

- Step 1** User A presses the hook flash button and dials service prefixes *34# as prompted. To change the service prefix, see [Changing Service Prefixes](#).
- Step 2** The system plays an announcement, indicating that the malicious call is recorded successfully. If user A wants to continue the call, press the hook flash button again.

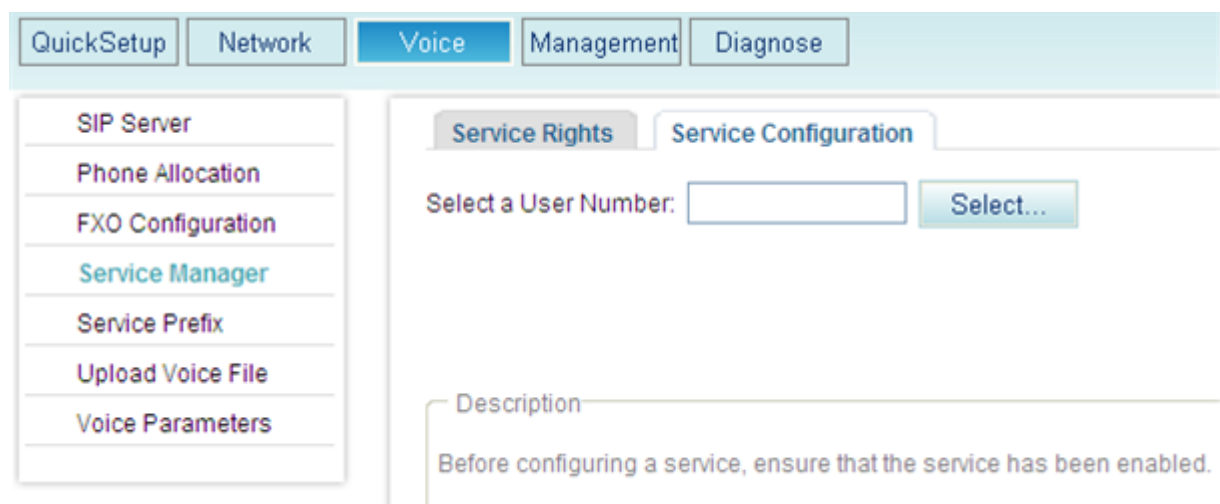
----End

View, download, and delete a malicious call.

- Step 1** On the web management system, choose **Voice > Service Manager** from the navigation tree.
- Step 2** Click the **Service Configuration** tab.

The page shown in [Figure 7-118](#) is displayed.

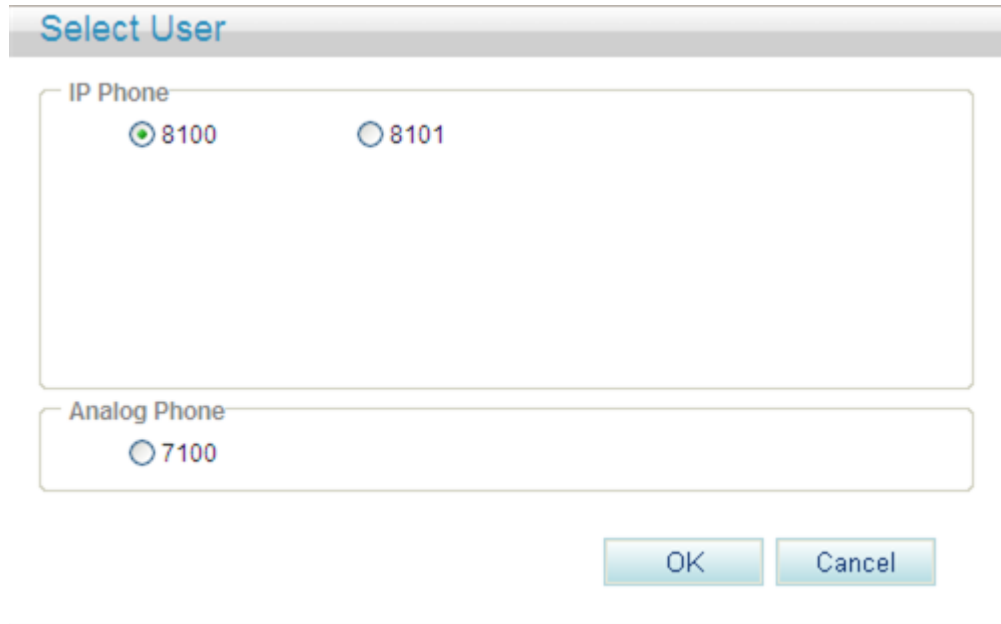
Figure 7-118 Configure Service tab page (1)

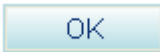


- Step 3** Click .

The page shown in [Figure 7-119](#) is displayed.

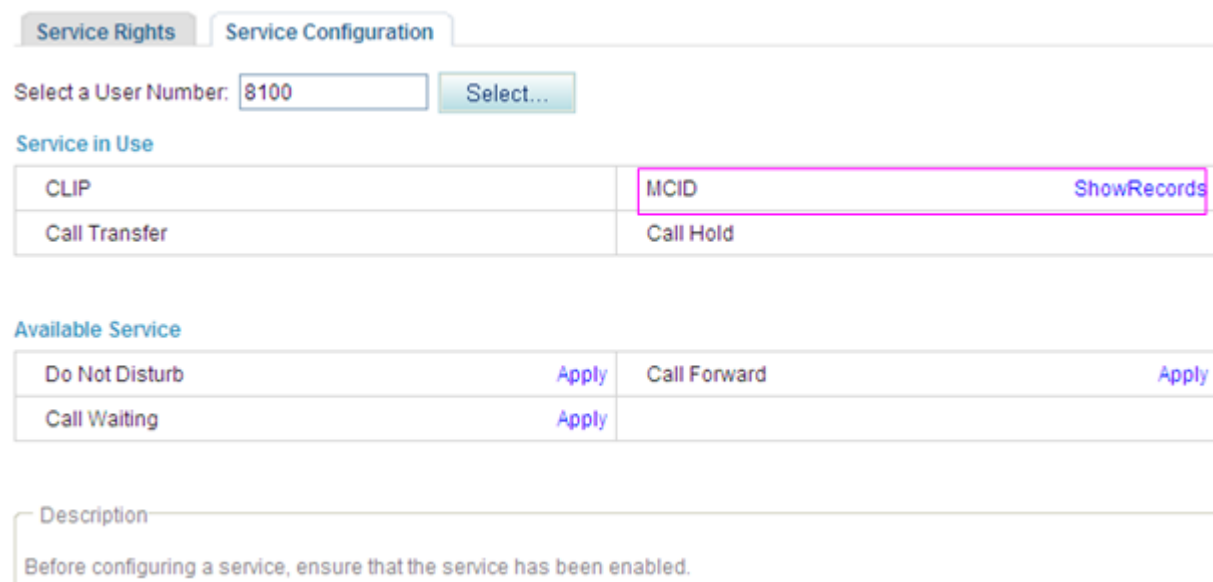
Figure 7-119 Selecting a user



Step 4 Select a user number, and click .

The page shown in [Figure 7-120](#) is displayed.

Figure 7-120 Configure Service tab page (2)

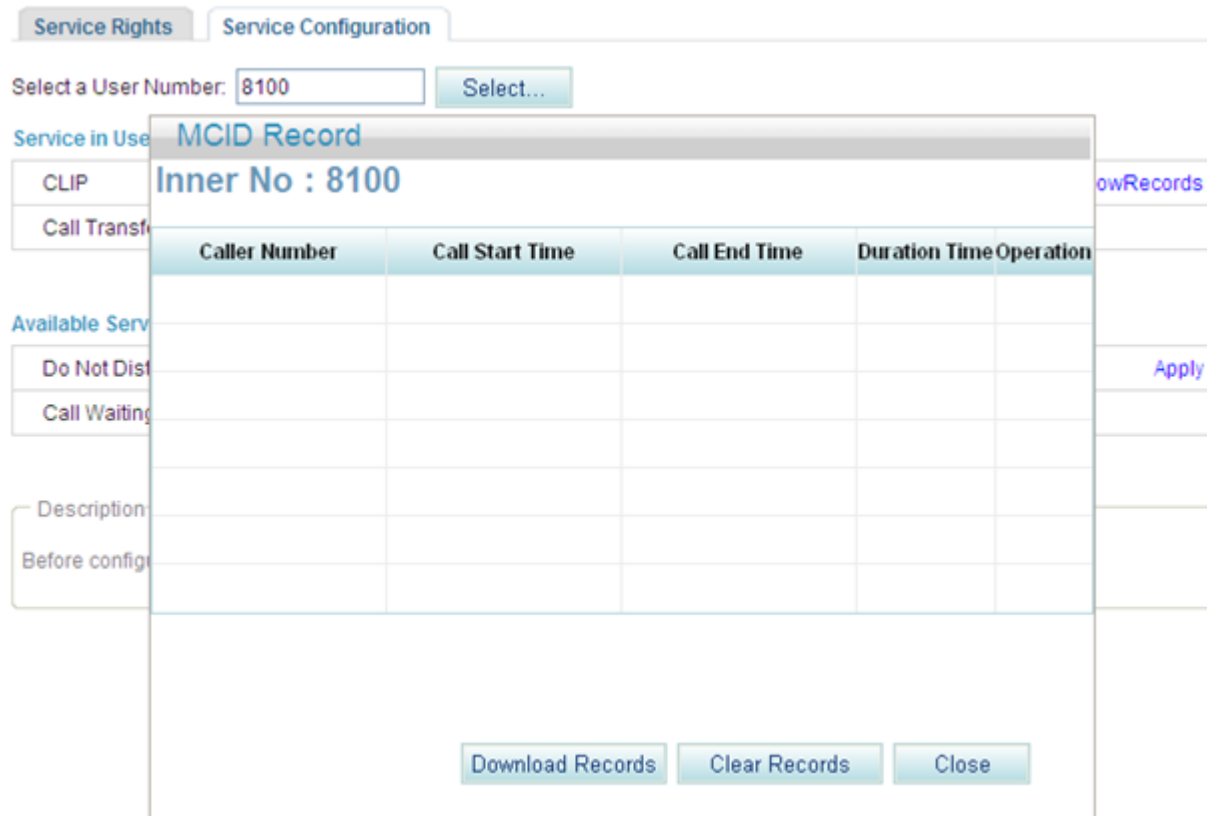


Step 5 Click **ShowRecords**.


The page shown in [Figure 7-121](#) is displayed.


You can view, download, or delete all malicious call records.

Figure 7-121 Configure Service tab page (3)



Step 6 (Optional) Click **Download Records**, and download malicious call records as prompted.

Step 7 (Optional) Click **Clear Records** to clear call malicious call records, or click  to delete a single record.

Step 8 Click  to close the page.

----End

?15. Anonymous Call Rejection

After a user enables the anonymous call rejection service, the EGW1520 will block all anonymous calls to the user.

Precautions

The anonymous call rejection service conflicts with some other services. For details, see [Service Conflicts](#).

Configuring the Service

Web mode

 **NOTE**

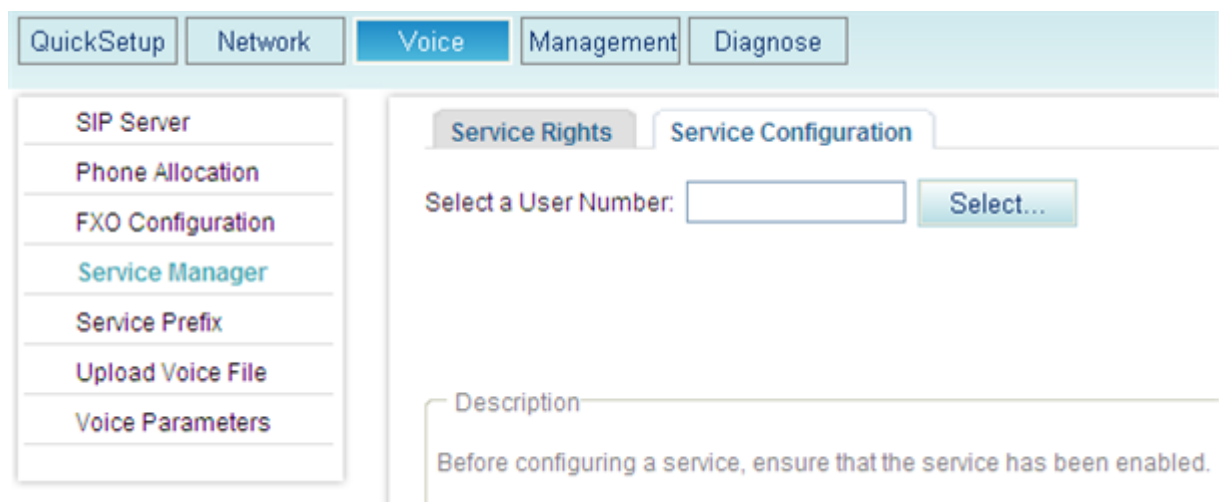
Before configuring a service, ensure that the service has been enabled. For details on how to enable voice services, see [Enabling Voice Services](#).

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

Step 2 Click the **Service Configuration** tab.

The page shown in [Figure 7-122](#) is displayed.

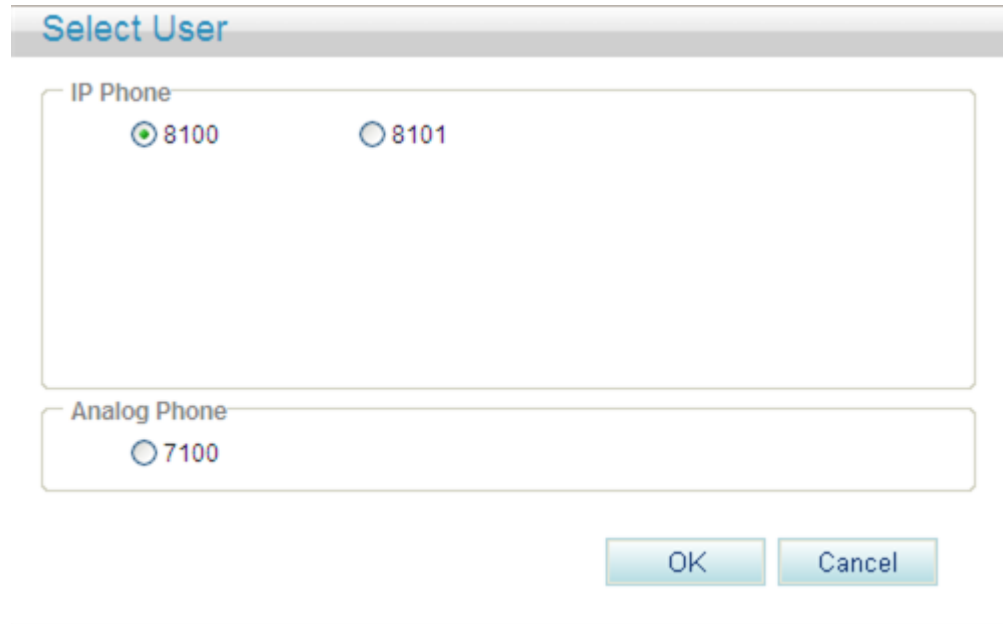
Figure 7-122 Configure Service tab page (1)



Step 3 Click  .

The page shown in [Figure 7-123](#) is displayed.

Figure 7-123 Selecting a user

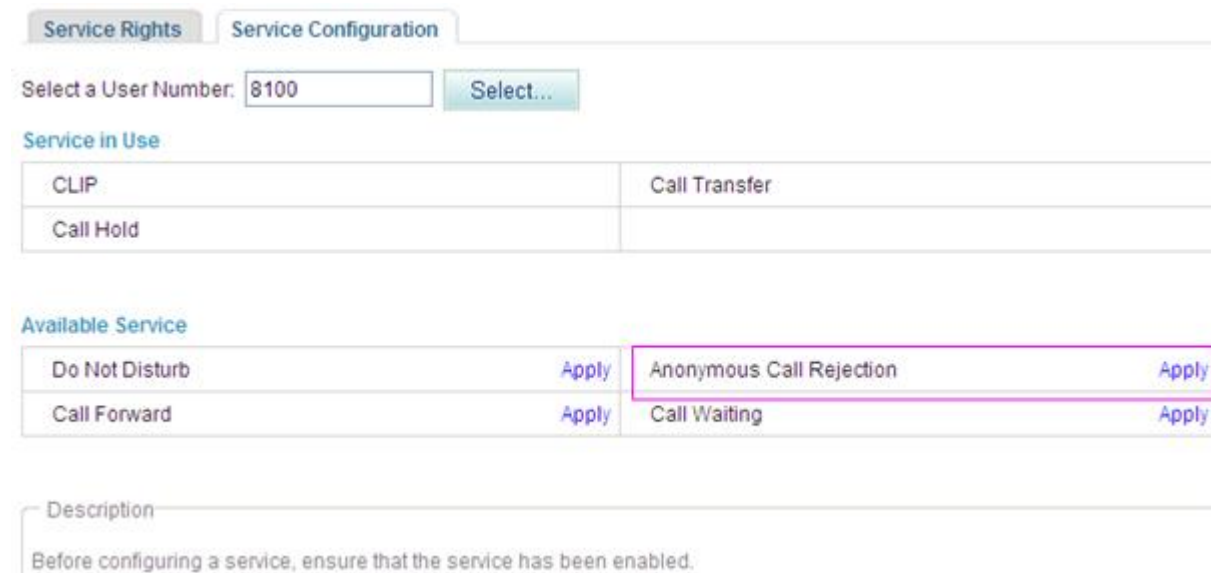


Step 4 Select a user number.

Step 5 Click .

The page shown in [Figure 7-124](#) is displayed.

Figure 7-124 Configure Service tab page (2)



Step 6 Click **Apply**.

[Figure 7-125](#) shows the configuration result.

Figure 7-125 Configuration result

The screenshot shows the 'Service Configuration' web page. At the top, there are two tabs: 'Service Rights' and 'Service Configuration'. Below the tabs, there is a 'Select a User Number' field with the value '8100' and a 'Select...' button. Underneath, the 'Service in Use' section contains a table with two rows: 'Anonymous Call Rejection' (with a 'Cancel' button) and 'Call Transfer'. Below that, the 'Available Service' section contains a table with two rows: 'Do Not Disturb' (with an 'Apply' button) and 'Call Forward' (with an 'Apply' button). At the bottom, there is a 'Description' box with the text: 'Before configuring a service, ensure that the service has been enabled.'

----End

Service prefix dialing mode

In addition to the preceding web mode, you can also dial a prefix to configure the service. For example, pick up the phone and dial default service prefix ***41#**. To change the service prefix, see [Changing Service Prefixes](#).

Using the Service

Assume that user A has enabled and configured the anonymous call rejection service and that user B is an anonymous user (for example, user B enables the CLIR service). User B's calls to user A will be blocked.

Canceling the Service

Web mode

Click **Cancel** on the **Service Configuration** tab page, as shown in [Figure 7-126](#).

Figure 7-126 Canceling the service

The screenshot shows a web interface for service configuration. At the top, there are two tabs: 'Service Rights' and 'Service Configuration'. Below the tabs, there is a field 'Select a User Number:' with the value '8100' and a 'Select...' button. The main content is divided into two sections: 'Service in Use' and 'Available Service'. The 'Service in Use' section contains a table with two rows: 'Anonymous Call Rejection' with a 'Cancel' button, and 'Call Transfer'. The 'Available Service' section contains a table with two rows: 'Do Not Disturb' with an 'Apply' button, and 'Call Forward' with an 'Apply' button. Below these sections is a 'Description' box containing the text: 'Before configuring a service, ensure that the service has been enabled.'

Service prefix dialing mode

A user picks up the phone and dials default service prefix #41#. To change the service prefix, see [Changing Service Prefixes](#).

?16. Automatic Call Rejection

After a user enables and configures the automatic call rejection service, the calls from a preset number will be rejected automatically.

Precautions

The automatic call rejection service conflicts with some other services. For details, see [Service Conflicts](#).

Configuring the Service

Web mode

NOTE

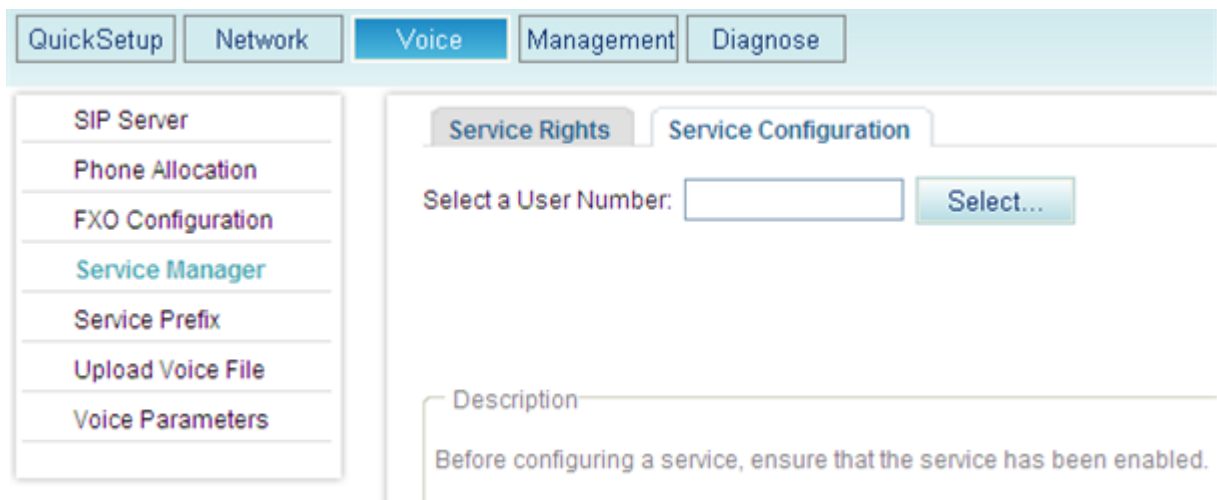
Before configuring a service, ensure that the service has been enabled. For details on how to enable voice services, see [Enabling Voice Services](#).

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

Step 2 Click the **Service Configuration** tab.

The page shown in [Figure 7-127](#) is displayed.

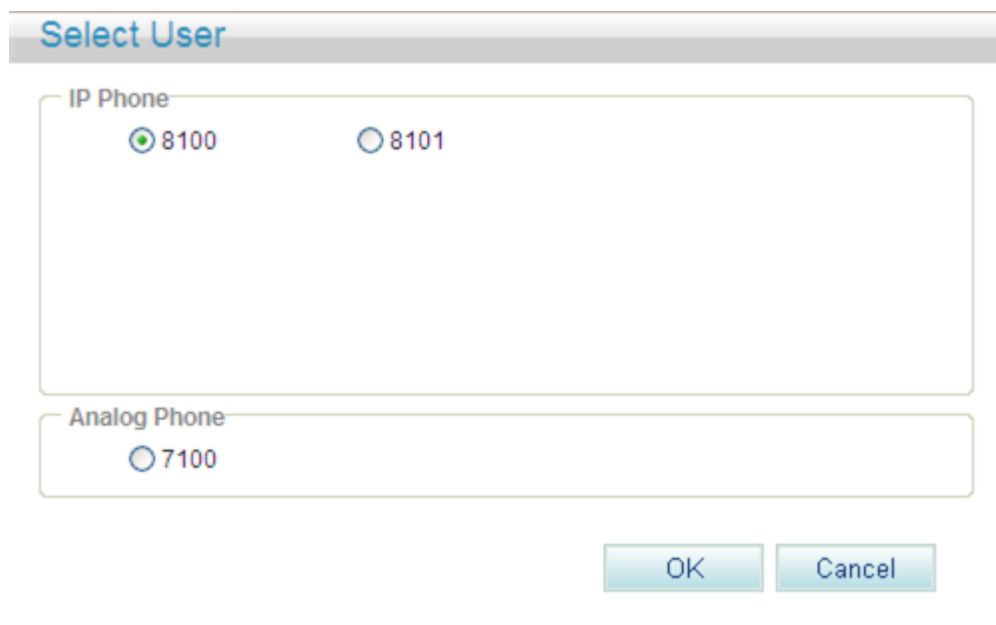
Figure 7-127 Configure Service tab page (1)

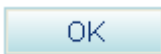


Step 3 Click .

The page shown in [Figure 7-128](#) is displayed.

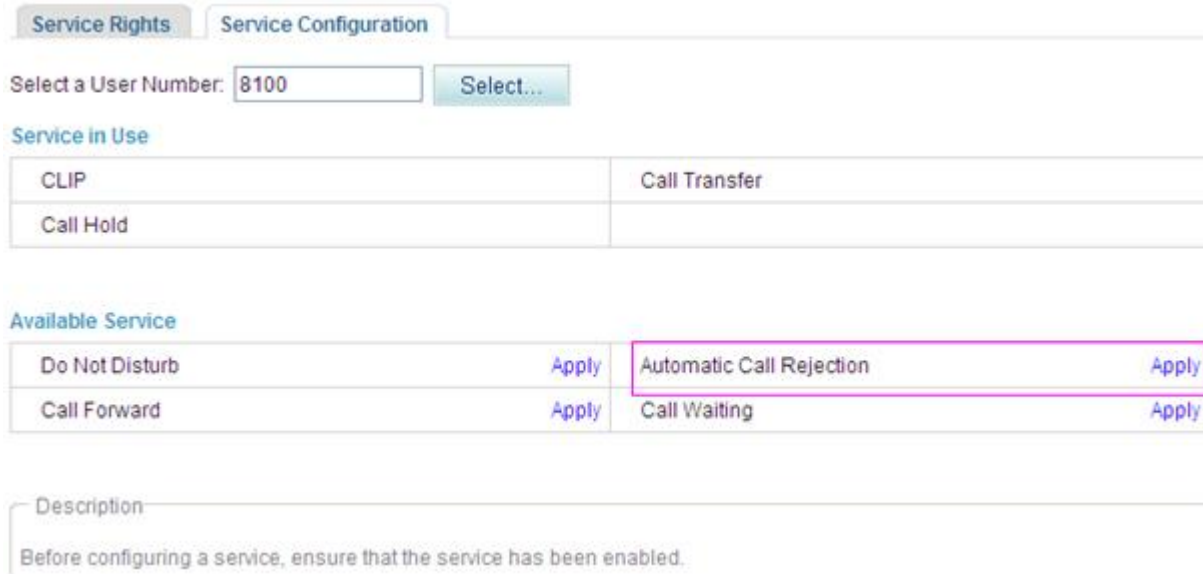
Figure 7-128 Selecting a user



Step 4 Select a user number, and click .

The page shown in [Figure 7-129](#) is displayed.

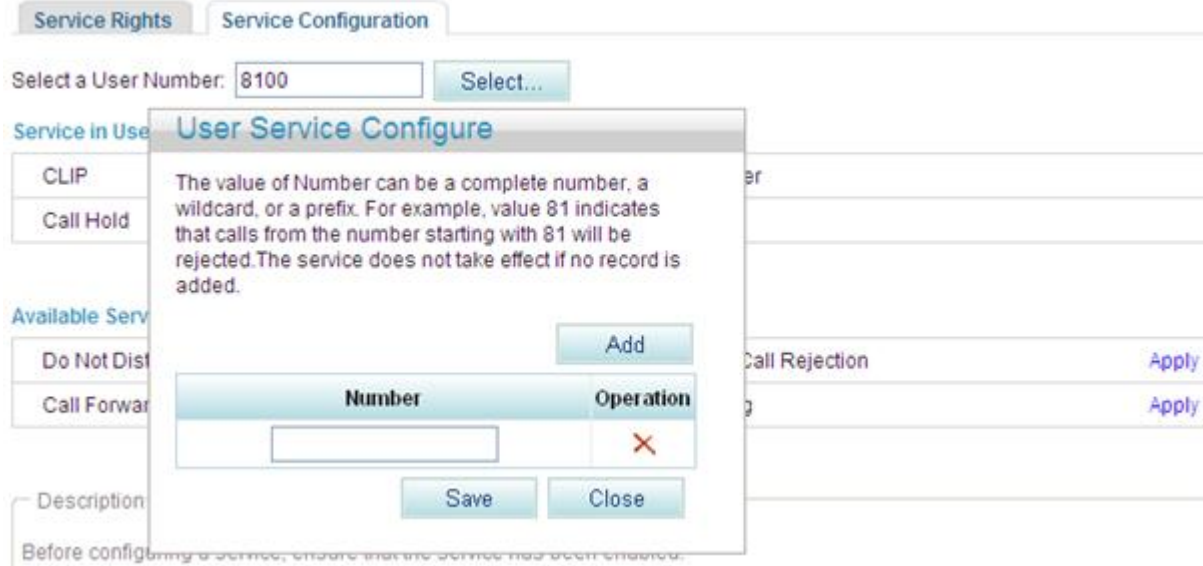
Figure 7-129 Configure Service tab page (2)




Step 5 Click **Apply**.

The page shown in [Figure 7-130](#) is displayed.

Figure 7-130 Configure Service tab page (3)



Step 6 Click , and enter a number that you want to reject.

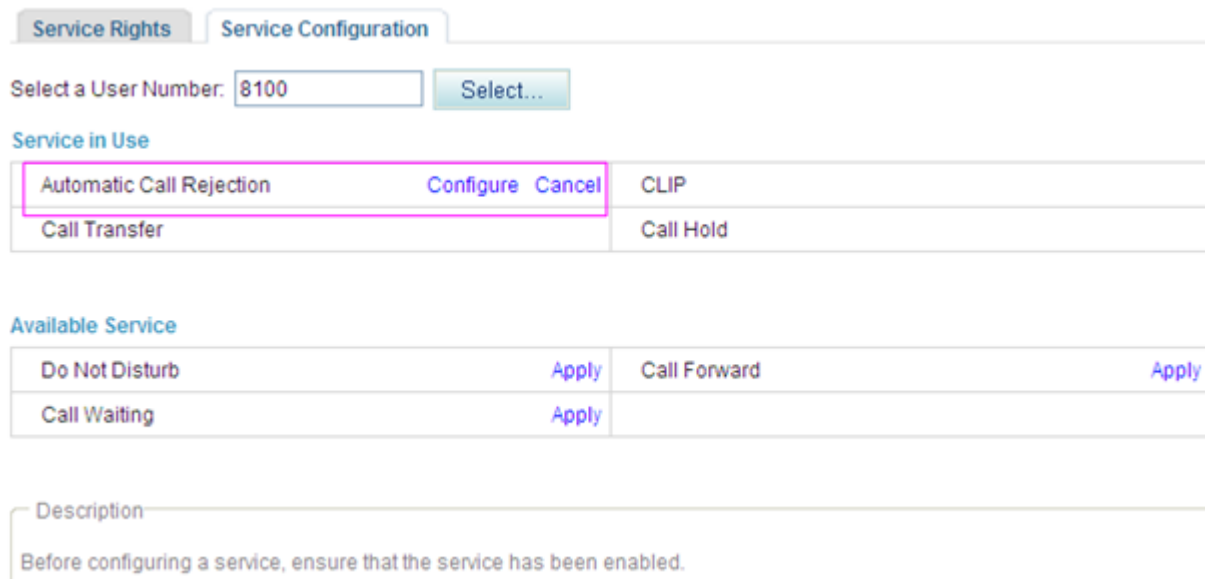
 **NOTE**

- You can enter a complete number or the first several digits of a number in the **Number** text box. For example, if you enter **8100**, the number **8100** and numbers that start with **8100** are rejected.
- A maximum of 10 numbers can be added. The length of each number must be equal to or less than 30 characters.
- When no rejected number is configured, the system saves the settings of the Automatic Call Rejection (ACR) service but does not reject the calls from any numbers.

Step 7 Click 

Figure 7-131 shows the configuration result.

Figure 7-131 Configuration result



Service in Use	
Automatic Call Rejection	Configure Cancel CLIP
Call Transfer	Call Hold

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

Description
Before configuring a service, ensure that the service has been enabled.

 **NOTE**

To modify the configuration, click **Configure**.

----End

Service prefix dialing mode

In addition to the preceding web mode, you can also dial a prefix to configure the service.

For example, pick up the phone and dial ***97*number1*number2*number3#**, where *number1*, *number2*, and *number3* indicate numbers that you want to reject and ***97*** is the default service prefix. The length of each number must be equal to or less than 27 characters. To change the service prefix, see [Viewing and Changing Service Prefixes](#).

Using the Service

Assume that user A has enabled and configured the automatic call rejection service and user B's number is rejected. User A's phone will automatically reject calls made by user B.

Canceling the Service

Web mode

Click **Cancel** on the **Service Configuration** tab page, as shown in [Figure 7-132](#).

Figure 7-132 Canceling the service

The screenshot shows the 'Service Configuration' tab in a web management system. At the top, there are two tabs: 'Service Rights' and 'Service Configuration'. Below the tabs, there is a 'Select a User Number' field with the value '8100' and a 'Select...' button. Underneath, there is a section titled 'Service in Use' containing a table with two rows. The first row is 'Automatic Call Rejection' with 'Configure' and 'Cancel' buttons next to it. The second row is 'Call Transfer' with 'Call Hold' text. Below this is an 'Available Service' section with a table containing 'Do Not Disturb' (with an 'Apply' button) and 'Call Forward' (with an 'Apply' button), and 'Call Waiting' (with an 'Apply' button'). At the bottom, there is a 'Description' box with the text: 'Before configuring a service, ensure that the service has been enabled.'

Service prefix dialing mode

- A user picks up the phone and dials **#97#** to cancel the rejection of all preset numbers.
- A user picks up the phone and dials **#97*number1*number2*number3#**, where *number1*, *number2*, and *number3* indicate numbers that the user does not want to reject any longer and **#97*** is the default service prefix. To change the service prefix, see [Changing Service Prefixes](#).

?17.Night Service

If a user configures the night service, all incoming calls at night are forwarded to the voice mailbox or a preset number.

Precautions

The night service conflicts with some other services. For details, see [Service Conflicts](#).

NOTE

Before configuring a service, ensure that the service has been enabled. For details on how to enable voice services, see [Enabling Voice Services](#).

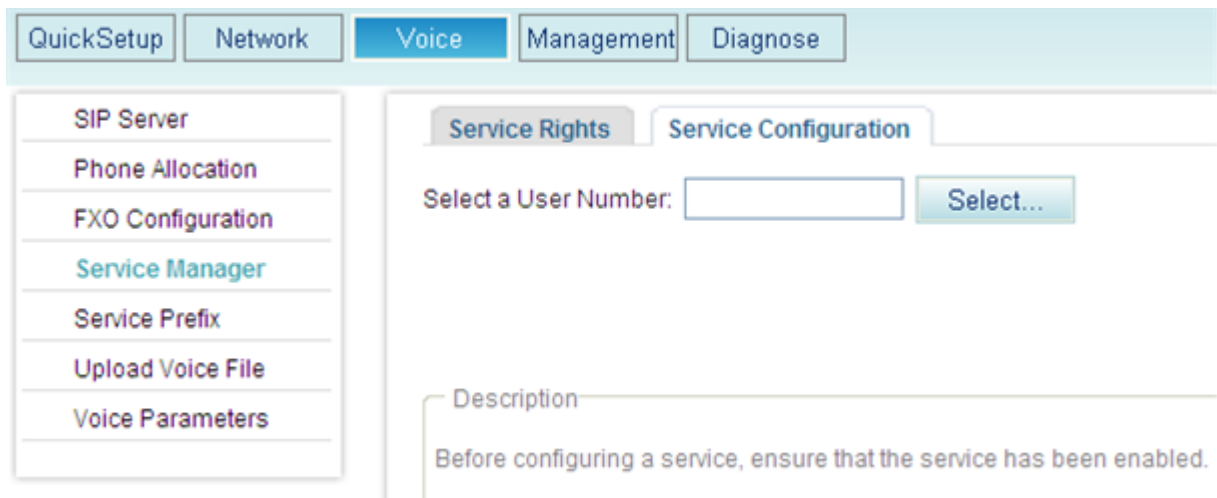
Configuring the Service

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

Step 2 Click the **Service Configuration** tab.

The page shown in [Figure 7-133](#) is displayed.

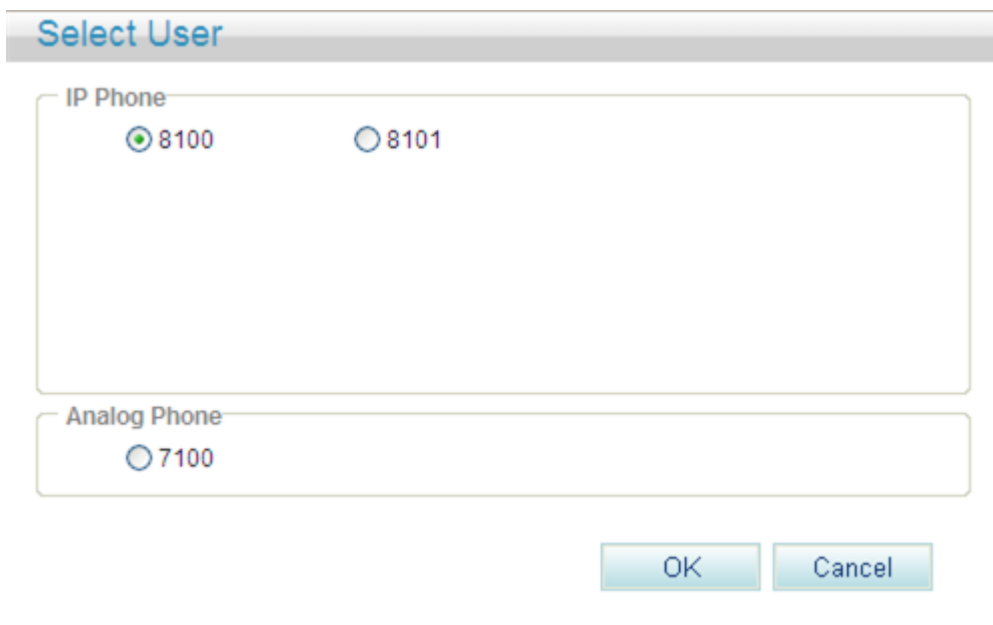
Figure 7-133 Configure Service tab page (1)



Step 3 Click .

The page shown in [Figure 7-134](#) is displayed.

Figure 7-134 Selecting a user



Step 4 Select a user number, and click .

The page shown in [Figure 7-135](#) is displayed.

Figure 7-135 Configure Service tab page (2)

Select a User Number:

Service in Use

CLIP	Call Transfer
Call Hold	

Available Service

Do Not Disturb	<input type="button" value="Apply"/>	Call Forward	<input type="button" value="Apply"/>
Call Waiting	<input type="button" value="Apply"/>	Night Service	<input type="button" value="Apply"/>

Step 5 Click **Apply**.

The page shown in [Figure 7-136](#) is displayed.

Figure 7-136 Configure Service tab page (3)

Select a User Number:

Service in Use

CLIP	
Call Hold	

Available Service

Do Not Disturb	<input type="button" value="Apply"/>	Call Forward	<input type="button" value="Apply"/>
Call Waiting	<input type="button" value="Apply"/>	Night Service	<input type="button" value="Apply"/>

User Service Configure

Night Service Configure Interface.

Service Number:

Week Range: from: to:

Time Range: from: to:

Description: Before configuring a service, ensure that the service has been enabled.

Step 6 Enter the forwarded-to number or voice mailbox prefix in the **Service Number** text box, and set **Week Range** and **Time Range**.

NOTE

The default voice mailbox prefix is 9898 (inner mailbox) or 9899 (network mailbox). To change the voice mailbox prefix, see [Viewing and Changing Service Prefixes](#).

Step 7 Click

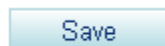


Figure 7-137 shows the configuration result.

Figure 7-137 Configuration result

The screenshot shows a web interface with two tabs: "Service Rights" and "Service Configuration". Under "Service Configuration", there is a field "Select a User Number:" with the value "8100" and a "Select..." button. Below this is a section titled "Service in Use" containing a table:

CLIP	Night Service	Configure	Cancel
Call Transfer	Call Hold		

Below the "Service in Use" table is a section titled "Available Service" containing a table:

Do Not Disturb	Apply	Call Forward	Apply
Call Waiting	Apply		



NOTE

To modify service configurations, click **Configure** corresponding to the service.

----End

Using the Service

Assume that user A has enabled and configured the night service. User A's incoming calls at night are forwarded to the voice mailbox or a preset number.

Canceling the Service

Click **Cancel** on the **Service Configuration** tab page, as shown in Figure 7-138.

Figure 7-138 Canceling the service

This screenshot is identical to Figure 7-137, but a pink rectangular box highlights the "Night Service" row in the "Service in Use" table, specifically the "Configure" and "Cancel" buttons.

?18.Three-Party Calling

A user in a call can invite a third party to start a three-party conversation. An EGW1520 supports a maximum of two concurrent three-party calls.

Configuring the Service

After enabling the three-party call service, users can directly use it without configuration. For details on how to enable voice services, see [Enabling Voice Services](#).



NOTE

- POTS users on the EGW1520 cannot initiate three-party calls.
- If a SIP user initiates a three-party call, the audio mixing is performed on the IP phone.

Using the Service

Assume that user A who is talking with user B has the three-party call service right. The process of using the service varies according to the phone that user A uses.

1. Press an idle line key (the indicator is off), dial user C's number, and press the **Send** key.
2. If user C is connected (the corresponding indicator is on), press the **CONF** key and the related line key (connecting users A and C) to start a three-party call.

If user C is not connected, press the related line key (connecting users A and B) to continue the talk with user B.



NOTE

- If user B (user C) hangs up the phone during the three-party call, user A talks with user C (user B). If user A hangs up the phone during the three-party call, users B and C listen to a busy tone.
- Operations vary according to IP phone model. For details, see the related IP phone user guide.

?19.Call Pickup

After dialing the call pickup access code and the called user's number, a user can answer the call for the called user whose phone is ringing.

Configuring the Service

After enabling the call pickup service, users can directly use it without configuration. For details on how to enable voice services, see [Enabling Voice Services](#).

Using the Service

Assume that user A has the call pickup service right.

Step 1 User C dials user B, and user B's phone rings.

Step 2 User A picks up the phone and dials *11*TN# (TN is user B's number). User B's phone stops ringing, and user A talks with user C.

In the preceding number, *11* is the default access code. To change the service prefix, see [Changing Service Prefixes](#).

----End

7.20. Call Barring

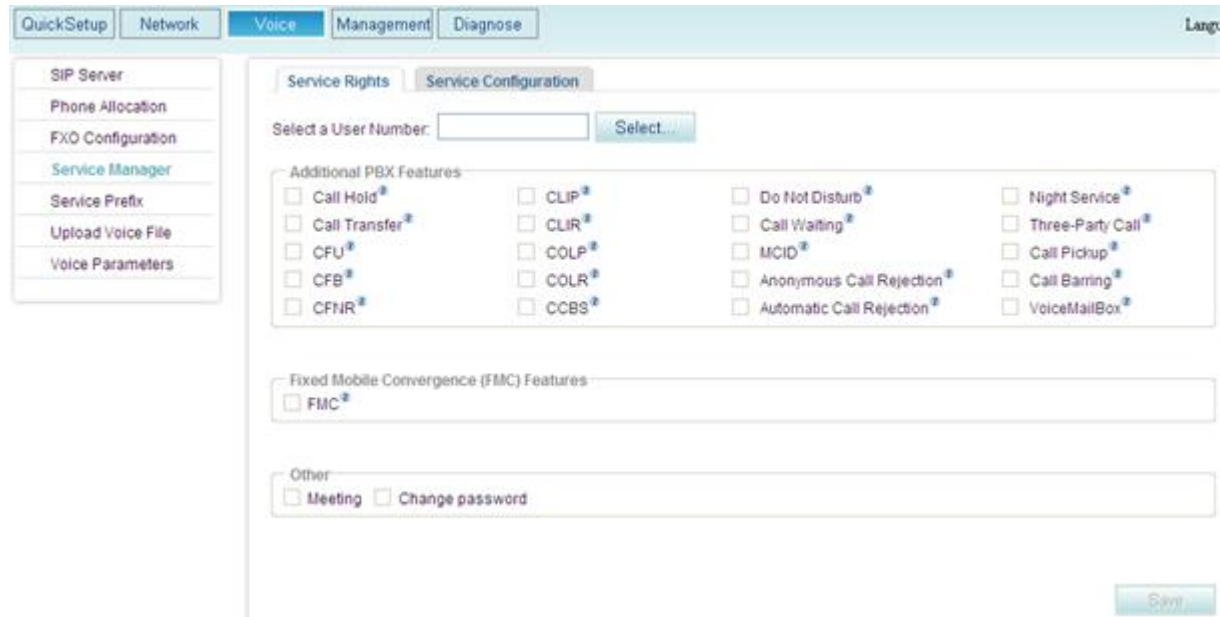
The call barring service limits calls to specified outer-office numbers. After the call barring service is enabled, the calls whose numbers match the restricted prefix are not accessible to the IMS or NGN.

Configuring the Service

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

The page shown in [Figure 7-139](#) is displayed.

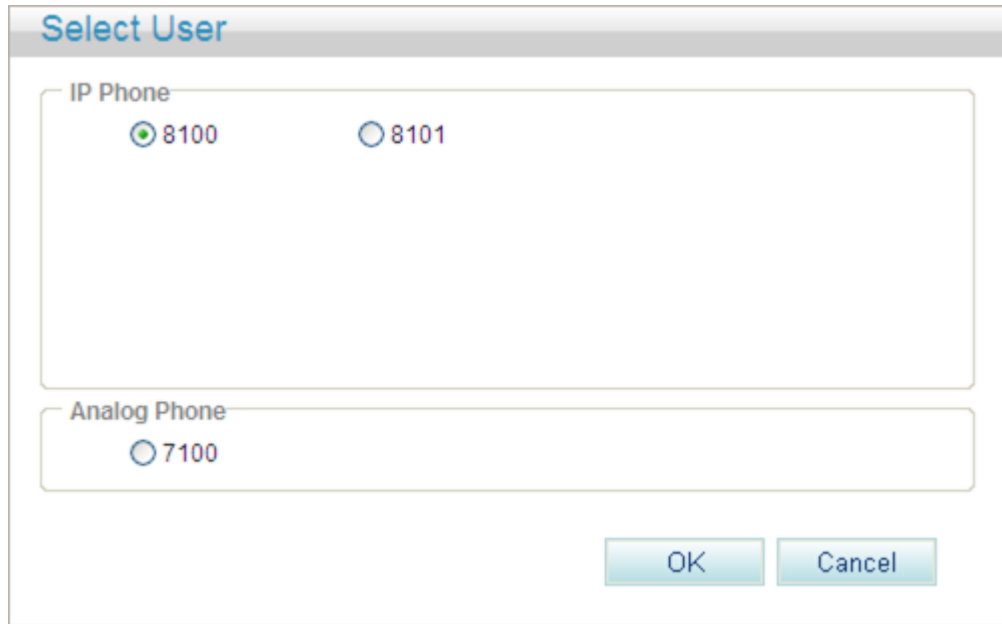
Figure 7-139 Service Rights tab page (1)



Step 2 Click .

The page shown in [Figure 7-140](#) is displayed.

