** to clear the IKE negotiation information from VPN servers at both ends.

Step 2 If the fault persists, see [11.2.5 Obtaining Technical Support](#).

----End

11.5 System Faults

System faults mainly include web management system fault and failure to obtain the system time from the NTP server.

11.5.1 Failing to Log In to the Web Management System Using HTTPS

This topic provides the method to use for troubleshooting when users cannot log in to the web management system by using the Hypertext Transfer Protocol Secure (HTTPS).

Symptom

When a user logs in to the web management system by HTTPS, Internet Explorer (IE) does not respond for a long time or displays a warning message indicating a certificate error.

Possible Causes

- The network connection between the computer (that is, the maintenance terminal) and the EGW1520 is abnormal.
- The IE on the computer is faulty.

Troubleshooting Procedure

Step 1 Check the network port indicator. The network connection is faulty if the indicator is off. To rectify the fault, see [11.4.1 Network Port Indicator Fault](#).

Step 2 Ensure that the IP addresses (192.168.1.1 by default) of the computer and the EGW1520 are on the same network segment. For example, if the IP address of the EGW1520 is 192.168.1.1, set the IP address of the computer to 192.168.1.x. The value of x ranges from 2 to 254.

Step 3 Check the IE on the computer. The EGW1520 supports only IE 6.0 version or a later version and does not support proxy servers.

 **NOTE**

If you use IE 7.0, login in HTTPS mode takes a long time.

Step 4 Verify that you have accepted the EGW1520 security certificate.

If you use IE 6.0, click **Yes** to continue when logging in in HTTPS mode.

The page shown in [Figure 11-26](#) is displayed.

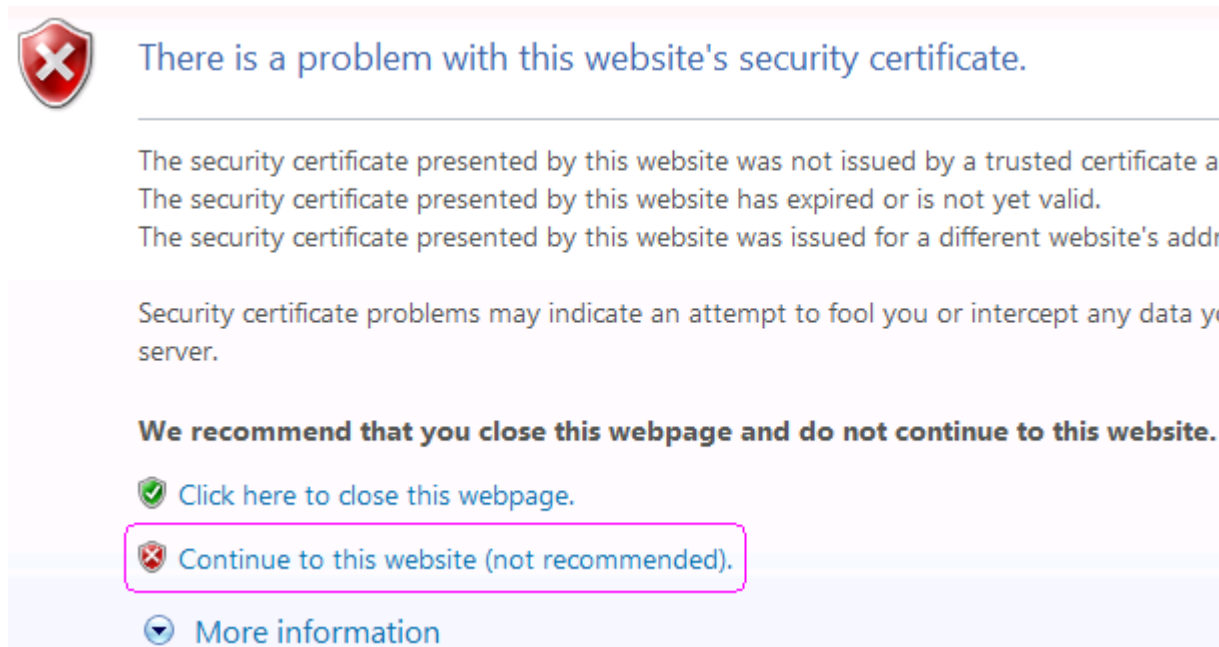
Figure 11-26 Using IE 6.0 to log in



If you use IE 7.0 or a later version, click **Continue to this website (not recommended)**, to continue when logging in in HTTPS mode.

The page shown in [Figure 11-27](#) is displayed.

Figure 11-27 Using IE 7.0 or a later version to log in



Step 5 If the fault persists after you perform the preceding operations, see [Obtaining Huawei Technical Support](#).

----End

11.5.2 Web Login Page Is Displayed Whatever Button or Link Users Click on a Page

This topic provides the method to use for troubleshooting when the system always displays the login page whenever a user clicks a button or link on a page.

Symptom

The system always displays the login page no matter what button or link a user clicks on a page.



NOTE

If you do not perform an operation within ten minutes after logging in to the web management system, the system locks the page and requires re-login to ensure security.

Possible Causes

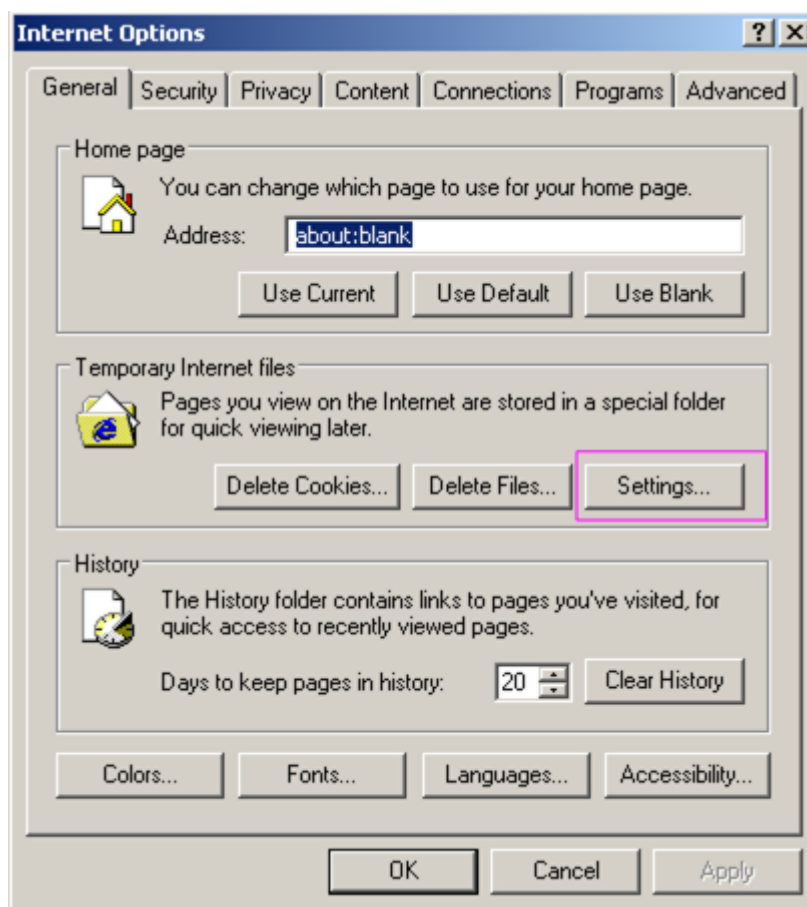
- The Internet Explorer (IE) settings are incorrect on the maintenance terminal.
- The cache of the IE on the maintenance terminal is faulty.

Troubleshooting Procedure

Step 1 Check the IE settings on the maintenance terminal.

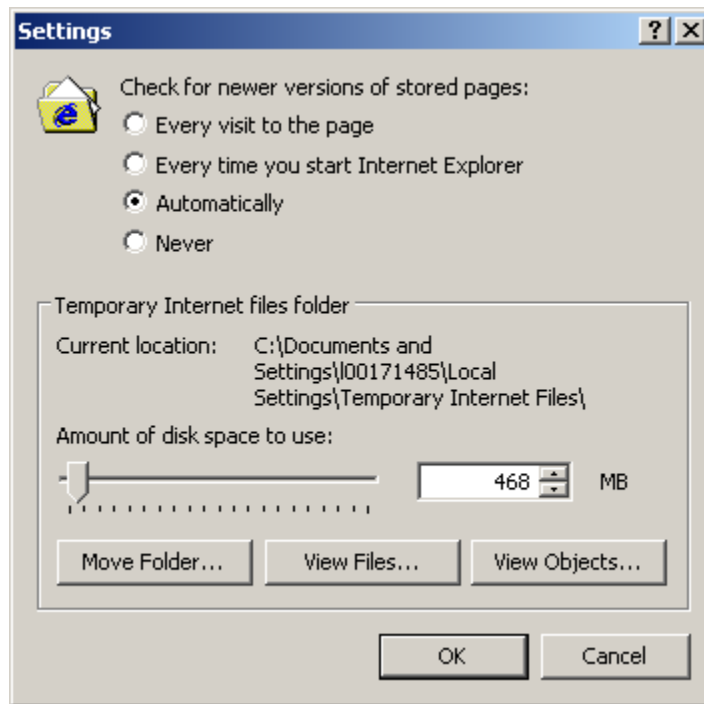
1. Start the IE, and choose **tools > Internet Options**.
The page shown in [Figure 11-28](#) is displayed.

Figure 11-28 Checking the IE settings on the maintenance terminal (1)



2. Click **Settings**.
The page shown in [Figure 11-29](#) is displayed.

Figure 11-29 Checking the IE settings on the maintenance terminal (2)

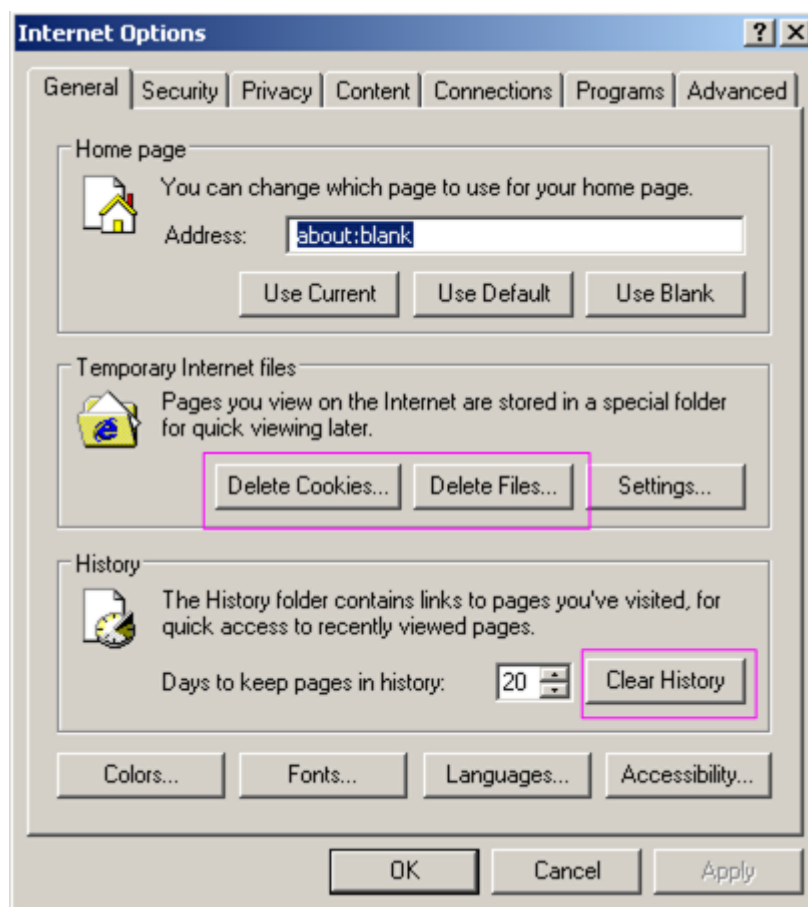


3. Select **Check on every visit to the page** or **Auto** (**Auto** indicates that the EGW1520 web management system determines whether to detect a later version of Web pages).

Step 2 If the fault persists, delete the cache data and history records.

The page shown in [Figure 11-30](#) is displayed.

Figure 11-30 Deleting the cache data and history records



Step 3 If the fault persists, see [Obtaining Huawei Technical Support](#).

----End

11.5.3 An Error Message Is Displayed or No Response Is Received When Users Click a Button or Link on a Page

This topic provides the method to use if an error message is displayed or no response is received when users click a button or link on a Web page.

Symptom

When a user clicks a button or link on a page, the system displays an error message or does not return a response.

Possible Causes

- The network connection between the maintenance terminal and the EGW1520 is abnormal or the network quality is poor.
- The IE settings are incorrect.
- The IE cache contains error files.

Troubleshooting Procedure

Step 1 Check the network port indicator. A network fault occurs if the indicator is off. To rectify the fault, see [11.4.1 Network Port Indicator Fault](#).

Step 2 Click  in IE or press **Ctrl+F5** to forcibly refresh the page.

Step 3 Check the IE settings on the maintenance terminal.

1. Start the IE, and choose **tools > Internet Options**.

The page shown in [Figure 11-31](#) is displayed.

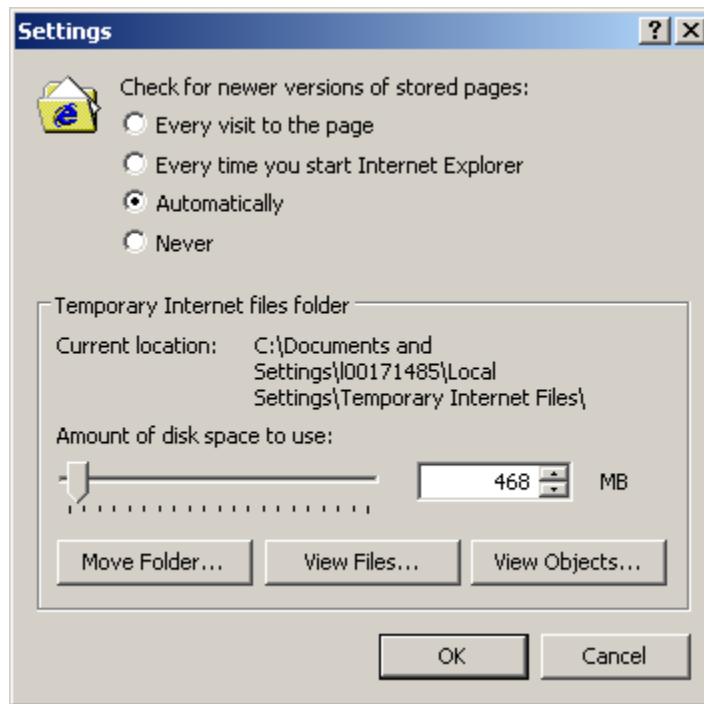
Figure 11-31 Checking the IE settings on the maintenance terminal (1)



2. Click **Settings**.

The page shown in [Figure 11-32](#) is displayed.

