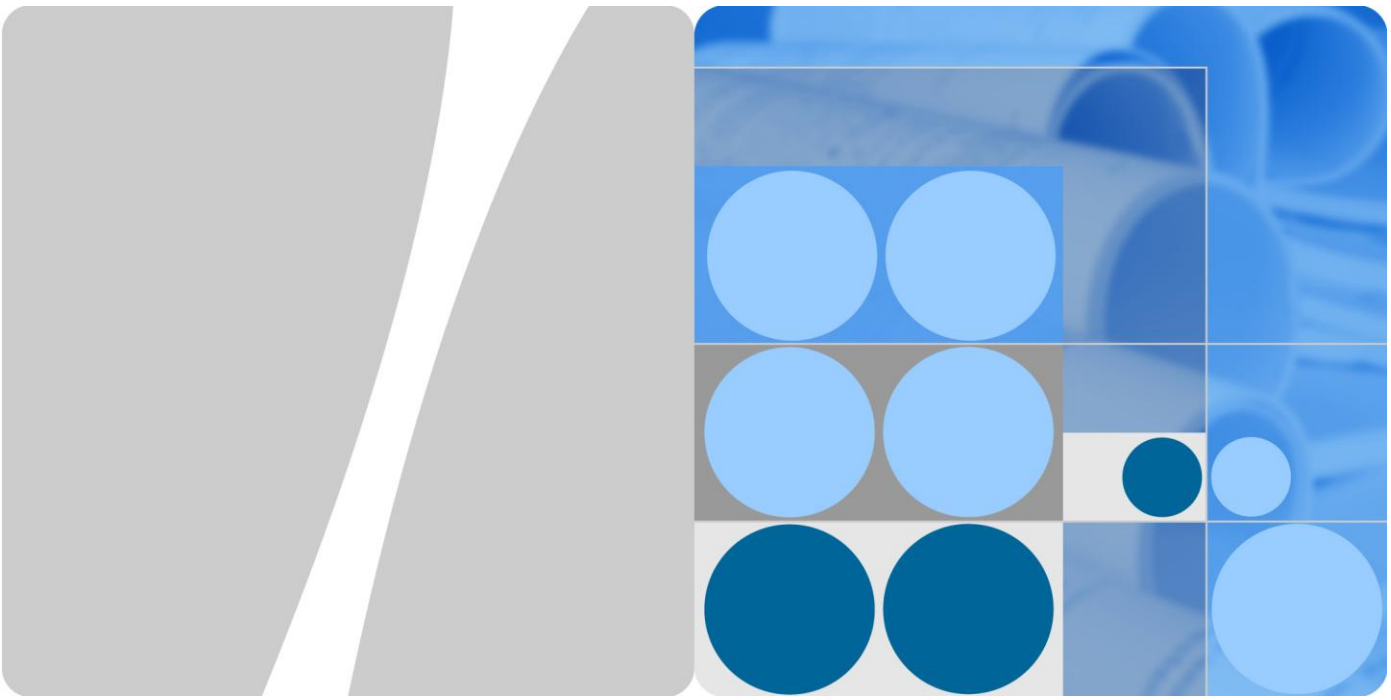


Huawei IP Phone eSpace 7810&7820&7830&7850&7870&7803X V100R001C02SPC100 Administrator Guide

Issue 01

Date 2012-06-20

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

 and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

Contents

1 Overview

1.1 Principle

Huawei IP phones use the digitalized transmission technology in packets based on the IP technology. The basic principles are as follows:

- Compress and encode voice data according to the voice compression algorithm.
- Package the voice data based on a certain protocol such as the IP protocol.
- Send data packets to the recipient through the IP network.
- Decode and decompress voice packets after collecting the voice packets to restore the voice packets to the original voice signals.

Voice data is transmitted through the IP network. The IP phone system converts the analog signals of a common phone into IP packets that can be transmitted through the Internet, and also converts the received IP packets to analog electric signals.

1.2 Function Description

In terms of the orientation, eSpace 7870, and 7850 are high-end-oriented products, eSpace 7830 and 7820 are a middle-end-oriented product, and eSpace 7810 is a low-end-oriented product. eSpace 7870, 7850, 7830, 7820and 7810 are a series of products.

In terms of the functions, eSpace 7870, 7850, 7830 and 7820 use the advanced digital signal processing (DSP) technology with the help of the automatic gain and comfort noise generation (CNG) technologies. Therefore, eSpace 7870 and 7830 provide voice of high quality, which is as good as the voice provided by the traditional public switched telephone network (PSTN).

Codec Function

eSpace 7870, 7850, 7830, 7820 and 7810 support GG.711 A-law/μ-law, G.722, G.723.1, G.726, G.729AB and iLBC codec mode, and configuration of voice codec priority. In general, retain the default configuration of voice codec priority for deployment. If the network environment is complex, you can adjust the codec priority according to the actual network bandwidth.

NOTE

If the network is in a good condition, G.711 is recommended, and the voice quality will be excellent. If the network is not in a good condition, G.729AB or G.723.1 is recommended.

PoE Function

eSpace 7870, 7850, 7830, 7820 and 7810 support the PoE function. When not being connected to a power adapter, a client can obtain power from a PSE device (a PoE switch such as the S3900) to work normally. eSpace 7870, 7850, 7830, 7820 and 7810 support the mode of free-line power supply and mode of signal-line power supply. When the PoE function is used, the reliable power supply distance is up to 100 meters.

Bridging Function

eSpace 7870, 7850, 7830, 7820 and 7810 support the bridging function. The device connected to the PC port of an IP phone can access the network connected to the LAN interface of the IP phone and can communicate with other devices in the network. In this case, the IP phone acts as a switch with two interfaces but the working mode is different from the working mode of a normal switch. Special configurations are performed at the lower layers of an IP phone to separate the broadcast packets between the two interfaces. Therefore, the IP phone is not affected by a large number of broadcast packets.

DSP Functions

The DSP chip of eSpace 7870, 7850, 7830, 7820 and 7810 supports comfort noise generation (CNG) and voice activity detection (VAD). These functions are controlled by the DSP automatically, which can be set on web pages. You can enable this function by selecting **Enabled** in **Voice** on the **Phone** page of the web configuration interface.

VLAN Function

eSpace 7870, 7850, 7830, 7820 and 7810 support the Virtual Local Area Network (VLAN) function. The packets sent by an IP phone are labeled with tags. This makes packets transmitted in a separate voice VLAN, and the stability of VoIP packets is ensured.

QoS Functions

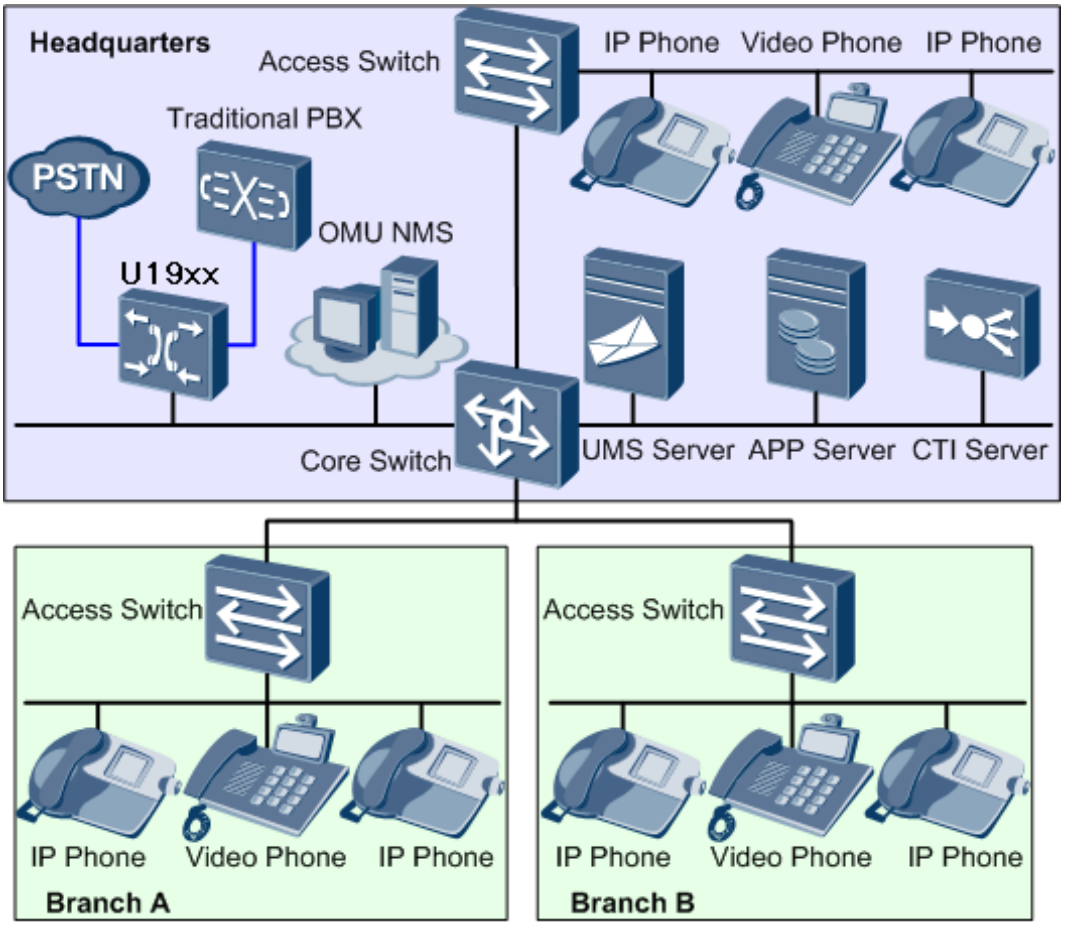
eSpace 7870, 7850, 7830, 7820 and 7810 support the layer 2 quality of service (QoS) technology based on 802.1q and 802.1p and the layer 3 QoS technology based on ToS. The deployment of QoS on the VoIP bearer network ensures the voice quality during the transmission.

PPPoE Function

eSpace 7870, 7850, 7830, 7820 and 7810 support the PPP over Ethernet (PPPoE) dialing function. By using the preset PPPoE user name and password, an IP phone can initiate the PPPoE dialing and set up a connection with the softswitch through ADSL. This facilitates the setup of VoIP conversations.

1.3 Network Introduction

In terms of network features, eSpace 7800 series IP phones can be deployed on enterprise networks to interoperate with application servers such as the IP PBX and UMS servers, implementing functions such as the basic call services, additional services, unified messaging, and phone book display. This improves the enterprise communication efficiency.



In the deployment of IP phones on the network with IPPBX, the original data networks of enterprises are used as the network that bears VOIP to deploy IP phones in distributed mode. With the help of the application servers, the functions such as the enterprise phone book function and voice message leaving function can be implemented.

2 Single IP Phone Configuration

Configure and upgrade IP phones one by one if any of the following conditions is met:

- There are only a few IP phones onsite.
- The centralized upgrade environment is unavailable onsite.
- Users require special services.

This chapter describes how to configure a single IP phone.

NOTE
The methods for configuring eSpace 7870, 7850, 7830, 7820 and 7810 are similar. The configuration for eSpace 7850 is the most complex. This document describes how to configure eSpace 7850. Only eSpace 7870, 7830, 7820 and 7810 configurations that are different from eSpace 7850 configurations are described.

2.1 Quick Phone Configuration

eSpace 7850 obtains an IP address by using Dynamic Host Configuration Protocol (DHCP) if there is a DHCP server onsite. By default, eSpace 7800 series obtain IP addresses through DHCP. When eSpace 7850 successfully obtains an IP address, press **OK** to view the IP address.

If there is no DHCP server onsite, you need to use the keypad to set network parameters for eSpace 7850.

The procedures for using the keypad to set the IP address, to configure the Session Initiation Protocol (SIP) server, and to set the SIP account are complex. Therefore, you are advised to set the IP address by using the keypad, and then access the web page to set other parameters.

2.1.1 Using the Keypad to Set Network Parameters

To use the keypad to set a static IP address, proceed as follows:

1. Press **Menu** on the IP phone to access the main menu.

   NOTE
   For eSpace 7810, press **MENU** to access the main menu.

2. Press **3**.

   The **Setting Type** page is displayed.

NOTE
For eSpace 7870, press **6** to access the **Setting Type** page.

3. Press **2**.
   The **Please enter Password** page is displayed.
4. Enter the password (the initial password is **admin**).
5. Press **Confirm**.
   The **Advanced Settings** page is displayed.
6. Press **2**.
   The **Network** page is displayed.
7. Press **1**.
   The **WAN Port Option** page is displayed.
8. Press **2**.
   The **Static IP Client** page is displayed.
9. Press the up arrow key or down arrow key to select **IP**, press **Del** to delete the default IP address, and enter the required IP address.

NOTE
For eSpace 7810, press **X** to delete the default IP address.

10. Set **Subnet Mask**, **Default Gateway**, **Pri DNS**, and **Sec. DNS**, and click **Save**.
    The **WAN Port Option** page is displayed.

NOTE
For eSpace 7810, press **OK** to save settings.

11. Press **Back** to return to the **Network** page.

NOTE
For eSpace 7810, press **MENU** to return to the **Network** page.

12. Press **Back**.
    The following messages are displayed:

```
Network updating
Please wait…
```

    The settings take effect after the IP phone is restarted.

NOTE
For eSpace 7810 and 7820, the following messages are displayed:

```
Network updating
Please wait…
```

Then the following messages are displayed:

```
Initializing
Please wait…
```

2.1.2 Configuring an IP Phone on Web Pages

Open the Internet Explorer, enter the IP address of an IP phone in the address box, and set parameters for the IP phone on the web configuration page that is displayed.

The web configuration page consists of the following tabs:

- **Status**: Set the network status, firmware version, MAC address, and other information on this tab page.
- **Account**: Set IP phone's SIP account parameters on this tab page. eSpace 7870 and 7850 supports a maximum of six accounts, eSpace 7830 and 7820 supports a maximum of three accounts, and eSpace 7810 supports a maximum of two accounts.
- **Network**: Set basic network parameters (such as the WAN port and LAN port) and advanced network parameters (such as LLDP, VLAN) on this tab page.
- **Phone**: Set the language, time, call forwarding, do-not-disturb (DND), hold, transfer, and other functions, and set the DSS keys, voice, ring tone, signal tone, and dialing rules. For eSpace 7850 and 7830, the soft key layout, keys on an expansion module, and short messages can also be configured on this tab page.
- **DSS** Key: Set DSS keys on this tab page. This tab page is available only to eSpace 7870. The DSS keys of other IP phones are configured on the **Phone** tab page.
- **Contacts**: Set the local phone book, blacklist, number dialing on web pages, remote phone book, and LDAP. The remote phone book and Lightweight Directory Access Protocol (LDAP) address book are supported only by eSpace 7870, 7850, 7830 and 7820.
- **Upgrade**: Set TR069 parameters for manual upgrade and automatic upgrade.
- **Security**: Change the password of an administrator or a common user, and upload the trust certificates to the TLS/SSL client and server.

Accessing the Web Configuration Page

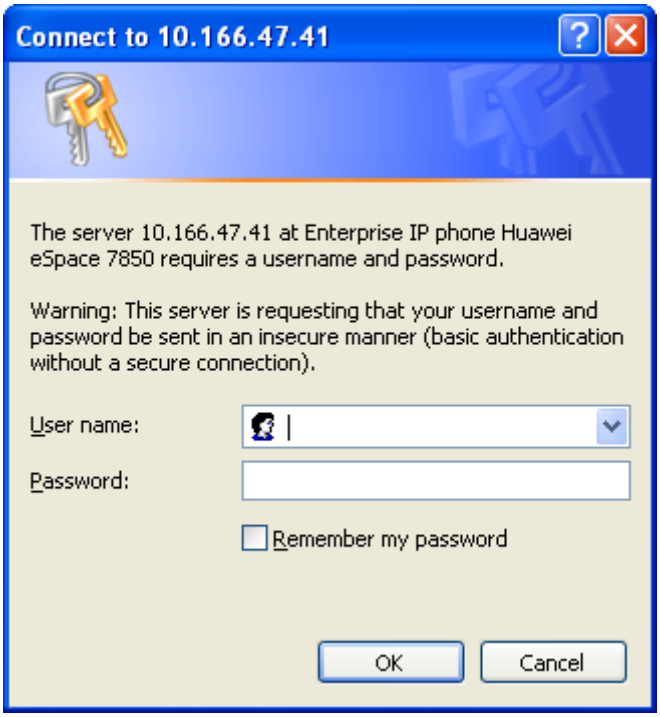
Before accessing the web configuration page, connect the IP phone and computer to the same hub or switch. If there is no hub or switch, connect the computer to the PC port of the IP phone.

To access the web configuration page, proceed as follows:

1. Start the web browser.
2. To view the IP address of the IP phone, press the **OK** key when the phone is connected to the network.
3. Enter an IP phone's IP address in the address box, and press **Enter**.

   The IP address is in the format xxx.xxx.xxx.xxx, in which xxx ranges from 0 to 255. For example, 10.10.10.1.
4. Enter **admin** in the **User name** text box, and enter the administrator password (default: **admin**) in the **Password** text box. Then click **OK**, as shown in Figure 2-1.

Figure 2-1 Login dialog box



Viewing the IP Phone Status

After logging in to the IP phone's web page, click the Status tab and view the IP phone status, as shown in Figure 2-2.

Figure 2-2 Status tab page

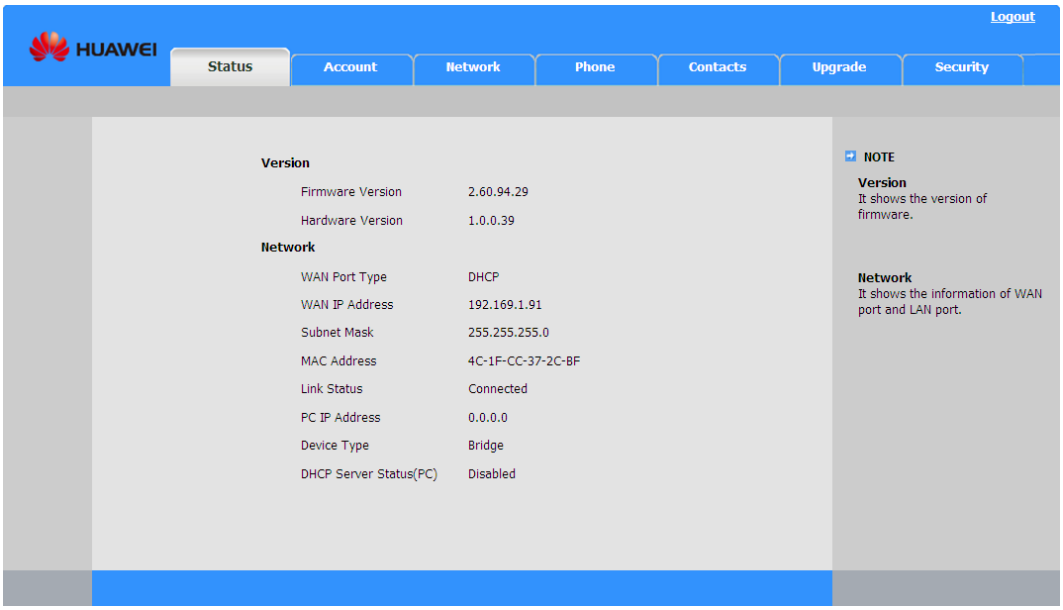


Table 2-1 lists the parameters on the **Status** tab page.

Table 2-1 Parameters on the Status tab page

Parameter	Description
Firmware Version	Firmware version number, which is used to check the upgrade result.
Hardware Version	Hardware version number, which is used to identify hardware.
WAN Port Type	Method of obtaining eSpace 7850 IP address.
WAN IP Address	IP address of an IP phone.
Subnet Mask	Subnet mask of an IP phone.
MAC Address	MAC address of an IP phone, which is a hexadecimal number. MAC addresses are important for configuring IP phones in batches.
Link Status	Connection status of the WAN port.
PC IP Address	IP address of the PC port.
Device Type	Connection type of the PC port.
DHCP Server Status(PC)	Status of the DHCP server connecting to the LAN port.

Setting Basic Parameters for a SIP Account

eSpace 7870, 7850, 7830, 7820 and 7810 provide six lines, six lines, three lines, three lines and two lines respectively. Each line can be configured with a SIP account.

The following procedure configures a SIP account.

1. Click the **Account** tab. On the **Account** tab page, select **Account 1** from the **Account** drop-down list box, and set SIP parameters, as shown in Figure 2-3.

   Figure 2-4shows the **Codecs** area for setting the voice coding types for SIP accounts.

2. In the **Basic** area, select **On** for **Account Active**, and set **User Name** and **Register Name**. Set the SIP server IP address and port number for **SIP Server**.

   NOTE

   The **Label** and **Display Name** parameters are optional. Unless otherwise specified, retain the default value for optional parameters.

   If authentication information is configured on the SIP server, enter the authentication password in the **Password** text box.

   If the outbound proxy server is required, select **Enabled** from the **Enable Outbound Proxy Server** drop-down list box, and enter the server IP address and port number provided by the carrier in the **Outbound Proxy Server** and the corresponding **Port** text box.

3. Set voice coding types in the **Codecs** area.
4. Click **Confirm**.

   Settings are saved, and the IP phone starts to register the account.

   After the web page is refreshed, you can check the registration status of the account in the **Register Status** area.

After the preceding operations are performed, the IP phone can make or answer calls. For details about parameters, see Parameters for setting a SIP account, Parameters in the Codecs area, and Parameters in the Advanced area.

2.2 Account Configuration

2.2.1 Setting Basic Parameters

Set basic parameters in the **Basic** area on the **Account** tab page, as shown in Figure 2-3.

Figure 2-3 Setting basic parameters

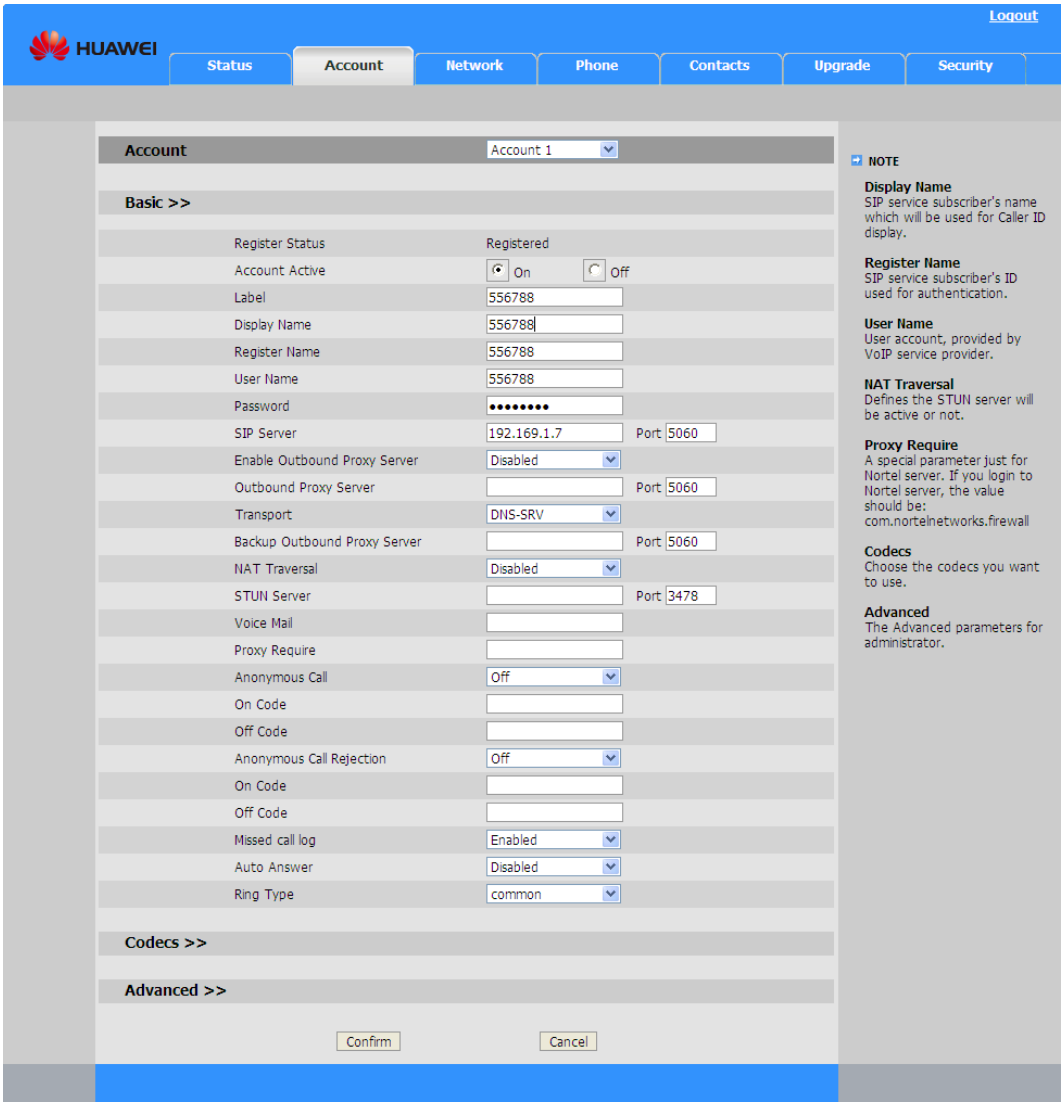


Table 2-2 lists the parameters in the **Basic** area on the **Account** tab page.

Table 2-2 Parameters for setting a SIP account

Parameter	Description
Register Status	Status of the selected account. Options are **Registered**, **Unregistered**, **Registering**, and **Register failed**.
Account Active	Indicates whether to activate the account.

Parameter	Description
	Default value: **Off**
Label	Label displayed on the LCD when the IP phone is in the standby state, for example, **Line1**.
Display Name	Account name displayed on the called party's phone LCD when the IP phone functions as a calling party. This function requires the SIP server.
Register Name	Authentication ID.
User Name	User name provided by the VoIP service provider. The value is similar to a phone number or is an actual phone number.
Password	Password corresponding to **Register Name**. The value is provided by the service provider.
SIP Server	SIP server's IP address or domain name, which is provided by the VoIP service provider.
Port	Port number of the SIP server. Default value: **5060**
Enable Outbound Proxy Server	Indicates whether to enable the outbound proxy server. It is used for the firewall or NAT penetration in different network environments. If the system detects that the symmetric NAT and STUN cannot work, only the outbound proxy server can provide solution for symmetric NAT.
Outbound Proxy Server	IP address or domain name of outbound proxy server, media gateway, or session border controller.
Port	Port number of the outbound proxy server. Default value: **5060**
Transport	The options are **UDP**, **TCP**, **TLS**, and **DNS-SRV**. The values **UDP**, **TCP**, and **TLS** are SIP transmission methods, in which **TLS** indicates encrypted transmission. The value **DNS-SRV** indicates that an IP phone determines the transfer type (UDP, TCP, or TLS) based on the information in the DNS SRV record sent by the server.
Backup Outbound Proxy Server	Standby proxy server, which starts to work when the outbound proxy server fails.
Port	Port number of the standby outbound proxy server. Default value: **5060**
NAT Traversal	Indicates whether to enable NAT traversal. If this parameter is set to **STUN**, eSpace 7850 decides whether to enable NAT traversal based on the STUN client configurations. In this mode, the STUN client built-in eSpace 7810 communicates with a specified STUN server to check firewalls or NAT and their types. If the NAT is the Full Cone, Restricted Cone, or Port-Restricted Cone mode, eSpace 7810 attempts to use the public IP address and port number to send all SIP and Service Data Point (SDP) information.

Parameter	Description
STUN Server	IP address or domain name of the STUN server.
Port	Port number of the STUN server. Default value: **3478**
Voice Mail	Voice mailbox access code. After setting this parameter, you can press the **Message** indicator to connect to the voice mailbox server.
Proxy Require	Parameter for the Nortel platform. If IP phones register with the Nortel platform, this parameter is mandatory. The parameter value is fixed at **com.nortelnetworks.firewall**. If the parameter value is incorrect, contact Nortel for help.
Missed call log	Indicates whether to record missed calls. If you select **Disabled**, an IP phone does not record missed calls.
Auto Answer	Indicates whether to enable the auto answer function. If the function is enabled, calls to the account are answered automatically.
Ring Type	Ring tone for the account.

2.2.2 Setting Codec Parameters

Set codec parameters in the **Codecs** area on the **Account** tab page, as shown in Figure 2-4.

Figure 2-4 Setting codec parameters

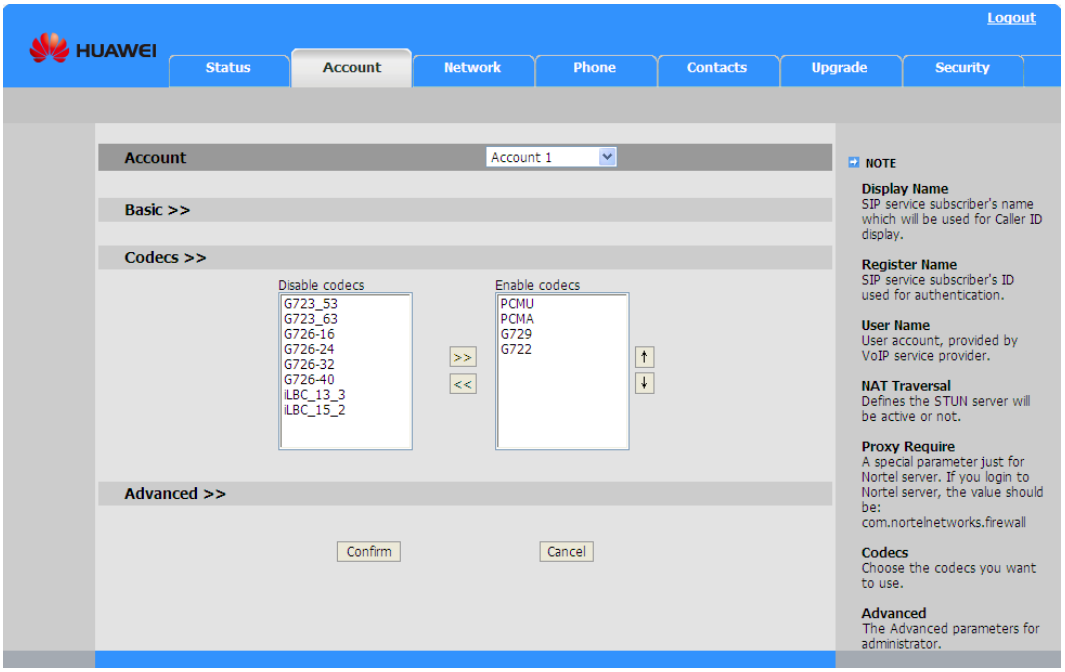


Table 2-3 lists the parameters in the **Codecs** area on the **Account** tab page.

Table 2-3 Parameters in the Codecs area

Parameter	Description
Disable codecs	Disabled voice coding types.
Enable codecs	Enabled voice coding types. The types are listed in descending order of priority.

2.2.3 Setting Advanced Parameters

Set advanced parameters in the **Advanced** area on the **Account** tab page, as shown in Figure 2-5.

Figure 2-5 Setting advanced parameters

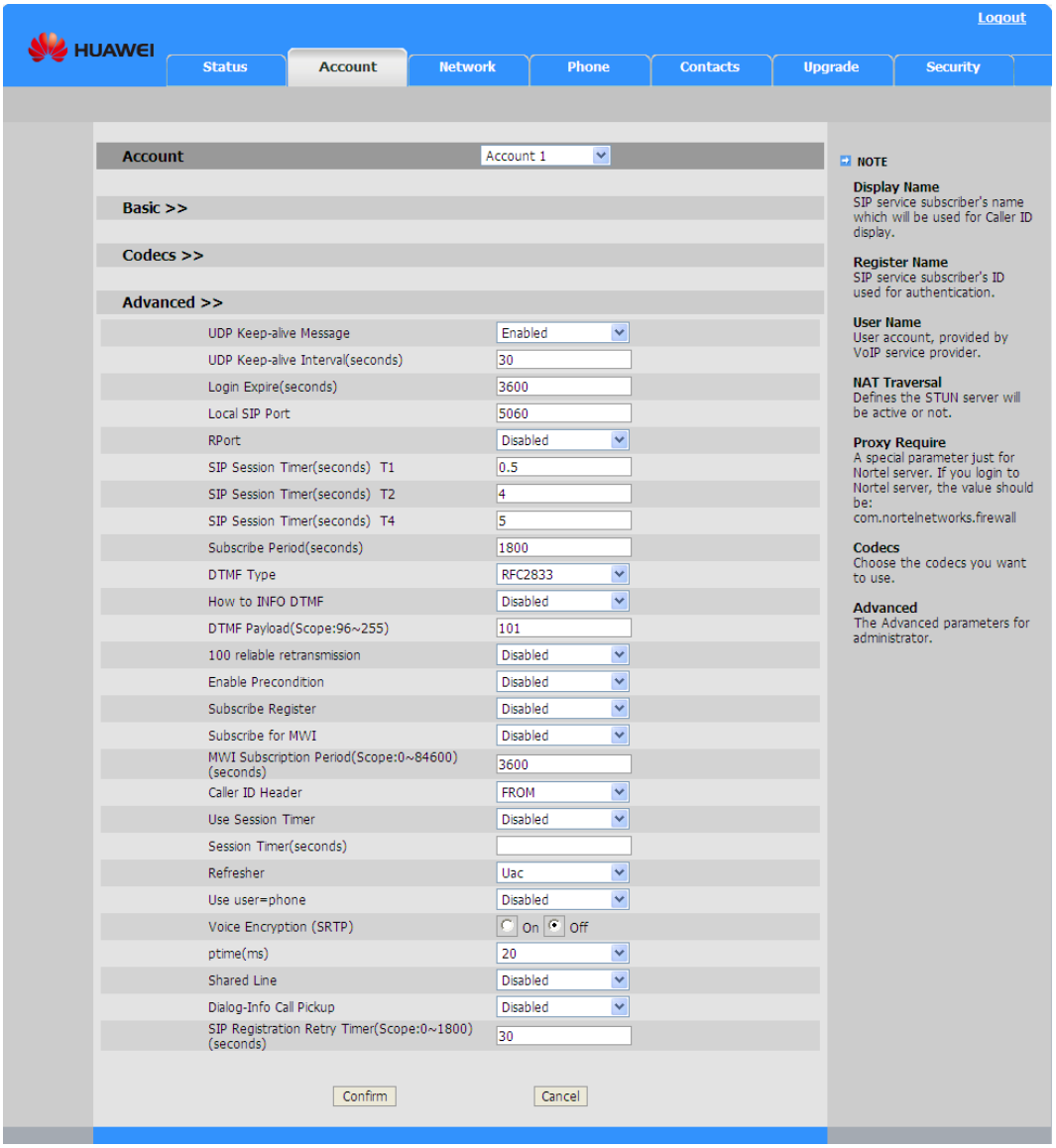


Table 2-4 lists the parameters in the **Advanced** area on the **Account** tab page.

Table 2-4 Parameters in the Advanced area

Parameter	Description
UDP Keep-alive Message	Indicates whether to send a UDP message at an interval to keep a port always available.
UDP Keep-alive Interval(seconds)	Interval for sending UDP messages. For example, 30 seconds.
Login Expire(seconds)	If a user does not perform any operations within the period specified by this parameter, logs the user out. Unit: second Default value: 3600
Local SIP Port	Port for the SIP server to communicate with IP Phone. Default value: 5060
RPort	Port through which the server sends a response to IP Phone. Details about this parameter are specified in RFC 3581.
SIP Session Timer(seconds) T1	Round trip time (RTT) between the server and the client. If the network latency is long, set it to a larger value. Details about RTT are specified in RFC 3261. Default value: 0.5
SIP Session Timer(seconds) T2	Interval between the INVITE response receiving and the non-INVITE request sending, in seconds. Details about this parameter are specified in RFC 3261. Default value: 4
SIP Session Timer(seconds) T4	Duration for sending information between the client and the server. Details about this parameter are specified in RFC 3261. Default value: 5
Subscribe Period(seconds)	Validity period for busy lamp field (BLF) subscription. Default value: 1800
DTMF Type	DTMF signal transmission type. The options are as follows: • **INBAND**: DTMF signals are sent as voice signals. • **RFC2833**: DTMF signals are transmitted based on Real-time Transport Protocol (RTP). The header in an RTP packet indicates transmission of DTMF signals and defines the DTMF signals. • **SIP INFO**: DTMF signals are transmitted in SIP INFO messages. The main defect is that DTMF

Parameter	Description
	signals may not be transmitted at the same time with media packets because SIP control signaling and media packets are sent separately. • **AUTO+SIP INFO**: The DTMF signal transmission type is determined by negotiation. The type can be **INBAND** or **RFC2833**. Default value: RFC2833
How to INFO DTMF	Method for using SIP INFO to transmit DTMF signals.
DTMF Payload (Scope: 96~255)	Payload for using RFC 2833 to transmit DTMF signals. Value range: 96 to 255 Default value: 101
100 reliable retransmission	Indicates whether to enable the PRACK function to make the temporary SIP response (1xx signaling) more reliable. The PRACK function must be enabled for the PSTN network.
Enable Precondition	The value **Enabled** indicates that resources are reserved. Details about this parameter are specified in RFC 3262.
Subscribe Register	Indicates whether to enable the subscription function for registration. This parameter is used to monitor account registration when the IP Multimedia Subsystem (IMS) system is involved.
Subscribe for MWI	Indicates whether to subscribe to the MWI service. The value **Enabled** indicates that the IP phone periodically sends subscription information to the server to update the MWI status.
MWI Subscription Period(Scope: 0~84600)(seconds)	Validity period for the MWI service. Default value: 3600
Caller ID Header	The options are **FROM** and **PAI. FROM**: The calling number displayed on the called phone is obtained from the **FROM** header. **PAI**: The calling number displayed on the called phone is obtained from the **PAI** header.
Use Session Timer	Indicates whether to update sessions as scheduled. The IP phone periodically sends a re-INVITE request to hold a session. The server uses the update request to monitor the session status. Details about this parameter are specified in RFC 4028.
Session Timer(seconds)	Interval for updating sessions.
Refresher	Party who updates sessions. The value **Uac** indicates that the client updates sessions, and the value **Uas**

Parameter	Description
	indicates that the server updates sessions.
Use user=phone	The value **Enabled** indicates that the **user=phone** flag is added to the **SIP URIS** header, identifying non-phone devices, for example, a gateway.
Voice Encryption(SRTP)	Secure RTP packet transfer.
ptime(ms)	Interval for transferring RTP packets.
Shared Line	Indicates whether to enable the shared line function.
Dialog-Info Call Pickup	Indicates whether to enable the Dialog-Info Call Pickup function. If this function is enabled, a DSS key can be assigned the call pickup function without a function code.
SIP Registration Retry Timer(Scope:0~1800)(seconds)	Interval between IP phone registration attempts.

2.3 Network Configuration

2.3.1 Configuring Network Ports

Set network port parameters in the **Internet Port(WAN)** area on the **Network** tab page, as shown in Figure 2-6.

To configure the network port for eSpace 7870, click the **Network** tab and click **Basic**.

Figure 2-6 Setting network port parameters

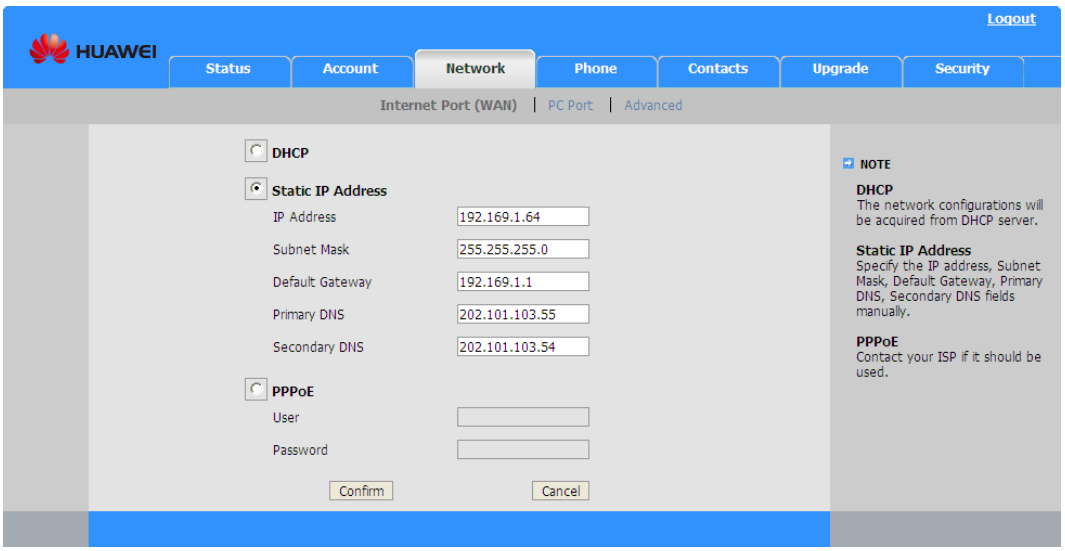


Table 2-5 lists the network port parameters.

Table 2-5 Network port parameters

Parameter	Description
DHCP	If this option is selected, eSpace 7850 automatically connects to the DHCP server for obtaining resources such as the IP address, subnet mask, gateway, and DNS server information.
Static IP Address	If this option is selected, you must set network parameters including **IP Address**, **Subnet Mask**, **Default Gateway**, **Primary DNS**, and **Secondary DNS**. For details about these parameters, contact the network administrator.
PPPoE	If an xDSL modem is used, PPPoE can be used to connect an IP phone to the network. If this option is selected, you must set **User** and **Password**. For details about these parameters, contact the network service provider.

2.3.2 Configuring PC Ports

When the network port on a PC connects to the PC port on an IP phone, the phone functions as a network bridge or a router.

Set PC port parameters in the **PC Port** area on the **Network** tab page, as shown in Figure 2-7.

To configure the PC port for eSpace 7870, click the **Network** tab and click **Basic**.

Figure 2-7 Setting PC port parameters

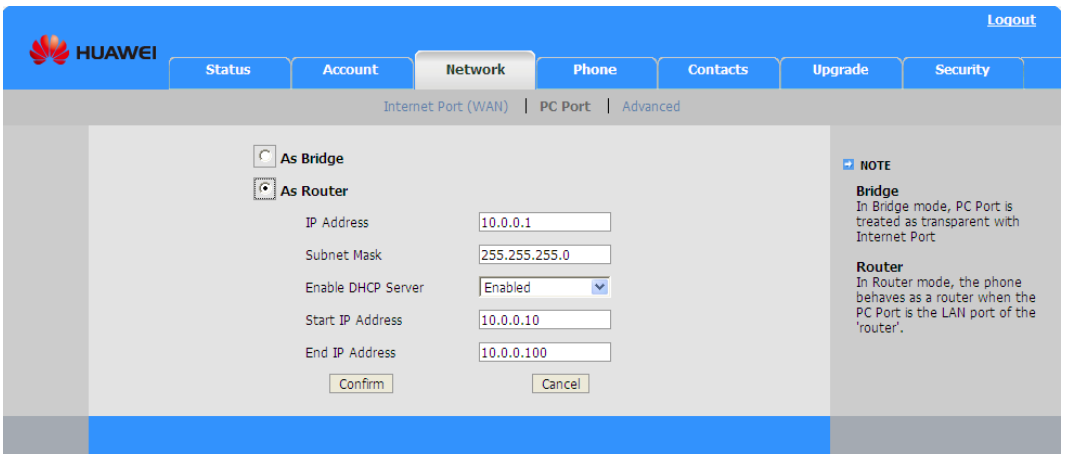


Table 2-6 lists the PC port parameters.

Table 2-6 PC port parameters

Parameter	Description
As Bridge	If you select **As Bridge**, the PC port functions as a bridge.
As Router	If you select **As Router**, eSpace 7850 functions as a router.

Parameter	Description
-IP Address	IP address of an IP phone when it functions as a router.
-Subnet Mask	Subnet mask for the IP address of an IP phone when it functions as a router.
-Enable DHCP Server	Indicates whether to enable the DHCP function for eSpace 7850.
-Start IP Address	Start IP address assigned to the device connected to the PC port when the DHCP function is enabled for eSpace 7850.
-End IP Address	End IP address assigned to the device connected to the PC port when the DHCP function is enabled for eSpace 7850.

2.3.3 Enabling the VLAN Function

Function Description

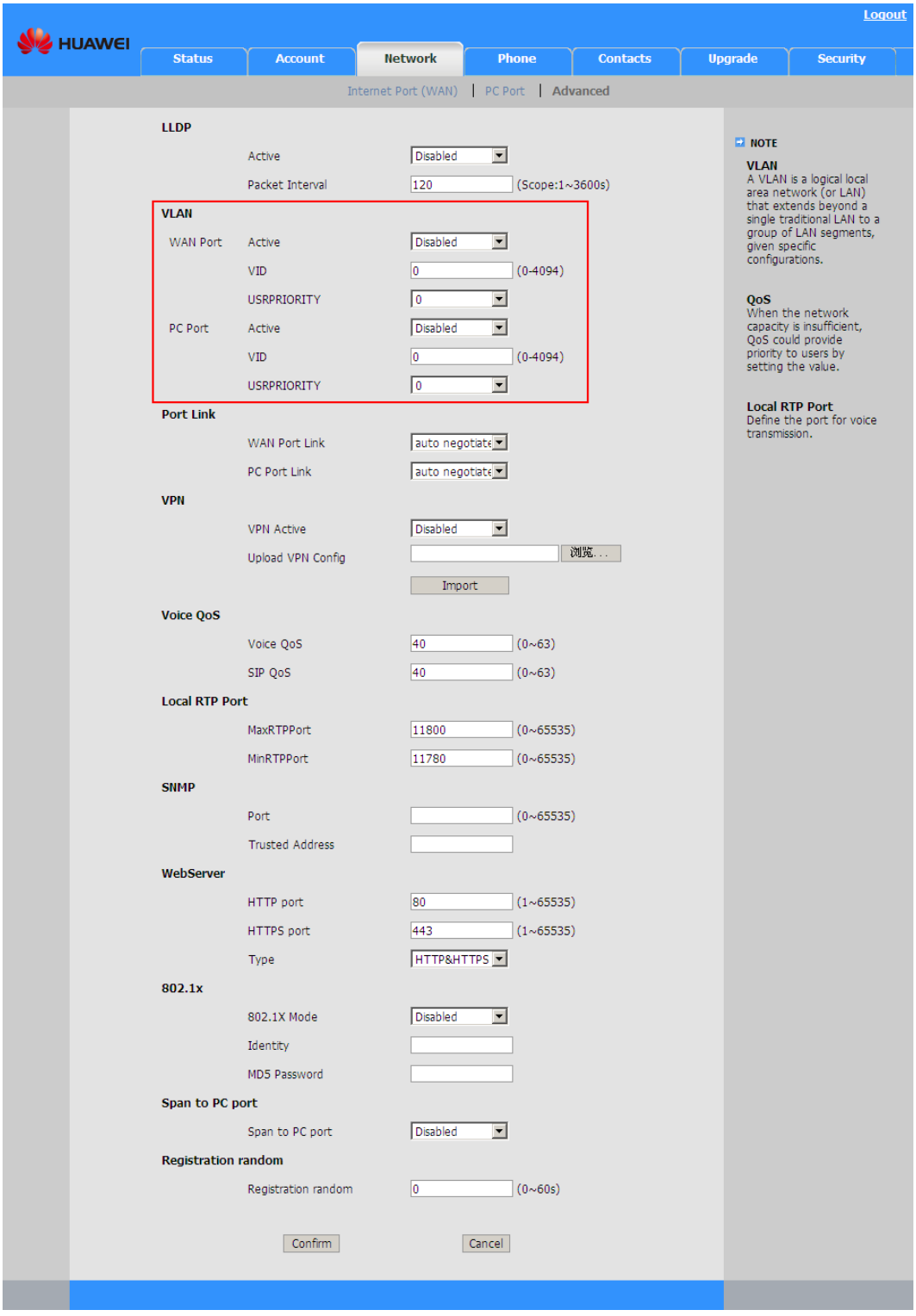
A VLAN is a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of their physical location. VLANs are mainly configured on switches and routes. Broadcast traffic and unicast traffic on a VLAN cannot be forwarded to other VLANs, which controls traffic, simplifies network management, and reduces broadcasts.