Figure 7-140 Selecting a user

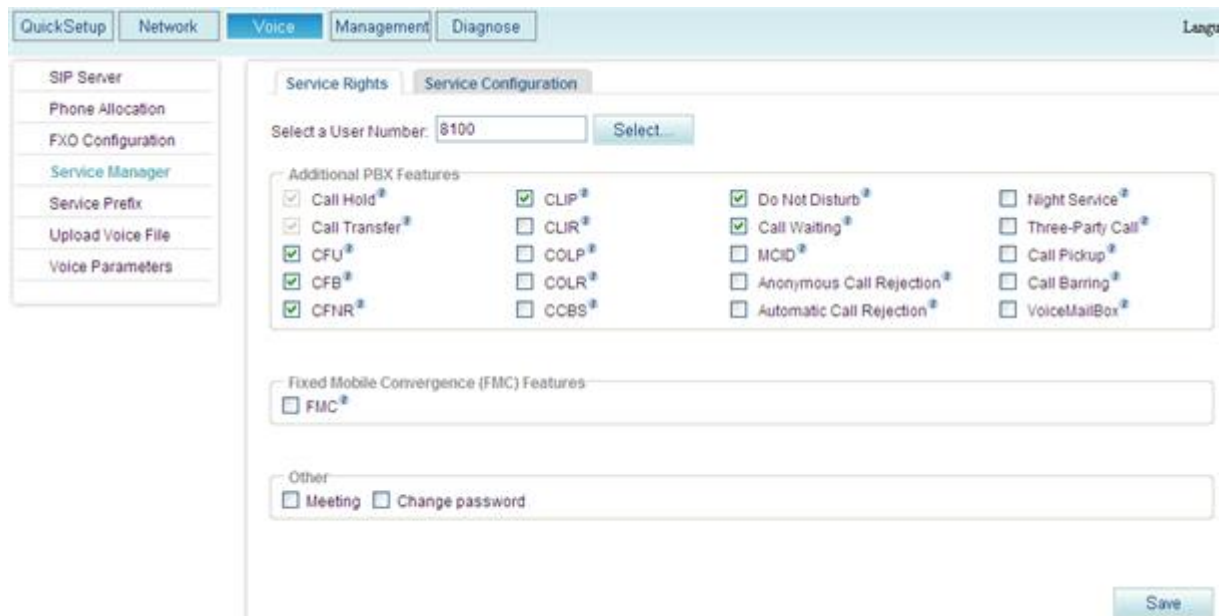


Step 3 Select a user number, and click



The page shown in [Figure 7-141](#) is displayed.

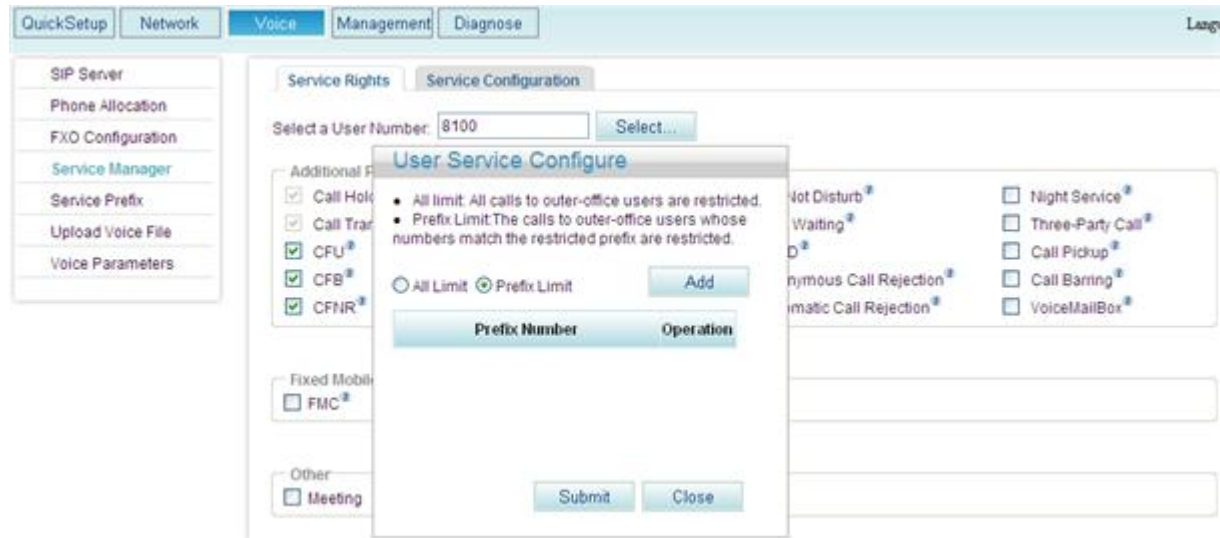
Figure 7-141 Service Rights tab page (2)



Step 4 Select **Call Barring**.

The page shown in [Figure 7-142](#) is displayed.

Figure 7-142 Call barring



Step 5 Set outer-office numbers to which calls are blocked according to [Table 7-33](#).

Table 7-33 Parameter description

Parameter	Description
All Limit	Calls are blocked to all outer-office numbers.
Prefix Limit	Calls are blocked to certain outer-office prefixes. You can set one or more service prefixes. If you add service prefix 81 , calls made by internal users to outer-office numbers starting 81 will be rejected. NOTE The call barring service limits calls to specified outer-office numbers. Calls to intra-office numbers, however, are not limited.

Step 6 Click .

[Figure 7-143](#) shows the configuration result.

Figure 7-143 Configuration result

The screenshot shows the 'Service Configuration' tab in a web interface. At the top, there are two tabs: 'Service Rights' and 'Service Configuration'. Below the tabs, there is a 'Select a User Number' field with the value '8100' and a 'Select...' button. The main area is divided into three sections: 'Additional PBX Features', 'Fixed Mobile Convergence (FMC) Features', and 'Other'. The 'Additional PBX Features' section contains a grid of checkboxes for various features. The 'Call Barring' checkbox is highlighted with a pink box. The 'Fixed Mobile Convergence (FMC) Features' section has a single checkbox for 'FMC'. The 'Other' section has checkboxes for 'Meeting' and 'Change password'. A 'Save' button is located at the bottom right of the interface.

Additional PBX Features			
<input checked="" type="checkbox"/> Call Hold	<input checked="" type="checkbox"/> CLIP	<input checked="" type="checkbox"/> Do Not Disturb	<input type="checkbox"/> Night Service
<input checked="" type="checkbox"/> Call Transfer	<input type="checkbox"/> CLIR	<input checked="" type="checkbox"/> Call Waiting	<input type="checkbox"/> Three-Party Call
<input checked="" type="checkbox"/> CFU	<input type="checkbox"/> COLP	<input type="checkbox"/> MCID	<input type="checkbox"/> Call Pickup
<input checked="" type="checkbox"/> CFB	<input type="checkbox"/> COLR	<input type="checkbox"/> Anonymous Call Rejection	<input checked="" type="checkbox"/> Call Barring
<input checked="" type="checkbox"/> CFNR	<input type="checkbox"/> CCBS	<input type="checkbox"/> Automatic Call Rejection	<input type="checkbox"/> VoiceMailBox

Fixed Mobile Convergence (FMC) Features

FMC

Other

Meeting Change password

Save

NOTE

To modify the configuration, click .

----End

Using the Service

Assume that user A has configured the call barring service and that the restricted prefix is 88. When user A calls outer-office user C on the IMS or NGN whose number starts with 88, the call will fail.

Canceling the Service

To remove the call barring right, deselect **Call Barring** on the **Service Rights** tab page.

?21.Voice Mailbox

After you configure the voice mailbox service, the voice mailbox can automatically answer incoming calls and ask the calling users to leave voice messages. Then the phone displays a message indicating that you have a voice message. The user can dial an access code to listen to the voice message.

Precautions

- The voice mailbox service conflicts with some other services. For details, see [Service Conflicts](#).

- An EGW1520 allows a maximum of 24 users to enable the voice mailbox service.
- The maximum duration of a voice message is 30 seconds.
- An EGW1520 user can leave at least one voice message. All EGW1520 users can leave 120 voice messages. When the number of voice messages reaches 120, no more voice messages are allowed. To leave new voice messages, you must delete old ones.
- If the CFU service is configured for your voice mailbox, you do not need to configure the call transfer to voice message on busy (CTVMB) service and call transfer to voice mailbox on no reply (CTVMNR) service.

Configuring the Service

Web mode

NOTE

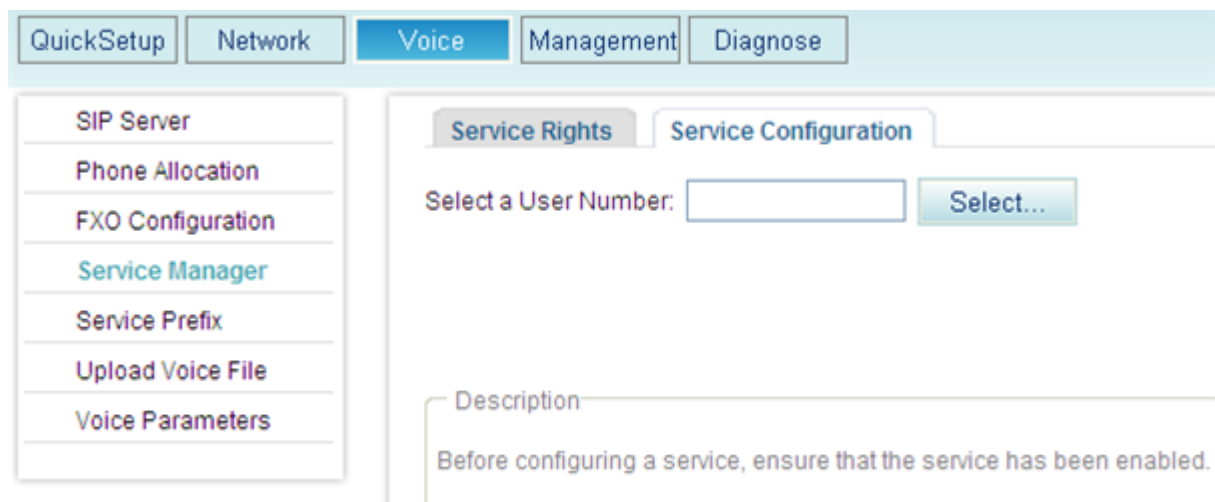
Before configuring a service, ensure that the service has been enabled. For details on how to enable voice services, see [Enabling Voice Services](#).

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

Step 2 Click the **Service Configuration** tab.

The page shown in [Figure 7-144](#) is displayed.

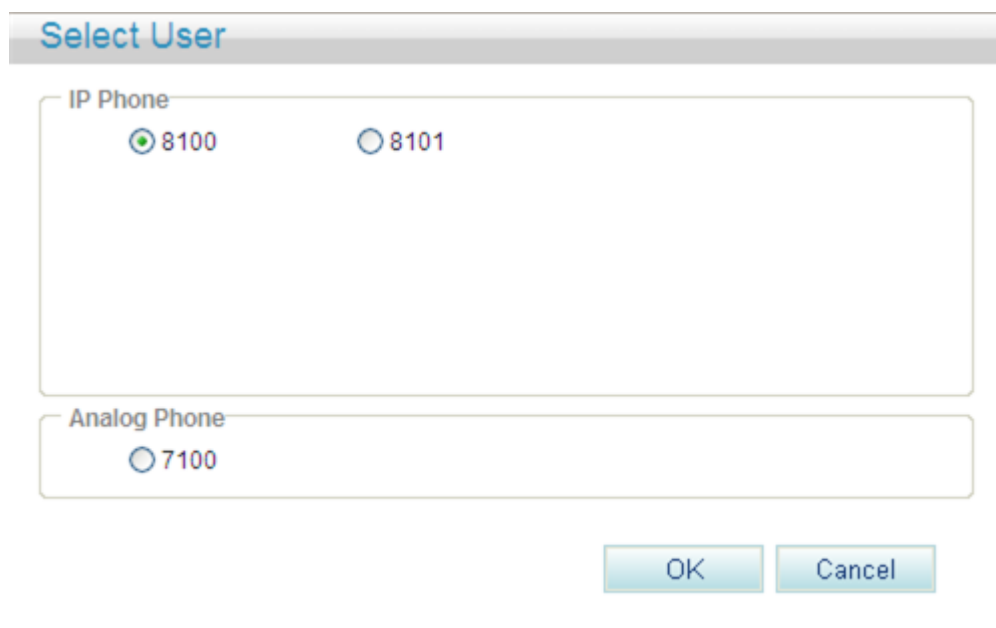
Figure 7-144 Configure Service tab page (1)



Step 3 Click  .

The page shown in [Figure 7-145](#) is displayed.

Figure 7-145 Selecting a user

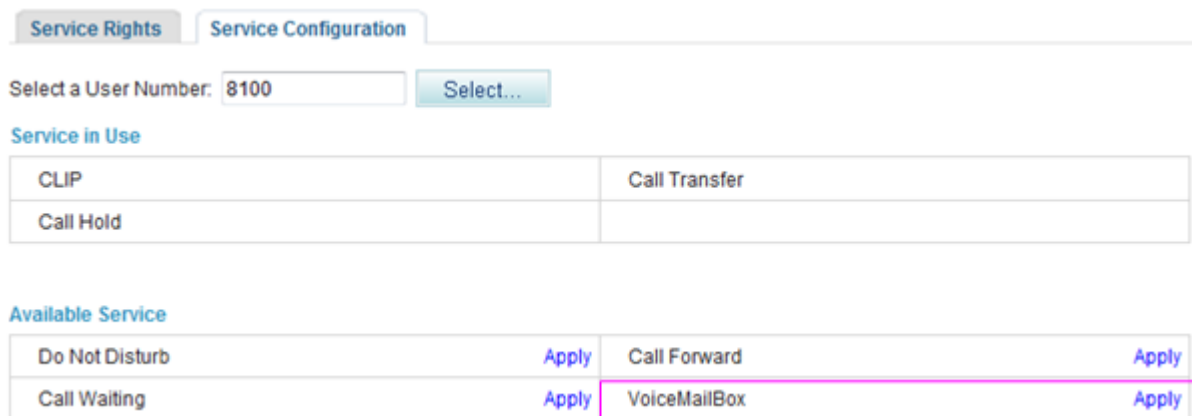


Step 4 Select a user number.

Step 5 Click .

The page shown in [Figure 7-146](#) is displayed.

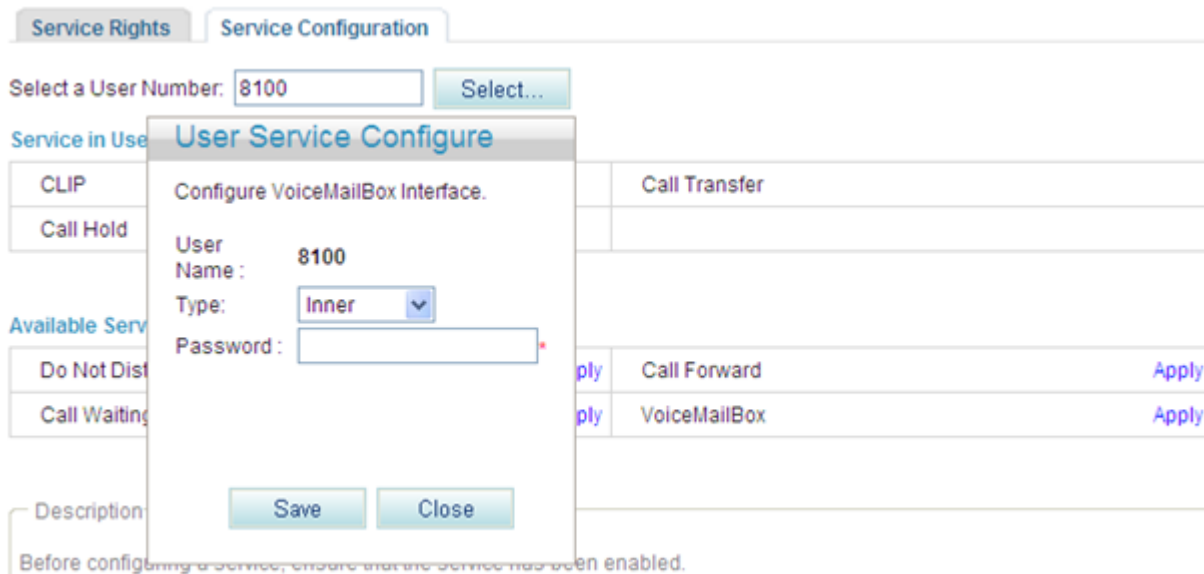
Figure 7-146 Configure Service tab page (2)



Step 6 Click **Apply**.

The page shown in [Figure 7-147](#) is displayed.

Figure 7-147 Configure Service tab page (3)



Step 7 Set parameters according to [Table 7-34](#).

Table 7-34 Parameter description

Parameter	Description
Type	Mailbox type. <ul style="list-style-type: none"> • Inner: voice mailbox on the EGW1520 • Network: voice mailbox of a carrier
Password	Password for a user to retrieve messages, consisting of 4 to 8 digits.

Step 8 Click



[Figure 7-148](#) shows the configuration result.

Figure 7-148 Configuration result

The screenshot shows a web interface for configuring services. At the top, there are two tabs: 'Service Rights' and 'Service Configuration'. Below the tabs, there is a field 'Select a User Number:' with the value '8100' and a 'Select...' button. Under the 'Service in Use' section, there is a table with two columns. The first column lists services: 'CLIP', 'Call Transfer', 'VoiceMailBox', and 'Call Hold'. The second column contains 'Configure' and 'Cancel' buttons. The 'VoiceMailBox' row is highlighted with a pink border. Below this, the 'Available Service' section contains another table with two columns. The first column lists services: 'Do Not Disturb', 'Call Forward', and 'Call Waiting'. The second column contains 'Apply' buttons.

Service in Use	
CLIP	VoiceMailBox Configure Cancel
Call Transfer	Call Hold

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

Step 9 When configuring the call forwarding or night service, you can set the forwarded-to number to the voice mailbox prefix. The default voice mailbox prefix is 9898 (inner mailbox) or 9899 (network mailbox). To change the voice mailbox prefix, see [Viewing and Changing Service Prefixes](#).

- For details on how to configure call forwarding services, see [Call Forwarding on Busy](#), [Call Forwarding on No Reply](#), and [Call Forwarding Unconditional](#).
- For details on how to configure the night service, see [Night Service](#).

----End

Service prefix dialing mode

A user picks up the phone and configures a forwarding service. The forwarded-to number is a voice mailbox prefix **9898** or **9899**. To change the service prefix, see [Changing Service Prefixes](#).

To configure forwarding services, see [Call Forwarding on Busy](#), [Call Forwarding on No Reply](#), and [Call Forwarding Unconditional](#).

NOTE

When you set the forwarded-to number to a voice mailbox prefix in the night service, you can only use the web mode.

Using the Service

Assume that user A has enabled and configured the voice mailbox service. If user B is an outer-office user, the process of using the voice mailbox service is as follows:

1. User B calls user A. After listening to the message-taking voice prompt, user B takes a voice message and then presses the pound key (#).
2. User B listens to an announcement saying that the voice message is taken successfully, and then hangs up. User B can also play the recorded voice message, take a voice message again, and cancel the voice message.
3. User A finds that the phone received a new voice message and dials access code **91001** to retrieve it from the EGW1520 voice mailbox or **91002** from the carrier's voice

mailbox. User A enters the retrieving ID (user number) and password as prompted, and presses the pound key (#). Then user A can listen to the voice message and perform other settings, such as changing the password, as prompted.

 **NOTE**

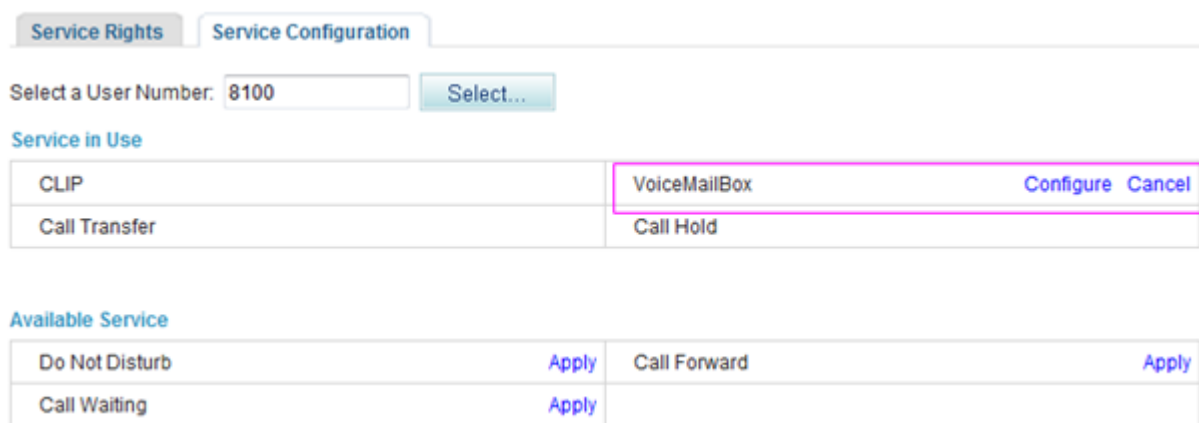
The default access codes for retrieving messages are 91001 and 91002. To change the access code, see [Viewing and Changing Service Prefixes](#).

4. After the voice message is played, user A can delete it as prompted.

Canceling the Service

Click **Cancel** on the **Service Configuration** tab page, as shown in [Figure 7-149](#).

Figure 7-149 Canceling the service



The screenshot shows a web interface with two tabs: 'Service Rights' and 'Service Configuration'. The 'Service Configuration' tab is active. Below the tabs, there is a 'Select a User Number' field with '8100' entered and a 'Select...' button. Underneath, there are two sections: 'Service in Use' and 'Available Service'. The 'Service in Use' section contains a table with two rows: 'CLIP' and 'Call Transfer'. The 'VoiceMailBox' service is highlighted in a pink box, and its 'Cancel' button is also highlighted. The 'Available Service' section contains a table with two rows: 'Do Not Disturb' and 'Call Waiting', each with an 'Apply' button.

Service in Use	
CLIP	VoiceMailBox Configure Cancel
Call Transfer	Call Hold

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

7.22.Fixed Mobile Convergence

The Fixed Mobile Convergence (FMC) service allows users to configure the simultaneous ringing, sequential ringing, call toggling, and voice mailbox services.

Introduction

- **Simultaneous ringing**
Configure a mobile number as the simultaneous ringing number of a fixed-line phone. When a user receives a call, the mobile phone and the fixed-line phone ring together. The user can pick up either of the phones to answer the call.
A user can be only configured with one simultaneous ringing number.
- **Sequential ringing**
Configure a mobile number as the sequential ringing number of a fixed-line phone. When a user receives a call, the fixed-line phone rings. If the user does not pick up the fixed-line phone for a specified period, the mobile phone rings.
A user can be only configured with one sequential ringing number.
- **Call toggling**

Configure a mobile number as the toggling number of a fixed-line phone. When a user is in a call, the user can release the call after toggling it to the mobile phone.

- Voice mailbox

After you configure the voice mailbox service, the voice mailbox can automatically answer incoming calls and ask the calling users to leave voice messages. Then the phone displays a message indicating that you have a voice message. To listen to the voice message, dial an access code.

Precautions

The FMC service conflicts with some other services. For details, see [Service Conflicts](#).

Configuring the Service

NOTE

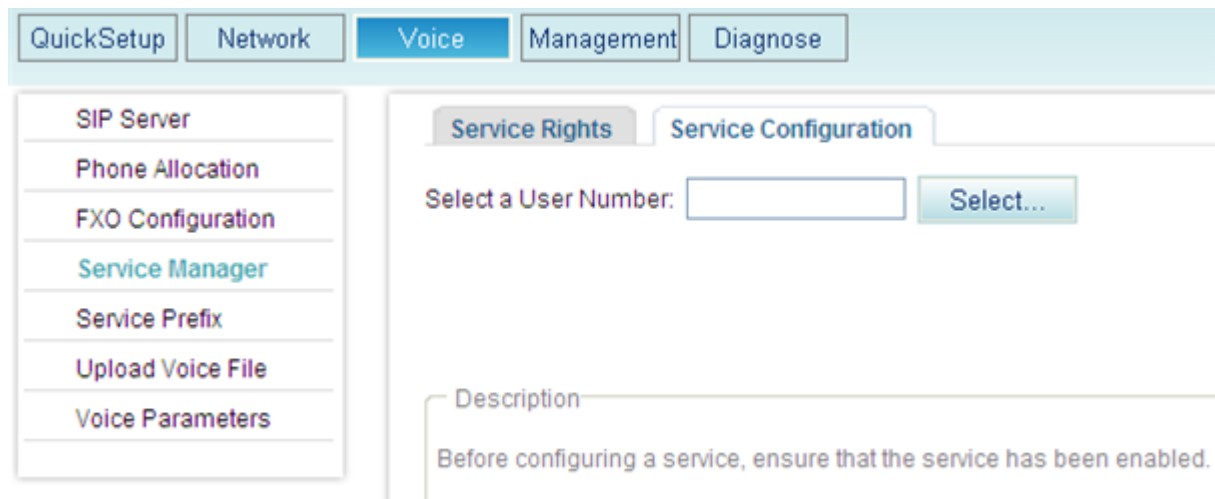
Before configuring a service, ensure that the service has been enabled. For details on how to enable voice services, see [Enabling Voice Services](#).

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

Step 2 Click the **Service Configuration** tab.

The page shown in [Figure 7-150](#) is displayed.

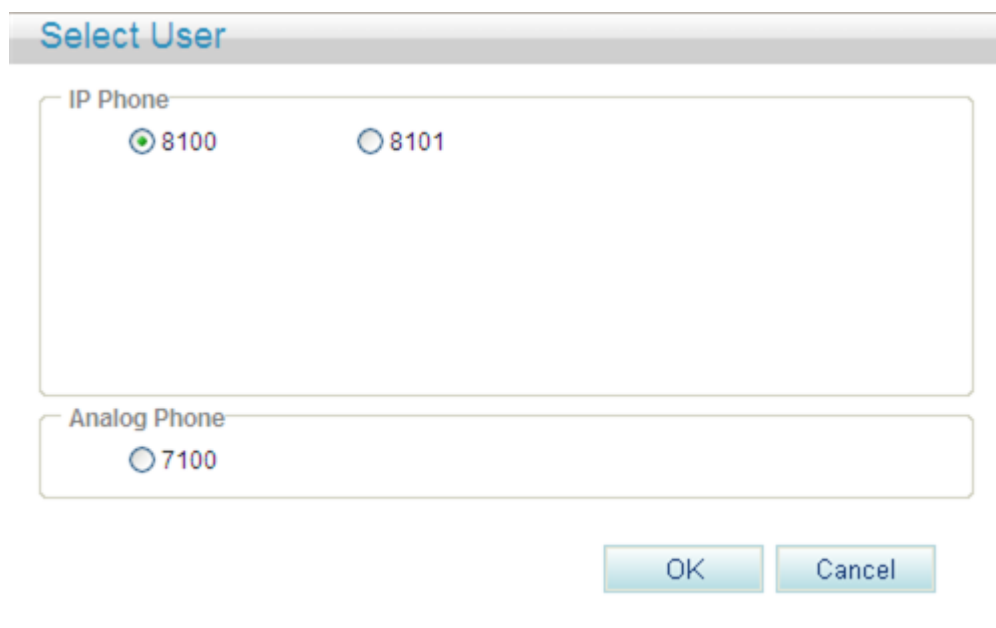
Figure 7-150 Configure Service tab page (1)



Step 3 Click .

The page shown in [Figure 7-151](#) is displayed.

Figure 7-151 Selecting a user

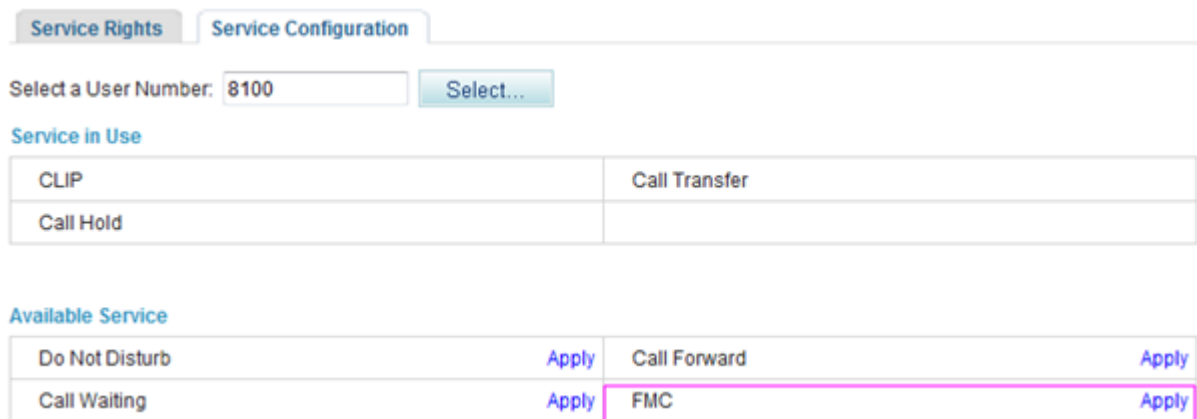


Step 4 Select a user number.

Step 5 Click .

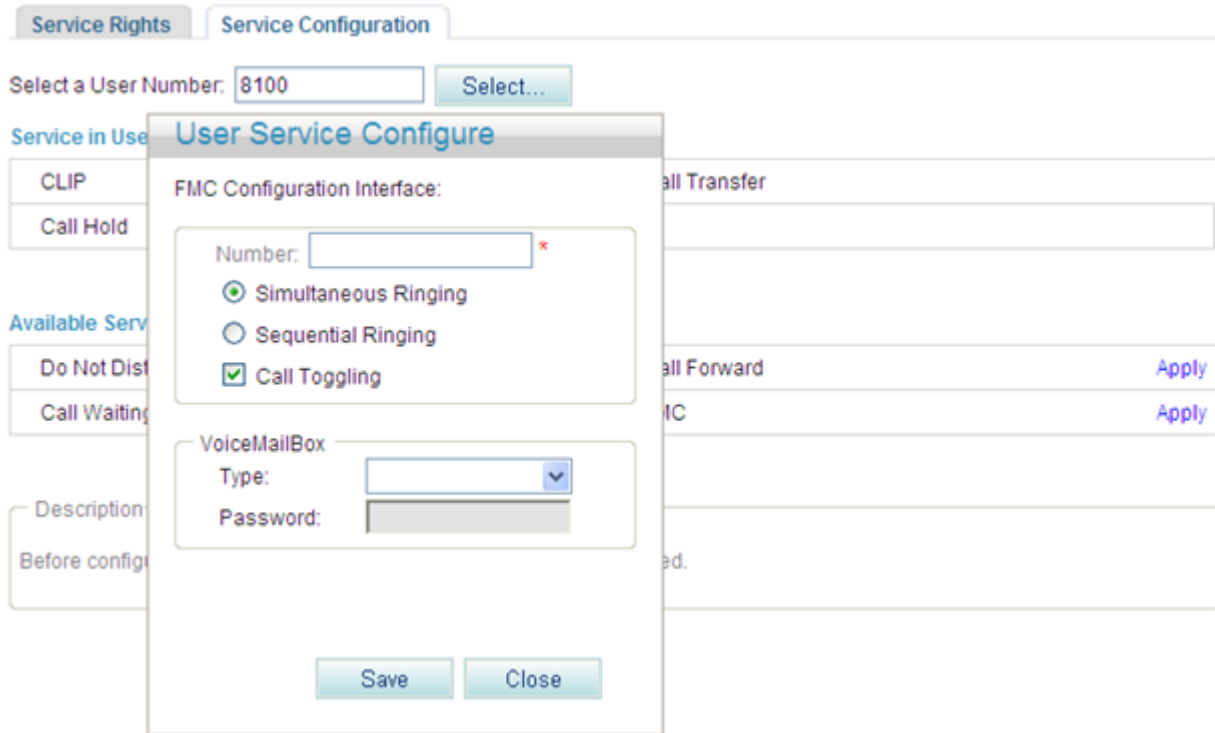
The page shown in [Figure 7-152](#) is displayed.

Figure 7-152 Configure Service tab page (2)



Step 6 Click **Apply**.

Figure 7-153 Configure Service tab page (3)



Step 7 Set parameters according to [Table 7-35](#).

Table 7-35 Parameter description

Parameter	Description
Mobile Number	Indicates the mobile number that you associate with the fixed-line number in the simultaneous ringing, sequential ringing, and call toggling services.
Simultaneous Ringing	When a user receives a call, the mobile phone and the fixed-line phone ring together. The user can pick up either of the phones to answer the call.
Sequential Ringing	If a user does not answer an incoming call for a specified period, the fixed-line phone stops ringing and the mobile phone starts ringing.
Call Toggling	A user can press the hook flash button and dial an access code to switch the call to the mobile phone.
VoiceMailBox	Allows you to set the voice mailbox information. For details, see Voice Mailbox .

Step 8 Click .

[Figure 7-154](#) shows the configuration result.

Figure 7-154 Configuration result

The screenshot shows a web interface for configuring services. At the top, there are two tabs: 'Service Rights' and 'Service Configuration'. Below the tabs, there is a field 'Select a User Number:' with the value '8100' and a 'Select...' button. Under the heading 'Service in Use', there is a table with two columns. The first column lists services: 'CLIP' and 'Call Hold'. The second column lists services: 'Call Transfer' and 'FMC'. The 'FMC' row is highlighted with a pink border, and it has 'Configure' and 'Cancel' buttons to its right. Below this, under the heading 'Available Service', there is another table with two columns. The first column lists services: 'Do Not Disturb' and 'Call Waiting'. The second column lists services: 'Call Forward'. The 'Do Not Disturb' and 'Call Waiting' rows have 'Apply' buttons to their right, and the 'Call Forward' row has an 'Apply' button to its right.

 **NOTE**

To modify the configuration, click **Configure**.

----End

Using the Service

Simultaneous ringing

Assume that user A has configured the simultaneous ringing service and user B's mobile number is the simultaneous ringing number. When user C calls user A, user A's and user B's phones ring at the same time. Both user A's and user B's phone can answer the call. When a phone is picked up, the other phone stops ringing.

Sequential ringing

Assume that user A has configured the sequential ringing service and user B's mobile number is the sequential ringing number. When user C calls user A but user A does not answer within 20 seconds, user A's phone stops ringing and user B's phone starts to ring. User B can answer the call from user C.

Call toggling

Assume that user A has configured the call toggling service and that user B is the one to whom the call is toggled. User A can exit the conversation with user C and enable user B to talk with user C. The process is as follows:

1. User A presses the hook flash button and dials default service prefix ***19#** after hearing a dialing tone. To change the service prefix, see [Changing Service Prefixes](#).
2. User B's phone rings. User B picks up the phone to talk with user C and user A releases the call.

Voicemail

For details on how to configure and use the voicemail service, see [Voice Mailbox](#).

Canceling the Service

Click **Cancel** on the **Service Configuration** tab page, as shown in [Figure 7-155](#).

Figure 7-155 Canceling the service

Service Rights Service Configuration

Select a User Number:

Service in Use

CLIP	Call Transfer
Call Hold	FMC <input type="button" value="Configure"/> <input type="button" value="Cancel"/>

Available Service

Do Not Disturb	<input type="button" value="Apply"/>	Call Forward	<input type="button" value="Apply"/>
Call Waiting	<input type="button" value="Apply"/>		

7.23. Instant Conference Call

The EGW1520 support an instance conference call that allows a maximum of six participants (including the moderator) to join. The moderator can invite other participants to join the conference.

Assigning the Conference Moderator Right

The conference moderator right is assigned by the enterprise IT administrator, and no configuration is required. For details, see [Enabling Voice Services](#).

NOTE

The moderator must be an intra-office user.

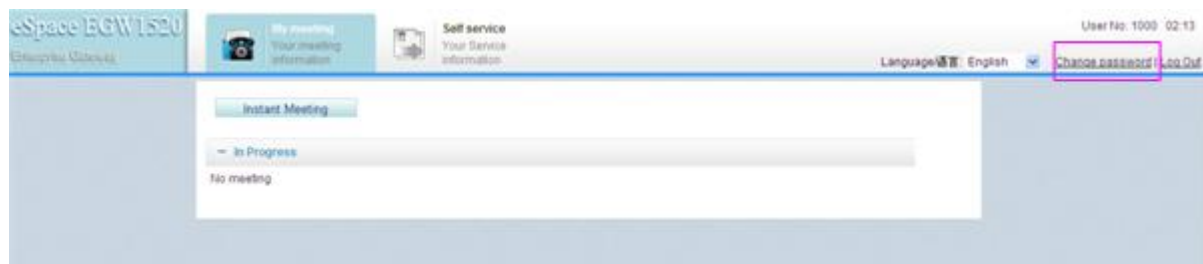
Initiating an Instance Conference Call

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

Step 2 Enter the user name and password. (Both the initial user name and password for the moderator are the moderator's internal number.)

The page shown in [Figure 7-156](#) is displayed.

Figure 7-156 Conference page



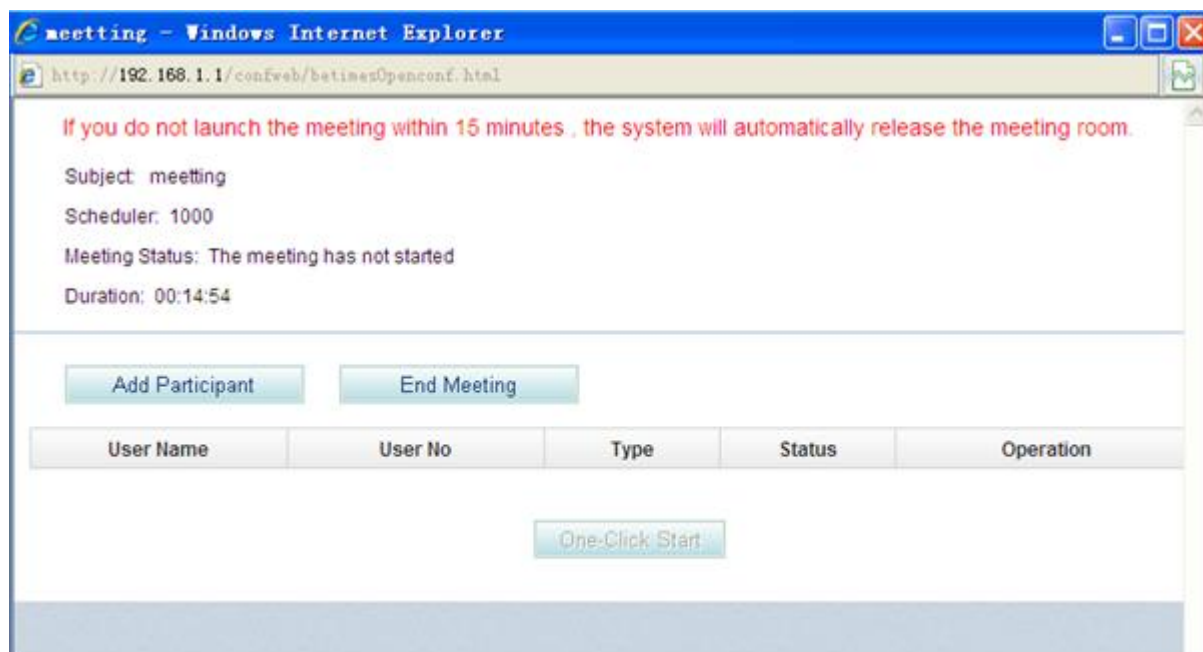
NOTE

- You are advised to change the initial password to ensure security. To change the initial password, click **Change password** in [Figure 7-156](#).
- If you forget the password, contact the enterprise IT administrator to reset the password. For details, see [Enabling Voice Services](#).

Step 3 Click  .

The page shown in [Figure 7-157](#) is displayed.

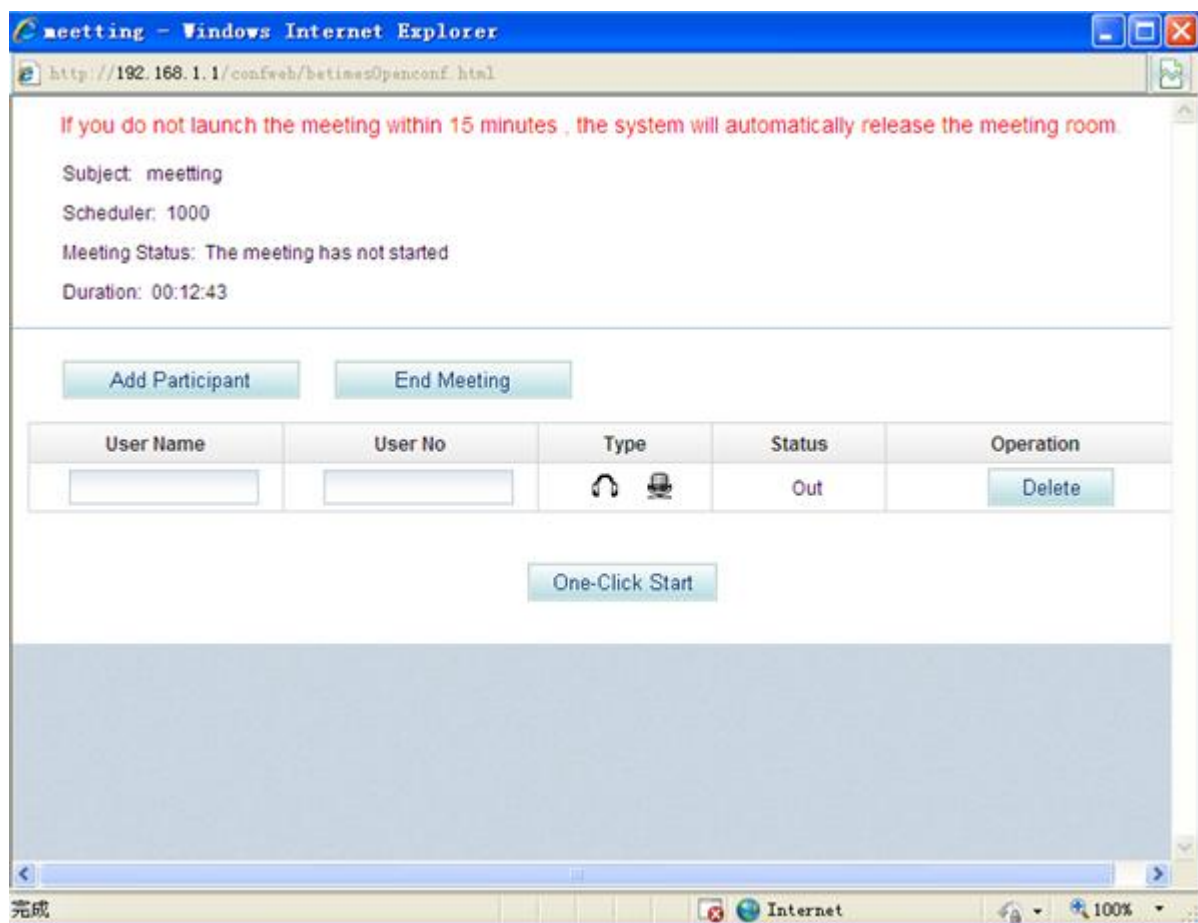
Figure 7-157 Joining a conference



Step 4 Click  .

The page shown in [Figure 7-158](#) is displayed.

Figure 7-158 Adding participants



Step 5 Set **User Name** and **User No** of a participant.

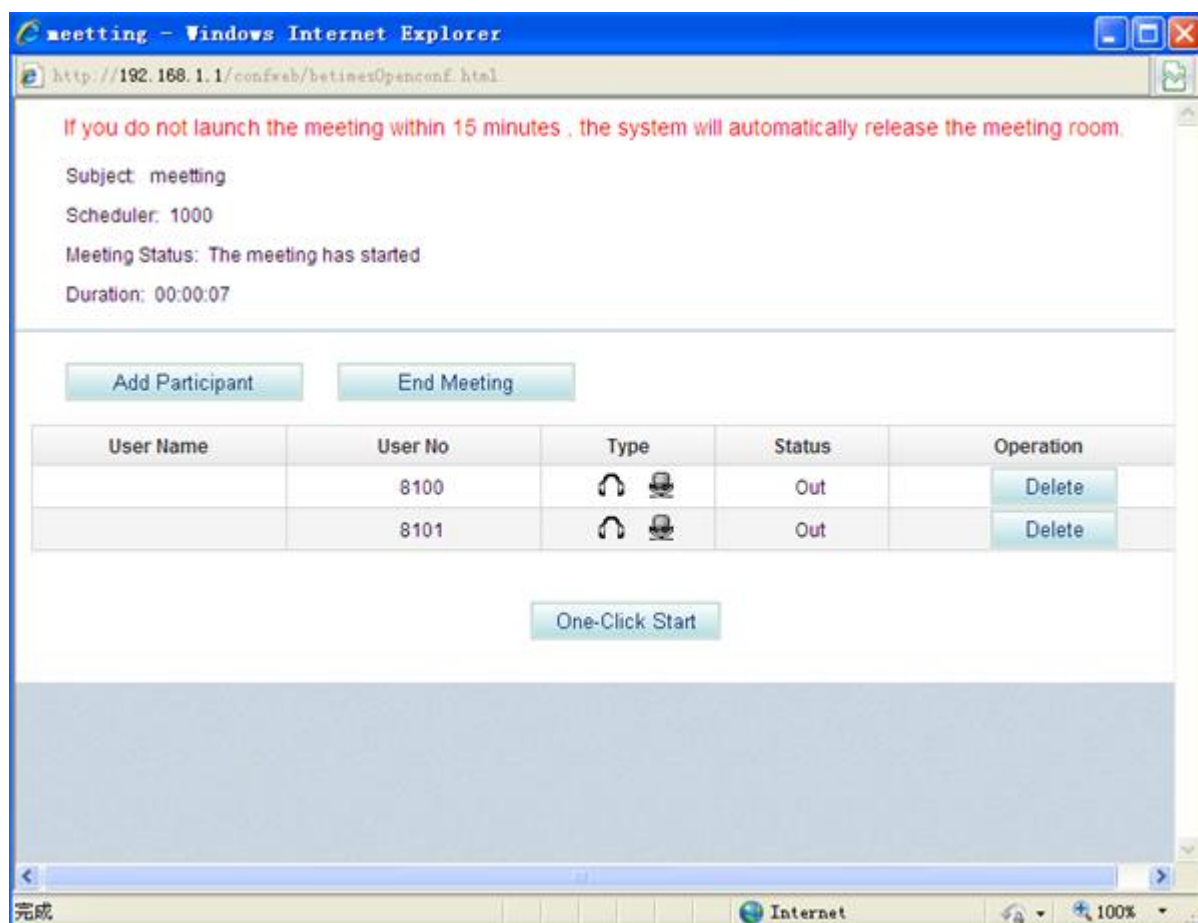
 **NOTE**

- A participant can be an intra-office or outer-office user (such as a PSTN, IMS, or NGN user).
- To invite an outer-office user to join the conference through the FXO port on EGW1520, you must set **User No** based on the FXO dialing rules, such as set **User No** to the outgoing prefix and the outer-office user's number.

Step 6 Click  to start the conference.

The page shown in [Figure 7-159](#) is displayed.

Figure 7-159 Conference participants



----End

Self-Service

The self-service function allows users to configure voice services that have been enabled.

Prerequisites

Voice services have been enabled by the enterprise IT administrator.

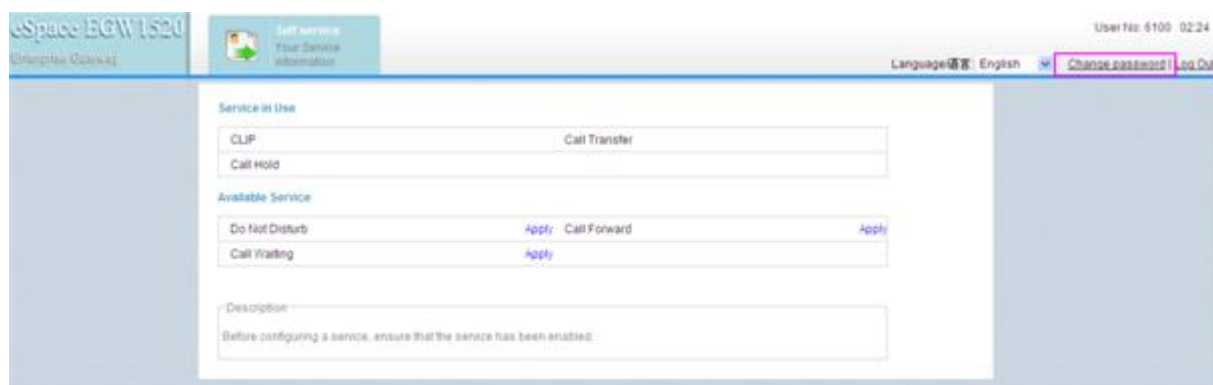
Using the Self-Service Function

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

Step 2 Enter the user name and password. (Both the initial user name and password are a user's internal number.)