Figure 11-32 Checking the IE settings on the maintenance terminal (2)

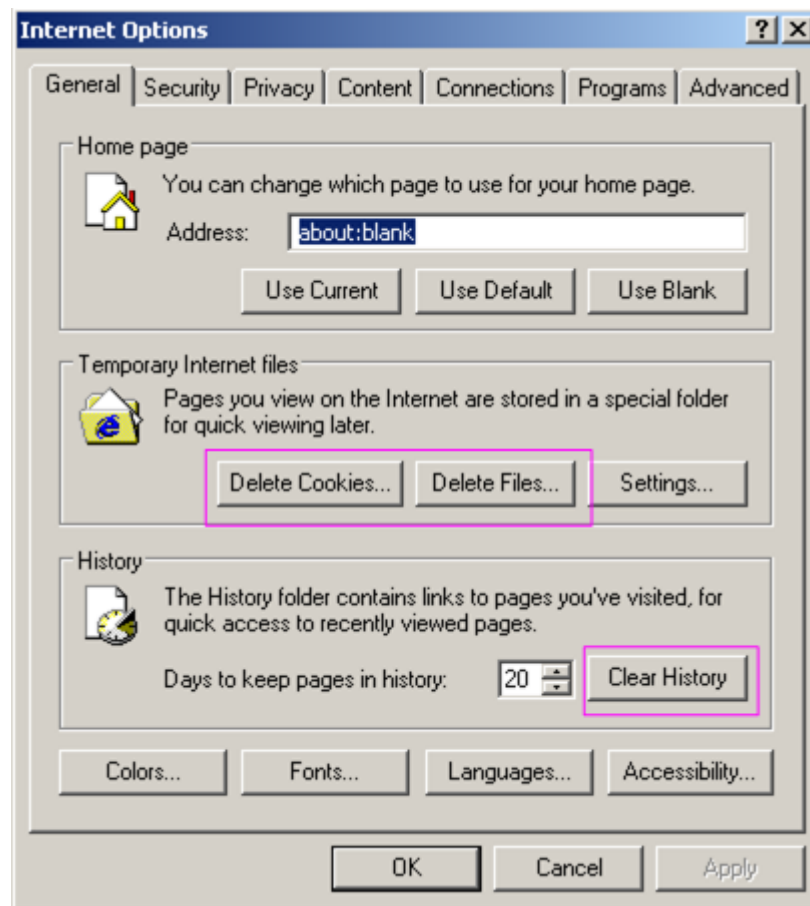


3. Select **Check on every visit to the page** or **Auto** (**Auto** indicates that the EGW1520 web management system determines whether to detect a later version of Web pages).

Step 4 If the fault persists, delete the cache data and history records.

The page shown in [Figure 11-33](#) is displayed.

Figure 11-33 Deleting the cache data and history records



Step 5 If the fault persists, see [Obtaining Huawei Technical Support](#).

----End

11.5.4 Word Display Is Incomplete or the System Does Not Respond After You Click a Button

This topic provides the method to use for troubleshooting when word display is incomplete or the system does not respond after you click a button.

Symptom

Word display is incomplete, the system does not respond after you click a button, or the word "undefined" is displayed after you click a button.

Possible Causes

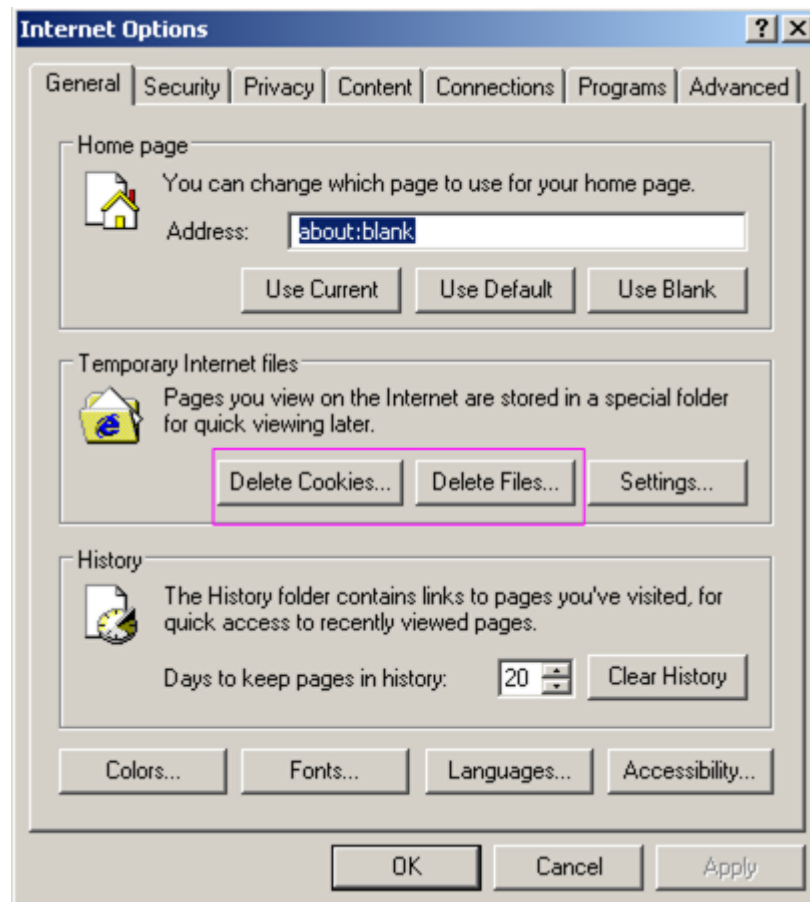
- A browser different from Internet Explorer is used.
- The Internet Explorer version is earlier than 6.0.
- The UI file has been updated after version upgrade, while the browser uses the old UI file in the cache.

Troubleshooting Procedure

- Step 1** Ensure that the Internet Explorer version is 6.0 or later.
- Step 2** Open Internet Explorer and choose **Tools > Internet Options > General**. Clear files and historical records about the URL from the browser cache.

The page shown in [Figure 11-34](#) is displayed.

Figure 11-34 Clearing the Internet Explorer cache and historical data



- Step 3** (Optional) Press **Ctrl+F5** to refresh the UI.
- Step 4** If the fault persists, see [11.2.5 Obtaining Technical Support](#).

----End

11.5.5 The IE Displays an Error Message When Multiple User Data Records Are Configured Simultaneously

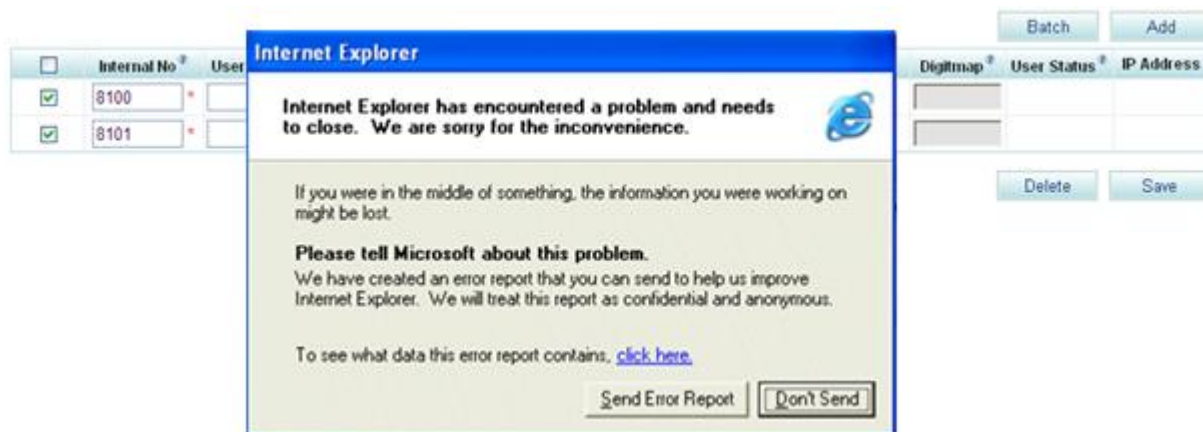
This topic provides the method to use for troubleshooting when the IE displays an error message when multiple user data records are configured simultaneously.

Symptom

The IE displays an error message when multiple user data records are configured simultaneously.

Figure 11-35 shows the error message.

Figure 11-35 Error message displayed by the IE



Possible Causes

- The version of the IE is earlier than 6.0.
- The memory of the PC is insufficient.
- IE files on the PC are damaged.

Troubleshooting Procedure

Step 1 Open IE, and choose **Help > About Internet Explorer** to view the version of the IE.

The page shown in Figure 11-36 is displayed.

Figure 11-36 Viewing the IE version



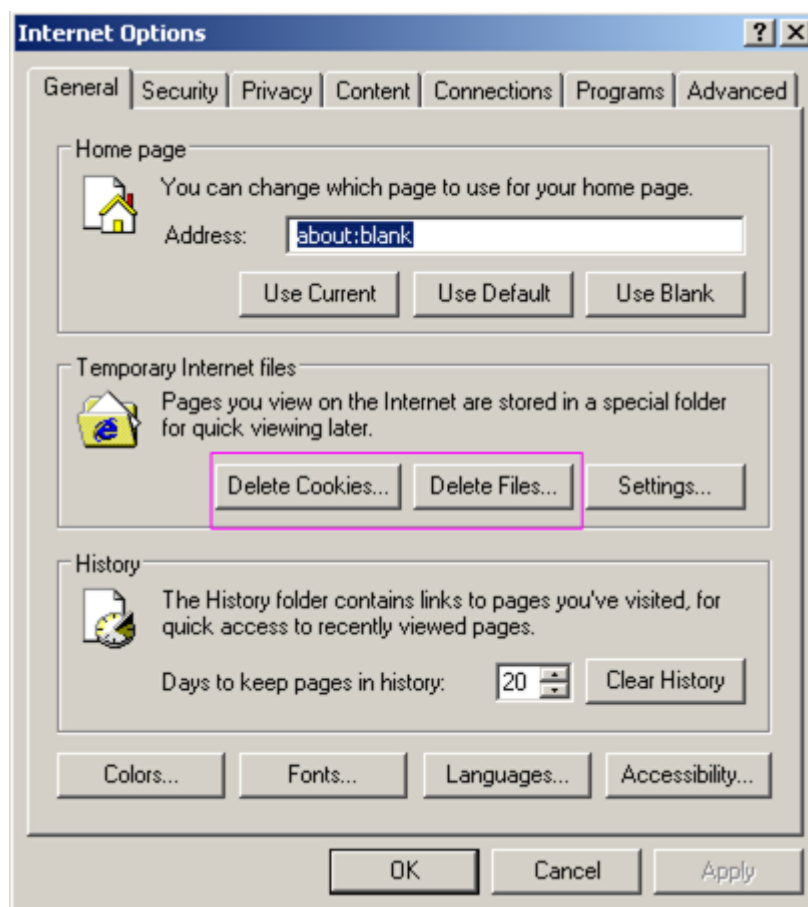
The EGW1520 requires IE 6.0 or a later version. If your IE version is earlier than 6.0, go to www.microsoft.com to upgrade it.

Step 2 Stop other running applications on your PC to free up memory space, and configure data again.

Step 3 If the fault persists, delete temporary Internet files from the cache of your IE.

The page shown in [Figure 11-37](#) is displayed.

Figure 11-37 Deleting temporary Internet files



Step 4 If the fault persists, restart your PC.

Step 5 If the fault still persists, uninstall your IE, and go to www.microsoft.com to download IE 6.0 or a later version and install it.

Step 6 If the fault persists, see [Obtaining Huawei Technical Support](#).

----End

11.5.6 System Time Cannot Be Obtained from the NTP Server or the Obtained Time Is Incorrect

This topic provides the method to use for troubleshooting when system time cannot be obtained from the NTP server or the time obtained is incorrect.

Symptom

System time cannot be obtained from the NTP server or the time obtained is incorrect.

Possible Causes

Possible causes are as follows:

- The uplink network connection is abnormal.
- The NTP server is unreachable.
- The time zone or Daylight Saving Time (DST) configuration is incorrect.

Troubleshooting Procedure

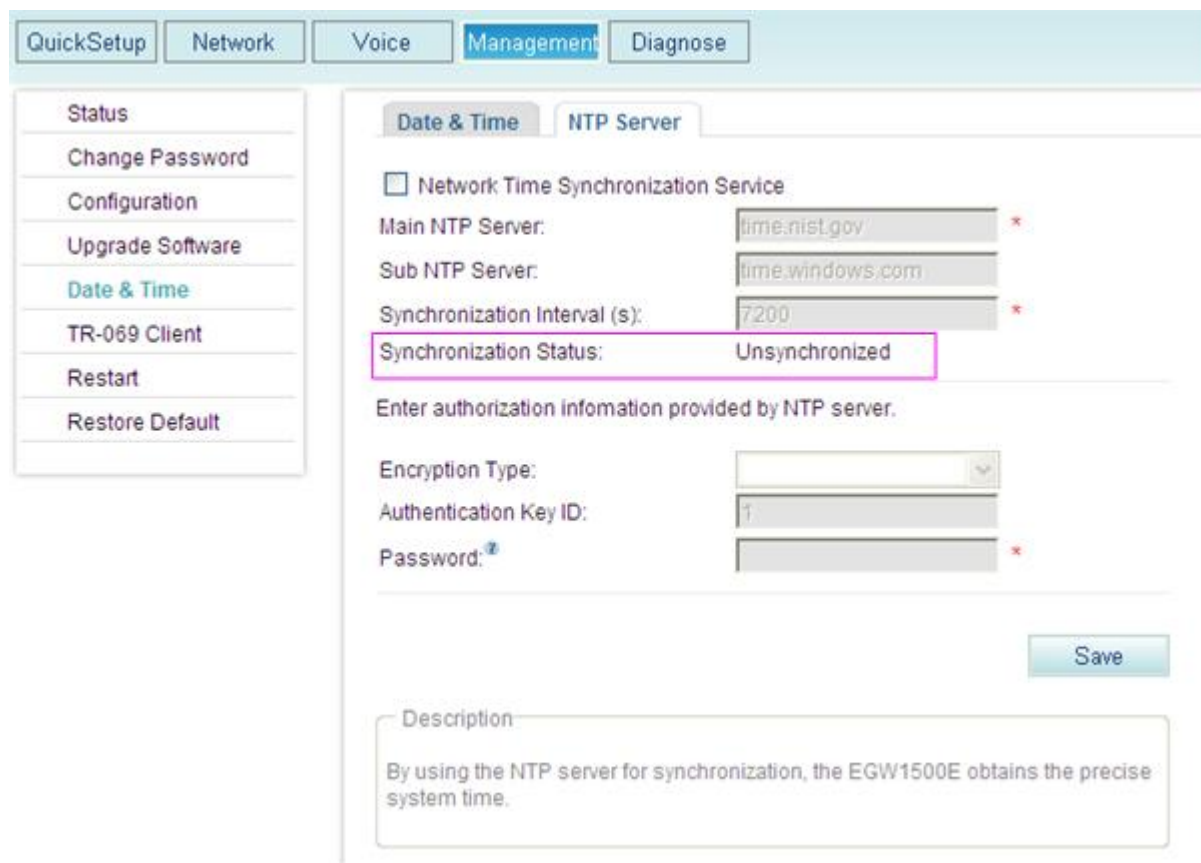
Step 1 Check the synchronization status of the NTP server.

Choose **Management > Date & Time** from the navigation tree on the web management system.