If the VLAN function is enabled on an IP phone, the IP phone can communicate only with computers on the same VLAN.

Phone Configuration

Set VLAN parameters in the **Advanced** area on the **Network** tab page, as shown in Figure 2-8.

Figure 2-8 Setting VLAN parameters



The VLAN function can be enabled for both the network port and PC port. Table 2-7 lists the VLAN parameters.

Table 2-7 VLAN parameters

Parameter	Description
WAN Port	Set VLAN parameters on the network port.
-Active	The value **Enabled** indicates that the VLAN function is enabled for the network port.
-VID	ID of the VLAN where the IP phone belongs to. The network administrator divides the network where the switch resides into multiple VLANs. Each VLAN has a unique ID.
-USPRIORITY	VLAN priority for the network port. The value ranges from **0** to **7**.
PC Port	Set VLAN parameters on the PC port.
-Active	The value **Enabled** indicates that the VLAN function is enabled for the PC port.
-VID	ID of the VLAN where the IP phone belongs to. The network administrator divides the network where the switch resides into multiple VLANs. Each VLAN has a unique ID.
-USPRIORITY	VLAN priority for the PC port. The value ranges from 0 to 7.

Configuration File

Table 2-8 eSpace 7850, 7830, 7820 and 7810 parameters in the VLAN configuration file

Section Header and Path	Parameters	Value Range	Description
[VLAN] path = /config/Network/Network.cfg	ISVLAN	0 or 1	Indicates whether to enable the VLAN function on the network port. • **0**: no • **1**: yes Default value: 0
	VID	0 to 4094	VLAN ID for the network port. Default value: 0
	USRPRIORITY	0 to 7	VLAN priority for the network port. Default value: 0
	PC_PORT_VLAN_ENAB	0 or 1	Indicates whether to enable the VLAN function on the

Section Header and Path	Parameters	Value Range	Description
	LE		PC port. • **0**: no • **1**: yes Default value: 0
	PC_PORT_VID	0 to 4094	VLAN ID on the PC port. Default value: 0
	PC_PORT_PRIORITY	0 to 7	VLAN priority for the PC port. Default value: 0

Table 2-9 eSpace 7870 parameters in the VLAN configuration file

Section Header and Path	Parameters	Value Range	Description
[cfg:/phone/config/system.ini,reboot=1]	VLAN.ISVLAN	0 or 1	Indicates whether to enable the VLAN function on the network port. • **0**: no • **1**: yes Default value: 0
	VLAN.VID	0 to 4094	VLAN ID for the network port. Default value: 0
	VLAN.USRPRIORITY	0 to 7	VLAN priority for the network port. Default value: 0
	VLAN.PC_PORT_VLAN_ENABLE = 1	0 or 1	Indicates whether to enable the VLAN function on the PC port. • **0**: no • **1**: yes Default value: 0
	VLAN.PC_PORT_VID	0 to 4094	VLAN ID on the PC port. Default value: 0
	VLAN.PC_PORT	0 to 7	VLAN priority for the

Section Header and Path	Parameters	Value Range	Description
	_PRIORITY		PC port. Default value: 0

2.3.4 Enabling the LLDP Function

Function Description

Link Layer Discovery Protocol (LLDP) organizes local device information into type-length-value (TLV) and encapsulates the information into Link Layer Discovery Protocol Data Unit (LLDPDU). LLDP sends LLDPDU to directly-connected neighbors and saves LLDPDU from neighbors in Management Information Base (MIB). LLDP enables a device to store and manage information about the device itself and directly-connected neighbors for the network management system to check the link communication status.

LLDP is used on the VoIP terminals in the following scenarios:

- LLDP packet receiving

  After an administrator configures LLDP broadcast information such as VLAN ID and QoS on a switch that supports LLDP, an IP phone automatically updates network information such as VLAN ID and QoS based on the received LLDP information after being powered on.

  Every time an IP phone moves on a network or a new VLAN is assigned to the switch port, the IP phone automatically checks its home VLAN and modifies local VLAN settings.
- LLDP packet sending

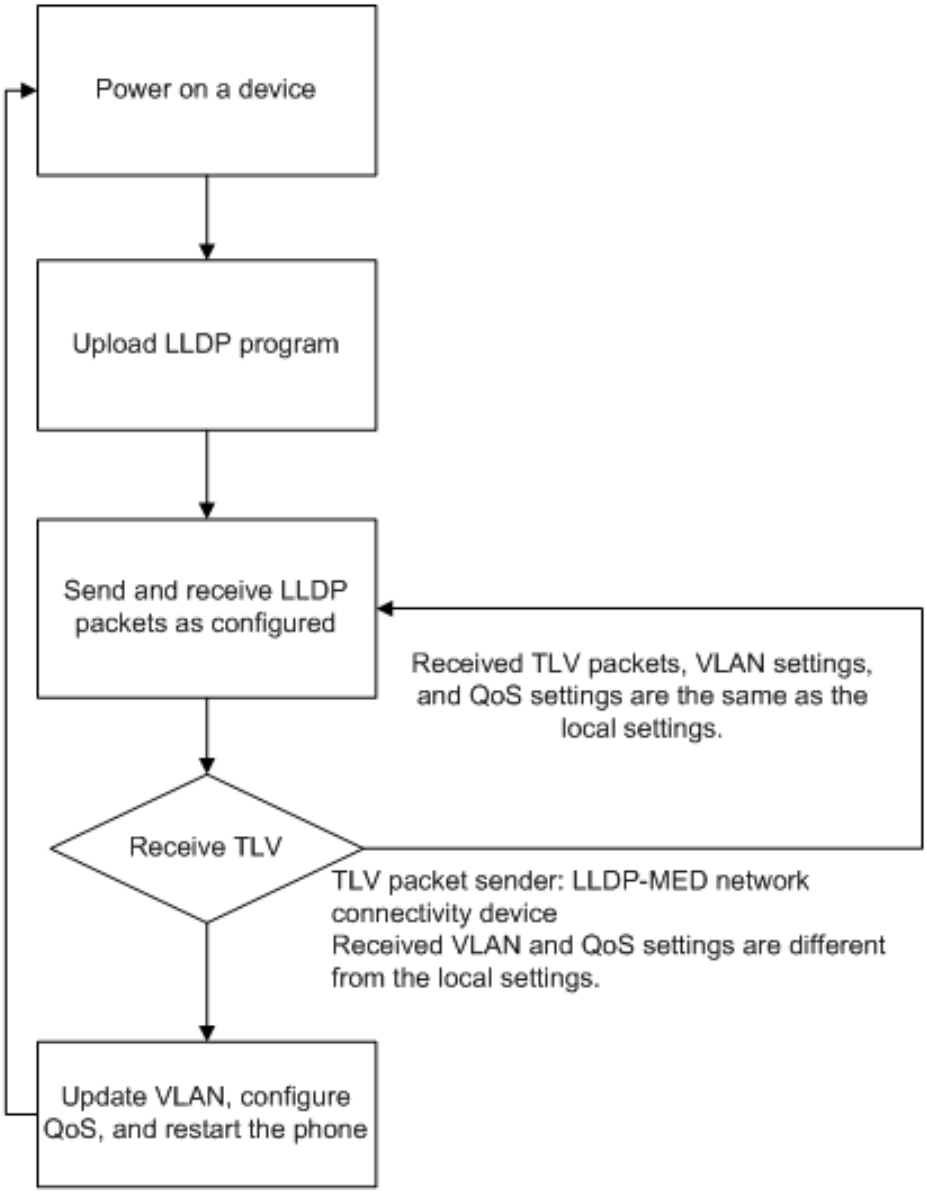
  Emergency call: LLDP information contains address information. When an emergency occurs, the position is quickly located based on the address information.

  System maintenance: LLDP provides accurate network mapping, traffic data, and other information for administrators to locate network faults.

Function Implementation

Figure 2-9 shows the flowchart for implementing LLDP.

Figure 2-9 Flowchart for implementing LLDP



After power-on, an IP phone updates the VLAN and QoS information by:

- Sending an LLDP packet

  If the LLDP function is enabled for an IP phone, the IP phone sends the switch an LLDP packet that contains local network information in multicast mode at an interval.

- Receiving an LLDP packet

  When an IP phone receives an LLDP packet from a server on the network and finds that the local VLAN ID is different from the VLAN ID in the packet or that the local VLAN is disabled, the IP phone updates the local VLAN information based on that in the packet. If the IP phone finds that the QoS in the packet is different from the local setting, the IP phone updates the local QoS setting.

Phone Configuration

Set LLDP parameters in the **Advanced** area on the **Network** tab page, as shown in Figure 2-10.

Figure 2-10 Setting LLDP parameters

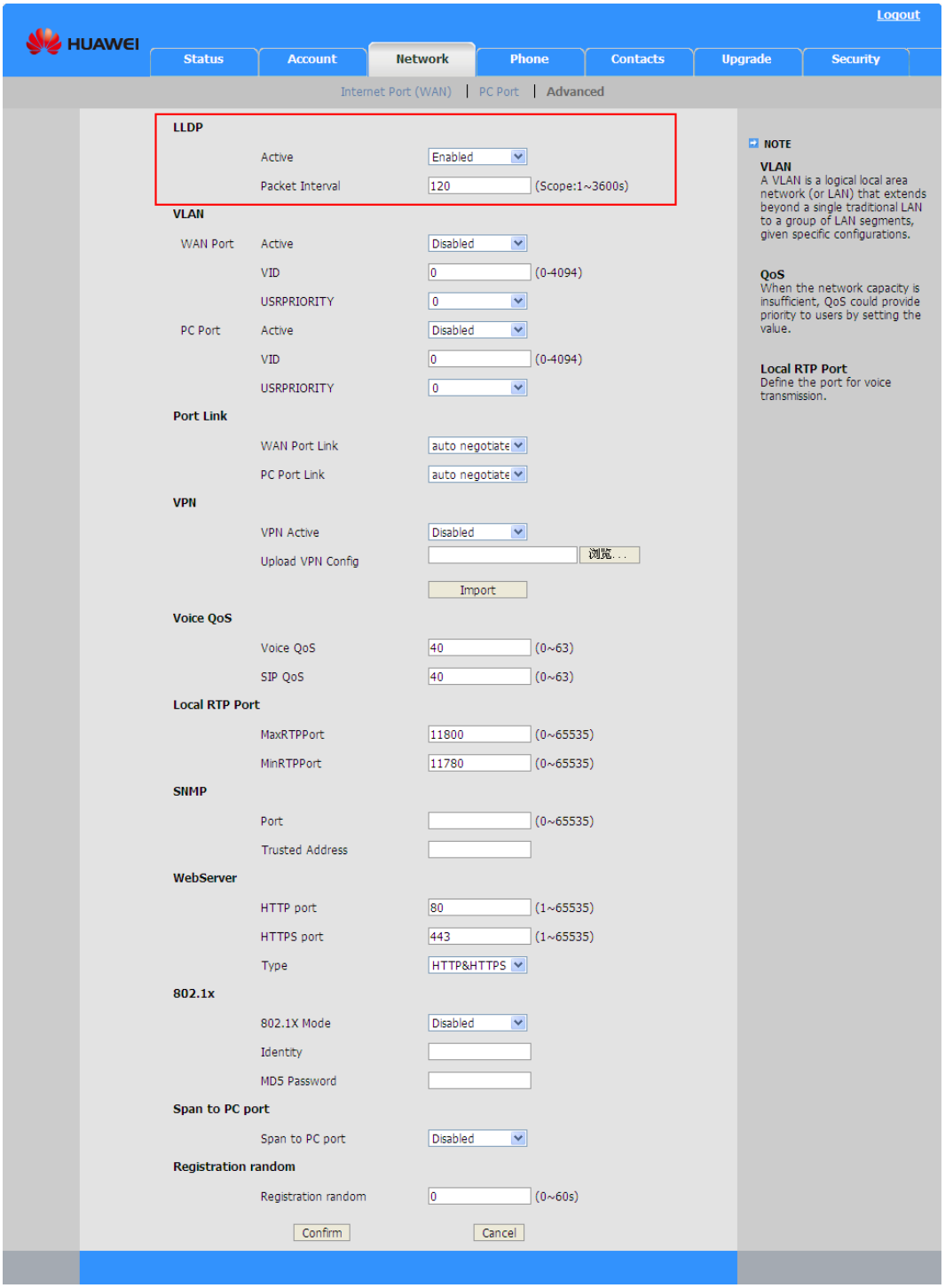


Table 2-10 lists the LLDP parameters.

Table 2-10 Description of LLDP parameters

Parameter	Description
Active	Indicates whether to enable the LLDP function.
Packet Interval(Scope:1 ~3600s)	Interval for sending an LLDP packet. Default value: 120

Configuration File

Table 2-11 eSpace 7850, 7830, 7820 and 7810 parameters in the LLDP configuration file

Section Header and Path	Parameters	Value Range	Description
[LLDP] path = /config/Network/Network.cfg	EnableLLDP	0 or 1	Indicates whether to enable the LLDP function. • **0**: no • **1**: yes Default value: 0
	PacketInterval	1 to 3600	Interval for sending LLDP packets, in seconds. Default value: 120

Table 2-12 eSpace 7870 parameters in the LLDP configuration file

Section Header and Path	Parameters	Value Range	Description
[cfg: /phone/config /system.ini,reboot=1]	LLDP.EnableLLDP	0 or 1	Indicates whether to enable the LLDP function. • **0**: no • **1**: yes Default value: 0
	LLDP.PacketInterval	1 to 3600	Interval for sending LLDP packets, in seconds. Default value: 120

2.3.5 Enabling the 802.1x Authentication

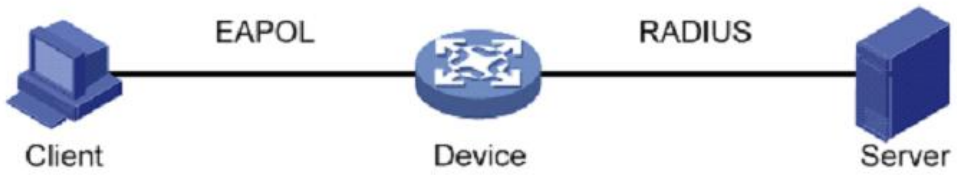
Function Description

802.1x is a protocol for port-based network access control. It provides an authentication mechanism to devices that attempt to connect to a LAN.

- If a device is authenticated, the device can access resources on the LAN.
- If a device fails the authentication, the device cannot access resources on the LAN.

An 802.1x system works in Client/Server mode, as shown in Figure 2-11. The 802.1x authentication involves three parties: a client, a device, and an authentication server.

Figure 2-11 Three parties involved in 802.1x authentication

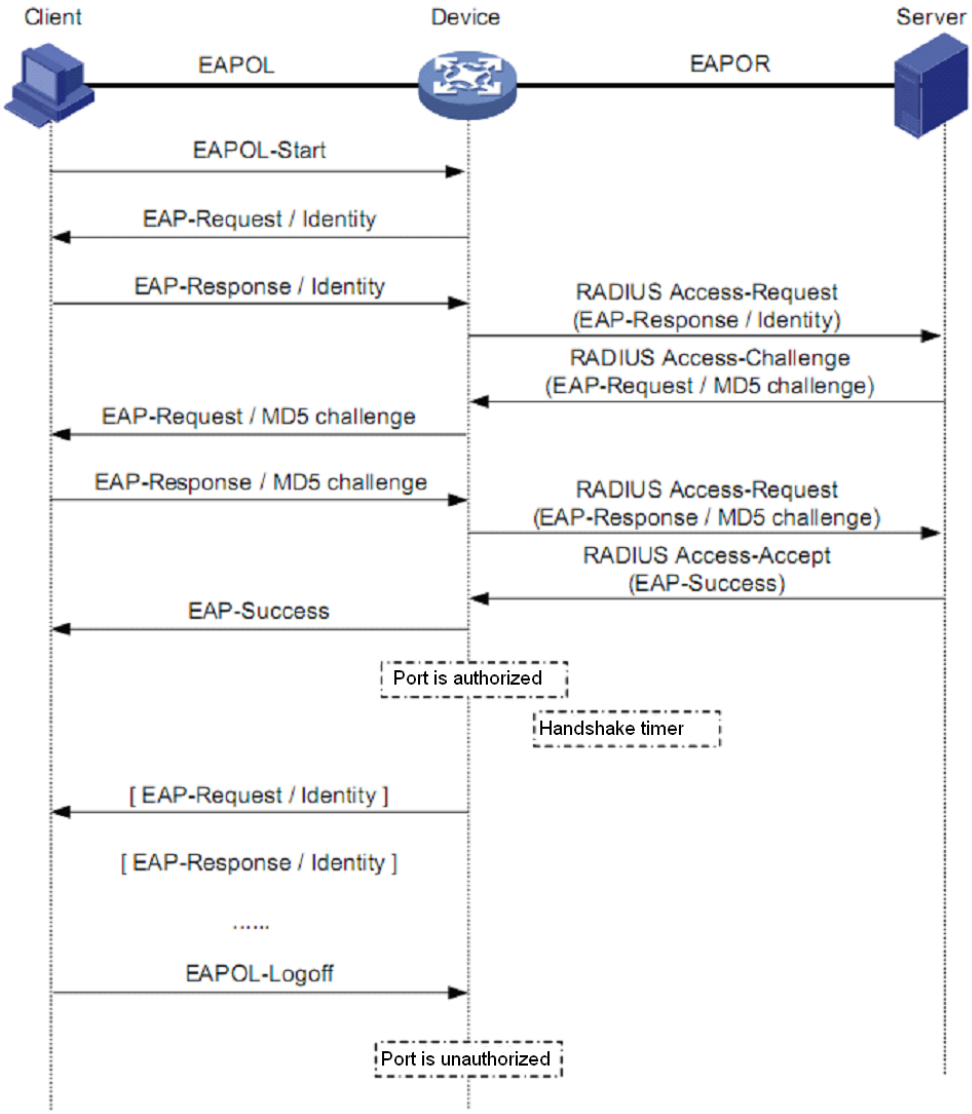


A device provides ports for clients to access a LAN. The ports support the following access control modes:

- Authorized-force: A port in this mode allows clients to access network resources without authenticating the clients.
- Unauthorized-force: The device does not authenticate clients accessed through a port in this mode.
- Auto: A port in this mode allows clients to send and receive packets but does not allow clients to access network resources before authentication succeeds. If authentication succeeds, the port allows clients to access network resources. This mode is mostly used.

eSpace 7870, 7850, 7830, 7820 and 7810 supports the EAP-MD5 authentication algorithm. Figure 2-12 hows the process of EAP-MD5-based 802.1x authentication.

Figure 2-12 Process of EAP-MD5-based 802.1x authentication



The authentication process is as follows:

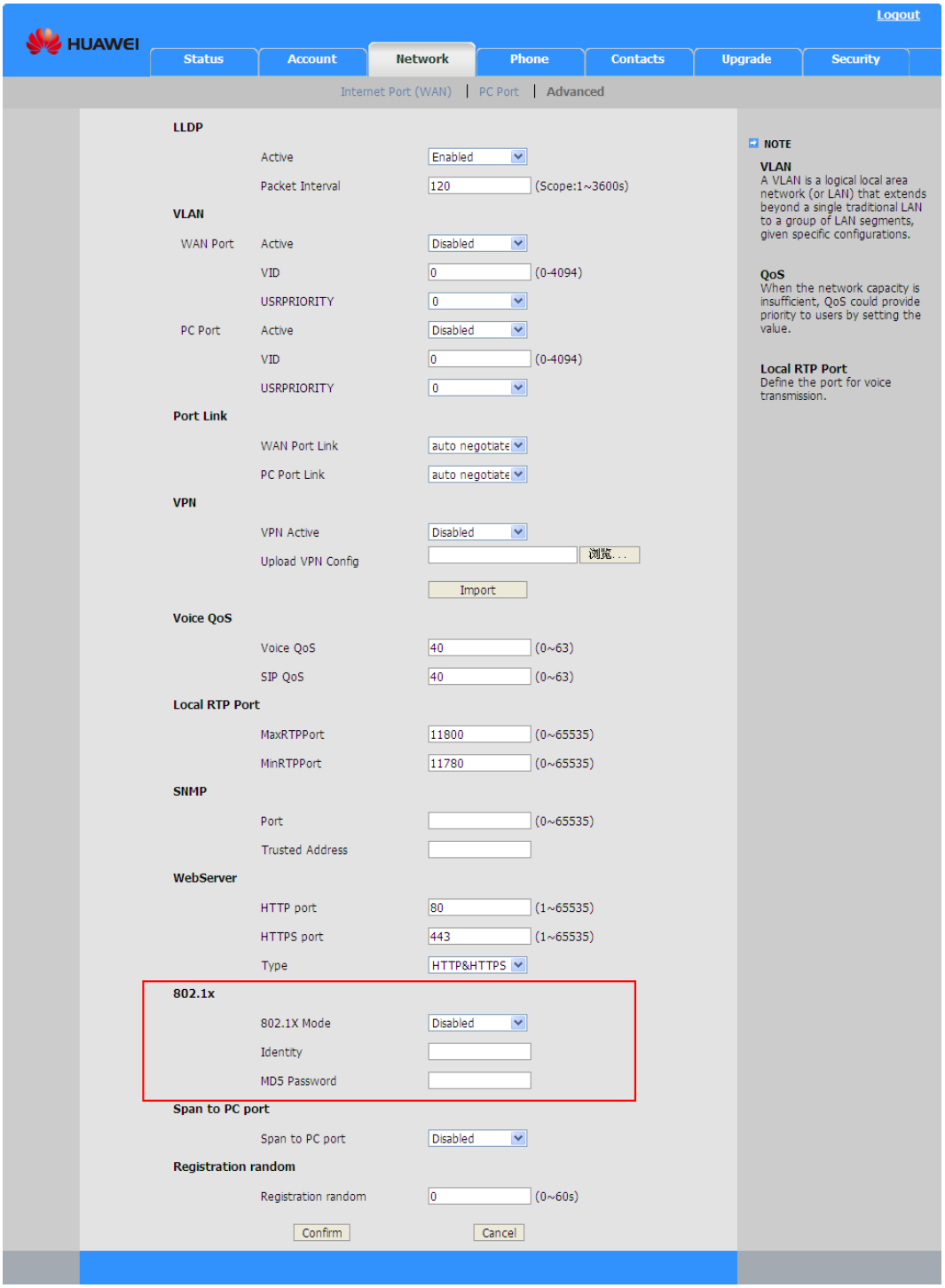
1. A client sends an EAPOL-Start packet to a device.
2. The device receives the packet and sends an EAP-Request/Identity packet, requesting the client to send the user name. The device encapsulates frames from the client into a packet and sends the packet to the authentication server.
3. The client sends the user name that is contained in the EAP-Response/Identity packet to the device.
4. The authentication server searches the database for the user name in the packet and obtains the corresponding password. The authentication server uses a randomly generated encryption key to encrypt the password and sends the encryption key to the device through the Access-Challenge packet.
5. The device sends the encryption key to the client.

6. The client receives the EAP-Request/MD5 Challenge packet containing the encryption key. The client uses the encryption key to encrypt the password, generates an EAP-Response/MD5 Challenge packet, and sends the packet to the device. The device sends the packet to the authentication server.
7. The encryption algorithm is irreversible normally.
8. The authentication server receives the RADIUS Access-Request packet containing the encrypted password. It compares the encrypted password and the password encrypted by the authentication server itself. If they are the same, the server regards that the user is authorized and sends a RADIUS Access-Accept packet and an EAP-Success packet to the device.
9. The device changes the port status and allows the client to access the network. The device periodically sends a handshake packet to the client to monitor the user status (online or offline). By default, if the device does not receive a response from the client after sending two handshake packets, the device takes the user offline, which enables the device to take the user offline if the user goes offline due to exceptions.
10. If the user name or password set for the IP phone is incorrect, the device sends a Failure packet. After authentication fails, the IP phone sends a Start packet to request for authentication again.
11. The client sends an EAPOL-Logoff packet to the device for going offline. The device changes the port status from authorized to unauthorized, and sends an EAP-Failure packet to the client.

Phone Configuration

1. Set **802.1X Mode** to **EAP-MD5**, and set **Identity** and **MD5 Password** in the **Advanced** area on the **Network** tab page, as shown in Figure 2-13.

Figure 2-13 Setting 802.1x parameters



2. Click **Confirm**.

   A dialog box is displayed, prompting you to restart the IP phone, as shown in Figure 2-14.

Figure 2-14 Restart dialog box

3. Click **OK**.

   The IP phone restarts.

   After the IP phone is restarted, the 802.1x authentication is enabled.

Basic Operations

The basic operations on an IP phone remain the same after 802.1x authentication is enabled.

If 802.1x authentication has been enabled when an IP phone is powered on, the IP phone sends a Start packet to the server three times at an interval of three seconds. Use Wireshark to catch authentication packets. The filter condition is eap||eapol. For details on how to use Wireshark, see 6.1.2 Using a Packet Capture Tool to Capture Packets.

If the server does not need to be authenticated, the server does not respond to the request.

Figure 2-15 shows a Wireshark page displayed when the server does not require authentication.

Figure 2-15 Wireshark page displayed when the server does not require authentication

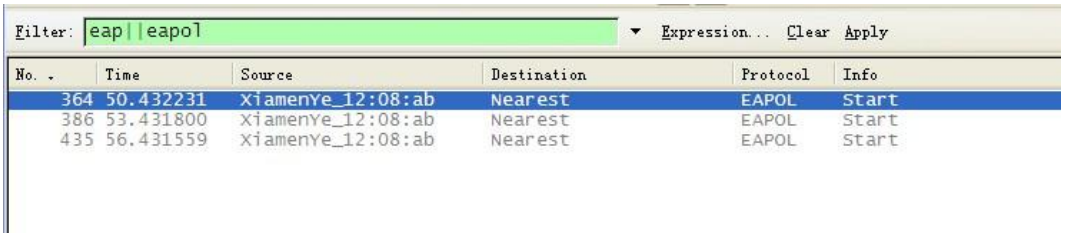
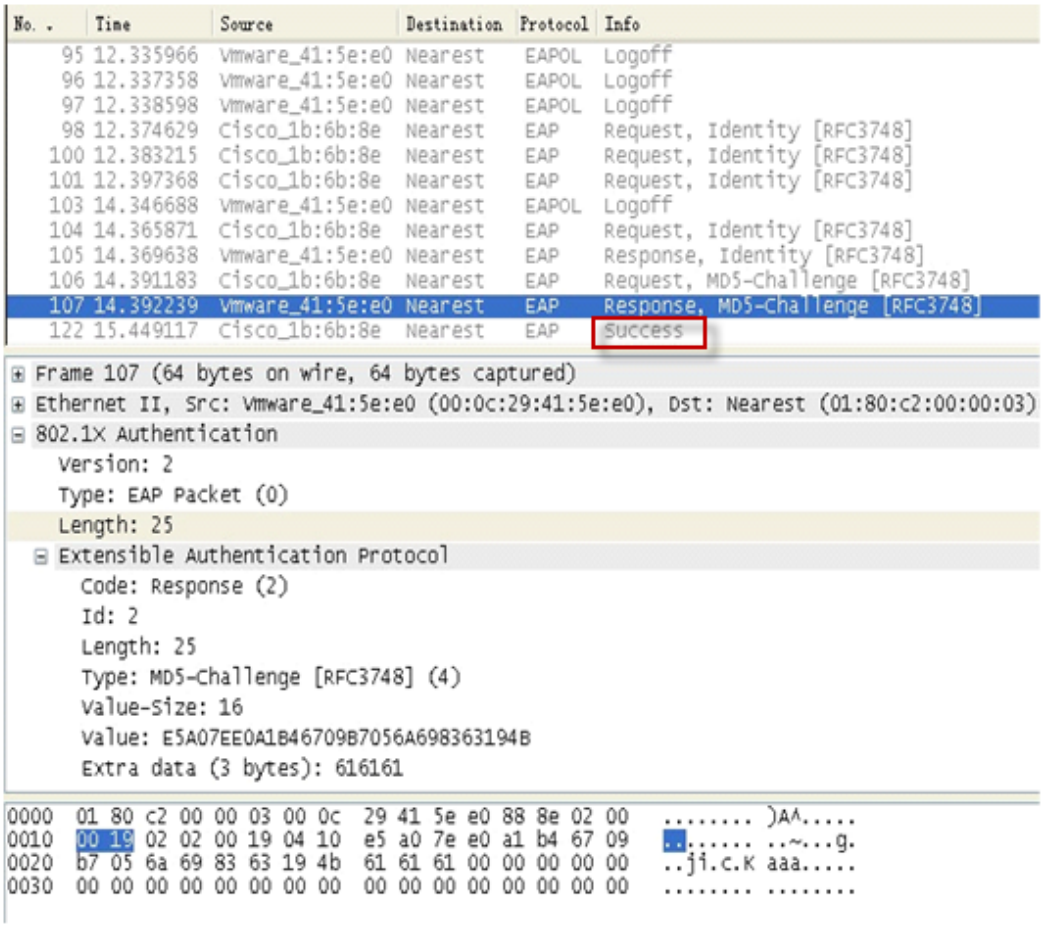


Figure 2-16 shows a Wireshark page displayed when the server requires authentication.

Figure 2-16 Wireshark page displayed when the server requires authentication



When authentication succeeds, the server sends a Success packet. If the user name or password set for the IP phone is incorrect, the server sends a Failure packet. If this happens, enter the correct user name and password on the web page.

Configuration File

Table 2-13 eSpace 7850, 7830, 7820 and 7810 parameters in the 802.1x configuration file

Section Header and Path	Parameters	Value Range	Description
[802.1X] path = /config/Network/Network.cfg	Mode	**0** or **1**	Indicates whether to enable the 802.1x function. **0**: no **1**: yes If the parameter is set to **1**, the EAP-MD5 algorithm is enabled. Default value: **0**

Section Header and Path	Parameters	Value Range	Description
	Identity	Character string	User name. The parameter is left blank by default.
	MD5Passwd	Character string	Password corresponding to the user name. The parameter is left blank by default.

2.3.6 Configuring Other Advanced Network Functions

This section describes other parameters in the **Advanced** area on the **Network** tab page, as shown in Figure 2-17.

Figure 2-17 Setting other advanced network parameters

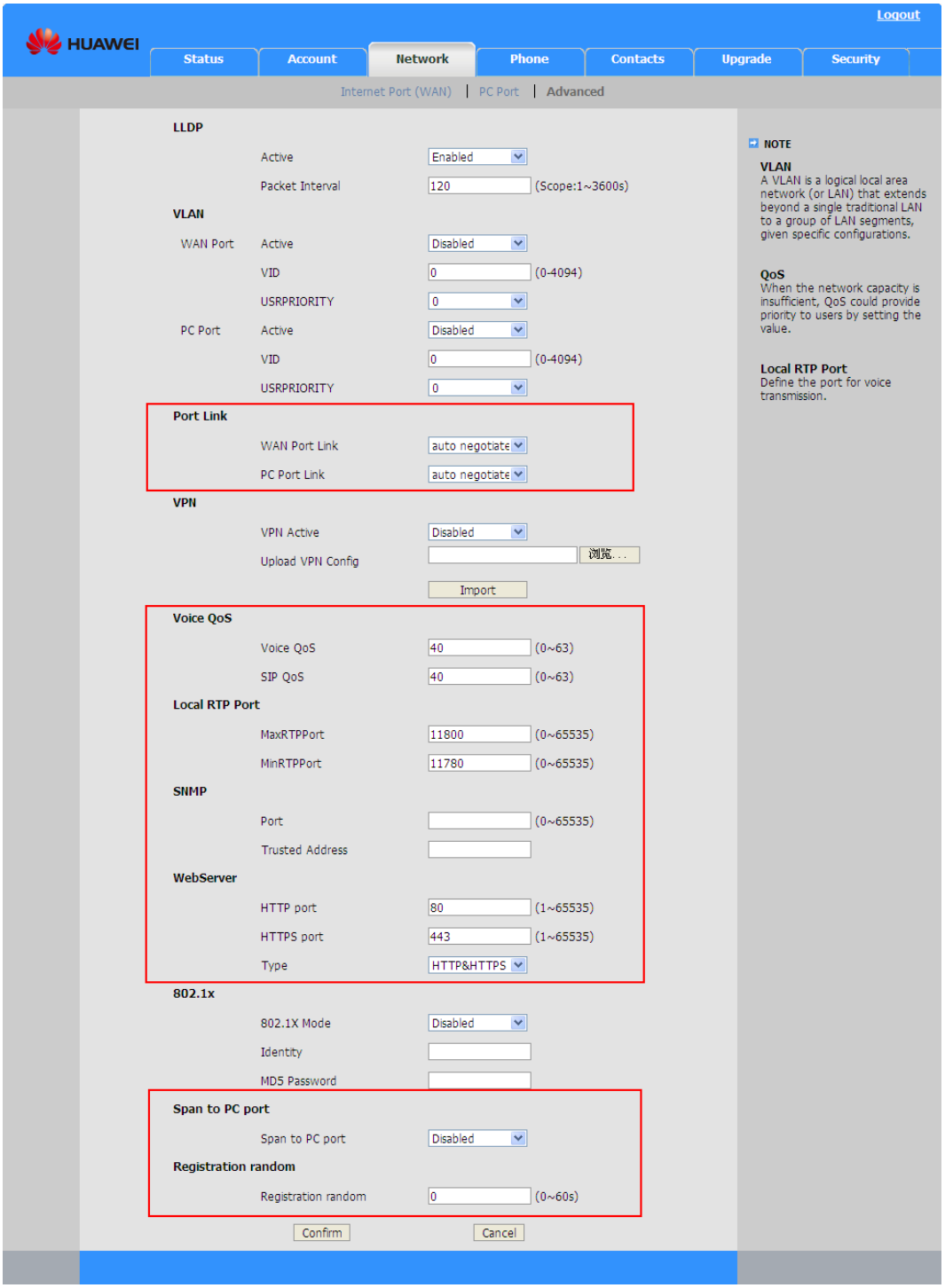


Table 2-14 lists advanced network parameters in the red-framed parts.

Table 2-14 Other advanced network parameters

Parameter	Description
Port Link	
WAN Port Link	Network connection rate for the network port. The options are as follows: • **auto negotiate**: An IP phone selects a connection mode based on the network environment. • **full duplex, 10 Mbps** • **full duplex, 100 Mbps** • **half duplex, 10 Mbps** • **half duplex, 100 Mbps** Only **auto negotiate** is available to eSpace 7870.
PC Port Link	Network connection rate for the PC port. The options are as follows: • **auto negotiate**: An IP phone selects a connection mode based on the network environment. • **full duplex, 10 Mbps** • **full duplex, 100 Mbps** • **half duplex, 10 Mbps** • **half duplex, 100 Mbps** Only **auto negotiate** is available to eSpace 7870.
QoS	
Voice QoS	Voice QoS. Value range: 0 to 63
SIP QoS	Signaling QoS. Value range: 0 to 63
Local RTP Port	
MaxRTPPort	Maximum port number.
MinRTPPort	Minimum port number. The value must not be greater than the value of **MaxRTPPort**.
SNMP (It is unavailable to eSpace 7870.)	
Port	Port number for listening on the IP phone.
Trusted Address	IP address of the management device, for example, a PC. A maximum of three IP addresses are supported. Separate each two IP addresses with a space character.
WebServer	
HTTP port	Port number used for using HTTP to access web pages. Default value: 80
HTTPS port	Port number used for using HTTPS to access web pages.

Parameter	Description
	Default value: 443
Type	Type for accessing web pages of the IP phone. The options are as follows: • **Disabled**: web pages cannot be accessed. • **HTTP&HTTPS**: HTTP or HTTPS can be used to access web pages. • **HTTP only**: Only HTTP can be used to access web pages. • **HTTPs only**: Only HTTPS can be used to access web pages.
Span to PC port	Indicates whether the PC port can receive Internet data packet. • **Disabled**: The PC port cannot receive Internet data packet. In this case, the IP phone functions as a switch. • **Enabled**: The PC port can receive Internet data packet. In this case, the IP phone functions as a hub. Default value: Disabled This parameter is unavailable to eSpace 7870 because it does not support transparent transmission.
Registration random	• **Enabled**: After power-on, an IP phone registers with the SIP server within the specified time segment. • **Disabled**: An IP phone registers with the SIP server immediately after power-on.

Table 2-15 lists SNMP MIBs.

Table 2-15 SNMP MIBs

OID	Name	Value
1.3.6.1.2.1.37459.2.1.1.0	phoneSyscontact.0	Sysadmin (root@localhost)
1.3.6.1.2.1.37459.2.1.2.0	phoneSysname.0	IPPHONE
1.3.6.1.2.1.37459.2.1.3.0	phoneSyslocation.0	Server Room
1.3.6.1.2.1.37459.2.1.4.0	phoneUptime.0	System running period. The value is an integer.
1.3.6.1.2.1.37459.2.1.5.0	phoneFirewareVersion.0	Phone firmware version. For example, **2.60.0.0**.
1.3.6.1.2.1.37459.2.1.6.0	phoneHardwareVersion.0	Hardware version. For example, **1.0.0.0**.
1.3.6.1.2.1.37459.2.1.7.0	phoneModel.0	Phone model. For example, **eSpace 7850**.
1.3.6.1.2.1.37459.2.1.8.0	phoneMacAddress.0	MAC address. Format: 001565******

OID	Name	Value
1.3.6.1.2.1.37459.2.1.9.0	phoneIPAddress.0	IP address. The value is a dot-decimal notation.
1.3.6.1.2.1.37459.2.1.10.0	phoneLastUpVersion.0	Target version to which the current version is automatically updated. Format: MacVersion[*]ComVersion[*]

Configuration File

Table 2-16 eSpace 7850, 7830, 7820 and 7810 parameters for configuring advanced network functions in the configuration file

Section Header and Path	Parameters	Value Range	Description
[Ethernet] path = /config/Network/Network.cfg	WANPortLink	0 to 4	Network connection rate for the network port. • **0**: An IP phone selects a connection mode based on the network environment. • **1**: full duplex, 10 Mbit/s • **2**: full duplex, 100 Mbit/s • **3**: half duplex, 10 Mbit/s • **4**: half duplex, 100 Mbit/s Default value: 0
	PCPortLink	0 to 4	Network connection rate for the PC port. • **0**: An IP phone selects a connection mode based on the network environment. • **1**: full duplex, 10 Mbit/s • **2**: full duplex, 100 Mbit/s • **3**: half duplex, 10 Mbit/s • **4**: half duplex, 100 Mbit/s Default value: 0
[QOS] path = /config/Network/Network.cfg	RTPTOS	0 to 63	Voice QoS. Default value: 40
	SIGNALTOS	0 to 63	Signaling QoS. Default value: 40
[snmp] path =	snmp_port	1 to 65535	Port number for listening on the IP phone.

Section Header and Path	Parameters	Value Range	Description
/config/Network/Network.cfg			The parameter is left blank by default.
	snmp_trusted_address	IP address	IP address for the management device. The parameter is left blank by default.
[RTPPORT] path = /config/Network/Network.cfg	MaxRTPPort	0 to 65535	Maximum RTP port number. Default value: 11800
	MinRTPPort	0 to 65535	Minimum RTP port number. Default value: 11780
[port] path = /config/Setting/AdvSetting.cfg	http_port	1 to 65535	Port number used for using HTTP to access web pages. Default value: 80
	https_port	1 to 65535	Port number used for using HTTPS to access web pages. Default value: 443
[Webserver Type] path = /config/Advanced/Advanced.cfg	WebType	0 to 3	Type for accessing web pages of the IP phone. The options are as follows: • **0**: web pages cannot be accessed. • **1**: HTTP or HTTPS can be used to access web pages. • **2**: Only HTTP can be used to access web pages. • **3**: Only HTTPS can be used to access web pages. Default value: 1
[LAN] path = /config/Network/Network.cfg	SpanToPCPort	0 or 1	Indicates whether the PC port can receive Internet data packet. • **0**: no • **1**: yes Default value: 0
[REGSURGE] path = /config/Network/Network.cfg	RegSurgePrevention	0 to 60	Interval between IP phone power-on and account registration. Default value: 0

Table 2-17 eSpace 7870 parameters for configuring advanced network functions in the configuration file

Section Header and Path	Parameters	Value Range	Description
[cfg:/phone/config/system.ini,reboot=1]	QoS.RTPTOS	0 to 63	Voice QoS. Default value: 40
	QoS.SIGNALTOS	0 to 63	Signaling QoS. Default value: 40
[cfg:/phone/config/system.ini,reboot=1]	RTPPORT.MaxRTPPort	2 to 65534	Maximum RTP port number. Default value: 11800
	RTPPORT.MinRTPPort	2 to 65534	Minimum RTP port number. Default value: 11780
[cfg:/phone/config/user.ini,reboot=0]	Port.http_port	1 to 65535	Port number used for using HTTP to access web pages. Default value: 80
	Port.https_port	1 to 65535	Port number used for using HTTPS to access web pages. Default value: 443
[cfg:/phone/config/user.ini,reboot=0]	Webserver Type.WebType	0 to 3	Type for accessing web pages of the IP phone. The options are as follows: • **0**: web pages cannot be accessed. • **1**: HTTP or HTTPS can be used to access web pages. • **2**: Only HTTP can be used to access web pages. • **3**: Only HTTPS can be used to access web pages. Default value: 1
[cfg:/phone/config/system.ini]	REGSURGE.RegSurgePrevention	0 to 60	Interval between IP phone power-on and account registration. Default value: 0

2.4 Phone Configuration

2.4.1 Configuring Common Operations

For details on how to configure an IP phone, see the *Huawei IP Phone eSpace xxxx IP Phone User Manual*, in which xxx represents the IP phone model.

2.4.2 Configuring Softkey Layout

The four soft keys on eSpace 7870, 7850, 7830 and 7820 are programmable when the IP phone is in the specified 12 states. You can configure the soft keys in the **Softkey Layout** area on the **Phone** tab page, as shown in Figure 2-18.

Figure 2-18 Configuring soft keys

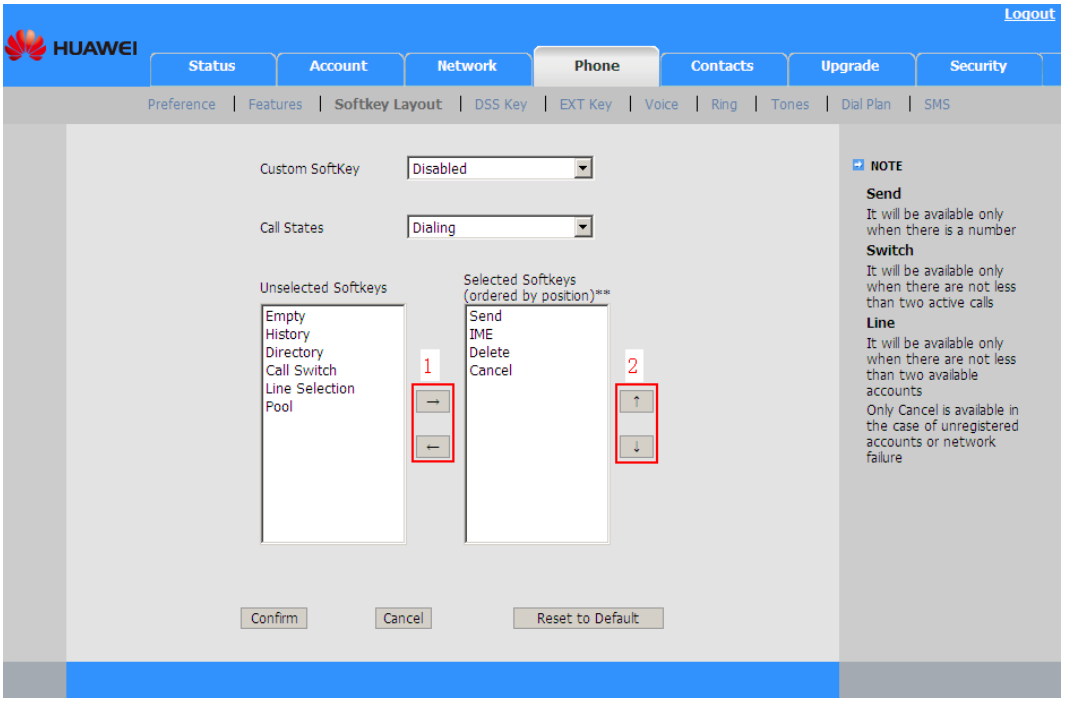


Table 2-18 Parameters for configuring soft keys

Field	Description
Custom SoftKey	The settings for soft keys take effect only when the parameter is set to **Enabled**.
Call States	The options are as follows: • Dialing • Connecting • Transfer Connecting • RingBack • Transfer RingBack

Field	Description
	• Call Failed • Call In • On Talk • Hold • Held • Transfer to • Conferenced
Unselected Softkeys	Functions that are not assigned to soft keys.
Selected Softkeys(ordered by position)	Functions that have been assigned to soft keys. If more than four keys are selected, the fourth key is automatically changed to **More**. The **More** key is used for switching to the next page.
<←>/<→>	The left and right arrow buttons marked by 1 in Figure 2-18 are used to move soft keys between the **Unselected Softkeys** and **Selected Softkeys(ordered by position)** list boxes.
<↑>/<↓>	The up and down arrow buttons marked by 2 in Figure 2-18 are used to adjust the order of soft keys in the **Selected Softkeys(ordered by position)** list box.
Reset to Default	Click this button to restore factory settings for soft keys.