The page shown in [Figure 7-160](#) is displayed.

Figure 7-160 Self-service



 **NOTE**

- You are advised to change the initial password to ensure security. To change the initial password, click **Change password** in [Figure 7-160](#).
- If you forget the password, contact the enterprise IT administrator to reset the password.

Step 3 Configure voice services as required. For details, see [Configuring and Using Voice Services](#).

----End

Viewing and Changing Service Prefixes


This topic describes how to view and change service prefixes. Users can configure and use voice services by dialing service prefixes.

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 **Voice > Service Prefix** from the navigation tree.

Step 2 Click  in the **Operation** column.

The page shown in [Figure 7-161](#) is displayed.

Figure 7-161 Current service prefix

Service Description	Prefix	Operation
Active Do Not Disturb	*56#	
DeactiveDo Not Disturb	#56#	
Active Anonymous Call Rejection	*41#	
Deactive Anonymous Call Rejection	#41#	
Active Call Forwarding Unconditional	*21*	
Deactive Call Forwarding Unconditional	#21#	
Active Call Forwarding on busy	*67*	
Deactive Call Forwarding on busy	#67#	
Active Call Forwarding on No Reply	*61*	
Deactive Call Forwarding on No Reply	#61#	
Active Automatic Call Rejection	*97*	
Deactive All Automatic Call Rejection Numbers	#97#	
Deactive Automatic Call Rejection Number	#97*	
Active Call Completion on Busy Subscriber	*37#	
Deactive Call Completion on Busy Subscriber	#37#	
Active Call Waiting	*43#	
Deactive Call Waiting	#43#	
Call Pickup Execute	*11*	
FMC-Call Toggling Execute	*19#	
Malicious Caller Identification	*34#	
VoiceMailBox Leave	9898	
VoiceMailBox Inner Retrieve	91001	
VoiceMailBox Network Leave	9899	
VoiceMailBox Network Retrieve	91002	

NOTE

For meanings and use of service prefixes, see [Configuring and Using Voice Services](#).

Step 3 Change the service prefix in the **Prefix** column.

 **NOTE**

Service prefix change rule: The asterisk (*) and number sign (#) cannot be changed. You can change numerals only. Service prefixes related to the voice mailbox cannot contain an asterisk (*) or a number sign (#). Therefore, a service prefix cannot conflict with any internal numbers, external numbers (including all outer-office numbers), or emergency numbers. [Table 7-36](#) lists Ireland's and New Zealand's emergency numbers.

Table 7-36 Ireland's and New Zealand's emergency numbers

Country	Emergency call numbers
Ireland	999, 112
New Zealand	111

Step 4 Click  to save the settings.

----End

7.4.2 FXO Port

This topic describes the principle, implementation, specification, and limitation for the FXO port on the EGW1520 and how to configure the FXO port.

Description

The EGW1520 provides four FXO ports used to connect to PSTN networks, allowing voice users on the EGW1520 to communicate with PSTN users.

Principle

The EGW1520 provides an FXO port for connecting to the PSTN network. An intra-office user can dial an outgoing prefix and the number of an outer-office user to make an outgoing call through the FXO port. An outer-office user dials the number that the PSTN network carrier allocates to any FXO port of the four FXO ports on the EGW1520 to make an incoming call.

The EGW1520 supports the switchboard, DDI, and dedicated line functions. By default, the switchboard function is enabled.

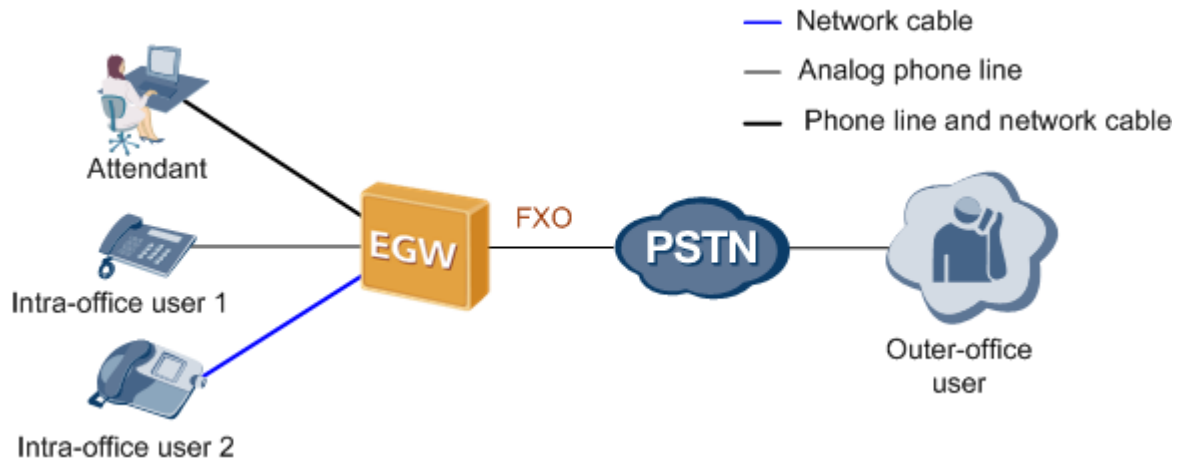
 **NOTE**

An intra-office user can be a POTS user or a SIP user.

Implementation for the Switchboard

[Figure 7-162](#) shows the application scenario for the switchboard.

Figure 7-162 Application scenario for the switchboard



The call process for the switchboard is as follows:

Outgoing call

1. An intra-office user dials the outgoing prefix for the FXO port (for example, 0) and the number of an outer-office user.
2. The EGW1520 automatically queries an idle non-dedicated FXO port for the user to make the outgoing call.



NOTE

A non-dedicated FXO port is a port for which the dedicated line is not configured. For details about the dedicated line, see [Implementation for the Dedicated Line](#).

3. The outer-office user answers the call.



NOTE

The number that the PSTN network carrier allocates to the FXO port (that is, the switchboard number) is displayed to the called party.

4. One party hangs up the phone to end the call.

Incoming call

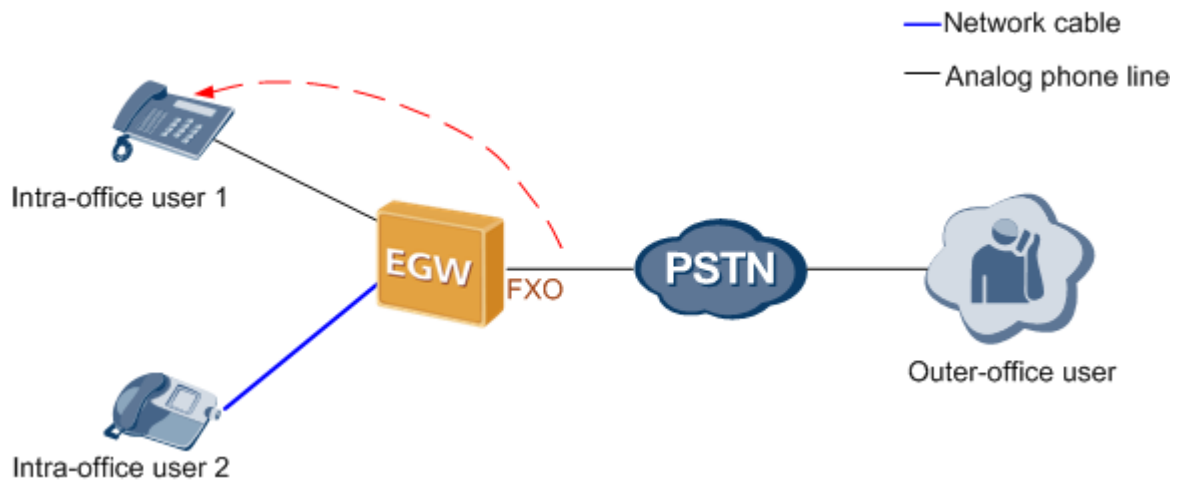
1. An outer-office user dials the number that the PSTN network carrier allocates to the FXO port, that is, the switchboard number.
The outer-office user hears an announcement, for example, "Thanks for calling XX company. Please dial the extension number. To query numbers, dial 9. End the number with a pound key."
2. The outer-office user dials an extension number (internal number) or dials 9 (to connect to the preset attendant number) as prompted, and presses the pound key (#).
3. The intra-office user or attendant answers the call.
4. One party hangs up the phone to end the call.

Implementation for the DDI

The DDI binds an intra-office user to an FXO port. When an outer-office user makes an incoming call to the intra-office user through the FXO port, the call is directly connected to the intra-office user. After the DDI is configured for an FXO port, other users can still make outgoing calls through the FXO port.

Figure 7-163 shows the application scenario for the DDI.

Figure 7-163 Application scenario for the DDI



The call process for the DDI is as follows:

Outgoing call

1. An intra-office user dials the outgoing prefix for the FXO port (for example, 0) and the number of an outer-office user.
2. The EGW1520 automatically queries an idle non-dedicated FXO port for the user to make the outgoing call.



NOTE

A non-dedicated FXO port is a port for which the dedicated line is not configured. For details about the dedicated line, see [Implementation for the Dedicated Line](#).

3. The outer-office user answers the call.



NOTE

The number that the PSTN network carrier allocates to the FXO port (that is, the switchboard number) is displayed to the called party.

4. One party hangs up the phone to end the call.

Incoming call

1. An outer-office user dials the number that the PSTN network carrier allocates to the FXO port.
2. The phone of the DDI user bound to the FXO port (for example, intra-office user 1 in [Figure 7-163](#)) rings.
3. The DDI user answers the call.
4. One party hangs up the phone to end the call.



NOTE

The number that the PSTN network carrier allocates to the FXO port is displayed to the called party.

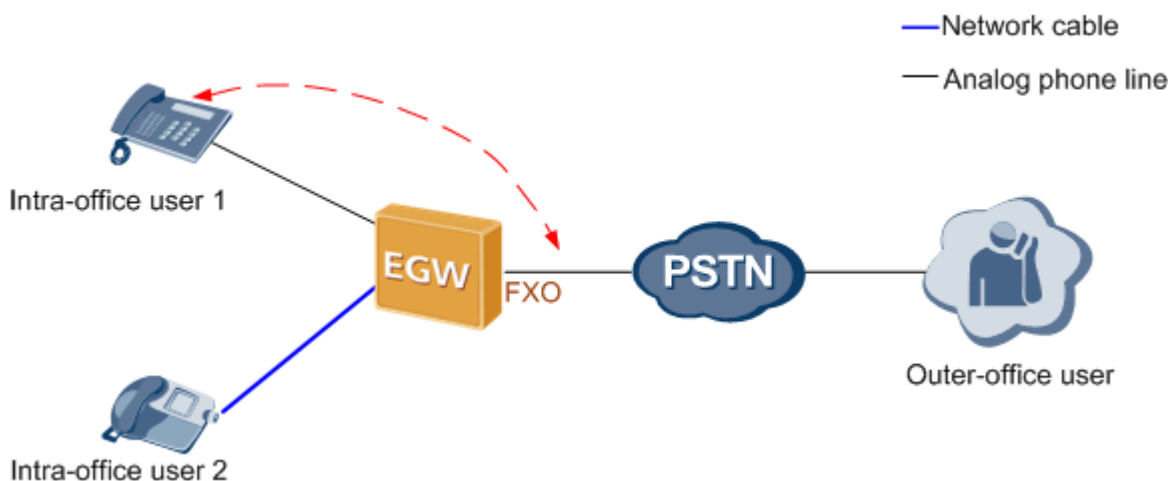
Implementation for the Dedicated Line

The dedicated line binds an intra-office user to an FXO port and sets the FXO port to be a dedicated port. When an outer-office user makes an incoming call to the intra-office user

through the FXO port, the call is directly connected to the intra-office user. Only the intra-office user can use the FXO port to make outgoing calls.

Figure 7-164 shows the application scenario for the dedicated line.

Figure 7-164 Application scenario for the dedicated line



The call process for the dedicated line is as follows:

Outgoing call

1. A dedicated user (for example, intra-office user 1 in Figure 7-164) dials the FXO outgoing prefix (configurable, for example, 0) and an outer-office user's number.
2. The EGW1520 automatically queries the FXO port bound to the user for the user to make the outgoing call.



NOTE

If the bound FXO port is unavailable (for example, no phone line is connected to the FXO port), the EGW1520 automatically queries an idle non-dedicated FXO port for the user to make the outgoing call.

3. The outer-office user answers the call.



NOTE

The number that the PSTN network carrier allocates to the FXO port is displayed to the called party.

4. One party hangs up the phone to end the call.

Incoming call

1. An outer-office user dials the number that the PSTN network carrier allocates to the FXO port.
2. The phone of the dedicated user bound to the FXO port (for example, intra-office user 1 in Figure 7-164) rings.
3. The dedicated user answers the call.
4. One party hangs up the phone to end the call.

Specification

Four FXO ports..

Limitation

- The FXO port supports only the one-stage dialing mode.
- Each FXO port allows one user to make an outgoing or incoming call through the FXO port at the same time.

Configuring an Outgoing Prefix

This topic describes how to configure an outgoing prefix for the FXO port on the EGW1520. After the outgoing prefix is configured, an intra-office user can dial the outgoing prefix and the number of an outer-office user to make an outgoing call through the FXO port.

Prerequisite

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

Background

For details about the function of outgoing prefixes and how to use outgoing prefixes, see [Description](#).

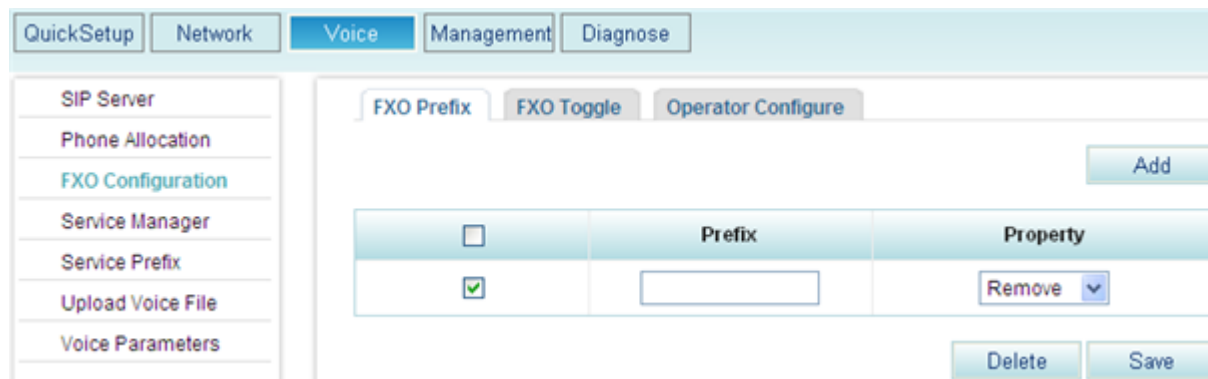
Procedure

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

Step 2 Click  .

The page shown in [Figure 7-165](#) is displayed.

Figure 7-165 Configuring an outgoing prefix for the FXO port

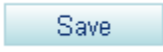


Step 3 Set parameters according to [Table 7-37](#).

Table 7-37 FXO prefix parameters

Parameter	Description
Prefix	Outgoing prefix for the FXO port. The value is a number consisting of 1 to 30 digits. An intra-office user can dial the outgoing prefix to make an

Parameter	Description
	<p>outgoing call through the FXO port. Assume that the outgoing prefix is 0 and the number of an outer-office user is 12345678. To call this user, an intra-office user dials 12345678.</p> <p>NOTE</p> <ul style="list-style-type: none"> • A maximum of 16 outgoing prefixes can be configured for the FXO port on the EGW1520. An intra-office user can use any one of the outgoing prefixes to make an outgoing call through the FXO port. • The outgoing prefix cannot conflict with internal numbers and emergency numbers. If an internal number is the same as the outgoing prefix plus an outer-office number, the internal user is connected.
Delete	<ul style="list-style-type: none"> • Yes: The outgoing prefix is deleted for outgoing calls. Assume that the outgoing prefix is 0 and the number of an outer-office user is 12345678. To call this user, an intra-office user dials 012345678. • No: The outgoing prefix is not deleted for outgoing calls. This mode is applicable to the situation where the outgoing prefix is the same as the first digit in the outer-office number. Assume that the outgoing prefix is 1 and the number of an outer-office user is 12345678. To call this user, an intra-office user dials 12345678. <p>NOTE</p> <p>The number that the PSTN carrier allocates to the FXO port is displayed to the called party.</p>

Step 4 Click  to save the settings.

----End

Verification

Step 1 An intra-office user dials the outgoing prefix for the FXO port (for example, 0) and the number of an outer-office user.

Step 2 The outer-office user answers the call.

----End

Verify that the call is set up successfully; otherwise, check the configuration.

Configuring the Switchboard

This topic describes how to configure the switchboard on the EGW1520.

Prerequisite

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

Background

For details about the application scenario and call process for the switchboard, see [Description](#).

NOTE

- The switchboard function conflicts with the DDI and dedicated line functions. If the DDI or dedicated line function is enabled, choose **Voice > FXO Configuration** and delete the binding number on the **FXO Toggle** tab page before configuring the switchboard function.
- The switchboard takes effect automatically after the dedicated line is disabled. No special configuration is required. The following describe how to configure an attendant number. If you do not need to configure an attendant number, skip the following procedure.
- Default voice prompts are loaded on the EGW1520 before delivery. To customize voice prompts, see [Customizing Voice Prompts for the Switchboard](#).

Procedure

NOTE

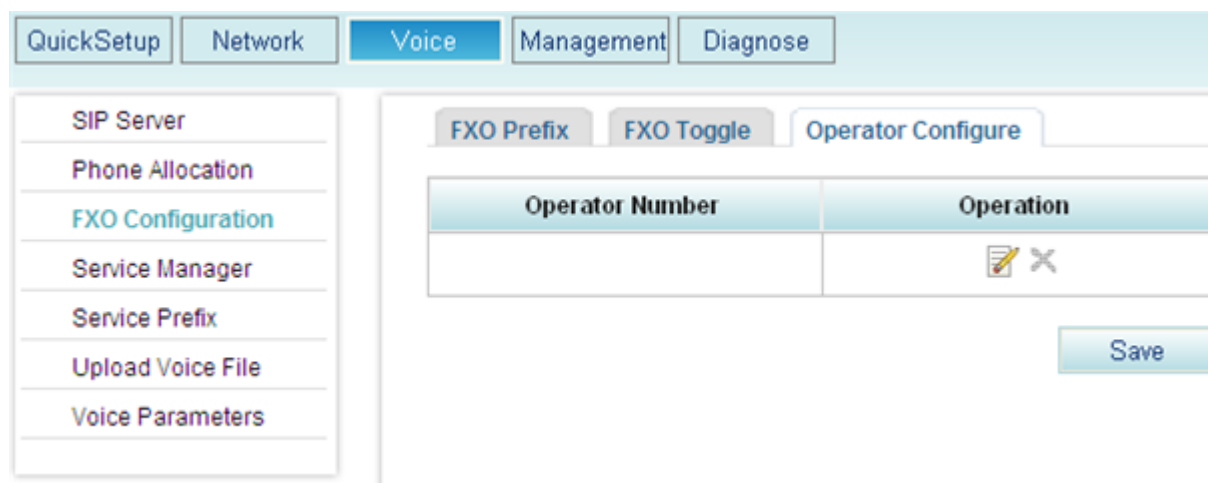
If you want to make an outgoing call, configure an outgoing prefix when you configure the switchboard. For the configuration method, see [Configuring an Outgoing Prefix](#).

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

Step 2 Click the **Operator Configure** tab.

The page shown in [Figure 7-166](#) is displayed.

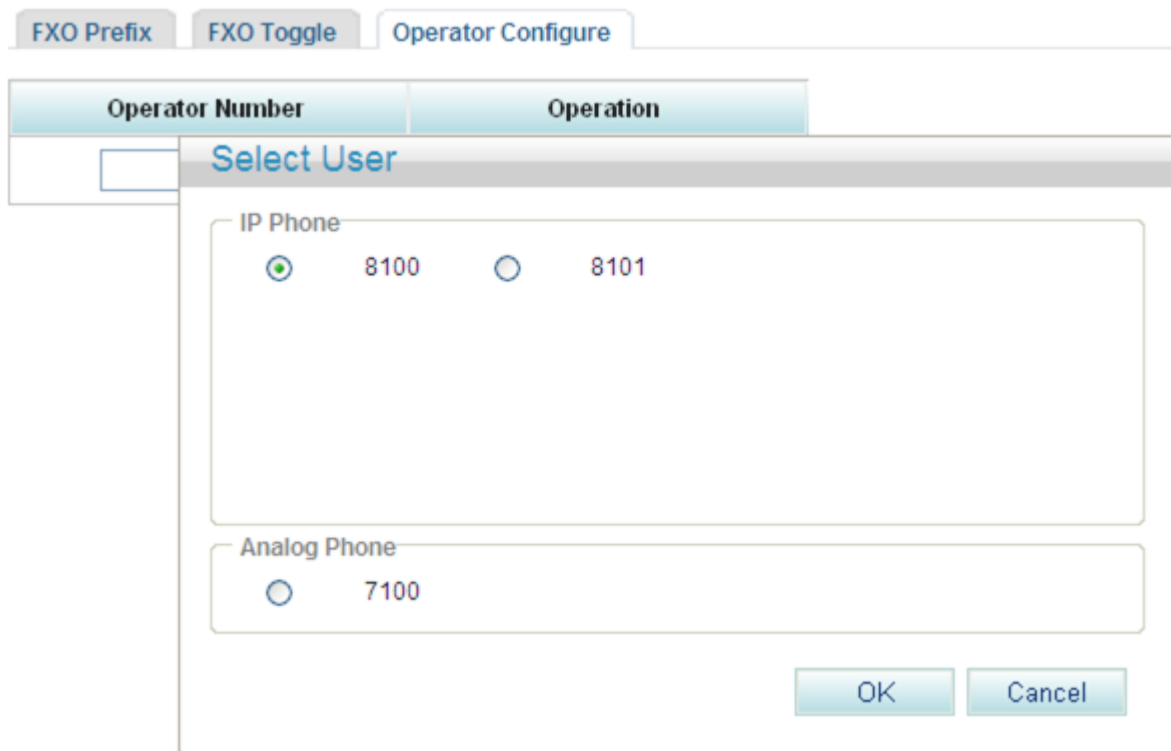
Figure 7-166 Configuring an attendant




Step 3 Click .

The page shown in [Figure 7-167](#) is displayed.

Figure 7-167 Selecting a user



Step 4 Select an internal number as the attendant number, and click .

For details about how to add an internal number, see [Adding Voice Users](#).

Step 5 Click  to save the settings.

----End

Verification

Incoming call

Step 1 An outer-office user dials the number that the PSTN network carrier allocates to the FXO port, that is, the switchboard number.

Step 2 The outer-office user dials an extension number (internal number) or dials 9 (to connect to the preset attendant number) as prompted, and presses the pound key (#).

Step 3 The intra-office user or attendant answers the call.

----End

Verify that the call is set up successfully; otherwise, check the configuration.

Outgoing call

Step 1 An intra-office user dials the outgoing prefix for the FXO port (for example, 0) and the number of an outer-office user.

Step 2 The outer-office user answers the call.

----End

Verify that the call is set up successfully; otherwise, check the configuration.

Configuring the DDI and Dedicated Line

This topic describes how to configure the DDI and dedicated line on the EGW1520.

Prerequisite

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

Background

For details about the application scenario and call process for the DDI and dedicated line, see [Description](#).

NOTE

The priority of the DDI or dedicated line is higher than that of the switchboard. When the DDI or dedicated line is configured, the switchboard automatically becomes invalid.

Procedure

NOTE

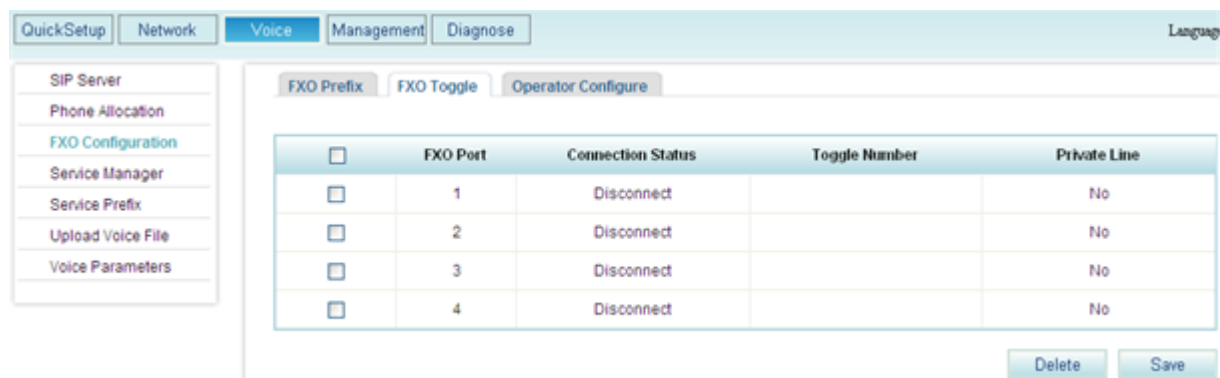
If you want to make an outgoing call, configure an outgoing prefix when you configure the DDI and dedicated line. For the configuration method, see [Configuring an Outgoing Prefix](#).

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

Step 2 Click the **FXO Toggle** tab.

The page shown in [Figure 7-168](#) is displayed.

Figure 7-168 Configuring the FXO binding number



Step 3 Select the FXO port you want to configure, set parameters according to [Table 7-38](#).

Table 7-38 Configuring the DDI and dedicated line

Parameter	Description
Toggle Number	Internal number bound to the FXO port. NOTE For details about how to add an internal number, see Adding Voice Users .
Private Line	Indicates whether to enable the dedicated line function.

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

Verification

Incoming call

- Step 1** An outer-office user dials the number that the PSTN network carrier allocates to the FXO port.
- Step 2** The phone of the intra-office user whose number is bound to the FXO port rings.
- Step 3** The intra-office user answers the call.
----End

Verify that the call is set up successfully; otherwise, check the configuration.

Outgoing call

- Step 1** The intra-office user whose number is bound to the FXO port dials the outgoing prefix for the FXO port (for example, 0) and the number of an outer-office user.
- Step 2** The outer-office user answers the call.
----End

Verify that the call is set up successfully; otherwise, check the configuration.

7.4.3 Power-off Survival

The FXO1 port of the EGW1520 can be used as a power-off survival port. When the EGW1520 is powered off, the analog phone connected to the PHONE port can be connected to the PSTN through the FXO1 port.

Principle and Implementation

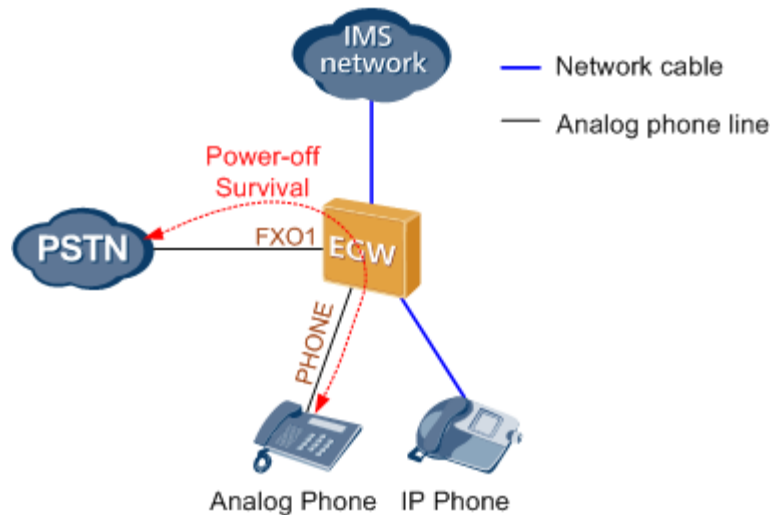
When the EGW1520 is powered off, the PHONE port automatically connects to the FXO1 port.

Generally, the EGW1520 power-off survival function is available once the cables are connected. You do not need to configure the function on the web management system. The cables are connected as follows:

- The FXO1 port on the EGW1520 has been connected to the PSTN.
- An analog phone has been connected to the PHONE port on the EGW1520.

When the EGW1520 is powered off, it automatically connects the analog phone connected to the PHONE port to the PSTN, as shown in [Figure 7-169](#).

Figure 7-169 Power-off survival



NOTE

- When the power-off survival function is enabled, the number of the analog phone connected to the PHONE port changes from the external number to the FXO1 port number, and the dialing rule changes from the EGW1520 dialing rule to the PSTN dialing rule.
- After the power-off survival function is enabled, the ongoing call does not end after the EGW1520 powers on again, but the voice services cannot be used until the call ends.
- After the power-off survival function is enabled, the FXO switchboard, DDI, and dedicated line functions cannot be used.

To verify that the power-off survival function is enabled, perform the following steps:

1. Cut the power supply of the EGW1520.
2. Use an analog phone that is connected to the PHONE port to call an external number.

If the call is connected, the power-off survival function is enabled. If the call is disconnected, check the connections between the PHONE port and the analog phone, and between the EGW1520 FXO1 port and the PSTN.

Specification

One PSTN Power-off survival port.

Limitation

- The Power-off survival function is available only when a power off occurs.
- Only the Analog Phone that connects to the PHONE port supports Power-off survival function.

7.4.4 Fax Service

The EGW1520 supports fax service.

Fax is a form of telegraphy for the transmission of fixed images with a view to their reproduction in a permanent form. In ITU-RV.662, faxing is defined as a form of telecommunication for the reproduction at a distance of graphic documents in the form of other graphic documents geometrically similar to the original.

Description

This topic describes the principle, implementation, specification, and limitation of the fax service.

By transmission rate, faxes are divided into low-speed faxes (≤ 14.4 kbit/s) and high-speed faxes (> 14.4 kbit/s).

Low-speed faxes on an IP network are divided into transparently transmitted faxes (using G.711A or G.711u) and T.38 faxes. High-speed faxes, however, can only use G.711A or G.711u featuring low compression rate due to the requirement for high quality.

The EGW1520 supports T.38 and transparent fax.

Principle

The fax service establishes a voice channel and switches the voice channel to a fax channel, including the IP address, port, codec, and channel types (audio, fax, and data).

The voice channel is switched to a fax channel after the access device detects fax signals. The access device checks fax signals to determine whether the current fax is a high-speed or low-speed fax, and then delivers the fax signals to the NGN or IMS.

The EGW1520 supports T.38 and transparent fax.

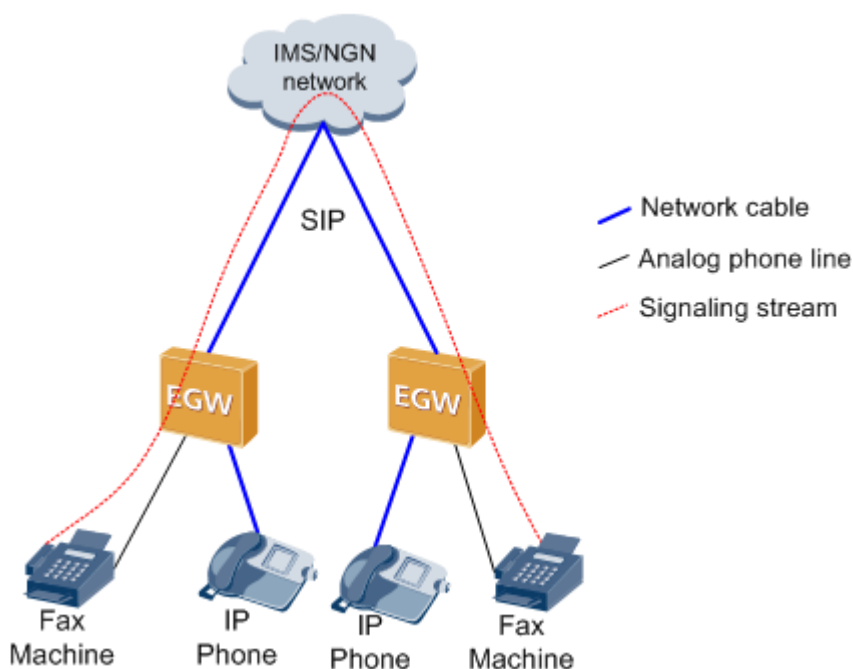
Transparent fax: Fax signals are transmitted transparently as G.711 packets. G.711 faxes feature low delay and simple implementation, but they occupy a high bandwidth (fixed at 64 kbit/s) and are easily affected by network conditions. Therefore, G.711 faxes are recommended on a good network condition and not recommended when network jitter or packet loss frequently occur. G.711 faxes are applicable to high-speed and low-speed faxes.

T.38 fax: T.30 fax signals are converted to T.38 packets for transmission on a packet switching network. T.38 faxes occupy a low bandwidth, provide high reliability with redundant frames and forward error checking (FEC), and are slightly affected by the network condition. However, the implementation is complicated. T.38 faxes are applicable only to low-speed fax services due to delay generated by the packet switching network.

Implementation

When a fax machine connected to the EGW1520 communicates with an outer-office machine, the NGN or IMS controls the call process. [Figure 7-170](#) shows the network diagram.

Figure 7-170 EGW1520 outer-office faxing



The NGN or IMS controls call signaling. The EGW1520 detects fax signals and encodes and decodes IP voice packets. After a fax call is established, fax media streams are transmitted over an IP network. The process for making a fax call is similar to that for making an inter-office call. After the fax call is complete, the EGW1520 detects the fax ending signals and sends them to the NGN or IMS. The NGN or IMS negotiates with the calling and called users about the fax media information. After the negotiation is successful, the EGW1520 switches to the fax channel according to the NGN or IMS's signaling to establish a fax call. After the fax call is complete, the EGW1520 detects the fax ending signals and sends them to the NGN or IMS. Then the NGN or IMS switches to the voice channel.

Specification

Standards supported by fax service:

- One FXS ports for fax machines
- T.30
- T.38
- V.17/V.21/V.27/V.29/V.34

Limitation

N/A

Configuring the Fax Service

Generally, the EGW1520 faxing function is available once the cables are connected, you do not need to configure the function on the web management system. This topic describes how to set the advanced parameters for faxing.

Prerequisites

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

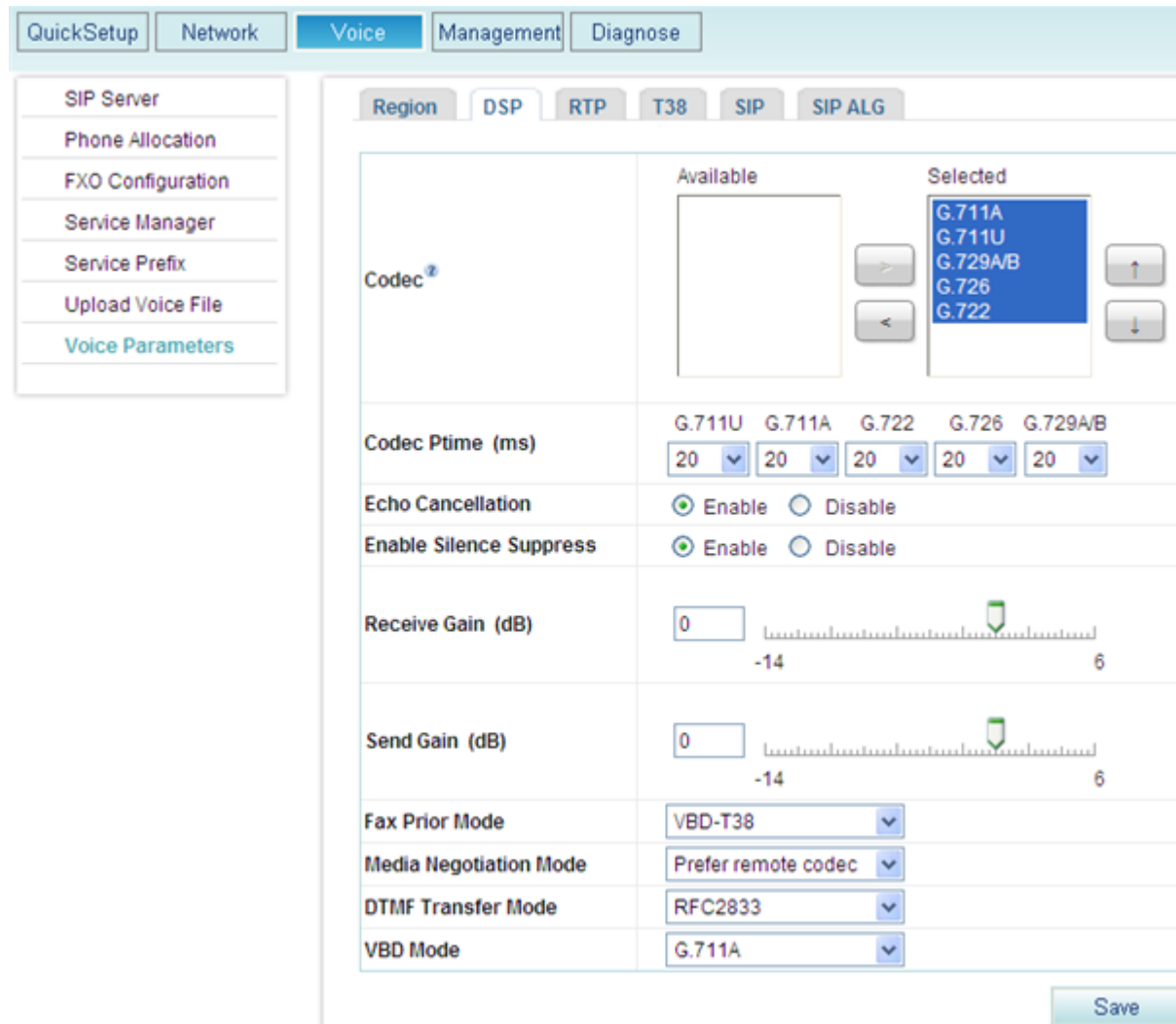
Configuring the Priority

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

Step 2 Click the **DSP** tab.

The page shown in [Figure 7-171](#) is displayed.

Figure 7-171 DSP tab page




Step 3 Set parameters according to [Table 7-39](#).

Table 7-39 DSP parameters

Parameter	Description
Codec	DSP codec type. If multiple options are selected, the system sends messages based on the specified codec rank. By default, all options are selected. NOTE Compared with other codec types, G729, G726, and G722 consume more DSP resources.
Codec Ptime (ms)	For each codec type, you can change the duration of packaging voice streams to 10 ms, 20 ms, or 30 ms. The default value is 20 ms.
Echo Cancellation	Indicates the echo cancellation switch. The options are Enable and Disable , and the default value is Enable . The high-speed transparent transmission mode has the echo processing mechanism. You are advised to disable the echo cancellation function for the high-speed transparent transmission mode and enable this function for low-speed transparent transmission mode.
Enable Silence Suppress	Indicates the silence suppression switch. The options are Enable and Disable . The default value is Enable , which indicates that the system sends silence packets if no voice packet is available.
Receive Gain (dB)	Indicates the receiving gain of DSP chips. The value ranges from -14 to 6. The default value is 0 .
Send Gain (dB)	Indicates the sending gain of DSP chips. The value ranges from -14 to 6. The default value is 0 .
Fax Prior Mode	Indicates the fax transmission mode. The options are as follows: <ul style="list-style-type: none"> • T38: Only T38 is supported. • VBD: Only voice band data (VBD) is supported. • T38-VBD: Both T38 and VBD are supported, and T38 has a higher priority. • VBD-T38: Both T38 and VBD are supported, and VBD has a higher priority. The default value is VBD-T38 .
Media Negotiation Mode	Indicates the priority used in media negotiation. <ul style="list-style-type: none"> • Prefer remote codec: During media negotiation, the codec priority at the remote end is preferred. • Prefer local codec: During media negotiation, the codec priority at the local end is preferred. The default value is Prefer remote codec .
DTMF Transfer Mode	Indicates the transmission mode in a session. <ul style="list-style-type: none"> • RFC2833: RFC2833 transmission mode. • Transfer: transparent transmission mode. Dialing tones are transmitted transparently as voice signals.

Parameter	Description
	The default value is RFC2833 .
VBD Mode	Indicates the codec type for transparent transmission. The options are G711A and G711U , and the default value is G711A .

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

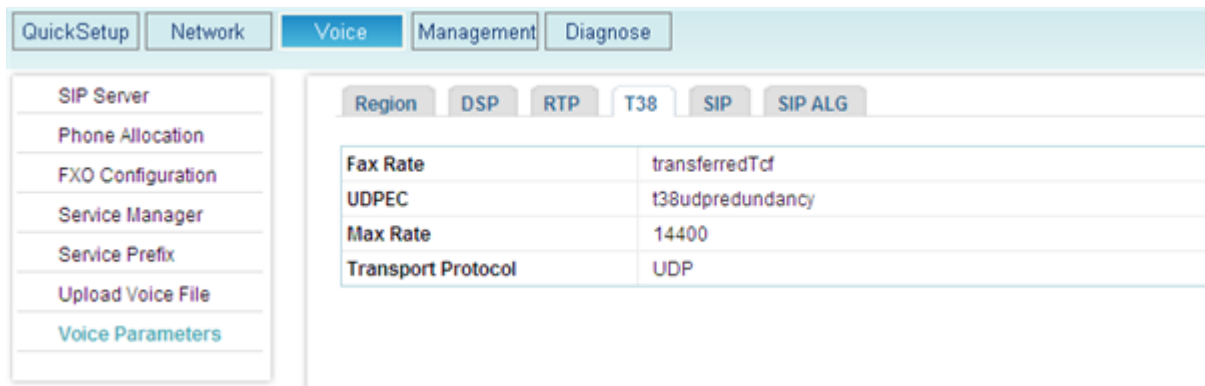
Viewing T38 Fax Parameters

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

Step 2 Click the **T38** tab.

The page shown in [Figure 7-172](#) is displayed.

Figure 7-172 T38 tab page



Step 3 Set parameters according to [Table 7-40](#).

Table 7-40 T.38 fax parameters

Parameter	Description
Fax Rate	Indicates the faxing rate mode. Value transferredTcf indicates remote training mode.
UDPEC	Indicates the UDP redundancy correction capability. The EGW1520 supports t38udpredundancy . If the redundancy correction capability is carried in fax negotiation signals, the EGW1520 uses the redundancy technology to send T38 data when the peer end also supports redundancy.
Max Rate	Indicates the maximum faxing rate. If the maximum faxing rate at the peer end is smaller than that at the local end, use the smaller one; otherwise, use the value of this parameter.

Parameter	Description
Transport Protocol	Indicates the transmission protocol. The EGW1520 supports UDP.

----End

7.4.5 Voice Parameters

This topic describes how to set voice parameters. Only network administrators can change the parameter settings. To ensure the normal running of the EGW1520, you are advised to use the default settings.

Prerequisites

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

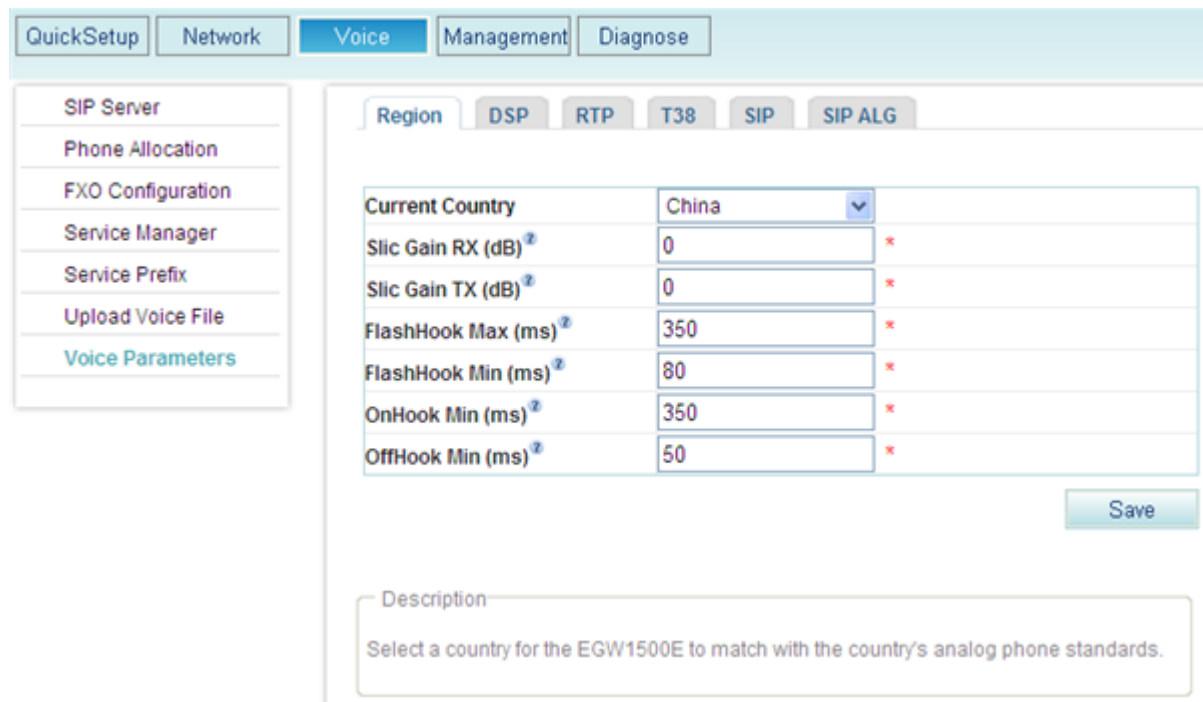
Configuring the Region

On the **Region** tab page, specify analog phone standards in different countries. Dialing tones and signal tone frequency vary according to area and country. Configure the parameters based on requirement.

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

The page shown in [Figure 7-173](#) is displayed.

Figure 7-173 Region tab page



The screenshot displays the 'Region' configuration page in a web management system. At the top, there are tabs for 'QuickSetup', 'Network', 'Voice', 'Management', and 'Diagnose'. Below these, a sub-menu includes 'SIP Server', 'Phone Allocation', 'FXO Configuration', 'Service Manager', 'Service Prefix', 'Upload Voice File', and 'Voice Parameters'. The 'Region' tab is active, showing a table of parameters:


Parameter	Value	Validation
Current Country	China	
Slic Gain RX (dB)	0	*
Slic Gain TX (dB)	0	*
FlashHook Max (ms)	350	*
FlashHook Min (ms)	80	*
OnHook Min (ms)	350	*
OffHook Min (ms)	50	*

A 'Save' button is located at the bottom right of the parameter table. Below the table, there is a 'Description' field with the text: 'Select a country for the EGW1500E to match with the country's analog phone standards.'

Step 2 Set parameters according to [Table 7-41](#).

Table 7-41 Region parameters

Parameter	Description
Current Country	Country name.
Slic Gain RX (dB)	Receiving gain of an analog phone. The value ranges from -12 dB to +6 dB.
Slic Gain TX (dB)	Sending gain of an analog phone. The value ranges from -12 dB to +6 dB.
FlashHook Max (ms)	Maximum interval for pressing the hook flash button. The value ranges from 0 to 1000, in milliseconds. If the hook flash button is not pressed within the duration specified by this parameter, the call will end.
FlashHook Min (ms)	Minimum interval for pressing the hook flash button. The value ranges from 0 to 1000, in milliseconds. If the interval is smaller than the value of this parameter, the hook flash operation does not take effect.
OnHook Min (ms)	Minimum interval for confirming hang-up. The value ranges from 0 to 2000, in milliseconds. If the hang-up interval is smaller than the value of this parameter, the hang-up operation does not take effect.
OffHook Min (ms)	Minimum interval for confirming pickup. The value ranges from 0 to 2000, in milliseconds. If the pickup interval is smaller than the value of this parameter, the pickup operation does not take effect.

Step 3 Click  to save the settings.