Click the **NTP Server** tab.

The page shown in [Figure 11-38](#) is displayed.

Figure 11-38 Checking the synchronization status of the NTP server



- If **Synchronization Status** is **Unsynchronized**, go to [2](#) and [3](#).
- If **Synchronization Status** is **Synchronized**, go to [4](#).

Step 2 Check the network connection.

Check the network connection in either of the following ways:

- Check whether the Internet indicator is on. If the indicator is on or blinks, the EGW1520 has been registered with the network service provider and the network connection is normal.

- Choose **Management > Status** from the navigation tree on the web management system, click the **Network** tab. If the value of **Status** is **Connected** on the **Network** page, the network connection is normal.

If the network connection is abnormal, see [Installation](#) to verify the cable connections and [7.2 Connection Modes](#) to verify the network configuration.

Step 3 Check whether the NTP server is reachable.

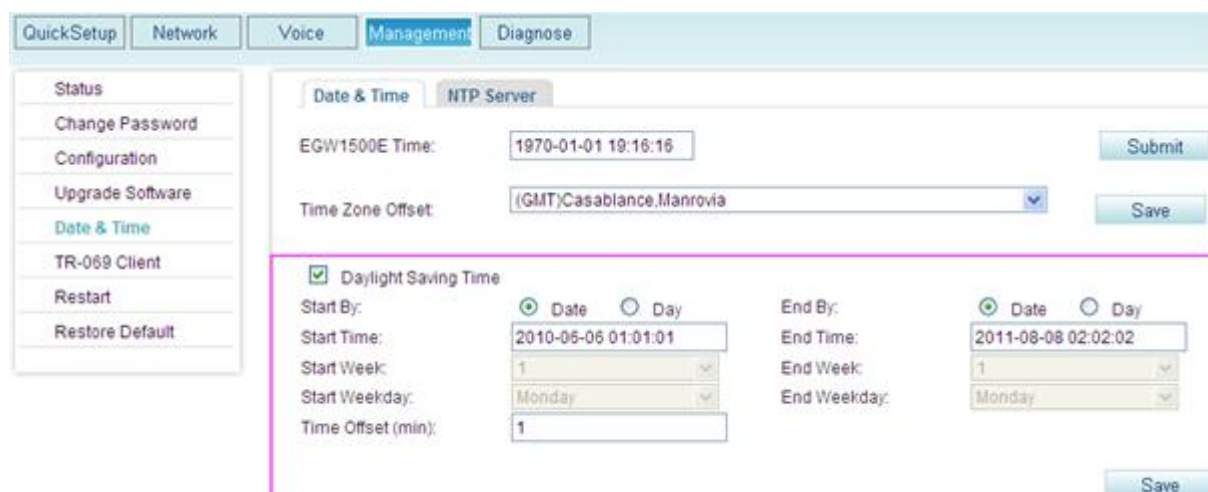
Run the **ping** command to check whether the NTP server is reachable. For example, enter **ping time.nist.gov** on the computer connected to the EGW1520. If this web site can be pinged, the NTP server is reachable. If the ping command fails, the NTP server is unreachable. Use another NTP server.

Step 4 Verify that the EGW1520 time zone and DST are configured correctly.

Choose **Management > Date & Time** from the navigation tree on the web management system.

The page shown in [Figure 11-39](#) is displayed.

Figure 11-39 Checking the time zone and DST configuration



Step 5 If the fault persists, see [Obtaining Huawei Technical Support](#).

----End

11.5.7 Failing to Restore Factory Settings by Pressing RESET

This topic provides the method to use for troubleshooting when the factory settings cannot be restored after the **RESET** button is pressed.

Symptom

The factory settings are not restored on the EGW1520 after a user presses the **RESET** button.

Possible Causes

Possible causes are as follows:

- The user holds the **RESET** button for less than six seconds. To restore the factory settings, the **RESET** button must be held for at least six seconds.
- The user does not hold the **RESET** button stably.

Troubleshooting Procedure

Step 1 Press and hold the **RESET** button for six seconds.

Step 2 If the fault persists after you perform the preceding operations, see [Obtaining Huawei Technical Support](#).

----End

12 Reference

About This Chapter

[Web_Parameters_Reference](#)

[12.1 TR-069 Parameter Reference](#)

This topic describes user-defined TR-069 parameters on the EGW1520.

[12.2 Security Log Information](#)

This topic describes the security log information displayed on the security log page.

[12.3 Customizing Voice Prompts for the Switchboard](#)

This topic describes how to customize voice prompts for the switchboard. Before delivery, the EGW1520 is loaded with switchboard voice prompts by default.

12.1 TR-069 Parameter Reference

This topic describes user-defined TR-069 parameters on the EGW1520.

NOTE

- [Table 12-1](#) lists the user-defined TR-069 parameters on the EGW1520. For details about other TR-069 parameters, see TR-069.
- In **Writable**, **W** represents **Write**.
- In **Default Value**, **false** represents **0** and **true** represents **1**.

Table 12-1 TR-069 Parameter

Parameter	Type	Writable	Description	Default Value
InternetGatewayDevice.DeviceInfo.	object	-	-	-
X_CPE_SwBui	string	-	Time when the software was	<Empty>

Parameter	Type	Writable	Description	Default Value
IdTimestamp			built.	
X_CPE_DslPhyDrvVersion	string	-	Version number of the Digital subscriber line (DSL) physical layer (PHY) and Driver.	<Empty>
X_CPE_VoiceServiceVersion	string	-	Version number of the voice software.	<Empty>
InternetGatewayDevice.X_CPE_SyslogCfg.	object	-	Syslog configuration file.	-
Status	string	W	Indicates whether the Syslog is enabled.	Disabled
Option	string	W	Path for storing exported syslogs. The values are local buffer , remote , and local buffer and remote .	local buffer
LocalLogLevel	string	W	Log level. The values are emergency , alert , critical , error , warning , notice , informational , and debug .	Error
ServerIPAddresses	string	W	IP address of the remote syslog server. This parameter is valid only if Option is set to remote , local buffer and remote , or local file and remote .	0.0.0.0
ServerPortNum	unsignedInt[1:6	W	Port of the	514

Parameter	Type	Writable	Description	Default Value
ber	5535]		remote syslog server.	
InternetGatewayDevice.ManagementServer.	object	-	-	-
X_CPE_BoundIfName	string	W	WAN port that TR-069 uses, for example, nas_0_35. This parameter can be set to Any_WAN and LAN . The value Any_WAN indicates that TR-069 will use any WAN connections. The value LAN indicates that TR-069 will use the default LAN subnet br0. Developers who have no WAN connection use the value LAN . The values are Any_WAN and LAN .	Any_WAN
InternetGatewayDevice.Time.	object	-	-	-
X_CPE_NTPSyncInterval	unsignedInt[300:604800]	W	Interval for synchronizing time with the NTP server.	7200
X_CPE_NTPAuthenticationType	string	W	Authentication type during time synchronization of the NTP server. The values are no-Auth , DES_Standard , DES_NTP_Standard .	no-Auth

Parameter	Type	Writable	Description	Default Value
			Standard, DES_ASCII, and MD5.	
X_CPE_NTPA uthenKeyid	unsignedInt[1:6 5535]	W	ID of the NTP server authentication key.	1
X_CPE_NTPA uthenKey	string(64)	W	NTP server authentication key. When X_CPE_NTPA uthenType is set to DES_Standard and DES_NTP Standard , the key is a string of 16 bytes that are internally converted to an 8-byte hexadecimal value. When X_CPE_NTPA uthenType is set to DES ASCII , the key is an ASCII string of 1-8 bytes. When X_CPE_NTPA uthenType is set to MD5 , the key is a string of 1-64 bytes.	<Empty>
InternetGatewa yDevice.WAN Device.{i}.WA NCommonInter faceConfig.	object	-	-	-
X_CPE_TxErro rs	unsignedInt	-	Total number of errors transmitted by a port.	-
X_CPE_RxErro rs	unsignedInt	-	Total number of errors received by a port.	-
X_CPE_TxDro	unsignedInt	-	Total number	-

Parameter	Type	Writable	Description	Default Value
ps			of dropped packets transmitted by a port.	
X_CPE_RxDrops	unsignedInt	-	Total number of dropped packets received by a port.	-
InternetGatewayDevice.WANDevice.{i}.X_CPE_XTM_Interface_Stats.{i}	object	-	This object contains the statistics on the xTM (ATM/PTM) port. This object is used to replace X_CPE_ATM_Interface_Stats , which is outdated.	-
Port	unsignedInt	-	Port number.	1
Status	string	-	Port status. The values are Enable and Disable .	Disabled
InOctets	unsignedInt	-	Number of bytes received by a port.	0
OutOctets	unsignedInt	-	Number of bytes transmitted by a port.	0
InPackets	unsignedInt	-	Number of AAL5, AAL0, and PTM packets received by a port.	0
OutPackets	unsignedInt	-	Number of AAL5, AAL0, and PTM packets transmitted by a port.	0
InOAMCells	unsignedInt	-	Number of ATM, OAM,	0

Parameter	Type	Writable	Description	Default Value
			and RM cells received by a port.	
OutOAMCells	unsignedInt	-	Number of ATM, OAM, and RM cells transmitted by a port.	0
InASMCCells	unsignedInt	-	Number of ATM, Bonding, and ASM cells received by a port.	0
OutASMCCells	unsignedInt	-	Number of ATM, Bonding, and ASM cells transmitted by a port.	0
InPacketErrors	unsignedInt	-	Number of error packets received by a port.	0
InCellErrors	unsignedInt	-	Number of error cells received by a port.	0
InternetGatewayDevice.WANDevice.{i}.WANDSLInterfaceConfig.	object	-	-	-
X_CPE_AdslModulationCfg	string	W	<p>Modulation mode. The supported values are ADSL_G.dmt, ADSL_G.lite, ADSL_G.dmt.bis, ADSL_re-adsl, ADSL_2plus, and ADSL_ANSI_T1.413.</p> <p>Note: 1. The ADSL_re-adsl parameter takes effect only</p>	ADSL_Modulation_All

Parameter	Type	Writable	Description	Default Value
			when it is set together with other parameters. 2. When the ADSL_Modulation_All parameter is set, other parameters do not need to be set. 3. The following parameters can be combined with a comma (.): ADSL_G.dmt, ADSL_2plus, ADSL_ANSI_T1.413, and ADSL_G.dmt.bis.	
X_CPE_PhoneLinePair	string	W	Inner pair or outer pair.	Inner Pair
X_CPE_Bitswap	string	W	Indicates whether the bit swap function is enabled.	On
X_CPE_SRA	string	W	Indicates whether the seamless rate adaptation function is enabled.	Off
X_CPE_LinkPowerState	string	-	Current link power state. The values are L0 (indicating steady on), L2 (indicating low power), and L3 (indicating idle).	L3
InternetGatewayDevice.WANDevice.{i}.WANDSLInterfaceConfig.Stats.To	object	-	-	-

Parameter	Type	Writable	Description	Default Value
tal.				
X_CPE_RxRsC orrectable	unsignedInt	-	Total number of correctable errors received by RS.	0
X_CPE_RxRsC orrectable_2	unsignedInt	-	Total number of correctable errors received by RS.	0
X_CPE_TxRsC orrectable	unsignedInt	-	Total number of correctable errors transmitted by RS.	0
X_CPE_TxRsC orrectable_2	unsignedInt	-	Total number of correctable errors transmitted by RS.	0
X_CPE_TxRsU ncorrectable	unsignedInt	-	Total number of uncorrectable errors transmitted by RS.	0
X_CPE_TxRsU ncorrectable_2	unsignedInt	-	Total number of uncorrectable errors transmitted by RS.	0
X_CPE_RxRsU ncorrectable	unsignedInt	-	Total number of uncorrectable errors received by RS.	0
X_CPE_RxRsU ncorrectable_2	unsignedInt	-	Total number of uncorrectable errors received by RS.	0
X_CPE_TxRs Words	unsignedInt	-	Total number of words transmitted by RS.	0
X_CPE_TxRs	unsignedInt	-	Total number	0

Parameter	Type	Writable	Description	Default Value
Words_2			of words transmitted by RS.	
X_CPE_RxRs Words	unsignedInt	-	Total number of words received by RS.	0
X_CPE_RxRs Words_2	unsignedInt	-	Total number of words received by RS.	0
X_CPE_ReceiveBlocks_2	unsignedInt	-	Total number of received blocks.	0
X_CPE_TransmitBlocks_2	unsignedInt	-	Total number of transmitted blocks.	0
X_CPE_ATUC FECErrors_2	unsignedInt	-	Total number of FEC errors detected by the ATU-C. FEC-CFE is defined in ITU-T Rec. G.997.1.	0
X_CPE_HECErrors_2	unsignedInt	-	Total number of detected HEC errors. HEC-P is defined in ITU-T Rec. G.997.1.	0
X_CPE_ATUC HECErrors_2	unsignedInt	-	Total number of HEC errors detected by the ATU-C. HEC-PFE is defined in ITU-T Rec. G.997.1.	0
X_CPE_UpstreamUas	unsignedInt	-	Upstream UAS counter.	0
X_CPE_DownstreamUas	unsignedInt	-	Downstream UAS counter.	0
X_CPE_UpstreamEs	unsignedInt	-	Upstream error rate.	0
X_CPE_Upstre	unsignedInt	-	Upstream sever	0

Parameter	Type	Writable	Description	Default Value
amSes			error rate.	
X_CPE_UpstreamBitErrors	unsignedInt	-	Upstream bit error.	0
X_CPE_UpstreamBitErrors_2	unsignedInt	-	Upstream bit error.	0
X_CPE_DownstreamBitErrors	unsignedInt	-	Downstream bit error.	0
X_CPE_DownstreamBitErrors_2	unsignedInt	-	Downstream bit error.	0
X_CPE_UpstreamDataCells	unsignedInt	-	Upstream data cell.	0
X_CPE_UpstreamDataCells_2	unsignedInt	-	Upstream data cell.	0
X_CPE_DownstreamDataCells	unsignedInt	-	Total downstream data cell.	0
X_CPE_DownstreamDataCells_2	unsignedInt	-	Total downstream data cell.	0
X_CPE_UpstreamTotalCells	unsignedInt	-	Total upstream cell.	0
X_CPE_UpstreamTotalCells_2	unsignedInt	-	Total upstream cell.	0
X_CPE_DownstreamTotalCells	unsignedInt	-	Total downstream cell.	0
X_CPE_DownstreamTotalCells_2	unsignedInt	-	Total downstream cells.	0
X_CPE_UpstreamLCD	unsignedInt	-	Upstream LCD.	0
X_CPE_UpstreamLCD_2	unsignedInt	-	Upstream LCD.	0
X_CPE_DownstreamLCD	unsignedInt	-	Downstream LCD.	0
X_CPE_DownstreamLCD_2	unsignedInt	-	Downstream LCD.	0
X_CPE_UpstreamOCD	unsignedInt	-	Upstream OCD.	0