Table 2-19 lists keys that can be set on the 12 different pages.

Table 2-19 Keys that can be set on the 12 different pages

Key Value	Key Function	Pages Where the Key Value Can Be Set
Empty	No function is assigned to the soft key. If this option is selected, no information is displayed on an IP phone's LCD.	Dialing, Connecting, Transfer Connecting, RingBack, Transfer RingBack, Call Failed, Call In, On Talk, Hold, Held, Transfer to, Conferenced
History	Views call history.	Dialing
Directory	Views address books.	Dialing, Transfer to
Pool	Accesses the address pool, including the call history, local address book, and remote address book.	Dialing

Key Value	Key Function	Pages Where the Key Value Can Be Set
Call Switch	Switches calls. The status of a call is changed to **Hold** after the key is pressed.	Dialing, Connecting, Transfer Connecting, RingBack, Transfer RingBack, Call Failed, Call In, On Talk, Hold, Held, Transfer to, Conferenced
SWAP	Switches calls. The call is resumed after the key is pressed.	On Talk
Line Selection	Selects an account to make a call.	Dialing
Send	Makes a call.	Dialing, Transfer to
IME	Changes the input method. The input methods abc, ABC, 2aB, and 123 are available.	Dialing, Transfer to
Delete	Deletes characters.	Dialing, RingBack, Transfer to
Cancel	Cancels an operation.	Dialing, Connecting, Transfer Connecting, Transfer RingBack, Call Failed, On Talk, Hold, Held, Transfer to, Conferenced
New Call	Accesses the dialing page to make a new call.	Call Failed, On Talk, Hold, Held
Answer	Answers an incoming call.	Call In, On Talk, Hold, Held, Conferenced
Reject	Rejects an incoming call.	Call In, On Talk, Hold, Held, Conferenced
Silence	Stops the ring tone.	Call In
Mute	Mutes the call. After a user presses this key, others cannot hear the user's voice.	On Talk, Conferenced
Resume	Resumes a call.	Hold
Forward	Forwards an incoming call.	Call In
Transfer	Transfers an incoming call.	Transfer Connecting, Transfer RingBack, On Talk, Hold, Transfer to
Conference	Initiates a conference.	On Talk

Key Value	Key Function	Pages Where the Key Value Can Be Set
Split	Splits a conference and establishes a call between the moderator and each participant.	Conferenced

Configuration File

For details, see the description of **[CustomSoftKey_Dialing]** to **[CustomSoftKey_CallFailed]** in the configuration file.

2.4.3 Configuring DSS Keys

Function Description

Users can configure memory keys, line keys, programmable keys, and expansion modules to implement specific functions.

Table 2-20 lists the number of DSS keys for eSpace 7870, 7850, 7830, 7820 and 7810.

Table 2-20 Number of DSS keys for eSpace 7870, 7850, 7830, 7820 and 7810

Model	Memory Key	Line Key	Programmable Key	eSpace 7803X
eSpace 7870	10	6	14	38*2
eSpace 7850	10	6	14	38 x 2
eSpace 7830	10	3	14	38 x 2
eSpace 7820	N/A	3	11	N/A
eSpace 7810	N/A	2	9	N/A

The four soft keys can be configured to make key distribution more user-friendly for users in various states, for example, when a user dialing a number, the ring tone is playing, or the calling and called parties are talking to each other. For details, see 2.4.2 Configuring Softkey Layout.

Memory Key

eSpace 7870, 7850, and 7830 have 10 memory keys for each.

Each memory key has 28 configuration types. You can configure the 10 memory keys under **Memory Key** in the **DSS Key** area on the Phone **tab** page, as shown in Figure 2-19.

You can configure the 10 memory keys for eSpace 7870 under **Memory Key** in the **DSS Key**.

Figure 2-19 Configuring memory keys

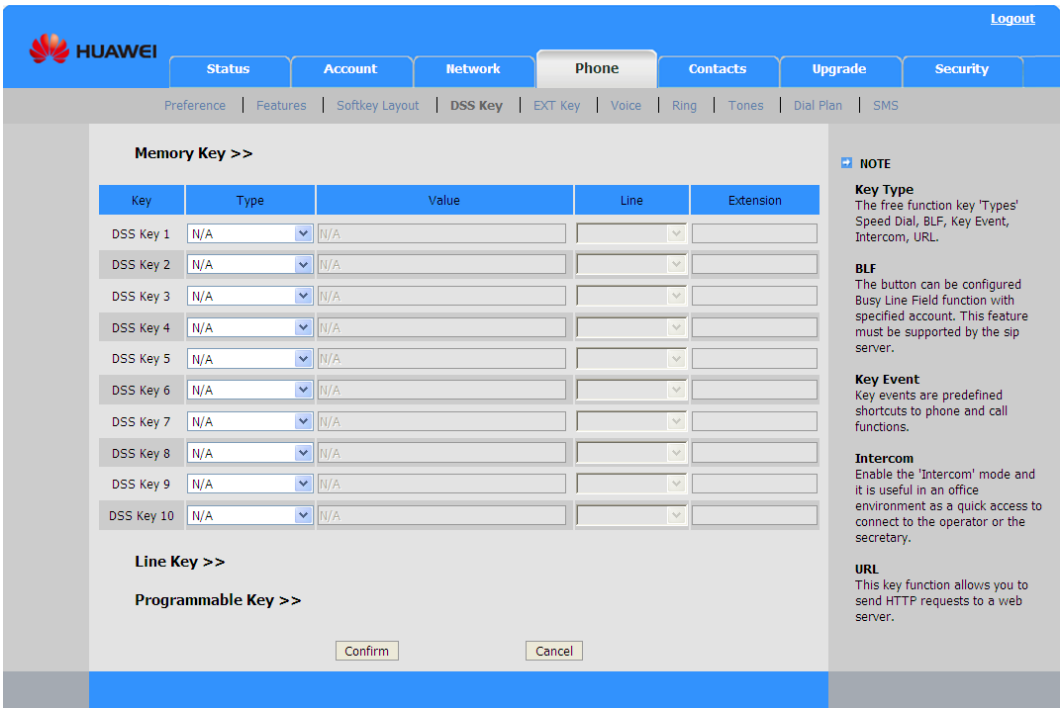


Table 2-21 Parameters for configuring memory keys

Parameter	Description
Key	Memory key.
Type	Key type. Table 2-22 lists details about the types.
Value	The setting varies according to the functions that you assign. For example, if you assign the speed dial function to a memory key, enter the speed dial number to the **Value** text box.
Line	Account or group address book that a function is assigned to. • If the value of **Type** is not **Local Group**, **XML Group**, or **LDAP**, the options for this parameter are **Auto** and **Line1** to **Line 6**. If **Auto** is selected, the default account is used. • If **Type** is set to **Local Group**, **XML Group**, or **LDAP**, group address books are available for this parameter.
Extension	Function code. Currently, this parameter needs to be set only when you configure the BLF function. Assume that the call pickup function code is ***83**. User A sets this parameter to *83 to configure the BLF function. When a call comes to user B, user A can press the BLF memory key to pick up the call for user B.

Table 2-22 Description of memory key types

Type	Description	Setting	Line Option
N/A	Assigns no function.	N/A	N/A
Line	Functions as a line key.	N/A	Auto, and Line 1 to Line 6
Speed Dial	Functions as the speed dial key.	Enter a speed dial number.	Auto, and Line 1 to Line 6
BLF	Listens on a number. When the BLF function is enabled, a user can know the current status (for example, idle, ringing, or talking) of the preset number.	Enter a number to be listened on.	Line 1 to Line 6
Voice Mail	Obtains voice messages.	Enter the code for connecting to a voice mailbox.	Line 1 to Line 6
Pick Up	Picks up calls for a preset number. When a preset number has an incoming call, a user can press the corresponding DSS key to pick up the call.	Enter the function code and the picked up number, for example, ***83123**. In ***83123**, ***83** is the function code indicating call pickup, and **123** is the picked up number.	Line 1 to Line 6
Group Pickup	Picks up calls for a group. When a preset group has an incoming call, a user can press the corresponding DSS key to pick up the call.	Enter the function code for picking up calls of a group. For example, ***78**.	Auto, and Line 1 to Line 6
Call Park	Parks a call when a user wants to store the call before retrieving it from another phone. For example, user A is in a conversation with user C. If user A wants to use another phone to continue the conversation, user A can park the call on an account of the SIP server.	Set an account that calls are parked for, for example, **123**.	Line 1 to Line 6
DTMF	DTMF key. If a number is dialed frequently at the second dialing stage, the number can be set for the memory key, which improves work efficiency.	Enter a DTMF number.	N/A
Prefix	Specifies the same prefix of numbers	Enter the prefix.	N/A

Type	Description	Setting	Line Option
	that you often dial. The prefix (for example, 0086592) is displayed on the eSpace 7850 screen when you press this key.		
Local Group	Views the local address book.	N/A	Select **Contacts** (containing all local contacts) or an existing group.
Remote Group	Views a remote address book. You must upload a remote address book before viewing it.	N/A	Select a remote address book that you want to view.
XML Browser	Specifies a browser based on the Extensible Markup Language (XML). The browser can be used to view weather forecast, stock information, and news. This type is unavailable to eSpace 7870.	Enter a URL.	N/A
LDAP	Views the LDAP address book. Before viewing the LDAP address book, you must configure it and set related parameters in the **LDAP** area on the **Contacts** tab page. For details, see 2.5.2 Configuring LDAP.	N/A	N/A
Conference	Sets up a conference during a conversation.	N/A	N/A
Forward	Forwards calls. The call forward function varies according to eSpace 7850 status. When the IP phone is in the standby state, the key of this type provides the following functions: • If the call forwarding unconditional (CFU) number is not configured on the eSpace IP phone, you can press the Programmable key to enter the CFU configuration page. • If the CFU number is configured on the eSpace IP phone, you	Enter the number that calls are forwarded to.	N/A

Type	Description	Setting	Line Option
	cannot enter the CFU configuration page by pressing the memory key. The Programmable key is only used to enable or disable the CFU service. When the IP phone is in the ringing state, the key of this type provides the following functions: • If the CFU number is not configured on the eSpace IP phone and the memory key value is configured, incoming calls are directly transferred to the number configured for the memory key. • If the CFU number is configured on the eSpace IP phone, you can press the memory key to transfer incoming calls to the CFU number.		
Transfer	Transfers calls.	If this parameter is left blank, this key functions as the transfer key. If this parameter is set to a number, press this key to transfer a call to the preset number.	N/A
Hold	Functions as the Hold/Retrieve key.	N/A	N/A
DND	Functions as the DND key.	N/A	N/A
Redial	Functions as the redial key. When a user presses the key of this type on the IP phone in the standby state, the IP phone accesses the **Dialed Calls** page.	N/A	N/A
Call Return	Calls back the last calling party.	N/A	N/A
Paging	Enables the broadcast function. You need a VoIP PBX server where a paging group is configured to support the broadcast function. After you press this key, numbers in the paging groups are connected.	Set numbers in the paging group.	Auto, and Line 1 to Line 6
Group Listening	Functions as the group listening key. Use this function if multiple persons participate in a conference. • During a conversation in the handset mode, after you press the	N/A	N/A

Type	Description	Setting	Line Option
	group listening key, the handset and speaker play voices, but the peer party can hear the voices only from the handset. • During a conversation in the headset mode, after you press the group listening key, the headset and speaker play voices, but the peer party can hear the voices only from the headset.		
Public Hold	Is used for SCA group members to pause or resume a conversation.	N/A	N/A
Private Hold	Is used for SCA group members to pause a conversation. Only the member who pauses the conversation can resume it.	N/A	N/A
Share Line	Shares an account. Members who share the same account can check whether other members are using the account.	Enter the SCA account.	Select an account that registers the SCA function.

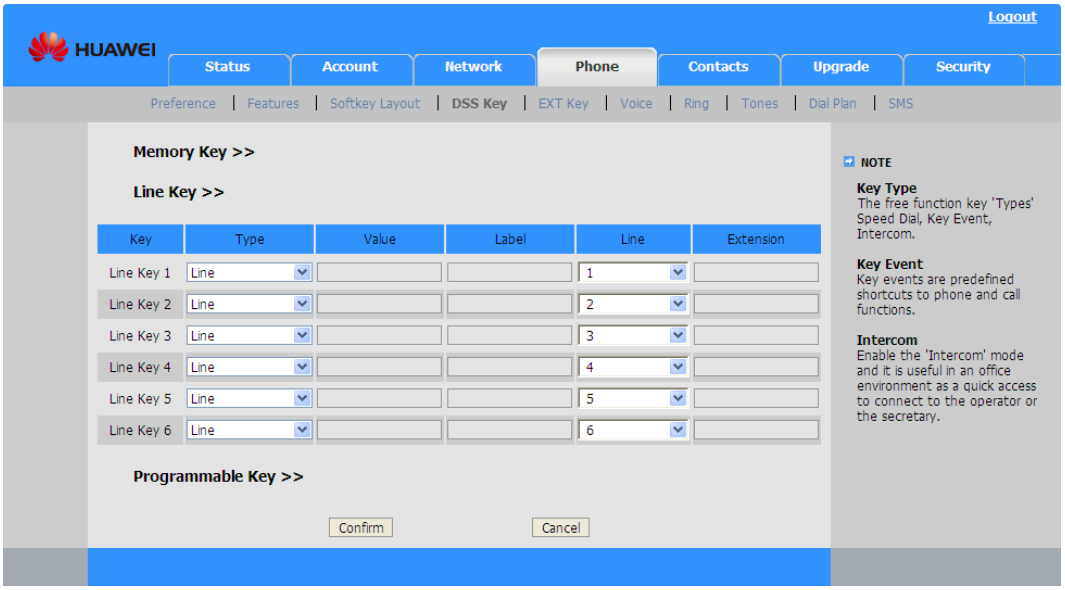
Configuration File

For details, see the description of **[memory1]** to **[memory10]** in the configuration file.

Line Key

You can configure the **line keys** under Line Key in the **DSS Key** area on the **Phone** tab page, as shown in Figure 2-20.

Figure 2-20 Configuring line keys



The differences between line key settings and memory key settings for eSpace 7870, 7850 and 7830 are as follows:

- Compared with memory keys, lines keys do not have the setting **N/A**.
- The default value of **Type** for line keys is **Line**, and the default value of **Type** for memory keys is **N/A**.

Compared with eSpace 7850, eSpace 7810 does not have the line key types:

- Remote group
- XML browser
- LDAP

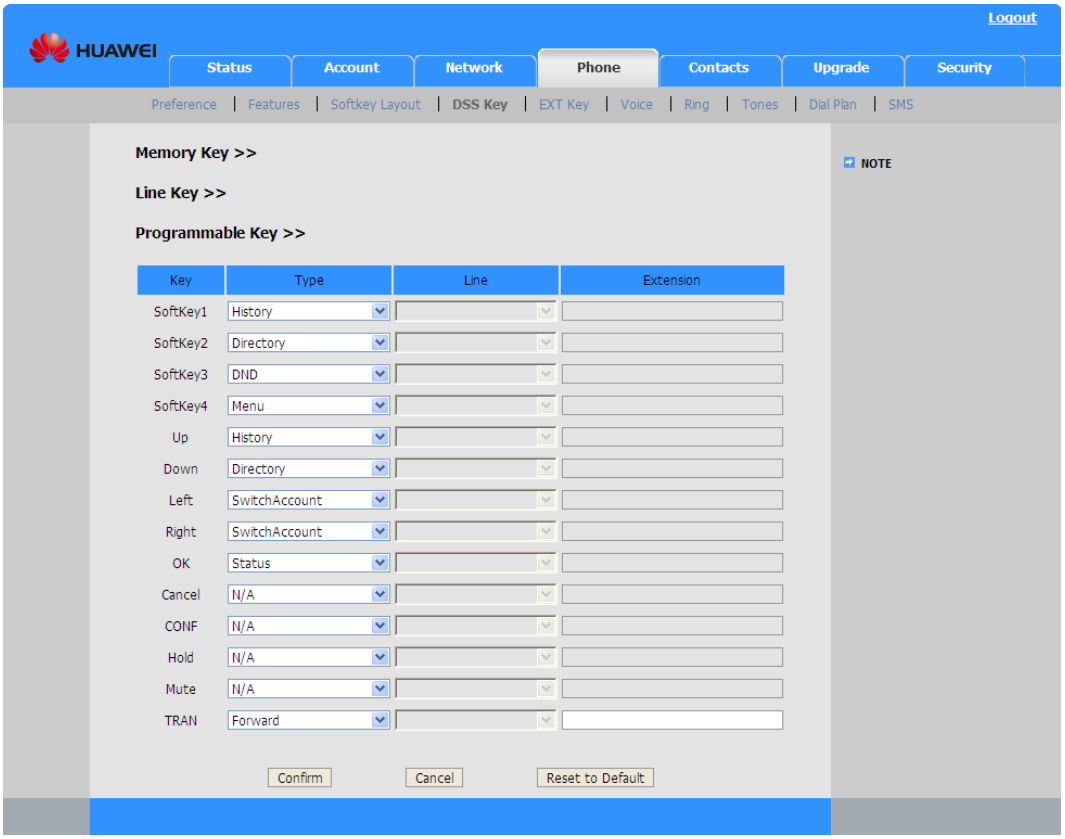
Configuration File

For details, see the description of **[memory11]** to **[memory16]** in the configuration file.

Programmable Key

eSpace 7870, 7850, and 7830 have 14 programmable keys for each, eSpace 7820 has 11 programmable keys and eSpace 7810 has 9 programmable keys. You can configure programmable keys under **Programmable Key** in the **DSS Key** area on the **Phone** tab page.

Figure 2-21 Configuring programmable keys



The programmable keys on eSpace 7870, 7850, and 7830 are as follows: four soft keys, four arrow keys (up, down, left, and right), **OK**, **X**, **CONF**, **HOLD**, **MUTE**, and **TRAN**.

The programmable keys on eSpace 7820 are as follows: four soft keys, four arrow keys (up, down, left, and right), **OK**, **X**, **TRAN**.

The programmable keys on eSpace 7810 are as follows: four arrow keys (up, down, left, and right), **OK**, **X**, **CONF**, **HOLD**, and **TRAN**.

CAUTION

- The programmable keys are valid only when an IP phone is in the standby state. When the IP phone is in other states, factory settings are valid for the keys.
- To restore factory settings, click **Reset to Default** under **Programmable Key**.

Table 2-23 lists the types of programmable key.

Table 2-23 Description of programmable key types

Type	Description	Line Option	Extension
N/A	• Keep the key **xX**, **CONF**, **HOLD**,	N/A	N/A

Type	Description	Line Option	Extension
	MUTE, or **TRAN** unselected, the keys remain original function. • Keep other keys unselected, the key has been set no function.		
Directory	Views address books. The local address book and remote address book can be set for eSpace 7850, 7820 and 7830. Only the local address book can be set for eSpace 7810.	N/A	N/A
History	Queries call history.	N/A	N/A
DND	Functions as the DND key.	N/A	N/A
Menu	Accesses the **Main Menu** page.	N/A	N/A
SwitchAccount	Switches accounts that are registered on eSpace 7850.	N/A	N/A
Forward	Forwards calls. • Enables or disables the CFU function when **Value** has been set. • Accesses the **Always Forward** page when **Value** is left blank.	N/A	N/A
Redial	Functions as the redial key. When a user presses the key of this type on the IP phone in the standby state, the IP phone accesses the **Dialed Calls** page.	N/A	N/A
Call Return	Calls back the last calling party.	N/A	N/A
Pick Up	Picks up calls for a preset number.	Line 1 to Line 6	Enter the function code and the picked up number, for example, ***83123**. In ***83123**, ***83** is the

Type	Description	Line Option	Extension
			function code indicating call pickup, and **123** is the picked up number.
XML Group	Views numbers of a group in the remote address book. This value is unavailable to eSpace 7810.	Select a remote address book that you want to view.	N/A
XML PhoneBook	Views a remote phone book. After a user presses the key of this type, the remote group list is displayed. This value is unavailable to eSpace 7810.	N/A	N/A
Status	Accesses the **Status** page.	N/A	N/A
Speed Dial	Functions as the speed dial key.	Auto, and Line 1 to Line 6	Enter a speed dial number.
Local Group	Views numbers of a group in the local address book. After a user presses the key of this type, the numbers of a group in the local address book are listed.	Select all contacts or a group.	N/A
Local PhoneBook	Views groups in the local address book.	N/A	N/A

Configuration File

For details, see the description of **[programablekey1]** to **[programablekey14]** in the configuration file.

2.4.4 Configuring eSpace 7803X

A maximum of two eSpace 7803Xs can be cascaded to eSpace 7870, 7850, and 7830 to extend DSS keys.

To configure eSpace 7803Xs, access the web page for the IP phone to which eSpace 7803Xs are cascaded, click the **Phone** tab, and click **EXT Key**, as shown in Figure 2-22.

To configure eSpace 7870, click the **DSS Key** tab and click **EXT Key**.

Figure 2-22 Configuring eSpace 7803X

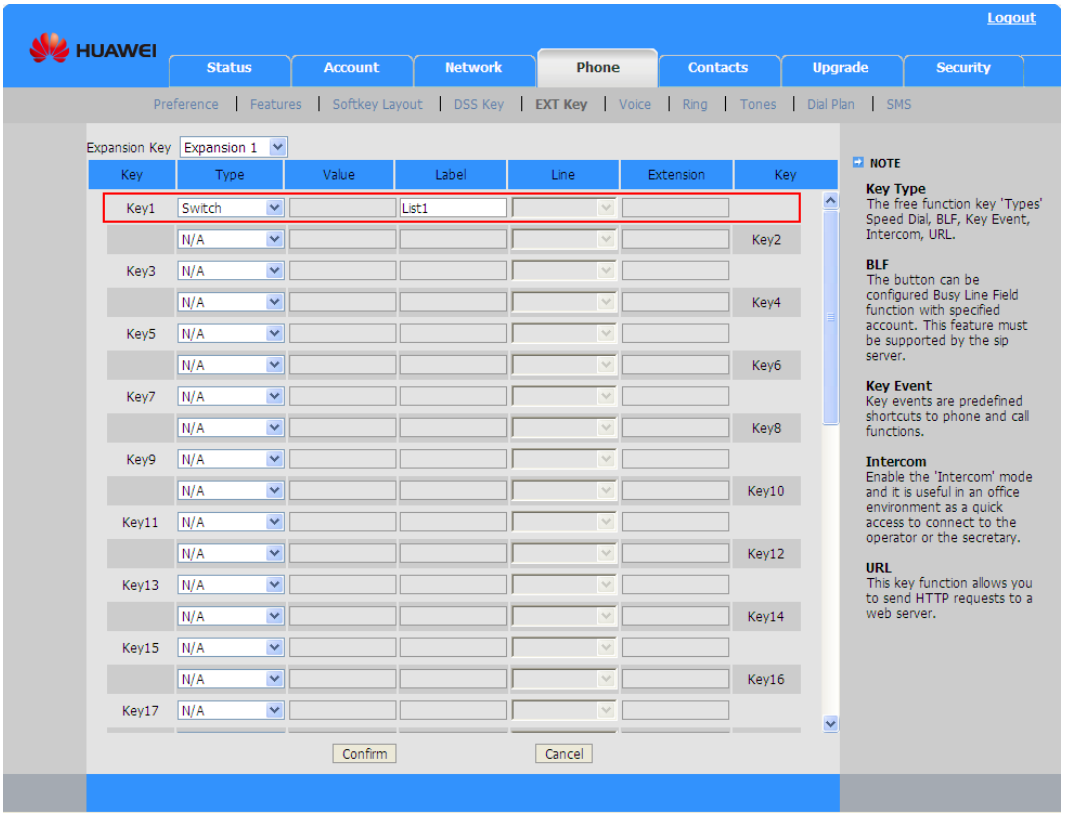


Table 2-24 Parameters for configuring eSpace 7803X

Field	Description
Expansion Key	ID of an expansion module. The value of **Expansion Key** for the first expansion module is **1**, and the value of **Expansion Key** for the second expansion module is **2**.
Type	There are 28 values of **Type** for keys (except Key1 and Key21), which are the same as the values for DSS keys. For details, see Table 2-22. For **Key1**, **Type** can be set to **Switch** in addition to the common 28 options so that users can switch two function pages. For **Key21**, **Type** can be set only to **Switch**.
Value/Line/Extension	The values for the three parameters are the same as those for memory keys. For details, see Table 2-21.
Label	Key function name that is displayed on the eSpace 7803X 's LCD.

Configuration File

For details, see the description in the line under **[memory16]** in the configuration file.

2.4.5 Configuration Ring

Function Description

The distinctive ring tone service allows a user to identify the callers based on the ring tone. The ring tone is specified in the Alert-Info message in the SIP Invite signaling. The ring tone can be a local ring tone or a remote ring tone.

Local ring tone: ring tone stored in the flash memory of an IP phone.

Remote ring tone: ring tone that an IP phone downloads from a URL specified in the SIP Invite signaling.

The SIP Invite signaling that the server sends control distinctive ring tones. Therefore, the distinctive ring tone service must be supported by the server.

Principles

The Alert-Info message in the SIP Invite signaling that the server sends to an IP phone specifies the ring tone. The Alert-Info message is in the following format:

Alert-Info:URL;info=info text

After receiving the message, the IP phone attempts to download the WAV ring tone file from the URL. If the IP phone fails to download the file, the IP phone plays the local ring tone associated with **info text**.

Phone Configuration

Set parameters for distinctive ring tones in the **Ring** area on the web configuration page, as shown in Figure 2-23.

Figure 2-23 Setting parameters for distinctive ring tones

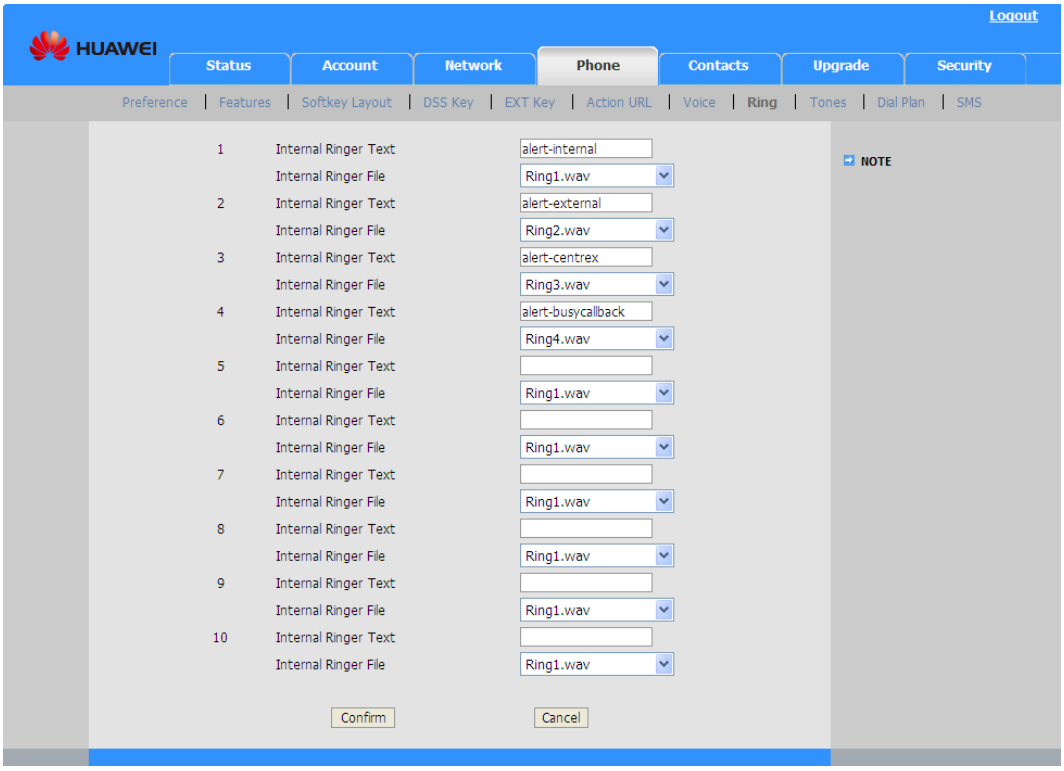


Table 2-25 lists parameters for configuring distinctive ring tones.

Table 2-25 Parameters for configuring distinctive ring tones

Field	Description
Internal Ringer Text	This parameter, same as the **info text** parameter in the Alert-Info message, is associated with a local ring tone file. The parameter values vary according to the server type. For example, the eSpace U19xx server has the following values: • **alert-internal** • **alert-external** • **alert-centrex** • **alert-busycallback**
Internal Ringer File	Ring tone file that is associated with the corresponding **info text**. In Figure 2-23, **alert-internal** is associated with **Ring1.wav**, **alert-external** is associated with **Ring2.wav**, **alert-centrex** is associated with **Ring3.wav**, and **alert-busycallback** is associated with **Ring4.wav**.

An example is as follows:

Alert-Info: http://www.example.com/sounds/moo.wav;info= alert-centrex

Assume that the settings in Figure 2-23 take effect.

When the IP phone receives a call, the IP phone receives the Alert-Info message. The phone attempts to download the ring tone file from http://www.example.com/sounds/moo.wav. If the ring tone file is successfully downloaded, the IP phone plays it. Otherwise, the IP phone plays the **Ring3.wav** file.

Configuration File

Table 2-26 eSpace 7850, 7830, 7820 and 7810 parameters in the configuration file for distinctive ring tones

Section Header and Path	Parameters	Permitted Values	Description
[AlertInfo0] path = /config/Setting/Setting.cfg	Text	Character string	This parameter corresponds to the first **Internal Ringer Text** parameter. The parameter is left blank by default.
	Ringer	Integer	Local ring tone that is associated with the first **Internal Ringer Text** parameter. The value **1** indicates **Ring1.wav**, the value **2** indicates **Ring2.wav**, and the value n indicates **Ringn.wav**. Default value: **1**
Parameters for the other nine **Internal Ringer Text** parameters are the same as those for the first one. The only difference is the numbers in the headers. The second header is **[AlertInfo1]**, the third header is **[AlertInfo2]**, and the nth header is **[AlertInfo(n-1)]**.			

Table 2-27 eSpace 7870 parameters in the configuration file for distinctive ring tones

Section Header and Path	Parameters	Permitted Values	Description
[cfg:/phone/config/user.ini,reboot=1]	AlertInfo0.Text	Character string	This parameter corresponds to the first **Internal Ringer Text** parameter. The parameter is left blank by default.
	AlertInfo0.Ringer	Integer	Local ring tone that is associated with the first **Internal Ringer Text** parameter. The value 1 indicates **Ring1.wav**, the value **2** indicates **Ring2.wav**, and the value n indicates Ringn.wav. Default value: **1**

Section Header and Path	Parameters	Permitted Values	Description
Parameters for the other nine **Internal Ringer Text** parameters are the same as those for the first one. The only difference is the numbers in the headers. The second header is **[AlertInfo1]**, the third header is **[AlertInfo2]**, and the nth header is **[AlertInfo(n-1)]**.			

2.4.6 Configuring the BLF Function

Function Description

The BLF function allows a user to listen on the status of other accounts. After the BLF function is assigned to a DSS key, users can press this key to implement the speed dial and call pick functions.

For eSpace 7870, 7850, 7830, 7820 and 7810, the BLF indicator's state (on, off, or blinking) and color show the status of the listened-on account.

Prerequisites

The BLF function has been enabled for an account on the SIP server. For details, see the *eSpace U19xx Unified Gateway Product Documentation*.

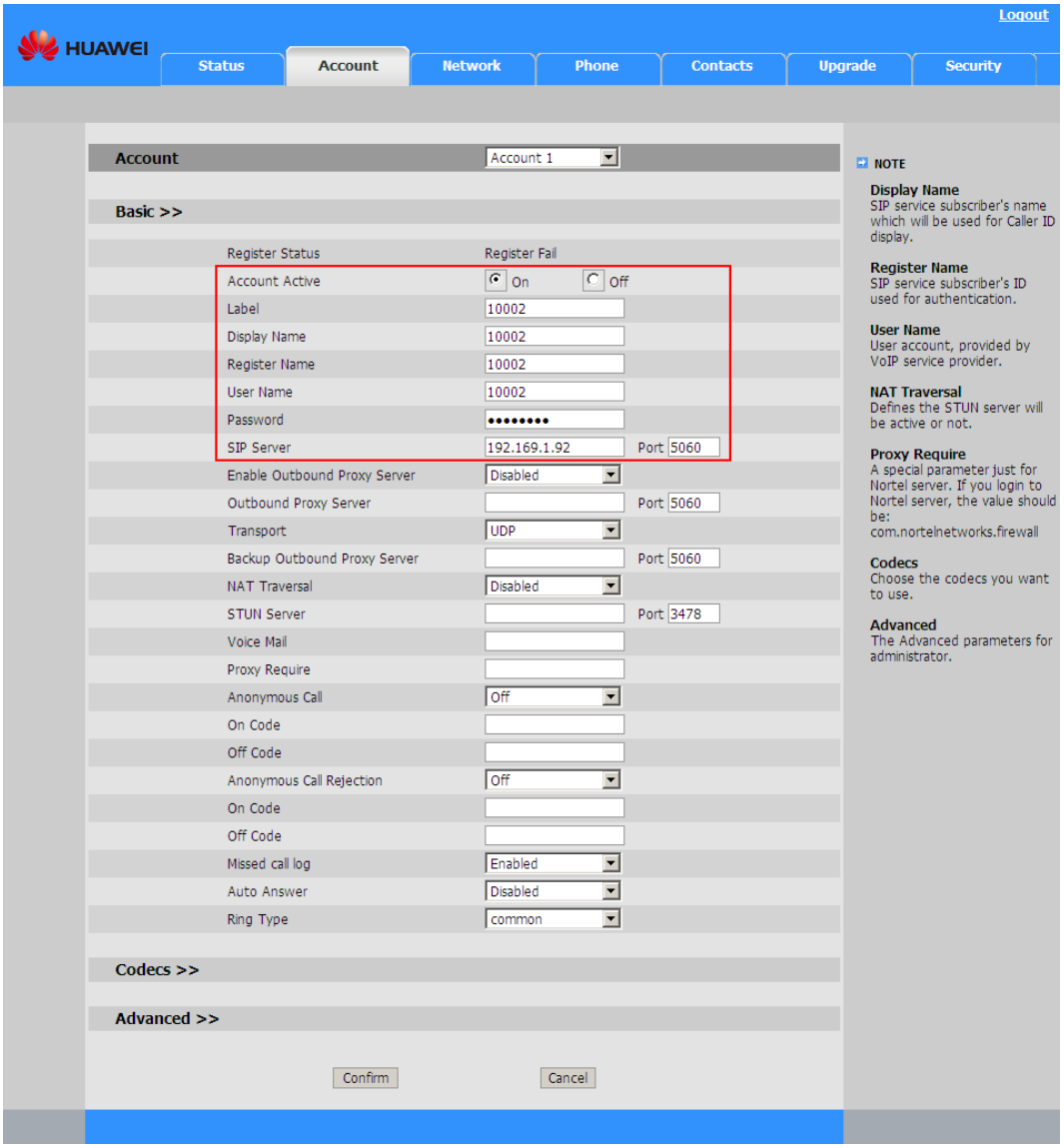
Phone Configuration

Assume that the account 10002 for listening on other accounts has been configured on the SIP server. After configuring the SIP server, proceed as follows to configure the BLF function for an IP phone:

1. Register the account 10002.

   Click the **Account** tab and set basic account parameters in the **Basic** area, as shown in Figure 2-24.

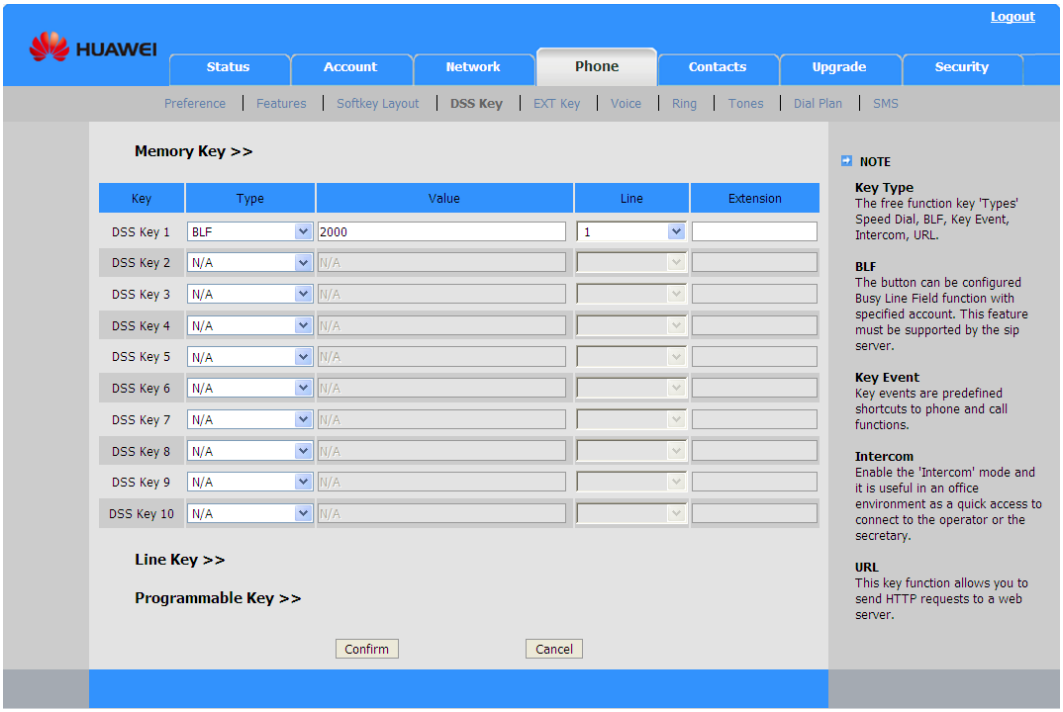
Figure 2-24 Setting basic account parameters



2. Set the type of a DSS key to **BLF**.

   A memory key, a line key, and an expansion key can be assigned the BLF function. The following describes how to set a memory key as a BLF key.

Figure 2-25 Setting a memory key as a BLF key



Access the web configuration page, click the **Phone** tab, and click **DSS Key**. Set a memory key under **Memory Key**. To set a memory key for eSpace 7870, click the **DSS Key** tab and click **Memory Key**.

- Set **Type** to **BLF**.
- Set **Value** to the listened-on account.
- Set **Line** to the line that the account 10002 registers, for example, **1**.
- Set **Extension** to the call pickup function code specified on the SIP server.

3. Click **Confirm** to save settings.

Indicator Status Monitoring

- When the listened-on account is in the idle state, press the BLF key to make a call to the listened-on account.
- When the listened-on account is in the ringing state, press the BLF key to pick up the call for the account.

Table 2-28 describes the mapping among the indicator type, indicator status, and account status.

Table 2-28 Mapping among the indicator type, indicator status, and account status

Indicator Type	Indicator Status	Account Status
Line Key assigned with the BLF function	Steady green	The listened-on account is in the idle state.
	Blinking green slowly	The listened-on account is in the talking state.

Indicator Type	Indicator Status	Account Status
	Blinking green quickly	The listened-on account is in the ringing state.
	Off	The BLF function is disabled.
Memory Key assigned the BLF function	Steady green	The listened-on account is in the idle state.
	Steady red	The listened-on account is in the talking state.
	Blinking red	The listened-on account is in the ringing state.
	Off	The BLF function is disabled.

2.4.7 Configuring the SCA Function

Function Description

The share call appearance (SCA) function allows one account to be used by multiple phones. Users can monitor the account status on each phone. The function is mainly applied to the secretary service.

After the manager and secretary service is enabled, a line of a manager can be bound to a line of the manager's secretary. When the manager's phone has an incoming call, the secretary's phone rings, and the indicator for the corresponding line of the manager blinks. After answering the call, the secretary can dial the manager's private phone number to forward the call to the manager.

A manager can be bound to a maximum of two secretaries, and a secretary can be bound to a maximum of four managers. The line that is bound with the manager and secretary service must be a shared line.

The following describes the manager and secretary service in the situation that a manager and a secretary are involved.

Prerequisites

- Two lines have been configured for the manager's phone.
  - Configured as an external line, line 1 is used by external users to call the manager and is bound to the secretary's phone. Line 2 is configured as a private line and is used by the secretary to call the manager.
  - If the manager needs to be configured with two secretaries, at least three lines must be configured for the manager's phone. Two of them are bound to two secretaries' phones, and one is configured as a private line.
- Line 1 has been configured for the secretary's phone.
  - The line 1 is bound to the manager's phone. Line 2 is configured as a private line and is used to call the manager.

  - When a secretary serves four managers, at least five lines must be configured for the secretary's phone. Four of them are bound to the external number of each manager, and one is configured as a private line.
- The manager and secretary service has been configured for both the manager's line1 and the secretary's line1. For details, see the *eSpace U19xx Unified Gateway Product Documentation*.

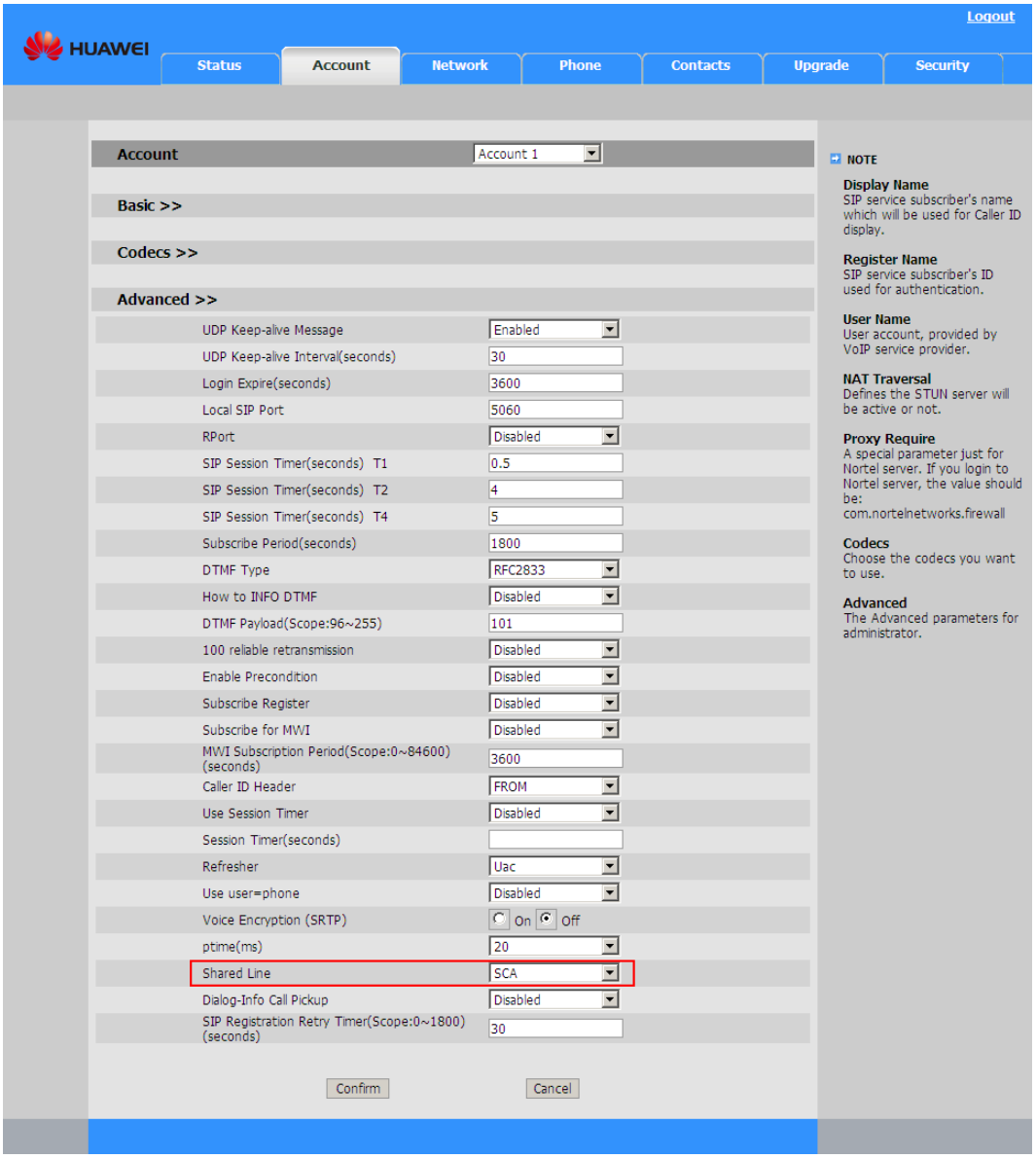
Phone Configuration

The following procedure configures a manager account on the IP phone. The procedure for configuring a secretary account is similar.