----End

Configuring the DSP

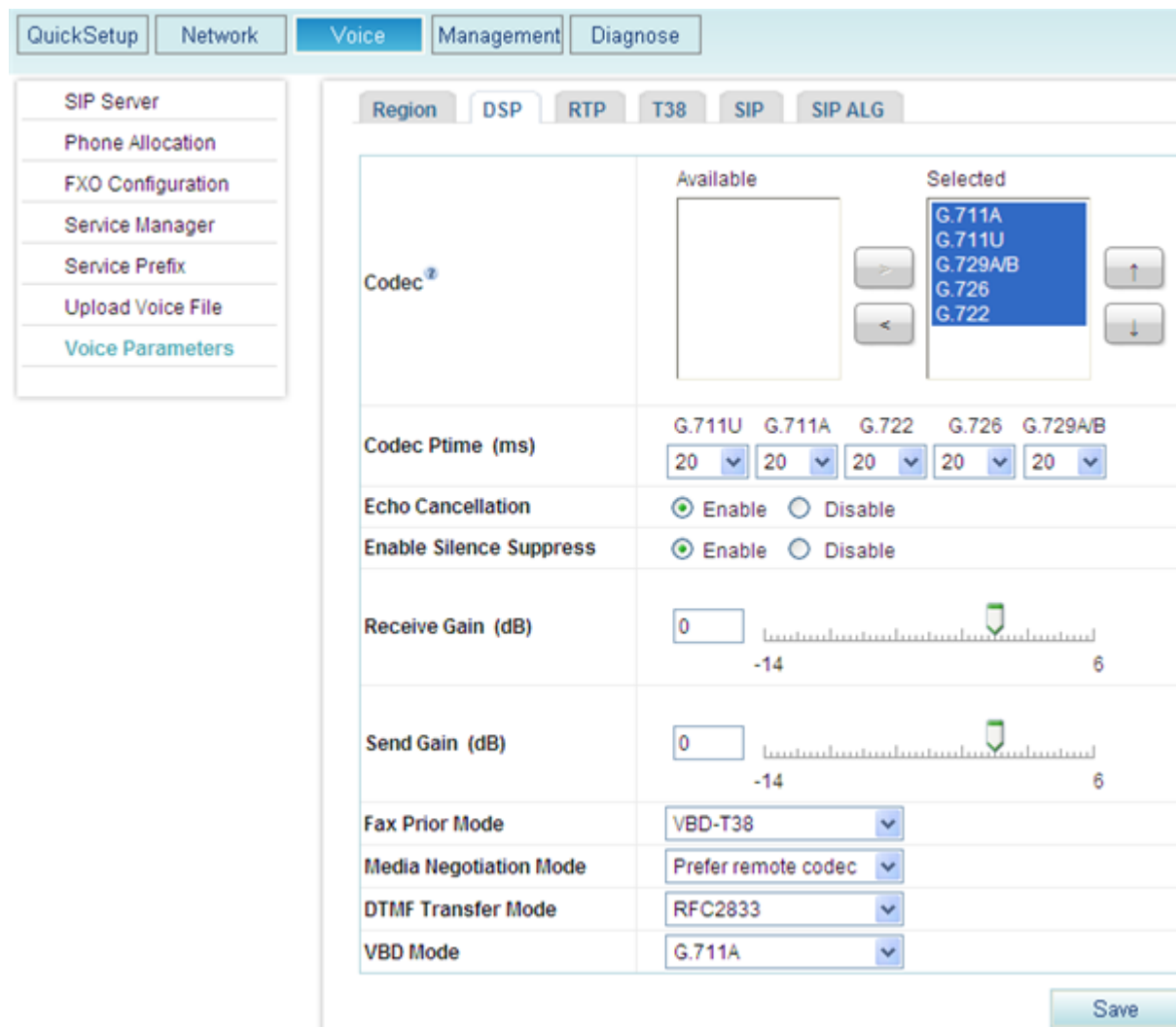
On the **DSP** tab page, configure voice quality information about DSP chips, such as codec type, noise and echo cancellation, silence suppression, and gains.

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

Step 2 Click the **DSP** tab.

The page shown in [Figure 7-174](#) is displayed.

Figure 7-174 DSP tab page




Step 3 Set parameters according to [Table 7-42](#).

Table 7-42 DSP parameters

Parameter	Description
Codec	DSP codec type. If multiple options are selected, the system sends messages based on the specified codec rank. By default, all options are selected. NOTE Compared with other codec types, G729, G726, and G722 consume more DSP resources.
Codec Ptime (ms)	For each codec type, you can change the duration of packaging voice streams to 10 ms, 20 ms, or 30 ms. The default value is 20 ms.
Echo Cancellation	Echo cancellation switch. The options are Enable and Disable , and the default value is Enable .

Parameter	Description
Enable Silence Suppress	Silence suppression switch. The options are Enable and Disable . The default value is Enable , which indicates that the system sends silence packets if no voice packet is available.
Receive Gain (dB)	Receiving gain of DSP chips. The value ranges from -14 to 6. The default value is 0 .
Send Gain (dB)	Sending gain of DSP chips. The value ranges from -14 to 6. The default value is 0 .
Fax Prior Mode	Fax transmission mode. The options are as follows: <ul style="list-style-type: none"> • T38: Only T38 is supported. • VBD: Only voice band data (VBD) is supported. • T38-VBD: Both T38 and VBD are supported, and T38 has a higher priority. • VBD-T38: Both T38 and VBD are supported, and VBD has a higher priority. The default value is VBD-T38 .
Media Negotiation Mode	Priority used in media negotiation. <ul style="list-style-type: none"> • Prefer remote codec: During media negotiation, the codec priority at the remote end is preferred. • Prefer local codec: During media negotiation, the codec priority at the local end is preferred. The default value is Prefer remote codec .
DTMF Transfer Mode	Transmission mode in a session. <ul style="list-style-type: none"> • RFC283: RFC2833 transmission mode. • Transfer: transparent transmission mode. Dialing tones are transmitted transparently as voice signals. The default value is RFC2833 .
VBD Mode	Codec type for transparent transmission. The options are G711A and G711U , and the default value is G711A .

Step 4 Click  to save the settings.

----End

Configuring RTP

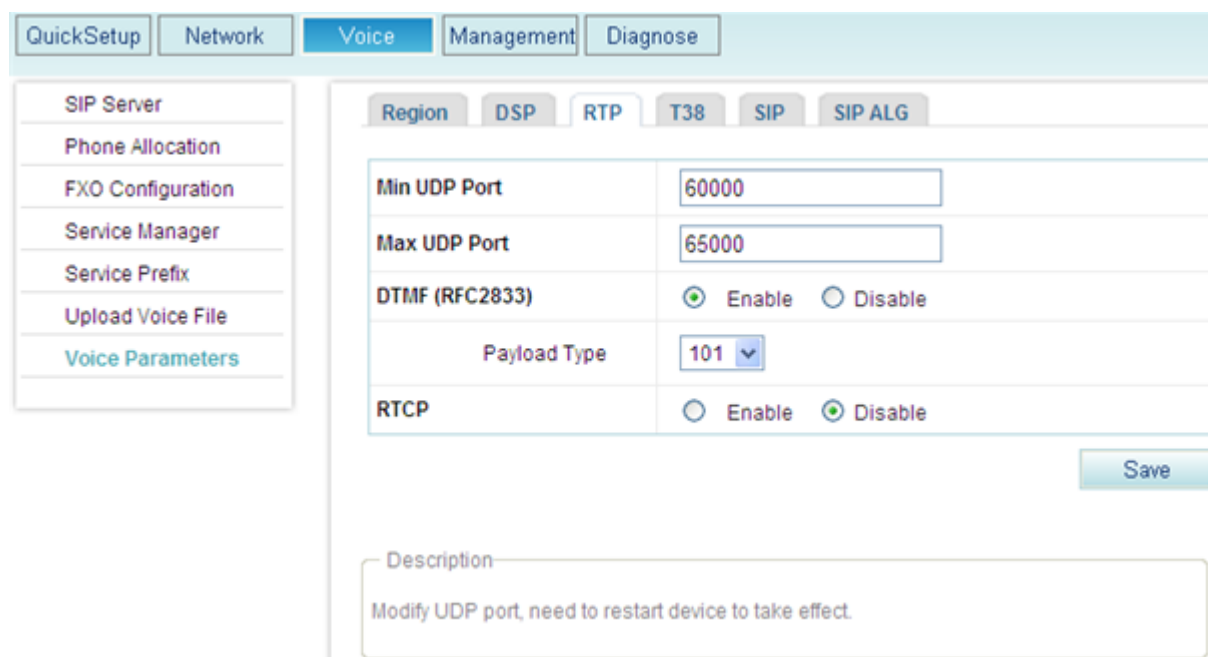
On the **RTP** tab page, set the parameters used for playing voices on analog phones such as the maximum and minimum media port numbers.

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

Step 2 Click the **RTP** tab.

The page shown in [Figure 7-175](#) is displayed.

Figure 7-175 RTP tab page




Step 3 Set parameters according to [Table 7-43](#).

Table 7-43 RTP parameters

Parameter	Description
Min UDP Port	Minimum media port number used for playing voices on analog phones.
Max UDP Port	Maximum media port number used for playing voices on analog phones.
DTMF (RFC2833)	Whether RFC2833 is used for encryption. The options are Enable and Disable . Payload Type: payload for RFC2833 used for encryption. The value must be unique on the EGW1520. It is recommended that you set this parameter to the payload type of the softswitch. If the parameter value is different from that on the softswitch, call connections may fail to be set up.
RTCP	Whether to enable the RTCP function. The options are Enable and Disable . The default value is Disable .

NOTE

After changing the UDP port number, restart the device to make the configuration take effect.

Step 4 Click  to save the settings.

----End

Viewing T38 Fax Parameters

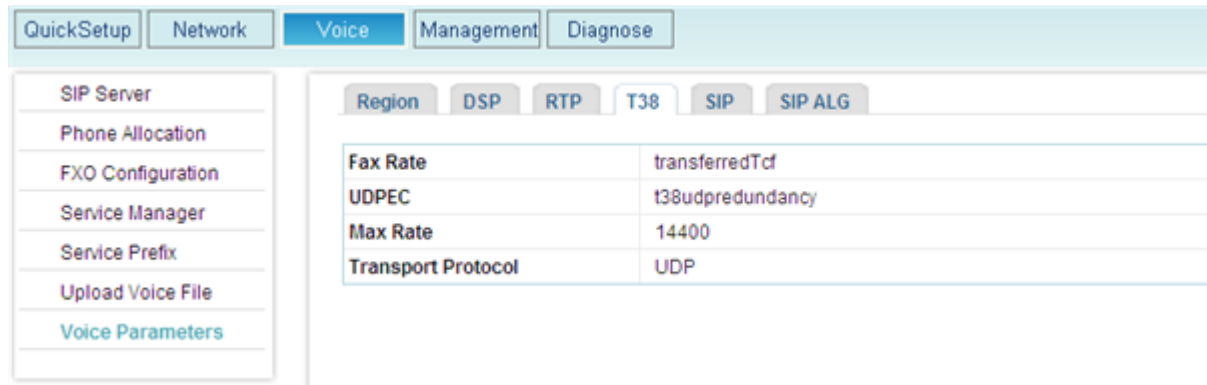
On the **T38** tab page, you can view T.38 fax parameters.

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

Step 2 Click the **T38** tab.

The page shown in [Figure 7-176](#) is displayed.

Figure 7-176 T38 tab page



Step 3 Set parameters according to [Table 7-44](#).

Table 7-44 T38 fax parameters

Parameter	Description
Fax Rate	Faxing rate mode. Value transferredTcf indicates remote training mode.
UDPEC	UDP redundancy correction capability. The EGW1520 supports t38udpredundancy . If the redundancy correction capability is carried in fax negotiation signals, the EGW1520 uses the redundancy technology to send T38 data when the peer end also supports redundancy.
Max Rate	Maximum faxing rate. If the maximum faxing rate at the peer end is smaller than that at the local end, use the smaller one; otherwise, use the value of this parameter.
Transport Protocol	Transmission protocol. The EGW1520 supports UDP.

----End

Configuring SIP

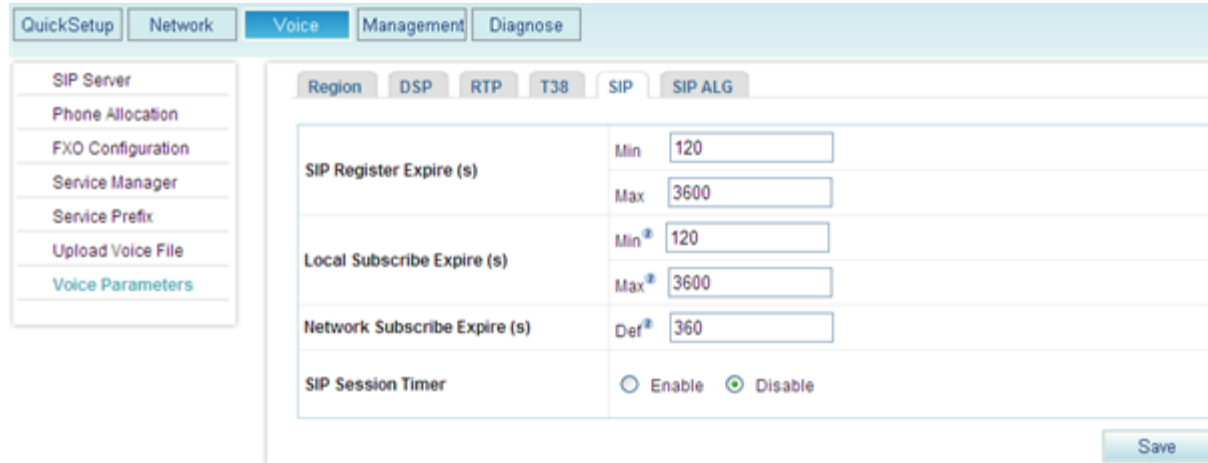
On the **SIP** tab page, configure the timeout interval for local SIP users to register with the EGW1520.

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

Step 2 Click the **SIP** tab.

The page shown in [Figure 7-177](#) is displayed.


Figure 7-177 SIP tab page



Step 3 Set parameters according to [Table 7-45](#).

Table 7-45 SIP parameters

Parameter	Description
SIP Register Expire (s)	Timeout interval for local SIP users to register with the EGW1520. <ul style="list-style-type: none"> Min: Minimum timeout interval for local SIP users to register with the EGW1520. The default value is 120. Max: Maximum timeout interval for local SIP users to register with the EGW1520. The default value is 3600.
Local Subscribe Expire (s)	Timeout interval for local SIP users to subscribe to a service (such as voice message and voice mailbox) with the EGW1520 <ul style="list-style-type: none"> Min: Minimum timeout interval for local SIP users to subscribe to a service with the EGW1520. The default value is 120. Max: Maximum timeout interval for local SIP users to subscribe to a service with the EGW1520. The default value is 3600.
Network Subscribe Expire (s)	Default timeout interval for the EGW1520 to subscribe to a service with the NGN or IMS.
SIP Session Timer	Whether to use the session timer. The session timer is disabled by default. When the session timer is enabled, the two parties can check the conversation status using the update or reinvite signaling.

Step 4 Click  to save the settings.

----End

Configuring SIP ALG

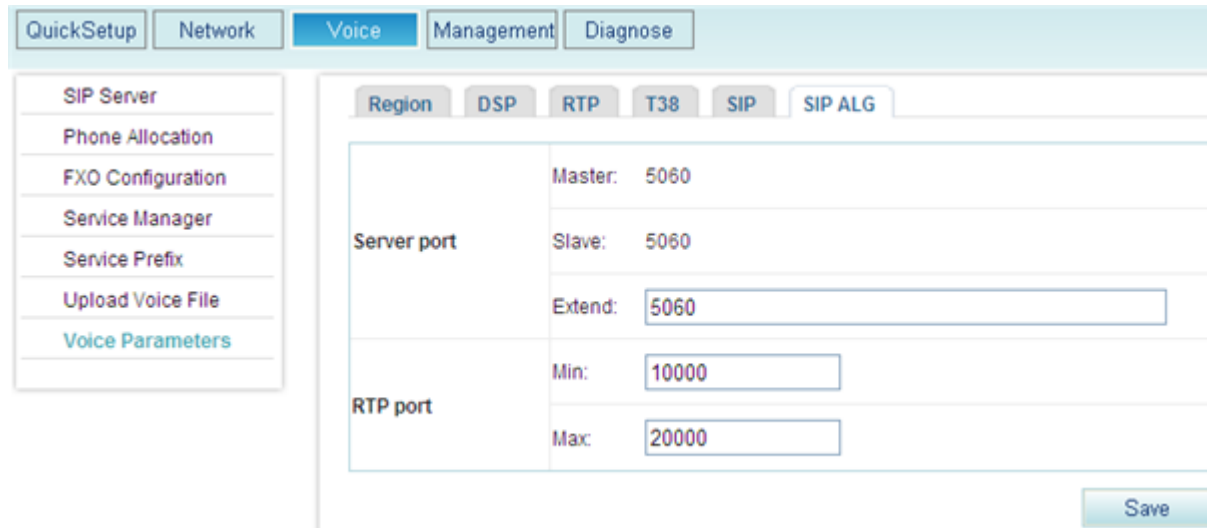
On the **SIP ALG** tab page, configure SIP servers in an outer office.

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

Step 2 Click the **SIP ALG** tab.

The page shown in [Figure 7-178](#) is displayed.


Figure 7-178 SIP ALG tab page



Step 3 Set parameters according to [Table 7-46](#).

Table 7-46 SIP ALG parameters

Parameter	Description
Server port	<ul style="list-style-type: none"> • Master: Port number used by the active SIP server to send and receive packets. • Slave: Port number used by the standby SIP server to send and receive packets. • Extended: Extended port number used by the SIP ALG to send and receive packets.
RTP port	<ul style="list-style-type: none"> • Min: Minimum media port that can be used by the RTP server. • Max: Maximum media port that can be used by the RTP server.

Step 4 Click  to save the settings.

----End

7.5 Data

This topic describes EGW1520 data features and how to configure the features.

7.5.1 LAN

The EGW1520 provides four LAN ports to connect terminals such as computers and IP phones. In addition, the EGW1520 can function as a Dynamic Host Configuration Protocol (DHCP) server to allocate private IP addresses to terminals. After network address translation (NAT), terminals are connected to the IP network and the IP network connects the terminals to the Internet or IMS/NGN.

Description

This topic describes the principle, implementation, specification, and limitation of LAN ports.

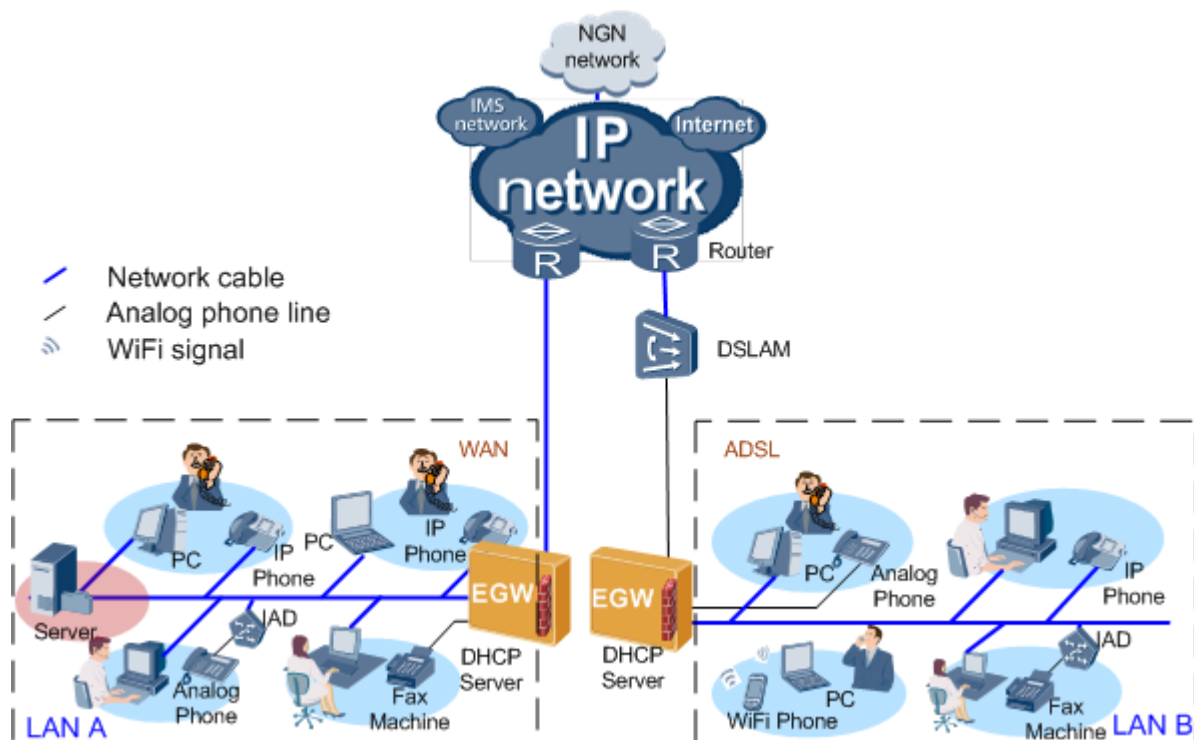
Principle

The EGW1520 complies with IEEE802.3u 100Base-T.

Implementation

The EGW1520 provides four LAN ports to connect terminals such as computers and IP phones, as shown in [Figure 7-179](#). The EGW1520 can function as a DHCP server to allocate private IP addresses to terminals. After NAT, terminals are connected to the IP network and the IP network connects the terminals to the Internet, IMS, or NGN.

Figure 7-179 LAN diagram



For details about the DHCP server and trunk, see the [DHCP Feature Description](#).

Specification

- Four 10/100 Mbit/s self-adaptive LAN ports.
- Default IP address of LAN ports: 192.168.1.1; subnet mask: 255.255.255.0.
- DHCP server function, allocating IP addresses to computers and IP phones that connect to LAN ports.
- Standards supported by LAN ports:
 - MAC Address (IEEE 802.3)
 - IPv4 Internet Protocol v4 (RFC 791)
 - ARP Address Resolution Protocol (RFC 826)
 - ICMP Internet Control Message Protocol (RFC 792)
 - An Ethernet Address Resolution Protocol (RFC 0826)
 - A Standard for the Transmission of IP Datagrams over Ethernet Networks (RFC 0894)
 - A Standard for the Transmission of IP Datagrams over IEEE 802 Networks (RFC 1042)
 - DHCP (RFC 2131), TCP Transmission Control Protocol (RFC 793)
 - UDP User Datagram Protocol (RFC 768)

Limitation

- The LAN port supports half-duplex and full-duplex self adaptation, but cannot be forced to use full duplex or half duplex.
- IPv6 is not supported.

Configuration

This topic describes how to configure a LAN.

Prerequisites

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

Background

LAN configuration for the EGW1520 includes:

- Set the IP address of the LAN gateway. For details, see [Setting the IP Address of the LAN Gateway](#).
- Configure the EGW1520 as the DHCP server or DHCP relay. For details, see [Configuring the DHCP Server](#) and [Configuring the DHCP Relay](#).

Setting the IP Address of the LAN Gateway

Terminals such as PCs and IP phones use the IP address of the LAN gateway to communicate with other networks and to connect to the EGW1520.

The default IP address of the LAN gateway is **192.168.1.1**.

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

The page shown in [Figure 7-180](#) is displayed.

Figure 7-180 Setting the IP address of the LAN gateway



Step 2 Set parameters according to [Table 7-47](#).

Table 7-47 Parameter description

Parameter	Description
IP Address	Indicates the IP address of the LAN gateway. Terminals use it to connect to the LAN port on the EGW1520. The default value is 192.168.1.1 . You can change this value. CAUTION <ul style="list-style-type: none"> The IP addresses of the LAN gateway, ADSL port, and WAN port cannot be on the same network segment. The IP address of the LAN gateway cannot conflict with that of any other device on the same network segment.
Subnet Mask	Indicates the subnet mask of the IP address of the LAN gateway. The default value is 255.255.255.0 .
Web Access Mode	Indicates the protocol that is used to access the web page of the EGW1520. <ul style="list-style-type: none"> Http: The web browser interacts with the EGW1520 using HTTP. Https: The web browser interacts with the EGW1520 using HTTPS, which ensures user information security. The HTTPS protocol is used by default.
LAN Side Firewall	<ul style="list-style-type: none"> Enable: Enable the firewall on the LAN side.

Parameter	Description
	<p>NOTE</p> <p>When this function is enabled, the firewall blocks all packets that are sent to the upstream network or the EGW1520 over the LAN network. To allow specified packets to pass the firewall, choose Advanced > Security and set related parameters on the Filter incoming IP tab page.</p> <ul style="list-style-type: none"> • Disable: Disable the firewall on the LAN side. <p>By default, this function is disabled.</p>
LAN Side ICMP	<ul style="list-style-type: none"> • Enable: ICMP packets on the LAN side can be sent to the EGW1520. • Disable: ICMP packets on the LAN side cannot be sent to the EGW1520. <p>By default, this function is enabled.</p>

----End

Configuring the DHCP Server

After you configure the EGW1520 as the DHCP server, terminals such as PCs and IP phones that connect to the EGW1520 obtain the IP address information through the EGW1520.

Step 1 Click **Advanced** on the **LAN Setup** page.

The page shown in [Figure 7-181](#) is displayed.

Figure 7-181 Configuring the DHCP server (1)

The screenshot shows the 'LAN Setup' configuration page. The 'Advanced' section is expanded, and the 'Enable DHCP Server' option is selected. The following parameters are configured:

- IP Address: 192.168.1.1
- Subnet Mask: 255.255.255.0
- LAN MAC Address: 00:18:82:ac:16:12
- Web Access Mode: Http Https
- LAN Side Firewall: Enable Disable

In the 'Advanced' section, the 'Enable DHCP Server' option is selected. The following parameters are configured:

- Start IP Address: 192.168.1.2
- End IP Address: 192.168.1.254
- Leased Time (hour): 24

Below these settings is a table for 'Static IP Lease List' with columns for 'MAC Address', 'IP Address', and 'Operation'. An 'Add' button is located below the table.

At the bottom of the page, there is a 'Save' button.

Step 2 Set parameters according to [Table 7-48](#).

Table 7-48 Parameter description

Parameter	Description
Start IP Address	Indicates the start IP address in the address pool. It must be on the same network segment as the LAN gateway. The default value is recommended.
End IP Address	Indicates the end IP address in the address pool. It must be on the same network segment as the LAN gateway. The default value is recommended.
Leased Time (hour)	Indicates the IP address lease interval. If the lease expires and the DHCP client does not renew the lease, the DHCP server releases the IP addresses that are granted to the DHCP client for other clients.

Step 3 (Optional) Allocate IP addresses by binding them with MAC addresses statically.

After configuration, the DHCP server finds the IP address based on the bound MAC address and allocates the IP address to the corresponding DHCP client. This mode is applicable to clients that require a fixed IP address such as the FTP server.


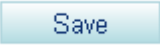
1. Click  .
The page shown in [Figure 7-182](#) is displayed.

Figure 7-182 Configuring the DHCP server (2)



2. Enter the MAC address of the DHCP client and the IP address that you want to bind with the MAC address.
3. Click  to save the settings.

 **NOTE**

- To obtain the MAC address of a PC, choose **Start > Run**, type **cmd**, and press **Enter**. On the command-line interface (CLI) that is displayed, run the **ipconfig /all** command. The value of **Physical Address** corresponding to the 192.168.x.y indicates the MAC address.
- To obtain the MAC address of other network devices such as IP phones, see the related document.

- Step 4** Click  to save the settings.

----End

Configuring the DHCP Relay

If the DHCP server has been deployed but it is on a different network segment from terminals (such as PCs and IP phones), configure the EGW1520 as the DHCP relay. After configuration, the EGW1520 forwards terminals' DHCP requests to the DHCP server. The DHCP server sends the IP address allocation information to the EGW1520, and the EGW1520 forwards the information to terminals.

The DHCP client enables terminals that connect to the EGW1520 and DHCP clients on other networks to use the same DHCP server. This reduces costs and simplifies management.



NOTE

- The DHCP relay conflicts with the NAT function. Before configuring the EGW1520 as the DHCP relay, you must disable the NAT function.
- When configuring the EGW1520 as the DHCP relay, ensure that a reachable route exists between the EGW1520 and DHCP server.

Step 1 Click **Enable DHCP Server Relay**, as shown in [Figure 7-183](#).


Figure 7-183 Configuring the DHCP relay

Enable DHCP Relay

DHCP Server IP Address:

Save

Step 2 Enter the IP address of the DHCP server.

Step 3 Click  to save the settings.

----End

LAN Setting Example (EGW1520 as DHCP Server)

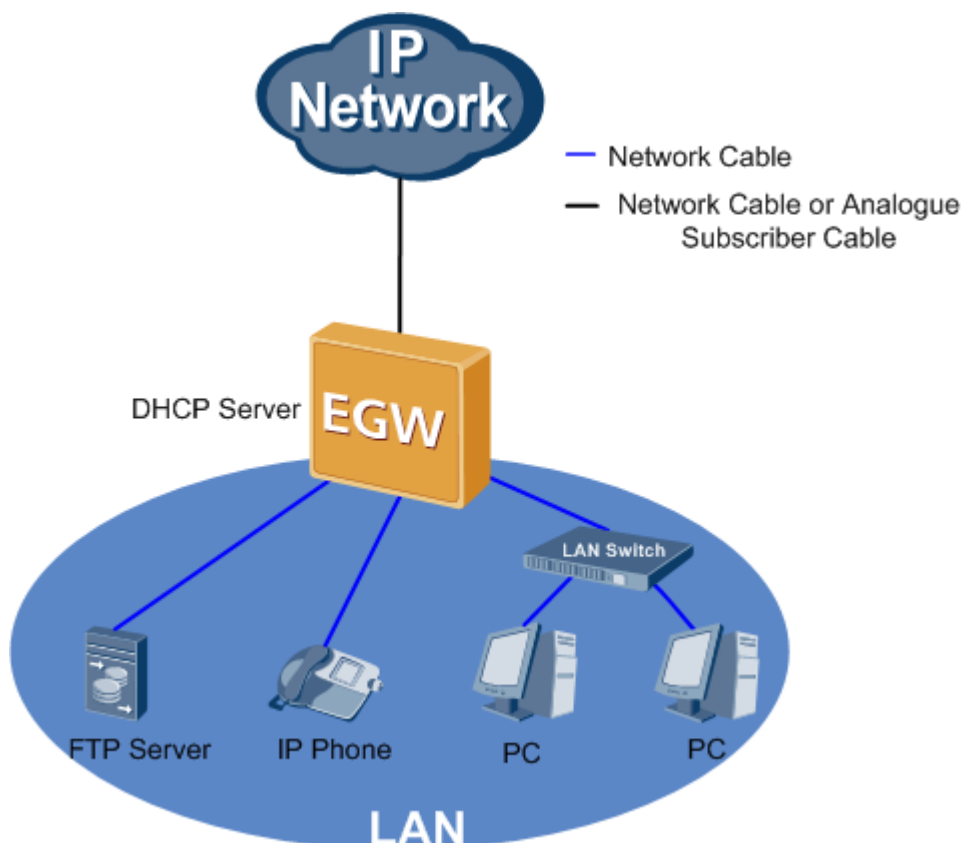
Network Requirements

- PCs use the LAN switch to connect to the LAN port on the EGW1520, while the IP phone and FTP server connect to the LAN port on the EGW1520 directly.
- The EGW1520 functions as the DHCP server and automatically allocates IP addresses for the PCs, IP phone, and FTP server.
- After configuration, the FTP server obtains a fixed IP address, while the IP phone and PCs obtain dynamic IP addresses through the EGW1520.

Typical Network

[Figure 7-184](#) shows the typical network.

Figure 7-184 Typical network (1)



Procedure

- Step 1** Configure that the FTP server, IP phone, and PCs obtain IP addresses automatically. For details, see the related user guide.
- Step 2** Configure the EGW1520 as the DHCP server. For details, see step 1 in [Configuring the DHCP Server](#).
- Step 3** Query and record the MAC address of the FTP server. For details, see [Obtain the MAC address](#).
- Step 4** Allocate the IP address that is bound to the MAC address to the FTP server. For details, see step 2 in [Configuring the DHCP Server](#).

----End

Verification

Verify that the FTP server, PCs, and IP phone have obtained IP addresses and that IP address that the FTP server obtains is bound to its MAC address.

LAN Setting Example (EGW1520 as DHCP Relay)

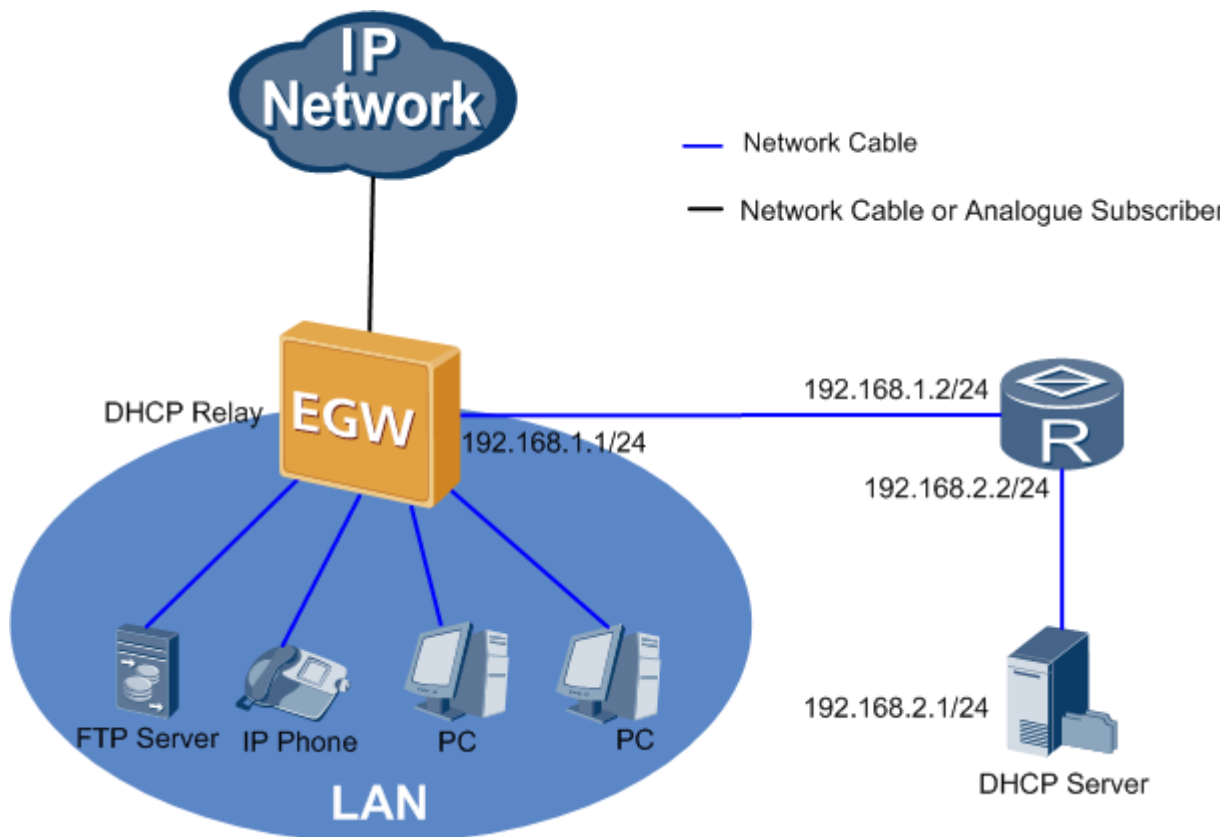
Network Requirements

- The DHCP server (IP address: 192.168.2.1) is deployed on the network. The LAN port on the EGW1520 connects to the DHCP server through a router.
- The PCs, IP phone, and FTP server directly connect to the LAN port on the EGW1520.
- The EGW1520 functions as the DHCP relay and allocates IP addresses for the PCs, IP phone, and FTP server.
- After configuration, the FTP server obtains a fixed IP address, while the IP phone and PCs obtain dynamic IP addresses through the EGW1520.

Typical Network

Figure 7-185 shows the typical network.

Figure 7-185 Typical network (2)



Procedure

- Step 1** Configure that the FTP server, IP phone, and PCs obtain IP addresses automatically. For details, see the related user guide.
- Step 2** Configure the EGW1520 as the DHCP relay, and set the IP address of the DHCP server to 192.168.2.1. For details, see [Configuring the DHCP Relay](#).
- Step 3** Add a static route on the EGW1520, and set the destination network segment to 192.168.2.0/24. For details, see [7.5.5 Static Route](#).
- Step 4** Set the gateway IP address to 192.168.2.2/24 on the DHCP server. For details, see the DHCP server user guide.

Step 5 Add an address pool whose start IP address is 192.168.1.0 and end IP address is 192.168.1.24 for the DHCP server, and allocate the IP address that is bound to the MAC address to the FTP server. For details, see the DHCP server user guide.

----End

Verification

Verify that the FTP server, PCs, and IP phone have obtained IP addresses in the network segment 192.168.1.0/24, and that IP address that the FTP server obtains is bound to its MAC address.

7.5.2 DHCP

Dynamic Host Configuration Protocol (DHCP) is a protocol for dynamically managing and configuring users in a centralized manner. It uses the Client/Server structure. A DHCP client sends the DHCP server a request to apply for parameter settings, including the IP address, subnet mask, and default gateway. Then the DHCP server sends the parameter settings to the DHCP client. The EGW1520 can function as a DHCP server or a DHCP relay to allocate IP addresses to PCs, IP phones, and Wi-Fi terminals that are connected to the EGW1520. The EGW1520 can also function as a DHCP client.

Description

This topic describes the principle, implementation, specification, and limitation of the DHCP.

Principle

Network scales and complexity grow fast, and therefore the network configurations become increasingly complicated. For example, the locations of hosts such as portable computers and wireless terminals frequently change, and the number of hosts often exceeds the number of available IP addresses. The DHCP was developed to solve these problems.

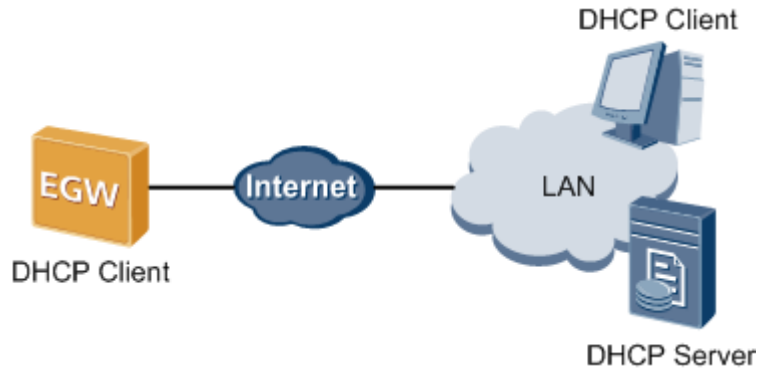
The DHCP uses the Client/Server structure. A DHCP client sends the DHCP server a request to apply for parameter settings. Then the DHCP server sends the parameter settings such as the IP address information to the DHCP client. This achieves dynamic IP address allocation.

Implementation

DHCP client

The EGW1520 can function as a DHCP client and dynamically obtain IP addresses and configuration data from the DHCP server, as shown in [Figure 7-186](#).

Figure 7-186 DHCP client

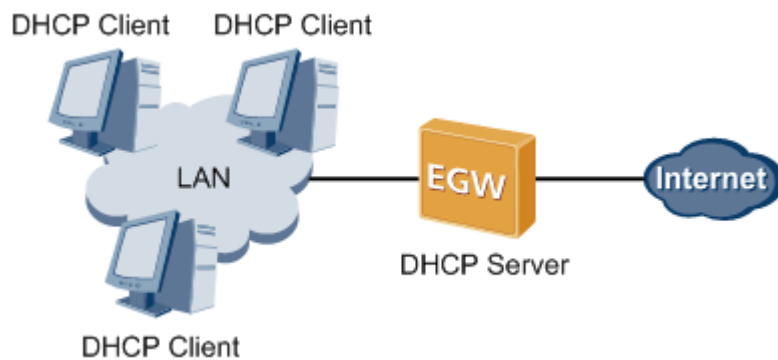


DHCP server

The EGW1520 can also function as a DHCP server, allocating IP addresses to DHCP clients dynamically or statically.

A DHCP client requests an IP address and applies for a lease period for this IP address. During the release period, the DHCP server will not allocate the IP address to another client unless the DHCP client releases the IP address before lease expiration. When the first half of the lease period passes, the DHCP client sends a lease renewal request to the DHCP server. After a negotiation, the DHCP client continues to use this IP address in a new lease period until half of this lease period passes or client releases the IP address, as shown in [Figure 7-187](#).

Figure 7-187 DHCP server



The DHCP server allocates IP addresses to DHCP clients in the following order of priority:

1. IP addresses in the DHCP server's database that are statically bound to DHCP clients' MAC addresses
2. IP addresses allocated to DHCP clients before, namely, IP addresses specified in the **Requested IP Addr Option** field in the DHCP_Discover packet sent by DHCP clients
3. Allocatable IP addresses in the DHCP address pool

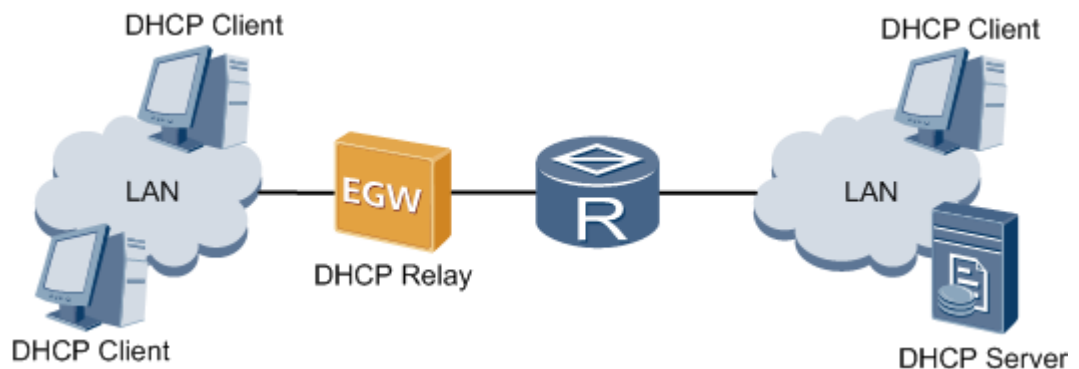
 **NOTE**

If the DHCP address pool has no available IP address, the DHCP server searches timeout and conflicting IP addresses in sequence for an unused IP address, and then allocates the IP address to the DHCP client. If all the IP addresses are used, an error is reported.

DHCP relay

The initial DHCP protocol applies to scenarios where DHCP clients and their DHCP server are on the same network segment. Therefore, to implement dynamic host configuration, you must configure a DHCP server on each network segment, which requires high investment. To solve this problem, you can use the DHCP relay function to connect DHCP clients on different network segments to the only DHCP server. DHCP packets on different network segments are sent to the same target DHCP server or client. By doing so, DHCP clients can use the same DHCP server, which is cost-effective and convenient for centralized management. [Figure 7-188](#) shows a DHCP relay.

Figure 7-188 DHCP relay



The DHCP relay works as follows:

1. After being initialized, the DHCP client broadcasts configuration request packets on the local network.
2. If a DHCP server exists on the local network, the DHCP client communicates with the DHCP server without the DHCP relay.
3. If there is no DHCP server on the local network, a local device enabled with the DHCP relay function processes the broadcast packets, and then forwards the packets to the specified DHCP server on another network.
4. The DHCP server sets parameters in the packets and sends the configuration to the DHCP client through the DHCP relay.

Specification

- As a DHCP server, the EGW1520 can configure an IP address pool. The default IP address ranges from 192.168.1.2 to 192.168.1.254.
- As a DHCP relay, the EGW1520 complies with RFC 3361.
- As a DHCP client, the EGW1520 supports Option42/43/60/61/66/67/120/125/150.

Limitation

N/A

Configuration

This topic describes how to configure the EGW1520 as a DHCP Server, DHCP client, or DHCP Relay.

Prerequisites

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

Configuring the DHCP Client

The EGW1520 uses an ADSL or a WAN port to connect to the IP network. You can configure the EGW1520 as a DHCP client. After configuration, the EGW1520 obtains configurations such as the IP address information from the DHCP server. For details, see [DHCP\(ADSL\)](#) and [DHCP\(WAN\)](#).

Configuring the DHCP Server

After you configure the EGW1520 as the DHCP server, terminals such as PCs and IP phones that connect to the EGW1520 obtain the IP address information through the EGW1520.

Step 1 Click **Advanced** on the **LAN Setup** page.

The page shown in [Figure 7-189](#) is displayed.

Figure 7-189 Configuring the DHCP server (1)

The screenshot shows the 'LAN Setup' page in a web management system. The page has a navigation bar with tabs: QuickSetup, Network (selected), Voice, Management, and Diagnose. On the left, there is a sidebar menu with options: ADSL, WAN, 3G, WLAN, LAN (selected), DNS, Security, Routing, VPN, Certificate, VLAN, QoS, and AntiAttack. The main content area is titled 'LAN Setup' and contains the following fields and options:

- IP Address: 192.168.1.1
- Subnet Mask: 255.255.255.0
- LAN MAC Address: 00:18:82:ac:16:12
- Web Access Mode: Http Https
- LAN Side Firewall: Enable Disable

Below these fields is an 'Advanced' section, which is highlighted with a pink border in the image. It contains the following options and fields:

- Disable DHCP Server
- Enable DHCP Server
- Start IP Address: 192.168.1.2
- End IP Address: 192.168.1.254
- Leased Time (hour): 24
- Static IP Lease List: (empty table)

MAC Address	IP Address	Operation
		<input type="button" value="Add"/>

Below the 'Advanced' section, there is an option to 'Enable DHCP Relay' with a text field for 'DHCP Server IP Address'. A 'Save' button is located at the bottom right of the page.

Step 2 Set parameters according to [Table 7-49](#).

Table 7-49 Parameter description

Parameter	Description
Start IP Address	Indicates the start IP address in the address pool. It must be on the same network segment as the LAN gateway. The default value is recommended.
End IP Address	Indicates the end IP address in the address pool. It must be on the same network segment as the LAN gateway. The default value is recommended.
Leased Time (hour)	Indicates the IP address lease interval. If the lease expires and the DHCP client does not renew the lease, the DHCP server releases the IP addresses that are granted to the DHCP client for other clients.

Step 3 (Optional) Allocate IP addresses by binding them with MAC addresses statically.

After configuration, the DHCP server finds the IP address based on the bound MAC address and allocates the IP address to the corresponding DHCP client. This mode is applicable to clients that require a fixed IP address such as the FTP server.


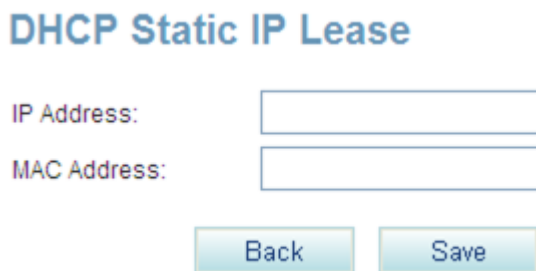
- Click  .
The page shown in [Figure 7-190](#) is displayed.


Figure 7-190 Configuring the DHCP server (2)



DHCP Static IP Lease


IP Address:

MAC Address:

- Enter the MAC address of the DHCP client and the IP address that you want to bind with the MAC address.
- Click  to save the settings.

 **NOTE**

- To obtain the MAC address of a PC, choose **Start > Run**, type **cmd**, and press **Enter**. On the command-line interface (CLI) that is displayed, run the **ipconfig /all** command. The value of **Physical Address** corresponding to the 192.168.x.y indicates the MAC address.
- To obtain the MAC address of other network devices such as IP phones, see the related document.

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

Configuring the DHCP Relay

If the DHCP server has been deployed but it is on a different network segment from terminals (such as PCs and IP phones), configure the EGW1520 as the DHCP relay. After configuration, the EGW1520 forwards terminals' DHCP requests to the DHCP server. The DHCP server sends the IP address allocation information to the EGW1520, and the EGW1520 forwards the information to terminals.