Parameter	Type	Writable	Description	Default Value
X_CPE_UpstreamOCD_2	unsignedInt	-	Upstream OCD.	0
X_CPE_DownstreamOCD	unsignedInt	-	Downstream OCD.	0
X_CPE_DownstreamOCD_2	unsignedInt	-	Downstream OCD.	0
InternetGatewayDevice.WANDevice.{i}.WANEthernetInterfaceConfig.	object	-	-	-
X_CPE_IfName	string(32)	-	Linux port name, for example, eth0, eth1, eth1.2, and eth1.3.	<Empty>
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANDSLLinkConfig.	object	-	-	-
X_CPE_ATMMinimumCellRate	unsignedInt	-	Number of errors detected during header error check at the ATM layer.	-
X_CPE_SchedulerAlgorithm	string	-	Scheduling algorithm.	SP
X_CPE_ATMStatus	string	-	ATM status.	<Empty>
X_CPE_MacAddress	string(17)	-	MAC address of the PVC port. This parameter is used in the PPPoE, bridge, and MER modes.	<Empty>
X_CPE_IfName	string	-	Port name.	<Empty>
InternetGatewayDevice.WANDevice.{i}.WANConnectionDe	object	-	ATM initialization parameters.	-

Parameter	Type	Writable	Description	Default Value
vice.{i}.WAND SLLinkConfig. X_CPE_ATM_ PARMS.				
ATMFreeCellQ Size	unsignedInt	-	Length of the free ATM cell queue.	-
ATMFreePacke tQSize	unsignedInt	-	Length of a free ATM packet queue.	-
ATMFreePacke tQBufferSize	unsignedInt	-	Length of a free ATM packet queue in the buffer.	-
ATMFreePacke tQBufferOffset	unsignedInt	-	Offset of a free ATM packet queue in the buffer.	-
ATMReceiveC ellQSize	unsignedInt	-	Length of the queue of cells received by the ATM.	-
ATMReceivePa cketQSize	unsignedInt	-	Length of the queue of cells received by the ATM.	-
ATMTransmitF ifoPriority	unsignedInt	-	FIFO priority in ATM transmission.	-
ATMAal5Cpcs MaxSduLength	unsignedInt	-	Maximum SDU length of ATM AAL5 CPCS.	-
ATMAal2Sscs MaxSsarSduLe ngth	unsignedInt	-	Maximum SDU length of ATM AAL2 CPCS.	-
InternetGatewa yDevice.WAN Device.{i}.WA NConnectionDe vice.{i}.X_CPE _WANUSB.	object	-	WANUSB configurations.	-
IfName	string(32)	-	Port name.	ppp0
ManulDialFlag	boolean	-	Dialing mode. The values are true (Manual)	false

Parameter	Type	Writable	Description	Default Value
			and false (Auto).	
ConnectStatus	int[0:4]	-	Connection status. The values are Connecting , Connected , and Disconnected .	0
SIMPIN	string(32)	-	PIN code of a SIM card.	1234
SimPinLockEnable	boolean	-	Indicates whether to enable the system to use the PIN code to lock the SIM card.	false
DialStringTD	string(32)	-	-	-
APNTD	string(32)	-	-	-
DailMethod	int[0:2]	-	Dialing mode.	0
SimCardState	int[0:5]	-	SIM card status. The values are 0 (ready), 1 (no device), 2 (PIN required), 3 (PUK required), and 4 (internal error).	1
ISP	string(64)	-	Network carrier.	vodafone
SigIntensity	int[0:99]	-	Signal intensity. The values are 0 to 5 . The value 0 indicates no signal.	0
localIP	string(32)	-	Local IP address.	0.0.0.0
DNS	string(64)	-	IP address of the domain name server (DNS).	0.0.0.0

Parameter	Type	Writable	Description	Default Value
PrimaryDNS	string(32)	-	IP address of the active DNS.	0.0.0.0
SecondDNS	string(32)	-	IP address of the standby DNS.	0.0.0.0
IMEI	string(32)	-	International mobile equipment identity (IMEI).	NoDataCard
ConDuration	unsignedInt	-	Connection duration.	0
SYSMODE	string	-	System mode.	No Service
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANIPConnection.{i}	object	W	-	-
X_CPE_IfName	string	-	Port name.	-
X_CPE_Op42NTPSrv	string(128)	-	Option 42. IP address of the NTP server. The value format is IP1,IP2.	<Empty>
X_CPE_Op43VSI	string(256)	-	Option 43. Specific vendor information. The value is a string.	<Empty>
X_CPE_Op66TFTPSrvName	string(256)	-	Option 66. TFTP server name. The value is a string.	<Empty>
X_CPE_Op67Bootfile	string(256)	-	Option 67. Boot file name. The value is a string.	<Empty>
X_CPE_Op120SIPSrv	string(256)	-	Option 120. SIP server. The value format complies with	<Empty>

Parameter	Type	Writable	Description	Default Value
			RFC3361.	
X_CPE_Op150 TFTPSrvIP	string(256)	-	Option 150. IP address of the TFTP server. The value format is IP1,IP2.	<Empty>
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANIPConnection.{i}.Stats.	object	-	-	-
X_CPE_RxDrops	unsignedInt	-	Total number of received packets that are dropped during a connection.	0
X_CPE_TxDrops	unsignedInt	-	Total number of transmitted packets that are dropped during a connection.	0
X_CPE_RxErrors	unsignedInt	-	Total number of received errors.	0
X_CPE_TxErrors	unsignedInt	-	Total number of transmitted errors.	0
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANPPConnection.{i}.	object	W	-	-
X_CPE_ConnectionEstablishedTime	unsignedInt	-	Duration for establishing PPP connections.	0
X_CPE_IfName	string	-	Port name.	-
X_CPE_DefaultGateway	string	-	Default gateway for the WAN port.	<Empty>

Parameter	Type	Writable	Description	Default Value
			The PPPoE/PPPoA WAN gateway is used only in the MDM mode.	
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANPPConnection.{i}.Stats.	object	-	-	-
X_CPE_RxDrops	unsignedInt	-	Total number of received packets that are dropped during a connection.	0
X_CPE_TxDrops	unsignedInt	-	Total number of transmitted packets that are dropped during a connection.	0
X_CPE_RxErrors	unsignedInt	-	Total number of received errors.	0
X_CPE_TxErrors	unsignedInt	-	Total number of transmitted errors.	0
InternetGatewayDevice.Services.VoiceService.{i}.	object	-	-	-
X_CPE_SipMinExpire	unsignedInt[30:65535]	W	Minimum timeout duration for the local SIP user to send a registration request to EGW1520.	120
X_CPE_SipMaxExpire	unsignedInt[30:65535]	W	Maximum timeout duration for the local SIP user to send a registration	3600

Parameter	Type	Writable	Description	Default Value
			request to EGW1520.	
X_CPE_SessionTimerStart	boolean	W	Indicates whether to enable the SIP session timer.	false
X_CPE_SessionTimerInterval	unsignedInt[90:65535]	W	Session interval.	1800
X_CPE_SessionTimerMinInterval	unsignedInt[90:65535]	W	Minimum session interval.	90
X_CPE_MinSubExpires	unsignedInt[120:3600]	W	Minimum timeout duration for the local SIP user to send a subscription request to EGW1520.	120
X_CPE_DefaultSubExpires	unsignedInt[120:3600]	W	Default timeout duration for EGW1520 to send a subscription request to the upper-level device.	360
X_CPE_MaxSubExpires	unsignedInt[120:3600]	W	Maximum timeout duration for the local SIP user to send a subscription request to EGW1520.	3600
InternetGatewayDevice.Services.VoiceService.{i}.Capabilities	object	-	-	-
X_CPE_MaxRegGroupCount	unsignedInt	-	Maximum number of X_CPE_IMS_RegGroup groups that are supported.	0

Parameter	Type	Writable	Description	Default Value
InternetGatewayDevice.Services.VoiceService.{i}.Capabilities.Codecs.{i}.	object	W	-	-
X_CPE_PTimeDefault	unsignedInt	W	Packing duration.	20
InternetGatewayDevice.Services.VoiceService.{i}.Capabilities.X_CPE_Codecs_Ext.	object	-	-	-
EcEnable	boolean	W	Indicates whether to enable the echo suppression.	true
SilenceSuppEenable	boolean	W	Indicates whether to enable the silence suppression.	true
CodecList	string(64)	W	DSP codec type. A device can be configured with multiple codec types. The local device preferentially selects the first type to negotiate with the peer device. The priorities are in descending order. The values are G711A , G711U , G729A/B , G726 , and G722 .	G711A,G711U, G729A/B,G726, G722
RecvGain	int[-96:32]	W	Receiving gain.	-2
SendGain	int[-96:32]	W	Transmission gain.	-8

Parameter	Type	Writable	Description	Default Value
MediaNegMode	string	W	Media negotiation mode. The values are RemotePri and LocalPri .	RemotePri
VBDAlgo	string	W	Codec type used in fax transparent transmission. The values are G711A and G711U .	G711A
FaxPriorMode	string	W	Fax transmission mode. The values are VBD_T38 , T38_VBD , T38 , and VBD .	VBD_T38
InternetGatewayDevice.Services.VoiceService.{i}.VoiceProfile.{i}	object	-	-	-
X_CPE_NumberOfRegGroup	unsignedInt	-	Number of X_CPE_IMS_RegGroup groups in a voice file.	0
InternetGatewayDevice.Services.VoiceService.{i}.VoiceProfile.{i}.X_CPE_IMS_RegGroup.{i}	object	W	Registration group of a SIP user.	-
X_CPE_RegId	unsignedInt	-	ID of the registration group of a SIP or POTS user.	4294967295
X_CPE_RegisterType	string	W	Registration type. The values are Single , Group , and Wildcard . The value single indicates	Single

Parameter	Type	Writable	Description	Default Value
			that a registration groups can only have one user. The value Group indicates that multiple users can be in a registration group. The value Wildcard indicates that the users in a registration group register with the IMS or NGN network based on certain rules provided by the network carrier.	
X_CPE_AuthType	string	W	Mode for authenticating a SIP user when registering with EGW1520. This parameter value must be the same as that specified on the SIP user's terminal. The values are NoAuth , AuthByMD5 , AuthByMD5ess , and AuthByHW .	NoAuth
X_CPE_IMSI MPIInfo	string(130)	W	SIP trunk ID when a registration group registers with the IMS or NGN network, which is provided by the network carrier. This parameter is mandatory.	<Empty>

Parameter	Type	Writable	Description	Default Value
X_CPE_IMSI MPUInfo	string(257)	W	SIP trunk name when a registration group registers with the IMS or NGN network, which is provided by the network carrier.	<Empty>
X_CPE_AuthP WD	string(130)	W	Password for authenticating the registration group when registering with the IMS or NGN network, which is provided by the network carrier.	<Empty>
X_CPE_IMSD omainName	string(255)	W	Domain name of the IMS network that a registration group is to be registered with, which is provided by the network carrier. This parameter value must be a valid domain name.	<Empty>
InternetGatewa yDevice.Servic es.VoiceService . {i}.VoiceProfil e. {i}.SIP.	object	-	-	-
X_CPE_IfDom ain	boolean	W	-	false
X_CPE_Server Type	string	W	-	NGN_Server
X_CPE_IfSrv	boolean	W	-	false
X_CPE_Option sInterval	unsignedInt[10: 900]	W	Interval for switching between the master node and the slave node.	60

Parameter	Type	Writable	Description	Default Value
X_CPE_IfChangeToMaster	boolean	W	Indicates whether to enable the switching between the master node and the slave node.	false
InternetGatewayDevice.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.X_CPE_BackupServer	object	-	-	-
ProxyServer	string(255)	W	Proxy server. This parameter value must be the same as the value of RegistrarServer .	<Empty>
ProxyServerPort	unsignedInt[1024:65535]	W	Port number of the SIP server, which is provided by the network carrier. This parameter value must be the same as the value of RegistrarServerPort .	5060
RegisterExpires	unsignedInt[0:14400]	W	Interval for a registration group user to send registration requests to the SIP server, in seconds.	360
X_CPE_IfDomain	boolean	W	-	false
RegistrarServer	string(255)	W	IP address or DNS name of the SIP server, which is provided by the	<Empty>

Parameter	Type	Writable	Description	Default Value
			network carrier.	
RegistrarServerPort	unsignedInt[1024:65535]	W	-	5060
X_CPE_ServerType	string	W	SIP server type. The values are NGN_Server and NGN_Server .	NGN_Server
X_CPE_IsSrv	boolean	W	-	false
InternetGatewayDevice.Services.VoiceService.{i}.X_CPE_SipRtpPort.	object	-	-	-
MaxRtpPort	string	W	-	20000
MinRtpPort	string	W	-	10000
SipPort	string	W	-	5060
InternetGatewayDevice.Services.VoiceService.{i}.VoiceProfile.{i}.FaxT38.	object	-	-	-
X_CPE_IsUdpTl	boolean	-	Transmission protocol. The values are true (UDP) and false (TCP).	true
X_CPE_FaxUdpEc	string	-	Error correction mode of faxes.	T38UdpRedundancy
X_CPE_TCFMmethod	string	-	Fax rate.	Network
X_CPE_MaxBitRate	unsignedInt	-	Maximum rate.	14400
InternetGatewayDevice.X_CPE_NetworkConfig.	object	-	The network configuration object contains the default gateway information (a WAN router) and DNS information (WAN port name or static	-

Parameter	Type	Writable	Description	Default Value
			IP address).	
DNSIfName	string	W	Use a comma (,) to separate multiple DNS servers. The first one has the highest priority, and the last one has the lowest priority.	<Empty>
DNSServers	string(33)	W	Static DNS server.	<Empty>
ActiveDNSServers	string	-	This string contains a list of DNS IP addresses that are same in resolv.conf . The default value 0.0.0.0 , indicating that the active DNS server is not running.	0.0.0.0
InternetGatewayDevice.X_CPE_MultiRegionConfig.	object	-	Adaption to multiple countries.	-
CurrentRegion	string(32)	W	Current country. The example values are CHINA , NEW ZEALAND , and IRELAND .	-
InternetGatewayDevice.X_CPE_MultiRegionConfig.RegionConfig.{i}.	object	-	Region.	-
RegionName	string(32)	-	Region name.	-
InternetGatewayDevice.X_CPE_MultiRegionConfig.RegionConfig.{i}.Gain	object	-	Region gain.	-

Parameter	Type	Writable	Description	Default Value
Config.				
Rxgain	int[-12:6]	W	Receiving gain of an analog phone, in dB.	-
Txgain	int[-12:6]	W	Transmission gain of an analog phone, in dB.	-
InternetGatewayDevice.X_CPE_MultiRegionConfig.RegionConfig.{i}.TimeParameterConfig.	object	-	Region time.	-
on-hookmintime	unsignedInt[0:2000]	W	Minimum on-hook confirmation duration, in milliseconds.	-
off-hookmintime	unsignedInt[0:2000]	W	Minimum off-hook confirmation duration, in milliseconds.	-
Flashhookmintime	unsignedInt[0:1000]	W	Minimum hookflash duration, in milliseconds.	-
Flashhookmaxtime	unsignedInt[0:1000]	W	Maximum hookflash duration, in milliseconds.	-

12.2 Security Log Information

This topic describes the security log information displayed on the security log page.