1. Access the web configuration page of the IP phone.
2. Set line 1 as the shared line.

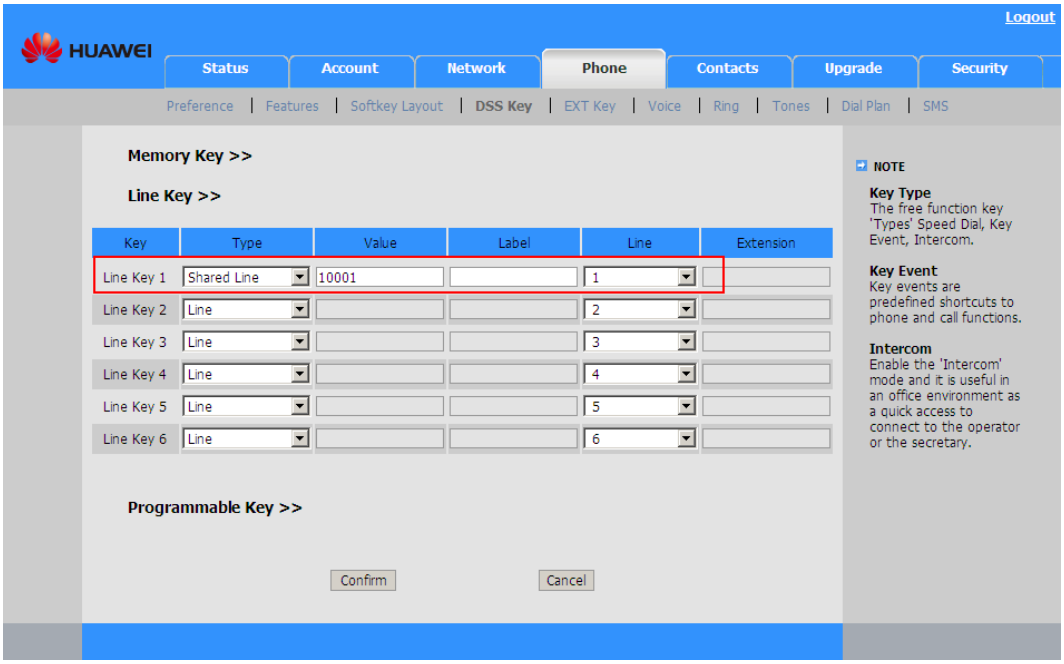
   Click the **Account** tab, and set **Shared Line** to **SCA** in the **Advanced** area, as shown in Figure 2-26.

Figure 2-26 Setting Shared Line



3. Click **Confirm** to save settings.
4. Click the **Phone** tab. Click **DSS Key** and set **Line Key 1** in the **Line Key** area, as shown in Figure 2-27.
   - Set **Type** to **Shared Line**.
   - Set **Value** to the account number of line 1.
   - Set **Line** to **1**.

Figure 2-27 Setting Line Key 1



5. Click **Confirm** to save settings.

2.4.8 Configuring the XML Browser

Function Description

The XML browser is developed for eSpace 7850, 7830 and 7820 based on XML and HTTP/HTTPS service. The XML browser can be used to browse only the XML files that are generated based on specific syntax by using tools such as PHP and JavaScript. HTTP or HTTPS is used to download the files to the IP phone.

The XML browser enables users to use customized services such as weather report, stocks query, date query, address book, Google, news viewing, music playing, and terminal configuring.

XML File Type

The XML browser supports the following XML files:

- TextMenu: menu item list in text format. For example, on the news main page, select a menu item to link to the corresponding news.
- TextScreen: text page, for example, a page for viewing news.
- InputScreen: input page, for example, a page for registering an account.
- Directory: page for downloading address books.
- Execute: page prompting an IP phone to run a command, for example, restart command or call making command.
- Status: page that displays the IP phone status dynamically, for example, the DND service status and call forwarding status.
- Configuration: file for setting IP phone parameters.

For details on the parameters in the seven types of XML files, see 7.8 XML Files Supported by the XML Browser. The seven types template of XML files are delivered with the software version and are available at http://enterprise.huawei.com/en/support/.

NOTE

You must apply for permission to download XML file from the website. If you need to download the XML file, contact system or service providers.

The path is **Software Downloads** > **Unified Communication** > **IP Phone** > **Version (For example, IP Phone V100R001C02)** > **software**.

Server Configuration

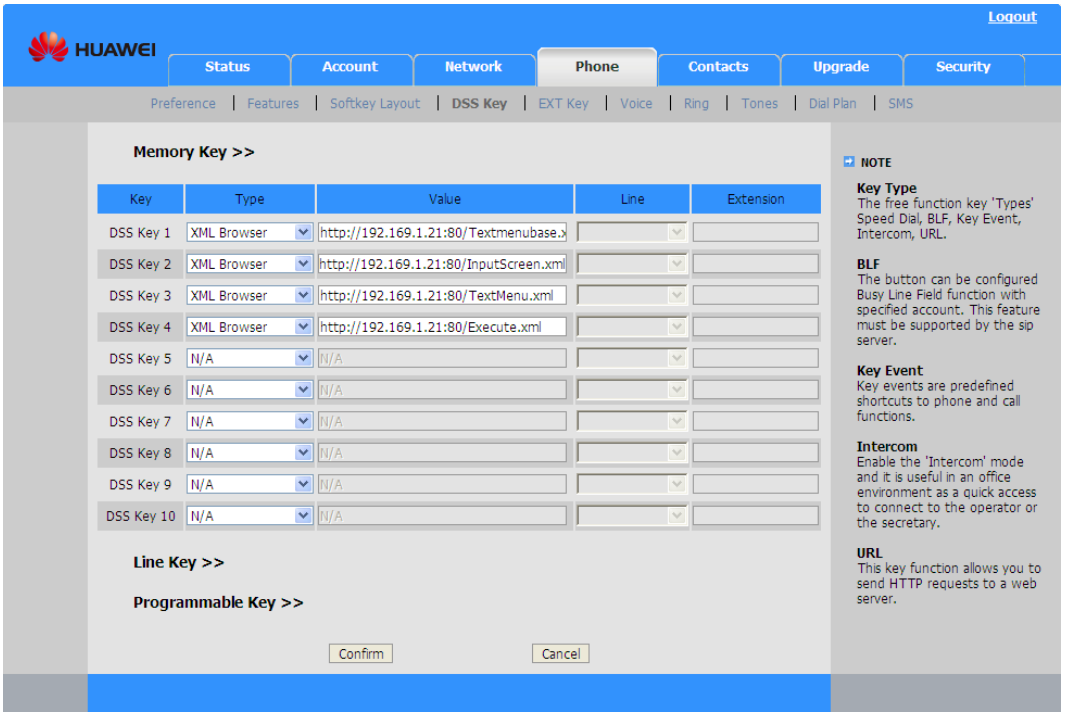
HTTP and HTTPS can be used to download files for the XML browser. For details on how to configure the HTTP server, see 7.2 Setting Up the HTTP Server.

Phone Configuration

To assign the XML browser function to a DSS key, for example, a memory key, proceed as follows:

1. Click **DSS Key** on the web configuration page.
2. Under **Memory Key**, select **XML Browser** from the **Type** drop-down list box, and enter an XML address in the **Value** text box.

Figure 2-28 Setting a DSS key type to XML browser



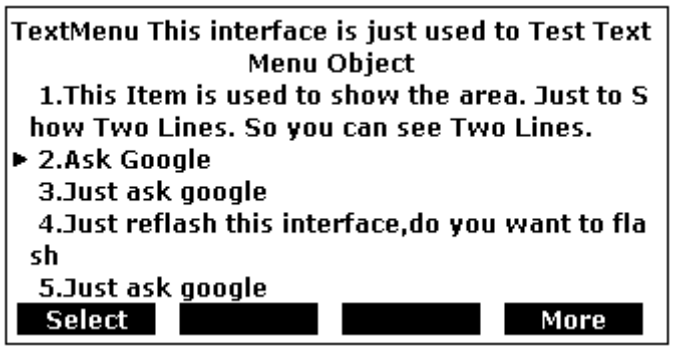
3. Click **Confirm**.

Basic Operations

1. When an IP phone is in the standby state, press a DSS key of the XML browser type.
2. After the page shown in Figure 2-29 is displayed, press the **Select** soft key to access the corresponding link address.

   You can press the **More** soft key to perform other operations such as dialing a number or enabling the DND service. The available operations are defined in the XML file on the server.

Figure 2-29 XML browser page



2.4.9 Customizing the Phone Desktop (for eSpace 7870 Only)

Function Description

Users can customize desktop background and layout for their IP phones in an XML file. To use the customized desktop background and layout, users need only to upload this file. The XML file configures the following information:

- Whether to display the following items on the desktop and their positions:
  - Clock: time
  - Date: date
  - State: icons indicating the current account and missed calls
  - Icon: icons indicating the DND, auto answer, voice message, and call transfer functions
- Whether to display soft key icons on the desktop

  The positions of soft key icons are fixed and cannot be changed.
- Wallpaper

Each account can customize its own desktop. After an account switches to another account, the customized desktop changes accordingly. When the desktop customization function is disabled for an account, the default desktop is displayed on the main GUI.

CAUTION

The customized desktop is applicable only to the main GUI of an IP phone. Other GUIs such as the menu and call interfaces are displayed in their default styles.

XML File Generation

Use the following tool to generate an XML file. Huawei technical support will notify you of any update on this tool promptly.

Log in to http://enterprise.huawei.com/en/support/ to download XMLIdleScreen.exe.

NOTE

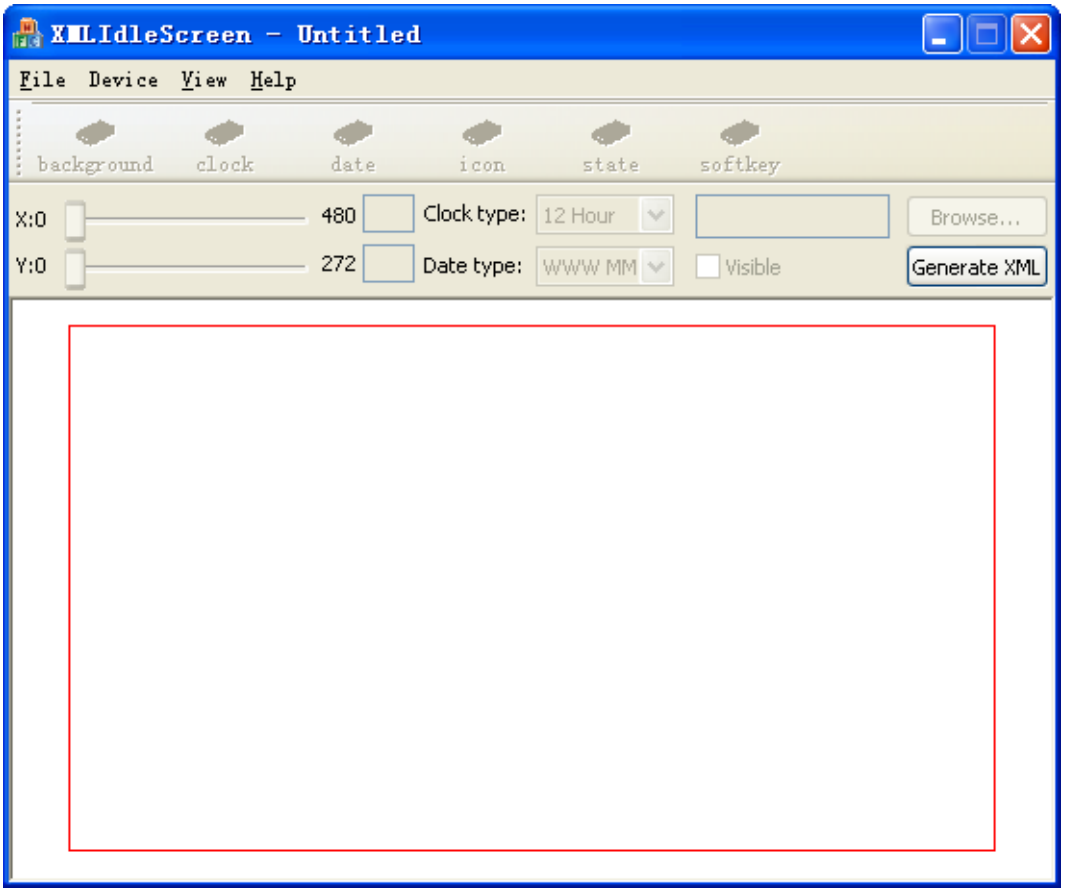
You must apply for permission to download XMLIdleScreen.exe from the website. If you need to download the tool, contact system or service providers.

The path is **Software Downloads** > **Unified Communication** > **IP Phone** > **Version (For example, IP Phone V100R001C02)** > **tools**.

1. Run **XMLIdleScreen.exe**.

   The main page is displayed, as shown in Figure 2-30.

Figure 2-30 Main page



2. Choose **File** > **New**, and create a file, as shown in Figure 2-31.

Figure 2-31 Creating an XML file

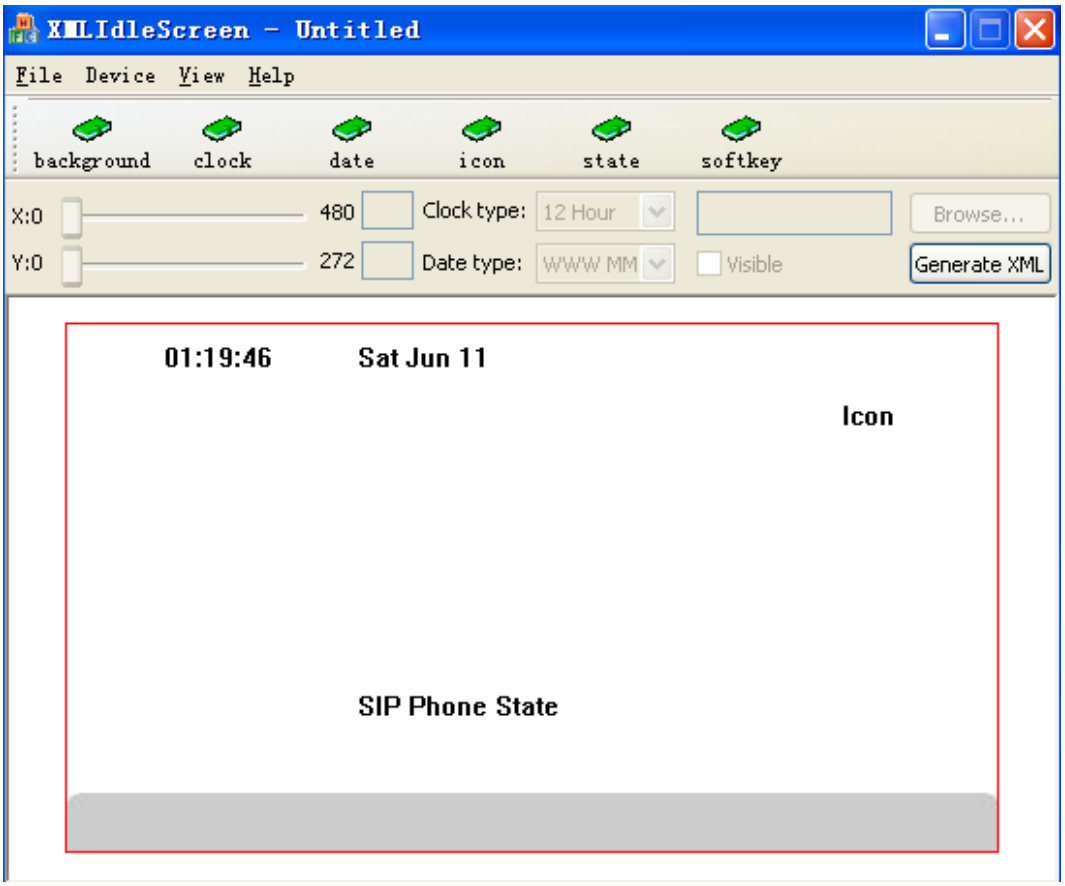
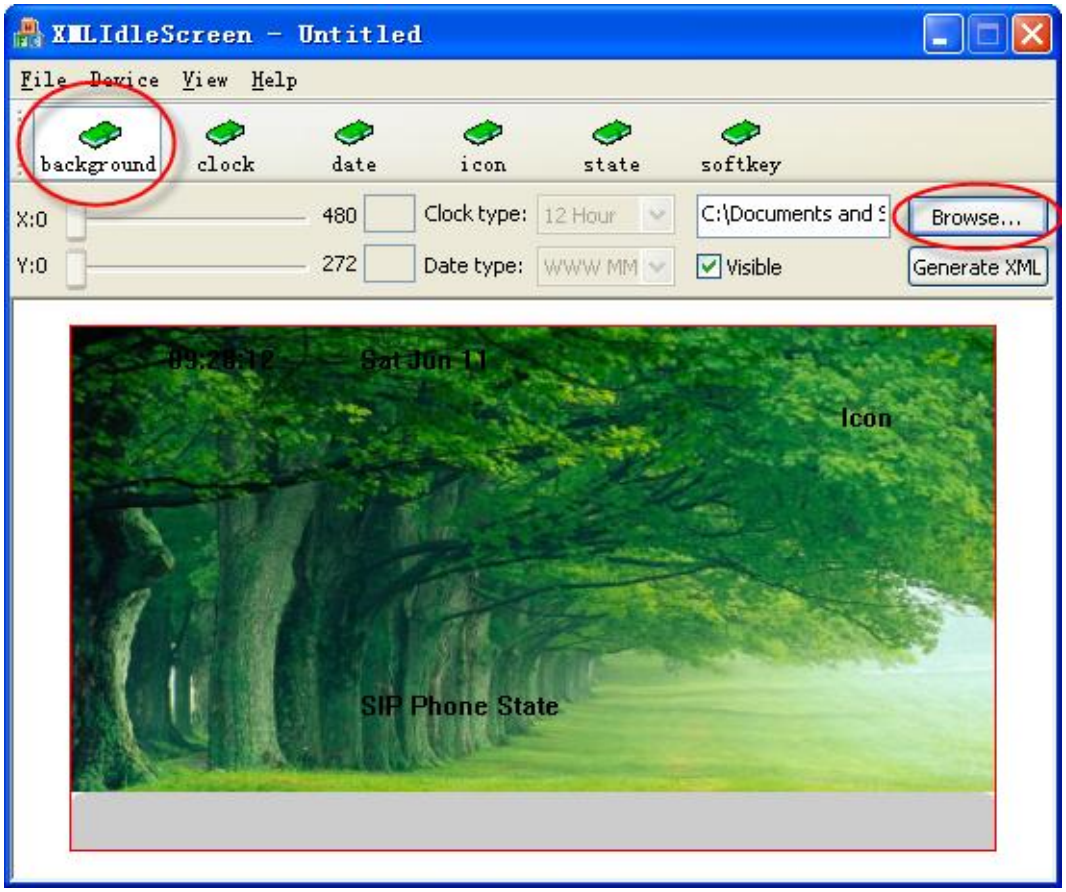


Figure 2-31 shows the default position of each item on the phone main GUI.

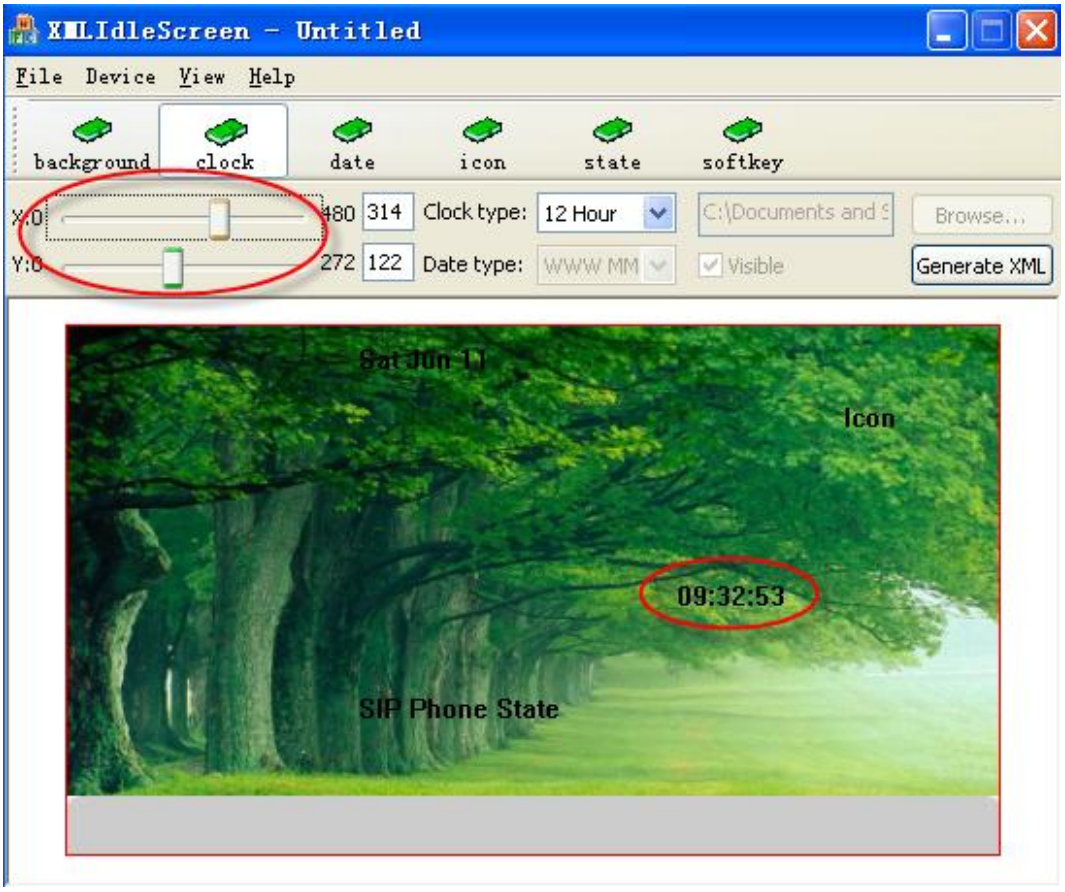
3. Click **background**, and click **Browse** to select a wallpaper, as shown in Figure 2-32.

Figure 2-32 Configuring a wallpaper



4. Click **clock**, and drag the sliders on the X and Y coordinates to adjust the time position, as shown in Figure 2-33.

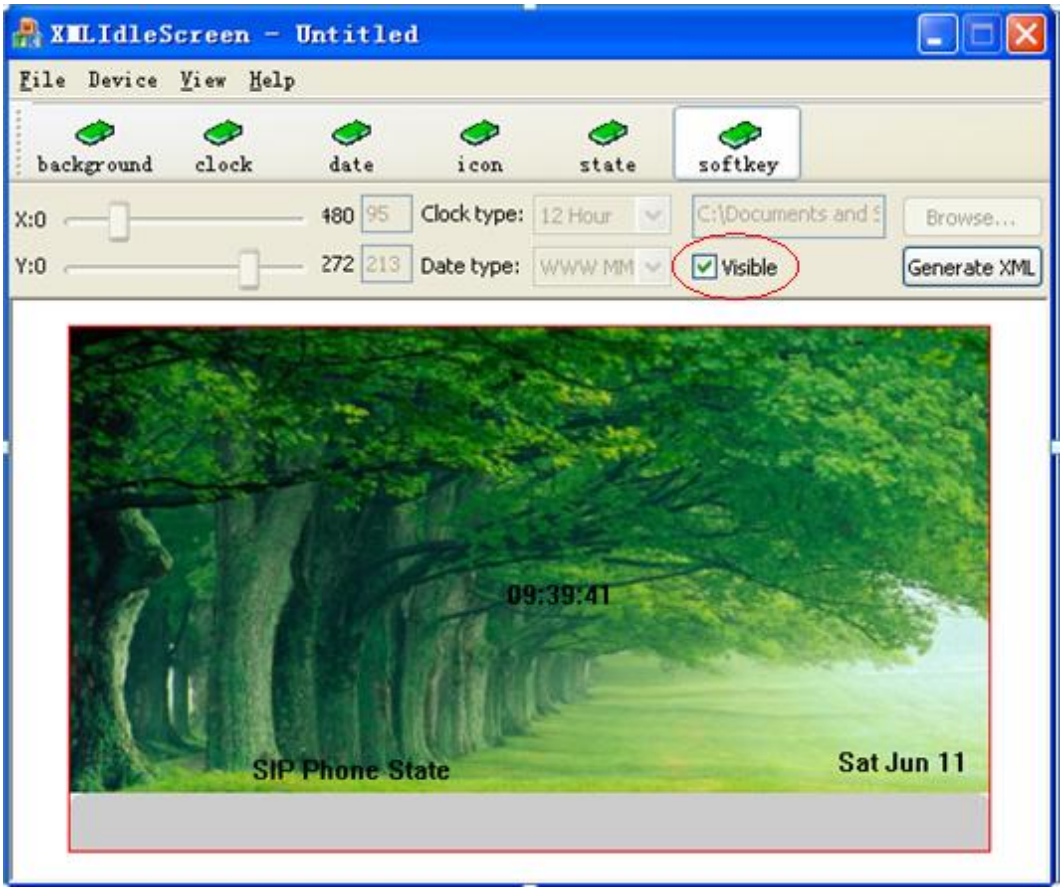
Figure 2-33 Setting the time position



The methods of setting the date, status, and icons are similar.

5. Click **softkey**, and select the **Visible** check box, as shown in Figure 2-34.
   After the **Visible** check box is selected, soft key icons will be displayed on the desktop.

Figure 2-34 Determining whether to display soft key icons

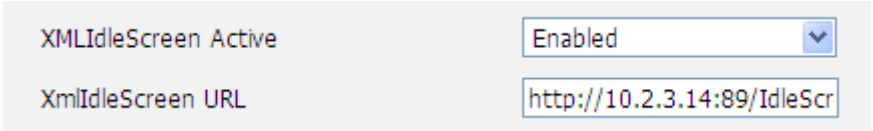


6. Click **Generate Xml**, and select a path for storing the file.

Phone Configuration

1. Access the web configuration page and click the **Account** tab. In the **Basic** area, select and enable the account that requires a customized desktop.
2. Set **XMLIdleScreen Active** to **Enabled**, as shown in Figure 2-35.

Figure 2-35 Setting XMLIdleScreen Active



3. Upload the new XML file to the SIP server using HTTP, HTTPS, TFTP, or FTP.

   For details on how to configure the SIP server, see 7.1 Configuring the TFTP Server (3CDaemon TFTP Server for Example) and 7.2 Setting Up the HTTP Server.
4. Set **XmlIdleScreen URL** and click **Confirm**.

Application Scenario

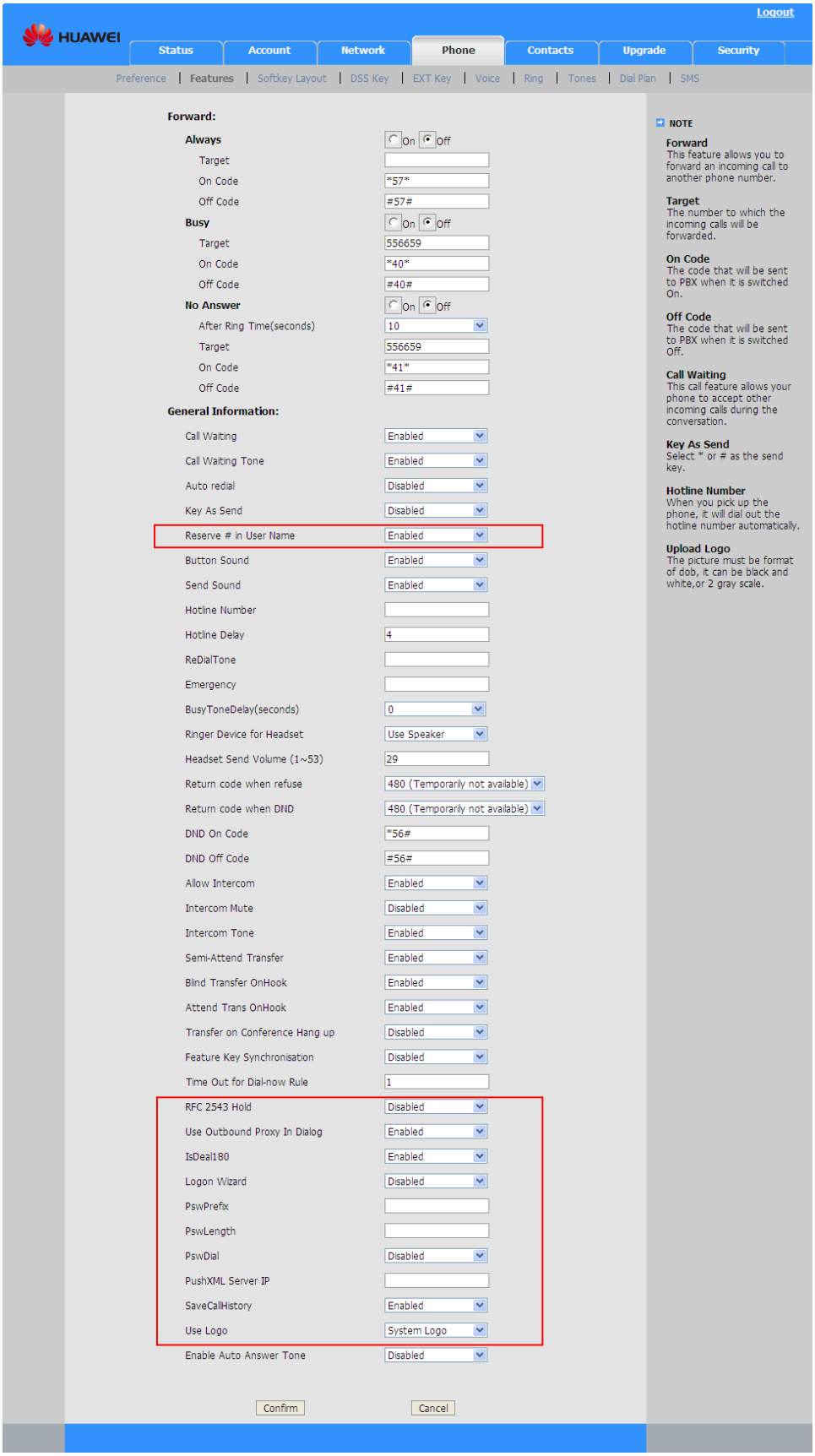
After the desktop is customized and the desktop customization function is enabled for an account, the IP phone will automatically download the XML file from the URL specified by **XmlIdelScreen URL**.

If multiple accounts have customized desktops, press the left and right arrow keys to switch accounts to display the corresponding desktop. If an account has no customized desktop or has disabled the desktop customization function, the default desktop is displayed on the main GUI.

2.4.10 Advanced Functions

On the web configuration page, click the **Phone** tab, and click **Features** to set advanced functions, as shown in Figure 2-36.

Figure 2-36 Setting advanced functions



The parameters framed in red in Figure 2-36 are not described in the *Huawei IP Phone eSpace 78XX User Manual*. Table 2-29lists the parameters.

Table 2-29 Parameters for advanced functions

Parameter	Description
Reserve # in User Name	If this parameter is set to **Enabled**, the number sign (#) in an account name will be converted into %23.
RFC 2543 Hold	The call hold function supports both RFC 2543 and RFC 3261. If this parameter is set to **Disabled**, RFC 3261 is used.
Use Outbound Proxy	If this parameter is set to **Enabled**, information exchanged between the calling and called parties is transferred through the outbound proxy server.
IsDeal180	If this parameter is set to **Enabled**, the SIP server will handle a 180 message following a 183 message.
Logon Wizard	If this parameter is set to **Enabled**, an IP phone will automatically enter the account setting GUI at startup when no account has been registered. This parameter is unavailable to eSpace 7870.
PswPrefix	If **PswDial** is set to **Enabled**, the N (specified by **PswLength**) digits dialed following xxx (specified by **PswPrefix**) are displayed as asterisks (*). This parameter is unavailable to eSpace 7870.
PswLength	
PswDial	
PushXML Server IP	IP address of the XML server from which an IP phone receives XML files. The XML files must be of the format supported by the XML Browser. For details, see 7.8 XML Files Supported by the XML Browser. This parameter is unavailable to eSpace 7870 and 7810.
SaveCallHistory	If this parameter is set to **Disabled**, no call history is saved.

2.5 Contacts Configuration

2.5.1 Configuring the Remote Phone Book

Function Description

In addition to local phone books on IP phones, enterprises usually publish public address books, which are maintained and updated on the SIP server or IP PBX. The function of accessing remote phone books must be enabled for IP phones to download the latest public address book. eSpace 7870, 7850, 7830 and 7820 can download and search for remote phone books and save contact information to the local phone book.

Remote Address Book URL

The URL for a remote address book must be linked to an XML address book and must be in either of the following formats:

- Common URL format: http://<host:port>/[folder name]/phonebook name.xml
- PHP format: http://<host:port>/[folder name]/search.php?[IP_ADDR=#IP][&MAC_ADDR=#MAC][&NAME=#SEARCH]

NOTE
The fields in the square brackets are optional.

The server determines the content of the data file to be sent based on the parameters in a PHP URL, and therefore the obtained data file is also an XML file.

The fields in a PHP URL are described as follows:

- IP_ADDR=#IP

  Replace #**IP** with an IP address. The server verifies whether the IP address has the right to download XML address books.
- MAC_ADDR=#MAC

  Replace #**MAC** with a MAC address. The server verifies whether the MAC address has the right to download XML address books.
- NAME=#SEARCH

  Replace #**SEARCH** with a contact name. The server searches for the contact name and records the search result into an XML file. Then the server sends the file to the IP phone. If the URL contains this field, the IP phone regards that the server has the search function.

Downloading a Remote Phone book

To download a remote phone book, proceed as follows:

1. Prepare an XML file.

   Remote phone books are classified into contact XML files and menu XML files. You can use UltraEdit to edit XML files.

   The three .xml files are delivered with the software version and are available at http://enterprise.huawei.com/en/support/.

   NOTE
   You must apply for permission to download XML file from the website. If you need to download the XML file , contact system or service providers.

   The path is **Software Downloads** > **Unified Communication** > **IP Phone** > **Version (For example, IP Phone V100R001C02)** > **software**.

   NOTE
   - The attachments are only examples. Add XML files and modify them as required.
   - The IP phone downloads the **Menu.xml** file first, and then downloads the **PC.xml** and **Tester.xml** files based on the URLs in the **Menu.xml** file.
2. Configure the server.

   FTP, TFTP, HTTP, and HTTPS can be used to download remote phone books. This document describes how to use HTTP to download remote phone books. For details on how to configure the HTTP server, see 7.2 Setting Up the HTTP Server.
3. Set parameters related to the remote phone book on the IP phone's web page.

To set parameters related to the remote phone book on the IP phone's web page, proceed as follows:

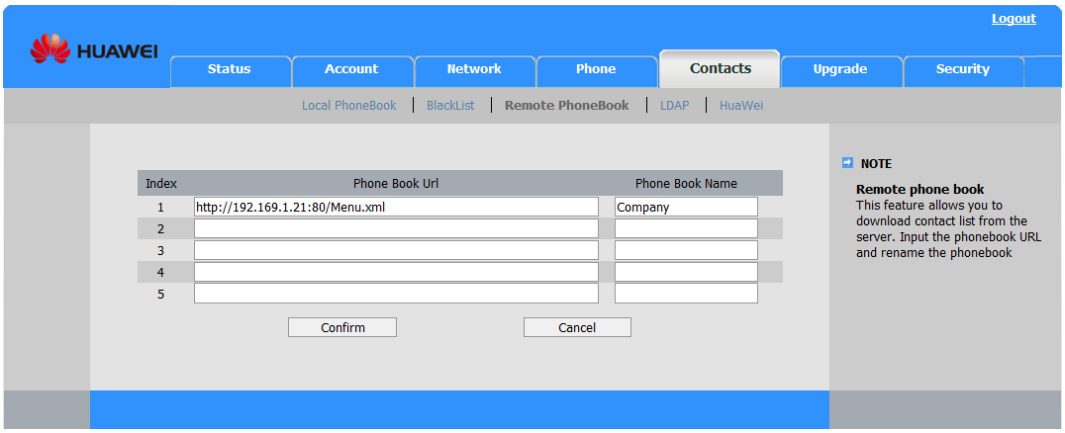
a. Log in to the IP phone's web page.

b. Click the **Contacts** tab, and click **Remote PhoneBook**. Set **Phone Book Url** and **Phone Book Name**, as shown in Figure 2-37.

c. The **Phone Book Url** parameter indicates the URL for downloading the file, for example,**http://192.169.1.21:80/Menu.xml**. The **Phone Book Name** parameter indicates the name to be displayed on the IP phone's LCD. You can set **Phone Book Name** to any value, for example, **Company**.

A total of five remote phone books are supported by eSpace 7870, 7850, 7830 and 7820.

Figure 2-37 Setting remote phone books



d. Click **Confirm**.

4. View the remote phone book on the IP phone.

a. Press the **Directory** soft key when the IP phone is in the standby state.

The **[Directory]** page is displayed.

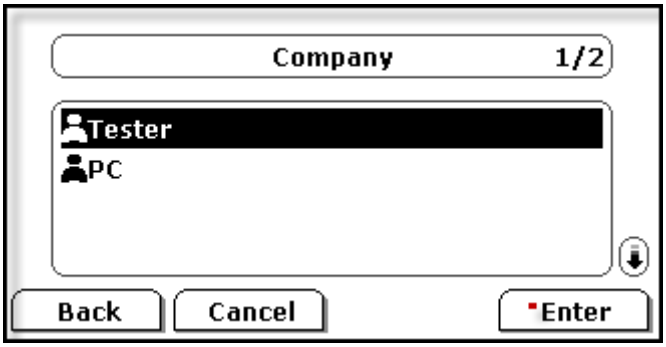
b. Press the number key **3**.

You can view **Company** on the **[Remote Group]** page that is displayed.

c. Press the **Enter** key.

The contact page is displayed, as shown in Figure 2-38.

Figure 2-38 Contact page



d. Press the up arrow key or down arrow key to select **Tester** or **PC**.

e. Press the **Enter** key.

The contacts in the group are listed.

Searching a Remote Phone book

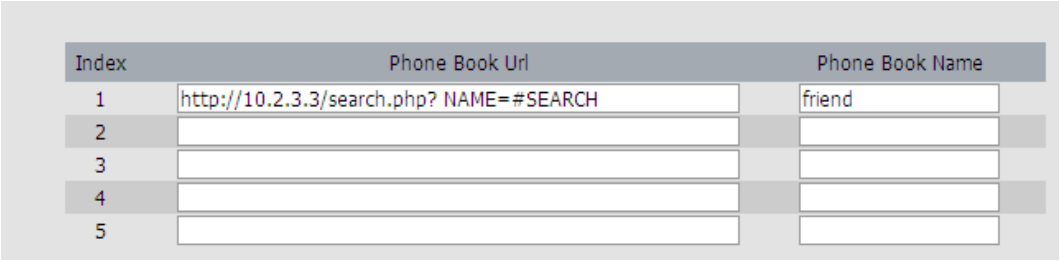
Enter the URL with the search function under **Phone Book URL**, as shown in Figure 2-39.

http://<host:port>/search.php?NAME=#SEARCH

NOTE

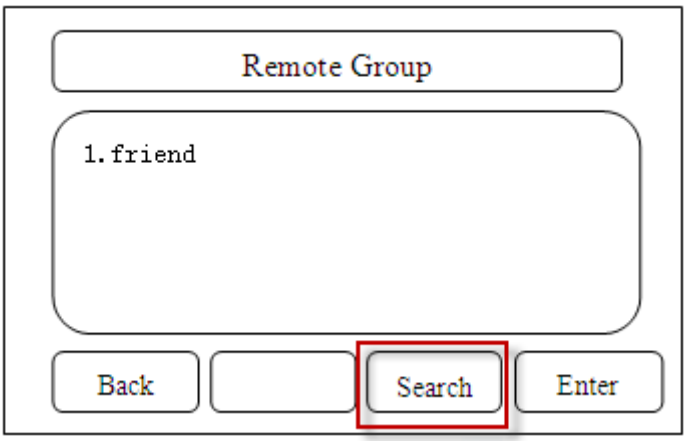
HTTP servers do not support PHP URLs and therefore cannot function as a search server. To implement the search function, install the AppServ on a server.

Figure 2-39 Setting the search function for remote phone books



After the URL with the search function is set, you can find the **Search** button on the remote phone book page, as shown in Figure 2-40.

Figure 2-40 Searching a remote phone book



Press the **Search** soft key to search for contacts.

Configuration File

Table 2-30 eSpace 7850, 7830, 7820 and 7810 parameters in the configuration file for remote phone books

Section Header and Path	Parameters	Permitted Values	Description
[RemotePhoneBook 0] path = /config/Setting/Setting.cfg	URL	Character string	URL for the first remote address book, which must be in XML format. Example: http://10.2.3.3/phonebook/friend.xml The parameter is left blank by default.
	Name	Character string	Name of the first remote address book. The parameter is left blank by default.
Parameters for the other four remote addresses are the same as those for the first one. The only difference is the numbers in the headers. The header for the second remote address book is **[RemotePhoneBook1]**, the header for the third remote address book is **[RemotePhoneBook2]**, and the header for the nth remote address book is **[RemotePhoneBook(n-1)]**.			

Table 2-31 eSpace 7870 parameters in the configuration file for remote address books

Section Header and Path	Parameters	Permitted Values	Description
[cfg:/phone/config/user.ini,reboot=0]	RemotePhoneBook0.URL	Character string	URL for the first remote address book, which must be in XML format. Example: http://192.168.0.231/vin/phonebook1.xml The parameter is left blank by default.
	RemotePhoneBook0.Name	Character string	Name of the first remote address book. The parameter is left blank by default.
Parameters for the other four remote addresses are the same as those for the first one. The only difference is the numbers in the headers. The header for the second remote address book is **[RemotePhoneBook1]**, the header for the third remote address book is **[RemotePhoneBook2]**, and the header for the nth remote address book is **[RemotePhoneBook(n-1)]**.			

2.5.2 Configuring LDAP

Function Description

Based on X.500, the Lightweight Directory Access Protocol (LDAP) is an application protocol for reading and editing directories over an IP network. LDAP supports TCP/IP.

For example, in a tree structure, the root is the company name, the company contains departments, and a department contains employees. The IP phone can search for contacts based on specific rules. For example, the IP phone searches for contacts whose department names contain J.

eSpace 7870, 7850, 7830 and 7820 that support LDAP provide the following functions:

- Search for contacts.

  After a user presses the LDAP DSS key and enters a number or letter, the IP phone searches the LDAP server for contacts based on a specific rule and displays the search result on the LCD. The user then can select a contact and initiate a call, or add the contact to the local address book or blacklist.
- Display the calling party's name.

After receiving a call, the IP phone searches the local address book for the calling number. If no record is found, the IP phone searches the LDAP server for the contact and displays the search result on the IP phone's LCD.

- Search for the number that a user dials.

  Each time a user presses a number key, the IP phone searches the LDAP server for the matching number. If records are found, the IP phone displays the records on the LCD. Then the user can select a contact to make a call.

Web Configuration

Before using the lightweight directory access protocol (LDAP) directory, you must first set up the LDAP server(For example, Windows 2003 Server active directory (AD)). For details about how to install and set up the Windows 2003 Server AD, see 7.6 Using Windows 2003 Server AD.

Table 2-32 lists common LDAP attributes for eSpace 7870, 7850, 7830 and 7820.

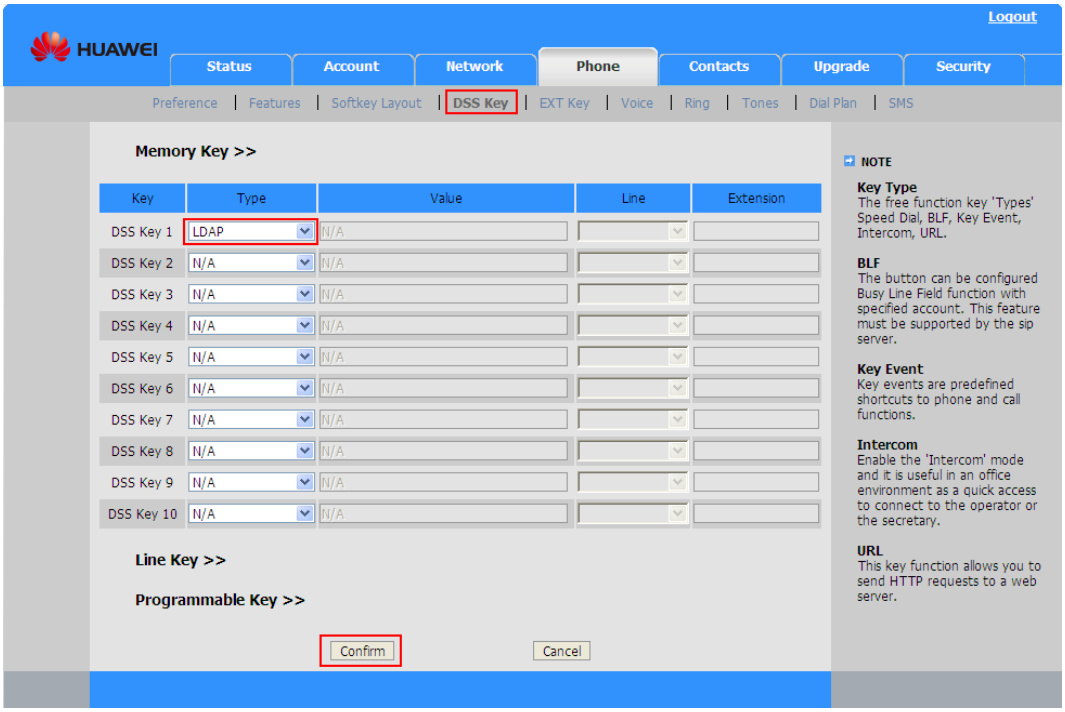
Table 2-32 Common LDAP attributes

Attribute	Full Name	Description
cn	Common Name	Attributes in the character string for connecting an IP phone to a server to implement the LDAP function. The character string is in the format ldap://servername/DN, in which DN contains cn, ou, and dc. For example, cn=test,ou=developer,dc=domainname,dc=com indicates that the test object is in the developer unit in the domainname.com domain. The value of cn must be unique. The LDAP directory is similar to the file system directory, for example, dc=Redmond,dc=wa,dc=Microsoft,dc=com, which is similar to com\Microsoft\wa\ Redmond in the file system.
ou	Organizational Unit Name	
dc	Domain Component	
o	Organization Name	Organization name.
sn	Surname	Family name.
gn	Given Name	First name.

To use LDAP function, prepare the server environment first. (For example, the Windows 2003 Server AD is installed and contacts are added to the server.)Then set parameters on the IP phone's web page as follows:

1. Access the web configuration page.
2. Click the **Phone** tab, and click **DSS Key**. Select a memory key or a line key, and select **LDAP** from **Type**, as shown in Figure 2-41.

Figure 2-41 Assigning LDAP to a DSS key



3. Click **Confirm**.
4. Click the **Contacts** tab, and click **LDAP**.
5. Set LDAP parameters, as shown in Figure 2-42.