The DHCP client enables terminals that connect to the EGW1520 and DHCP clients on other networks to use the same DHCP server. This reduces costs and simplifies management.

 **NOTE**

- The DHCP relay conflicts with the NAT function. Before configuring the EGW1520 as the DHCP relay, you must disable the NAT function.
- When configuring the EGW1520 as the DHCP relay, ensure that a reachable route exists between the EGW1520 and DHCP server.

Step 1 Click **Enable DHCP Server Relay**, as shown in [Figure 7-191](#).

Figure 7-191 Configuring the DHCP relay



Step 2 Enter the IP address of the DHCP server.

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

LAN Setting Example (EGW1520 as DHCP Server)

Network Requirements

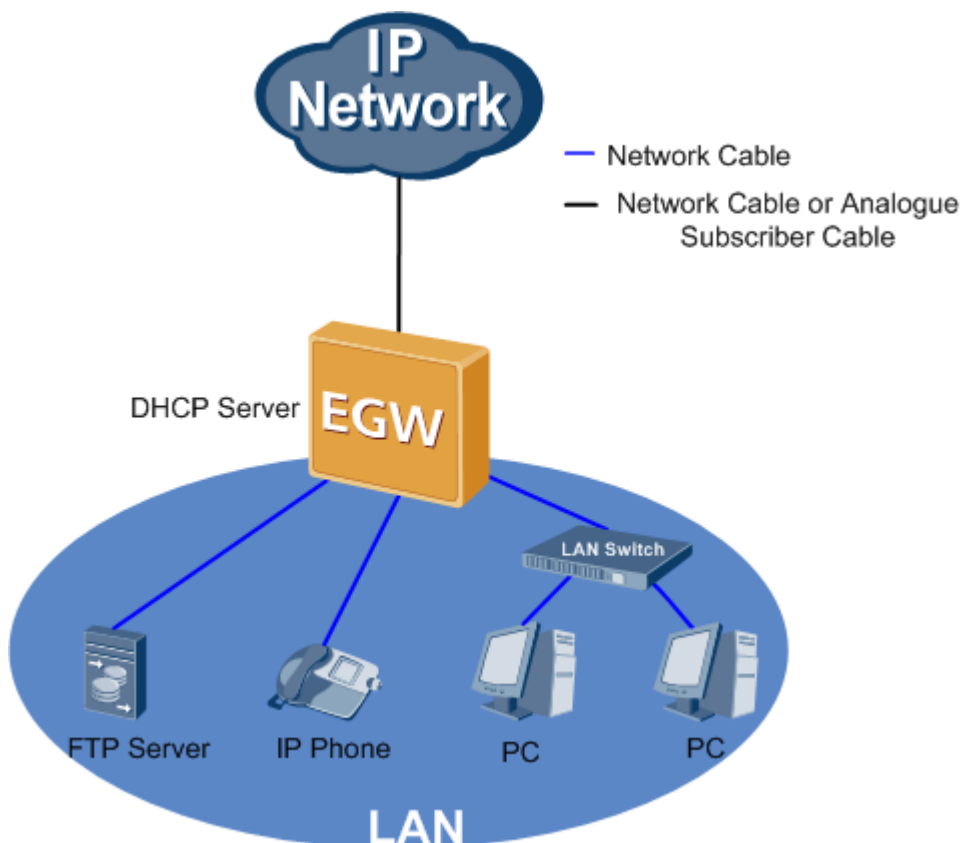
- PCs use the LAN switch to connect to the LAN port on the EGW1520, while the IP phone and FTP server connect to the LAN port on the EGW1520 directly.

- The EGW1520 functions as the DHCP server and automatically allocates IP addresses for the PCs, IP phone, and FTP server.
- After configuration, the FTP server obtains a fixed IP address, while the IP phone and PCs obtain dynamic IP addresses through the EGW1520.

Typical Network

Figure 7-192 shows the typical network.

Figure 7-192 Typical network (1)



Procedure

- Step 1** Configure that the FTP server, IP phone, and PCs obtain IP addresses automatically. For details, see the related user guide.
 - Step 2** Configure the EGW1520 as the DHCP server. For details, see step 1 in [Configuring the DHCP Server](#).
 - Step 3** Query and record the MAC address of the FTP server. For details, see [Obtain the MAC address](#).
 - Step 4** Allocate the IP address that is bound to the MAC address to the FTP server. For details, see step 2 in [Configuring the DHCP Server](#).
- End

LAN Setting Example (EGW1520 as DHCP Relay)

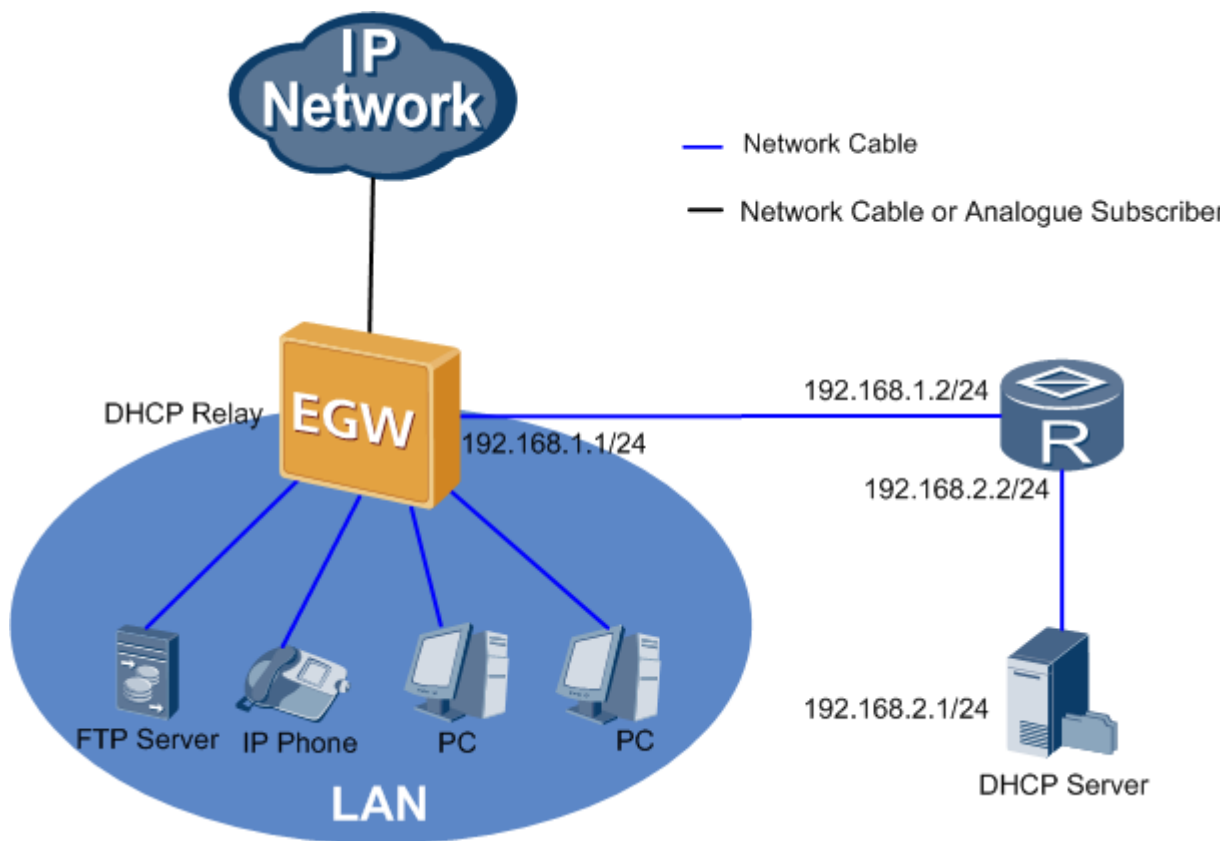
Network Requirements

- The DHCP server (IP address: 192.168.2.1) is deployed on the network. The LAN port on the EGW1520 connects to the DHCP server through a router.
- The PCs, IP phone, and FTP server directly connect to the LAN port on the EGW1520.
- The EGW1520 functions as the DHCP relay and allocates IP addresses for the PCs, IP phone, and FTP server.
- After configuration, the FTP server obtains a fixed IP address, while the IP phone and PCs obtain dynamic IP addresses through the EGW1520.

Typical Network

Figure 7-193 shows the typical network.

Figure 7-193 Typical network (2)



Procedure

- Step 1** Configure that the FTP server, IP phone, and PCs obtain IP addresses automatically. For details, see the related user guide.
- Step 2** Configure the EGW1520 as the DHCP relay, and set the IP address of the DHCP server to 192.168.2.1. For details, see [Configuring the DHCP Relay](#).
- Step 3** Add a static route on the EGW1520, and set the destination network segment to 192.168.2.0/24. For details, see [7.5.5 Static Route](#).

- Step 4** Set the gateway IP address to 192.168.2.2/24 on the DHCP server. For details, see the DHCP server user guide.
- Step 5** Add an address pool whose start IP address is 192.168.1.0 and end IP address is 192.168.1.24 for the DHCP server, and allocate the IP address that is bound to the MAC address to the FTP server. For details, see the DHCP server user guide.

----End

7.5.3 WLAN

The EGW1520 can connect to the wireless network to provide Wi-Fi services. This provides small enterprises with a network solution integrating wired and wireless technologies.

Description

This topic describes the principle, implementation, specification, and limitation of the EGW1520 WLAN.

Principle

A WLAN is a LAN using wireless channels. It is an important supplement to wired network access. WLAN is widely used in areas requiring mobile data processing or ease of installation. As an interoperability standard of WLAN, Wireless Fidelity (Wi-Fi) works in short-distance wireless areas such as offices and homes. The EGW1520 complies with IEEE802.11b/g/n.

Implementation

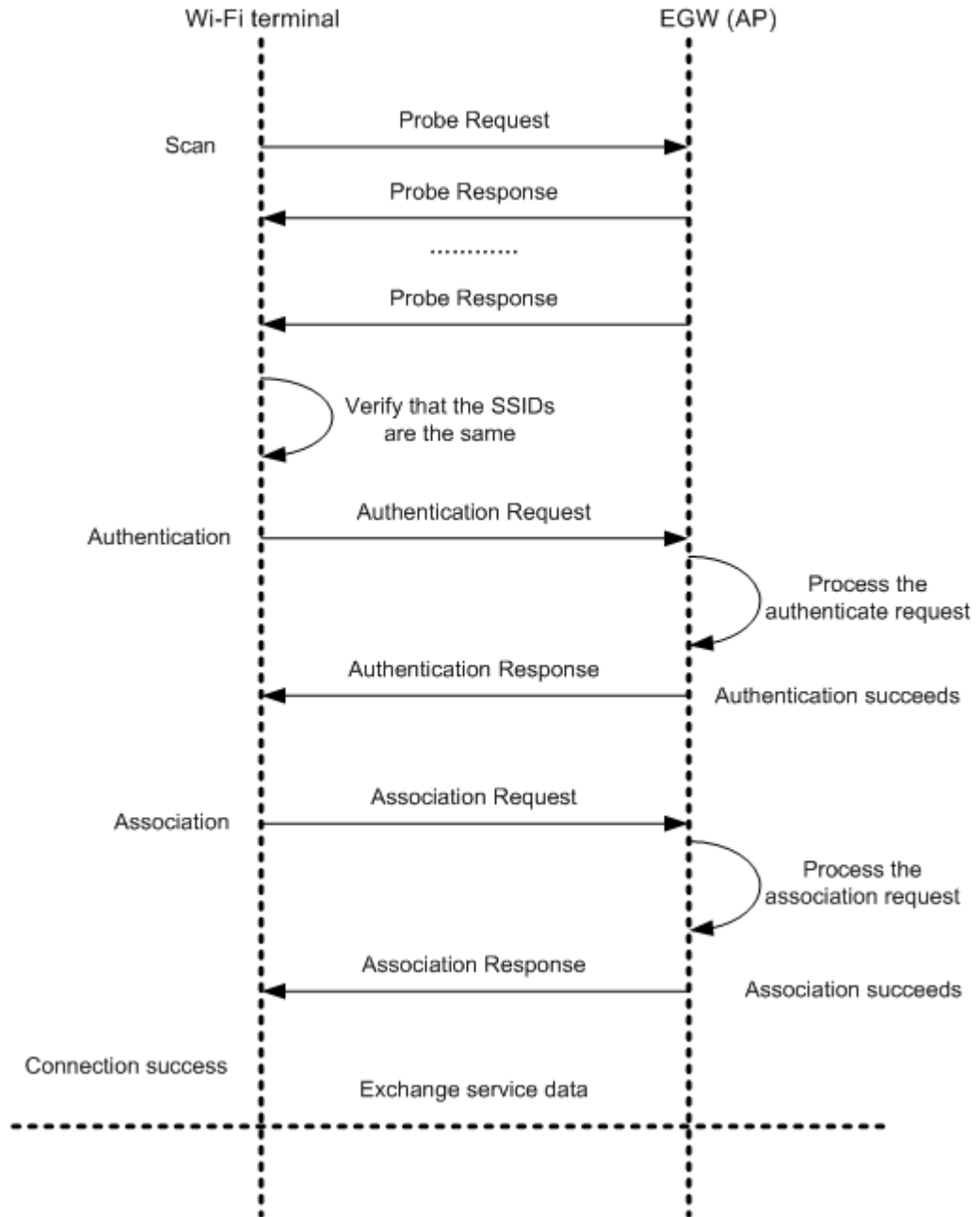
The EGW1520 functions as an Access Point (AP) to provide WLAN services. It encapsulates data into packets and sends the packets to the carrier network through an IP network. Wi-Fi terminals are connected to the EGW1520 in wireless mode. The EGW1520 connects these Wi-Fi terminals to the Internet by providing WLAN services, as shown in [Figure 7-194](#).

Figure 7-194 WLAN network diagram



A Wi-Fi terminal connects to an EGW1520 in three phases: Scan, Authentication, and Association, as shown in [Figure 7-195](#).

Figure 7-195 Connection phases



The phases are as follows:

1. Scan

The Wi-Fi terminal uses a wireless network adapter that complies with IEEE802.11 b/g/n to scan available EGW1520s. The following scan modes are provided:

- Active scan

The Wi-Fi terminal sends Probe Request frames in all channels to search for an AP that has the same service set identifier (SSID). The Wi-Fi terminal does not stop sending Probe Request frames until a required AP is found. When receiving a Probe Request frame, the AP sends a Probe Response frame to the Wi-Fi terminal.

- Passive scan

The Wi-Fi terminal passively receives Beacon frames (with a broadcast or hidden SSID) that are sent by APs periodically.

When the Wi-Fi terminal finds an AP with the same SSID, authentication starts.



NOTE

When finding multiple APs, the Wi-Fi terminal connects to the AP whose signals are the strongest.

2. Authentication

The Wi-Fi terminal sends an authentication message to the AP. The AP authenticates the Wi-Fi terminal based on the message that is received. If the authentication is successful, the AP sends the success notification to the Wi-Fi terminal.

3. Association

After receiving the authentication success response, the Wi-Fi terminal sends an association request to the AP. The AP processes the request, sets up a connection, and sends a response to the Wi-Fi terminal.

After the association, the Wi-Fi terminal can use the AP to send data frames to the network.

Specification

- IEEE802.11b, IEEE802.11g, and IEEE802.11n are supported.
 - IEEE802.11b, with the maximum transmission rate of 11 Mbit/s and frequency of 2.4 GHz
 - IEEE802.11g, with the maximum transmission rate of 54 Mbit/s and frequency of 2.4 GHz (compatible with IEEE802.11b)
 - IEEE802.11n, with the maximum transmission rate of 300 Mbit/s and Multi-Input Multi-Output (MIMO) supported
- A maximum of 16 WiFi terminals can be connected.
- Four service set identifiers (SSIDs) are supported and SSID broadcast and hiding are supported.
 - The default value of the primary SSID is eSpace EGW_XXXX.
 - Three subordinate SSIDs are eSpace EGW_XXXX_S1, eSpace EGW_XXXX_S2, and eSpace EGW_XXXX_S3. XXXX is the last four bits in the WLAN MAC address.
- A maximum of 16 MAC addresses can be filtered.
- Wi-Fi authentication standards:
 - 64 bit or 128 bit Wired Equivalent Privacy (WEP)
 - WPA-PSK, WPA2-PSK, and Combination of WPA-PSK and WPA2-PSK
 - Maximum transmit power:
 - 802.11b/g/n (SISO): 16±2 dBm
 - 802.11n (MIMO): 18±2 dBm
 - Wi-Fi Protected Setup (WPS)

Limitation

Wi-Fi bridging is not supported.

Configuring the WLAN Function for the EGW1520

The EGW1520 uses WLAN to connect WLAN terminals, such as PCs and mobile phones. If the EGW1520 connects to the upstream network, it functions as an access point (AP), which allows terminals to access the Internet.

Prerequisite

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

Context

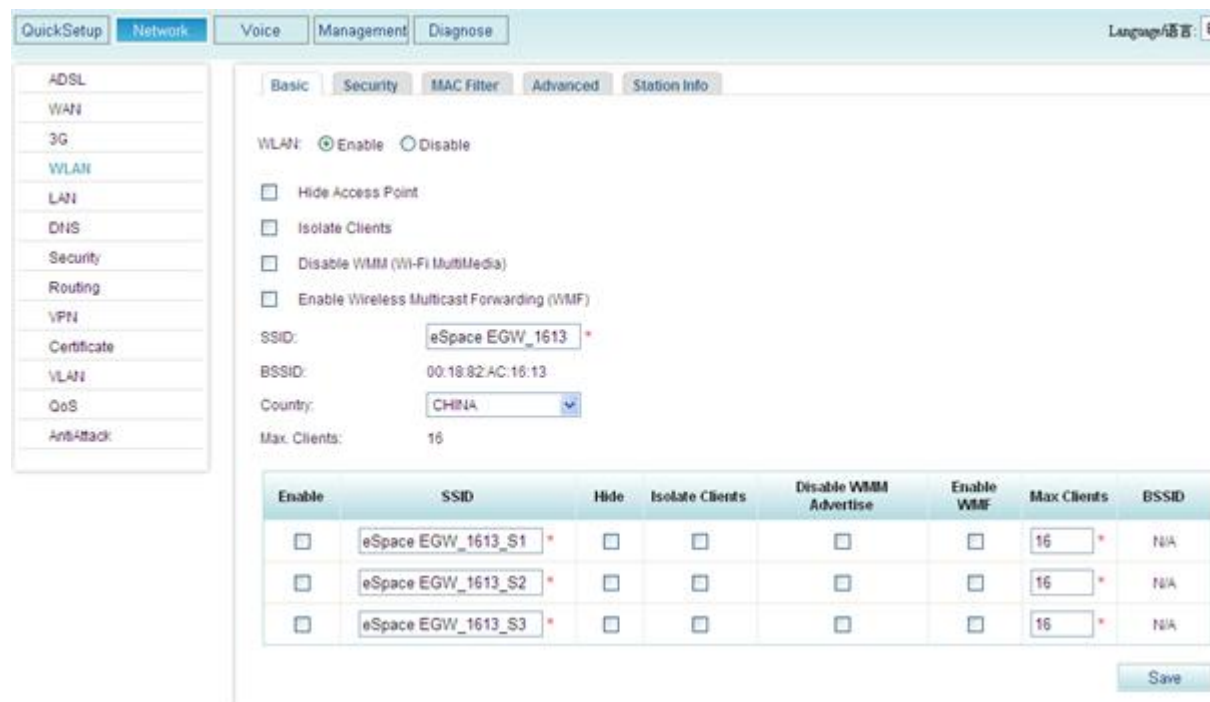
The following describes how to enable and configure the WLAN function. For terminal configuration, see the user guide of each WLAN terminal.

Enable the WLAN Function

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

The page shown in [Figure 7-196](#) is displayed.

Figure 7-196 Enabling the WLAN function



Step 2 Set parameters according to [Table 7-50](#).

Table 7-50 Parameter description

Parameter	Description
WLAN	Enables or disables the WLAN function. The options are as follows: <ul style="list-style-type: none"> • Enable • Disable By default, the WLAN function is enabled.
Hide Access Point	Hides the access point EGW1520. When connecting a Wi-Fi terminal to an AP, enter the service set identifier (SSID) of the AP.
Isolate Clients	Isolates Wi-Fi terminals connected to the EGW1520 to disable the data communication among terminals.
Disable WMM (Wi-Fi MultiMedia)	Disables the Wi-Fi Multimedia (WMM) advertising function. Packets of this service are marked priorities. In response to these markings, routers and switches use various queuing strategies to tailor performance to requirements.
Enable Wireless Multicast Forwarding (WMF)	Enables the WMF function.
SSID	Indicates the ID of the EGW1520, which is displayed on the terminal when searching for an AP. The default value is eSpace EGW_****, where **** indicates the last four digits in the MAC address of the Wi-Fi AP. The value can be defined by users. NOTE EGW1520 supports four SSIDs to divide subnets.
BSSID	Indicates the MAC address of the AP.
Country	Indicates the country name. The Wi-Fi frequency band is determined by the WLAN frequency band of the country.
Max Clients	Indicates the maximum number of WLAN terminals(16) accessing to the EGW1520.

Step 3 Click  to save the settings.

----End

Configure the WLAN Security

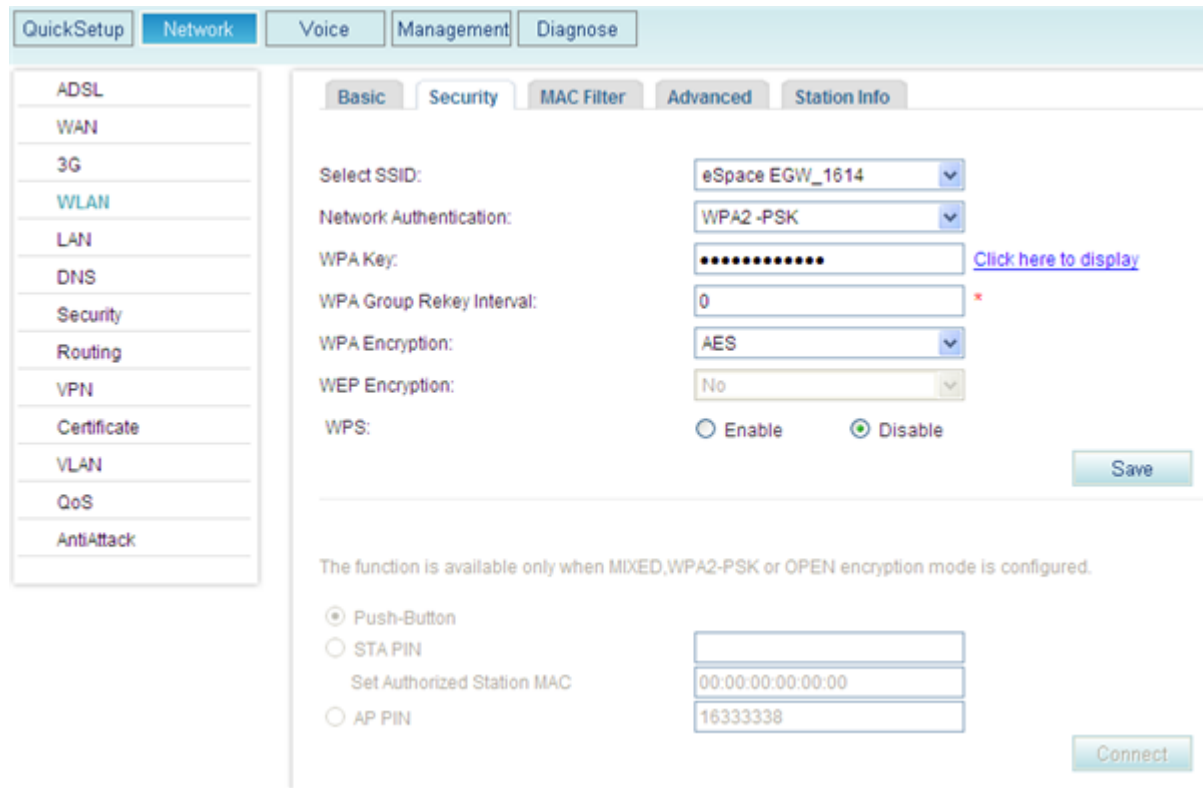
The WLAN security configuration prevents unauthorized users from accessing or listening on your wireless network.

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

Step 2 Click the **Security** tab.

The page shown in [Figure 7-197](#) is displayed.

Figure 7-197 Configuring the WLAN security



Step 3 Set parameters according to [Table 7-51](#).

Table 7-51 Parameter description

Parameter	Description
Select SSID	Indicates the SSID. The default value is eSpace EGW_**** where **** indicates the last four digits in the MAC address.
NetWork Authentication	<p>Authenticates the network.</p> <ul style="list-style-type: none"> Open: All Wi-Fi terminals can access the WLAN network. Shared: A shared key is used to authenticate the network access. 802.1X: a protocol for port-based network access control. Clients connected to the port can have access to the network only after being authenticated. WPA: a new technology that inherits the features and overcomes the shortcomings of WEP. It enhances the algorithm for generating keys. In WPA, keys are frequently changed to achieve higher security. WPA-PSK: Simplified WPA mode is used to authenticate the network access. The EGW1520 uses WPA to pre-share a key for encrypting all communications.

Parameter	Description
	<ul style="list-style-type: none"> WPA2: latest WPA version, which provides CCMP, a standard encryption protocol, for access to wireless LANs. CCMP is more secure than the WEP protocol and TKIP protocol of WPA. WPA2-PSK: Simplified WPA2 mode is used to authenticate the network access. The EGW1520 uses WPA2 to pre-share a key for encrypting all communications. Mixed WPA2/WPA: The WPA2 and WPA are used together to authenticate network access. Mixed WPA2/WPA-PSK: The WPA2-PSK and WPA-PSK are combined to authenticate the network access. <p>The default value is Mixed WPA2/WPA-PSK. Parameters relating to the preceding authentication modes are described on web pages.</p>

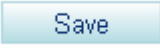

Step 4 Enable the Wi-Fi Protect Setup (WPS) function according to [Table 7-52](#).



The WPS quickly sets up an encrypted connection between a wireless terminal and the EGW1520. You do not need to set an encryption mode or a key for the WPS function. Instead, enter the correct PIN code and use the Push-Button to access the wireless network. By default, the WPS function is disabled.

 **NOTE**

The WPS works only when the wireless terminal has a proper network adapter. For details, see the network adapter description.

Table 7-52 Parameter description

Parameter	Description
WPS	<p>Enables or disables the WPS function. The options are as follows:</p> <ul style="list-style-type: none"> Enable Disable <p>By default, the WPS function is disabled. After enabling or disabling the WPS function, click  to save the setting.</p>
Push-Button	<p>Use the Push-Button to connect to the network. The procedure is as follows:</p> <ul style="list-style-type: none"> Select Push-Button, and click  or press the Wi-Fi button on the EGW1520 for six seconds or longer. Press the WPS button on the network adapter of the wireless terminal within two minutes.
STA PIN	<ul style="list-style-type: none"> Enter the STA PIN code to connect to the network. If you want

Parameter	Description
	<p>to use this mode, you must know the STA PIN code of the wireless network. The procedure is as follows:</p> <ul style="list-style-type: none"> - Select STA PIN and enter the STA PIN code of the wireless terminal in the right text box. - Click  . <ul style="list-style-type: none"> • Set Authorized Station MAC: Used to authenticate the Wi-Fi client.
AP PIN	<p>Enter the PIN code to connect to the network. The procedure is as follows:</p> <ul style="list-style-type: none"> • Select PIN and click  . • Enter the PIN code of the EGW1520 (AP) on the wireless terminal.

----End

Configuring the WLAN MAC Address Filter

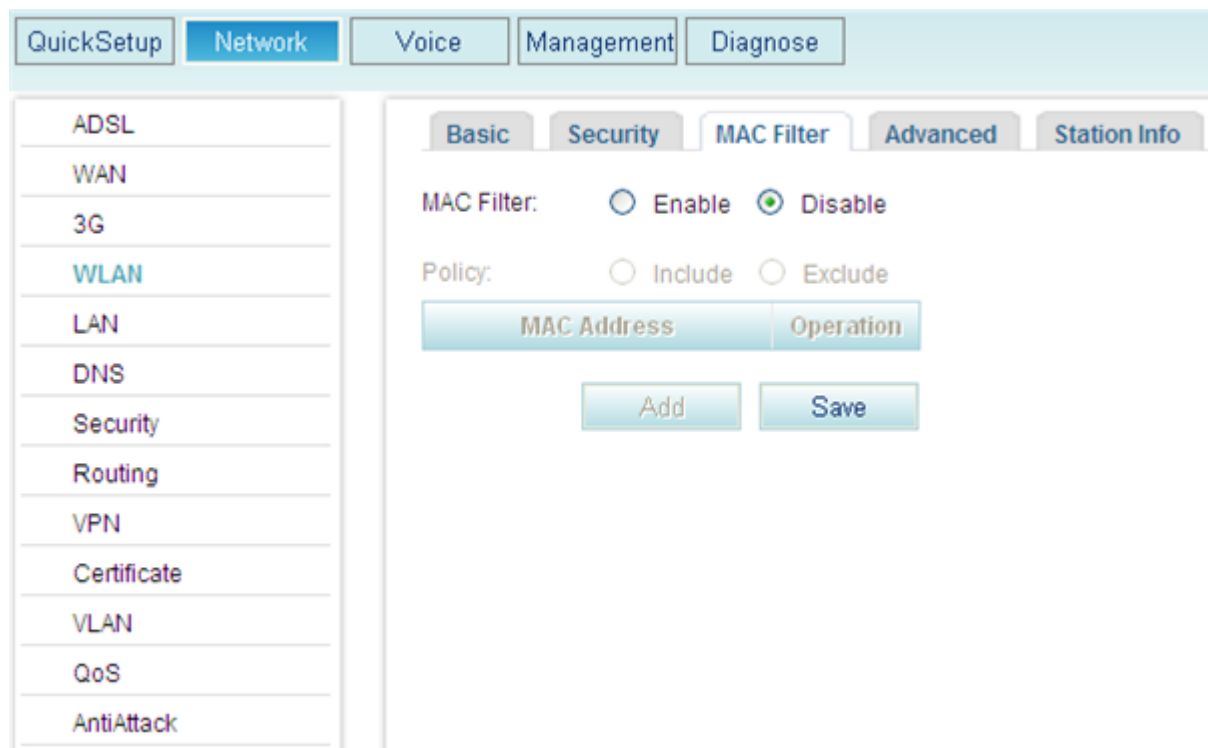
The WLAN MAC address filter prevents users accessing the wireless network with unauthorized MAC addresses.

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

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

The page shown in [Figure 7-198](#) is displayed.


Figure 7-198 Configuring the WLAN MAC address filter (1)



Step 3 Set parameters according to [Table 7-53](#).

Table 7-53 Parameter description

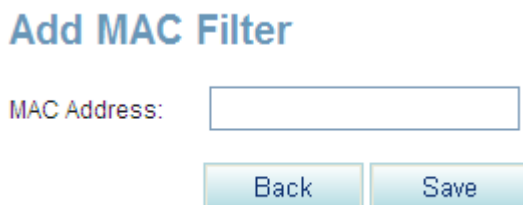
Parameter	Description
MAC Filter	<p>Enables or disables the MAC address filter function. The options are as follows:</p> <ul style="list-style-type: none"> • Enable: Enable MAC address filtering. • Disable: Disable MAC address filtering.
Policy	<ul style="list-style-type: none"> • Include: WLAN terminals in the MAC address list can access the WLAN. • Exclude: WLAN terminals in the MAC address list cannot access the WLAN.

Step 4 Click  to save the settings.

Step 5 Click .

The page shown in [Figure 7-199](#) is displayed.

Figure 7-199 Configuring the WLAN MAC address filter (2)



Step 6 Enter the MAC address of the WLAN terminal that needs to be filtered and click



----End

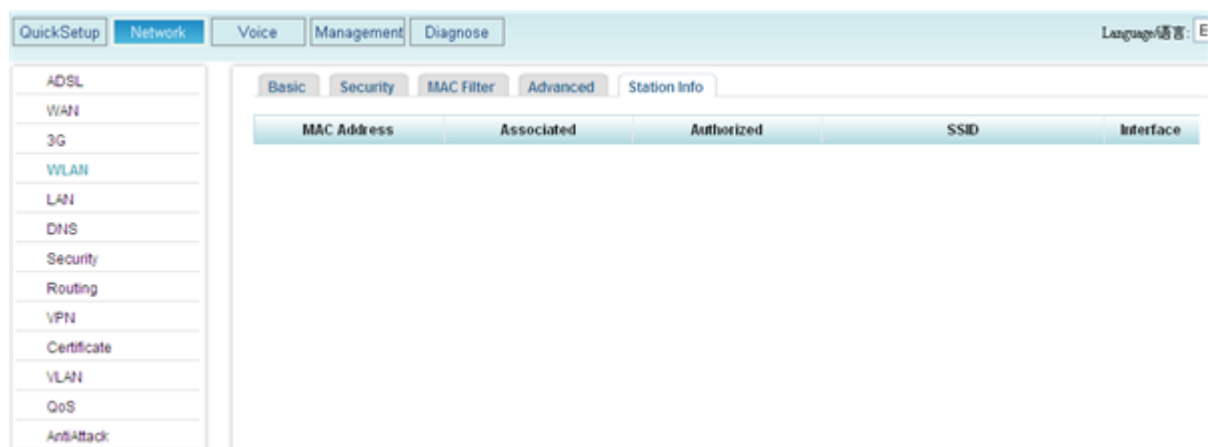
Checking the Status of the WLAN Terminals Connected to the EGW1520

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

Step 2 Click the **Station Info** tab.

The page shown in [Figure 7-200](#) is displayed.

Figure 7-200 Checking the WLAN terminal status



----End

Connecting a PC to the EGW1520 Wirelessly

This topic describes how to use a WLAN card to connect a PC that runs the Windows XP to the EGW1520.

Prerequisites

- The WLAN function has been enabled and configured on the EGW1520.

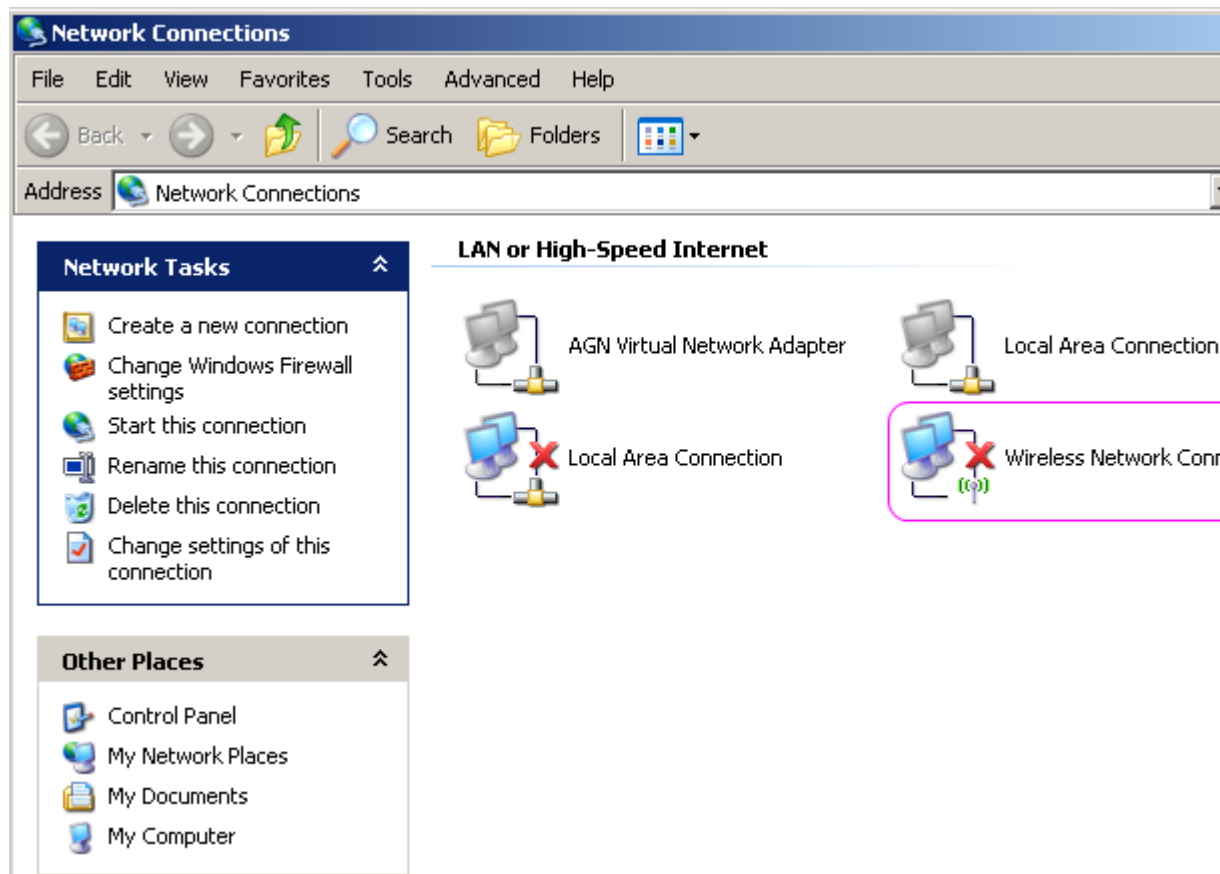
- The EGW1520 has been connected to the upstream network so that the computer can access the Internet through the EGW1520. For details, see [7.2 Connection Modes](#).
- A WLAN card has been installed on the PC.

Procedure

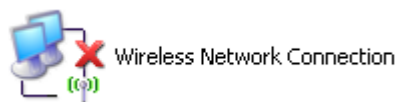
Step 1 Right-click **My Network Places** and choose **Properties**.

The page shown in [Figure 7-201](#) is displayed.

Figure 7-201 Configuring the wireless connection (1)

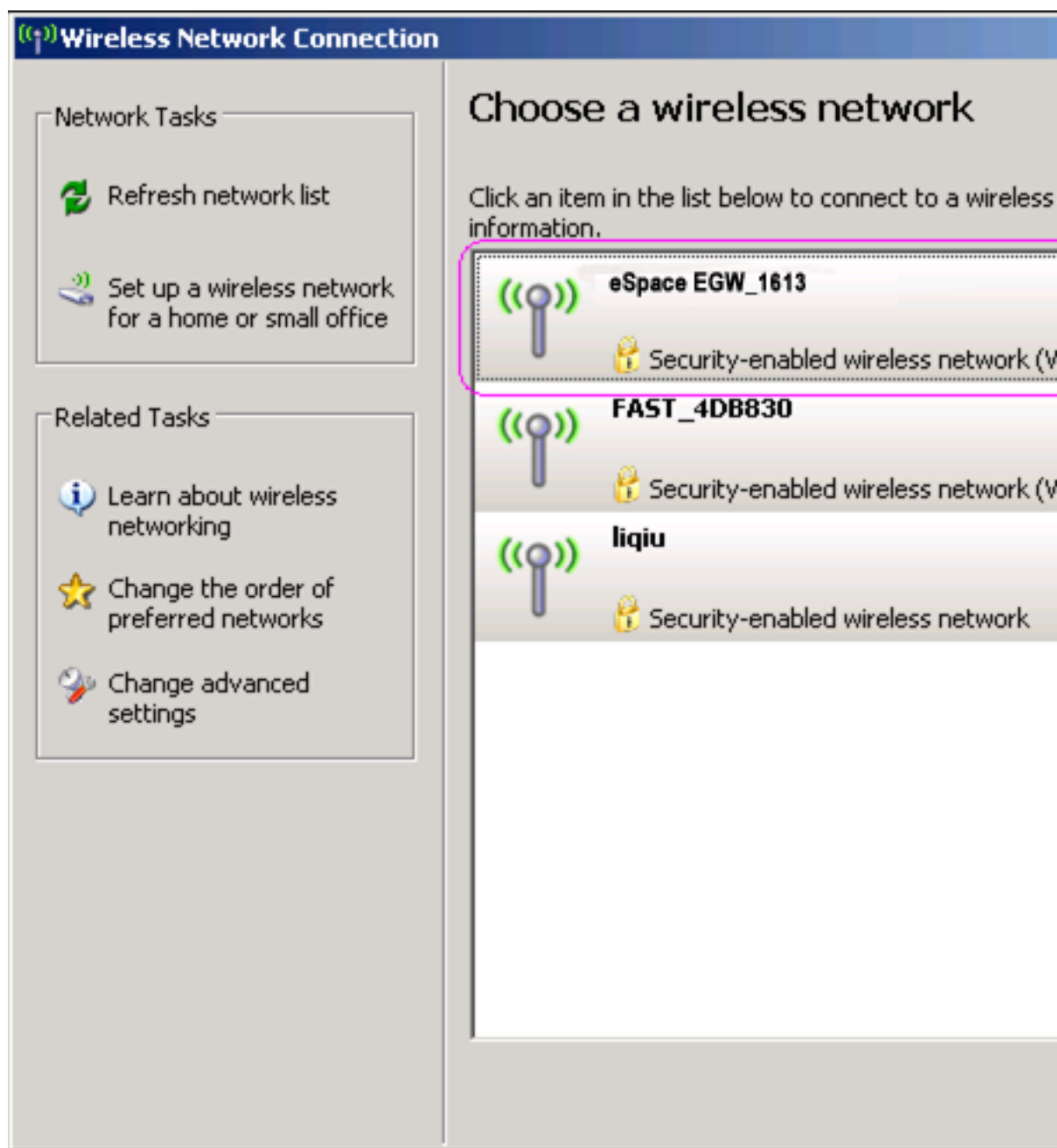


Step 2 Double-click



The page shown in [Figure 7-202](#) is displayed.

Figure 7-202 Configuring the wireless connection (2)



 **NOTE**

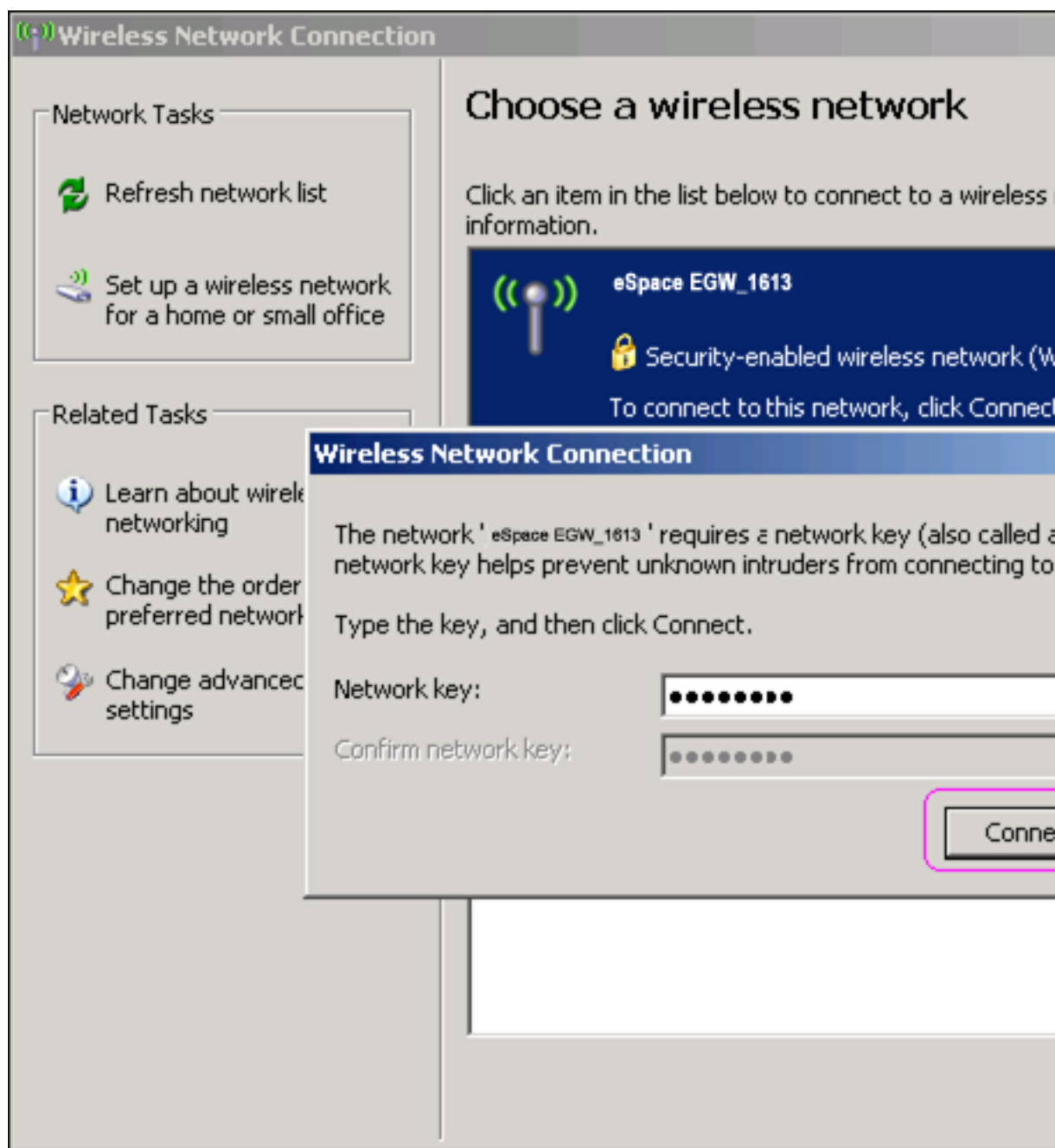
If no available wireless network (for example, eSpace EGW_1613 in [Figure 7-202](#)) is listed, click **Refresh network list**.

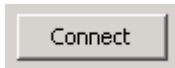
Step 3 Select **eSpace EGW_1613** and click



The page shown in [Figure 7-203](#) is displayed.

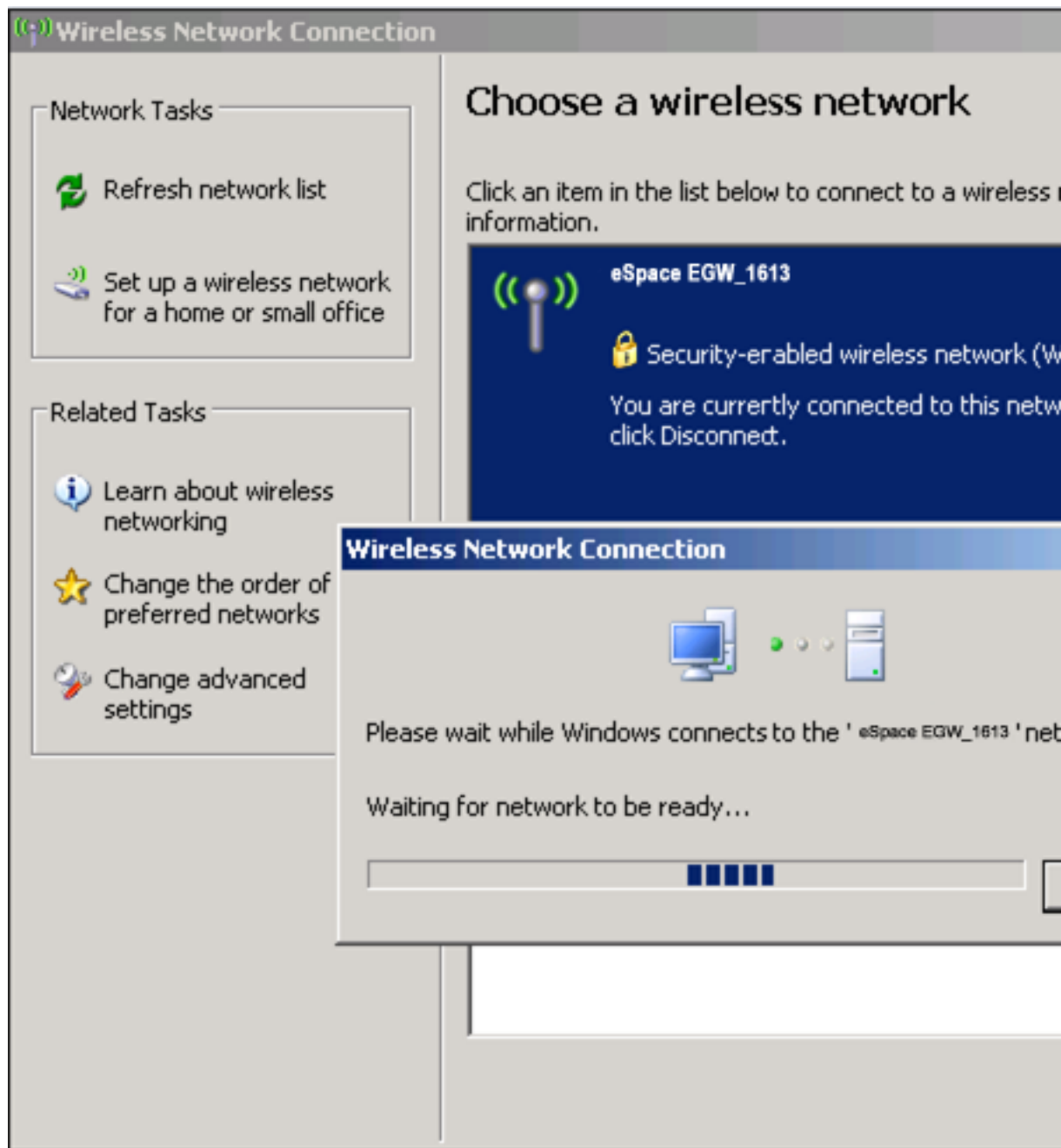
Figure 7-203 Configuring the wireless connection (3)



Step 4 Enter a key that is the same as that on the EGW1520, and click .