Table 12-2 Security log information

No.	Information	Module
1	Added an ATM interface	ADSL

No.	Information	Module
2	Deleted an ATM interface	
3	Added ADSL configuration	
4	remove adsl PPPOE Service	
5	Added WAN configuration succeed	WAN
6	remove wan IPOE Service succeed	
7	Modified 3G configuration	3G
8	Saved basic configuration of the wireless network	WLAN
9	Modified security configuration of the wireless network	
10	Added the MAC filter information about the wireless network succeed	
11	Deleted the MAC filter information about the wireless network succeed	
12	Saved the MAC filter information about the wireless network succeed	
13	Saved advanced configuration of the wireless network	
14	Saved LAN information succeed	LAN
15	Added LAN information succeed	
16	Deleted LAN information succeed	
17	Modified DNS information	DNS
18	Added an incoming IP address filtering rule	Security
19	Deleted an outgoing IP address filtering rule	
20	Added an outgoing IP address filtering rule	
21	Deleted an outgoing IP address filtering rule	
22	Changed Mac filtering policy	
23	Added Filter MAC	
24	Deleted Filter MAC	
25	Added security URL filter information	
26	Deleted security URL filter information	

No.	Information	Module
27	Saved security URL filter information	
28	Added Virtual Server	
29	Deleted Virtual Server	
30	Modified Dmz host IP address	
31	save Remote login info	
32	Added a static route	Routing
33	Deleted a static route	
34	Added a VPN tunnel	VPN
35	Modified a VPN tunnel	
36	Deleted a VPN tunnel	
37	Deleted a VPN tunnel	
38	Added a VPN Stream	
39	Modified a VPN Stream	
40	Deleted a VPN Stream	
41	Added a local certificate	Certificate
42	Imported a local certificate	
43	Deleted a local certificate	
44	Imported a ca certificate	
45	Deleted a ca certificate	
46	Saved VLAN configuration	VLAN
47	Saved QoS configuration management information	QoS
48	Added QoS queue configuration	
49	Deleted QoS queue configuration	
50	Saved QoS queue configuration	
51	Added QoS stream classification information	
52	Enable QoS stream classification information	
53	Disable QoS stream classification information	
54	Deleted QoS stream classification information	

No.	Information	Module
55	Modified anti-attack information	AntiAttack
56	Modified the SIP registration	SIP Server
57	Modified the phone configuration	Phone Allocation
58	Modified FXO prefix	FXO Configuration
59	Modified FXO bound number	
60	Modified attendant configuration	
61	Modified voice service permission	Service Manager
62	Modified voice service configuration	
63	Changed the service prefix	Service Prefix
64	Uploaded a voice file	Upload Voice File
65	Saved country configuration in voice parameters	Voice parameters
66	Modified DSP configuration in voice parameters	
67	Saved RTP information in voice parameters	
68	Saved SIP information in voice parameters	
69	change the info of Voice Parameters SIP ALG	
70	Changed the password	Change Password
71	Backed up a configuration file	Configuration
72	Imported a configuration file	
73	Imported a configuration file	
74	Set the date and time	Date&Time
75	Configured the TR069 client	TR-069 Client
76	Updated the image file	Update Software
77	Auto Upgrade image file	
78	Restarted the system	Restart
79	Restored to factory settings	Restore Default
80	Saved system logs	System Logs
81	Downloaded system logs	
82	Deleted system logs	

No.	Information	Module
83	Modified and saved debug logs	Debug Logs
84	Downloaded alarm logs	Warning info
85	Deleted alarm logs	
86	Downloaded security logs	SecurLog info
87	Deleted security logs	
88	Modified and saved captured packets from an imaged port	Packet Mirroring
89	Downloaded the black box file	Black Box
90	Deleted the black box file	
91	Run the ping command	Ping Diagnose
92	Saved call records	Call Recording
93	Downloaded call records	
94	Clicked one button to download information	One-Click Download
95	user login failed	Login
96	users been locked	
97	user login succeed	
98	User logout succeed	Logout

12.3 Customizing Voice Prompts for the Switchboard

This topic describes how to customize voice prompts for the switchboard. Before delivery, the EGW1520 is loaded with switchboard voice prompts by default.

Background

The following describes how to use the recording software of Windows to customize voice prompts for the switchboard.

NOTE

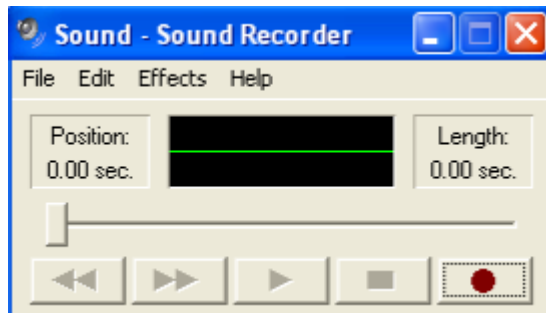
The voice file is **200.pcm**. You must name the voice file to **200.pcm** to replace the original one.

Procedure


Step 1 Choose **Start > All Programs > Accessories > Entertainment > Sound Recorder**

The page shown in [Figure 12-1](#) is displayed.

Figure 12-1 Sound recorder



Step 2 Click  to record a voice prompt.

Step 3 Click  to stop recording.

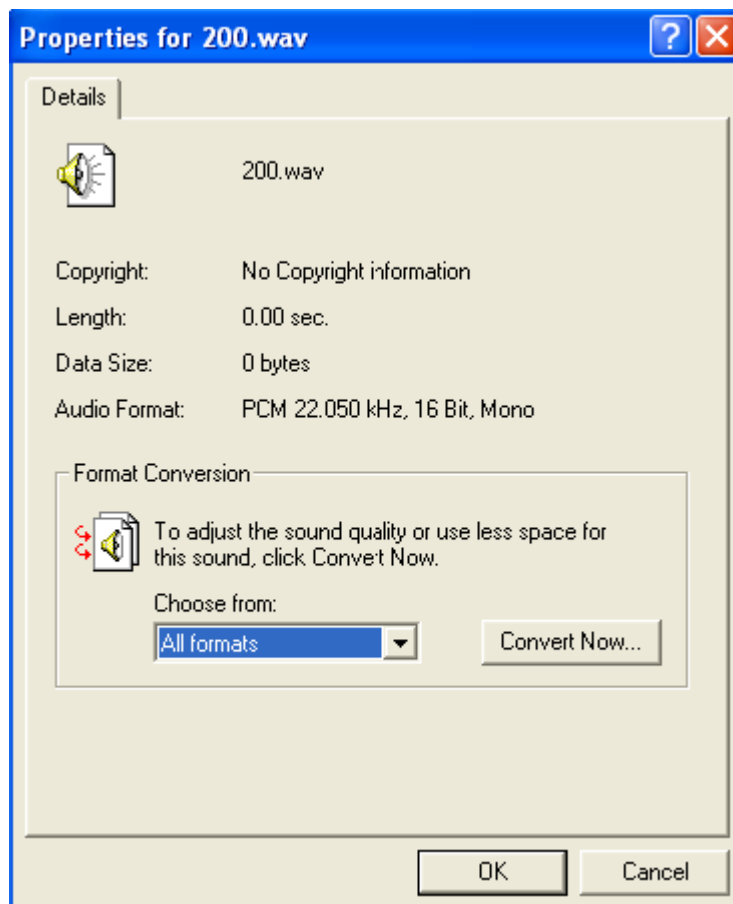
Step 4 Choose **File > Save** to save the recording.

Step 5 Convert the recording to a file in the CCITT A-Law, 8000 Hz, 8 bit, mono format.

1. Choose **File > Properties**

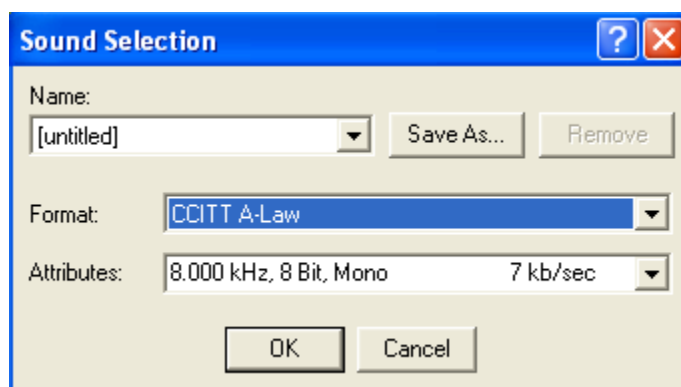
The page shown in [Figure 12-2](#) is displayed.

Figure 12-2 Modifying recording properties (1)



2. Click **Convert Now**.
The page shown in [Figure 12-3](#) is displayed.

Figure 12-3 Modifying recording properties (2)



3. Set **Format** to **CCITT A-Law**, and set **Attribute** to **8.000 kHz, 8 bit, mono 7 Kbit/s**.
4. Click **OK**.

Step 6 Choose **File > Save As** to save the recording as the **200.pcm** file.

Step 7 Upload the **200.pcm** file.

For details, see [9.12 Uploading Voice Files](#).

----End

13 Glossary

About This Chapter

This section provides the glossary of documentation.

[13.1 Numerics](#)

[13.2 A](#)

[13.3 B](#)

[13.4 C](#)

[13.5 D](#)

[13.6 E](#)

[13.7 F](#)

[13.8 G](#)

[13.9 H](#)

[13.10 I](#)

[13.11 L](#)

[13.12 M](#)

[13.13 N](#)

[13.14 O](#)

[13.15 P](#)

[13.16 Q](#)

[13.17 R](#)

[13.18 S](#)

[13.19 T](#)

[13.20 U](#)

[13.21 V](#)

[13.22 W](#)

13.23 Z

13.1 Numerics

3WC	See three-way calling
802.11n	A wireless transmission standard released after 802.11a/b/g by Wi-Fi Alliance. As a new member to the 802.11 protocol family, 802.11n supports the 2.4 GHz and 5 GHz frequency bands and provides a higher bandwidth (300 Mbit/s, much higher than the 54 Mbit/s provided by 802.11a/g) for WLAN access users. In addition, 802.11n supports the MIMO technology, which provides two methods of increasing the communication rate: by increasing the bandwidth and by improving the channel usage.

13.2 A

AC mains	The principal conduit in a system for conveying AC power utility.
access point	Any entity that has station functionality and provides access to the distribution services, via the wireless medium (WM) for associated stations.
access server	Any device that enables multiple remote users to access a network.
active	A state of a piece of equipment in normal operation.
adapter	A universal protocol conversion device. The adapter is responsible for the conversion between external protocols and internal messages.
address	A number that identifies the location of a device in a network or the location on the hard disk or the memory, such as the IPv4 address or IPv6 address of a network entity.
address pool	A set of IP addresses assigned by Internet Assigned Number Authority (IANA) or an organization tied to IANA.
Address Resolution Protocol	An Internet Protocol used to map IP addresses to MAC addresses. It allows hosts and routers to determine the link layer addresses through ARP requests and ARP responses.
administrator	A user who has authority to access all the Management Domains of the product. He or she has access to the whole network and to all the management functionalities.
application layer	It provides applications such as game center, conference center, friend center, enterprise applications, IM, streaming and general telecommunication services. It can also invoke the service capability of the lower layer through the API interface provided by OSA to implement various services.
application server	A service processing node (a computer device) in the network. Application programs of data services are run on the application server.

application service provider	A company that provides Internet download and related services for various organizations. Without ASP, these organizations have to store such information in their own computers.
area code	The national area code assigned for a local network, which is used in call connection.
ARP	See Address Resolution Protocol
ASP	See application service provider
audio	The sound portion of a program or a track recorded on a videotape which contains sound, music or narration.
authentication	A process of checking whether a user can be awarded with access right or what kinds of users can access a resource.

13.3 B

backup	A periodic operation performed on the data stored in the database for the purposes of database recovery in case that the database is faulty. The backup also refers to data synchronization between active and standby boards.
band	The range of frequencies between two defined limits.
bandwidth	A range of transmission frequencies that a transmission line or channel can carry in a network. In fact, it is the difference between the highest and lowest frequencies the transmission line or channel. The greater the bandwidth, the faster the data transfer rate.
base	A kind of bus or plane used to load software, transmit alarms and maintain information exchange.
baseband	A form of modulation in which the information is applied directly onto the physical transmission medium.
basic service	This term is used as a common reference to both bearer services and teleservices.
bidirectional	Pertaining to a link where the transfer of users' information is possible simultaneously in both directions between two points. Notes: 1. The transmission channel capacity and signaling rate are not necessarily the same in both directions. 2. Do not use this term to describe the directions of call setups.
bit	The smallest unit of information handled by a hardware component. One bit expresses a 1 or a 0 in a binary numeral, or a true or a false logical condition, and is represented physically by an element such as a high or low voltage at one point in a circuit or a small spot on a disk magnetized one way or the other. A single bit conveys little information a human would consider meaningful. A group of eight bits, however, makes up a byte, which can be used to represent many types of information, such as a letter of the alphabet, a decimal digit, or other character.

bit error rate	Ratio of received bits that contain errors. BER is an important index used to measure the communications quality of a network.
blacklist	A method of filtering packets based on their source IP addresses. Compared with ACL, the match condition for the black list is much simpler. Therefore, the black list can filter packets at a higher speed and can effectively screen the packet sent from the specific IP address.
BRAS	See broadband remote access server
bridge	A device that connects two or more networks and forwards packets among them. Bridges operate at the physical network level. Bridges differ from repeaters because bridges store and forward complete packets, while repeaters forward all electrical signals. Bridges differ from routers because bridges use physical addresses, while routers use IP addresses.
bridging	The action of transmitting identical traffic on the working and protection channels simultaneously.
broadband access server	A server providing features as user access, connection management, address allocation and authentication, authorization and accounting. It also works as a router featuring effective route management, high forwarding performance and abundant services.
broadband remote access server	A new type of access gateway for broadband network. As a bridge between backbone networks and broadband access networks, BRAS provides methods for fundamental access and manages the broadband access network. It is deployed at the edge of network to provide broadband access services, convergence, and forwarding of multiple services, meeting the demands for transmission capacity and bandwidth utilization of different users. Hence, BRAS is a core device for the broadband users' access to a broadband network.
broadcast domain	A group of network stations that receives broadcast packets originating from any device within the group. Broadcasts do not pass through a router, which bound the domains. In addition, the set of ports between which a device forwards a multicast, broadcast, or unknown destination frame.
buffer	A storage area used for handling data in transit. Buffers are used in networking to compensate for differences in processing speed between network devices. Bursts of data can be stored in buffers until they can be handled by slower processing devices. In a program, buffers are created to hold some amount of data from each of the files that will be read or written. In a streaming media application, the program uses buffers to store an advance supply of audio or video data to compensate for momentary delays.
buffer overflow	A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity.

bus	A path or channel for signal transmission. The typical case is that, the bus is an electrical connection that connects one or more conductors. All devices that are connected to a bus, can receive all transmission contents simultaneously.
byte	A unit of computer information equal to eight bits.