Figure 2-42 Setting LDAP parameters

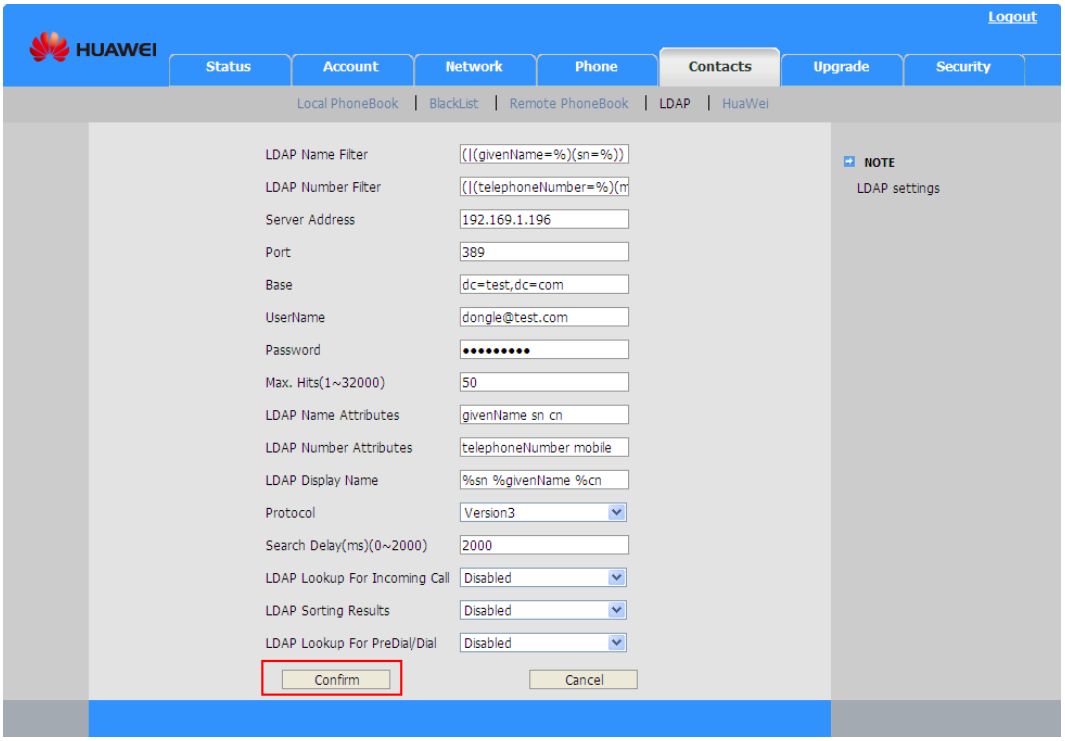


Table 2-33 lists parameters in the LDAP area.

6. Click **Confirm**.
7. Then presses the LDAP DSS key and enters a number or letter, the IP phone searches the LDAP server (the Windows 2003 Server AD) for contacts based on a specific rule and displays the search result on the LCD.

Table 2-33 Parameters for configuring LDAP

Parameter	Description	Example
LDAP Name Filter	Name filter. After you enter a name, the IP phone uses the name filter to search the LDAP server for the contact. The settings for the name filter must be based on RFC 2254. The entered names will replace % in the name filter. Examples are as follows: • (|(cn=%)(sn=%)) The LDAP server sends the IP phone the records with cn or sn starting with the characters dialed by a user. • (!(cn=%)) The LDAP server does not send the IP phone the records with cn or sn starting with the characters dialed by a user.	(|(givenName=%)(sn=%))

Parameter	Description	Example
LDAP Number Filter	Number filter. After you enter a number, the IP phone uses the number filter to search the LDAP server for the contact. The settings for the number filter must be based on RFC 2254. The entered numbers will replace % in the number filter. Examples are as follows: • (|(telephoneNumber=%)(Mobile=%)(ipPhone=%)) The LDAP server sends the IP phone the records with telephoneNumber, Mobile, or ipPhone starting with the characters dialed by a user. • (&(telephoneNumber=%)(sn=%)) The LDAP server does not send the IP phone the records with telephoneNumber or sn starting with the characters dialed by a user.	(|(telephoneNumber=%)(mobile=%))
Server Address	IP address or domain name of the LDAP server. Examples are as follows: • 192.168.1.100 • lday.company.com	IP address of the LDAP server (The Windows 2003 Server AD).
Port	Port number of the LDAP server. Default value: 389	389
Base	Root directory that the IP phone searches. For example, if the value is dc=Redmond,dc=wa, the root directory is wa\Redmond.	dc=test,dc=com
UserName	User name for logging in to the LDAP server. If the LDAP server allows anonymous visitors to access, leave the parameter blank; otherwise, set UserName and Password to the values set by the LDAP server administrator. For example: cn=manager,dc=company,dc=cn.	dongle@test.com An existing user name in the Windows 2003 Server AD.
Password	Password for logging in to the LDAP server. The password is set by the LDAP server administrator.	Huawei123
Max.Hits(1~32000)	Maximum number of records in the search result. If the number of records found in the LDAP server is larger than the setting, the server sends records (total number: Max.Hits) to the IP phone. The server sends all records in the search result to the IP phone if this parameter is left blank. The factory setting is 50. NOTE If excessive contact records are found, the search speed is slow. Set the parameter based on the	50

Parameter	Description	Example
	network bandwidth.	
LDAP Name Attributes	LDAP name attributes. The search result that the LDAP server sends to the IP phone must contain these name attributes. Examples are as follows: • cn sn displayName The search result that the LDAP server sends to the IP phone must contain the cn, sn, and displayName attributes. • givenName The search result that the LDAP server sends to the IP phone must contain the givenName attribute. • vorName nachName The search result that the LDAP server sends to the IP phone must contain the vorName and nachName attributes.	givenName sn cn
LDAP Number Attributes	LDAP number attributes. The search result that the LDAP server sends to the IP phone must contain these number attributes. Examples are as follows: • Mobile telephoneNumber ipPhone The search result that the LDAP server sends to the IP phone must contain the Mobile, telephoneNumber, and ipPhone attributes. • Home Private Office The search result that the LDAP server sends to the IP phone must contain the Home, Private, and Office attributes.	telephoneNumber mobile
LDAP Display Name	Attributes whose information is displayed on the IP phone's LCD. Example: %cn %sn The example indicates that the values of cn and sn are displayed on the IP phone's LCD.	%sn %givenName %cn
Protocol	Protocol version. The options are Version2 and Version3. The protocol version selected on the IP phone must be the same as the parameter setting.	Version3
Search Delay(ms)(0~2000)	Search delay period. A delay period later than the search operation, the IP phone displays the search results on the LCD. Unit: millisecond	2000
LDAP Lookup For	The value Enabled indicates that the IP phone searches the LDAP server for the calling number and displays the calling party's name on the LCD. The	Disabled

Parameter	Description	Example
Incoming Call	value Disabled indicates that the IP phone does not search the LDAP server for the calling number.	
LDAP Sorting Results	The value Enabled indicates that the IP phone sorts records that are found by display name (or by number if only numbers are contained in the search result). The value Disabled indicates that the IP phone does not sort records that are found.	Disabled
LDAP Lookup For PreDial/ Dial	The value Enabled indicates that the IP phone searches the LDAP server for the characters that a user dials.	Disabled

2.6 TLS/SSL Authentication

Function Description

Transport Layer Security (TLS) and its predecessor, **Secure Sockets Layer (SSL)**, are cryptographic protocols that provide communications security over the Internet. TLS and SSL encrypt the segments of network connections above the transport layer, using cryptography for privacy and a keyed message authentication code for message reliability. TLS is used to encapsulate specific application protocols such as HTTP, FTP, SMTP, NNTP, and XMPP. For details about TLS and SSL, visit the website http://en.wikipedia.org/wiki/SSL_certificate#TLS_version_1.1.

TLS/SSL authentication is used in the following scenarios:

- An IP phone uses HTTPS to perform automatic provision, during which the IP phone functions as a client.
- When a user uses HTTPS to access an IP phone's web page, the IP phone functions as a server.

Encryption Algorithm

Encrypted transmission occurs when data sender uses the encryption key to encrypt information and then sends the encrypted information to the recipient. The data recipient uses the decryption key to decrypt the information and reads the information. Two common encryption algorithms are described as follows:

- Symmetric-key algorithm: The encryption key is trivially related to the decryption key, in that they may be identical or there is a simple transformation to go between the two keys.
- Asymmetric-key algorithm: This algorithm involves a public key and a private key. If the public key is used for encryption, only the corresponding private key can be used for decryption; if the private key is used for encryption, only the corresponding public key can be used for decryption.

TLS/SSL Communication Principle

The process for TLS/SSL communication is as follows:

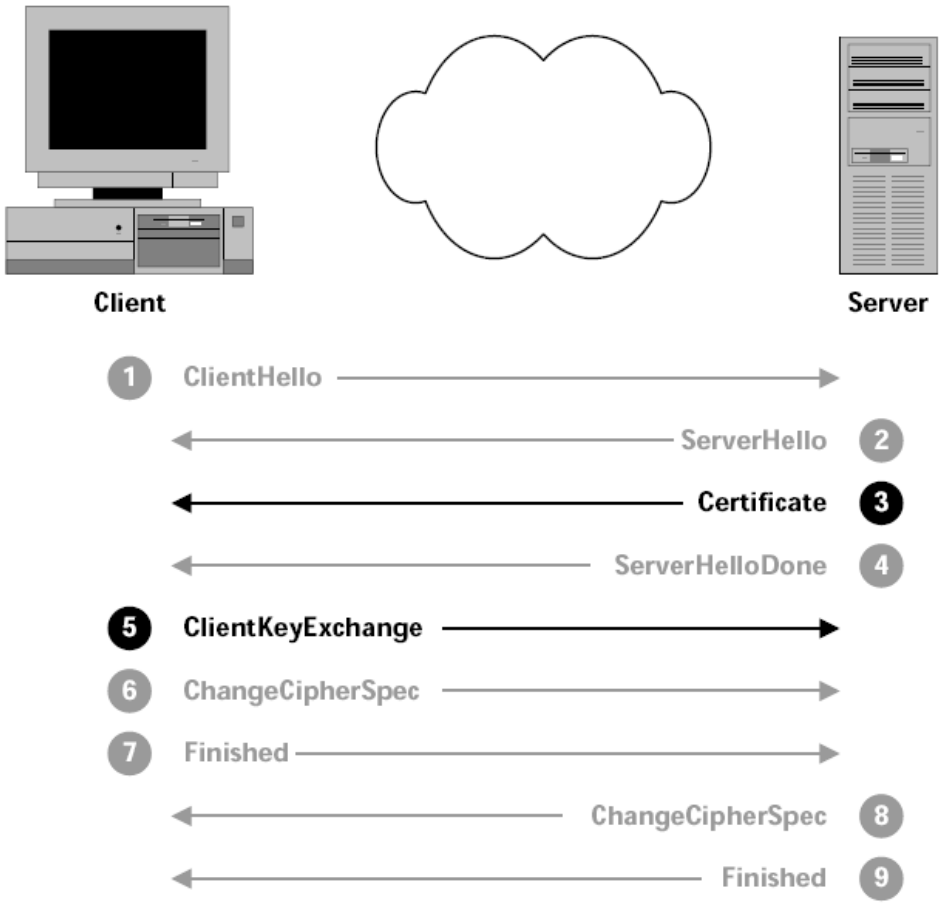
1. The client and the server use the asymmetric encryption algorithm to negotiate a session key. The sender generates a symmetric session key and uses the public key to encrypt the session key. Then the sender sends the encrypted information to the recipient.
2. The recipient uses the private key to decrypt the session key.
3. The sender uses the session key to encrypt a file and sends the encrypted file to the recipient.
4. The recipient uses the session key to decrypt the file into a plain text.

The file transmission is secure because only the private key of the recipient can be used for decrypting the session key.

Communication Process

After the TLS/SSL connection is set up, data can be transmitted securely. Figure 2-43 shows the transmission process.

Figure 2-43 TLS/SSL data transmission process



1. The client sends a ClientHello request to the server, asking to set up a connection. The request contains the encryption methods supported by the client for negotiation.
2. The server sends a ServerHello message back to negotiate an encryption method and sends a trusted certificate to the client. The certificate contains the public key of the server.
3. If the client trusts the server, the client sends the server the session key that is encrypted by the public key of the server. The client also asks the server to use the session key for file encryption and transmission.
4. The server receives the information from the client and uses the session key to encrypt all of the information that will be sent to the client.

An IP phone functions as a client

When an IP phone initiates an SSL connection, the IP phone functions as a client. Generally, the client uses the authentication certificate to determine whether the server is reliable, for example, when an IP phone is automatically upgraded in HTTPS mode. To configure the auto provision function, click the **Security** tab, and click **Trusted Certificates**, as shown in Figure 2-44.

Figure 2-44 Configuring the auto provision function

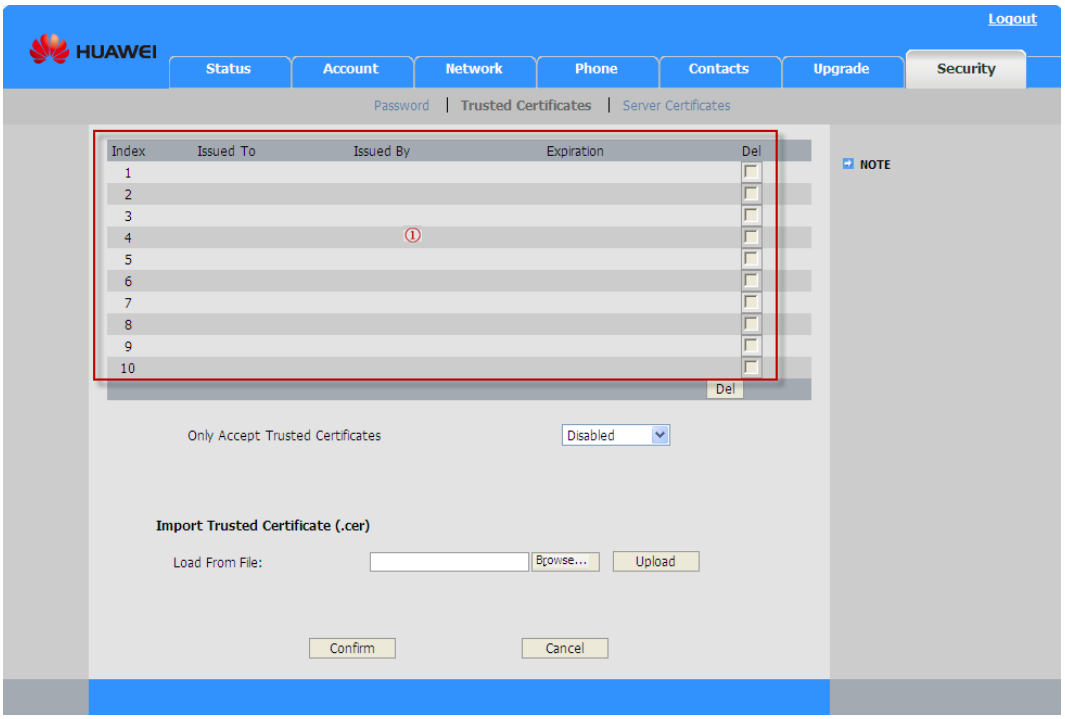


Table 2-34 ists parameters for configuring the auto provision function.

Table 2-34 Parameters for configuring the auto provision function

Parameter	Description
Area	Root certificate list imported to an IP phone.
Only Accept Trusted	Indicates whether to enable the trust connection.

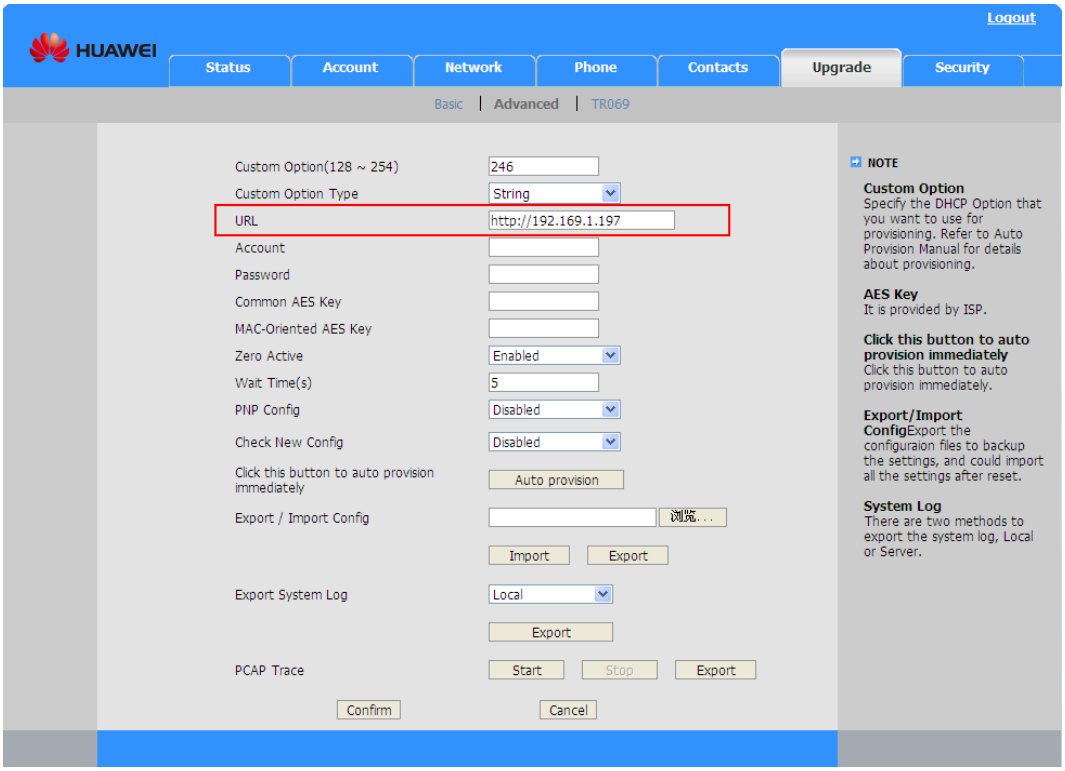
Parameter	Description
Certificate	If **Enabled** is selected, the imported root certification is used to authenticate the signature in the server certificate. If the authentication fails, the IP phone stops communicating with the server. If **Disabled** is selected, the IP phone always communicates with the server even if the trusted certificate does not exist or is incorrect.
Import Trusted Certificate	Click **Browse** under **Import Trusted Certificate**, select a certificate file, and click **Upload** to import the root certificate.

To configure the auto provision function, proceed as follows:

1. Configure an HTTPS server and provide the IP phone user with a root certificate.
2. Access the web configuration page, click the **Security** tab, and click **Trusted Certificates**.
3. Select **Enabled** from the **Only Accept Trusted Certificate** drop-down list box.
4. Click **Browse** under **Import Trusted Certificate**, select a certificate file, and click **Upload** to import the root certificate.
5. In the **Advanced** area on the **Upgrade** tab page, set **URL** to a value starting with https://, as shown in Figure 2-45.

   To configure the auto provision function for eSpace 7870, click the **Phone** tab and click **Auto Provision**.

Figure 2-45 Setting URL for HTTPS auto provision function



The IP phone uses HTTPS to communicate with the server and uses the imported root certificate to authenticate the server. If the server can be authenticated, the IP phone uses HTTPS to download files.

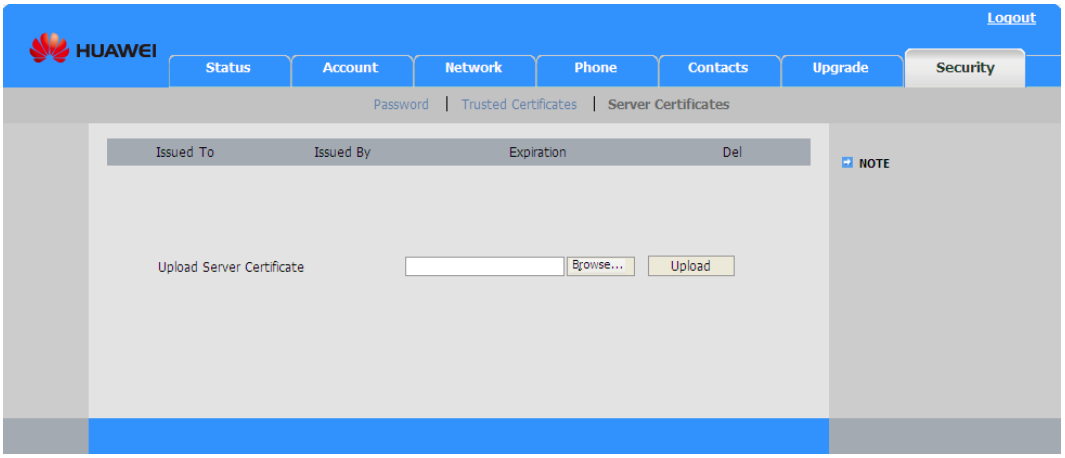
NOTE

For details about the auto provision function, see 3 Batch Configuration and Upgrade of IP Phones.

An IP phone functions as a server

When a user uses HTTPS to access an IP phone's web page, the IP phone functions as a server. During communication, the IP phone sends trusted certificate to the browser. You can upload a trusted certificate in the **Server Certificates** area on the **Security** tab page, as shown in Figure 2-46.

Figure 2-46 Uploading a trusted certificate



An IP phone is authenticated as a client

Generally, the client verifies whether the server is reliable. In some cases, the server verifies whether the client is reliable, which is determined by the server configurations. When an IP phone is connected to an HTTPS server, the IP phone sends its client certificate to the server. The client certificate is uploaded in the **Server Certificates** area on the **Security** tab page.

2.7 Upgrade and Restore

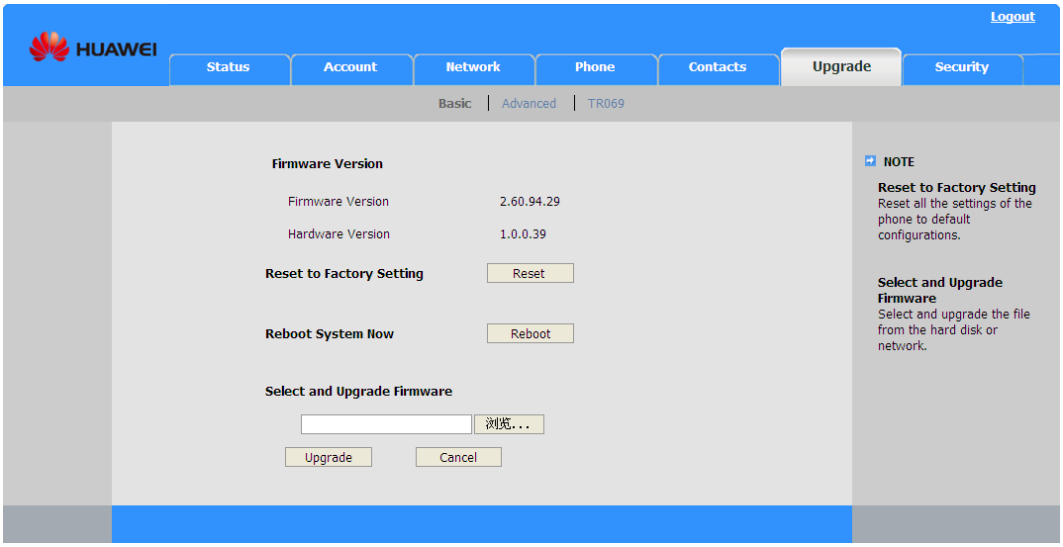
CAUTION

Do not power off an IP phone during the upgrade. Otherwise, writing to the flash memory fails and the IP phone is down. If the IP phone is down, perform the emergent recovery or deliver the IP phone to the factory for repairing.

2.7.1 Upgrading an IP Phone Manually

You can manually upgrade an IP phone on the web page shown in Figure 2-47.

Figure 2-47 Upgrading an IP phone manually



1. In the **Basic** area on the **Upgrade** tab page, click **Browse** under **Select and Upgrade Firmware**, and select the software to be upgraded.

   To upgrade eSpace 7870, click the **Phone** tab and click **Upgrade**.
2. Click **Upgrade**.

   The IP phone starts to upgrade. After the upgrade finishes, the IP phone automatically restarts.
3. Verify that the setting of **Firmware Version** on the **Status** tab page is the target version number.

After the phone restarts, access the web configuration page, and verify that the value of **Firmware Version** on the **Status** tab page is updated.

2.7.2 Configuring the TR069 Protocol

An IP phone can be connected to the eSpace EMS by using the TR069 protocol, as shown in Figure 2-48. Table 2-35 describes the TR069 parameters.

Figure 2-48 Configuring the TR069 parameters

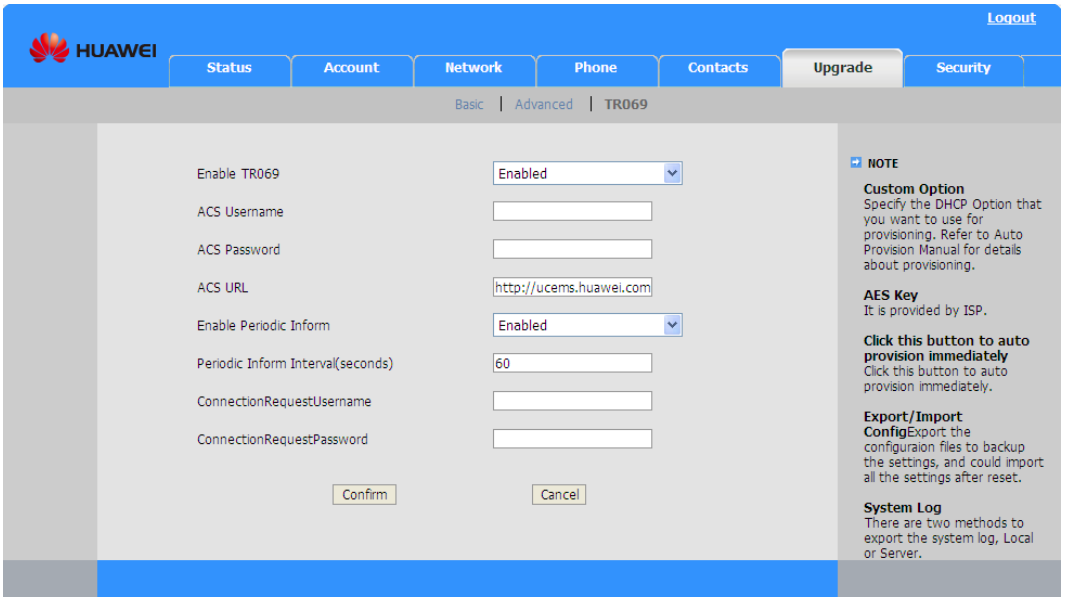


Table 2-35 Parameter description

Parameter	Description
Enable TR069	• If this parameter is set to **Enabled**, the IP phone sends a session connection request to the ACS. To make the TR069 settings take effect, the ACS must be enabled. • If this parameter is set to **Disabled**, the IP phone does not send a session connection request to the ACS. Default value: **Enabled**
ACS Username	User name for authenticating a TR069 IP phone when the IP phone attempts to connect to the ACS. The user name must be the same as that configured on the ACS.
ACS Password	Password for authenticating a TR069 IP phone when the client attempts to connect to the ACS. The password must be the same as that configured on the ACS.
ACS URL	This parameter is mandatory when TR069 is enabled. Set ACS URL. The URL can be in either of the following formats: • IP address: For example: http://10.10.10.1:8080 • Domain name: For example: http://huawei.acs.com:8080 8080 is the port number of the ACS.
Enable Periodic Inform	If this parameter is set to **Enabled**, the IP phone sends the session connection request to the ACS periodically.
Periodic Inform	Interval for initiating sessions to the ACS.

Parameter	Description
Interval (seconds)	
ConnectionRequest Username	User name for authenticating the ACS when the ACS attempts to connect to a phone. The user name must be the same as that configured on the ACS.
ConnectionRequest Password	Password for authenticating the ACS when a phone attempts to connect to ACS. The password must be the same as that configured on the ACS.

2.7.3 Automatically Upgrading IP Phones

This topic describes how to automatically upgrade IP phones on the web page.

Prerequisites

- eSpace IP phones are automatically upgraded using a loaded configuration file, such as 7850.cfg. Therefore, you must first create a configuration file to be loaded. For details about how to create a configuration file, see 3.2 Making Configuration File Templates.
- Save the configuration file to the automatic upgrade server.

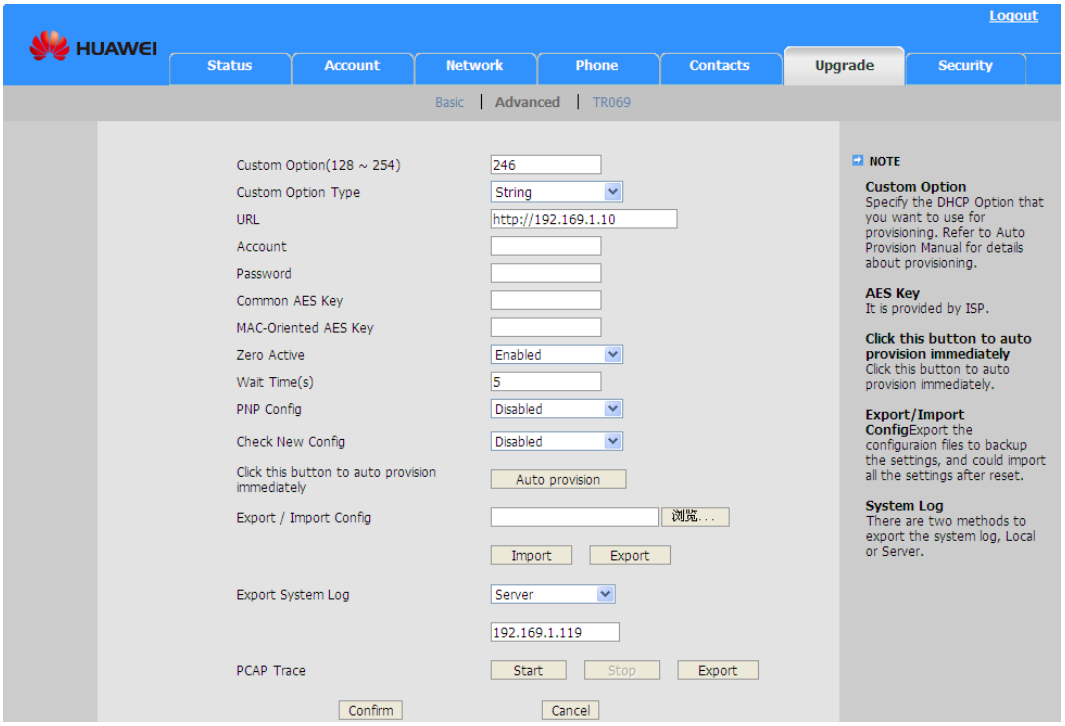
  For example, if the Apache server is the automatic upgrade server, save the configuration file to the **C:\Program Files\Apache Software Foundation\Apache2.2\htdocs** directory on the Apache server. For details, see 7.2.2 Using the Apache Server.

Procedure

Step 1 Choose **Upgrade** > **Advanced**, as shown in Figure 2-49.

NOTE
To upgrade eSpace 7870 IP phones, choose **Phone** > **Auto Provision**.

Figure 2-49 Configuring the automatic upgrade



Step 2 Table 2-36 describes mandatory parameters **URL** and **Check New Config**.

Table 2-36 Automatic upgrade parameters

Parameter	Description
Custom Option(128 ~ 254)	Enter the option used for DHCP upgrade. Default value: **246**.
Custom Option Type	Server address type, including **String** and **IP Address**.
URL	Domain name or IP address of the automatic upgrade server.
Account	FTP server account for FTP upgrade.
Password	FTP server password for FTP upgrade.
Common AES Key	Public key for loading the upgrade file encrypted by the public encryption library.
MAC-Oriented AES Key	MAC key for loading the upgrade file encrypted by using MAC addresses.
Zero Active	Configures network parameters during the automatic upgrade. Default value: **Enabled**
Wait Time (s)	Time for automatically upgrading configurations. Default value: **5**

Parameter	Description
PNP Config	If this parameter is set to **Enabled**, once the IP phone is powered on, the IP phone will automatically upgrade the configurations. Default value: **Disabled**
Check New Config	If this parameter is set to **Enabled**, the IP phone is automatically upgraded by detecting the latest version. Default value: **Disabled**
Click this button to auto provision immediately	If a new version is detected, click **Auto provision** to upgrade the IP phone immediately.
Export / Import Config	Imports or exports the configuration files of IP phones.
Export System Log	• Select **Local** and click **Export**. The system logs of the IP phone are exported to a local disk. • Select **Server** and enter the server IP address. The IP phone exports the system logs to the server.
PCAP Trace	Click **Start** to capture IP phone packets. A maximum of 500 KB data packets can be stored.

----End

Result

Follow-up Procedure The **Check New Config** mode determines the time when an eSpace IP phone automatically upgrades configurations. For example, if the mode for checking new firmware is **Repeatedly**, and the interval is 10 minutes, the eSpace IP phone downloads the configuration file every 10 minutes to upgrade configurations.

2.7.4 Firmware-based Restore

Function Description

If exceptions occur during firmware upgrade, the upgrade fails, and devices cannot be started. In this case, send the devices to the manufacturer to for repairing. This function is provided for administrators who are responsible for maintenance.

CAUTION

This function is implemented in BootLoad on an IP phone, but BootLoad cannot be upgraded. Therefore, this function is supported only when the original version of the bin file is A.40.C.D (for example, 2.60.94.2) or a later version. If the original version of the bin file is A.30.C.D or an earlier version, the IP phone does not support this function, and only manufacturer engineers can repair it.

This section is applicable to eSpace 7870, 7850, 7830, 7820 and 7810. If eSpace 7870 fails to be upgraded, power it off and on. An IP address will be displayed on the LCD at startup. Use this IP address to access the web configuration page and upgrade the phone again.

Prerequisites

Before using the firmware to restore software, prepare the following items:

- Computer where the TFTP server is installed.

  For details on how to set up the TFTP server environment, see 7.1 Configuring the TFTP Server (3CDaemon TFTP Server for Example).

  Verify that the phone IP address and the computer IP address are on the same network segment.
- Firmware file for restoring software.

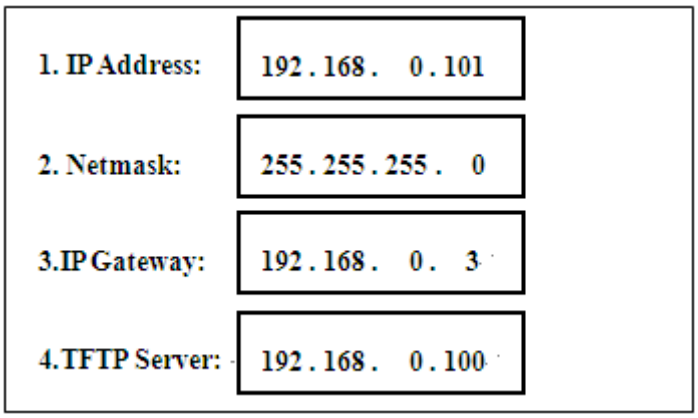
Upgrade Procedure

1. Connect the computer to a LAN and set the IP address to a proper value, for example, **192.168.0.100**.
2. Copy the firmware file to the TFTP server path (for example, C:/TFTP) specified in the **Upload/Download** area, and rename the file based on the phone model.
   - To upgrade eSpace 7850, rename the file to **t28.rom**.
   - To upgrade eSpace 7830, rename the file to **t26.rom**.
   - To upgrade eSpace 7820, rename the file to **t22.rom**.
   - To upgrade eSpace 7810, rename the file to **t20.rom**.
3. Use the network cable to connect a faulty IP phone to the LAN.
4. Hold down the **SPK** key and power on the eSpace 7850.

   Three seconds later, the firmware restore page is displayed.

   Figure 2-50 shows the restore page for eSpace 7850.

Figure 2-50 Firmware restore page



5. Press numbers keys and arrow keys to set the IP address of the IP phone, for example, **192.168.0.101**.

Ensure that the IP address of the phone is in the same segment as the IP address of the computer.

6. Press the down arrow key.
7. Set **Netmask** and press the down arrow key.

   Set **IP Gateway** and press the down arrow key. Set **TFTP Server**. The value of TFTP Server is the IP address of the computer where the **TFTP server** is installed.
8. Press the **OK** key.

   The IP phone sends a request to the specified TFTP server, downloads the firmware file, and displays the following information:

   Updating Firmware.

   Do not Poweroff!!!

   The IP phone restarts automatically, and the following information is displayed on the LCD:

   System is booting.

   Please wait…
9. After the IP phone restarts, press the **OK** key. Access the **Status** page. View the firmware version and verify that the IP phone is upgraded to the software version on the TFTP server.

3 Batch Configuration and Upgrade of IP Phones

3.1 Overview

The global configuration file on the HTTP server is used to configure and upgrade IP phones in batches.

During DHCP server configuration, a 246 parameter is defined for setting the URL of the global configuration file. After this parameter is set, the DHCP server sends the URL to the IP phone that applies for an IP address. The IP phone then downloads the configuration file from this URL.

The configuration file contains the IP addresses of the servers where the firmware version file, ring tone files, and local address book files are stored.

The batch configuration and upgrade of IP phones have the following features:

- IP phones of the same model use the same configuration file.

  For example, you only need to prepare one configuration file for all eSpace 7850 phones.
- IP phones obtain the required firmware version file URL from the configuration file.

  After obtaining the global configuration file, IP phones download the firmware version file based on the URL in the configuration file for batch upgrade.
- IP phones obtain URLs from the configuration file to download ring tone files, local address book files, and other files.

3.2 Making Configuration File Templates

IP phones of the same model use the same configuration file. The configuration file name for each phone model is as follows:

- For eSpace 7810, the file name is **7810.cfg**.
- For eSpace 7820, the file name is **7820.cfg**.
- For eSpace 7830, the file name is **7830.cfg**.
- For eSpace 7850, the file name is **7850.cfg**.
- For eSpace 7870, the file name is **7870.cfg**.

3.2.1 Modifying Configuration File Templates

A global configuration file template is provided for deployment. When making a configuration file, modify parameter settings such as the IP address of the IP phone registration server and NTP address in the template to meet onsite requirements.

The global configuration file template is delivered with the software version and is available at http://enterprise.huawei.com/en/support/.

NOTE

You must apply for permission to download the global configuration file template from the website. If you need to download the file, contact system or service providers.

The path is **Software Downloads** > **Unified Communication** > **IP Phone** > **Version (For example, IP Phone V100R001C02)** > **software**.

NOTE

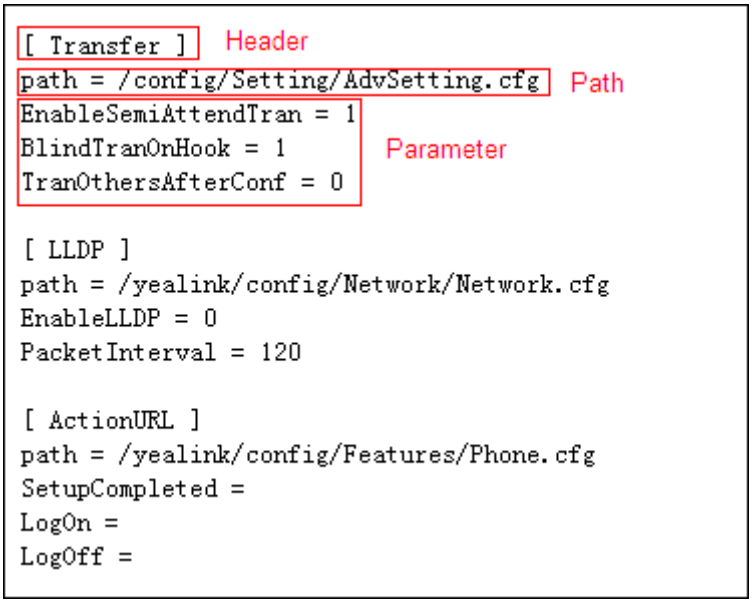
eSpace 7810, eSpace 7820, eSpace 7830, eSpace 7850 use the same configuration file. When loading the configuration file to a phone, change the name of the configuration file to the model name of the phone.

The configuration template is a .cfg file. Each section in the template consists of a header, a path, and several parameters.

Use the Wordpad to open the file template, and modify parameter settings.

Figure 3-1 shows the configuration file template.

Figure 3-1 Configuration file template



The attachment *eSpace 7810&7820&7830&7850 Configuration File Parameter Description* describes parameters in the configuration file for eSpace 7850, 7830, 7820 and 7810 is available at http://enterprise.huawei.com/en/.

The attachment *eSpace 7870 Configuration File Parameter Description* describes parameters in the configuration file for eSpace 7870 is available at http://enterprise.huawei.com/en/.

The path is **SUPP0RT** > **Documentation Center** > **UC&C** > **Unified Communications** > **IP Phones** > **Phone Model(For example, eSpace 7870)** > **Reference**.

3.2.2 Updating Files

The configuration file lists the files that an IP phone needs to update.

Updating the Firmware Version File

To update the firmware version file, you need to configure information about the server where the firmware version file is stored.

CAUTION

The following describes the **[firmware]** section in the configuration file for eSpace 7850, 7830, 7820 and 7810. For details about the **[firmware]** section for eSpace 7870, see the relevant configuration file.

The firmware information is specified by the following fields in the configuration file:

```
######################################################################
[ firmware ]
path = /tmp/download.cfg
server_type = http                    #Upgrade server type.
server_ip = 192.168.0.231             #IP address of the upgrade server.
server_port =                         #Port number of the upgrade server.
login_name =                          #User name for logging in to the upgrade server. This field
can be left blank if no user name is required for login. This field is usually set for FTP servers.
login_pswd =                          #Password for logging in to the upgrade server.
http_url = http://192.168.0.231/    #URL of the upgrade server. This field is mandatory only
when HTTP or HTTPS is used for upgrade.
firmware_name = 0.0.0.143.rom         #Firmware version number.
######################################################################
```

Downloading Ring Tones

The ring tone information is specified by the following fields in the configuration file:

```
######################################################################
[ ringtone ]
path = /tmp/download.cfg
server_address =        #Path for storing a ring tone file. The ring tone file must be in .wav
format, and the file size does not exceed 100 KB.
```

```
######################################################################
```

Updating the Local PhoneBook

The local PhoneBook information is specified by the following fields in the configuration file:

```
######################################################################
[ ContactList ]
path = /tmp/download.cfg
server_address =              #Path for storing a local address book.
######################################################################
```

CAUTION

- The file name of the local phone book must be **contactData1.xml**. If it is not, update will fail.
- The content format in the local phone book file is different from that in the remote phone book file. To configure a local phone book file, access the web configuration page, click the **Contacts** tab, and click **Local PhoneBook**. Click **Export XML** to export a local phone book file, and modify the file as required.

The template of local phone book file exported on the web configuration page is delivered with the software version and is available at http://enterprise.huawei.com/en/support/.

NOTE

You must apply for permission to download the template of local phone book file from the website. If you need to download the filel, contact system or service providers.

The path is **Software Downloads** > **Unified Communication** > **IP Phone** > **Version (For example, IP Phone V100R001C02)** > **software**.

3.3 Configuring and Upgrading IP Phones in Batches

CAUTION

Ensure the power supply of an IP phone during the upgrade. Otherwise, result in upgrade failed.

3.3.1 Preparations for Configuration and Upgrading IP Phones

To configure and upgrade IP phones in batches during the deployment, prepare the following items:

- Configuration file template

The configuration template is a .cfg file. You can change the parameter values in the template based on the site scenarios.

- File server

  The HTTP server is used. For details on how to set up the HTTP server environment, see 7.2 Setting Up the HTTP Server.

- DHCP server

  For details on how to set up the DHCP server environment, see 7.4 Setting Up the DHCP Server.

- DNS server

  A DNS server is required when you use domain names to configure the configuration file URL.

  For details on how to set up the DNS server environment, see 7.3 Guidelines for Setting Up the DNS Server.

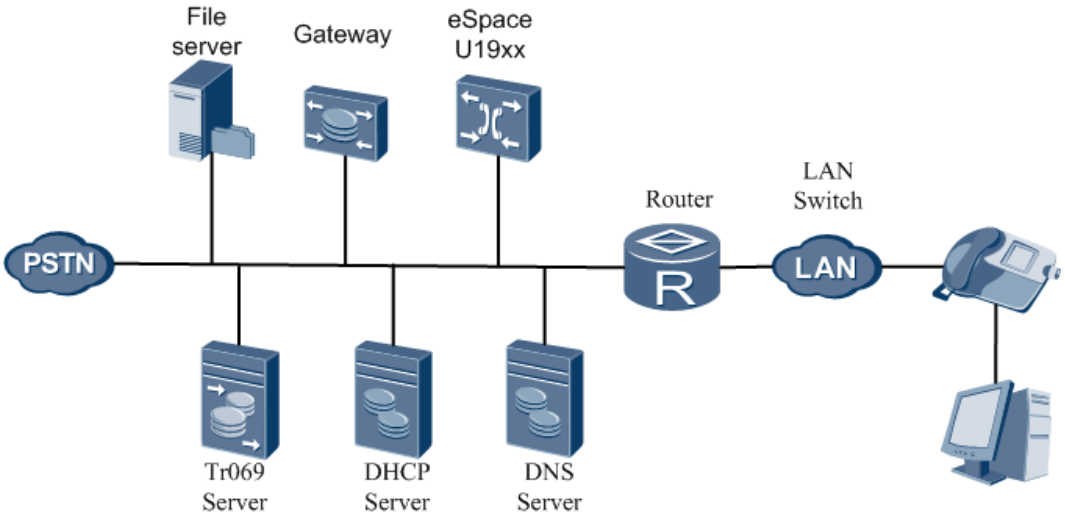
- Files that need to be updated

  Prepare the firmware version file, ring tone files, and local phone book files based on your site scenario.

Prepare the firmware version file, ring tone files, and local phone book files based on your site scenario.

Figure 3-2 shows the general network diagram for deployment.

Figure 3-2 Network diagram



3.3.2 Procedure for Configuring and Upgrading IP Phones in Batches

Procedure

1. Store the phone version files and configuration file in the HTTP server root directory.

   To load ring tones or local phone books, store the files in the HTTP server root directory, and set related parameters in the global configuration file.