The page shown in [Figure 7-204](#) is displayed.

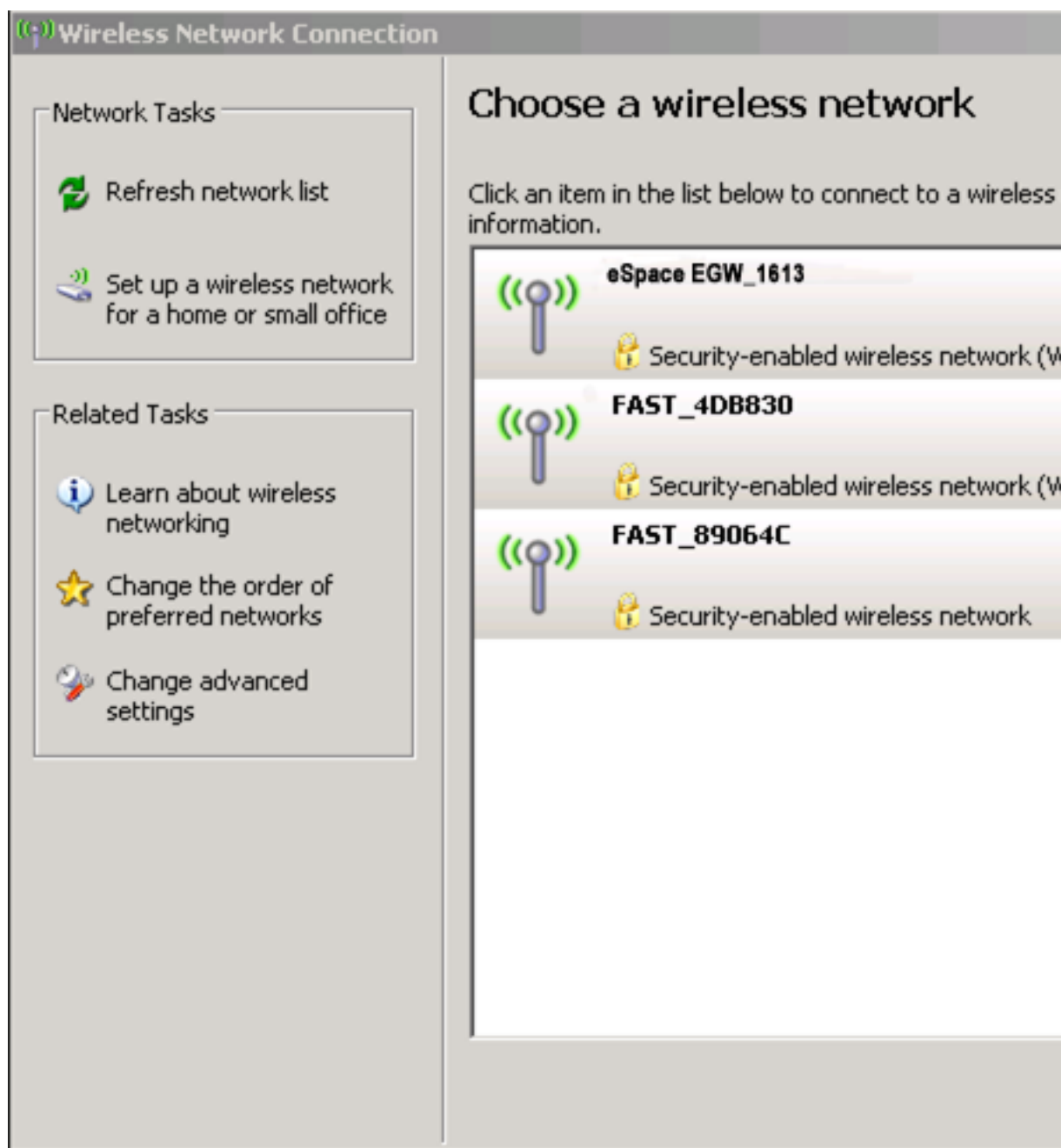
Figure 7-204 Configuring the wireless connection (4)



Information **Connected** indicates that the PC is connected to the EGW1520.

The page shown in [Figure 7-205](#) is displayed.

Figure 7-205 Configuring the wireless connection (5)



----End

Verification

Start the Microsoft Internet Explorer, and enter IP address of the EGW1520. The default value is **192.168.1.1**. If the EGW1520 login page is displayed, the wireless connection is successful. If the page is not displayed, verify that all prerequisites are met. For details, see [Prerequisite](#).

Advanced Configurations

This topic describes the advanced WLAN configurations. Only network administrators can change the advanced parameter settings. To ensure the normal running of the EGW1520, you are advised to use the default settings.

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 > WLAN** from the navigation tree.

Step 2 Click the **Advanced** tab.

The page shown in [Figure 7-206](#) is displayed.

Figure 7-206 Advanced WLAN configurations

QuickSetup	Network	Voice	Management	Diagnose
------------	----------------	-------	------------	----------

ADSL	WLAN	LAN	DNS	Security	Routing	VPN	Certificate	VLAN	QoS	AntiAttack
------	------	-----	-----	----------	---------	-----	-------------	------	-----	------------

Basic	Security	MAC Filter	Advanced	Station Info
-------	----------	------------	-----------------	--------------


Current Channel:	11 (interference: acceptable)
Channel:	Auto
Auto Channel Timer (min)	0
802.11n/EWC:	Auto
Current Bandwidth:	20MHz
Bandwidth:	20MHz in Both Bands
Current Control Sideband:	None
Control Sideband:	Lower
802.11n Rate:	Auto
802.11n Protection:	Auto
Support 802.11n Client Only:	Off
RIFS Advertisement:	Off
OBSS Co-Existence:	Enable
RX Chain Power Save:	Disable
RX Chain Power Save Quiet Time:	10
RX Chain Power Save PPS:	10
Radio Power Save:	Disable
Radio Power Save Quiet Time:	10
Radio Power Save PPS:	10
Radio Power Save On Time:	
54g™ Rate:	1 Mbps
Multicast Rate:	Auto
Basic Rate:	Default
Fragmentation Threshold:	2346
RTS Threshold:	2347
DTIM Interval:	1
Beacon Interval:	100
Global Max Clients:	16
XPress™ Technology:	Disabled
Transmit Power:	100%
WMM (WiFi Multimedia):	Enabled
WMM No Acknowledgement:	Disable
WMM APSD:	Enable

Step 3 Set parameters according to [Table 7-54](#).

Table 7-54 Advanced WLAN parameters

Parameter	Description
Current Channel	Indicates the channel that is being used.
Channel	Value Auto indicates that the system automatically selects the best channel from all channels for use. CAUTION If multiple EGW1520s are deployed, set channels of neighboring EGW1520s to different values. For example, set the channel of the first EGW1520 to 1, and the channel of the neighboring EGW1520 to 6 or 11.
Auto Channel Timer (min)	Any non-zero values indicate that the system reselects a channel when the timer times out.
802.11n/EWC	Indicates whether the EGW1520 supports 802.11n. Value Auto indicates that support for 802.11n varies according to network environment.
Current Bandwidth	Displays the current bandwidth.
Bandwidth	Sets the frequency bandwidth.
Current Control Sideband	Indicates the current sideband control mode.
Control Sideband	Indicates the sideband control mode.
802.11n Rate	Indicates the Wi-Fi rate. Value Auto indicates that the system automatically selects an optimal rate.
802.11n Protection	Indicates the 802.11n protection mechanism.
Support 802.11n Client Only	Only clients that comply with 802.11n are supported.
RIFS Advertisement	Provides a shorter delay between OFDM transmissions than in 802.11g.
OBSS Co-Existence	Both 20 MHz and 40 MHz overlapping Basic Service Set (OBSS) are supported on the WLAN network. When a user sets 40 MHz BSS on the network supporting 20 MHz BSS, the bandwidth automatically decreases from 40 MHz to 20 MHz.
RX Chain Power Save	Power is saved in the receiving channel.
RX Chain Power Save Quiet Time	Indicates the quiet time of the power saving in the receiving channel.
RX Chain Power Save PPS	Indicates the maximum number of packets per second that can be processed by the WLAN port for a duration specified by Quiet Time .
Radio Power Save	Power is saved in the sending channel.
Radio Power Save Quiet Time	Indicates the quiet time of the power saving in the sending channel.

Parameter	Description
Radio Power Save PPS	Indicates the maximum number of packets per second that can be processed by the WLAN port for a duration specified by Quiet Time .
Radio Power Save On Time	Indicates the time when the power saving takes effect in the sending channel.
54g™ Rate	Indicates the 54g™ rate.
Multicast Rate	Indicates the multi-antenna transmission rate. Value Auto indicates that the system automatically selects an optimal rate.
Basic Rate	Value All indicates that the EGW1520 automatically selects 1 Mbit/s or 2 Mbit/s based on the network environment.
Fragmentation Threshold	Indicates the threshold for triggering the fragmentation.
RTS Threshold	Indicates the threshold for triggering the transmission.
DTIM Interval	Indicates the multi-point transmission interval.
Beacon Interval	Indicates the interval between two consecutive beacons.
Global Max Clients	Indicates the maximum number of clients supported by the EGW1520.
XPress™ Technology	Indicates the wireless multimedia extension technology.
Transmit Power	Indicates the transmission power.
WMM (WiFi Multimedia)	Indicates the Wi-Fi multi-media (WMM) application. Value Auto indicates that the system automatically selects a Wi-Fi network based on the network environment.
WMM No Acknowledgment	Indicates the WMM mode without the Ack message.
WMM APSD	Indicates WMM Automatic Power Shutdown (APSD).

Step 4 Click  to save the settings.

----End

7.5.4 DNS

The Domain Name System (DNS) is a hierarchical naming system built on a distributed database. It translates human-friendly domain names into IP addresses and is applicable to TCP/IP programs. The EGW1520 can function as a DNS client to resolve domain names on the DNS server.

Configuration

To configure the DNS server without changing the ADSL or WAN configuration, perform the following steps:

Prerequisites

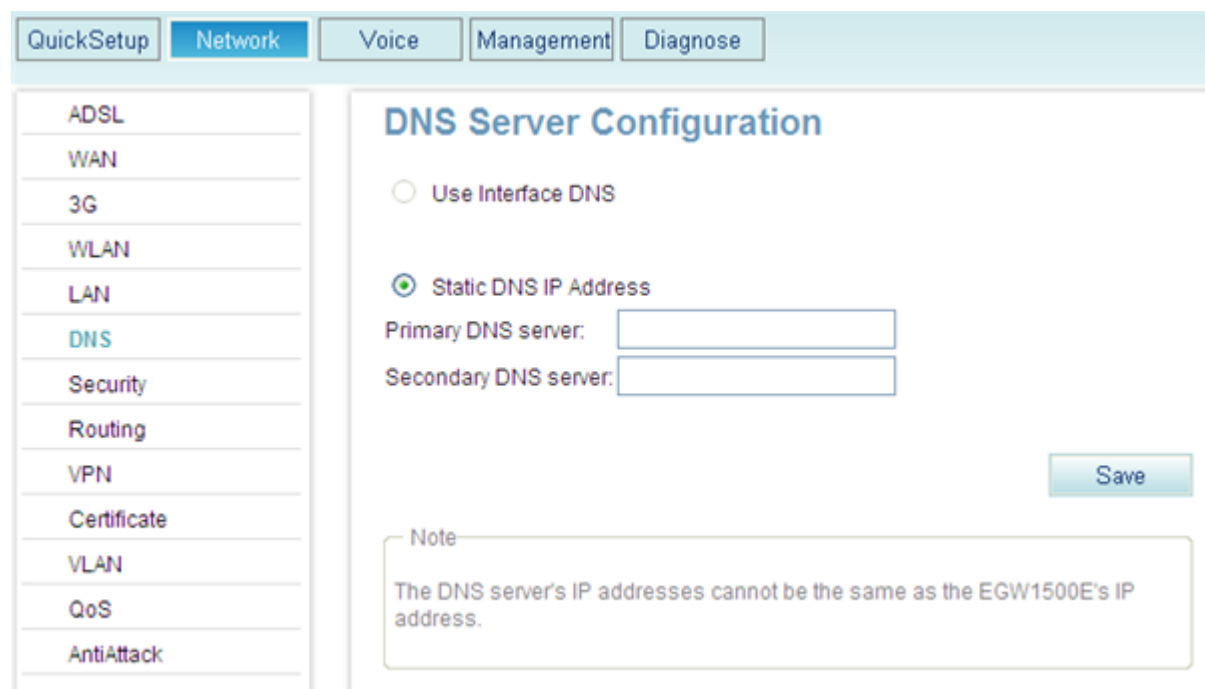
You have logged in to the web management system. For details, see [7.7.1 Web Management](#).

Procedure

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

The page shown in [Figure 7-207](#) is displayed.

Figure 7-207 Configuring a DNS server




Step 2 Configure a DNS server.

The system provides the following configuration methods:

- Method 1: Obtain the IP address of the DNS server through the interface that connects to the DNS server.
- Method 2: Set the IP address of the DNS server manually. The IP address of the DNS server is provided by the network carrier.

Method 2 is applicable when you know the IP address of the DNS server.

Step 3 Click  to save the settings.

----End

7.5.5 Static Route

This topic describes how to configure the static route in a simple network.

Compared with the dynamic route, the static route uses less network resources, saves bandwidth, and is easy to configure. The static route can improve the network performance and ensure the bandwidth for important applications. When the network is unavailable or the topology is changed, the management personnel must change the static route manually.

Configuration

Prerequisites

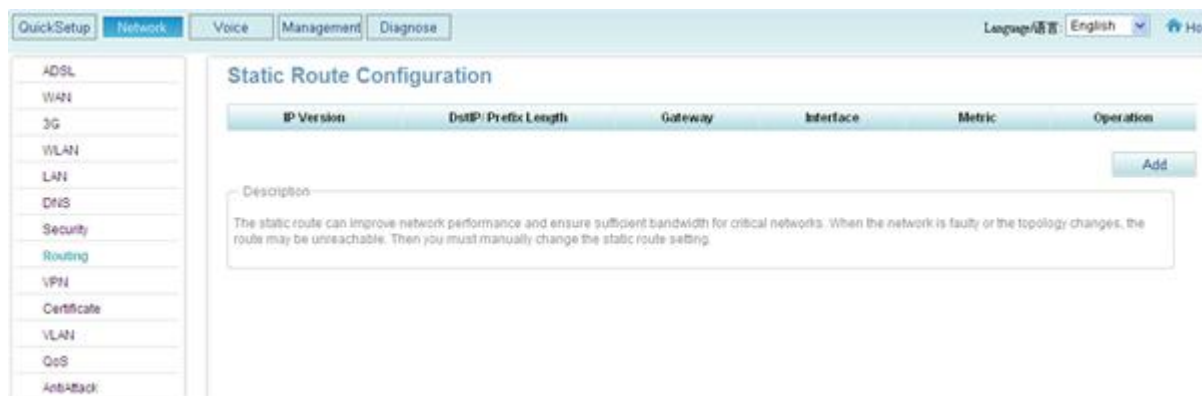
You have logged in to the web management system. For details, see [7.7.1 Web Management](#).

Procedure

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

The page shown in [Figure 7-208](#) is displayed.

Figure 7-208 Configuring the static route (1)



Step 2 Click  to add a static route.

The page shown in [Figure 7-209](#) is displayed.

Figure 7-209 Configuring the static route (2)

Add Static Route

Destination IP address/prefix length:

Interface:

Gateway IP Address:

Metric:

Step 3 Set parameters according to [Table 7-55](#).

Table 7-55 Parameter description

Parameter	Description
Destination IP address[/prefix length]	Indicates the destination IP address and subnet mask length of the static route, for example, 192.168.2.0/24.
Interface	Indicates the outbound port of the static route through which packets are sent to the destination network segment. The options are as follows: <ul style="list-style-type: none"> br0/br0: ports on the LAN side (LAN ports 1–4 and Wi-Fi port). pppoe_0_0_35/ppp1: ADSL port.
Gateway IP address	Indicates the next hop IP address for the static route.
Metric	Indicates the route metric, which must be an integer. If there are multiple routes to a destination IP address, the route with the smaller route metric has the higher priority. This parameter is optional.

Step 4 Click to save the settings.

[Figure 7-210](#) shows the configuration result.

Figure 7-210 Configuration result

Static Route Configuration

IP Version	DstIP/ Prefix Length	Gateway	Interface	Metric	Operation
4	192.168.2.0/24	192.168.1.3	br0	10	✘

[Add](#)

Description

The static route can improve network performance and ensure sufficient bandwidth for critical networks. When the network is faulty or the topology changes, the route may be unreachable. Then you must manually change the static route setting.

----End

7.5.6 VPN

EGW1520 can connect a branch network to the headquarters network using a VPN tunnel.

Description

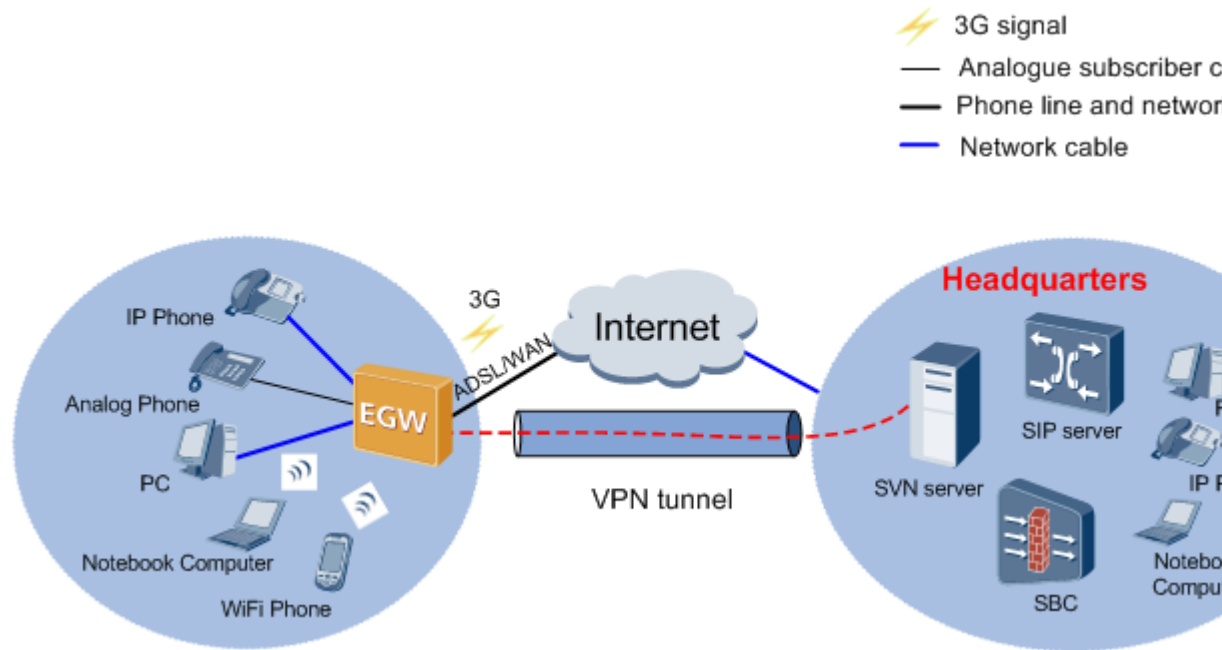
This topic describes the principle, implementation, specification, and limitation of the VPN features supported by the EGW1520.

Principle

Virtual Private Network (VPN) is a virtual network established based on the existing public network.

As a private network, a VPN exclusively occupies network resources. Additionally, internal data in a VPN cannot be accessed by external devices. [Figure 7-211](#) shows the typical VPN networking.

Figure 7-211 VPN networking



A VPN has the following advantages:

- It ensures data transmission security between the headquarters and remote users, remote branches, partners, and suppliers.
- The VPN reduces communication costs for enterprises because it is set up based on the public network.
- VPN users can be added and deleted by software configuration, without modifying hardware.
- Remote users can access the VPN any time and anywhere.

Implementation

EGW1520 uses the IP Security (IPSec) protocol to set up site-to-site (gateway to gateway) VPN tunnels between small branches and headquarters.

EGW1520 can set up VPN tunnels using the following methods.

Method	Usage Scenario	Remarks
The initiator and responder use fixed public IP address to set up VPN tunnels.	Both ends can specify the peer public IP address to initiate negotiation. The initiator and responder are not fixed. The two ends can only use tunnels to match traffic based on traffic characteristics.	Only large enterprises can apply fixed IP addresses for branches. EGW1520 is located on small branches, so it does not need to apply fixed IP addresses. Therefore, this scenario is rarely used.
The initiator uses a dynamic public IP address, and the responder uses a	The initiator EGW1520 accesses the Internet using a dynamic method, for example, PPPoE. The initiator's IP address	The initiator's IP address is not fixed, so VPN streams (the streams to be protected by IPSec) must be configured on

Method	Usage Scenario	Remarks
fixed public IP address.	changes every time it performs PPPoE dial-up. Therefore, the responder cannot specify the initiator's IP address. The responder does not need to specify the initiator's IP address, but the initiator must specify the responder's IP address; otherwise, negotiation will fail. The two ends can only use tunnels to match traffic based on traffic characteristics.	the initiator. The responder does not need to be configured with VPN streams because it can accept the VPN streams sent by the initiator during negotiation.
The initiator uses the 3G mode, and the responder uses a fixed public IP address.	When EGW1520 uses a 3G data card to dial up, it obtains a private IP address. The EGW1520 is the initiator and obtains IP addresses dynamically. Therefore, this scenario is similar to scenario 2.	Because the EGW1520 obtains a private IP address, IKE negotiation must use the aggressive mode and NAT traversal must be enabled.
The initiator uses domain names to set up VPN tunnels with the responder.	The initiator must know the domain name of the responder. The initiator uses domain names to set up VPN tunnels with the responder.	The responder uses a dynamic IP address and supports domain names.

Specification

- EGW1520 can connect to the headquarters using IPsec VPN tunnels.
- EGW1520 uses IPsec to set up site-to-site tunnels with the headquarters. As the initiator of VPN tunnels, EGW1520 uses the peer IP address or fully qualified domain name (FQDN) as the ID for IKE negotiation.

Limitation

- A maximum of 6 IPsec VPN tunnels are supported.
- The throughput of the IPsec VPN tunnel is not lower than 2 Mbit/s.
- A maximum of 32 concurrent connections are supported in an IPsec VPN.

Configuration

This topic describes how to set up VPN tunnels between branches and the headquarters.

Prerequisites

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

Procedure

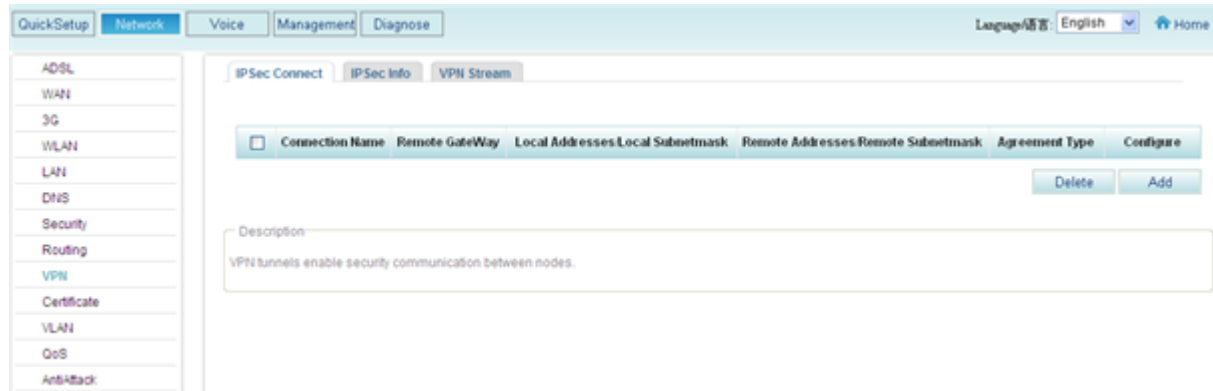
 **NOTE**

If the authentication method is **Certificate**, configure the certificate according to [7.5.7 Certificate](#).

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

The page shown in [Figure 7-212](#) is displayed.

Figure 7-212 Configuring the VPN (1)



Step 2 Click  .

The page shown in [Figure 7-213](#) is displayed.

Figure 7-213 Configuring the VPN (2)

The screenshot shows a web-based configuration interface for an Enterprise Gateway. The top navigation bar includes 'QuickSetup', 'Network', 'Voice', 'Management', and 'Diagnose'. The left sidebar lists various network services: ADSL, WAN, 3G, WLAN, LAN, DNS, Security, Routing, VPN (highlighted), Certificate, VLAN, QoS, and AntiAttack. The main configuration area is titled 'IPSec Connect' and contains several sections:

- IPSec Connect**: Includes fields for 'IPSec Connection Name', 'Tunnel Mode' (set to ESP), 'Remote IPsec Gateway Type' (radio buttons for IP and Domain, with IP selected), 'Remote IPsec Gateway Address (IPv4 address in dotted decimal)', 'Tunnel access from local IP addresses' (set to Subnet), 'IP Address for VPN' (192.168.1.0), and 'IP Subnetmask' (255.255.255.0).
- Remote IPsec Gateway**: Includes 'Tunnel access from remote IP addresses' (set to Subnet), 'IP Address for VPN', and 'IP Subnetmask' (255.255.255.0).
- Gateway ID**: Includes 'Gateway ID', 'Local ID Type' (IP Address), and 'Remote ID Type' (IP Address).
- Key Exchange and Authentication**: Includes 'Key Exchange Method' (Auto(IKE)), 'Authentication Method' (Pre-Shared Key), and 'Pre-Shared Key' (key).
- Perfect Forward Secrecy**: Includes radio buttons for 'Enable' and 'Disable' (with 'Disable' selected).
- Advanced IKE Settings**: Includes a 'Show' button.

At the bottom right, there are 'Back' and 'Save' buttons.

Step 3 Set parameters according to [Table 7-56](#).

NOTE

Both ends must use the same IPSec policies, including authentication methods, encryption methods, and negotiation modes.

Table 7-56 VPN parameters

Parameter	Description
IPSec Connection Name	Indicates the name of an IPSec tunnel, which is similar to a VPN ID. It is unique and can be customized. The value consists of numerals, letters, and underlines, and cannot start with a space, numeral, or underline.
Tunnel Mode	Indicates the security protocol used to create a tunnel. <ul style="list-style-type: none"> AH: implements data origin authentication, data integrity check, and packet anti-replay. It prevents data modification, but does not encrypt data. AH applies to non-confidential data transmission. ESP: implements data encryption, data origin authentication, and packet anti-replay. ESP applies to confidential data transmission. AH-ESP: AH and ESP are used together to protect data.
Remote IPSec Gateway Type	Indicates the remote gateway type: <ul style="list-style-type: none"> IP Name
Remote IPSec Gateway Address (IPv4 address in dotted decimal):	Indicates the peer gateway IP address.
Remote IPSec Gateway Name	Indicates the remote gateway domain name.
Tunnel access from local IP addresses	Indicates the filtering mode used by the local end to set up a VPN tunnel: <ul style="list-style-type: none"> Subnet: network segment where data needs to be transmitted over the VPN tunnel. Single Address: IP address of a terminal, such as PC.
IP Address for VPN	Indicates the network segment that the local device belongs to or fixed IP address of a terminal device.
IP Subnetmask	Indicates the subnet mask on the local end.
Tunnel access from remote IP addresses	Indicates the filtering mode used by the remote end to set up the VPN tunnel: <ul style="list-style-type: none"> Subnet: network segment where data needs to be transmitted over the VPN tunnel. Single Address: IP address of a terminal, such as PC.
IP Address for VPN	Indicates the network segment that the remote device belongs to or fixed IP address of a terminal device.
IP Subnetmask	Indicates the subnet mask on the remote end.
Local ID Type	Indicates the authentication type on the local end: <ul style="list-style-type: none"> IP Address: The IP address is used for IKE negotiation. Name: The domain name is used for IKE negotiation, which can be customized.

Parameter	Description
	<p>NOTE</p> <p>If the name is used as gateway ID, the Mode field in Advanced IKE Settings must be set to Aggressive.</p>
Remote ID Type	<p>Indicates the authentication type on the remote end:</p> <ul style="list-style-type: none"> • IP Address: The IP address is used for IKE negotiation. • Name: The domain name is used for IKE negotiation. <p>NOTE</p> <ul style="list-style-type: none"> • The domain names on the local end and remote end must be the same. • If the name is used as gateway ID, the Mode field in Advanced IKE Settings must be set to Aggressive.
Key Exchange Method	<p>Indicates the method of setting up secure communication:</p> <ul style="list-style-type: none"> • Manual: The configuration is complex. All SA information must be manually configured. The IPSec function is implemented independent of IKE. This mode is applicable when there are a few communicating devices on networks or the network size is small. • Auto (IKE): The configuration is simple. You only need to configure an IKE policy. The SA is set up and maintained through IKE negotiation. <p>The IKE mode is recommended.</p>
Authentication Method	<p>Indicates the authentication method:</p> <ul style="list-style-type: none"> • Pre-Shared Key: Use pre-shared key to perform authentication. • Certificate(X.509): Use certificate to perform authentication. Local certificate must be configured. For details, see 7.5.7 Certificate. <p>NOTE</p> <p>The CA certificates on the two ends must be the same.</p>
Pre-Shared Key	<p>Indicates the pre-shared key value, which can be entered by a user. The pre-shared keys on the two ends must be the same.</p>
Perfect Forward Secrecy	<p>Diffie-Hellman (DH) algorithm is a public key algorithm. The two communicating parties do not transmit a key but exchange data to calculate a shared key. The DH algorithm enables communicating parties to securely obtain public information.</p>
Advanced IKE Settings	<p>Indicates advanced parameters of VPN tunnels. For details, see Web Parameters Reference.</p>

Step 4 Confirm the settings and click  to save the settings.

----End

Configuring VPN Streams

VPN implements secure communication between the headquarters and branches. You can configure VPN streams so that branches can communicate through the VPN.

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

Step 2 Click the **VPN Stream** tab.

The page shown in [Figure 7-214](#) is displayed.

Figure 7-214 Configuring VPN streams (1)



Step 3 Click



The page shown in [Figure 7-215](#) is displayed.


Figure 7-215 Configuring VPN streams (2)



Step 4 Set parameters according to [Table 7-57](#).

Table 7-57 VPN stream parameters

Parameter	Description
VPN Stream Name	Indicates the name of a VPN stream, which can be customized. The value consists of numerals, letters, and underlines, and cannot start with a space, numeral, or underline.
IPSec Policy	Indicates the IPSec policy applied to VPN streams.
Tunnel access from local IP addresses	Indicates the filtering mode used by the local end to set up a VPN tunnel: <ul style="list-style-type: none"> Subnet: network segment where data needs to be transmitted over the VPN tunnel. Single Address: IP address of a terminal, such as PC.
IP Address for VPN	Indicates the fixed IP address in the local network segment or LAN.
IP Subnet mask	Indicates the subnet mask on the local end.
Tunnel access from remote IP addresses	Indicates the filtering mode used by the remote end to set up the VPN tunnel: <ul style="list-style-type: none"> Subnet: network segment where data needs to be transmitted over the VPN tunnel. Single Address: IP address of a terminal, such as PC.
IP Address for VPN	Indicates the fixed IP address in the remote network segment or LAN.
IP Subnetmask	Indicates the subnet mask on the remote end.

Step 5 Click  to save the settings.

----End

Typical Configuration Example

Network Requirements

- EGW1520 communicates with the headquarters through a VPN tunnel.
- The LAN port address of the EGW1520 belongs to 192.168.20.0/24 and the gateway address on the WAN port is 2.17.1.24.
- The SVN server at the headquarters is located on 192.168.30.0/24, and the gateway address is 6.16.5.6.

Typical Network

[Figure 7-216](#) shows the typical network.

Figure 7-216 Typical VPN network

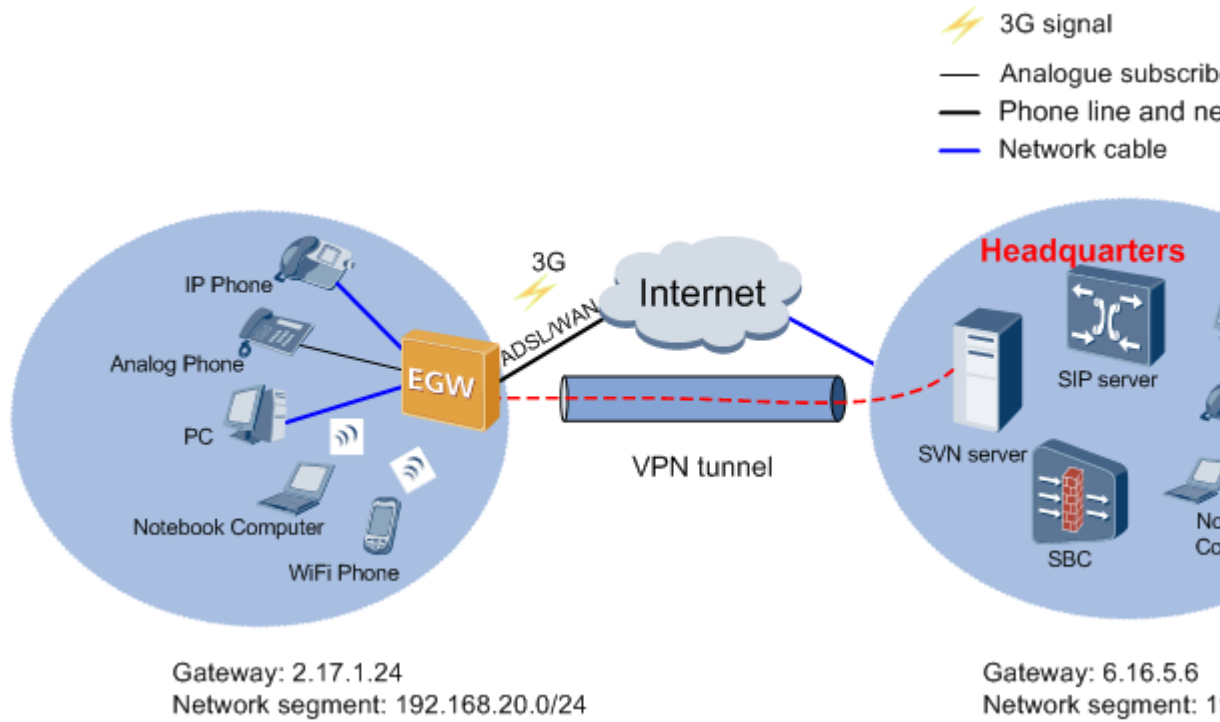


Table 7-58 lists the data plan.

Table 7-58 Parameter settings

Parameter	Example	
Local device	Remote IPsec gateway type	IP
	Remote IPsec gateway address	Headquarters gateway address: 6.16.5.6
	Tunnel access from local IP addresses	Subnet
	Source address	Network segment where the local device is located, for example, 192.168.20.0
	Tunnel access from remote IP addresses	Subnet
	Destination address	Network segment where the remote device is located, for example, 192.168.30.0

Remote device	Remote IPsec gateway type	IP
	Remote IPsec gateway address	Peer gateway IP address, for example, 2.17.1.24
	Tunnel access from local IP addresses	Subnet
	Source address	Network segment where the local device is located, for example, 192.168.30.0
	Tunnel access from remote IP addresses	Subnet
	Destination address	Network segment where the remote device is located, for example, 192.168.20.0

Configure the local end:


Step 1 Choose **VPN > IPsec Connect**.

Step 2 Set **Remote IPsec Gateway Type** to **IP**. Enter headquarters gateway address **6.16.5.6** in **Remote IPsec Gateway Address (IPv4 address in dotted decimal)**.

Step 3 Set **Tunnel access from local IP addresses** to **Subnet** and enter local end network segment **192.168.20.0** in **IP Address for VPN**.

Step 4 Set **Tunnel access from remote IP addresses** to **Subnet** and enter remote end network segment **192.168.30.0** in **IP Address for VPN**.

Step 5 Retain the default values for other parameters.

Step 6 Click  to save the settings.

----End

Configure the remote end:

 **NOTE**


In this example, the remote end is also an EGW1520.

Step 1 Set **Remote IPsec Gateway Type** to **IP**. Enter the remote gateway address **2.17.1.24** in **Remote IPsec Gateway Address (IPv4 address in dotted decimal)**.

Step 2 Set **Tunnel access from local IP addresses** to **Subnet** and enter remote end network segment **192.168.30.0** in **IP Address for VPN**.

Step 3 Set **Tunnel access from remote IP addresses** to **Subnet** and enter EGW1520 network segment **192.168.20.0** in **IP Address for VPN**.

Step 4 Retain the default values for other parameters.

Step 5 Click  to save the settings.

----End

Verifying the Configuration

The PCs at the EGW1520 side can communicate with the PCs at the headquarters.

Checking Monitoring Information

VPN monitoring information includes the connection status and traffic characteristics of the VPN tunnel.

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

Step 2 Click the **IPSec Info** tab.

The page shown in [Figure 7-217](#) is displayed.

Figure 7-217 Checking monitoring information



Connection Name	Remote Addresses	Phase 1 Connection States	Phase 2 Connection States	The Latest Error
a	190.168.5.1	Unconfigured	Unconfigured	

Remote Addresses	Type	SPI	Out/In Packets	Out/In Bytes	Clear SPI
190.168.5.1	src192.168.1.0/255.255.255.0des192.168.3.0/255.255.255.0		0/0	0/0	×

Step 3 View the parameters by referring to [Table 7-59](#).

Table 7-59 VPN monitoring parameters

Parameter	Description
Connection Name	Indicates the name of an IPSec tunnel.
Remote Addresses	Indicates the gateway IP address or domain name of the remote device.
Phase 1 Connection States	Indicates the phase 1 connection status in advanced settings.
Phase 2 Connection States	Indicates the phase 2 connection status in advanced settings.
The Latest Error	Indicates the last connection error of the VPN tunnel.
Type	Indicates the source address/subnet mask and destination

Parameter	Description
	address/subnet mask.
SPI	Indicates the Security Parameter Index (SPI) value. An SPI is a 32-bit string uniquely identifying an SA. It is transmitted in AH or ESP headers. NOTE After SPIs are deleted, the packet statistics are not cleared.
Out/Int Packets	Indicates the total number of packets sent and received by the VPN tunnel.
Out/In Bytes	Indicates the total number of bytes sent and received by the VPN tunnel.

 **NOTE**

The phase 1 and 2 connection status is displayed only when IKE negotiation mode is enabled.

----End

7.5.7 Certificate

The EGW1520 can use certificates to authenticate the VPN tunnel. The local certificate is used to authenticate the VPN tunnel set up between the EGW1520 and remote device. The local certificate requires the CA certificate signature.

 **NOTE**

Both the local certificate and CA certificate need to be configured.

CA Certificate

A CA certificate is issued by a certificate authority to authenticate the users attempting to access the virtual gateway.

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 **Network > Certificate** from the navigation tree.

Step 2 Click the **CA certificate** tab.

The page shown in [Figure 7-218](#) is displayed.

Figure 7-218 Configuring CA certificate (1)

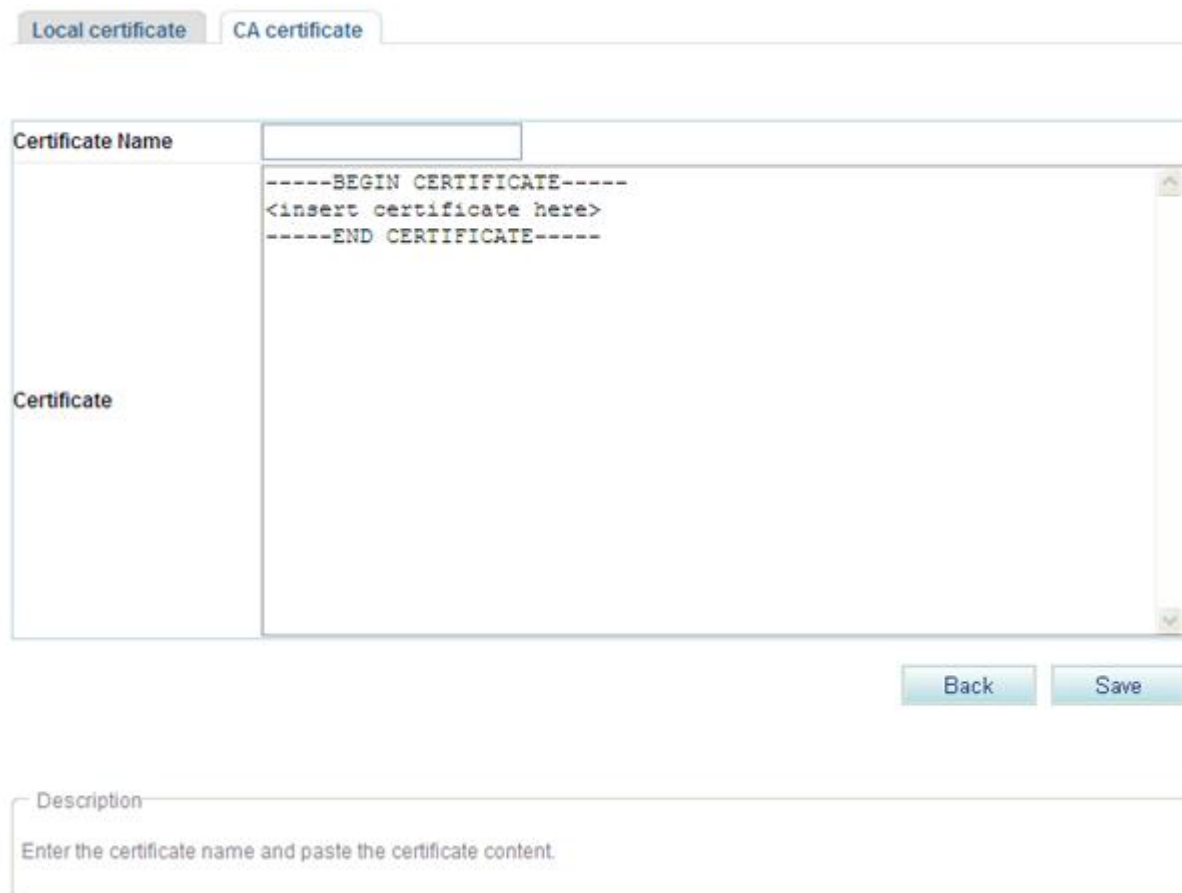


Step 3 Click



The page shown in [Figure 7-219](#) is displayed.

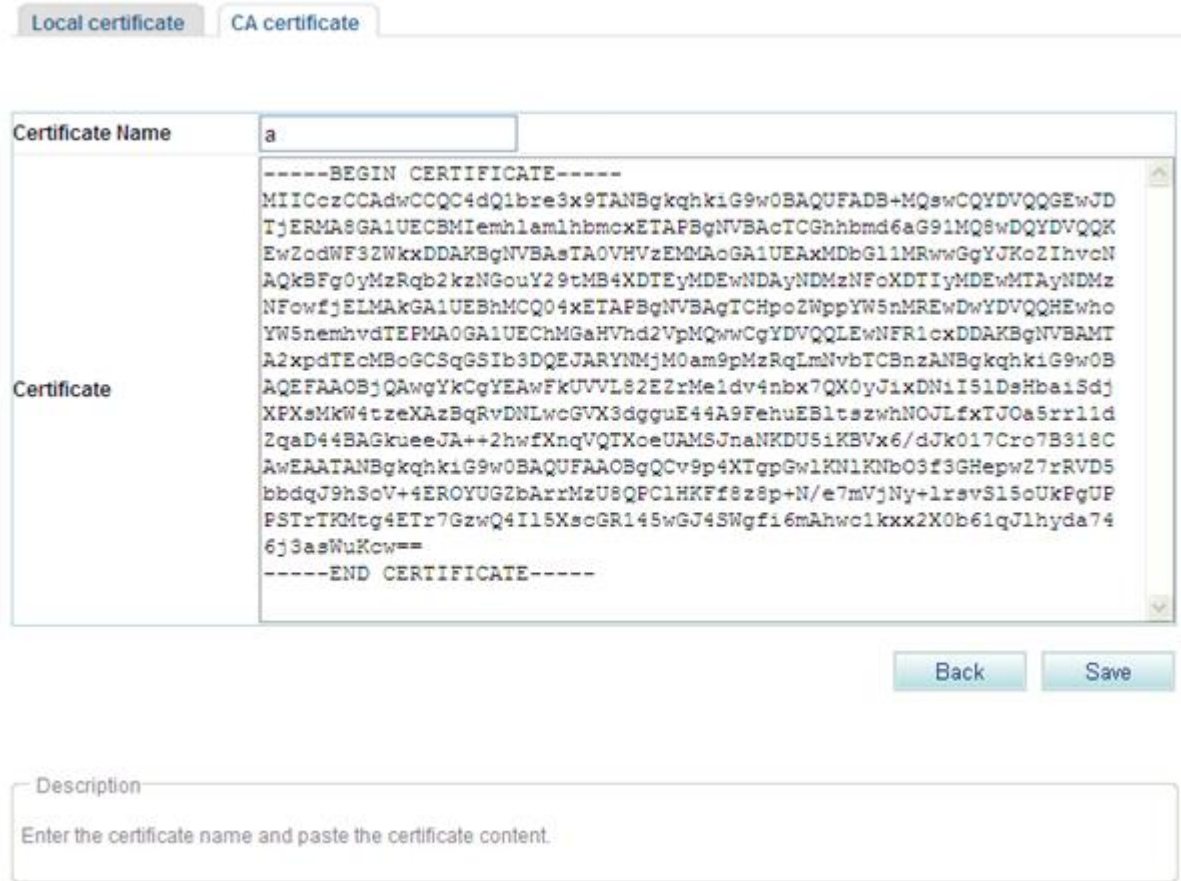
Figure 7-219 Configuring CA certificate (2)



Step 4 Enter the certificate name (customized) and paste the CA certificate into the **Certificate** text box.

The page shown in [Figure 7-220](#) is displayed.