13.4 C

call control	A set of functions used to process a call, including establishing, supervising, maintaining, connecting, and releasing calls, and provide service features.
call forwarding	A feature on telephone networks that allows an incoming call to a called party, who is unavailable, to be redirected to another telephone.
call hold	A service that permits a subscriber to hold a call already set up. In this case, the transmission of media streams between the caller and callee is stopped, but the call resources are not released. The call can be resumed when required.
call transfer	A feature on telephone networks that enables a user to relocate an existing call to another telephone by using the transfer button and dialing the required location.
carriage return	The keyboard key used to signal the end of a line of data or the end of a command.
carrier	An organization that has telecom network resources and can provide communications service.
CDR	Call Detail Record.
CFU	Call Forwarding Unconditional.
Challenge Handshake Authentication Protocol	A method to periodically verify the identity of the peer using a 3-way handshake. During the setting up of a link, the authenticator sends a "challenge" message to the peer. The peer responds with a value calculated using a "one-way hash" function. The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged. CHAP provides protection against playback attack.
channel	A telecommunication path of a specific capacity and/or at a specific speed between two or more locations in a network. Channels can be established through wire, radio (microwave), fiber or a combination of the three. The amount of information transmitted per second in a channel is the information transmission speed, expressed in bits per second. For example, bit/s, kbit/s, Mbit/s, Gbit/s, and Tbit/s.
CHAP	See Challenge Handshake Authentication Protocol
claw hammer	Used to knock or shape a workpiece, or extract a nail.
client mode	The login mode of a client, which includes the single-user mode and multi-user mode. By default, the login mode is the multi-user mode.

Client/Server	The model of interaction in a distributed system in which a program at one site sends a request to a program at another site and awaits a response. The requesting program is called a client. The program satisfying the request is called the server.
CLK	clock.
CNG	comfort noise generation.
code	A method of replacing Chinese characters with English letters. Usually, you can perform code through the methods such as simple spelling, full spelling, initials, and full spelling of the last word but initials of other words. For example, the simple spelling of Huawei in the number library is hw.
CODEC	See coder and decoder
coder and decoder	Coder transforms analog data into a digital bit stream. Decoder transforms digital signals into analog data.
collision	A condition in which two packets are being transmitted over a medium at the same time. Their interference makes both unintelligible.
command line	A string of text written in the command language and passed to the command interpreter for execution.
concentrator	A switching device allowing simultaneous different connections between a plurality of inlets on one side and a small number of traffic circuits on the other. Note: The concentrator performs a traffic concentration in one direction and a traffic expansion.
congestion	An extra intra-network or inter-network traffic resulting in decreasing network service efficiency.
congestion management	A flow control measure to solve the problem of network resource competition. When the network congestion occurs, it places the packet into the queue for buffer and determines the order of forwarding the packet.
core	A memory, especially one consisting of a series of tiny doughnut-shaped masses of magnetic material.
cross-sectional area	The area of a two-dimensional slice of a three-dimensional object.

13.5 D

data flow	A process that involves processing the data extracted from the source system, such as filtering, integration, calculation, and summary, finding and solving data inconsistency, and deleting invalid data so that the processed data meets the requirements of the destination system for the input data.
data model	When we use IT systems to manage business information, we extract the main features of the information according to the business requirements, and then abstract a model that can reflect the

relationship between the business information (objects). This model is called data model.

database	A database stores a combination of data. Serving various applications, the data is configurable and has no harmful or unnecessary redundancy. The data is stored separately from the relevant programs. You can use a common and controllable method to insert new data into the database in addition to modifying and searching the data in the database. If several databases totally separated in structure exist in a system, the system contains a database combination.
datagram	A kind of PDU which is used in Connectionless Network Protocol, such as IP datagram, UDP datagram.
daylight saving time	Time during which clocks are set one hour or more ahead of standard time to provide more daylight at the end of the working day during late spring, summer, and early fall.
dBm	Absolute power level with respect to 1 milliwatt, expressed in decibels.
DC	See direct current
decoding	The process of restoring information from its coded representation to the original form.
default gateway	A configuration item for the TCP/IP protocol that is the IP address of a directly reachable IP router.
delay	An average time taken by the service data to transmit across the network.
demodulation	In communications, the means by which a modem converts data from modulated carrier frequencies (waves that have been modified in such a way that variations in amplitude and frequency represent meaningful information) over a telephone line. Data is converted to the digital form needed by a computer to which the modem is attached, with as little distortion as possible.
DHCP	See Dynamic Host Configuration Protocol
DHCP relay	Dynamic Host Configuration Protocol relay.
DHCP server	A program that allocates the IP addresses of the local address pool to the users at the user side and allocates the IP addresses of the relay address pool to the users that pass through the DHCP proxy at the network side.
dial tone	A dial tone is a telephony signal used to indicate that the telephone exchange is working, has recognized an off-hook, and is ready to accept a call. The tone stops when the first numeral is dialed. If no digits are forthcoming, the permanent signal procedure is invoked, often eliciting a special information tone.
digital subscriber line	A technology for providing digital connections over the copper wire or the local telephone network. DSL performs data communication over the POTS lines without affecting the POTS service.
digital subscriber line access	A network device, usually situated in the main office of a telephone company that receives signals from multiple customer Digital

multiplexer	Subscriber Line (DSL) connections and puts the signals on a high-speed backbone line using multiplexing techniques.
direct current	Electrical current whose direction of flow does not reverse. The current may stop or change amplitude, but it always flows in the same direction.
Distributed Object-oriented Programmable Realtime Architecture	An OS-layer, middleware-level, highly-tailorable, component-based, open software platform. It helps to accommodate the difference of upper-layer OS, hardware, network, and system scale.
DND	do not disturb.
DNS	domain name server.
DNS server	A device that can provide domain name resolution for the client on the network
domain name	A name composed of numbers or characters. Each domain name corresponds to an IP address.
DOPRA	See Distributed Object-oriented Programmable Realtime Architecture
downstream	In an access network, where there is a clear indication in each deployment as to which end of a link is closer to a subscriber, transmission toward the subscriber end of the link.
DSL	See digital subscriber line
DSLAM	See digital subscriber line access multiplexer
DST	See daylight saving time
dual core	Dual core means that the processor has two full execution cores, both running at the same clock, in one physical processor.
dual homing	A network topology in which a device is connected to the network at two independent access points. One point is the primary connection and the other a standby connection that is activated in the event of a failure of the primary connection.
duplex	Capable of carrying information in both directions over a communications channel. A system is full-duplex if it can carry information in both directions at once; it is half-duplex if it can carry information in only one direction at a time.
Dynamic Host Configuration Protocol	A client-server networking protocol. A DHCP server provides configuration parameters specific to the DHCP client host requesting, generally, information required by the host to participate on the Internet network. DHCP also provides a mechanism for allocation of IP addresses to hosts.

13.6 E

EC	See echo cancellation
-----------	---------------------------------------

echo cancellation	Echo cancellation indicates the configuration of an echo canceler (usually called EC) in the communication network with the echo problem to reduce or eliminate echoes.
element	A document structuring unit delimited by tags. An element is delimited by a start-tag and an end-tag, except an empty element that is delimited by an empty-element tag.
encapsulation	The technique used by layered protocols in which a lower level protocol accepts a message from a higher-level protocol and places it in the data portion of the low level frame. Handling protocol A's packets, the packets are complete with A's header information, as data carried by protocol B. Encapsulated protocol A packets have a B header, followed by an A header, followed by the information that protocol A is carrying its own data. Note that A could equal to B, as in IP inside IP.
encryption	A function used to transform data to hide its information content to prevent unauthorized use.
equipment serial number	A string of characters that identify a piece of equipment and ensures correct allocation of a license file to the specified equipment. It is also called "equipment fingerprint".
ES	echo suppression.
Ethernet	A technology complemented in LAN. It adopts Carrier Sense Multiple Access/Collision Detection. The speed of an Ethernet interface can be 10 Mbit/s, 100 Mbit/s, 1000 Mbit/s or 10000 Mbit/s. The Ethernet network features high reliability and easy maintaining.

13.7 F

fast Ethernet	Any network that supports transmission rate of 100 Mbit/s. The Fast Ethernet is 10 times faster than 10BaseT, and inherits frame format, MAC addressing scheme, MTU, and so on. Fast Ethernet is extended from the IEEE802.3 standard, and it uses the following three types of transmission media: 100BASE-T4 (4 pairs of phone twisted-pair cables), 100BASE-TX (2 pairs of data twisted-pair cables), and 100BASE-FX (2-core optical fibers).
fault location	A technique for fault location estimation which uses data from both ends of the transmission line and which does not require the data to be synchronized.
fault management	The fault management of Ethernet OAM includes the connectivity detection of the network, the location and the confirmation of failures, protection switching triggered by the cooperation with automatic protection switching protocol.
fax call	A call that a user initiates by dialing a specified phone number on a fax machine. After the call is connected, the call center platform converts the content to be faxed into an email and sends the email to an agent. Then the agent provides services for the user by replying to the email.

FE	See fast Ethernet
FIFO	See first in first out
filter	The filter is used to filter the matched logs and have the unmatched one left.
firewall	A combination of a series of components set between different networks or network security domains. By monitoring, limiting, and changing the data traffic across the firewall, it masks the interior information, structure and running state of the network as much as possible to protect the network security.
firmware	The programmable software part in a hardware component. A firmware is a part of hardware, but is scalable as software.
first in first out	A stack management mechanism. The first saved data is first read and invoked.
flow	An aggregation of packets that have the same characteristics. On the network management system or NE software, flow is a group of classification rules. On boards, it is a group of packets that have the same quality of service (QoS) operation.
forwarded to number	A destination number set by a subscriber who has subscribed to the call forwarding service, that is, a number to which an incoming call is forwarded.
frame	A frame, starting with a header, is a string of bytes with a specified length. Frame length is represented by the sampling circle or the total number of bytes sampled during a circle. A header comprises one or a number of bytes with pre-specified values. In other words, a header is a code segment that reflects the distribution (diagram) of the elements pre-specified by the sending and receiving parties.
frequency	The measure of how often a periodic event occurs, such as a signal going through a complete cycle.
field replaceable unit	A unit that can function as a circuit board, part, or component of an electronic device. It can be quickly and easily removed from a personal computer or other electronic devices. If an FRU becomes faulty, users can replace it with a new one instead of sending the entire product or system for maintenance.
FTP server	A file server that uses the File Transfer Protocol (FTP) to permit users to upload or download files through the Internet or any other TCP/IP network.
FTPS	See FTP server
full-duplex	A full-duplex, or sometimes double-duplex system, allows communication in both directions, and, unlike half-duplex, allows this to happen simultaneously. Land-line telephone networks are full-duplex, since they allow both callers to speak and be heard at the same time. A good analogy for a full-duplex system would be a two-lane road with one lane for each direction.
function module	A set of code to perform a particular task with inputs to be passed. The Function module enables you to write your own script to control

what the module does.

13.8 G

G.711	Audio codec standard (A-law or u-law) that uses pulse code modulation (PCM). Its data rate is 64 kbit/s.
G.722	Audio codec standard that uses adaptive differential pulse-code modulation (ADPCM). Its data rate is 48 kbit/s, 56 kbit/s, or 64 kbit/s.
gain	The ratio between the optical power from the input optical interface of the optical amplifier and the optical power from the output optical interface of the jumper fiber, which expressed in dB.
gate	An electronic switch that is the elementary component of a digital circuit. It produces an electrical output signal that represents a binary 1 or 0 and is related to the states of one or more input signals by an operation of Boolean logic, such as AND, OR, and XOR.
gateway	A device that connects two network segments using different protocols. It is used to translate the data in the two network segments.
grounding resistance	One of the important parameters in the lightning-protection design of electric power systems. The grounding resistance of electrode decreases as large currents are injected to the electrode by electric discharges in soil.

13.9 H

half-duplex	A transmitting mode in which a half-duplex system provides for communication in both directions, but only one direction at a time (not simultaneously). Typically, once a party begins receiving a signal, it must wait for the transmitter to stop transmitting, before replying.
hammer drill	Used to drill holes. Choose different drill bits according to the depth of holes and expansion bolt models.
handshake	Sequence of messages exchanged between two or more network devices to ensure transmission synchronization.
hop	A network connection between two distant nodes. For Internet operation a hop represents a small step on the route from one main computer to another.
HSPA	High Speed Packet Access.

13.10 I

ICMP	See Internet Control Message Protocol
-------------	---

ID	identity.
IE	See Internet Explorer
IMS	See IP Multimedia Subsystem
insulation	A non-conducting material that prevents heat, sound, or electricity from passing through it.
interconnection	The connection that allows users to communicate in different networks and systems.
interface	A boundary between two systems or between two parts of the same system, defined by the specification of suitable characteristics, usually for the purpose of ensuring format, function, signal and interconnection compatibility at the boundary.
interface module	The module that accommodates the front-end host port and back-end disk port.
interference	A phenomenon resulting from the superposition of two or more coherent oscillations or waves of equal or nearly equal frequency and appearing as a variation of the resultant amplitude, in space in the form of interference patterns and in time in the form of beats.
International Telecommunication Union	A United Nations agency, one of the most important and influential recommendation bodies, responsible for recommending standards for telecommunication (ITU-T) and radio networks (ITU-R).
Internet Control Message Protocol	A network-layer (ISO/OSI level 3) Internet protocol that provides error correction and other information relevant to IP packet processing. For example, it can let the IP software on one machine inform another machine about an unreachable destination. See also communications protocol, IP, ISO/OSI reference model, packet (definition 1).
Internet Explorer	Microsoft's Web browsing software. Introduced in October 1995, the latest versions of Internet Explorer include many features that allow you to customize your experience on the Web. Internet Explorer is also available for the Macintosh and UNIX platforms.
Internet Protocol	The protocol within TCP/IP that governs the breakup of data messages into packets, the routing of the packets from sender to destination network and station, and the reassembly of the packets into the original data messages at the destination. IP runs at the internetwork layer in the TCP/IP model-equivalent to the network layer in the ISO/OSI reference model.
Internet service provider	An organization that offers users access to the Internet and related services.
interval	In mathematics, an interval is a set of real numbers with the property that any number that lies between two numbers in the set is also included in the set.
intranet	A private network based on Internet protocols such as TCP/IP but designed for information management within a company or organization.
IP	See Internet Protocol

IP Multimedia Subsystem	A standardized Next Generation Networking (NGN) architecture for telecommunications carriers who want to provide mobile and fixed multimedia services. It uses a Voice-over-IP (VoIP) implementation based on a 3rd Generation Partnership Project (3GPP) standardized implementation of Session Initiation Protocol (SIP), and runs over the standard Internet Protocol (IP). Existing phone systems (both packet-switched and circuit-switched) are supported. The aim of IMS is not only to provide new services but all the services, current and future, that the Internet provides. In this way, IMS will provide carriers and service providers with the ability to control and charge each service. In addition, users have to be able to execute all their services when roaming as well as from their home networks. To achieve these goals, IMS uses open standard IP protocols, defined by the Internet Engineering Task Force (IETF). A multimedia session between two IMS users, between an IMS user and an Internet user, or between two Internet users is established using the same protocol. The interfaces for service developers are also based on IP protocols. This is why IMS truly merges the Internet with the cellular world; it uses cellular technologies to provide ubiquitous access and Internet technologies to provide appealing services.
IPoA	Internet Protocol over ATM.
ISP	See Internet service provider
ITU	See International Telecommunication Union

13.11 L

LAN	See local area network
LAN switch	A piece of equipment used to allocate communication links in a LAN.
latency	The time it takes for the original data to go through a series of processing steps such as coding, to be transmitted through the channel, to arrive at the receiver, and to be decoded.
layer	A concept used to allow the transport network functionality to be described hierarchically as successive levels; each layer being solely concerned with the generation and transfer of its characteristic information.
layer 2 switch	A data forwarding method. In LAN, a network bridge or 802.3 Ethernet switch transmits and distributes packet data based on the MAC address. Since the MAC address is the second layer of the OSI model, this data forwarding method is called layer 2 switch.
level	An element in the dimension hierarchy structure. Levels describe the hierarchy of data from the top layer to the bottom layer. Each dimension contains levels according to the attributes of the data. For example, a time dimension contains four levels: year, quarter, month, and date.
link	1. In the topology view, a link is used to identify the physical or

logical connection between two topological nodes. 2. A network communication channel consisting of a circuit or transmission path and all related equipment between a sender and a receiver. A link is used to connect signaling points (SPs) and signaling transfer points (STPs) and transmit signaling messages.

list box	A control in Windows that enables the user to choose one option from a list of possibilities.
loading	A process of importing information from the storage device to the memory to facilitate processing (when the information is data) or execution (when the information is program).
local area network	A network formed by the computers and workstations within the coverage of a few square kilometers or within a single building. It features high speed and low error rate. Ethernet, FDDI, and Token Ring are three technologies used to implement a LAN. Current LANs are generally based on switched Ethernet or Wi-Fi technology and running at 1,000 Mbit/s (that is, 1 Gbit/s).
log	A type of file that records the system events occurring during the running of the system. The system events include the running, input/output (I/O) operations, exceptions, and security events. Logs provide a basis for the querying and maintenance of the system.
log management	A measure that is used to find illegal operations and fault reasons by querying and monitoring logs, and to protect network security by taking appropriate measures.
loop	Electricity. A closed circuit.