2. Change the **Option246** parameter value of the DHCP server to the configuration file URL.7.5 Setting the Option246 Parameter document describes how to set the Option246 parameter.
   - The configuration file URL specified by the **Option246** parameter has the highest priority than other specified URLs.
   - It is optional to specify the configuration file name. The IP phone will automatically search for and download the configuration file mapping its model.

   Table 3-1 describes the **Option246** parameter settings.

Table 3-1 Option 246 parameter settings

Setting Format	Example
IP	http://**server IP**
IP:port	http://**server IP:port**
Domain	http://**domain**
Domain:port	http://**domain:port**

3. Power on all IP phones.

   After being powered on, a phone obtains the IP address from the DHCP server. Then the DHCP server delivers the configuration file URL to the phone using the **Option246** parameter. After receiving the URL, the phone obtains the global configuration file from the file server to update the phone configurations, and downloads files such as the firmware version file from the URLs specified in the configuration file.

Verifying the Configuration and Upgrade

After you complete the preceding procedure, test on certain IP phones to ensure that the IP phones run normally.

Use the following methods to verify that the batch configuration and upgrade are successful:

- Configuration result

  Access the web configuration page and verify that the configurations are the same as those in the configuration file.
- Upgrade result

In the standby state, press **OK** to access the **Status** GUI, and verify that the version number corresponding to **Firmware** is the same as that of the firmware version file.

If some phones failed to be configured or upgraded, the possible cause is that too many phones send configure and upgrade requests to the server at the same time, and the server cannot handle all those requests. You are advised to restart these phones. The phone downloads the configuration file and firmware version from the file server during the restart.

4 Managing an IP Phone by Using eSpace EMS

4.1 Connecting IP Phones to eSpace EMS

This topic describes how to add IP phones one by one to the eSpace EMS if the number of required IP phones is small.

Prerequisites

- The mapping between the domain name, **ucems.huawei.com**, and the ACS IP address has been configured on the DNS. Or the ACS IP address has been configured on the IP phone.

NOTE
If no DNS server is connected to the network, connect the IP phones to the eSpace EMS by referring to 4.1.1 Configuring ACS Addresses.

- The physical serial number of the IP phone has been obtained.

NOTE
The physical serial number, that is, the MAC address, can be obtained in either of the following ways:

- Obtain the MAC address that is printed at the bottom of the IP phone, for example, **00156529EE10**.
- Press **OK** on the IP phone. **00:15:65:29:EE:10** is displayed in the **MAC:** column. The physical serial number is **00156529EE10**.

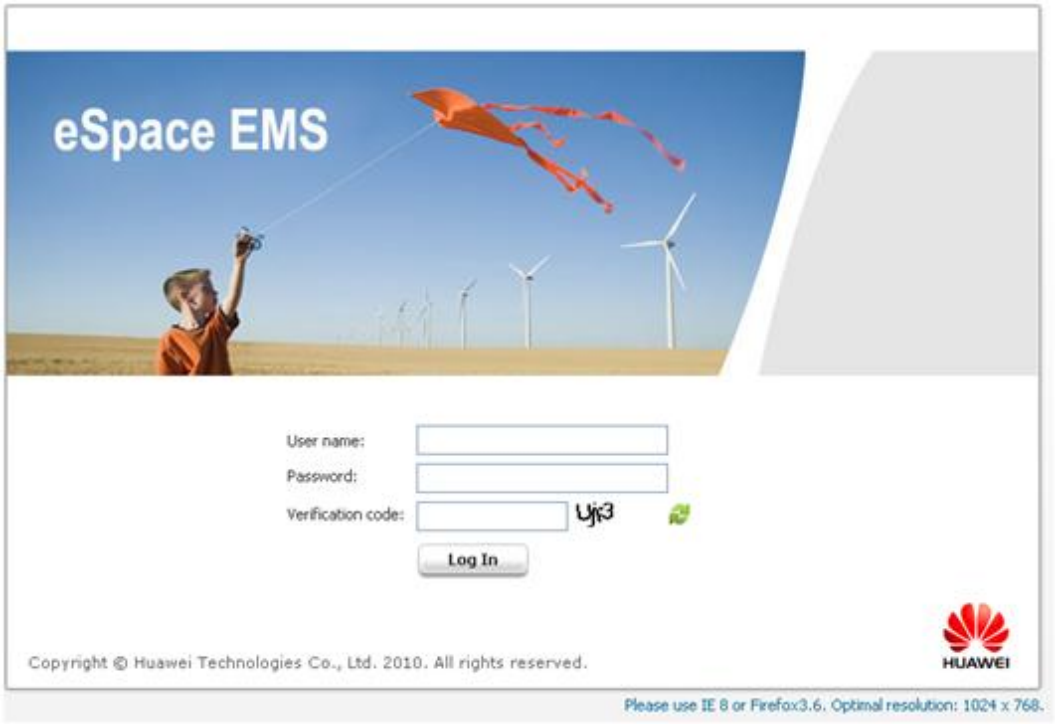
- The eSpace EMS service has been started.

Procedure

1. Enter the eSpace EMS address in the address box, for example: http://192.169.1.10:8080.
   The eSpace EMS web page as shown in Figure 4-1.

NOTE
Please use IE 8 or Firefox3.6 for login.

Figure 4-1 Logging in to the eSpace EMS web page



2. Choose **Resource** > **Resource Management**.
3. Select a subnet from the navigation tree. Click Create Resource.
4. Select IP Phone from **Physical Devices**, as shown in Figure 4-2.

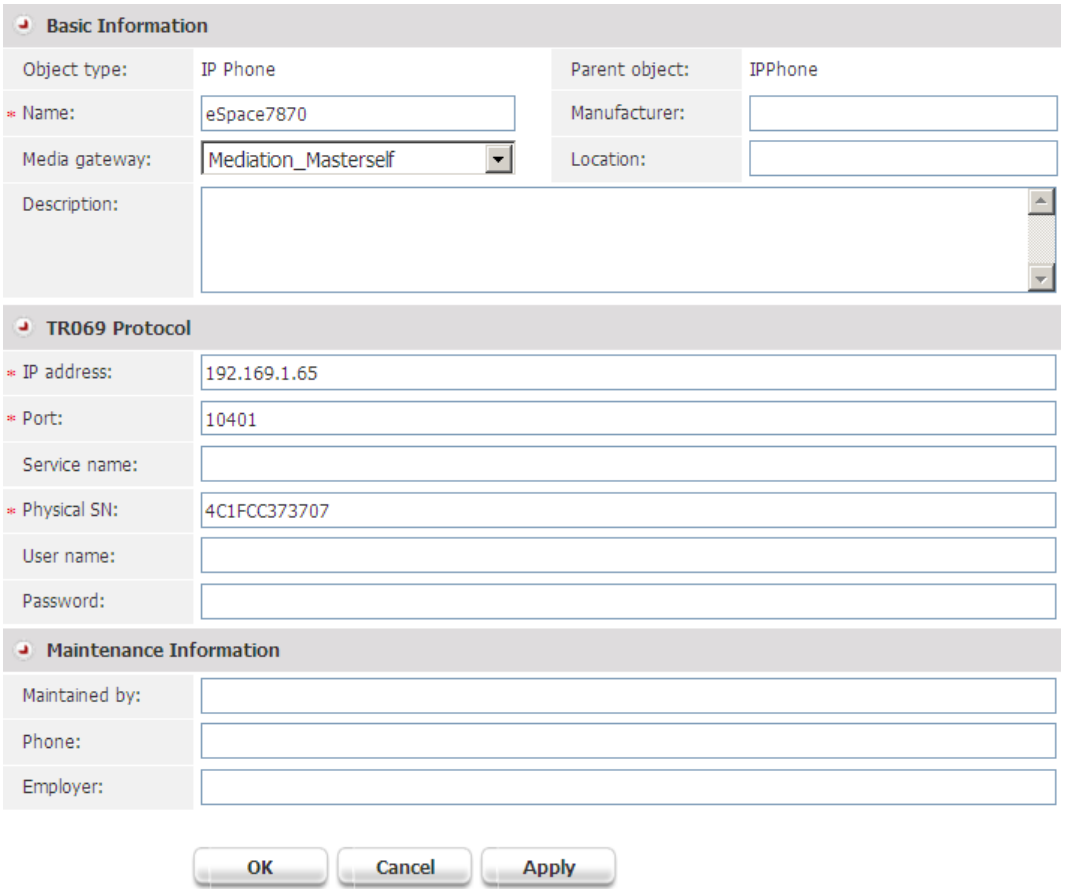
Figure 4-2 Creating an IP phone

5. On the **Configure Parameters** page, set **Name**, **IP Address**, **Port**, and **Physical SN**. Set other parameters as required.

NOTE

The default port number of eSpace 7800 series is **10401**.

Figure 4-3 Configuring parameters



6. Click **OK**.

NOTE
Click **Apply** to continue creating IP phones.

Results

- If the IP phone is created successfully, the IP phone is displayed in the navigation tree on the left pane.
- If the IP phone failed to be created, a dialog box is displayed indicating the cause. Click **OK** to reset parameters.

4.1.1 Configuring ACS Addresses

If no DNS is connected to the network, you can configure an ACS address for an IP phone to connect to the eSpace EMS. This topic describes how to configure a MAC address. This topic takes eSpace 7870 as an example.

Procedure

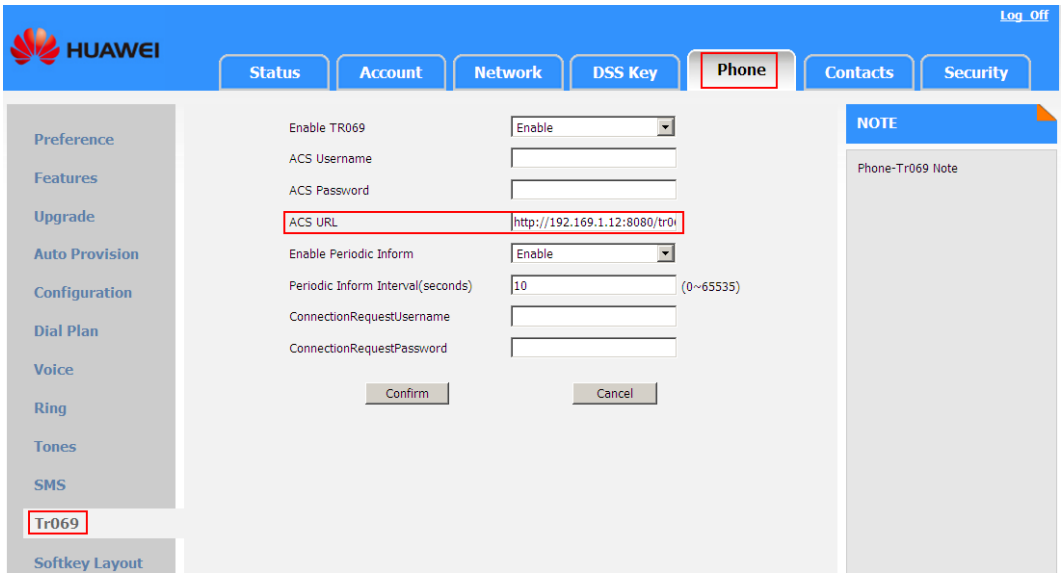
1. Log in to the IP phone web page.
   a. Enter the IP phone address in the address box and press **Enter**.
   b. In the displayed dialog box, enter the user name and password and click **OK**. The default user name and password are both **admin**.

2. Configure the ACS address.
   a. Click the **Phone** tab.
   b. Click **Tr069** in the navigation tree.
   c. Enter the ASC IP address in the **ACS URL** text box, as shown in Figure 4-4. If the IP address for logging in to the eSpace EMS is **192.169.1.10**, enter **http://192.169.1.10:8089/tr069/services/acs** in the ACS URL text box.

NOTE

To access the page for configuring ACS address for eSpace 7810&7820&7830&7850 IP phones, choose **Upgrade** > **TR069**.

Figure 4-4 Configuring ACS addresses



3. Set **TR069** and **Enable Periodic Inform** to **Enable**.
4. Click **Confirm**.

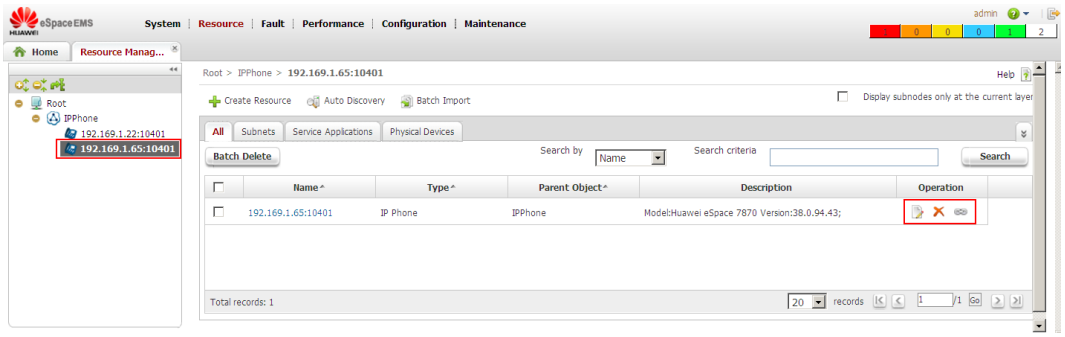
4.2 Managing IP Phones

This topic describes how to modify, delete, and manage IP phones on the eSpace EMS.

- Click . The **Modify** page is displayed.
- Click to **Delete** the IP phone. The IP phone cannot be managed by the eSpace EMS.
- Click . The **Manage** page is displayed.

  The following describes how to restart a device, load configuration files, export logs, export configuration files, and set basic IP phone parameters.

Figure 4-5 Managing an IP phone

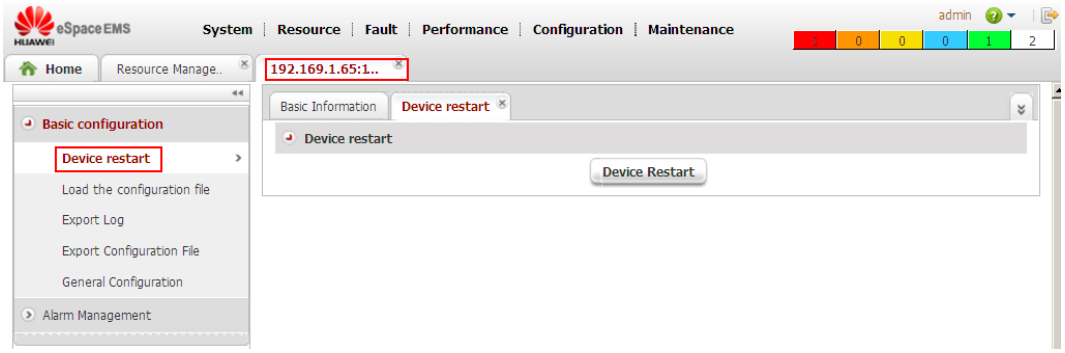


Restarting a Device

To restart an IP phone, perform the following operations:

1. Click . Choose **Basic Information** > **Device restart**. The page for restarting IP phones is displayed, as shown in Figure 4-6.

Figure 4-6 Device restart page



2. Click Device Restart.

NOTE

You can also restart IP phones on the IP phone web page.

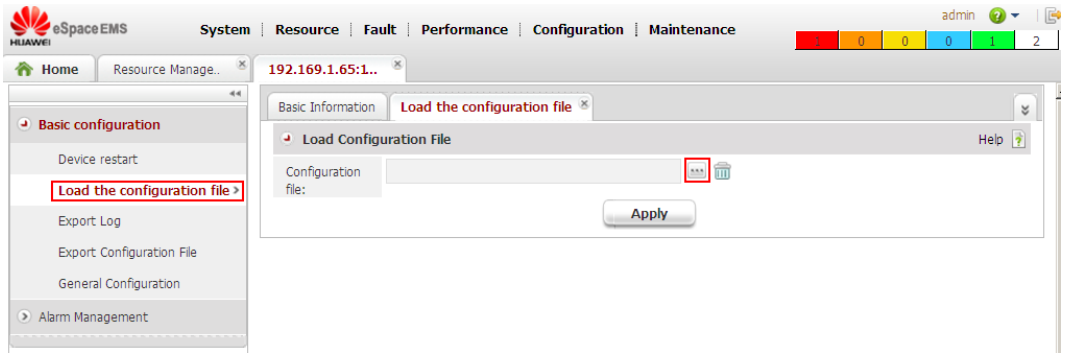
- To access the eSpace 7870 restart page, choose **Upgrade** > **Basic** > **Reboot System Now**.
- To access the eSpace 7810&7820&7830&7850 restart page, choose **Phone** > **Upgrade** > **Reboot**.

Loading a Configuration File

You can configure an IP phone by using the eSpace EMS.

To modify the IP phone parameters, you can create a configuration file or modify the original configuration file, and load the configuration file. For details about how to load configuration files in batches, see 5.2.3 Loading a Configuration File.

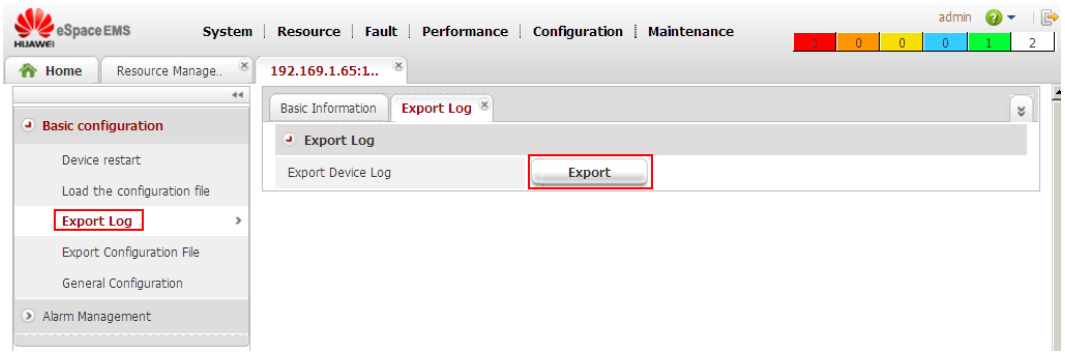
Figure 4-7 Loading the configuration file



Exporting Logs

You can export log files (syslog.tar) of IP phones and view operations on the IP phones.

Figure 4-8 Export Log



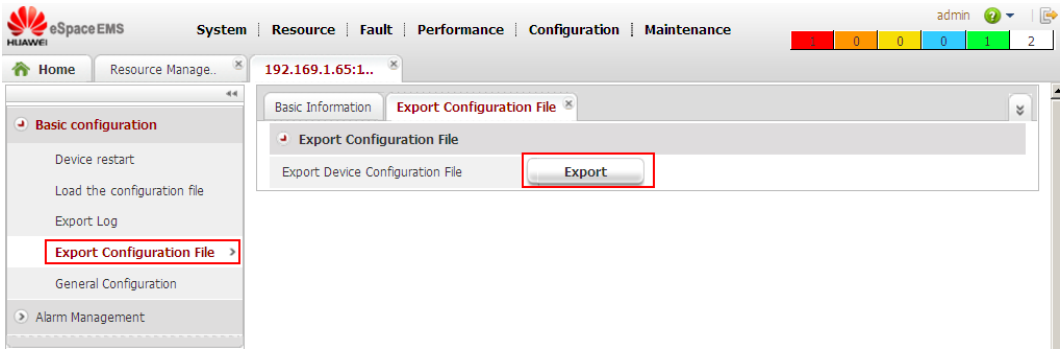
Exporting Configuration Files

You can export configuration files of IP phones and view and back up configuration files by using the eSpace EMS.

NOTE

- You can also export configuration files on the IP phone web page. To access the page for exporting eSpace 7870 configuration files, choose **Phone** > **Configuration** > **Export / Import Config**. To access the page for exporting eSpace 7810&7820&7830&7850 configuration files, choose **Upgrade** > **Advanced** > **Export / Import Config**.
- You can import the **config.bin** file into other IP phones of the same model.

Figure 4-9 Exporting configuration files

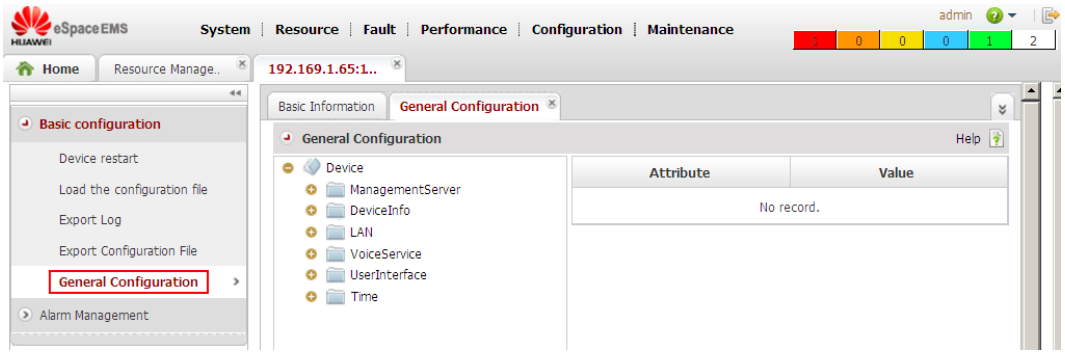


Setting Basic IP Phone Parameters

You can set IP phone parameters by using the eSpace EMS. The following describes the basic IP phone configuration items in the **Device** directory:

- ManagementServer: Manage server. The parameters include ACS URL, Username, and Password.
- DeviceInfo: Device information. The parameters include ManufacturerOUI, SerialNumber, and HardwareVersion.
- Configuration parameters of the Local Area Network (LAN). The parameters include AddressingType and SubnetMask.
- VoiceService: Voice service parameters. The parameters include SIP server, RTP server, and lines.
- UserInterface: User interface. The parameters include WebUserName and WebPassword.
- GatewayInfo: Gateway information. The parameters include ManufacturerOUI and SerialNumber.
- Time: Time server. The parameters include NTPServer and LocalTimeZone.

Figure 4-10 General configuration page



5 Managing IP Phones in a Centralized Manner by Using eSpace EMS

5.1 Connecting IP Phones to eSpace EMS

This topic describes how to add IP phones to the eSpace EMS if the number of required IP phones is large.

Prerequisites

To connect IP phones to the eSpace EMS, the following environment should be set up:

- Dynamic Host Configuration Protocol (DHCP) server environment: For details about how to set up the DHCP server environment, see 7.4 Setting Up the DHCP Server.
- Domain Name Server (DNS) environment. For details about how to set up the DNS server environment, see 7.3 Guidelines for Setting Up the DNS Server.

NOTE

If no DNS is connected to the network, configure the Auto Configuration Server (ACS) IP address for an IP phone to allow the IP phone to connect to the eSpace EMS. For details, see 4.1.1 Configuring ACS Addresses.

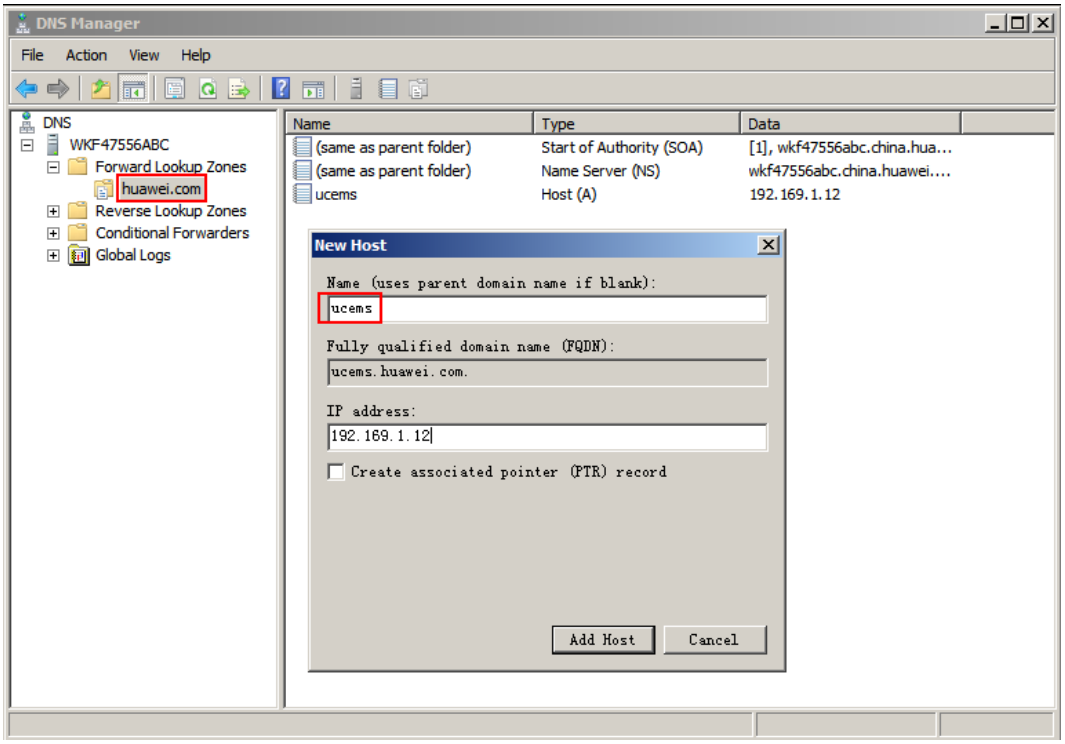
Principle

Use a network cable to connect an IP Phone to the network during the first deployment. After powering on the IP Phone, obtain the IP address and DNS address from the DHCP server, and send a request to the DNS server for resolving the domain name ucems.huawei.com. Upon obtaining the IP address of the ACS, the eSpace 8850 sends a request to the ACS server for accessing eSpace EMS. Information about the connected IP Phone is displayed on the management page of eSpace EMS.

Procedure

1. Obtain the IP address of the ACS server. This IP address is used for logging in to eSpace EMS using Internet Explorer.
2. Add the domain name ucems.huawei.com on the DNS server, as shown in Figure 5-1. Set the IP address mapping the domain name to the IP address of the eSpace EMS.

Figure 5-1 Creating a host on the DNS

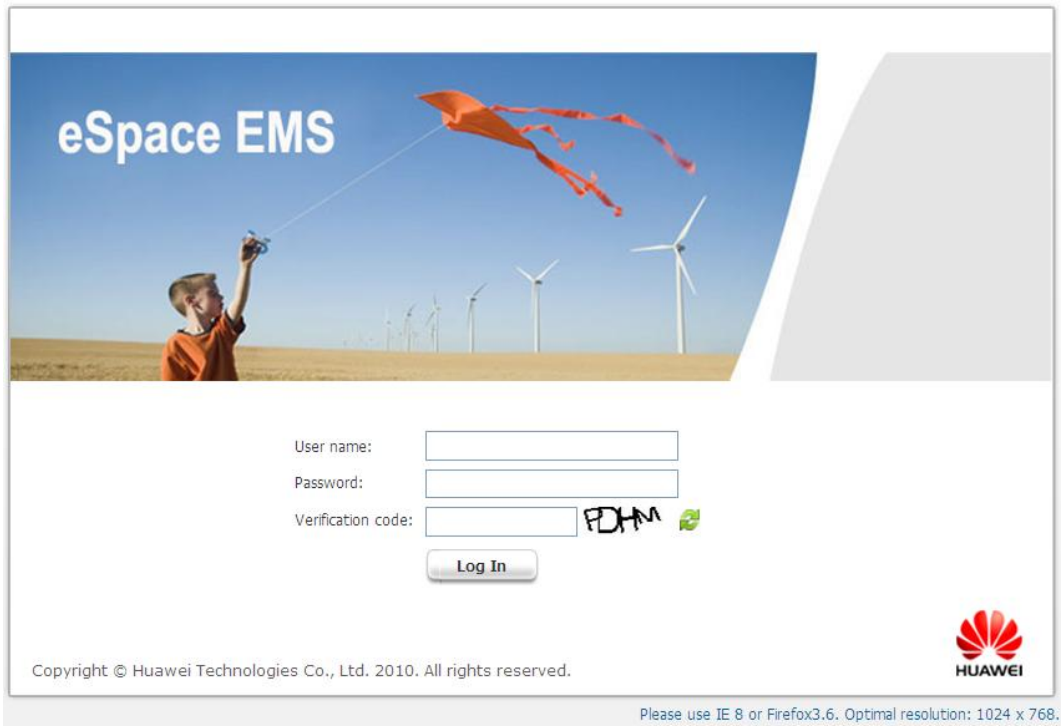


3. Log in to the eSpace EMS by using a web browser, as shown in Figure 5-2.

NOTE

Microsoft Internet Explorer 8 or Firefox 3.6 is recommended.

Figure 5-2 Logging in to the eSpace EMS by using a web browser



4. Choose **Resource** > **Resource Management**, click Create Resource.

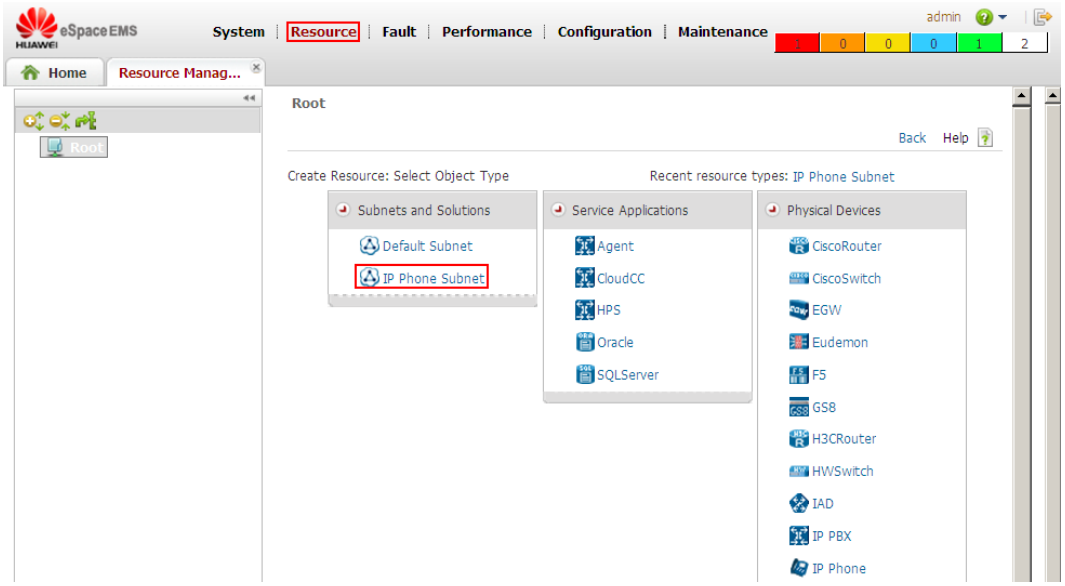
NOTE

After connecting to the eSpace EMS, the IP phones can be managed by the eSpace EMS. The eSpace EMS provides three IP phone connection methods: manual creation, automatic discovery, and batch import. This topic takes automatic discovery as an example. For details about the batch import, click to see the *eSpace EMS Help*.

Figure 5-3 Resource management page

5. Select IP Phone Subnet from **Subnets and Solutions**, as shown in Figure 5-4.

Figure 5-4 IP phone subnet creation

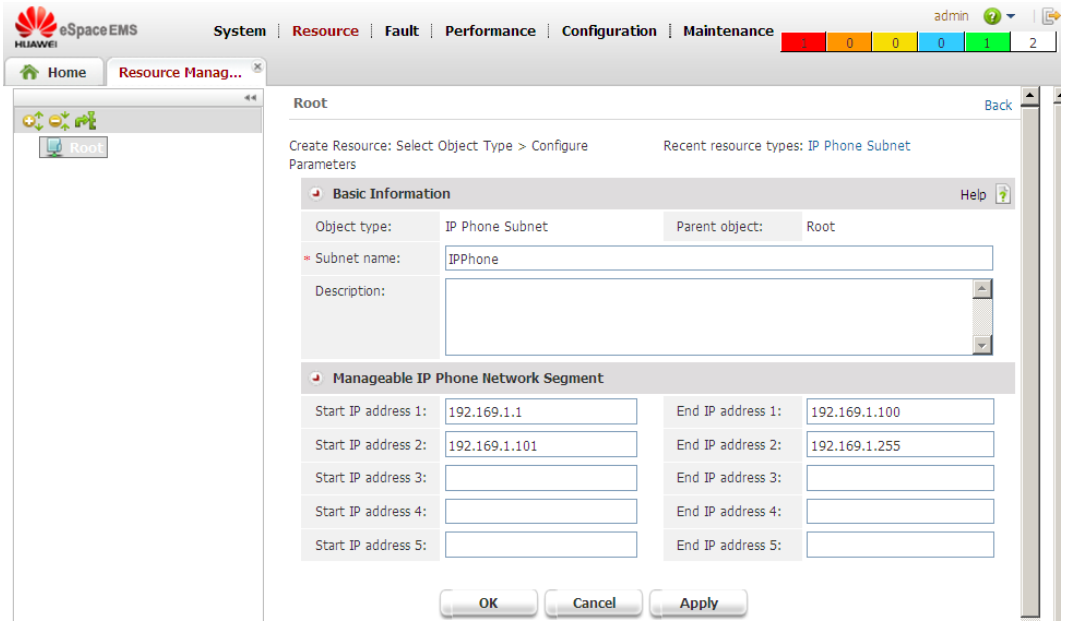


6. Set the subnet name, start IP address, and end IP address on the page for creating an IP phone subnet. as shown in Figure Figure 5-5.

NOTE

When you create multiple IP phone subnets, their IP address segments can contain each other but cannot overlap or duplicate. For details about the subnet plan, click , see the *eSpace EMS Help*.

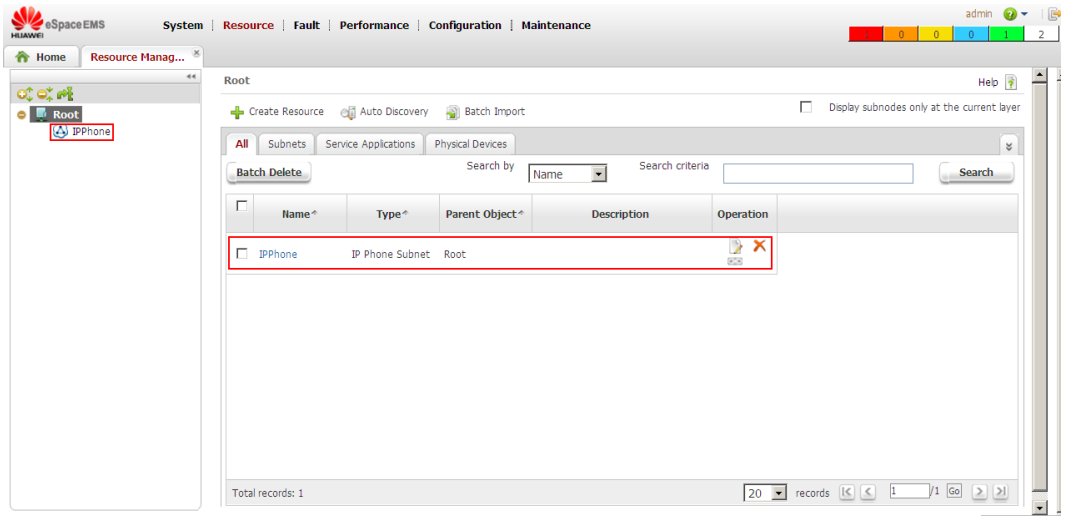
Figure 5-5 Setting IP phone subnet parameters



7. Click **OK**.

   The created IP phone subnet is displayed in the navigation tree, as shown in Figure 5-6.

Figure 5-6 IP phone subnet created successfully



8. Power on all IP phones.

   Detailed information about IP phones is displayed on the eSpace EMS.

Results

The IP phone registration request is sent to the eSpace EMS. If the IP address of the IP phone is out of the IP address range of the created IP phone subnet, the system stores the IP phone information to **Unregistered IP Phone** for later query.

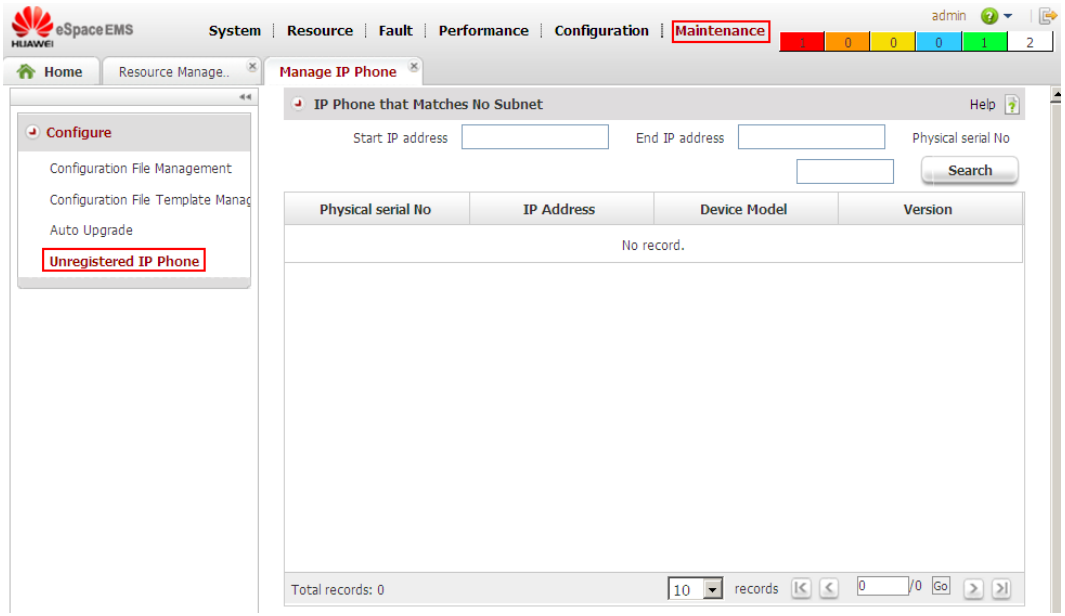
To view the IP phones that are not added to the eSpace EMS, choose **Maintenance** > **Manage IP Phone** > **Unregistered IP Phone**, as shown in Figure 5-7.

NOTE

You can add the unregistered IP phones to the eSpace EMS in one of the following ways:

- Add an IP phone subnet or change the IP address range of the original IP phone subnet.
- Change the IP address of the unregistered IP phone.
- Connect a few IP phones to the eSpace EMS by referring to 4.1 Connecting IP Phones to eSpace EMS.

Figure 5-7 Viewing unregistered IP phones



5.2 Configuring IP Phones in a Centralized Manner

This topic describes how to configure eSpace 7800 series IP phones in a centralized manner by using the eSpace EMS.

To configure IP phones by using the eSpace EMS, perform the following operations:

1. Connect all IP phones to configure to the , and create a subnet.
2. Upload a configuration file template, for example, 7870.cfg.

NOTE

The configuration file template is released with the eSpace EMS software. This template provides only configurations of the eSpace 7800 series IP phones. You can change some configuration parameters in the template before uploading the template.

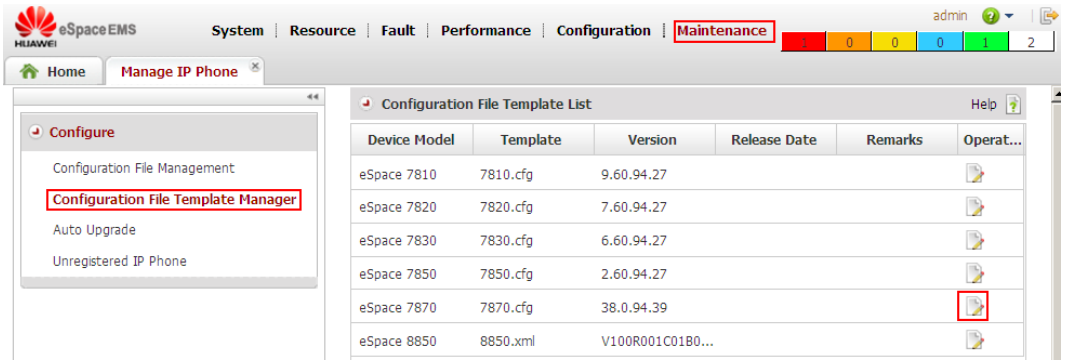
3. Create a configuration file. For details, see 5.2.2 Managing Configuration Files.
4. Deliver the configuration file to the IP phone. For details, see 5.2.3 Loading a Configuration File.

5.2.1 Managing Configuration File Templates

This topic describes how to manage the configuration file template by using 7870.cfg as an example.

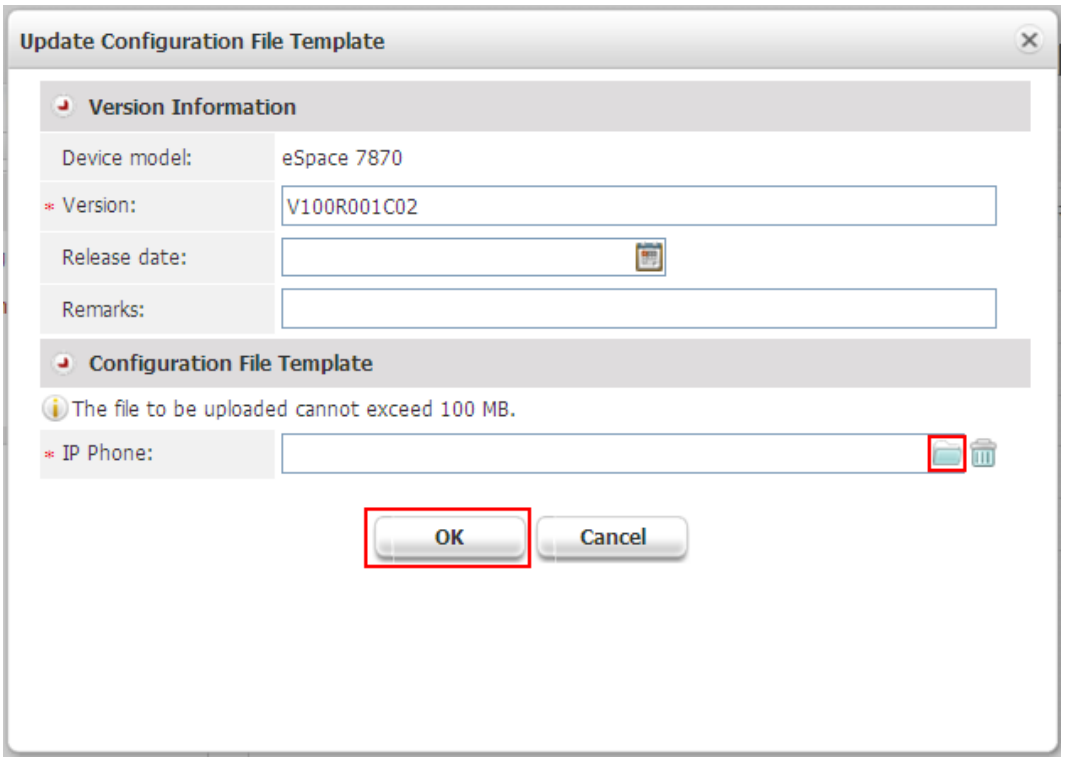
1. Choose **Maintenance** > **Manage IP Phone** > **Configuration File Template Manager**.

Figure 5-8 Configuration file template list



2. Click  . The **Update Configuration File Template** page is displayed.

Figure 5-9 Updating the configuration file template

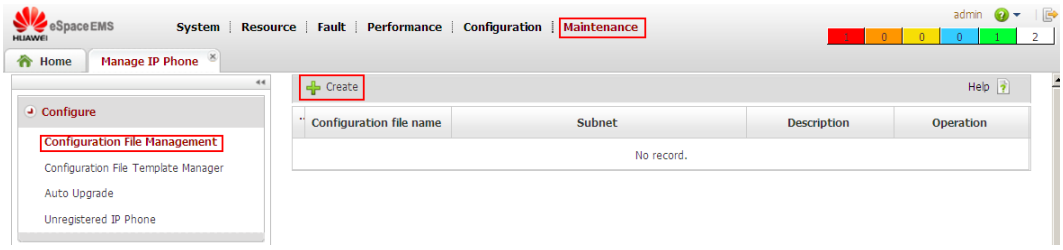


3. Click  to upload the configuration file template.

5.2.2 Managing Configuration Files

1. Choose **Maintenance** > **Manage IP Phone** > **Configuration File Management**, as shown in Figure 5-10.

Figure 5-10 Creating configuration files



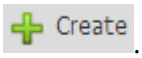
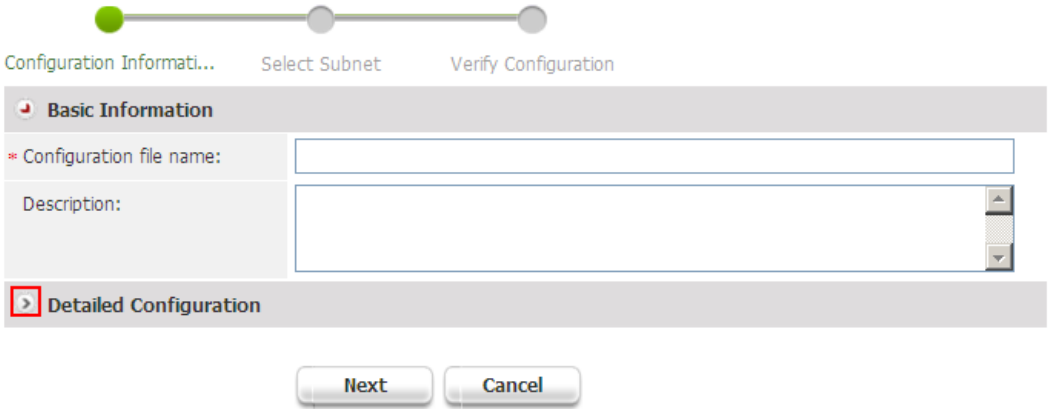
2. Click  . On the displayed **Configuration Information** page shown in Figure 5-11, enter the configuration file name.

Figure 5-11 Configuration information 1/2



3. Click  to view the detailed information.
   On the page shown in Table 5-1, set parameters based on the site requirements.