Figure 7-220 Configuring CA certificate (3)



Local certificate CA certificate

Certificate Name a

Certificate

```
-----BEGIN CERTIFICATE-----
MIICozCCAdwCCQC4dQ1bre3x9TANBqkqhkiG9w0BAQUFADB+MQswCQYDVQQGEwJD
TjERMA8GA1UECBMIemhlamlhbmcxETAPBqNVBAcTCGhhbmd6aG91MQ8wDQYDVQQK
EwZodWF3Zm93Zm93Zm93Zm93Zm93Zm93Zm93Zm93Zm93Zm93Zm93Zm93Zm93Zm93
AQkBFg0yMzRqb2kzNGouY29tMB4XDTEyMDEwMDUyMjE1MDEwMDUyMjE1MDEwMDUy
NFowfjELMAkGA1UEBhMCQ04xETAPBqNVBAgTCHpoZWppYW5nMREwDwYDVQQHEwho
YW5nemhvdTEPMA0GA1UEChMGaHVhd2VpMQwwCgYDVQQLEwNFR1cxDDAKBqNVBAMT
A2xpdTEcMB0GCSqGSIb3DQEJARYNMjM0am9pMzRqLmNvbTCBnzANBqkqhkiG9w0B
AQEFAAOBjQAwwYkCgYEAwFkUVVL82E2rMe1dv4nbx7QX0yJ1xDN1I51DsHba1Sdj
XPXsMkW4tzeXAzBqRvDNLwGVX3dggue44A9FehuEB1tszwhNOJLfxTJOa5rr11d
ZqaD44BAGkueeJA++2hwfXnqVQTxeUAMSJnaNKDU5iKBVx6/dJk017Cro7B318C
AwEAATANBqkqhkiG9w0BAQUFAAOBqQCv9p4XTgpGw1KN1KNbO3f3GHepw27rRVD5
bbdqJ9hSoV+4EROYUGZbArrMzU8QPCLHKFf8z8p+N/e7mVjNy+1revS15oUkPqUP
PSTrTKMtg4ETr7GzwQ4I15XsoGR145wGJ4SWgf16mAhwc1kxx2X0b61qJlhyda74
6j3asWuKcw==
-----END CERTIFICATE-----
```


Back Save

Description

Enter the certificate name and paste the certificate content.

 **NOTE**

Obtain a CA certificate from a certificate authority.

Step 5 Click  to save the settings.

The page shown in [Figure 7-221](#) is displayed.

Figure 7-221 Configuring CA certificate (4)



----End

Local Certificate

Local certificate is used to authenticate VPN tunnels. It uses CA certificate to authenticate the users attempting to access the virtual gateway.

Prerequisites

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

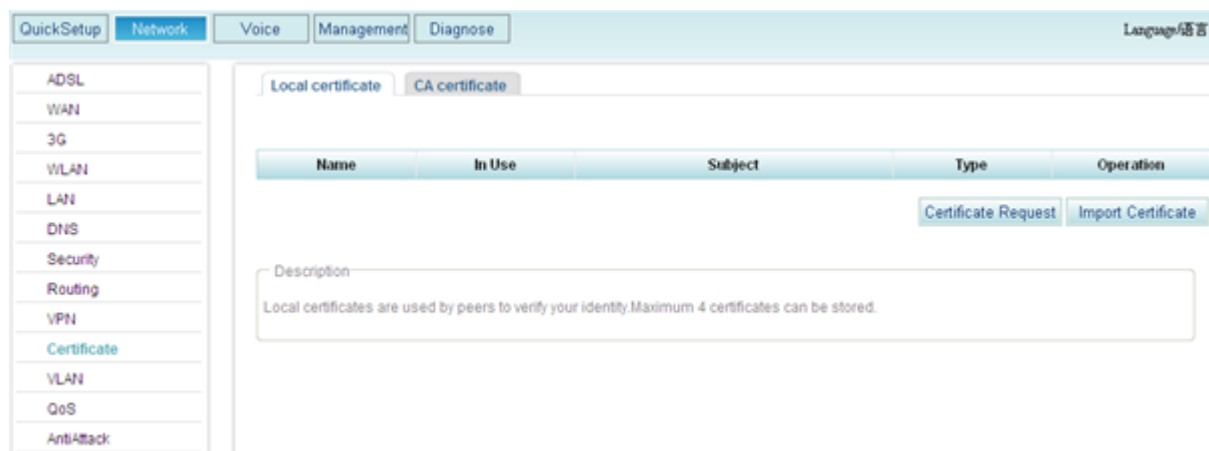
Procedure

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

Step 2 Click the **Local certificate** tab.

The page shown in [Figure 7-222](#) is displayed.

Figure 7-222 Configuring the local certificate (1)



Step 3 Select the certificate mode.

The local certificate can be created in either of the following ways:

- [Certificate Request](#)
- [Import Certificate](#)

If the **Certificate Request** mode is selected, perform the following operations:

1. Click [Certificate Request](#) to create a certificate request.
The page shown in [Figure 7-223](#) is displayed.

Figure 7-223 Configuring the local certificate (2)

2. Set parameters according to [Table 7-60](#).

Table 7-60 Certificate parameters

Parameter	Description
Certificate Name	Indicates the name of the created certificate, which can be customized.
Common Name	Indicates the common name of the certificate. For example, if the common name is a, a can contain the certificate names b and c.
Organization Name	Indicates the company name. NOTE This is the name of the company that applies for the CA certificate.
State/Province Name	Indicates the province where the company is located.

Parameter	Description
Country/Region Name	Indicates the country where the company is located.


- Click  to generate the certificate request file.
The page shown in [Figure 7-224](#) is displayed.

Figure 7-224 Configuring the local certificate (3)

Local certificate
CA certificate

Name	s
Type	request
Subject	CN=s/O=s/ST=s/C=CN
Signing Request	<pre>-----BEGIN CERTIFICATE REQUEST----- MIIBcDCB2gIBADAxMQowCAYDVQQDEwFzMQowCAYDVQQKEwFzMQowCAYDV QQIEwFzMQowCQYDVQQGEwJDTjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgY kCgYEAvm/NYU94gAKB1K6yXap8LCs/mpu30Z3k1Dc1URKgc6IUL98AOzk XsBJbq6A7UAzKG/AEoMXd8b1RwkzYNKRdNGw4dPSoc3w5DS4itVFKAuJq EUt/0IVBbj2EV8GehRAXHrq2IhJ1fjTXwahHdek33uWhmj8w7e1AO3eF8 tnSbsecCAwEAAaAAMA0GCSqGSIb3DQEBAUAA4GBAHqwJMz4Uu6PuGIFrC 9eyTMVzdDvWJWMDHNKU5z4mUFcd+J+Azu+NFFgERgddsCukaxrj3erd5D OVwPpYdx/1ut6aH5iBY25i1vibfrHqg9v54gbywFMCmo/5TB1Tk4v2Ovs dSQnq2ovyVKibHXNQtMJ+j50U5pgunTFHcFsF6hd-----END CERTIFICATE REQUEST-----</pre>

Back Load Certificate

Description

The certificate request file to sign has been created. To authenticate the certificate, the request file must be signed by the Certificate Authority (CA) and downloaded to the device.

 **NOTE**

This step only creates a certificate request file, but cannot make the certificate effective. To implement the certificate function, a CA signature is required.

The CA signature is obtained using the dedicated software, such as OpenSSL.

- Click .

The page shown in [Figure 7-225](#) is displayed.

Figure 7-225 Configuring the local certificate (4)

Local certificate CA certificate

Certificate Name s

Certificate

```
-----BEGIN CERTIFICATE-----  
<insert certificate here>  
-----END CERTIFICATE-----
```

Save

Description

Paste signed certificate.

Save

5. Paste the signed certificate into the **Certificate** text box and click  to save the settings.

If the **Import Certificate** mode is selected, perform the following operations:

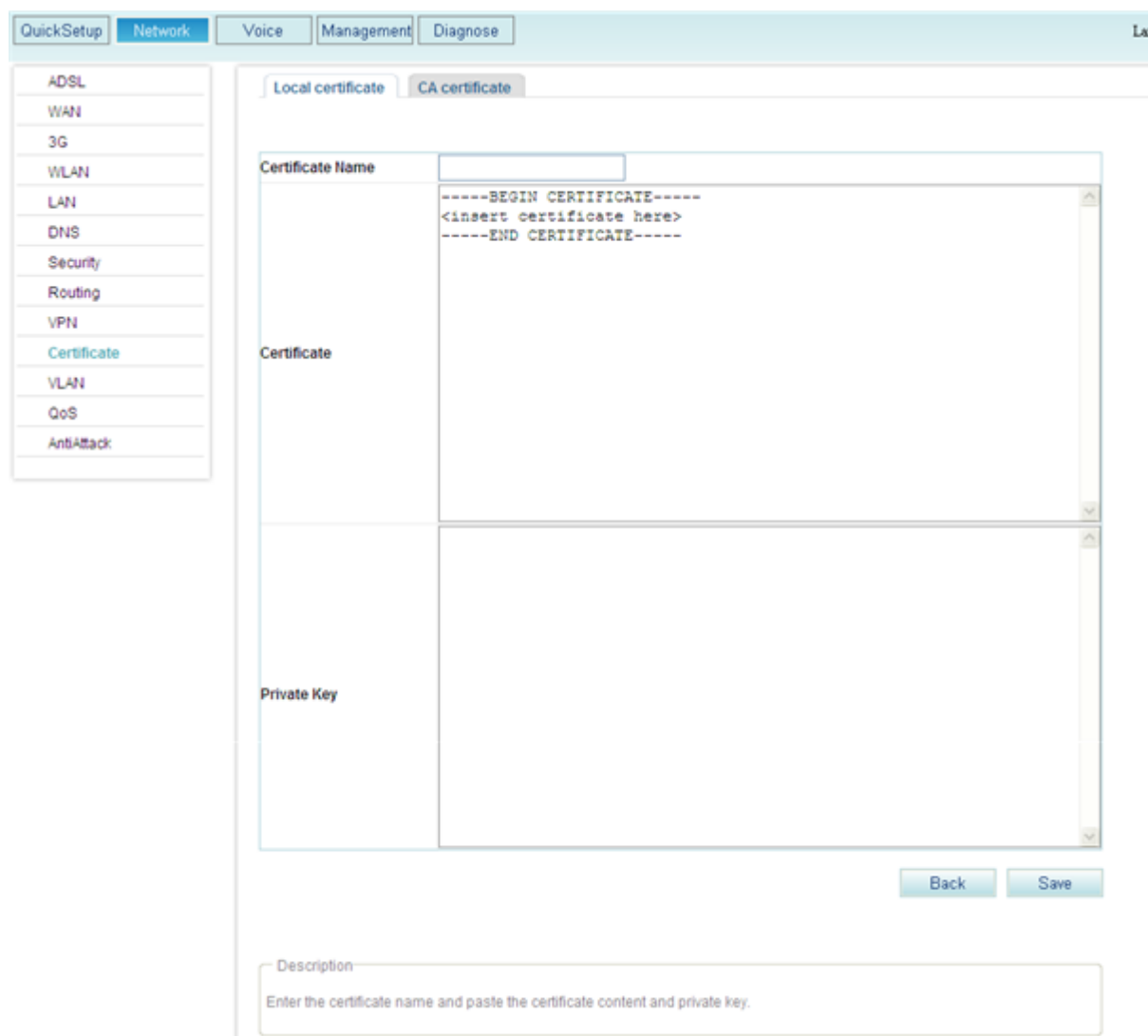
 **NOTE**


Ensure that a valid certificate file has been loaded to the local device.

1. Click .

The page shown in [Figure 7-226](#) is displayed.

Figure 7-226 Configuring the local certificate (5)



2. Enter the certificate name (customized), paste the certificate into the **Certificate** and **Private Key** text boxes.
3. Click  to save the settings.

 **CAUTION**

If the two ends cannot communicate with each other after the certificates are configured, change the system time in the EGW1520 systems according to [9.1 Configuring the System Time](#). The changed time must be later than the current time.

----End

7.5.8 VLAN

The VLAN technology divides a LAN to multiple virtual LANs (VLANs). Communication between hosts in a VLAN is the same as that in a LAN. A VLAN cannot directly communicate with another one. The EGW1520 supports port-based VLANs. Ports on the EGW1520 are classified into different VLANs, which separates users and creates virtual work groups.

Description

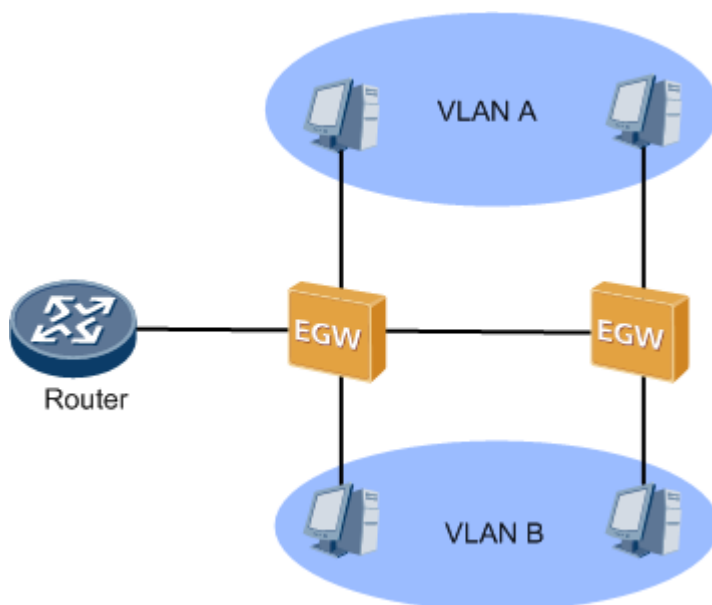
This topic describes the principle, implementation, specification, and limitation of the virtual local area network (VLAN) technology.

Principle

Based on Carrier Sense Multiple Access (CSMA) or Collision Detect (CD), Ethernet defines the data network communication technology related to media sharing. Numerous hosts may cause serious conflicts, excessive broadcast packets, and poor performance, and even network unavailability. Using switches to connect LANs reduces conflicts but cannot separate broadcast packets. In this background, the VLAN technology is generated to divide a LAN to multiple VLANs.

The VLAN is a technology to implement virtual work groups. The VLAN technology divides LAN devices to several logical network segments instead of physical network segments. Each VLAN is a broadcast domain. Hosts in a VLAN communicate with each other as if they were in a LAN. Hosts in different VLANs cannot directly communicate with each other, as shown in [Figure 7-227](#).

Figure 7-227 VLAN diagram



The VLAN has the following advantages:

- Restricts the broadcast domain

The broadcast domain is restricted to a VLAN, which saves bandwidth and improves network's processing ability.

- Enhances LAN security
Packets in a VLAN are separated from another VLAN. This makes users between VLANs unable to communicate with each other directly. A Layer 3 device (such as a router or a Layer 3 switch) is required to achieve cross-VLAN communication.
- Creates virtual work groups
The VALN classifies users to different work groups. Users in a work group are not limited to a certain physical scope, which makes network creating and maintenance flexible.

Implementation

VLANS can be created based on the port, MAC address, protocol, IP address mapping, multicast, or policy.

The EGW1520 supports only port-based VLANs. Ports connected to users are added to different VLANs so that users are separated and virtual work groups are divided.

When forwarding packets, ports process the tags contained in packets. Based on the processing mode, ports are classified into the following types:

- 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 VLANs, and are always connected to other EGW1520s or switches. Two ports that are connected must belong to the same VLAN.

Type	Processing for a Received Packet		Processing for a Packet to Be Sent
	Packet Without a Tag	Packet with a Tag	
Access port	Adds the VLAN ID of the port to the packet as the tag.	<ul style="list-style-type: none"> • Accepts the packet when the VLAN ID of the packet is the same as the VLAN ID of the port. • Discards the packet when the VLAN ID of the packet is different from the VLAN ID of the port. 	Removes the tag and sends the packet.
Trunk port	Adds the VLAN ID of the port to the packet as the	<ul style="list-style-type: none"> • Accepts the packet when the VLAN ID of the packet is allowed to pass 	<ul style="list-style-type: none"> • Removes the tag and sends the packet when the VLAN ID of the packet is the same as the VLAN ID of the port and the VLAN ID is

Type	Processing for a Received Packet		Processing for a Packet to Be Sent
	Packet Without a Tag	Packet with a Tag	
	tag.	through the port. <ul style="list-style-type: none"> Discards the packet when the VLAN ID of the packet is not allowed to pass through the port. 	allowed to pass through the port. <ul style="list-style-type: none"> Retains the tag and sends the packet when the VLAN ID of the packet is different from the VLAN ID of the port and the VLAN ID is allowed to pass through the port.

Specification

A maximum of four ports used to assign VLANs

Restriction

The VLAN ports support only the port-based VLANs.

Configuration

This topic describes how to change the default VLAN for a port and add a port to a VLAN.

Prerequisites

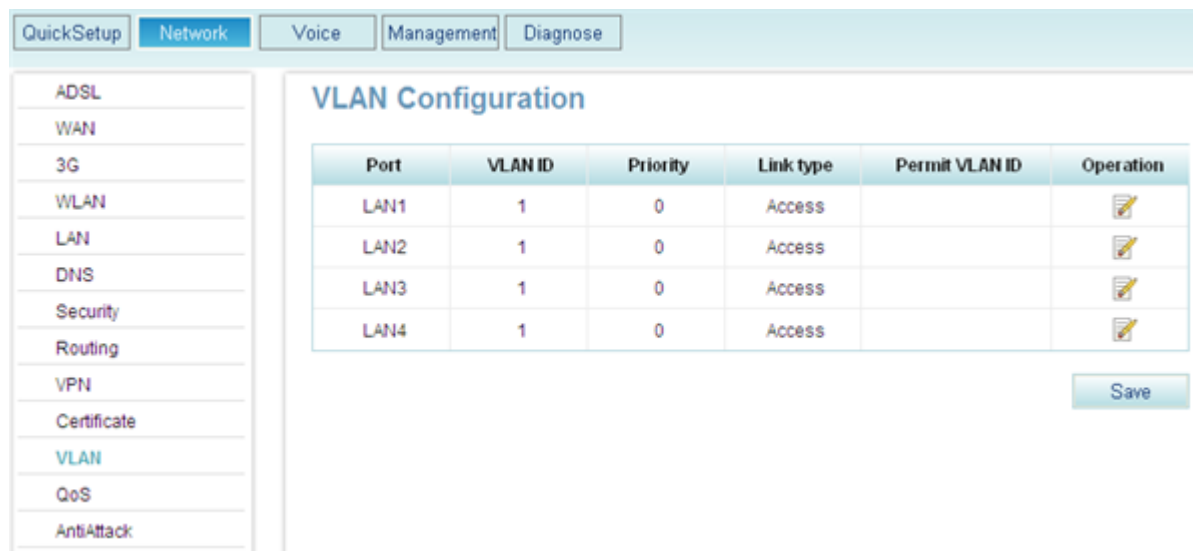
You have logged in to the web management system. For details, see [7.7.1 Web Management](#).

Procedure

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

The page shown in [Figure 7-228](#) is displayed.

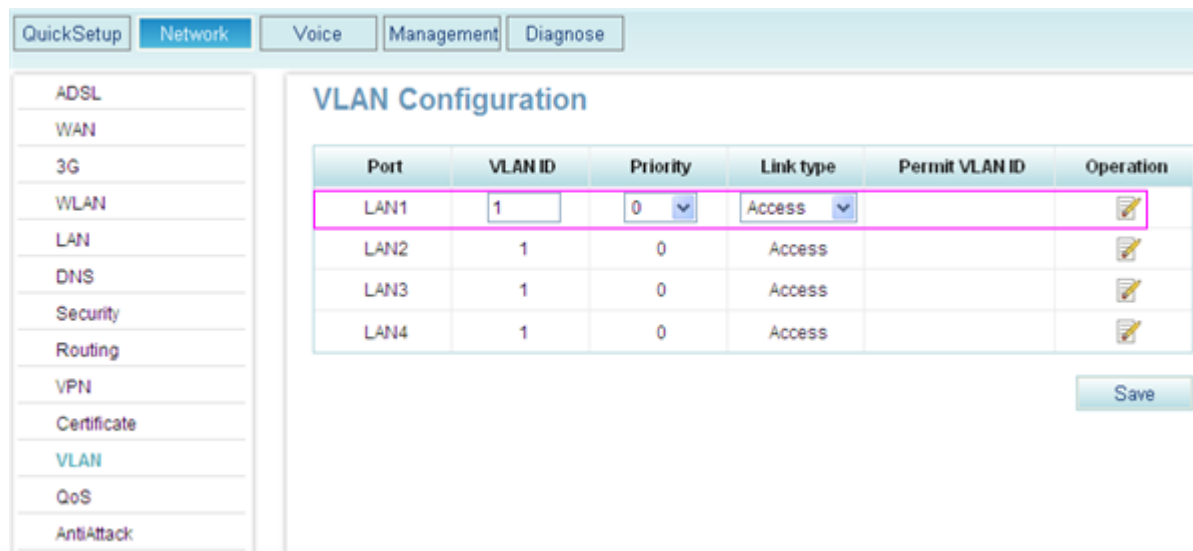
Figure 7-228 Configuring the VLAN (1)



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

The page shown in [Figure 7-229](#) is displayed.

Figure 7-229 Configuring the VLAN (2)




Step 3 Set parameters according to [Table 7-61](#).

Table 7-61 VLAN parameters

Parameter	Description
Port	Indicates the LAN port on the EGW1520. The EGW1520 provides four LAN ports (LAN1 to LAN4).

Parameter	Description
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

Typical Configuration Example

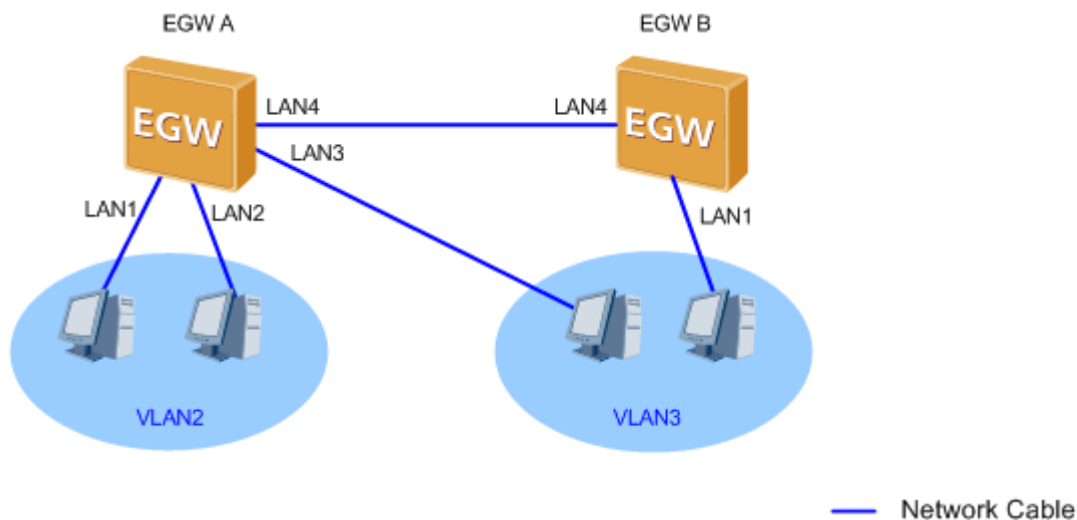
Network Requirements

- VLAN3 is a cross-device VLAN. VLAN2 contains LAN1 and LAN2 on the EGW1520 A. VLAN3 contains LAN3 on EGW1520 A and LAN1 on EGW1520 B.
- The requirement is that hosts in the same VLAN can communicate with each other. Hosts in VLAN2 can communicate with each other and hosts in VLAN3 can communicate with each other.

Typical Network

Figure 7-230 shows the typical network.

Figure 7-230 Typical VLAN network



Procedure

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**.
2. Change the connection type to **Trunk** for LAN4 on EGW1520 A, and set the VLAN changing range to 3.



3. Click  to save the settings.

[Figure 7-231](#) shows the configuration result.

Figure 7-231 Configuration result (1)

The screenshot shows the Network Configuration page with the VLAN Configuration section expanded. The configuration table is as follows:

Port	VLAN ID	Priority	Link type	Permit VLAN ID	Operation
LAN1	2	0	Access		
LAN2	2	0	Access		
LAN3	3	0	Access		
LAN4	1	0	Trunk	3	

A Save button is located at the bottom right of the configuration table.

4. Change the VLAN IDs to **VLAN 3** for LAN1 on EGW1520 B. Set the connection type to **Access**.

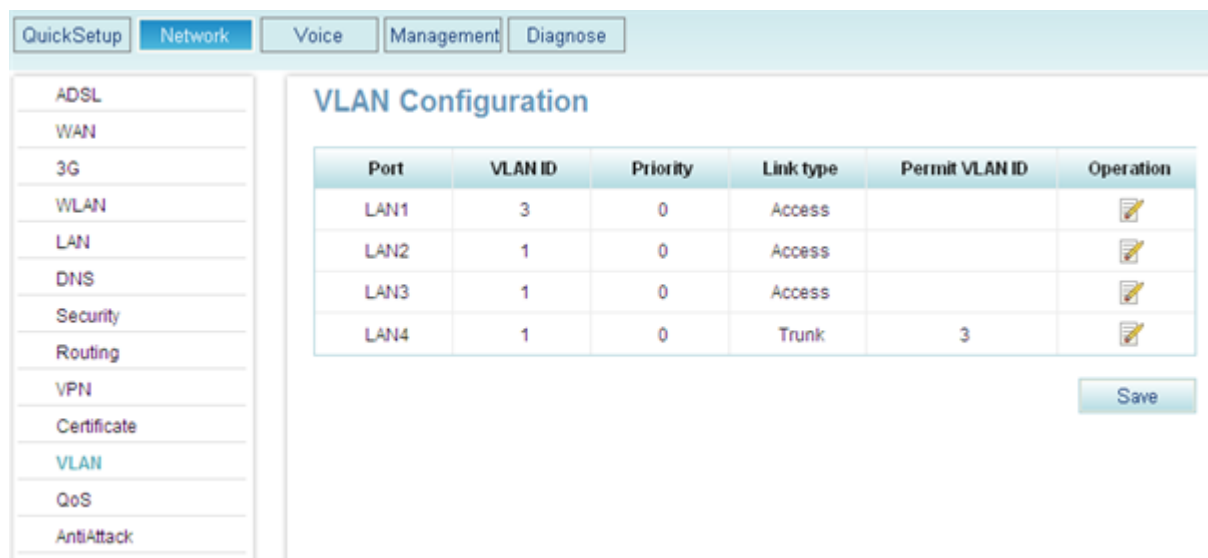
- Change the connection type to **Trunk** for LAN4 on EGW1520 B, and set the VLAN changing range to 3.



- Click  to save the settings.

[Figure 7-232](#) shows the configuration result.

Figure 7-232 Configuration result (2)



Verification

Hosts in the same VLAN can communicate with each other.

7.5.9 QoS

The EGW1520 provides a comprehensive QoS mechanism, for example, make QoS policies as required. This ensures precedence of core services. In addition, the EGW1520 limits bandwidth for ordinary services (such as web upload) and saves it for core services (such as voice streams). The EGW1520 supports the following Diff-Serv-based QoS technologies: priority mark, congestion management, and traffic policy.

Description

This topic describes the principle and implementation of QoS.

Principle

Traditional IP network handles all packets equally and uses the First In First Out (FIFO) method to transfer packets. Resources used to forward packets are allocated in the arrival order of packets. All packets share network resources, for example, bandwidth. The quantity of the resources that can be obtained depends on the arrival time of packets. This policy is called Best-Effort (BE). The device in this mode transmits packets to the destination. The BE mode, however, does not ensure the short delay, jitter, packet loss ratio, or high reliability.

With the rapid development of the computer network, an increasing number of networks access the Internet. The Internet expands greatly in size, scope, and user quantity.

More and more users use the Internet as a platform for data transmission and implementation of various applications. Apart from traditional applications such as WWW, email, and File Transfer Protocol (FTP), the Internet has been expanded to provide other services such as eLearning, eHealth, video calling, video conferencing, and video on demand (VoD). Enterprise users want to join their branches in different areas through a Virtual Private Network (VPN) to access an enterprise's databases. In addition, the headquarters of the enterprise can manage remote devices through Telnet. In addition, service providers also want to develop new services to increase revenues.

The new services pose special requirements for bandwidth, delay, and jitter. For example, video conferencing and VoD require a high bandwidth, low packet loss ratio, short delay, and low jitter. Key tasks (such as transaction processing and Telnet) do not require a high bandwidth. They, however, focus on short delays and preferential handling in case of congestion.

New services pose higher requirements for the IP network's service capability. Users are not only satisfied with packet transmission to the destination. They need better services, for example, dedicated bandwidth, lower packet loss ratio, management and avoidance of network congestion, and network traffic control. These requirements demand better service capabilities from the network.

QoS is used to assess the ability of the network to transmit packets. It provides various functions, such as priority mark, congestion management, and traffic policing.

Implementation

The EGW1520 provides a comprehensive QoS mechanism, for example, make QoS policies as required. This ensures precedence of core services. In addition, the EGW1520 limits bandwidth for ordinary services (such as web upload) and saves it for core services (such as voice streams). EGW1520 forwards voice data first when network congestion occurs. The EGW1520 supports the following Diff-Serv-based QoS technologies: priority mark, congestion management, and traffic policy.

Priority Mark

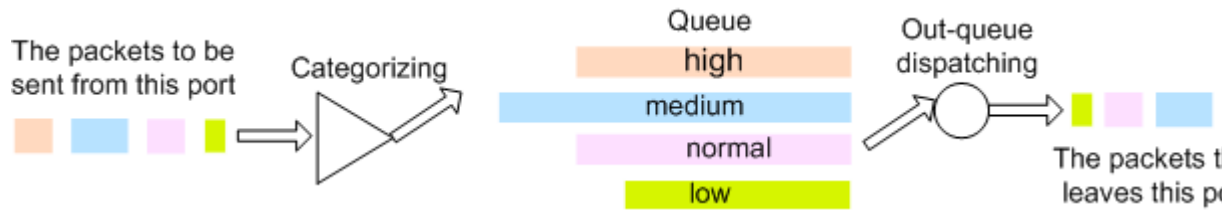
EGW1520 marks priorities of packet categories as a user requires. For example, increase the voice packet priority to achieve short delay and low jitter, and to ensure call quality. Priorities can be marked with a differentiated services code point (DSCP) value, DSCP value ranges from 0 to 63.

Congestion Management

Congestion management is a solution to resource competition. Packets are buffered in queues and a scheduling algorithm is used to determine the packet forwarding sequence. Congestion management is applied to the outbound interface.

EGW1520 uses the Priority Queue (PQ) scheduling mechanism. For the IP network, PQ classifies packets based on the IP precedence, quintuple information, and DSCP value. Then PQ sends packets to queues by packet type. When leaving queues, packets with a low priority are not sent until packets with a higher priority have been sent, as shown in [Figure 7-233](#).

Figure 7-233 PQ scheduling



If a new packet comes when packets with a lower priority are being sent, the new packet will be sent immediately while packets with the lower priority stop to be sent. This enables the packets related to cores services (such as VoIP) to be handled earlier. The packets related to ordinary services (such as email) are handled when core services are all handled and the network is idle. By doing so, key services are handled earlier and network resources are also fully used.

Traffic Policing

EGW1520 can limit the upstream and downstream bandwidth for the specified flows.

Configuration

This topic describes how to configure the QoS function. Only network administrators can change the QoS setting. To ensure the normal running of the EGW1520, you are advised to use the default settings.

Prerequisite

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

Context

[Table 7-62](#) describes an example of QoS configuration. The actual configuration varies according to service requirement.

Table 7-62 Configuring QoS

Data Flow	Classification Interface	Classification Parameter	QoS Interface	QoS Scheme
SIP signaling data flow generated on an analog phone	Local	Protocol: User Datagram Protocol (UDP); Port number: UDP port number 5060	WAN, ADSL	Put the flow to a queue, the precedence value of which is 1. Mark the Differentiated Services Code Point (DSCP) value of the packets.
RTP/RTCP service flow generated on an	Local	Protocol: UDP; Port number: UDP port	WAN, ADSL	Put the flow to a queue, the precedence

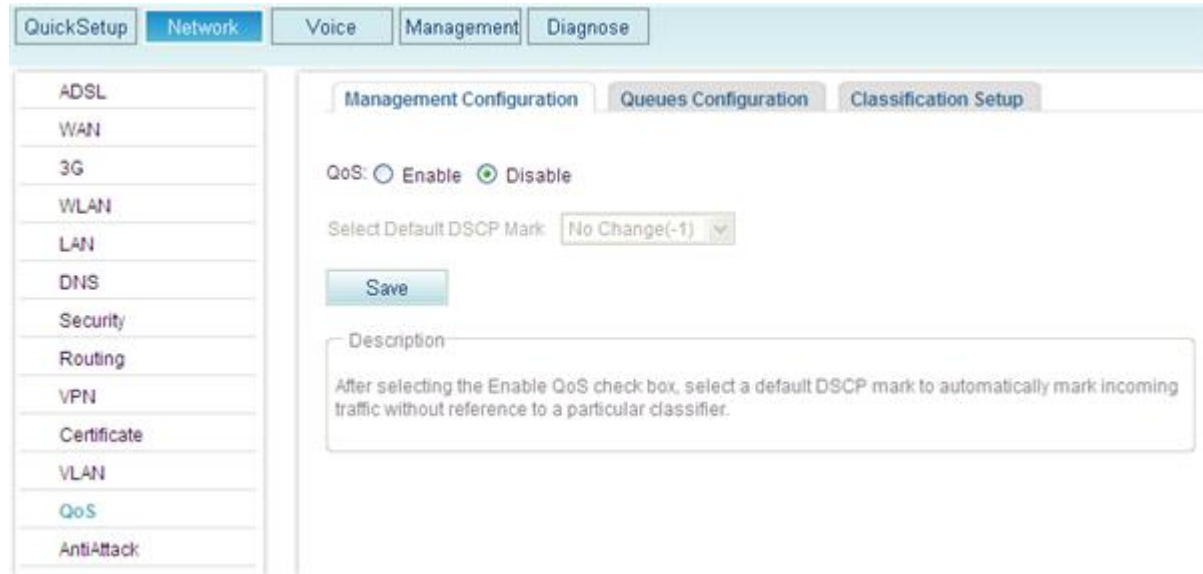
Data Flow	Classification Interface	Classification Parameter	QoS Interface	QoS Scheme
analog phone		number		value of which is 2. Mark the DSCP value of the packets.
Data flow generated by management and support operations on EGW1520	Local	Select the protocol and port number based on the actual situation.	WAN, ADSL	Put the flow to a queue, the precedence value of which is 3. Mark the DSCP value of the packets.
SIP signaling data flow generated on an IP phone	LAN (Eth0–Eth3)	Source IP address; Protocol: UDP; Port number: UDP port number 5060.	WAN, ADSL	Put the flow to a queue, the precedence value of which is 1. Mark the DSCP value of the packets.
RTP/RTCP service flow generated on an IP phone	LAN (Eth0–Eth3)	Source IP address; Protocol: UDP; Port number: UDP port number	WAN, ADSL	Put the flow to a queue, the precedence value of which is 2. Mark the DSCP value of the packets.
Data flow generated on the terminals (such as, HTTP, Email, and P2P)	LAN (Eth0–Eth3)	Select the protocol and port number based on the actual situation.	WAN, ADSL	Put the flow to a queue, the precedence value of which is 3. Mark the DSCP value of the packets and set the upper limit of transmission rate.


Procedure

Step 1 Enable the QoS function.

1. On the web management system, choose **Network > QoS** from the navigation tree.
The page shown in [Figure 7-234](#) is displayed.

Figure 7-234 Enabling the QoS function globally

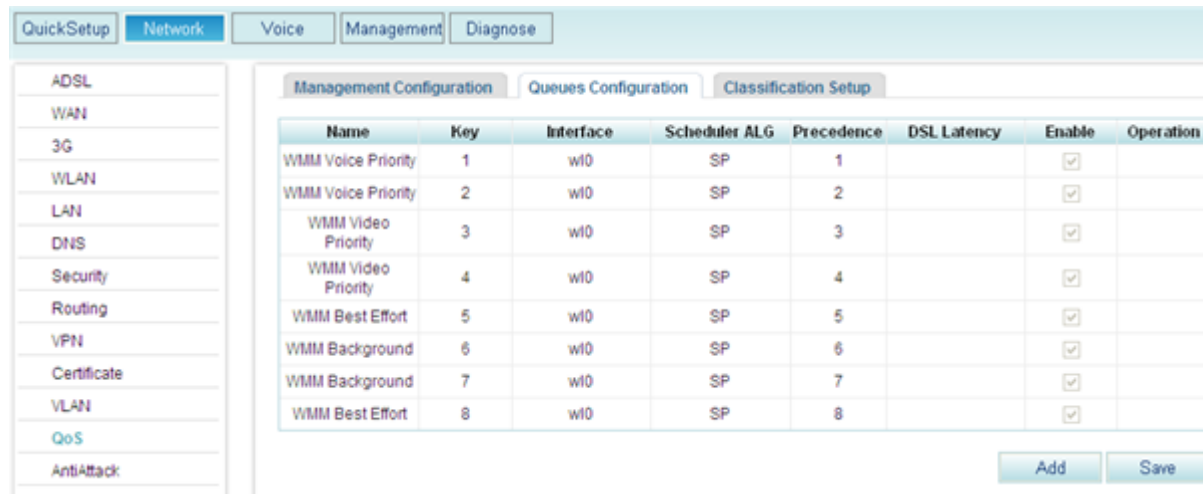


2. Click **Enable**.
3. (Optional) Select a DSCP value from the **Select Default DSCP Mark** drop-down list box. To allow an upstream device to implement QoS, you must mark packets that match no QoS rule with a DSCP value. For example, if AF13(001110) is selected, packets that do not match any QoS rule are marked with AF13(001110).
4. Click .

Step 2 Set a precedence value to a queue.

1. Click the **Queues Configuration** tab.
The page shown in [Figure 7-235](#) is displayed.

Figure 7-235 Setting the queue priority on interfaces (1)




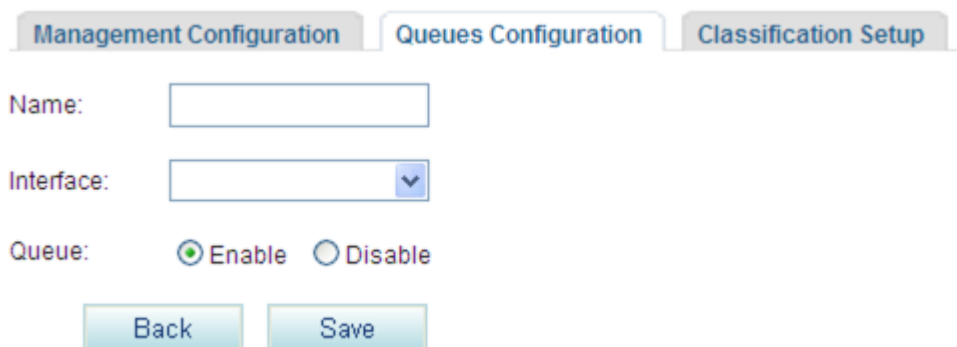
2. Click  .
The page shown in [Figure 7-236](#) is displayed.

Figure 7-236 Setting the queue priority on interfaces (2)



3. Set parameters according to [Table 7-63](#).

Table 7-63 Parameter description

Parameter	Description
Name	Indicates the name of a queue.
Interface	Indicates the interface that takes QoS behaviors. The options are as follows: <ul style="list-style-type: none"> • eth-lan: LAN port. LAN ports 1–4 are available. • eth-wan(wan): WAN port. • atm0: ADSL port.
Queue	Indicates whether to enable the queue. The options are as follows: <ul style="list-style-type: none"> • Enable • Disable

4. Click  to save the settings.

Step 3 Classify data flows and add a data flow in a queue.

1. Click the **Classification Setup** tab.
The page shown in [Figure 7-237](#) is displayed.

Figure 7-237 Classifying data flows (1)




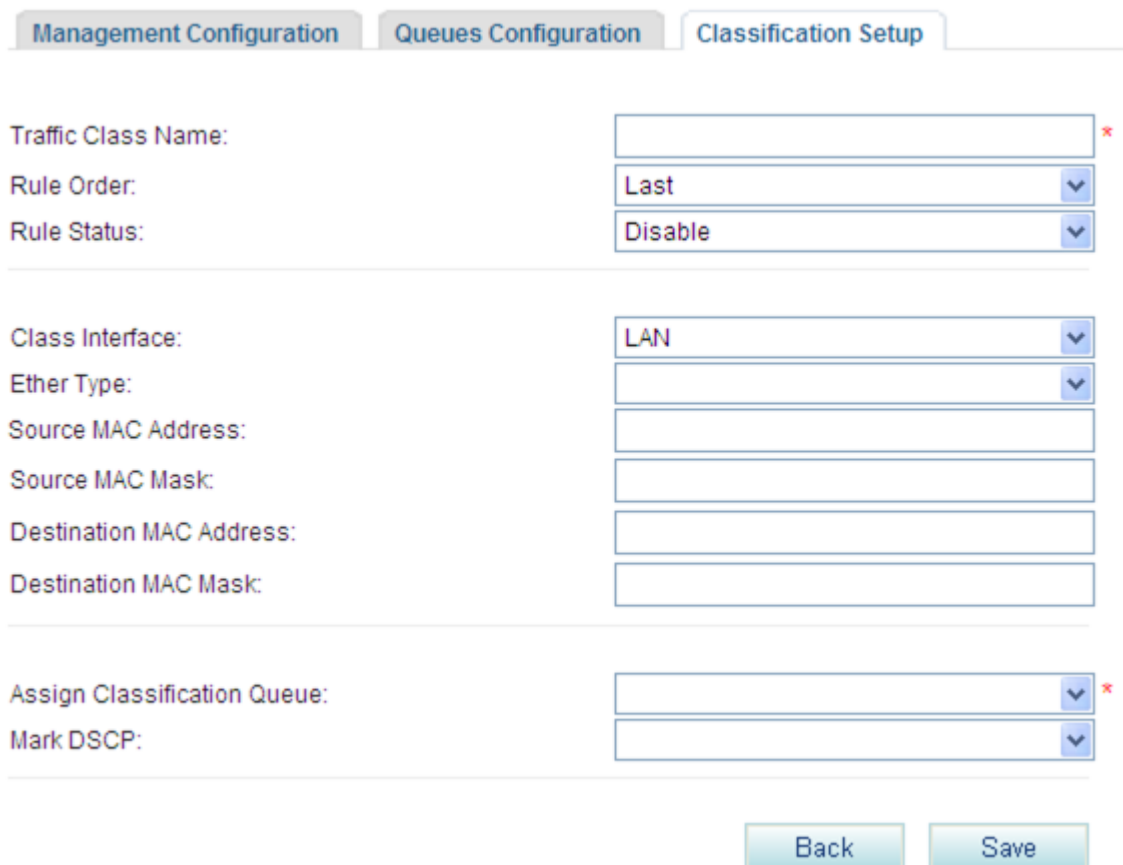
2. Click  .
The page shown in [Figure 7-238](#) is displayed.

Figure 7-238 Classifying data flows (2)



3. Set parameters according to [Table 7-64](#).

Table 7-64 Parameter description

Parameter	Description
Traffic Class Name	Name of a data flow class.
Rule Order	Order for sending data flows. The Last value indicates a data flow is the last one to be sent.
Rule Status	Whether to enable the rule. The options are as follows: <ul style="list-style-type: none"> • Enable • Disable
Class Interface	Port that requires data flow classification. <ul style="list-style-type: none"> • LAN: LAN ports 1–4 and Wi-Fi port. • WAN: ADSL and WAN ports. • local: data flows that the EGW1520 generates. • eth-lan: LAN ports 1–4. • wl0: WLAN port. • atm0: ADSL port. • eth-wan: WAN port.
Ether Type	Type of packets that need to be classified. <ul style="list-style-type: none"> • IP(0x800): IP packets. • ARP(0x806): ARP packets. • IPv6(0x86DD): IPv6 packets. • PPPoE_DISC(0x8863): packets in the PPPoE discovery stage. • PPPoE_SES(0x8864): packets in the PPPoE session stage. • 8865(0x8865): 8865 packets. • 8866(0x8866): 8866 packets. • 8021Q(0x8100): 802.1q packets. <p>NOTE The following uses IP packets as an example.</p>
Source MAC Address	Source MAC address in the packet.
Source MAC Mask	Source MAC mask in the packet.
Destination MAC Address	Destination MAC address in the packet.
Destination MAC Mask	Indicates the destination MAC mask in the packet.
Assign Classification Queue	Adds the packet to a configured queue.
Mark DSCP	Marks the packet with a DSCP value.

 **NOTE**

For details about other parameters, see [Web Parameter Reference](#).

4. Click  to save the settings.

----End

Typical Example: Transmitting Voice Service Packets First

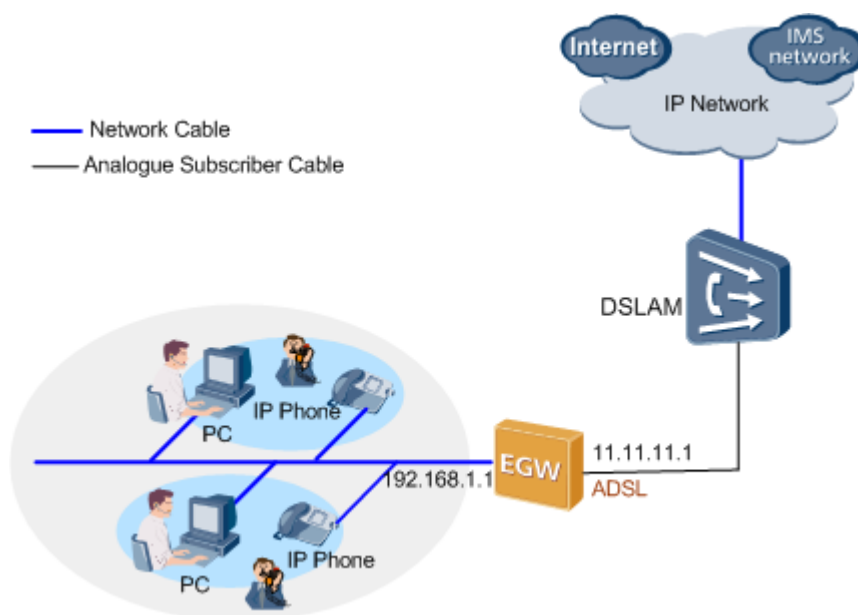
Network Requirements

- The EGW1520 uses an ADSL port to connect to the Internet. The IP address of the WAN port is 11.11.11.1.
- Computers and IP phones use LAN ports to connect to the EGW1520. As the DHCP server, the EGW1520 allocates IP addresses for the computers and IP phones.
- Configure the QoS to make voice service packets transmitted before data service packets. Voice service packets are transmitted first during heavy-traffic periods.

Typical Network

Figure 7-239 shows the typical network.

Figure 7-239 QoS typical network



Configuration Procedure

 **NOTE**

- For details on how to use an ADSL port to connect to the upstream network, see [7.2.1 ADSL](#).
 - For details on how to configure the DHCP server, see [Configuration](#).
 - For details on how to add SIP users, see [Adding Voice Users](#).
1. [Enable the QoS function](#).

2. Configure two queues (queue-voice1 and queue-voice2) for the voice flow. Set the LAN and ADSL ports to where the QoS works, and set the two queues to the highest precedence (0). For details, see [Set a precedence value to a queue](#).
3. Determine fields in the voice flow according to the network requirements. For example, the source IP address (IP address of the IP phone), protocol type (UDP) and port number (5060) of IP phone's SIP signaling.
4. Configure the voice flow classification field. Add the matching voice flow to the queues with higher precedence (queue-voice1 and queue-voice2). In addition, mark the DSCP flag of the voice flow with the highest precedence. For details, see [Configure data flow classification parameters and add a data flow in a queue](#).

After the configuration is complete, the EGW1520 transmits voice flow through the ADSL and LAN ports. Based on the DSCP flag, the network device that supports QoS (Router A in this example) performs QoS scheduling for the voice flow that the EGW1520 transmit.