13.12 M

mains supply	The commercial power supply of a nation.
maintenance	The process of taking measures to ensure that a hardware, software, or database system is functioning properly and is up to date.
MAN	metropolitan area network.
mapping	A procedure by which tributaries are adapted into virtual containers at the boundary of an SDH network.
mask	A pattern of characters, bits, or bytes used to control the elimination or retention of another pattern of characters, bits, or bytes.
media information	Information about digital media content such as the artist, title, album, producer, and so forth.
media negotiation	Through it, two UEs reach an agreement on media combinations used by a session and coding schemes used by media.
medium	A physical medium for storing computer information. A medium is used for data duplication and keeping the data for some time. Original data can be obtained from a medium.
microwave	The portion of the electromagnetic spectrum with much longer

wavelengths than infrared radiation, typically above about 1 mm.

middleware	<p>1. Software that sits between two or more types of software and translates information between them. Middleware can cover a broad spectrum of software and generally sits between an application and an operating system, a network operating system, or a database management system. Examples of middleware include CORBA and other object broker programs and network control programs. 2. Software that provides a common application programming interface (API). Applications written using that API will run in the same computer systems as the middleware. An example of this type of middleware is ODBC, which has a common API for many types of databases. See also application programming interface, ODBC. 3. Software development tools that enable users to create simple programs by selecting existing services and linking them with a scripting language.</p>
mode	<p>One solution of Maxwell's equations, representing an electromagnetic field in a certain space domain and belonging to a family of independent solutions defined by specified boundary conditions.</p>
modem	<p>A device or program that enables a computer to transmit data over, for example, telephone or cable lines. Computer information is stored digitally, whereas information transmitted over telephone lines is transmitted in the form of analog waves. A modem converts between these two forms.</p>
modulated signal	<p>An oscillation or wave produced by modulation.</p>
modulation	<p>A process by which a quantity which characterizes an oscillation or wave follows the variations of a signal or of another oscillation or wave.</p>
module	<p>A set of program statements (the combination of functional codes and data structure) that are executed on hardware and separately named to implement certain functions independently.</p>
multicast	<p>A process of transmitting packets of data from one source to many destinations. The destination address of the multicast packet uses Class D address, that is, the IP address ranges from 224.0.0.0 to 239.255.255.255. Each multicast address represents a multicast group rather than a host.</p>
multicast group	<p>A set of members participating in the packet multicast service. The multicast group is defined by a rule (or set of rules) which identifies a collection of members implicitly or explicitly. This rule may associate members for the purpose of participating in a call, or may associate members who do not participate in data transfer but participate in management, security, control, and accounting for the multicast group.</p>
MUX	<p>multiplexer.</p>

13.13 N

narrowband	Communication services that transmit over TDM timeslot. The PSTN is normally a narrowband network. A communication channel whose transmission rate is lower than 2 Mbit/s is usually considered to be narrowband.
NAT	See network address translation
NAT traversal	For the general datagram, the NAT device or firewall transforms only the IP, TCP or UDP header. For application-layer protocols such as H.323, SIP, MGCP and H.248, the IP addresses contained in the signaling protocols are private addresses. The private addresses carried in user signaling messages cannot be replaced, but the call addresses of media streams are negotiated dynamically by signaling protocols. Therefore, the correct media channel cannot be established. NAT traversal can identify and change the message contents of multiple signaling protocols, and pre-assign the UDP ports of media streams.
network address translation	An IETF standard that allows an organization to present itself to the Internet with far fewer IP addresses than there are nodes on its internal network. The NAT technology, which is implemented in a router, firewall or PC, converts private IP addresses (such as in the 192.168.0.0 range) of the machine on the internal private network to one or more public IP addresses for the Internet. It changes the packet headers to the new address and keeps track of them via internal tables that it builds. When packets come back from the Internet, NAT uses the tables to perform the reverse conversion to the IP address of the client machine.
network jitter	A sound adjustment method. A higher network jitter contributes to a better connectivity of sounds. In a conference, the lip movements and voice of a speaker may not be synchronous. To solve this problem, users can adjust the network jitter value.
network layer	Layer 3 of the seven-layer OSI model of computer networking. The network layer provides routing and addressing so that two terminal systems are interconnected. In addition, the network layer provides congestion control and traffic control. In the TCP/IP protocol suite, the functions of the network layer are specified and implemented by IP protocols. Therefore, the network layer is also called IP layer.
network port	Numbers which are recognized by Internet and other network protocols, enabling the computer to interact with others.
network segment	A part of an Ethernet or other network, on which all message traffic is common to all nodes, that is, it is broadcast from one node on the segment and received by all others.
network service	A service that needs to be enabled at the network layer and maintained as a basic service.
Network Time Protocol	The Network Time Protocol (NTP) defines the time synchronization mechanism. It synchronizes the time between the distributed time server and the client.

network topology	The configuration or layout of a network formed by the connections between devices on a LAN (local area network) or between two or more LANs.
next generation network	A packet-based network aimed to address requirement of various services. It adopts an integrated and open network framework. In NGN, services are separated from call control; call control is separated from bearer. In this way, services are independent of network. NGN can provide various services, such as voice services, data services, multimedia services or the integration of several services.
next hop	The next router to which a packet is sent from any given router as it traverses a network on its journey to its final destination.
NGN	See next generation network
node	A managed device in the network. For a device with a single frame, one node stands for one device. For a device with multiple frames, one node stands for one frame of the device. Therefore, a node does not always mean a device.
NTP	See Network Time Protocol
NTP client	The bottom-level device in the time synchronization network. An NTP client obtains time from its superior NTP server and it does not provide the time synchronization service. Relative to the top-level NTP server, the medium NTP server sometimes is called an NTP client.

13.14 O

object-oriented	Of, pertaining to, or being a system or language that supports the use of objects.
operating environment	In computing, an operating environment is the environment in which users run application software, whether by a command-line interface (such as in MS-DOS or the Unix shell) or a graphical user interface (such as in the Macintosh operating system or a web browser).
option	An option right that the holder obtains by paying the cost. The holder can share the right, but does not shoulder the obligation in the specified time.
organizationally unique identifier	A 3-octet IEEE assigned identifier that can be used to generate Universal LAN MAC addresses and Protocol Identifiers per [IEEE802] for use in Local and Metropolitan Area Network applications.
originating address	Address of the node which has initiated the relationship with the remote application transport(APM) user application.
OUI	See organizationally unique identifier
outbound	For the routers that support the NetStream feature, outbound means the data transmitted from the router to the external links.

overwrite Text-entry mode in which newly typed characters replace existing characters under or to the left of the cursor insertion point.

13.15 P

packet An information block identified by a label at layer 3 of the OSI reference model.

packet loss compensation A technology of compensating packets according to an appropriate algorithm if packets are lost in the transmission.

panel A part used to ensure proper airflow within a shelf and to ensure electromagnetic compatibility (EMC) by sealing up the slots on the shelf. It is an external part of a board and is vertically placed with the printed circuit board (PCB). It includes the ejector lever, indicator, and port.

PAP See [Password Authentication Protocol](#)

parameter A value or reference passed to a function, command, or program that serves as input or to control actions. The value is supplied by a user or by another program or process.

Password Authentication Protocol A method of verifying the identity of a user who attempts to log in to a PPP server. This protocol is adopted when a stricter authentication protocol, such as CHAP, cannot take effect, or the user name and password submitted by the user for authentication must be forwarded to other programs without being encrypted.

path A performance resource object defined in the network management system. The left end of a path is a device node whose port needs to be specified and the right end of a path is a certain IP address which can be configured by the user. By defining a path in the network management system, a user can test the performance of a network path between a device port and an IP address. The tested performance may be the path delay, packet loss ratio or other aspects.

PC See [personal computer](#)

peer end Router or device that participates as an endpoint.

permanent virtual circuit A permanent logical connection between two nodes on a packet-switching network. The PVC appears as a dedicated line to the nodes, but the data can be transmitted on a common carrier.

personal computer A computer used by an individual at a time in a business, a school, or at home.

ping A method used to test whether a device in the IP network is reachable according to the sent ICMP Echo messages and received response messages.

point to point A type of service in which data is sent from a single network termination to another network termination.

Point-to-Point A protocol on the data link layer, provides point-to-point transmission and encapsulates data packets on the network layer. It is located in

Protocol	layer 2 of the IP protocol stack.
Point-to-Point Protocol over Ethernet	PPPoE, point-to-point protocol over Ethernet, is a network protocol for encapsulating PPP frames in Ethernet frames. It is used mainly with DSL services. It offers standard PPP features such as authentication, encryption, and compression.
pointer	An indicator whose value defines the frame offset of a virtual container with respect to the frame reference of the transport entity on which it is supported.
port	1. Of a device or network, a point of access where signals may be inserted or extracted, or where the device or network variables may be observed or measured. 2. In a communications network, a point at which signals can enter or leave the network en
power adapter	A power supply for just about every electronic device on the market. Also called an "AC adapter" or a "charger" if used to recharge a battery, it plugs into the wall and converts AC current to a single DC voltage in most cases. There are also adapters that output a different AC voltage. Laptops have both an external power adapter, also called a "power brick", and an internal power supply. If an external power adapter is not used with an electronic product such as a desktop computer, the DC current is created in a power supply inside the unit.
power module	A module that provides power supply to operate other boards or modules.
power up	To start up a computer; to begin a cold boot procedure; to turn on the power
power-off survival	A feature that allows part of the analog phone users to make calls by connecting to the PSTN through analog trunks in the case that the device is powered off. This feature is available when there are analog trunks connecting the SoftCo device and the PSTN.
PPP	See Point-to-Point Protocol
PPPoA	Point-to-Point Protocol over ATM.
PPPoE	See Point-to-Point Protocol over Ethernet
PPPoEoA	Point-to-Point Protocol over Ethernet over ATM.
pre-shared key	A pre-shared key is an alpha-numeric string of 8 - 80 characters. A pre-shared key can be used instead of certificates to authenticate both parties during IKE Phase 1 negotiations. The pre-shared key is entered on both of the communicating devices.
preference	Preference is an extended tariff mode. It is the balance obtained through calculating the two tariff modes.
prefix	The attribute of the called party. Prefix, also called call prefix, refers to the prefix of the called number. Prefix is a key factor for defining services related to a call. The prefixes of different subscribers and trunk groups can be the same. Therefore, a call service is related to the prefix and the call source.
priority queue	An abstract data type in computer programming that supports the following three operations: 1. Add an element to the queue with an

associated priority. 2. Remove the element from the queue that has the highest priority, and return it. 3. (optional) Look at the element with highest priority without removing it.

process	A service process in which all or part of the activities are supported or automatically performed by the computer, for example, the service request process and leave application process.
product documentation	Documents that are delivered to customers along with Huawei products. Product documentation includes the solution description, system description, product description, installation manuals, and reference manuals. These documents provide guidance for customers to understand, operate, and maintain Huawei products.
protocol	A formal set of conventions and rules governing the formatting and sequencing of message exchange between two communicating systems.
protocol stack	A set of related communications protocols that operate together and, as a group, address communication at some or all of the seven layers of the OSI reference model.
protocol type	A multiplexing field that defines the type of packet in which only a single field appears in the packet. In contrast, an SAP type of multiplexing field has a source SAP and a destination SAP. The two SAP values are numerically unrelated.
proxy	Computer programs that forward protocols between clients and servers. They are like clients at the server end and are like servers at the client end.
proxy server	A server located on a network between client software, such as a Web browser, and another server. It intercepts all requests to the server to determine whether it can fulfill them itself. If not, it forwards the request to another server.
PUK code	The key to decode the PIN code. It is a string of 8 characters. User does not know it.
PVC	See permanent virtual circuit

13.16 Q

QoS	See quality of service
quality of service	A commonly-used performance indicator of a telecommunication system or channel. Depending on the specific system and service, it may relate to jitter, delay, packet loss ratio, bit error ratio, and signal-to-noise ratio. It functions to measure the quality of the transmission system and the effectiveness of the services, as well as the capability of a service provider to meet the demands of users.
Quick Start	Something that helps you to quickly get familiar with the features and the user interface.
quintuple	A parameter set used to check whether the network is legal during the IMS AKA authentication. The quintuple contains the following

parameters: 1. RAND: A pseudo-random number generated by the random number generator. The network provides RAND to the User Equipment (UE). The UE uses RAND to calculate XRES, IK and CK. 2. XRES: A value used for comparison with SRES in the authentication response message sent by the UE. It checks whether the UE can pass the authentication handled by the network. 3. CK: IMS AKA ciphering key. 4. IK: IMS AKA integrity key. 5. AUTN: A parameter used by the UE to perform the authentication for the network.