Figure 5-12 Configuration information 2/2

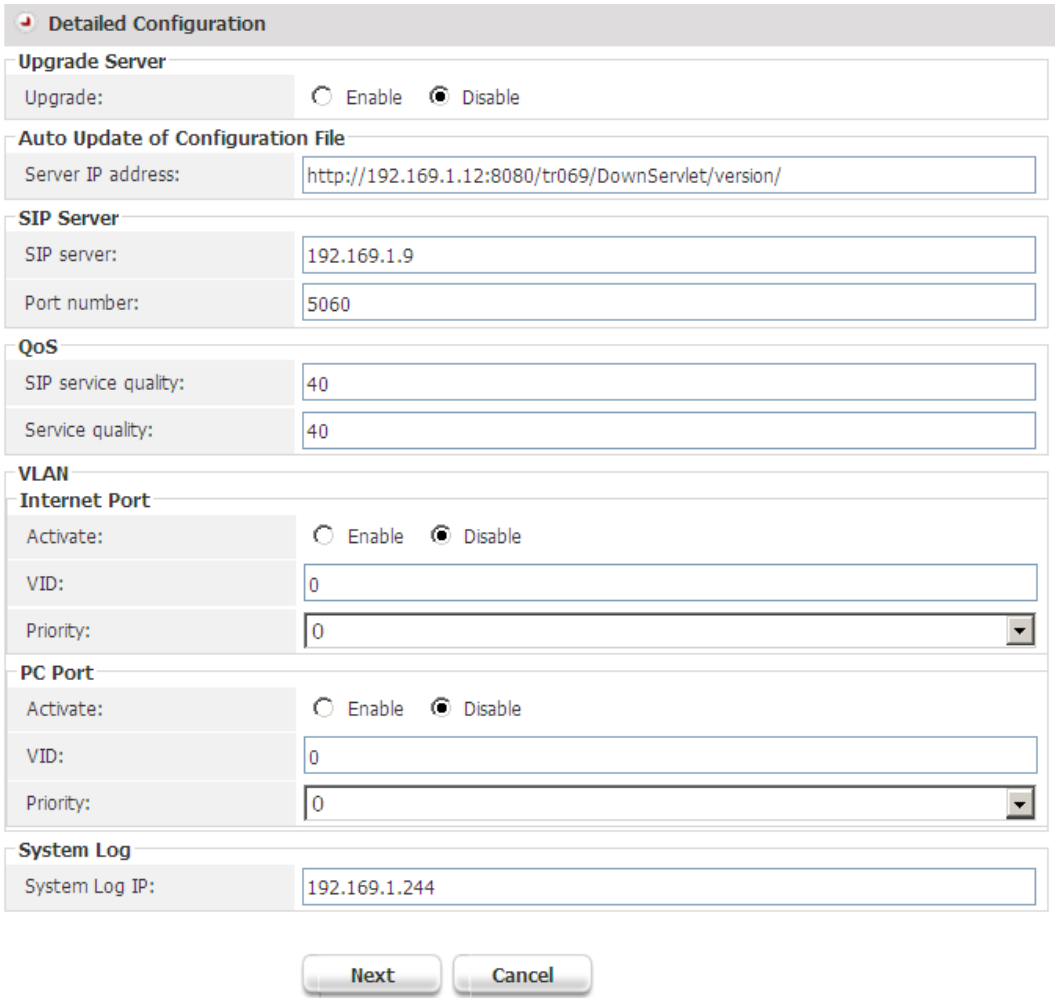
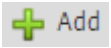


Table 5-1 Parameter description

Configuration Item	Parameter	Setting
Upgrade Server	Upgrade	Disables or enables the upgrade server.
Auto Update of Configuration File	Server IP address	Enter the IP address of the upgrade server, for example, the IP address of the Apache server.
SIP Server	SIP server	Enter the IP address of the SIP server.
	Port number	Default value: 5060.
QoS	SIP service quality	Signaling QoS. Value range: 0 to 63.
	Service quality	Voice QoS. Value range: 0 to 63.

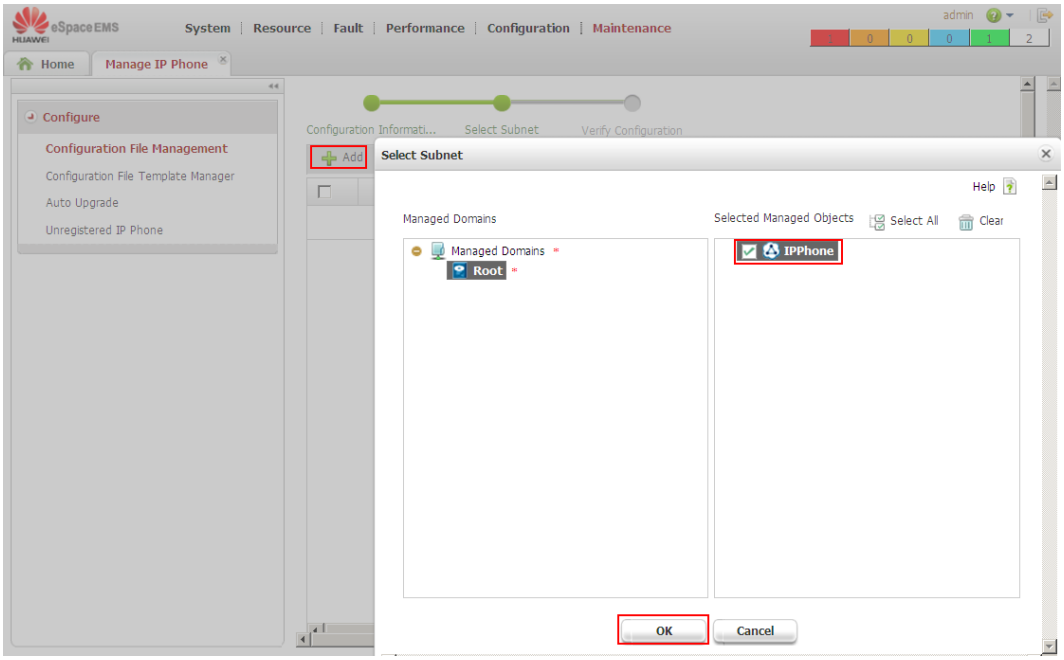
Configuration Item	Parameter		Setting
VLAN	Internet Port	Activate	**Enabled** indicates that the VLAN function is enabled for the network port.
		VID	ID of the VLAN where the IP phone belongs to. The network administrator divides the network where the switch resides into multiple VLANs. Each VLAN has a unique ID.
		Priority	VLAN priority for the network port. The value ranges from 0 to 7.
	PC Port	Activate	**Enabled** indicates that the VLAN function is enabled for the PC port.
		VID	ID of the VLAN where the IP phone belongs to. The network administrator divides the network where the switch resides into multiple VLANs. Each VLAN has a unique ID.
		Priority	VLAN priority for the PC port. The value ranges from 0 to 7.
System Log	System Log IP	Enter the IP address or domain name of the log server, for example, the IP address of the 3CDaemon server. For details, see 6.1.1 Viewing Debugging Logs.	

4. Click **Next**. The **Select Subnet** page is displayed.
5. Click  . Add a subnet from the **Managed Domains** area to the **Selected Managed Objects** area. Select managed objects.

NOTE

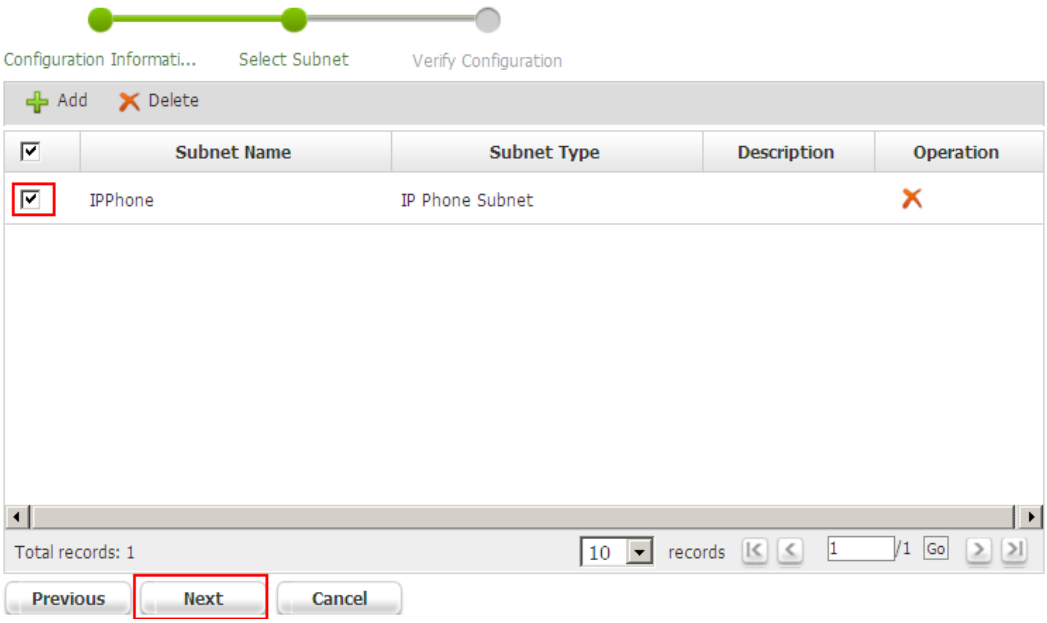
This step is optional. You can click **Next** to skip this procedure.

Figure 5-13 Adding a subnet



6. Click **OK**. The added subnet is displayed. Select the subnet, as shown in Figure 5-14.

Figure 5-14 Selecting the subnet



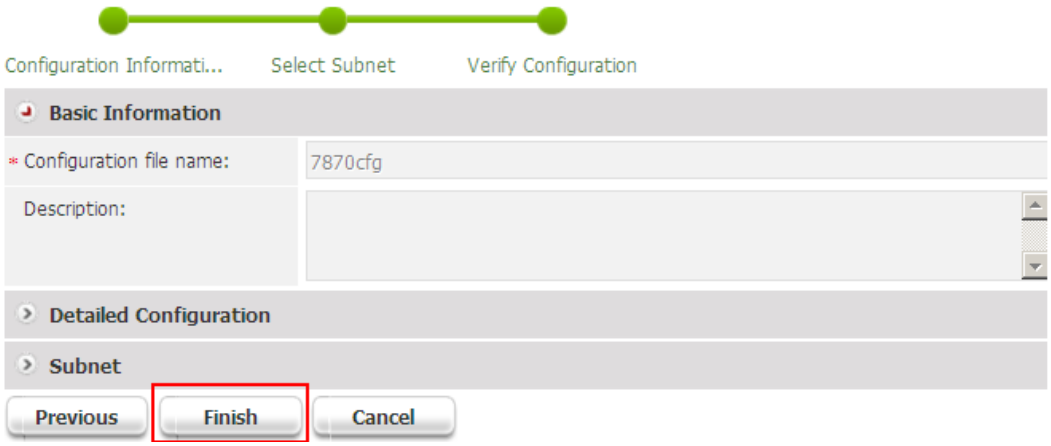
7. Click **Next** to check the configuration information. If the configuration is correct, click **Finish**.

NOTE

The configuration file is not delivered to the IP phone immediately when being created. The eSpace EMS will automatically deliver the configuration file to the IP phone in following conditions:

- The IP phone is added to the eSpace EMS subnet for the first time.
- The IP phone is restored to the factory defaults.
- The IP phone failed to load the configuration file and is restarted.

Figure 5-15 Verifying the configuration result

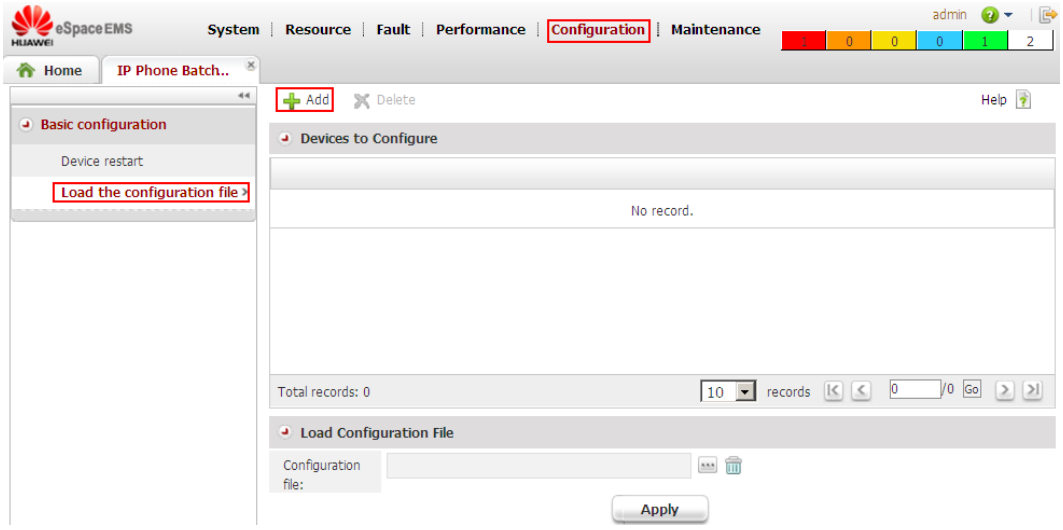


5.2.3 Loading a Configuration File

1. Choose **Configuration** > **IP Phone Batch Configuration** > **Load the configuration file**.

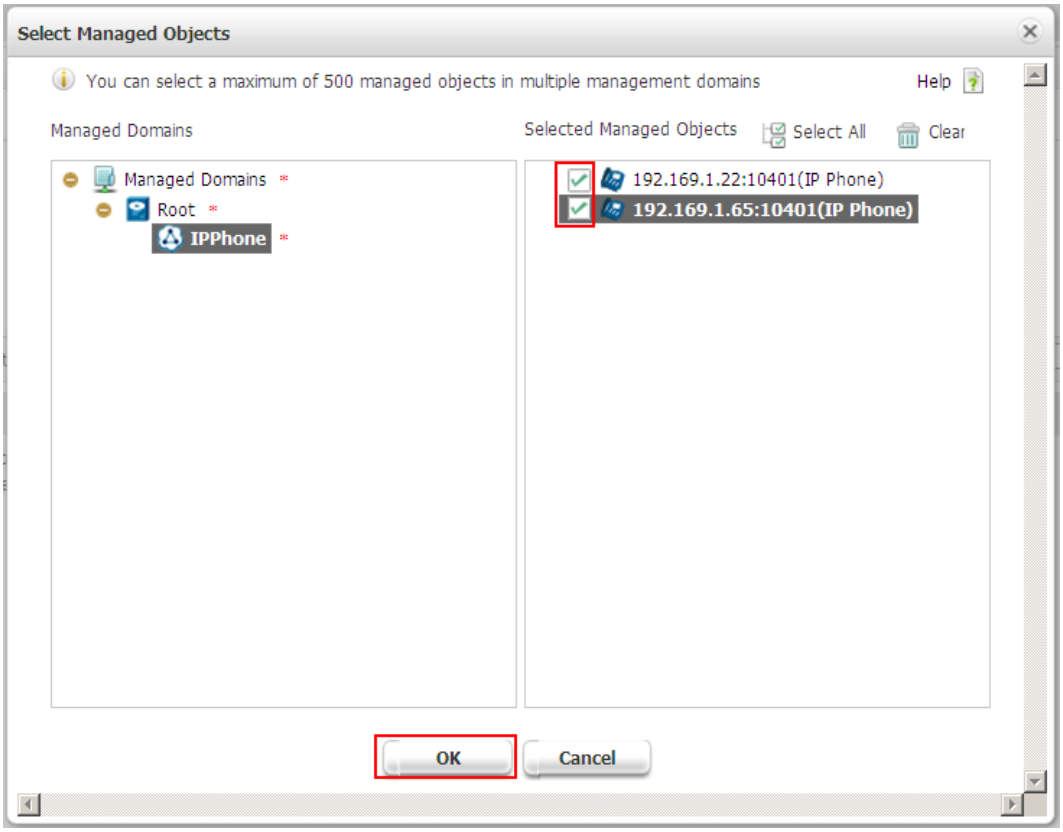
   The page for adding devices is displayed, as shown in Figure 5-16.

Figure 5-16 Adding devices



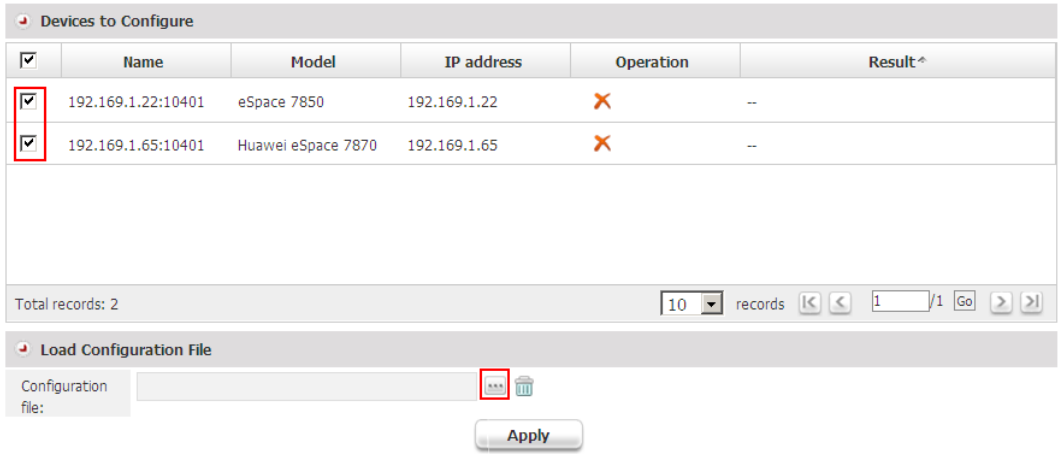
2. Click Add. Add devices under the management domain to the **Selected Managed Objects** area. Select the managed objects.

Figure 5-17 Selecting managed objects



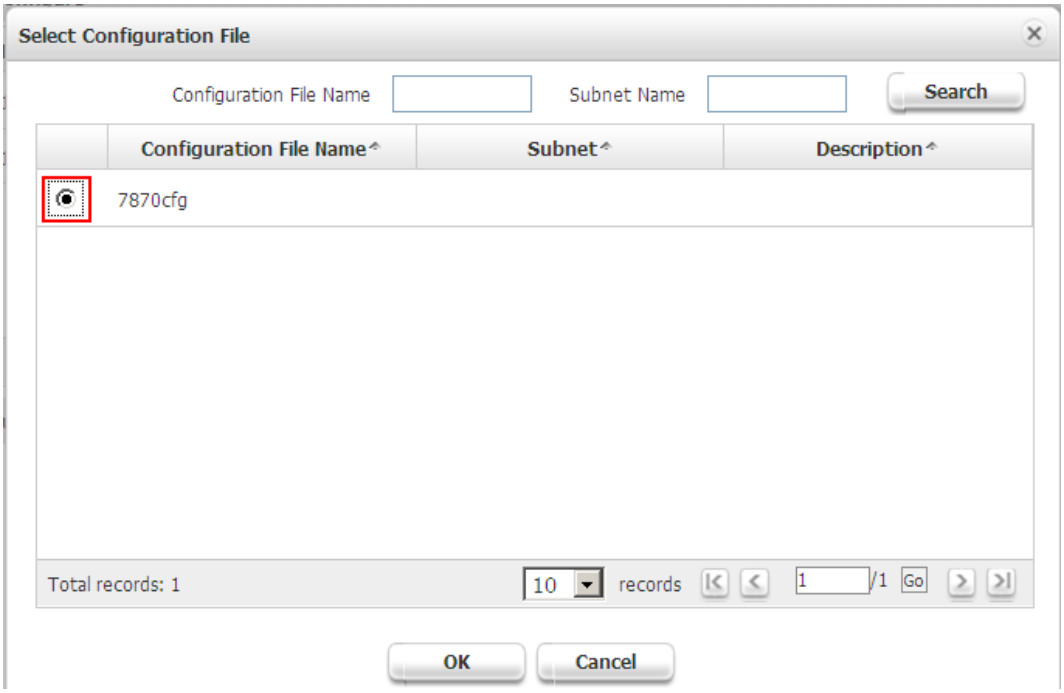
3. Click **OK**.
   The selected managed objects are added to the **Devices to Configure** area.

Figure 5-18 List of devices to configure



4. Click  next to **Configuration file**. Select a configuration file and click **OK**.

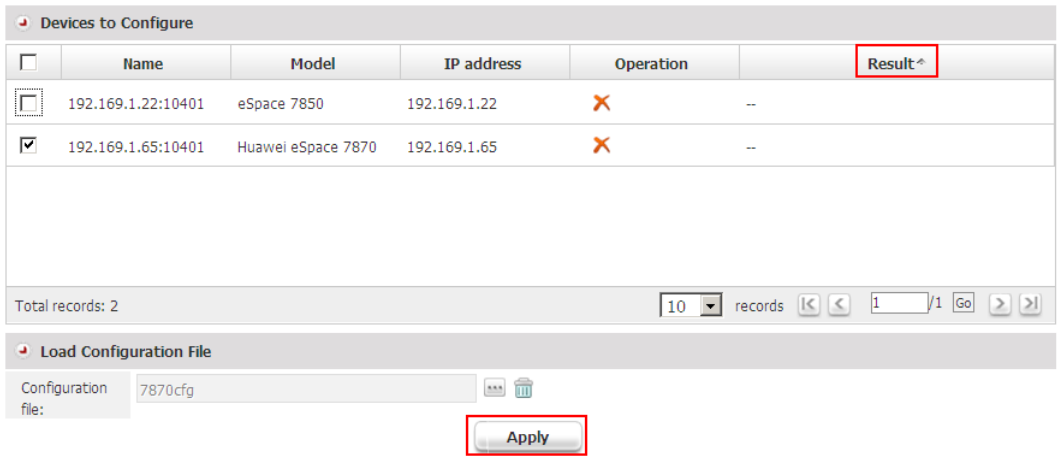
Figure 5-19 Selecting a configuration file



5. Select IP phones to configure and click **Apply**.

   The IP phones start to load the configuration file. You can view the configuration result in the **Result** area.

Figure 5-20 Configuration result



5.3 Upgrading IP Phones in a Centralized Manner

This topic describes how to upgrade eSpace 7800 series IP phones in a centralized manner by using the eSpace EMS.

Prerequisites

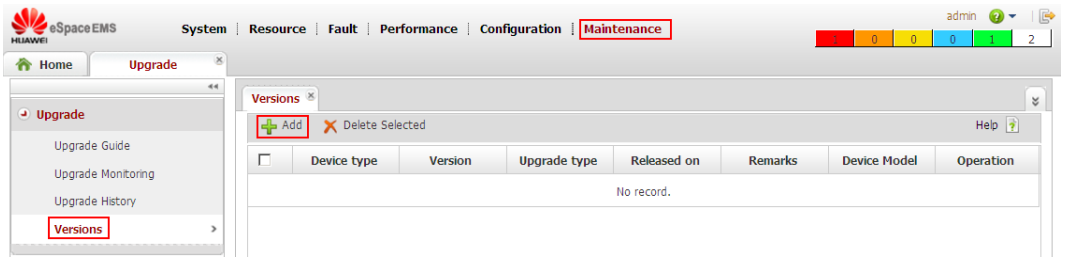
All IP phones to configure have been connected to eSpace EMS, and subnets have been configured.

Procedure

1. Upload the version file to eSpace EMS.

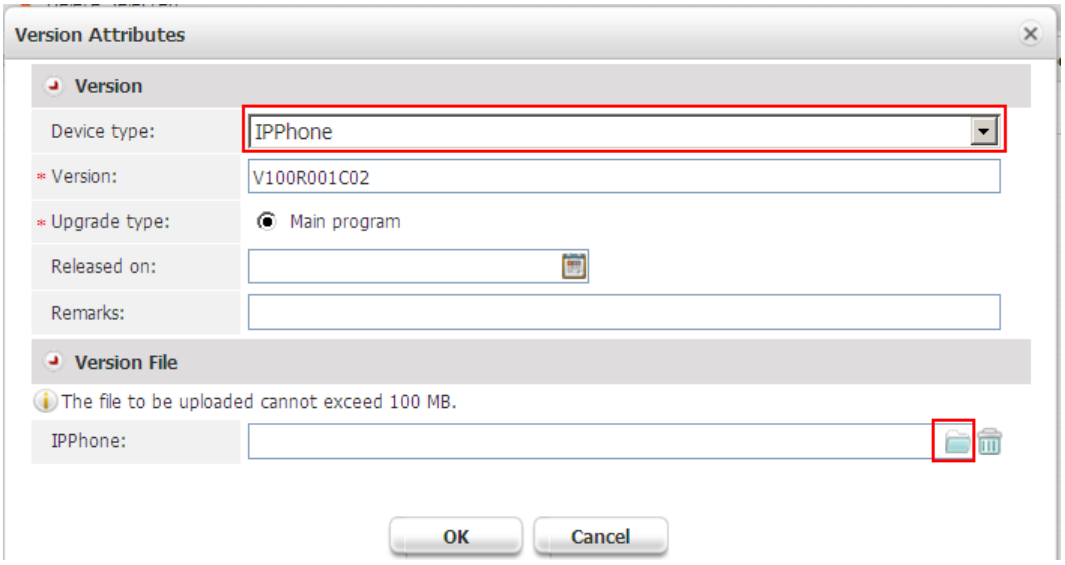
   Choose **Maintenance** > **Upgrade** > **Version**, as shown in Figure 5-21.

Figure 5-21 Version management



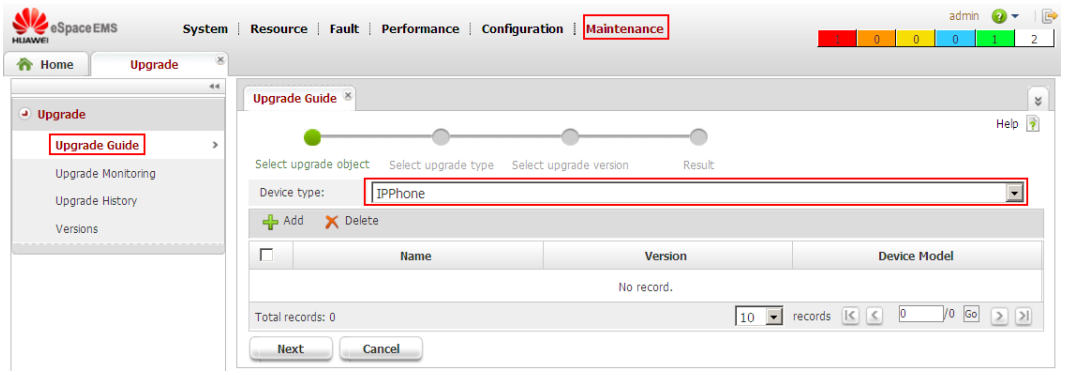
2. Click Add. The **Version Attributes** page is displayed, as shown in Figure 5-22.

Figure 5-22 Version Attributes page



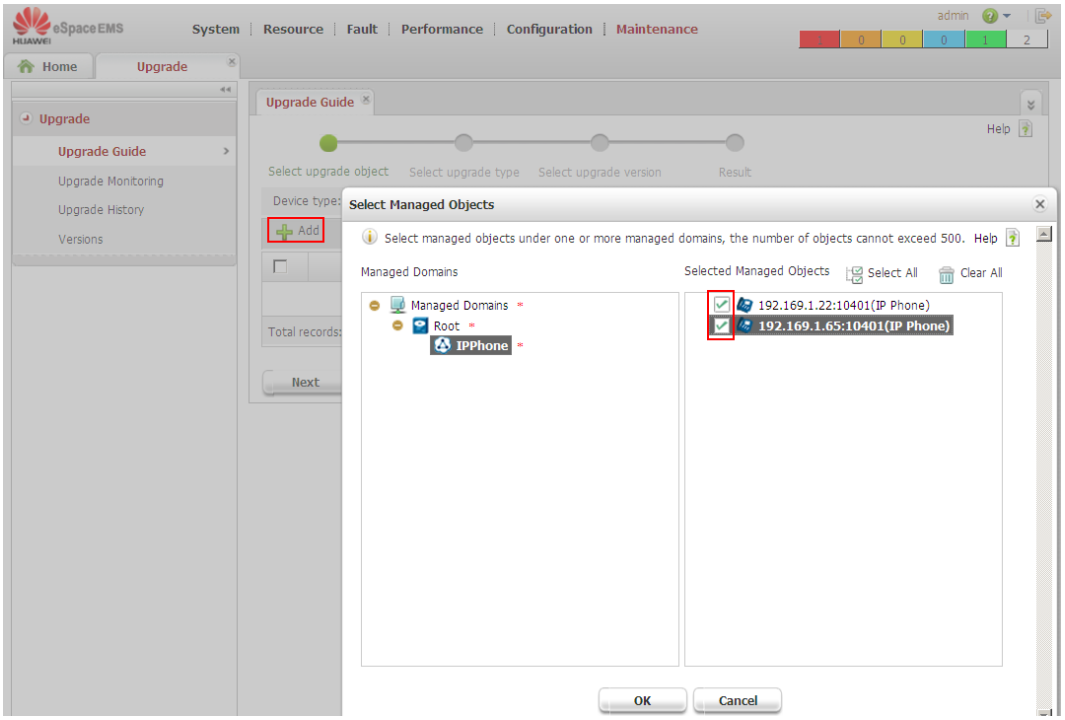
3. Select **IPPhone** from the **Device type** drop-down list box, and set information such as version. Click to select the version file, for example, **38.0.94.43.rom** that is the version file of eSpace 7870 IP phones.Click **OK** to upload the version file
4. Choose **Maintenance** > **Upgrade** > **Upgrade Guide**. The **Upgrade Guide** page is displayed, as shown in Figure 5-23.

Figure 5-23 Selecting upgrade objects



5. Select **IPPhone** from the **Device type** drop-down list box, and click Add. Select an IP phone to upgrade in the displayed **Select Managed Objects** dialog box, as shown in Figure 5-24.

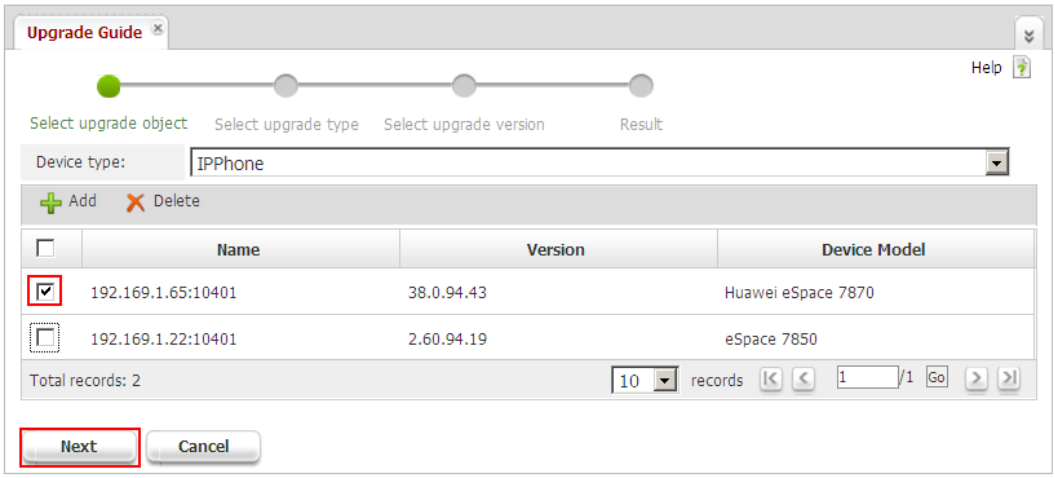
Figure 5-24 Selecting managed objects



6. Click **OK**.

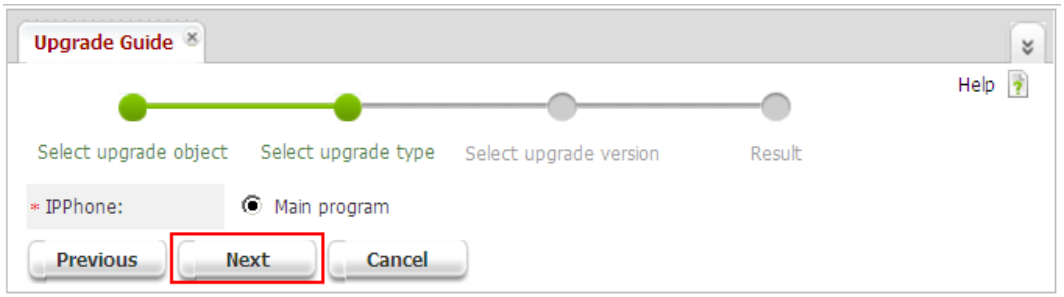
   The **Select Upgrade Object** page is displayed.

Figure 5-25 Selecting upgrade objects



7. Select all IP phones, and click **Next**.
   The **Select upgrade type** page is displayed.

Figure 5-26 Selecting an upgrade type

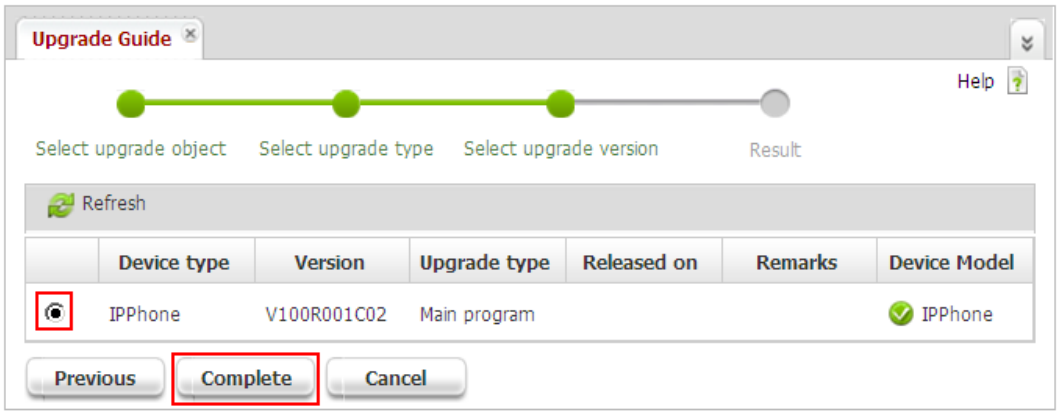


8. Click **Next**.
   The **Select upgrade version** page is displayed.

NOTE

If the main program that you want to upload is not in the list, click Refresh to refresh the list.

Figure 5-27 Selecting an upgrade version



9. Select a main program, and click **Complete**. The **Result** page is displayed.
10. Click **Upgrade Monitoring** to view the upgrade result.

result

After performing the preceding operations, verify that eSpace IP phones are upgraded successfully in one of following ways:

- On eSpace EMS, check the progress parameter value on the **Upgrade Monitoring** page.
- On eSpace EMS, choose **Resource** > **Manage** and click the subnet of upgraded eSpace IP phones on the **Manage** page to verify that the version number of eSpace IP phones is the same as that of the firmware file.
- On the web configuration page of an eSpace IP phone, open the **Status** tab page and verify that the **Firmware Version** parameter value is correct.
- On an eSpace IP phone, press **OK** when the phone is in standby state and verify that the **Firmware Version** parameter value is correct on the phone status page.

If eSpace IP phones fail to be upgraded in a batch, possible causes are as follows:

- The uploaded version file is incorrect. For example, if the eSpace 7850 version file name is **2.60.94.36.rom** while the uploaded file name is **2.60.94.35.rom** or **38.0.94.43.rom**, eSpace 7850 cannot be upgraded successfully.
- eSpace IP phones are powered off or disconnected from the network during the upgrade process.

When faults are rectified, you must delete the upgrade record on the **Upgrade Monitoring** page before re-upgrade eSpace IP phones. Otherwise, the message "The device is in the upgrade monitoring queue" will be displayed on the **Upgrade Guide** page and the upgrade cannot succeed.

5.4 Upgrading eSpace IP Phones Automatically

eSpace IP phones of the same model can automatically download the new version file from eSpace EMS and can be upgraded automatically when the **Check New Config** parameter is enabled.

Prerequisites

You have obtained the configuration file template and version file.

The global configuration file template is delivered with the software version and is available at http://enterprise.huawei.com/en/support/.

NOTE

You must apply for permission to download the global configuration file template from the website. If you need to download the file, contact system or service providers.

The path is **Software Downloads** > **Unified Communication** > **IP Phone** > **Version (For example, IP Phone V100R001C02)** > **software**.

NOTE

eSpace 7810, eSpace 7820, eSpace 7830, eSpace 7850 use the same configuration file. When loading the configuration file to a phone, change the name of the configuration file to the model name of the phone.

Procedure

eSpace 7810&7830&7850&7870 can be upgraded automatically on eSpace EMS. The following uses eSpace 7850 as an example to describe the process of upgrading eSpace IP phones in a batch on eSpace EMS.

NOTE

To upgrade an eSpace IP phone automatically on eSpace EMS, choose **Upgrate** > **Advanced** on the eSpace IP phone web page, set the **URL** parameter on the **Advanced** page (for example, set the parameter to **http://ucems.huawei.com:8089/tr069/DownServlet/version/**), enable the **Check New Config** parameter, and perform operations described in 3.

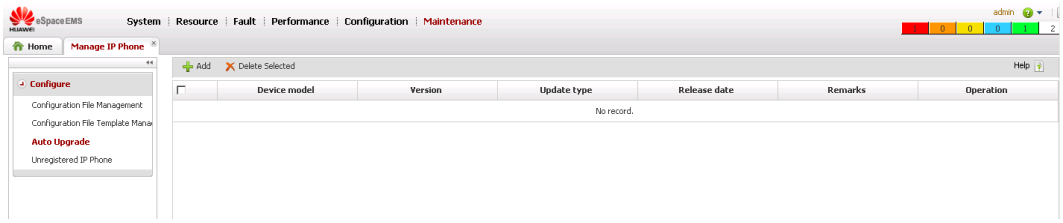
1. Connect eSpace 7850s to eSpace EMS. For details, see 5.1 Connecting IP Phones to eSpace EMS.
2. Deliver the eSpace 7850 configuration file to all eSpace 7850s. For details, see 5.2.2 Managing Configuration Files and 5.2.3 Loading a Configuration File.

NOTE

To automatically upgrade eSpace IP phones, you must set **Upgrade** to **Enable** on the **Configuration File Management** page.

3. Upload the version file to eSpace EMS.
   a. Choose **Maintenance** > **Manage IP Phone** > **Auto Upgrade**, as shown in Figure 5-28.

Figure 5-28 Adding eSpace IP phones

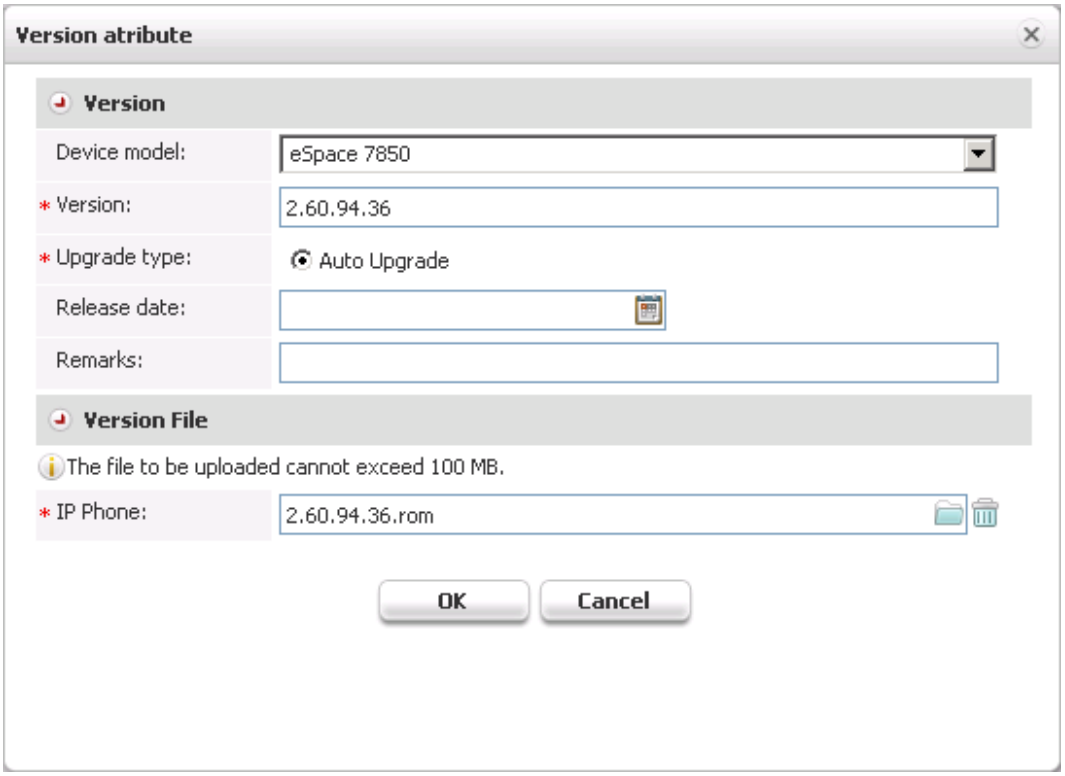


   b. Click Add. The **Version attribute** dialog box is displayed, as shown in Figure 5-29. Select the device model **eSpace 7850**, and enter the version number. Click and upload the eSpace 7850 version file.

NOTE

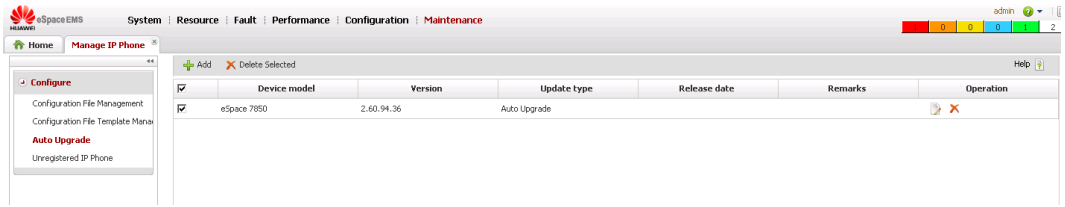
You are advised to set the version number to that of the version file to facilitate further maintenance.

Figure 5-29 Version attribute



c. Click **OK**. Figure 5-30 lists eSpace IP phones to be upgraded automatically.

Figure 5-30 eSpace IP phones to be automatically upgraded



Follow-up Procedure

Wait for the upgrade to be triggered.

- If the version file configured on eSpace EMS is the same as that of eSpace IP phones, eSpace IP phones restart and download the configuration file from eSpace EMS.
- If the version file configured on eSpace EMS is the different from that of eSpace IP phones, eSpace IP phones restart, download the configuration file from eSpace EMS, and upgrade automatically.

6 Troubleshooting

6.1 Fault Locating Methods

6.1.1 Viewing Debugging Logs

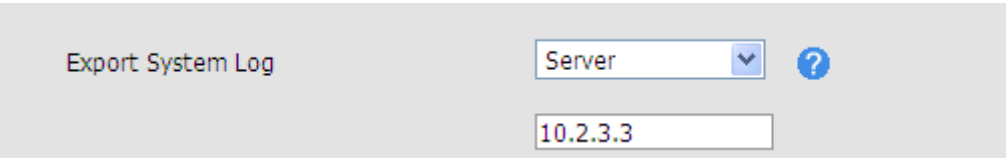
IP phone logs help users to locate the cause of a fault on an IP phone and learn the operating status of an IP phone. The log file can be stored on the server so that maintenance personnel can query the logs. The log file can be stored to the computer of a user so that the user can query them.

Configuring the IP phone

To export a log file to the server, proceed as follows:

1. Log in to an IP phone's web page, click the **Upgrade** tab, and click **Advanced**.
   Log in to eSpace 7870's web page, click the **Phone** tab, and click **Configuration**.
2. Select **Server** from the **Export System Log** drop-down list box, and enter the system log server address, as shown in Figure 6-1.

Figure 6-1 Setting the Export System Log parameter



3. Click **Confirm**.
   The IP phone automatically restarts, and the settings take effect.

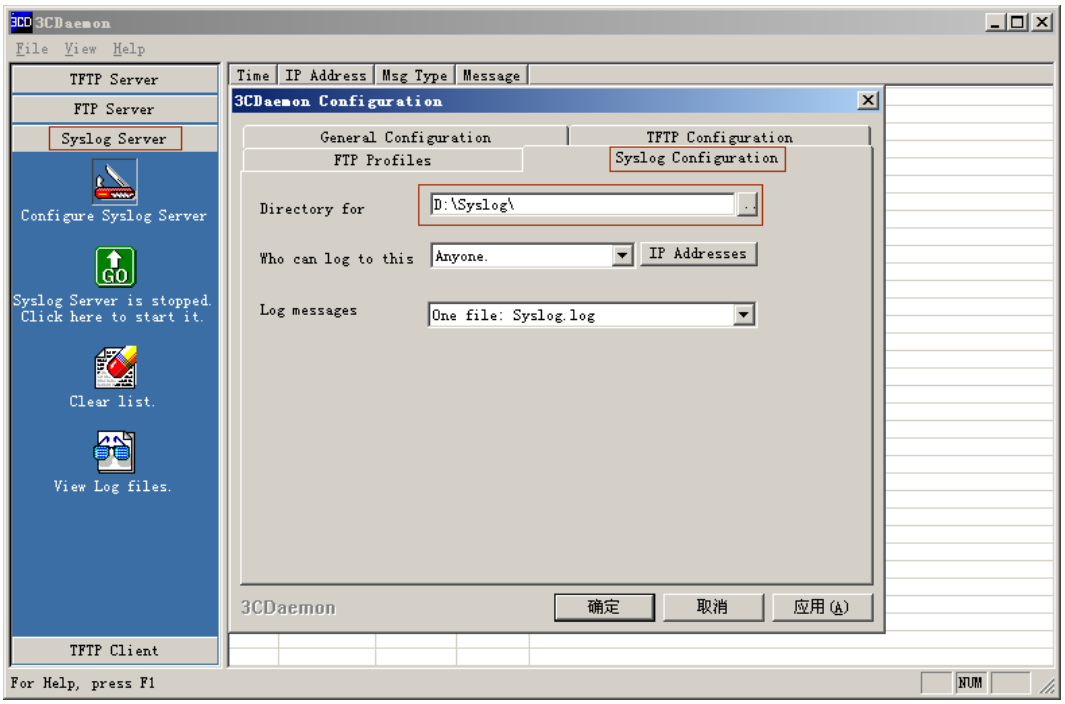
Configuring the log server

You must configure the log server before exporting log files to the server. A common file server can function as a log server and 3CDaemon is recommended. To configure a log server, proceed as follows:

1. Double-click **3CDaemon.EXE**.
2. Start the log server, click **Syslog Server** and click **Configure Syslog Server**.