Typical Example: Limiting Bandwidth for Web Upload Service

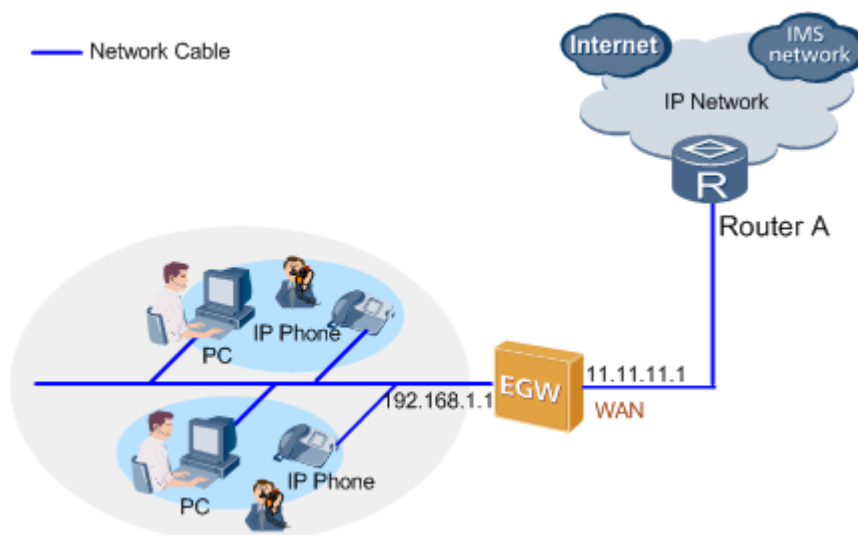
Network Requirements

- The EGW1520 uses a WAN port to connect to the Internet. The IP address of the WAN port is 11.11.11.1.
- Computers and IP phones use LAN ports to connect to the EGW1520. As the DHCP server, the EGW1520 allocates IP addresses for the computers and IP phones.
- QoS is required to limit bandwidth for the web upload service.

Typical Network

Figure 7-240 shows the typical network.

Figure 7-240 QoS typical network



Configuration Procedure



NOTE

- For details on how to use a WAN port to connect to the upstream network, see [7.2.2 WAN](#).
- For details on how to configure the DHCP server, see [Configuration](#).
- For details on how to add SIP users, see [Adding Voice Users](#).

1. [Enable the QoS function](#).
2. Configure a queue (queue-web) for web upload service packets. Set the WAN port to where the QoS works, and set the queue to a low precedence (for example, 3). For details, see [Set a precedence value to a queue](#).
3. Determine fields in the web upload data flow according to the network requirements. For example, the source IP address (IP address of the computer), protocol type (TCP) and port number (80) of web upload data flow.
4. Configure the web upload data flow classification field. Add the matching web upload data flow to the queue-web. In addition, set the maximum rate for transmitting web upload data flow (for example, 10 kbit/s). For details, see [Configure data flow classification parameters and add a data flow in a queue](#).



NOTE

When configuring QoS, enter the source or destination IP addresses of the flows to be matched.

After the configuration is complete, the EGW1520 transmits the web upload data flow through the WAN port at a lower precedence, and limits the bandwidth within 10 kbit/s.

7.5.10 Anti-attack

The EGW1520 can protect networks against various attacks such as flood attack and malformed packet attack, ensuring normal operation of internal networks and systems.

Description

The EGW1520 can prevent the following attacks.

Type	Description
Special source IP attack	An attacker sends packets with forged source IP address 0.0.0.0, 255.255.255.255, X.X.X.0, or X.X.X.255.
Large ICMP packet attack	An attacker sends oversized ICMP packets to the target system. Some systems or devices cannot process oversized ICMP packets. If they receive such packets, they may stop responding, crash, or restart.
Unknown protocol attack	The protocol type field in an IP header is set to an invalid value, which cannot be identified by the target system. Frequent processing of this type of packets wastes system resources and causes performance deterioration.
ICMP Flood attack	An attacker sends a large number of ICMP packets, such as ping packets, to a server. As a result, the server is overloaded and cannot process normal data packets.
SYN Flood attacks	The TCP/IP protocol stack permits limited TCP connections due to resource restriction. Taking advantage of the defect of TCP/IP, the SYN Flood attack forges a SYN packet whose source address is a bogus or non-existent address and initiates a connection to the server. Accordingly, the server will not receive the ACK packet for its SYN-ACK packet, which forms a semi-connection. A large number of

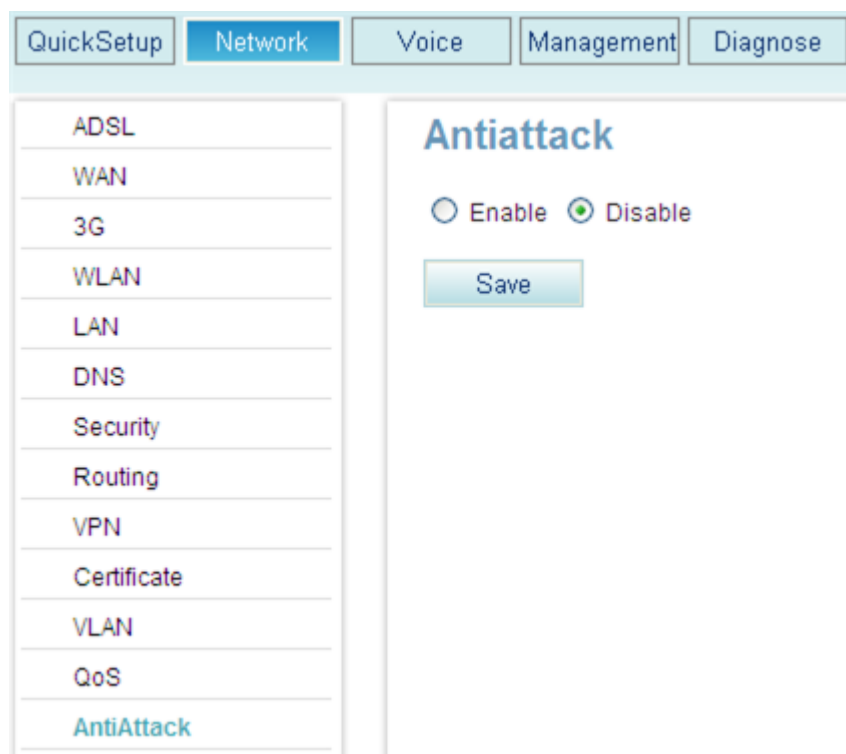
Type	Description
	semi-connections will exhaust network resources. As a result, authorized users cannot access the network until the semi-connections time out. The SYN Flood attack also occurs in the applications whose connection number is not limited to consume the system resources such as memories.
UDP Flood attack	When initiating a UDP flood attack, the attacker sends a large number of UDP packets to the specific target in a short time so that the target system is unable to transmit valid packets.
Land attack	Land attack sets both the source and destination addresses of a TCP SYN packet to the IP address of the attacked target. The target then sends the SYN-ACK message and sends back the ACK message to itself. This creates a null connection. Each null connection will be saved until timeout. Different attacked targets have different responses to the Land attack. For example, UNIX hosts may crash and Windows NT hosts will slow down.
Fraggle attack	UDP port 7 (Echo) and port 19 (Chargen) respond after receiving UDP packets. When port 7 receives a packet, it returns the received contents. When port 19 receives a packet, it generates a character flow. Similar to ICMP, these two UDP ports generate massive useless response messages, exhausting network bandwidth. The attacker may send a UDP packet to the network where the target host is located. The source IP address is the target host, the destination IP address is the broadcast address or network address of the subnet where the target host resides, and the destination port is port 7 or port 19. On the subnet, each system enabled with UDP 7 or 19 sends a response message to the target host. Therefore, heavy traffic is generated, congesting the target network or making the target host crash. Systems not enabled with UDP 7 or 19 return ICMP unreachable messages, which also occupy bandwidths.
ICMP-Redirect attack	A network device sends an ICMP-redirect packet to the hosts on the same subnet, requesting the hosts to change routes. Generally, network devices do not send ICMP-redirect packets to the devices except hosts. However, some malicious attackers cross a network segment and send a fraudulent ICMP-redirect packet to the hosts of another network. In this way, the attackers change the routing tables of the hosts and cause interference to normal IP packet forwarding on the hosts.
Tracert attack	Tracert attack traces the path of an ICMP timeout packet returned when the value of Time To Live (TTL) is 0 or traces a returned ICMP port-unreachable packet. In this way, the attacker obtains the network structure.
ICMP-Unreachable attack	After receiving the ICMP-unreachable packets, some systems consider the route to this destination as unreachable. The systems then disconnect the destination from the host.

Procedure

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

The page shown in [Figure 7-241](#) is displayed.

Figure 7-241 Anti-attack (1)

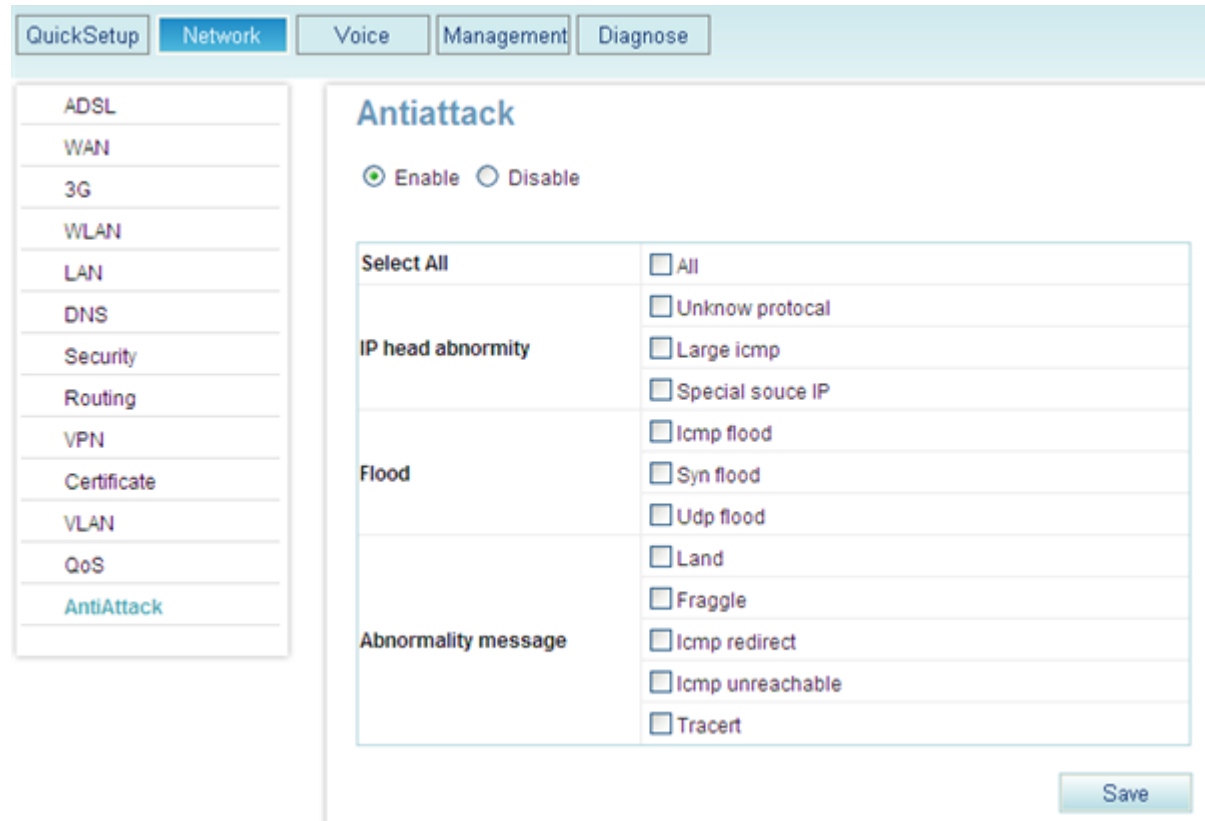


Step 2 Select **Enable** and click




The page shown in [Figure 7-242](#) is displayed.

Figure 7-242 Anti-attack (2)



Step 3 Select packet types.

Step 4 Click  to save the settings.

----End

7.6 Security

This topic describes EGW1520 security features.

7.6.1 NAT

Network Address Translation (NAT) is the process of converting a private IP address in an IP packet header to a public IP address. This function enables computers with private IP addresses to connect to a public network. NAT solves the problem of insufficient IP addresses and prevents the attack from other networks, hiding and protecting computers on the private network.

Principle

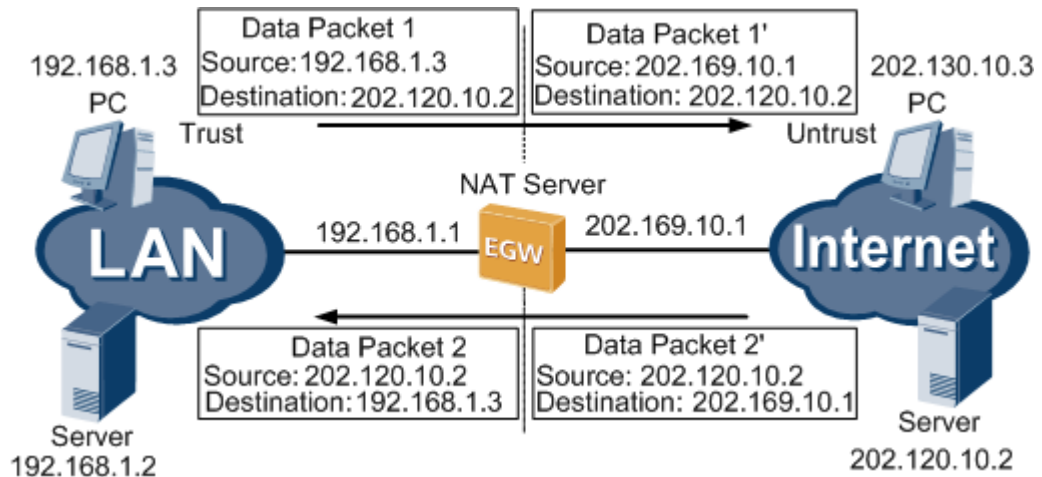
In applications, private networks use private IP addresses. Network Address Translation (RFC) 1918 reserves the following private IP address ranges:

- Class A: 10.0.0.0 to 10.255.255.255 (10.0.0.0/8)
- Class B: 172.16.0.0 to 172.31.255.255 (172.16.0.0/12)
- Class C: 192.168.0.0 to 192.168.255.255 (192.168.0.0/16)

IP addresses in the preceding ranges are not allocated on the Internet. They can be used freely inside a company or on the intranet. Enterprises do not need to apply for them to the Internet Service Provider (ISP) or the registration center.

Figure 7-243 shows a basic NAT application.

Figure 7-243 Basic NAT Application



An NAT server, for example, EGW1520, is located at the boundary between a private network and a public network. All packets sent between an internal PC and an external server will be sent to the NAT server. The address translation process is as follows:

1. After datagram 1 sent from the internal computer at 192.168.1.3 to the external server at 202.120.10.2 reaches the NAT server, the NAT server checks the content in the header 1 and finds that datagram 1 is destined for the external network.
2. The NAT server replaces the private source address 192.168.1.3 in datagram 1 with the public address 202.169.10.1 on the Internet. The NAT server sends datagram 1 to the external server and records the mapping entry in the network address translation table.
3. After receiving datagram 1, the external server sends a response packet (datagram 2) to the internal computer. The destination address of datagram 2 is 202.169.10.1.
4. After receiving datagram 2, the NAT server checks the content in the header and searches for the network address translation table. The NAT server replaces the destination IP address with 192.168.1.3 and sends datagram 2 to the internal computer.

The network translation process is transparent for the internal computer and the external server. This means that the internal computer considers that the packets exchanged with the external server are not processed by the NAT server; the external server considers that the IP address of the internal computer is 202.169.10.1, not 192.168.1.3.

Implementation

NAT implementation modes consist of static translation, dynamic translation, and Network Address Port Translation (NAPT). At present, EGW1520 uses only one public IP address and therefore uses NAPT to perform many-to-one address translation. NAPT is used to map

several private IP addresses to different port numbers of the same public IP address, as shown in Figure 7-244.

Figure 7-244 NATP implementation on EGW1520

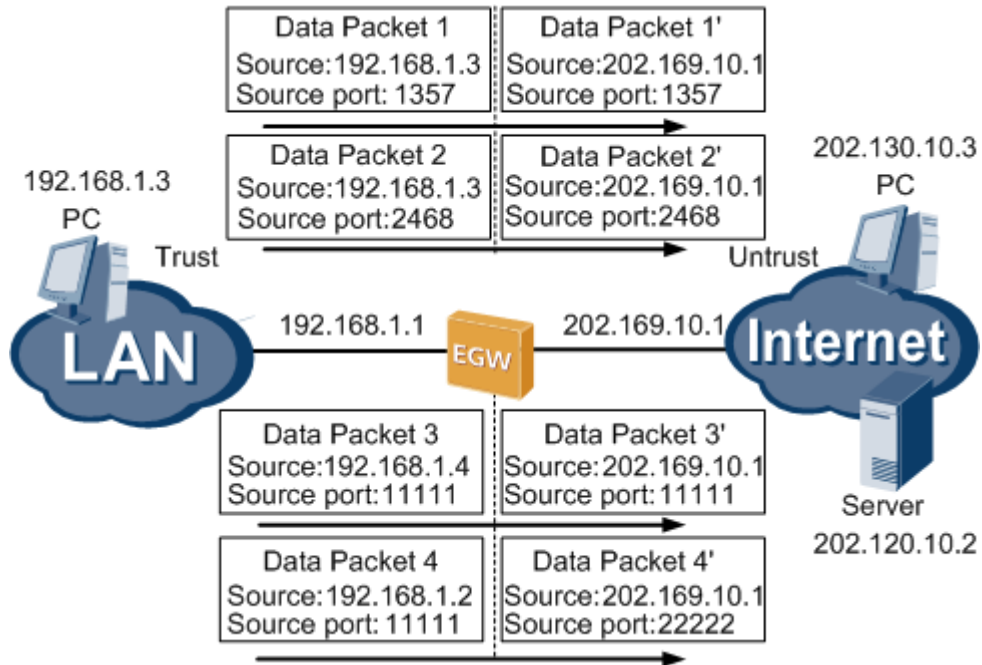


Figure 7-244In the preceding figure, datagrams 1 and 2 come from the same private IP address but have different source port numbers; datagrams 3 and 4 come from different private IP addresses but have the same source port number. When NAT is performed, the four datagrams are sent to the same public IP address, which has four different source port numbers. When response packets arrive, the NAT server checks their destination addresses and port numbers to distinguish the four datagrams. Then the NAT server translates IP addresses in the packets and then forwards them to internal computers.

By doing this, if only one public IP address is available, EGW1520 still allows several computers or other network elements (NEs) to access the same public network concurrently.

Specification

A maximum of 1024 NAT table entries.

Limitation

N/A

NOTE

For details on how to enable the NAT function, see [Configuring the ADSL](#) and [Configuring the WAN](#).

7.6.2 Incoming Packet Filter

This topic describes how to deploy an incoming packet filter on the network ingress to filter packets that are sent to the EGW1520.

Description

If the firewall is enabled on the LAN side, the firewall blocks packets that are sent to the EGW1520 or upstream device. If the firewall is enabled on the WAN side, the firewall blocks packets that are sent to the EGW1520 or downstream device. To enable specified packets to pass the firewall on the LAN side and WAN side, configure the incoming packet filter.

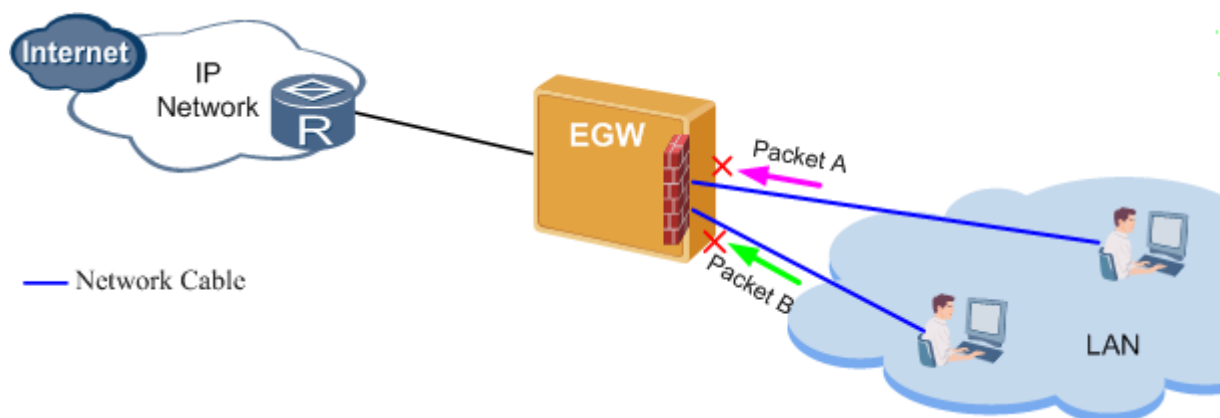
The following describes the effect after you configure the incoming packet filter when the firewall is enabled on the LAN side or WAN side.

- Enable the firewall on the LAN side.

If you do not configure the incoming packet filter function, the firewall blocks all packets that are sent to the EGW1520 and upstream device, for example packets A and B are blocked, as shown in [Figure 7-245](#).

By configuring the incoming packet filter function, you can specify packets that can be sent through the firewall on the LAN side, such as packet B in [Figure 7-246](#).

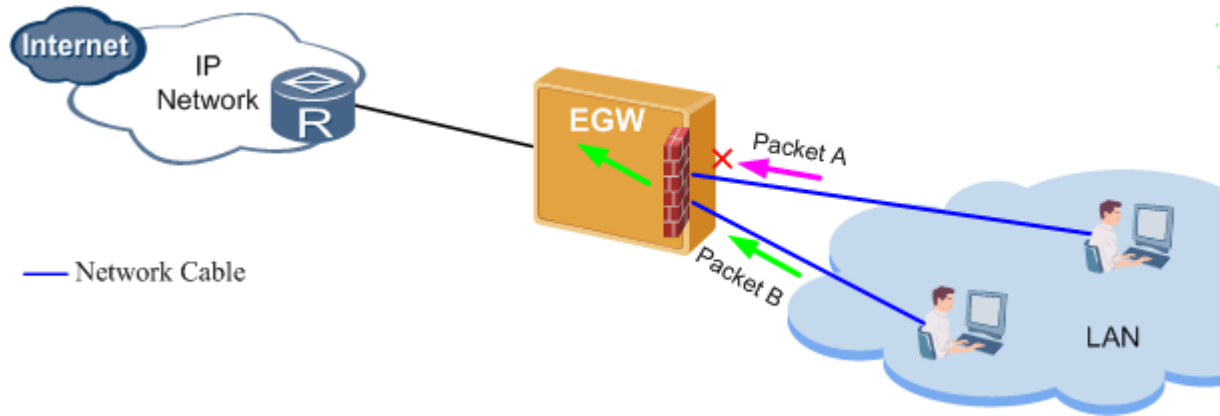
Figure 7-245 Incoming packet filter function not enabled



NOTE

The firewall on the LAN side can block only packets sent to an upstream device or an EGW1520. It cannot block packets within the LAN.

Figure 7-246 Incoming packet filter function enabled



- Enable the firewall on the WAN side.

If you do not configure the incoming packet filter function, the firewall blocks all packets that are sent to the EGW1520 and downstream device, for example packets A and B are blocked, as shown in [Figure 7-247](#).

By configuring the incoming packet filter function, you can specify packets that can be sent through the firewall on the WAN side, such as packet B in [Figure 7-248](#).

Figure 7-247 Incoming packet filter function not enabled

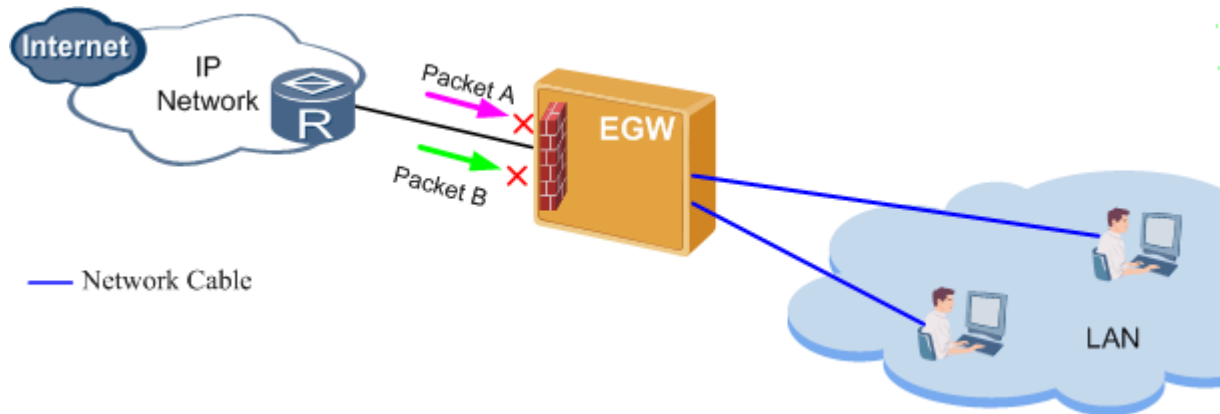
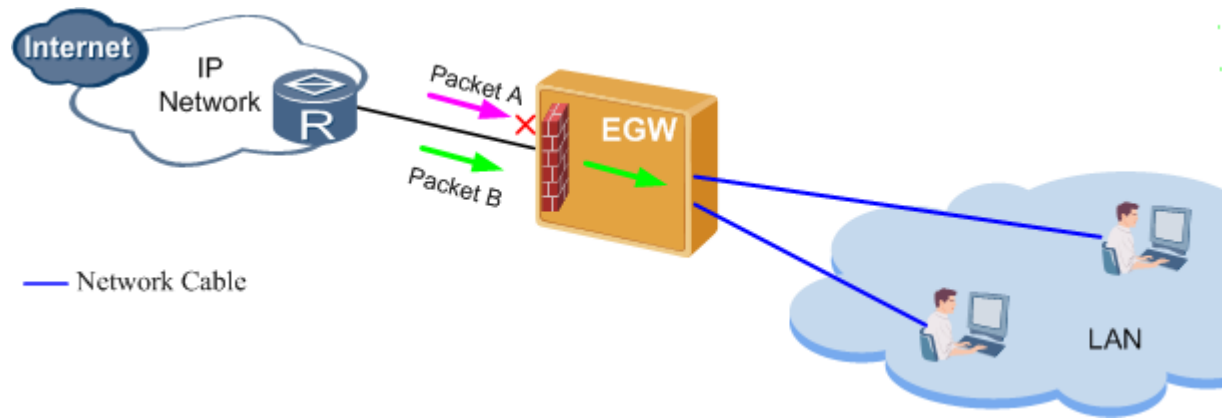


Figure 7-248 Incoming packet filter function enabled



Configuration

Prerequisites

- You have enabled the firewall on the LAN side (see [Configuring the LAN](#) for details) or on the WAN side (see [Configuring the ADSL](#) or [Configuring the WAN](#) for details).
- 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.

The page shown in [Figure 7-249](#) is displayed.

Figure 7-249 Configuring the incoming packet filter (1)



Step 2 Click  to add a filter. The filter is used to identify packets that need to be filtered out.

The page shown in [Figure 7-250](#) is displayed.


Figure 7-250 Configuring the incoming packet filter (2)

Step 3 Set parameters according to [Table 7-65](#).

Table 7-65 Parameter description

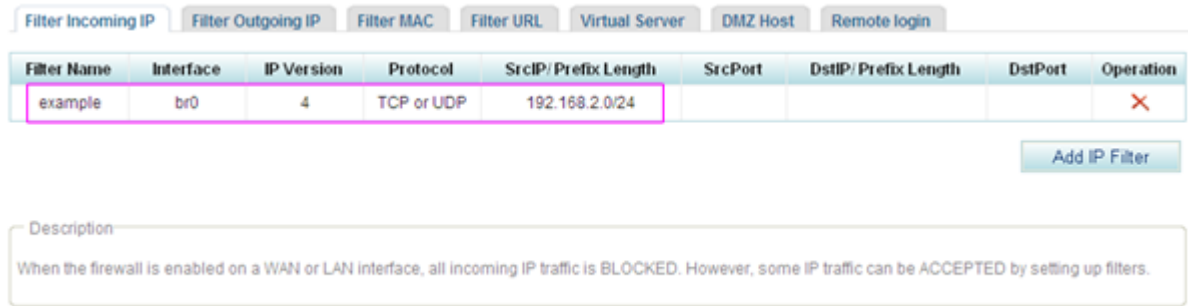
Parameter	Description
Filter Name	Indicates the filter name, which can be changed.
Protocol	Indicates the protocol type based on which packets are filtered. The options are as follows: <ul style="list-style-type: none"> • TCP/UDP: TCP/UDP packets can be sent to the upstream network from the EGW1520. • TCP: TCP packets can be sent to the upstream network from the EGW1520. • UDP: UDP packets can be sent to the upstream network from the EGW1520. • ICMP: ICMP packets can be sent to the upstream network from the EGW1520, such as messages indicating whether the network is connected, whether the route to the host is reachable, and whether the route is available.
Source IP Address/Segment	Indicates the source IP address (for example, 192.168.1.2), or source IP address/subnet mask length (for example, 192.168.1.0/24). Value 192.168.1.2 indicates that packets whose source IP addresses are 192.168.1.2 can be sent to the upstream network from the EGW1520. Value 192.168.1.0/24 indicates that packets whose source IP addresses are on the 192.168.1.0 network segment can be sent to the upstream network from the EGW1520. If this parameter is left blank, all packets can be sent to the upstream network from the EGW1520.
Source Port(port or port:port)	Indicates the source port number (for example, 80), or source port number range (for example, 80:90).

Parameter	Description
	<p>Value 80 indicates that packets whose source port numbers are 80 can be sent to the upstream network from the EGW1520. Value 80:90 indicates that packets whose source port numbers range from 80 to 90 can be sent to the upstream network from the EGW1520.</p> <p>If this parameter is left blank, all packets can be sent to the upstream network from the EGW1520.</p>
Destination IP Address/Segment	<p>Indicates the destination IP address (for example, 192.168.1.1), or destination IP address/subnet mask length (for example, 192.168.1.0/24).</p> <p>Value 192.168.1.1 indicates that packets whose destination IP addresses are 192.168.1.1 can be sent to the upstream network from the EGW1520. Value 192.168.1.0/24 indicates that packets whose destination IP addresses are on the 192.168.1.0 network segment can be sent to the upstream network from the EGW1520.</p> <p>If this parameter is left blank, all packets can be sent to the upstream network from the EGW1520.</p>
Destination Port(port or port:port)	<p>Indicates the destination port number (for example, 90), or destination port number range (for example, 90:100).</p> <p>Value 90 indicates that packets whose destination port numbers are 90 can be sent to the upstream network from the EGW1520. Value 90:100 indicates that packets whose destination port numbers range from 90 to 100 can be sent to the upstream network from the EGW1520.</p> <p>If this parameter is left blank, all packets can be sent to the upstream network from the EGW1520.</p>
Interface to Apply This Rule	<p>Indicates the interface where the filter takes effect. For example,</p> <ul style="list-style-type: none"> br0/br0: ports on the LAN side (LAN ports 1–4 and Wi-Fi port). When you select br0/br0, the filter filters the packets that are sent to the EGW1520 and upstream device through the LAN port. pppoe_0_0_35/ppp1: ADSL port. When you select pppoe_0_0_35/ppp1, the filter filters the packets that are sent to the EGW1520 and upstream device through the ADSL port.

Step 4 Click  to save the settings.

[Figure 7-251](#) shows the configuration result.

Figure 7-251 Configuring the incoming packet filter (3)



----End

7.6.3 Outgoing Packet Filter

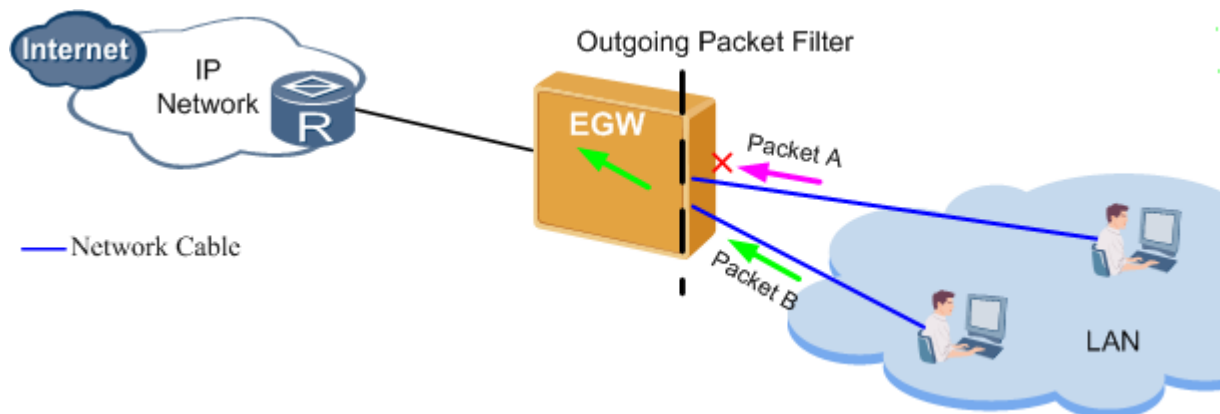
This topic describes how to deploy an outgoing packet filter on the network egress to filter packets that are sent to the upstream device through the LAN port.

Description

The outgoing packet filter allows you to disable specified packets from being sent to an upstream device through the LAN port when the firewall on the LAN side disabled. If you enable the firewall on the LAN side, the firewall will block all packets sent to an upstream device through the LAN port.

Packet A in [Figure 7-252](#) can be prevented from being sent to an upstream device through the LAN port when the firewall on the LAN side disabled.

Figure 7-252 Filtering outgoing packets



Configuration

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 **Network > Security** from the navigation tree.

Step 2 Click the **Filter Outgoing IP** tab.

The page shown in [Figure 7-253](#) is displayed.

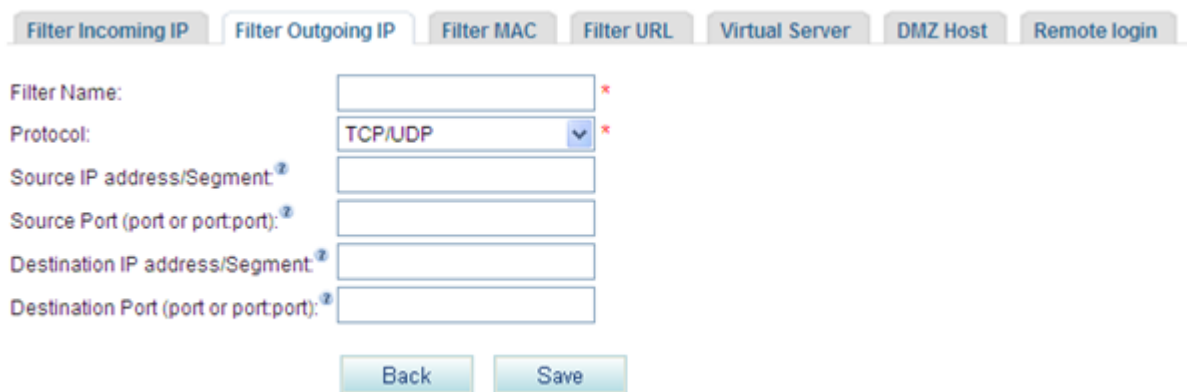
Figure 7-253 Configuring the outgoing packet filter (1)



Step 3 Click  to add a filter. The filter is used to identify packets that need to be filtered out.

The page shown in [Figure 7-254](#) is displayed.

Figure 7-254 Configuring the outgoing packet filter (2)



Step 4 Set parameters according to [Table 7-66](#).

Table 7-66 Parameter description

Parameter	Description
Filter Name	Indicates the filter name, which can be changed.

Parameter	Description
Protocol	<p>Indicates the protocol type based on which packets are filtered. The options are as follows:</p> <ul style="list-style-type: none"> • TCP/UDP: TCP/UDP packets cannot be sent to the upstream network through the LAN port. • TCP: TCP packets cannot be sent to the upstream network through the LAN port. • UDP: UDP packets cannot be sent to the upstream network through the LAN port. • ICMP: ICMP packets cannot be sent to the upstream network through the LAN port, such as messages indicating whether the network is connected, whether the route to the host is reachable, and whether the route is available.
Source IP Address/Segment	<p>Indicates the source IP address (for example, 192.168.1.2), or source IP address/subnet mask length (for example, 192.168.1.0/24).</p> <p>Value 192.168.1.2 indicates that packets whose source IP addresses are 192.168.1.2 cannot be sent to the upstream network through the LAN port. Value 192.168.1.0/24 indicates that packets whose source IP addresses are on the 192.168.1.0 network segment cannot be sent to the upstream network through the LAN port.</p>
Source Port(port or port:port)	<p>Indicates the source port number (for example, 80), or source port number range (for example, 80:90).</p> <p>Value 80 indicates that packets whose source port numbers are 80 cannot be sent to the upstream network through the LAN port. Value 80:90 indicates that packets whose source port numbers range from 80 to 90 cannot be sent to the upstream network through the LAN port.</p>
Destination IP Address/Segment	<p>Indicates the destination IP address (for example, 192.168.1.1), or destination IP address/subnet mask length (for example, 192.168.1.0/24).</p> <p>Value 192.168.1.1 indicates that packets whose destination IP addresses are 192.168.1.1 cannot be sent to the upstream network through the LAN port. Value 192.168.1.0/24 indicates that packets whose source IP addresses are on the 192.168.1.0 network segment cannot be sent to the upstream network through the LAN port.</p>
Destination Port(port or port:port)	<p>Indicates the destination port number (for example, 90), or destination port number range (for example, 90:100).</p> <p>Value 90 indicates that packets whose destination port numbers are 90 cannot be sent to the upstream network through the LAN port. Value 90:100 indicates that packets whose destination port numbers range from 90 to 100 cannot be sent to the upstream network through the LAN port.</p>


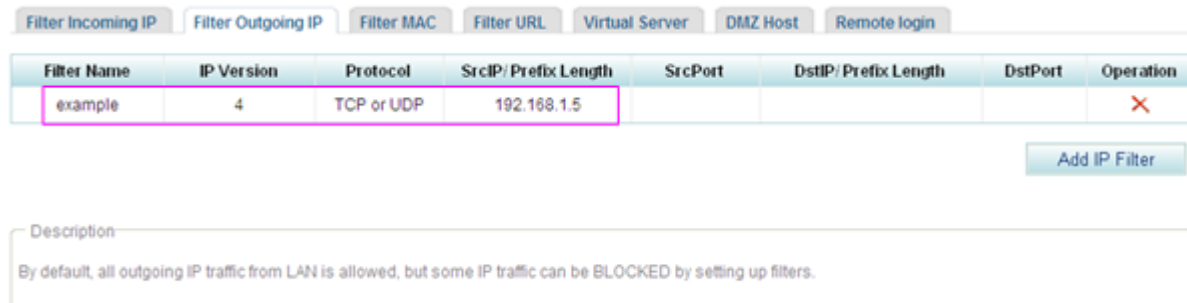
Step 5 Click  to save the settings.

Figure 7-255 shows the configuration result.

Figure 7-255 Configuring the outgoing packet filter (3)



----End

7.6.4 MAC Address Filter

If the ADSL service is in **Bridge** mode, you can configure MAC address filter to prevent the ADSL port from forwarding certain data frames.

Description

To configure the MAC address filter, configure both the MAC address filtering policy and filtering rule. The MAC address filtering policy specifies the mode of filtering data frames, and the MAC address filtering rule specifies the data frames to be filtered.

EGW1520 supports the following MAC address filtering policies:

- **FORWARD**: The ADSL port forwards all data frames except those specified in the filtering rule.
- **BLOCKED**: The ADSL port forwards only the data frames specified in the filtering rule.

The default filtering policy is **FORWARD**.

Configuring MAC Address Filter

Prerequisites

- The ADSL service is in **Bridge** mode. For details, see [Basic Configuration](#).
- You have logged in to the web management system. For details, see [7.7.1 Web Management](#).

Procedure

Step 1 Modify the MAC address filtering policy.

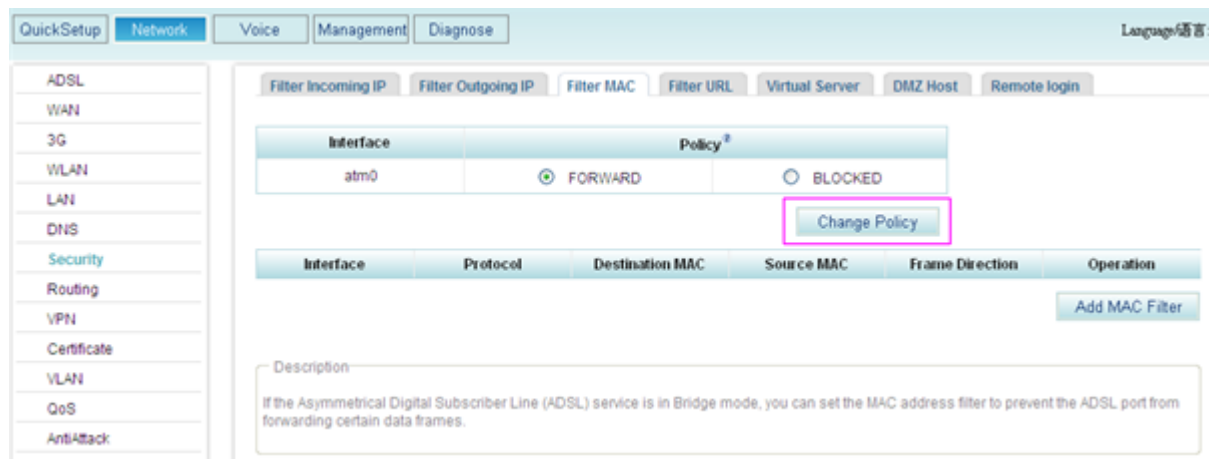
 **CAUTION**

When the MAC address filtering policy for a port is modified, the MAC address filtering rule for this port is automatically deleted. You must re-create the MAC address filtering rule.

1. On the web management system, choose **Network > Security** from the navigation tree.
2. Click the **Filter MAC** tab.

The page shown in [Figure 7-256](#) is displayed.

Figure 7-256 Filter MAC tab page (1)

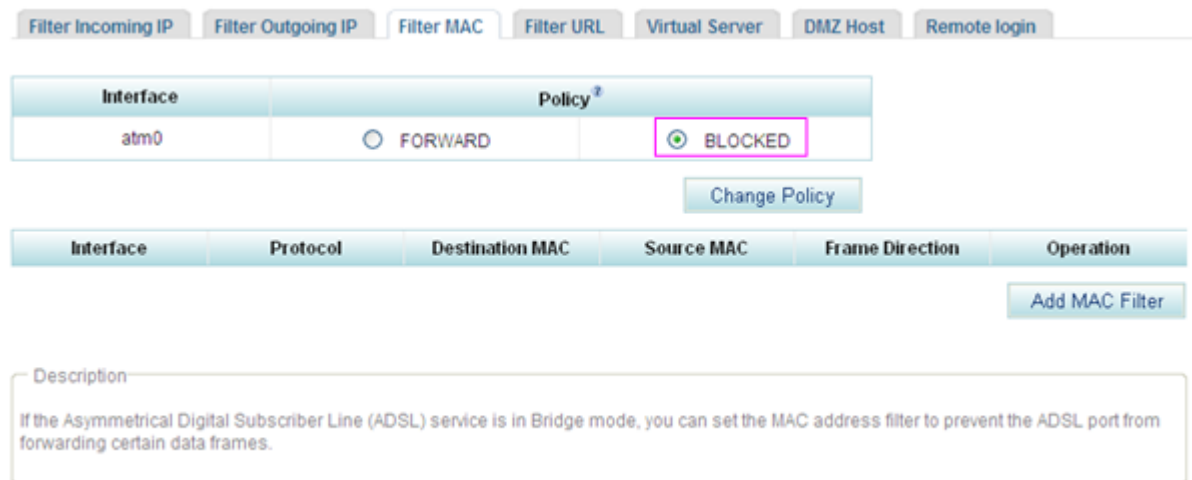


3. Select an MAC address filtering policy, for example, **BLOCKED**.

4. Click  to save the new policy.

[Figure 7-257](#) shows the configuration result.

Figure 7-257 Configuration result

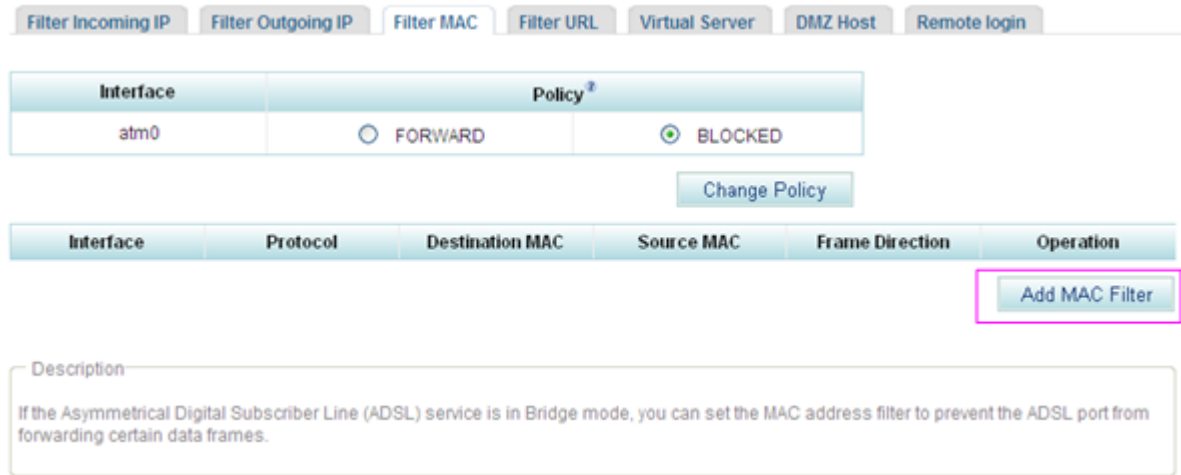



Step 2 Create the MAC address filtering rule.

1. On the web management system, choose **Network > Security** from the navigation tree.
2. Click the **Filter MAC** tab.

The page shown in [Figure 7-258](#) is displayed.

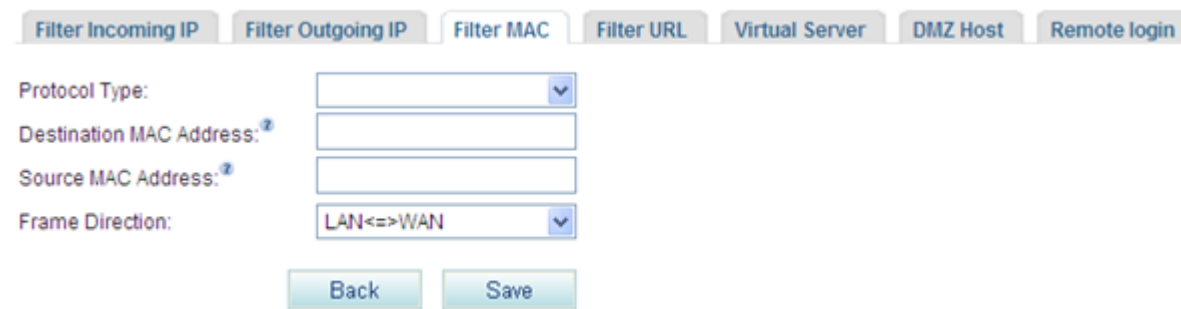
Figure 7-258 Filter MAC tab page (2)



3. Click  to add a filter.

The page shown in [Figure 7-259](#) is displayed.

Figure 7-259 Filter MAC tab page (3)



4. Set parameters according to [Table 7-67](#).

Table 7-67 Parameter description

Parameter	Description
Protocol Type	Indicates the protocol type based on which MAC addresses are filtered. The options are as follows: <ul style="list-style-type: none"> • PPPoE: Point-to-Point Protocol over Ethernet, which is used by remote devices to manage and charge users.