13.17 R

radio frequency	A type of electric current in the wireless network using AC antennas to create an electromagnetic field. It is the abbreviation of high-frequency AC electromagnetic wave. The AC with the frequency lower than 1 kHz is called low-frequency current. The AC with frequency higher than 10 kHz is called high-frequency current. RF can be classified into such high-frequency current.
random	Specifically, a reference to an arbitrary or unpredictable situation or event.
receive channel	The channel used for receiving user's information and which is relative to a given end of a circuit.
record file	A text file used to exchange and save data. A record file expresses the data content in text format. Each record serves as a line in the text. A record can contain multiple fields. Fields are separated by delimiters or defined in fixed length mode. A file can contain only records of the same type.
recovery time	The time period between a physical interruption within the broadcasting chain and the achievement of full functionality.
redirection number	A forwarding destination number set by a subscriber who has subscribed to the call forwarding service, that is, a number to which an incoming call to the subscriber is forwarded.
redundancy	1. The scheme to add more than one channel, elements or parts that have the same functions with the counterparts in the system or device at a critical place. When a fault occurs, the system or device can work well, and the reliability is then improved. 2. In the transmission of data, the excess of transmitted message symbols over that required to convey the essential information in a noise-free circuit. Note: Redundancy may be introduced intentionally (as in the case of error detection or correction codes)
refresh	Refresh is for status, while update for database.
registrar	A server that accepts REGISTER requests. A registrar is typically combined with a proxy or redirect server.
relative path	A designation of the location of a file that is related with the current working directory, as opposed to an absolute or full path which gives the exact location.

relay	An electronic control device that has a control system and a system to be controlled. The relay of the telepresence system is used to control the power of telepresence equipment and is controlled by the telepresence host.
release	To obtain a trouble ticket (TT) from the to-be-processed area of a service agent and put it to the TT pool of a skill group.
reliability	Reliability provides a measure of how often positioning requests that satisfy QoS requirements are successful.
request message	It is a SIP message sent from a client to a server for invoking a particular operation.
response message	It is used to respond to request messages, thus indicating the success or failure status of the call.
restore	Replace the damaged data with the backup data to restore the system.
RF	See radio frequency
RFC	Request For Comments.
RJ-11	A most commonly used type of phone interface registered with the Federal Communications Commission (FCC). An RJ-11 connector has six pins but only two or four are used in general. It is connected to an untwisted cable.
router	A device on the network layer that selects routes in the network. The router selects the optimal route according to the destination address of the received packet through a network and forwards the packet to the next router. The last router is responsible for sending the packet to the destination host. Can be used to connect a LAN to a LAN, a WAN to a WAN, or a LAN to the Internet.
routing protocol	A formula used by routers to determine the appropriate path onto which data are forwarded.
routing table	A table that stores and updates the locations (addresses) of network devices. Routers regularly share routing table information to be up to date. A router relies on the destination address and on the information in the table that gives the possible routes--in hops or in number of jumps--between itself, intervening routers, and the destination. Routing tables are updated frequently as new information is available.
RX	The receiving end of the interface that signals pass through.

13.18 S

scheduling algorithm	An algorithm that governs the proper timing of a sequence of events in an operating system or application. For example, an effective motion graphics scheduling algorithm would be able to retrieve the graphic objects, process them, and display them without causing stutter or disruptions.
scheduling	A mechanism used to avoid competition among packets for network

mechanism	resources when congestion occurs.
section	The portion of a SONET transmission facility, including terminating points, between (i) a terminal network element and a regenerator or (ii) two regenerators. A terminating point is the point after signal regeneration at which performance monitoring is (or may be) done.
sequence number	An identifying number used to designate a block of data, an operation, or part of an operation.
serial port	An input/output location (channel) that sends and receives data to and from a computer's CPU or a communications device one bit at a time. Serial ports are used for serial data communication and as interfaces with some peripheral devices, such as mice and printers.
server	1. On a local area network, a computer running administrative software that controls access to the network and its resources, such as printers and disk drives, and provides resources to computers functioning as workstations on the network. 2. On the Internet or other network, a computer or program that responds to commands from a client. For example, a file server may contain an archive of data or program files; when a client submits a request for a file, the server transfers a copy of the file to the client. 3. A network device that provides services to network users by managing shared resources, often used in the context of a client-server architecture for a LAN.
service and support	Product support, technical assistance, sales support, phone or computer-based configuration assistance, software upgrade help lines, and traditional help desk services.
service capability	The combination of human performance, business process, and technology that collectively represent an organization's ability to create value through a distinct part of its operation
service data	The user and/or network information required for the normal functioning of services.
service flow	An MAC-layer-based unidirectional transmission service. It is used to transmit data packets, and is characterized by a set of QoS parameters, such as latency, jitter, and throughput.
service processing	The execution of service control and basic call processing functions to provide a service.
session timer	A mechanism that is used after establishment of the session. It enables the UE to periodically originate REINVITE or UPDATE to ensure that the session is active.
shared key authentication	Shared key authentication requires that the STA and the AP be configured with the same shared key. The process of shared key authentication is as follows: A STA transmits an authentication request to an AP, and the AP randomly generates a "challenge text" (a character string) and transmits it to the STA. The STA then copies the received "challenge text" to a new message, and transmits the message encrypted with the shared key to the AP. Then, the AP decrypts the message by using the shared key, and compares the decrypted character string with the character string that has been provided to the STA. If the character strings are the same, it indicates that the STA has the same shared key with the AP, that is, the STA

	passes the shared key authentication; otherwise, the STA fails to pass the shared key authentication.
sideband	In electronic signal transmission, a sideband is the portion of a modulated carrier wave that is either above or below the basic (baseband) signal. The portion above the baseband signal is the upper sideband; the portion below is the lower sideband. In regular amplitude modulation (AM) transmission, both sidebands are used to carry a message. In some forms of transmission, one sideband is removed (single-sideband transmission) or a portion of one sideband is removed.
signal	1. In electronics, a signal is an electric current or electromagnetic field used to convey data from one place to another. 2. In some information technology contexts, a signal is simply "that which is sent or received," therefore including both the carrier and the signal. 3. In telephone, signals are special data used for setting up and controlling the communication.
signal tone	A digital announcement played at a specific frequency and cadence ratio, and represents the specific meanings. The dial tone, busy tone, ring back tone, test code tone, and mute tone are signal tones.
signaling	The information exchange concerning the establishment and control of a telecommunication circuit and the management of the network.
silent time	A set time threshold when a host stops accessing a designated storage area.
site	A group of IP systems with IP connectivity, which can be achieved independent of SP networks.
SOAP	Simple Object Access Protocol.
softswitch	A device that provides call control and connection control for real-time services. As main control of the NGN, softswitches separate the services from the call control and the call control from the bearer, and adopt the application programming interface (API) and standard protocols. This makes it easy for network carriers to develop new services and realize new features.
SOHO	small office home office.
space	The place where no character or image is displayed on the computer monitor or the paper.
specifications	Documents requirements for a process service system or product.
splitter	Filter that separates the high frequency signals (ADSL) from the voiceband signals; (frequently called POTS splitter even though the voiceband signals may comprise more than POTS).
startup	The process of starting or resetting a computer.
static route	A route that cannot adapt to the change of network topology. Operators must configure it manually. When a network topology is simple, the network can work in the normal state if only the static route is configured. It can improve network performance and ensure bandwidth for important applications. Its disadvantage is as follows: When a network is faulty or the topology changes, the static route

	does not change automatically. It must be changed by the operators.
station	A terminal, such as a laptop or a PC, with a wireless network interface card (NIC).
stream	1. A succession of data elements made available over time. 2. Stream refers to the directional logical path from one end to another end in an SCTP link.
sub-network	Sub-network is the logical entity in the transmission network and comprises a group of network management objects. The network that consists of a group of interconnected or correlated NEs, according to different functions. For example, protection subnet, clock subnet and so on. A sub-network can contain NEs and other sub-networks. Generally, a sub-network is used to contain the devices which are located in adjacent regions and closely related with one another, and it is indicated with a sub-network icon on a topological view. The U2000 supports multilevels of sub-networks. A sub-network planning can better the organization of a network view. On the one hand, the view space can be saved, on the other hand, it helps the network management personnel focus on the devices under their management.
subnet	A large network can be divided into a number of smaller networks according to a rule, for example, according to different districts. This facilitates the management of the large network. In the topology view, this type of a smaller network is termed subnet.
subnet mask	The technique used by the IP protocol to determine which network segment packets are destined for. The subnet mask is a binary pattern that is stored in the client machine, server or router and is matched with the IP address.
subscriber number	The number to be dialed or called to reach a telephone subscriber in the same local network or numbering area.
subsystem	An element in a hierarchical division or an open system that interacts directly with elements in the next higher division or the next lower division of that open system.
supplementary service	A service which modifies or supplements a basic telecommunication service. A supplementary service must be offered together with or in association with a basic telecommunication service. It includes: 1. Call forwarding services 2. Call barring services 3. Line identification services 4. Call completion services 5. Multiparty service 6. Unstructured supplementary service data 7. Closed user group service
supported connections	Connections that can be used.
swell fixture	A small cylindrical or tapered pin, as of wood, used to fasten things or plug a hole.
switch unit	As a critical component of the main control unit, the switch unit is also called the switch module (or switch network), with the functions of switching, allocation, scheduling, and control for packets between interface boards. Generally, the switch unit uses ASIC chips of high performance to provide line rate forwarding for packets.
synchronize	To synchronize parameter settings on devices to the database of the

network management system.

system bus A mechanism of the computer system to achieve connections between devices. It is characterized by the signal transmission between two devices on the bus. One device sends commands and data and the other device receives commands and data. Only one transfer can be operated on the bus at any time. Transfer requests of each device are ranked according to their priorities

13.19 T

TCP See [Transmission Control Protocol](#)

telecommunication 1. Communication by wire, radio, optical or other electromagnetic systems. 2. Any transmission, emission or reception of signs, signals, writing images and sounds or intelligence of any nature by wire, radio, optical or other electromagnetic systems.

Telnet Standard terminal emulation protocol in the TCP/IP protocol stack. Telnet is used for remote terminal connection, enabling users to log in to remote systems and use resources as if they were connected to a local system. Telnet is defined in RFC 854.

terminal A device that converts voice, sound, text, image, table, data and video from physical display to electronic signals or from electronic signals to physical display. A terminal generates and sends signals (such as telecommunications circuit setup or release) that maintain the normal running state of the telecommunications network, and it receives the call signals of telecommunications switch and transmission.

three-way calling A service that allows a subscriber to add a third party to an activated two-party call so that all the three parties can communicate in a three-way call.

time sharing A mode of operation of a data processing system that provides for the interleaving in time of two or more processes in one processor.

Time Synchronization Also called the moment synchronization, time synchronization means that the synchronization of the absolute time, which requires that the starting time of the signals keeps consistent with the UTC time.

time zone A division of the earth's surface, usually extending across 15 °of longitude devised such that the standard time is the time at a meridian at the center of the zone.

timeout It refers to that an event is expected in a certain time. An event that indicates that a predetermined amount of time has elapsed without some other expected event taking place.

timer Symbolic representation for a timer object (for example, a timer object may have a primitive designated as T-Start Request). Various MAC entities utilize timer entities that provide triggers for certain MAC state transitions.

trace	Find out or describe how something started or developed.
track	To restore a trouble ticket (TT) by a service agent after the TT is allocated to but not processed in the next stage.
traffic policing	It is a scheme that supervises the specific traffic entering the communication devices. By policing the speed of traffic that enters the network, it "punishes" the traffic out of the threshold, so the traffic going into network is limited to a reasonable range, protecting the network resources and the interests of the carriers.
transfer mode	A mode in which the AH or ESP is inserted behind the IP header but ahead all transport layer protocols.
transmission	The transfer of information from one point to one or more other points by means of signals. Notes: 1. Transmission can be effected directly or indirectly, with or without intermediate storage. 2. The use of the English word "transmission" in the sense of "emission" in radiocommunication and of "sending" is deprecated.
Transmission Control Protocol	The protocol within TCP/IP that governs the breakup of data messages into packets to be sent using Internet Protocol (IP), and the reassembly and verification of the complete messages from packets received by IP. A connection-oriented, reliable protocol (reliable in the sense of ensuring error-free delivery), TCP corresponds to the transport layer in the ISO/OSI reference model.
transmission performance	The reproducibility of a signal input to a telecommunications network under given conditions. The given conditions may include the effect of propagation performance where applicable.
transport network layer	transport network layer, is defined as [G. 805] a topological component solely concerned with the generation and transfer of characteristic information.
troubleshooting	Troubleshooting is a form of problem solving. It is the systematic search for the source of a problem so that it can be solved.
TX	The transmitting end of the interface that signals pass through.

13.20 U

UDP	See User Datagram Protocol
unlock	To free the locked goods so that they can be sold consumed or transferred between departments.
upstream	In an access network, where there is a clear indication in each deployment as to which end of a link is closer to a subscriber, transmission toward the subscriber end of the link.
User Datagram Protocol	A TCP/IP standard protocol that allows an application program on one device to send a datagram to an application program on another. User Datagram Protocol (UDP) uses IP to deliver datagrams. UDP provides application programs with the unreliable connectionless packet delivery service. UDP messages can be lost, duplicated,

delayed, or delivered out of order. UDP is used to try to transmit the data packet, that is, the destination device does not actively confirm whether the correct data packet is received.

13.21 V

VAD	See voice activity detection
video on demand	An interactive video service system through which you can demand desired programs at any time. VoD is a communication technology developed based on computer, telecommunication, and television technologies.
virtual circuit	A channel or circuit established between two points on an ATM /a network. Virtual circuits can be Permanent Virtual Circuits (PVCs) or Switched Virtual Circuits (SVCs).
VoD	See video on demand
voice activity detection	An algorithm used in speech processing wherein, the presence or absence of human speech is detected from the audio samples. The main uses of VAD are in speech coding and speech recognition. A VAD may not just indicate the presence or absence of speech, but also whether the speech is voiced or unvoiced, sustained or early, and so on.
voice file	Various voice materials recorded or edited by users, for example, dial tone, busy tone, ringing tone, and intelligence tone. These voice materials generally require an analog-to-digital conversion to form a voice file in PCM stream format.
voice mail service	A value-added service, when a service subscriber misses a call due to the reason such as power off or busy, the calling party can leave a message to the service subscriber, and then the system notifies the service subscriber of the missed call by sending a short message (or a multimedia message, Email).
voice mailbox	A new communications service that allows the voice data to be converted into digital data and stored on a server, and then the user can obtain the data stored on the server anytime at any place by using a phone or by other means.
voice message	Voice Message refers to a message that could be sent to a destination using voice media. Voice itself could be 'packaged' and sent through the IP backbone so that it reaches its marked 'address'. In a technical sense, the process of sending 'voice packets
volt	Basic unit of electrical potential. One volt is the force required to send one ampere of electrical current through a resistance of one ohm.

13.22 W

WAN	See wide area network
------------	---------------------------------------

web	A set of interlinked documents in a hypertext system.
wide area network	A network composed of computers which are far away from each other which are physically connected through specific protocols. WAN covers a broad area, such as a province, a state or even a country.
wireless fidelity	A short-distant wireless transmission technology. It enables wireless access to the Internet within a range of hundreds of feet wide.
wireless local area network	A hybrid of the computer network and the wireless communication technology. It uses wireless multiple address channel as transmission media and carries out data interaction through electromagnetic wave to implement the functions of the traditional LAN.
wireless terminal	A general term used for any mobile station, mobile terminal, personal station or personal terminal, with which non-fixed access to the network is used.
WLAN	See wireless local area network

13.23 Z

zone	The collection of all terminals, gateways, and Multipoint Control Units (MCUs) managed by a single gatekeeper. A zone has only one gatekeeper. A zone is independent from the network topology and can consist of multiple network segments connected using routing equipment.
-------------	--