The **3CDaemon Configuration** page is displayed, as shown in Figure 6-2.

Figure 6-2 Setting the log storage path



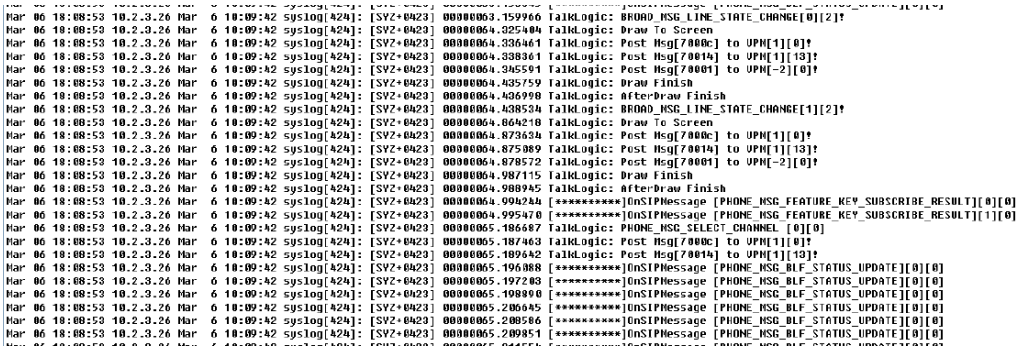
3. Click the **Syslog Configuration** tab.
4. On the **Syslog Configuration** tab page, click  corresponding to **Directory for**, and select the path for saving logs.
5. Access the specified path and verify that the **syslog.log** file exists.

   If the file exists in the directory, the log server is configured successfully.

Viewing logs

After the IP phone and server are configured, you can view log files in the path specified by **Directory for** when the server is running. Figure 6-3 shows an example of a log file.

Figure 6-3 An example of a log file



Exporting a Log File to the Local Computer

To export a log file to the local computer, proceed as follows:

1. Log in to an IP phone's web page, click the **Upgrade** tab, and click **Advanced**.
2. Select **Local** from the **Export System Log** drop-down list box, as shown in Figure 6-4.

Figure 6-4 Exporting a log file to the local computer

3. Click **Export**.
4. Select a path for storing the exported log file.

After the **syslog.tar** log file is exported, view the file in the specified path. Figure 6-5 shows an example of the syslog.tar file.

Figure 6-5 An example of the syslog.tar log file

```
Mar  2 00:00:00 syslogd started: BusyBox v1.10.3
Mar  2 00:00:06 syslog: [AutoP]: AutoP Release Version:[ 2.0.0.79 ]
Mar  2 00:00:06 ap: [AutoP]: Get hardware version: [1.0.0.0]
Mar  2 00:00:06 ap: [AutoP]: Get device mac: [001565111855]
Mar  2 00:00:16 syslog[366]: [sip] **init phone context** [0]
Mar  2 00:00:16 syslog[366]: ReservePound = [1] RFC2543Hold = [0] UseOutBoundInDialog = [1]
Mar  2 00:00:16 syslog[366]: Message sent: [(PHONE_MSG_BLA_STATUS_UPDATE) – (0xa001e)  wParam(0x0)-lParam(0x0)]
Mar  2 00:00:16 syslog[366]: [SYZ+0365] 00000021.266011 Registing thread "app_sipServer" ...
Mar  2 00:00:16 syslog[366]: [sip] ** Loading Account **
Mar  2 00:00:16 syslog[366]: [SYZ+0396] 00000024.438176 Registing thread "app_sipClient16" ...
Mar  2 00:00:16 syslog[366]: [SYZ+0406] 00000025.089721 Registing thread "app_sipClient1" ...
Mar  2 00:00:16 syslog[366]: SIP UA Release Version:[ 6.0.0.12 ]
Mar  2 00:00:16 syslog[366]: Build Dec 31 2010 10:53:08
Mar  2 00:00:16 syslog[366]:
Mar  2 00:00:16 syslog[366]: [ Audio codecs Configuration ]
Mar  2 00:00:16 syslog[366]: enable = 1 PayloadType = PCMU priority = 1 rtpmap = 0
Mar  2 00:00:16 syslog[366]: enable = 1 PayloadType = PCMA priority = 2 rtpmap = 8
Mar  2 00:00:16 syslog[366]: enable = 0 PayloadType = G723_53 priority = 0 rtpmap = 4
Mar  2 00:00:16 syslog[366]: enable = 0 PayloadType = G723_63 priority = 0 rtpmap = 4
Mar  2 00:00:16 syslog[366]: enable = 1 PayloadType = G729 priority = 3 rtpmap = 18
Mar  2 00:00:16 syslog[366]: enable = 1 PayloadType = G722 priority = 4 rtpmap = 9
Mar  2 00:00:16 syslog[366]: enable = 0 PayloadType = iLBC priority = 0 rtpmap = 102
Mar  2 00:00:16 syslog[366]: enable = 0 PayloadType = G726-16 priority = 0 rtpmap = 112
Mar  2 00:00:16 syslog[366]: enable = 0 PayloadType = G726-24 priority = 0 rtpmap = 102
Mar  2 00:00:16 syslog[366]: enable = 0 PayloadType = G726-32 priority = 0 rtpmap = 2
```

Exporting Network Packets to the Local Computer

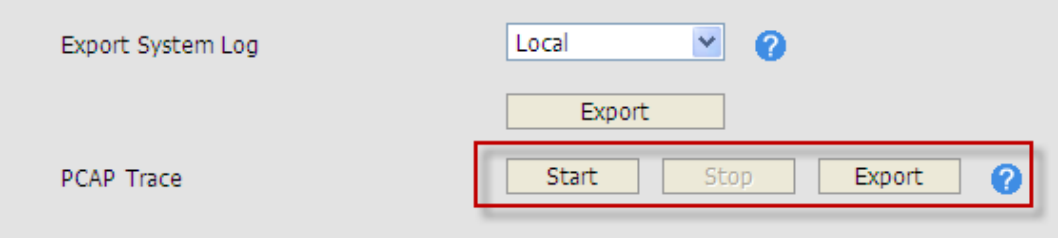
CAUTION

The size of network packets to export cannot exceed 500 KB. If the size exceeds 500 KB, the export fails.

To export network packets to a local computer, proceed as follows:

1. Log in to an IP phone's web page, click the **Upgrade** tab, and click **Advanced**.
   Log in to eSpace 7870's web page, click the **Phone** tab, and click **Upgrade**.
2. Click **Start** in the **PCAP Trace** area, as shown in Figure 6-6.

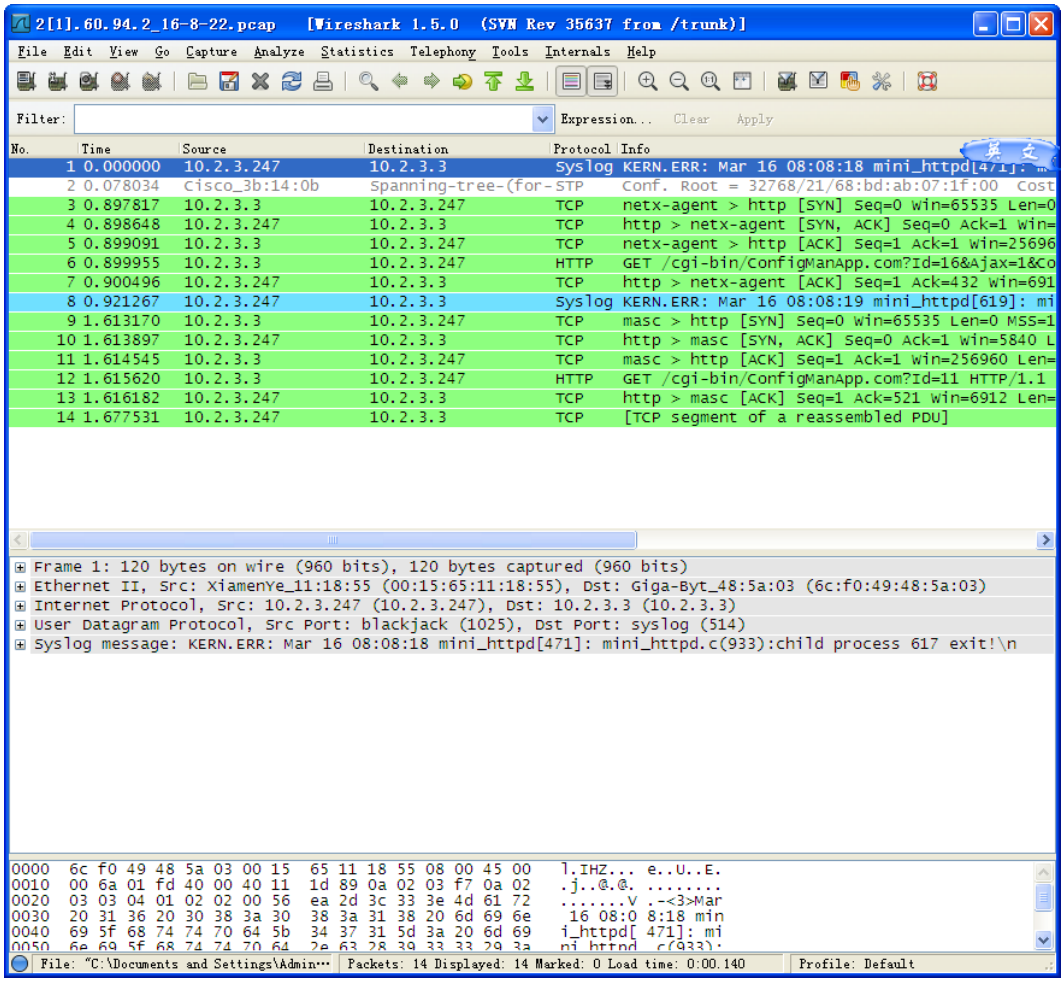
Figure 6-6 PCAP Trace area



3. Click **Stop**.
4. Click **Export**.
5. Select the path for saving captured network packets.

Use Wireshark to open a captured network packet and view packet information, as shown in Figure 6-7.

Figure 6-7 Viewing a captured network packet



6.1.2 Using a Packet Capture Tool to Capture Packets

Connect an IP phone's network port and a computer to the same hub, and use the packet capture software such as the Sniffer, Ethereal, or Wireshark to capture packets.

You can locate faults quickly by analyzing the captured packets.

For details on how to capture and analyze packets, see 7.7 Wireshark User Guide

6.1.3 How to Obtain Device Information by Observing the Status Indicators and LCD

Status Indicators

Indicators on eSpace 7870, 7850, 7830, 7820 and 7810 include the power supply indicator, message status indicator, account indicator, headset indicator(7810&7820 only have headset key), SCA indicator, and BLF indicator. Table 6-1 lists the status indicators.

Table 6-1 Status indicators

Indicator	Color	Status	Description
Power supply	Green	Steady on	The power supply is connected properly.
		Blinking	The IP phone receives a call, or a call is being muted.
		Steady off	The power supply is disconnected.
Message status indicator	Green	Steady on	There are new messages to the IP phone.
		Steady off	There is no message to the IP phone.
Headset status indicator	Green	Steady on	A headset is used.
		Steady off	No headset is used.
Account indicator	Green	Steady on	The account is occupied.
		Blinking	The account receives or holds a call.
		Steady off	The phone is in the on-hook state.
Line key assigned the SCA function	Green	Steady on	The listened-on account is in the idle state.
		Blinking	The listened-on account is in the occupied state.
		Steady off	The SCA function is disabled.
Line key assigned the BLF function	Green	Steady on	The listened-on account is in the idle state.
		Blinking green slowly	The listened-on account is in the talking state.
		Blinking green quickly	The listened-on account is in the ringing state.
		Steady off	The BLF function is disabled.
Memory key assigned the BLF function	Green	Steady on	The listened-on account is in the idle state.
	Red	Steady on	The listened-on account is in the talking state.
		Blinking	The listened-on account is in the ringing state.
	Green/Red/Orange	Steady off	The BLF function is disabled.

6.1.4 Icons

Table 6-2 lists icons that may occur on the eSpace 7850&7830&7810 screen.

Table 6-2 Icons on the eSpace 7850&7830&7820&7810 screen

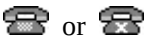
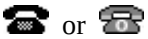
No.	Icon	Description
1		This icon blinks when network connection failed.
2		Indicates that an account failed to be registered.
3		Indicates that an account is being registered.
4		Indicates that an account is registered successfully.
5		Indicates a missed call.
6		Indicates an incoming call.
7		Indicates an outgoing call.
8		Indicates all input methods. To switch input methods, press the key corresponding to this icon.
9		Indicates digital input.
10		Indicates lower-case input.
11		Indicates upper-case input.
12		Indicates that a call is muted.
13		Indicates that a call is held.
14		Indicates a voice message.
15		Indicates that the call forward function is enabled.
16		Indicates that the DND function is enabled.
17		Indicates that the auto answer function is enabled.
18		Indicates the handset mode.
19		Indicates the headset mode.
20		Indicates the handsfree mode.

Table 6-3 lists icons that may occur on the eSpace 7870 screen.

Table 6-3 Icons on the eSpace 7870 screen

No.	Icon	Description
1		This icon blinks when network connection failed.
2		Indicates that an account failed to be registered.
3		Indicates that an account is being registered.
4		Indicates that an account is registered successfully.
5		Indicates a missed call.
6		Indicates an incoming call.
7		Indicates an outgoing call.
8		Indicates a missed call.
9	2aB	Indicates all input methods. To switch input methods, press the key corresponding to this icon.
10	123	Indicates digital input.
11	abc	Indicates lower-case input.
12	ABC	Indicates upper-case input.
13		Indicates that a call is muted.
14		Indicates that a call is held.
15		Indicates a voice mailbox.
16		Indicates that the call forward function is enabled.
17		Indicates that the DND function is enabled.
18		Indicates that the auto answer function is enabled.
19		Indicates the handset mode.
20		Indicates the headset mode.
21		Indicates the hand-free mode.
22		Indicates that the volume is 0.
23		Indicates that the recording function fails to be enabled.
24		Indicates that the recording function fails to be disabled.

No.	Icon	Description
25		Indicates that the recording memory is full.
26		Indicates that recording fails.
27		Indicates that recording is ongoing.
28		Indicates that the VPN function is started.
29		Indicates the keyboard lock mode.
30		Indicates that there is an ongoing conference.
31		Indicates the image of a called party.

Table 6-4lists the icons corresponding to the functions that are specified for account indicators. The icons are displayed on eSpace 7870's screen.

Table 6-4 Icons corresponding to the functions that are specified for account indicators

No.	Icon	Description
1		Indicates that an account indicator is set to implement a function other than line indicator, BLF, speed dial, or remote group.
2		Indicates that an account indicator is set as the BLF indicator, but the setting fails.
3		Indicates that an account indicator is set as the BLF indicator and the listened-on account is idle.
4		Indicates that an account indicator is set as the BLF indicator and the listened-on account is in the ringing state.
5		Indicates that an account indicator is set as the BLF indicator and the listened-on account is in the talking state.
6		Indicates that an account indicator is set to implement the speed dial function.
7		Indicates that an account indicator is set to implement the remote group function.

6.2 Common Faults and Fault Analysis

6.2.1 How to Obtain the MAC Address When the IP Phone Is Powered Off

You can obtain the MAC address in any of the following ways:

- The MAC address of an IP phone is pasted in the rear of the IP phone.
- According to the corresponding PO, you can ask the provider to provide the delivery information table that contains the MAC address.
- MAC addresses of all the IP phones are listed in the label on the large package box of the IP phone.
- The MAC address of an IP phone is pasted on the small package box of the IP phone.

6.2.2 An IP Phone Cannot Obtain an IP Address

Symptom

The icon  and the message "Network Unavailable" are displayed.

Cause

- A network cable is connected to the PC port of the IP phone.
- The network cable is disconnected from the IP phone.
- The network cable is damaged.
- Network parameter settings are incorrect, for example, the static IP address is unavailable.
- The network connection is abnormal.

Troubleshooting

- Verify that the network cable is connected to the network port.
- Verify that the network cable is intact and the connection is normal.
- Verify that network parameters such as IP addresses are correct.
- Verify that the network connection is normal. For example, the DHCP server is running properly and has available IP addresses, and DHCP servers do not conflict in a LAN.

6.2.3 IP Addresses of an IP Phone and Another Device Conflict

Symptom

The message "IP conflict" is displayed on an IP phone's LCD.

Cause

The static IP address of an IP phone conflicts with the IP address assigned by the DHCP server.

Troubleshooting

Set the IP address of the IP phone to an available value.

6.2.4 IP Phone Can Make Calls But Cannot Receive Calls

Symptom

An IP phone can make calls but cannot receive calls.

Cause

When the DND function is enabled, incoming calls are rejected.

Troubleshooting

If the DND icon is displayed on the IP phone's LCD, the DND function is enabled.

When eSpace 7810 is in the standby state, press the **Menu** soft key, select **Features**, and press **Enter**. Then select **DND** and press **Enter**. Press the left or right arrow key to select **Disabled**, and press the **OK** key.

When eSpace 7870, eSpace 7850, eSpace 7830 and eSpace 7820 is in the standby state, press the **DND** soft key to disable the DND function.

6.2.5 IP Phone Cannot Make and Receive Calls

Symptom

- The message "No service" is displayed on an IP phone's LCD.
- The  or  icon is displayed on an IP phone's LCD.
- When an IP phone's circuit board is changed, the blank screen (eSpace 7820/eSpace 7830/eSpace 7850) or full-screen characters (eSpace 7810) or red screen (eSpace 7870) are displayed, and the account indicator and message indicator are blinking (eSpace 7810/ eSpace 7820/eSpace 7830). Then the page is displayed normally and accounts can be registered, but the IP phone cannot make or receive calls.

Cause

- No account is registered.
- Account registration fails.
- The MAC address is not burned or an incorrect MAC address is burned after the circuit board is changed in the IP phone.

Troubleshooting

- Verify that an account has been registered.
- Verify that account information is correct and complete.
- Use a burning tool to burn the MAC address listed in the label on the rear of the IP phone to the new circuit board.

6.2.6 Causes of Crosstalk

- The MAC address of the IP phone conflicts, which has a small possibility.
- Sessions are not synchronized to the lower-level NAT and firewall when the SBC is used.

6.2.7 An IP Phone Rings but You Cannot Hear the Peer End When Picking Up the IP Phone

Symptom

An IP phone rings when receiving a call, but you cannot hear the peer end when picking up the IP phone.

Cause

This fault occurs when signaling messages can be transmitted but media streams cannot be transmitted. Signaling messages are transmitted by a server and media streams are transmitted from end to end.

In the case of unidirectional communication on the IP Phone network, you can make a call on a specified trunk circuit to locate the cause (upper-level office fault or internal office fault).

If no fault is found on all the trunk circuits, check the internal office fault. In the case of unidirectional communication in the internal office, you can use the packet capture tool to analyze whether the network setting is correct. The internal office fault may be the hardware or software fault.

- Hardware faults can be often detected. A fault occurs in an office direction or a fault often occurs. To locate a hardware fault, attempt to replace the hardware for testing, such as switching the MCU and replacing the trunk board or terminal. The overall principle is to trace the call where a fault occurs, make a summary of fault occurrence, eliminate possible causes one by one, and locate the actual cause.
- To locate a software fault, trace the call information when the fault occurs step by step and describe the scenario and recurrence conditions. Then send the information to the R&D personnel for further analysis.

Troubleshooting

- Media streams cannot be transmitted.
- The IP phone or headset is connected to an incorrect port. The headset ports of eSpace 7810, 7820, 7830, 7850 and 7870 use RJ-9 and the IP phone ports also adopt RJ-9.
- If RTP encryption is enabled on an IP phone but encryption is disabled on the peer end, unidirectional communication may occur. Verify that RTP encryption is enabled or disabled both on the two ends.

6.2.8 An IP Phone Cannot Obtain Time Information from the NTP Server

Symptom

When a computer functions as the NTP server, the IP phone cannot obtain time information.

Cause

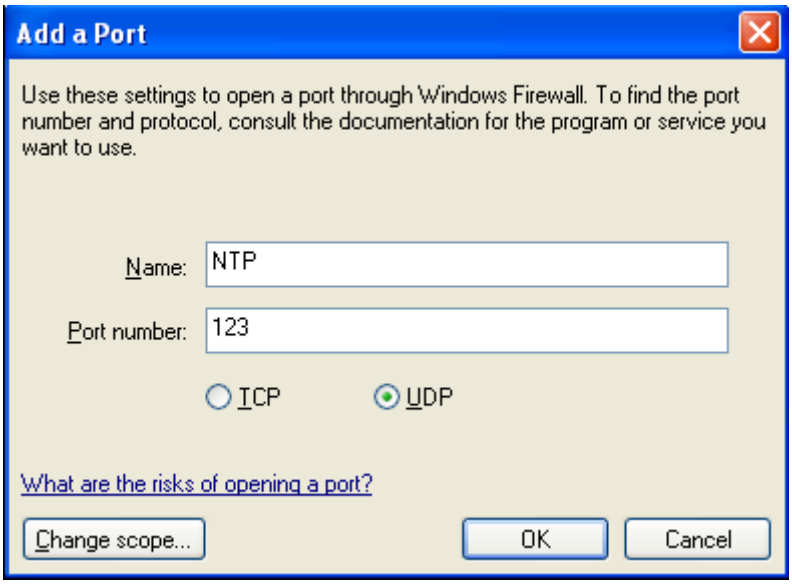
The firewall is installed on the computer; therefore, NTP packets sent by the IP phone are intercepted.

Troubleshooting

You can use either of the following methods to rectify the fault:

- Disable the firewall on the computer.
- Add a rule, which allows NTP packets to pass through the firewall. In the **Add a Port** dialog box, set **Port number** to **123** (a port number frequently used by the NTP server), select **UDP**, and set **Name** to any value, as shown in Figure 6-8.

Figure 6-8 Add a Port dialog box



6.2.9 Voices on an IP Phone Are Intermittent

Symptom

Voices on an IP phone are intermittent.

Cause

This fault is caused by packet loss or jitter.

- Packet loss is caused by network congestion or insufficient device capabilities.
- Jitter is caused by packet assembling on the transmitting device or receiving device, such as the timeout processing, retransmission mechanism, and insufficient buffer.

Troubleshooting

- Improve the network quality.

- Change the IP phone codec. Generally, the default codec of an IP phone is G.711 A-law/μ-law. If the network quality is low, you can set the codec to G.729AB or G.723.1.

6.2.10 Failed to Upgrade an IP Phone

Symptom

After an IP phone is upgraded, its firmware version does not change.

Cause

- The target firmware version is the same as the source firmware version.
- The target firmware version does not match the phone model.
- The source firmware or target firmware is protected by software.

Troubleshooting

Select a correct version to upgrade. The version formats for different IP phone models are as follows:

- For eSpace 7870, the version format is 38.x.x.x.
- For eSpace 7850, the version format is 2.x.x.x.
- For eSpace 7830, the version format is 6.x.x.x.
- For eSpace 7820, the version format is 7.x.x.x.
- For eSpace 7810, the version format is 9.x.x.x.

7 Appendix

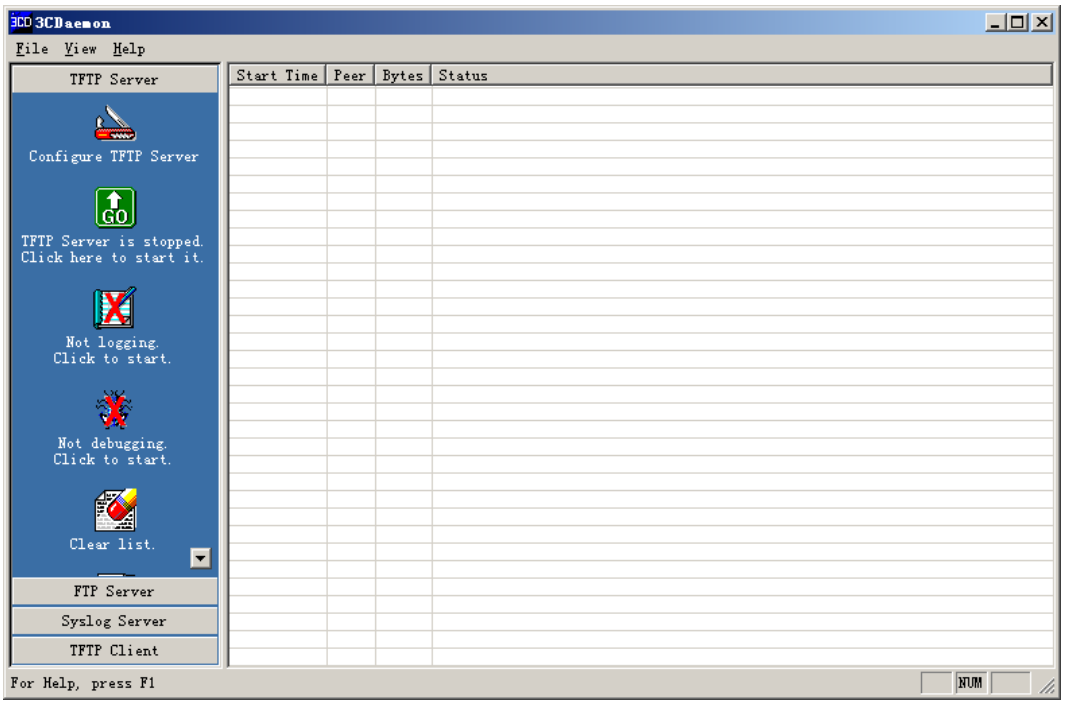
7.1 Configuring the TFTP Server (3CDaemon TFTP Server for Example)

NOTE

The TFTP server does not need to be installed. Download the TFTP server from the official website.

1. Start the TFTP server, as shown in Figure 7-1.

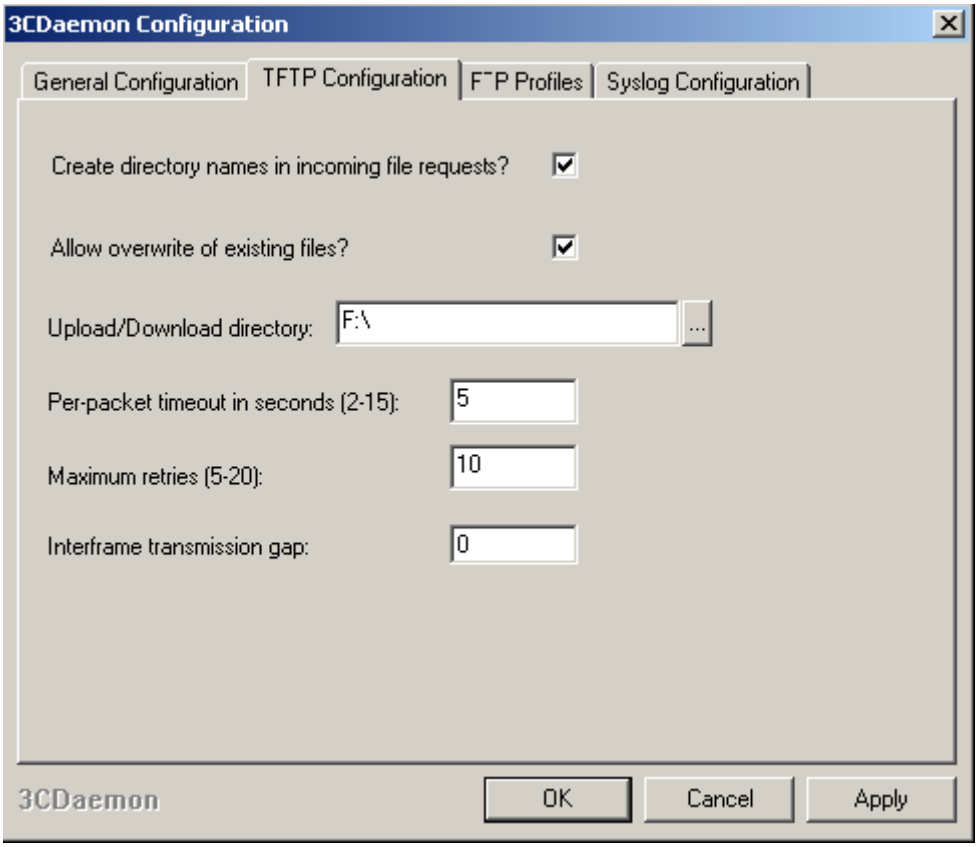
Figure 7-1 TFTP server main page



2. Click **Configure TFTP Server** under **TFTP Server**.

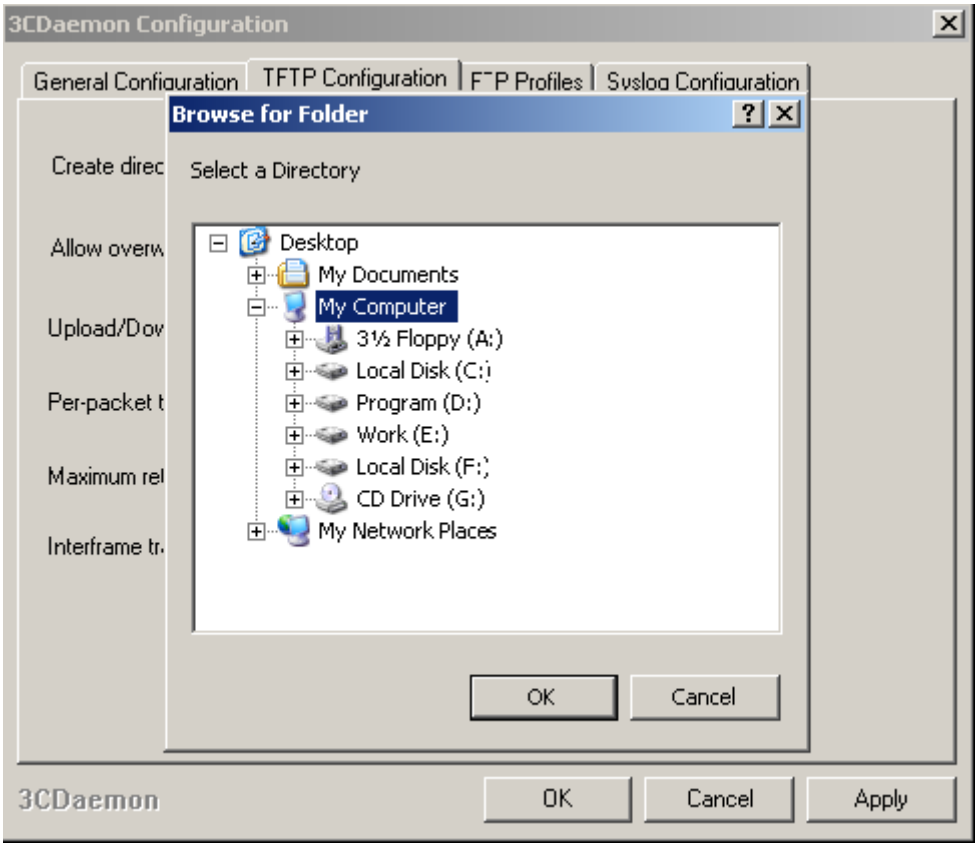
   A dialog box is displayed, as shown in Figure 7-2.

Figure 7-2 3CDaemon Configuration dialog box



3. Click the **TFTP Configuration** tab. On the tab page, click the  button corresponding to **Upload/Download**, and select a directory for storing uploaded files, as show in Figure 7-3.

Figure 7-3 Selecting a directory for storing uploaded files



7.2 Setting Up the HTTP Server

You can use an Apache or Windows Internet Information Service (IIS) server for setting up the HTTP server.

Stopping and Disabling Windows IIS

Stop and disable Windows IIS when you use the Apache server because they are incompatible.

- Method 1: Choose **Start** > **Control Panel** > **Management Tool** > **Service**.

  In the window that is displayed, stop and disable Windows IIS.

- Method 2: Right-click  and choose Open Apache Monitor.

  In the **Apache Service Monitor** window that is displayed, click **Services**, and stop and disable Windows IIS.

7.2.1 Using the Windows IIS Component

The Windows IIS component can be used to configure the HTTP server. Before the configuration, obtain the Windows operating system installation CD-ROM or the installation package URL and then install the Windows IIS component.

Context

To install the Windows IIS component in the Windows XP operating system, perform the following steps:

Procedure

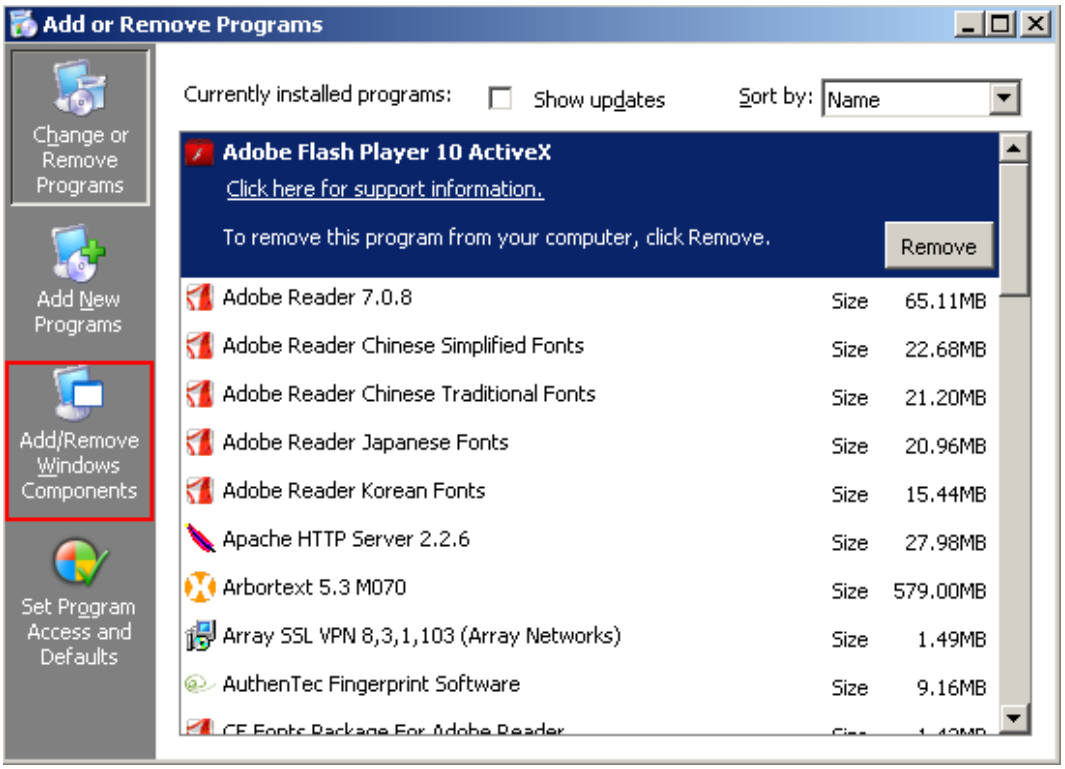
Step 1 Choose **Start** > **Control Panel**.

The **Control Panel** window is displayed.

Step 2 Double-click **Add or Remove Programs**.

The **Add or Remove Programs** window is displayed, as shown in Figure 7-4.

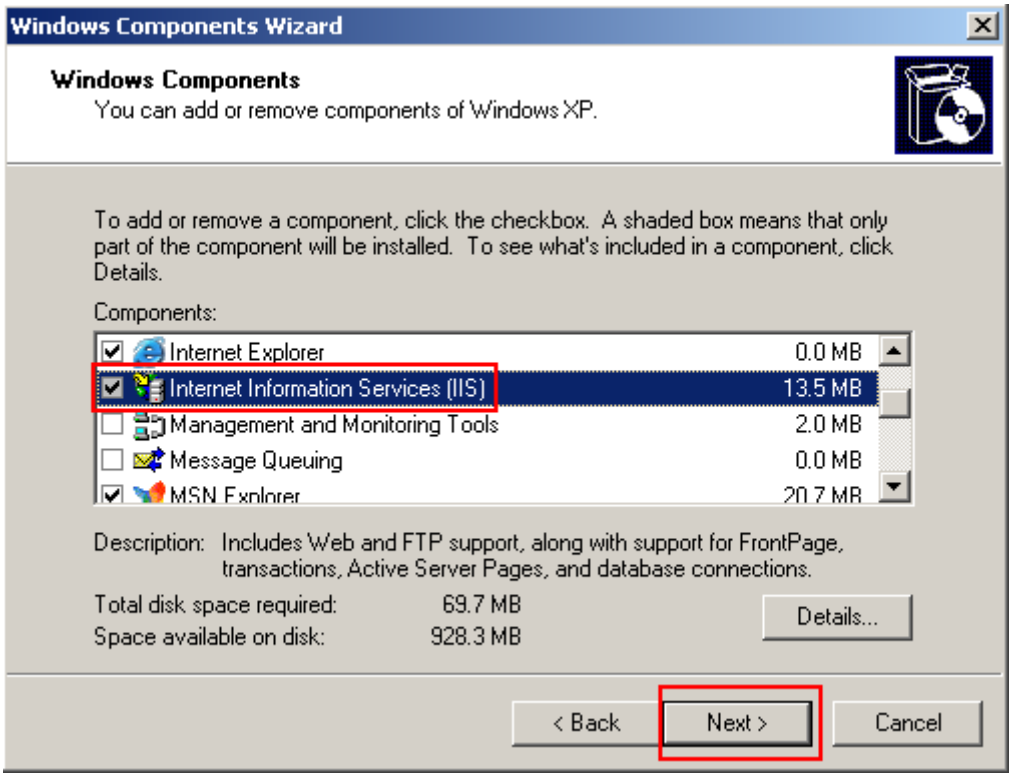
Figure 7-4 Add or Remove Programs window



Step 3 Click **Add/Remove Windows Components** in the left pane.

The **Windows Components Wizard** window is displayed, as shown in Figure 7-5.

Figure 7-5 Windows Components Wizard window



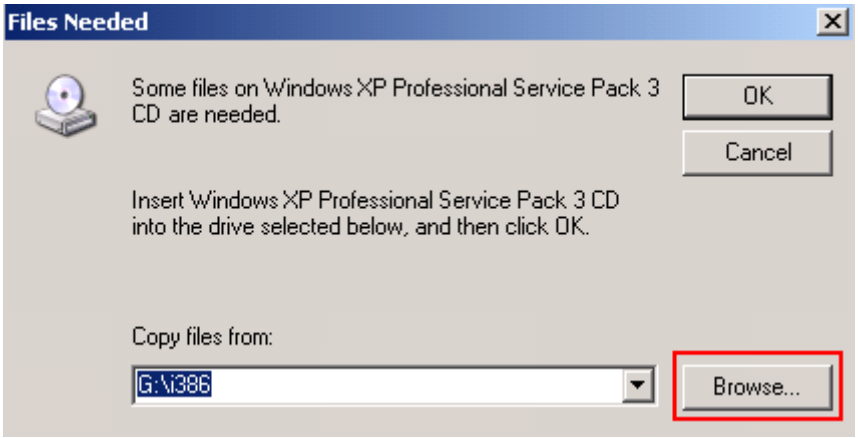
Step 4 Select the **Internet Information Services (IIS)** check box in the **Components** area and click **Next**.

The system displays a window asking you to insert the installation CD-ROM before the installation is started.

Step 5 Insert the installation CD-ROM, and click OK.

The Files Needed dialog box is displayed, as shown in Figure 7-6.

Figure 7-6 Files Needed dialog box

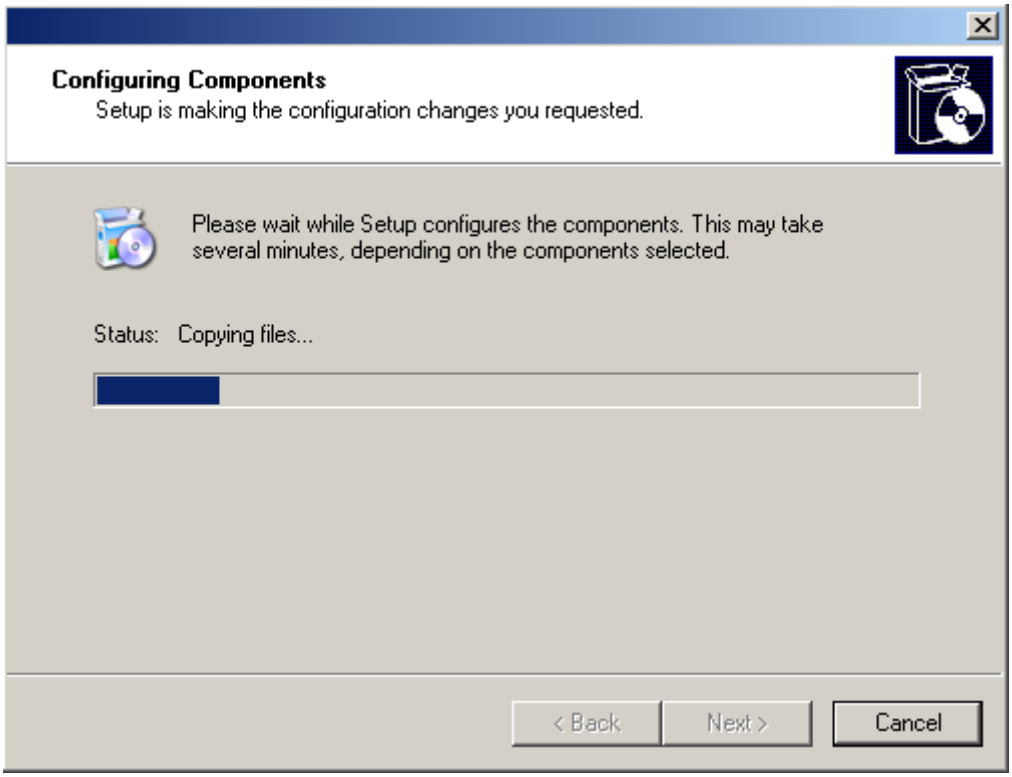


Step 6 Click **Browse** and set **Copy files from** to **G:\i386**.

Step 7 Click OK.

The system starts copying the files and installing the component, as shown in Figure 7-7.

Figure 7-7 Configuring Components dialog box



After the installation is complete, the dialog box automatically exits. You can check for the IIS component in **Control Panel**.

Step 8 h. After the installation is complete, store the version files and configuration file in the root directory **C:\Inetpub\wwwroot**.

----End

7.2.2 Using the Apache Server

You can obtain the Apache server installation software at **http://httpd.apache.org** and install the Apache server based on the installation wizard.

Context

The following uses Apache HTTP Server2.2 as an example in the Windows XP operating system.

Procedure

Step 1 Start the Apache server.Choose **Start** > **All Programs** > **Apache HTTP Server 2.2** > **Monitor Apache Servers**.

- If  is displayed on the taskbar, the Apache server has been stopped.
- If  is displayed on the taskbar, the Apache server is running. You can directly perform 3.

NOTE

You can enter **http://127.0.0.1** in the address box of Internet Explorer. If "It works!" is displayed, the Apache server is running.

Step 2 Start the Apache server. You can start the Apache server in either of the following ways:

- Click  and choose Start.
- Right-click  and choose **Open Apache Monitor**.

  In the **Apache Service Monitor** window that is displayed, click **Start**.

Step 3 Save the required files in the root directory of the Apache server. The default path is **C:\Program Files\Apache Software Foundation\Apache2.2\htdocs**.

- If the required files are placed directly in the root directory, enter the address in the format of http://IP address of the PC where the Apache server is installed to access the Apache server. For example, http://192.169.1.51.**http://192.169.1.51**.
- If the required files are placed under a subfolder of the root directory, enter the address in the format of http://IP address of the PC where the Apache server is installed/subfolder name to access the Apache server. For example, **http://192.169.1.51/filename**.

NOTE

You can change the root directory of the Apache server as required.

Open the httpd.conf file in **C:\Program Files\Apache Software Foundation\Apache2.2\conf\httpd.conf**, and change the path **C:/Program Files/Apache Software Foundation/Apache2.2/htdocs**, for example, change the path to **D:/upgrade/eSpace8850**.

----End

7.3 Guidelines for Setting Up the DNS Server

This document takes the DNS Server preinstalled in the Window 2003 Server for example to describe the procedure for setting up the DNS server.

Starting the DNS Service

Choose **Start** > **Programs** > **Administrative Tools** > **DNS** .

CAUTION

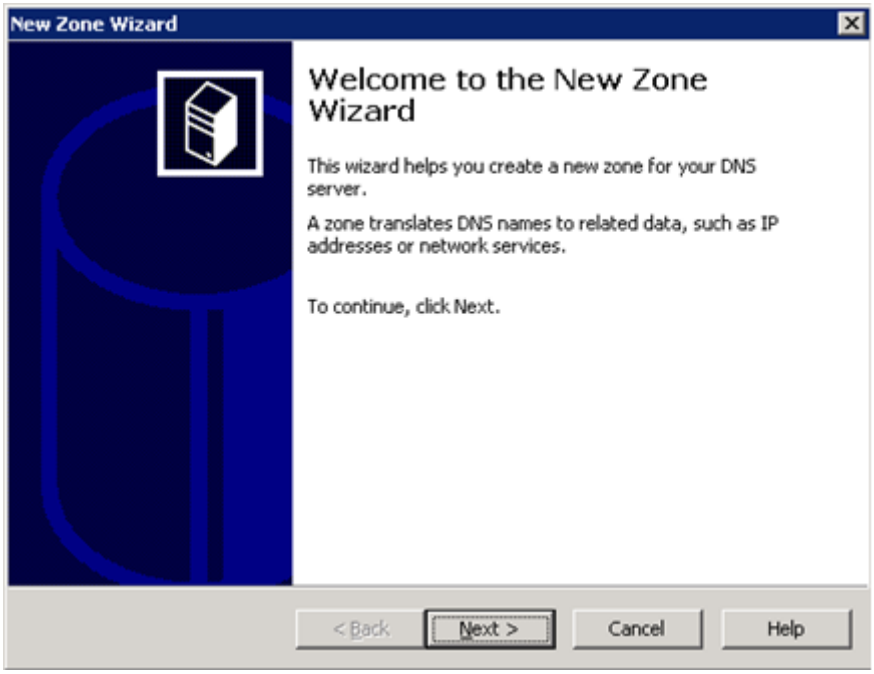
If the DNS service is not installed on the PC, install the DNS component firstly.

Creating a Zone

To create a zone, do as follows:

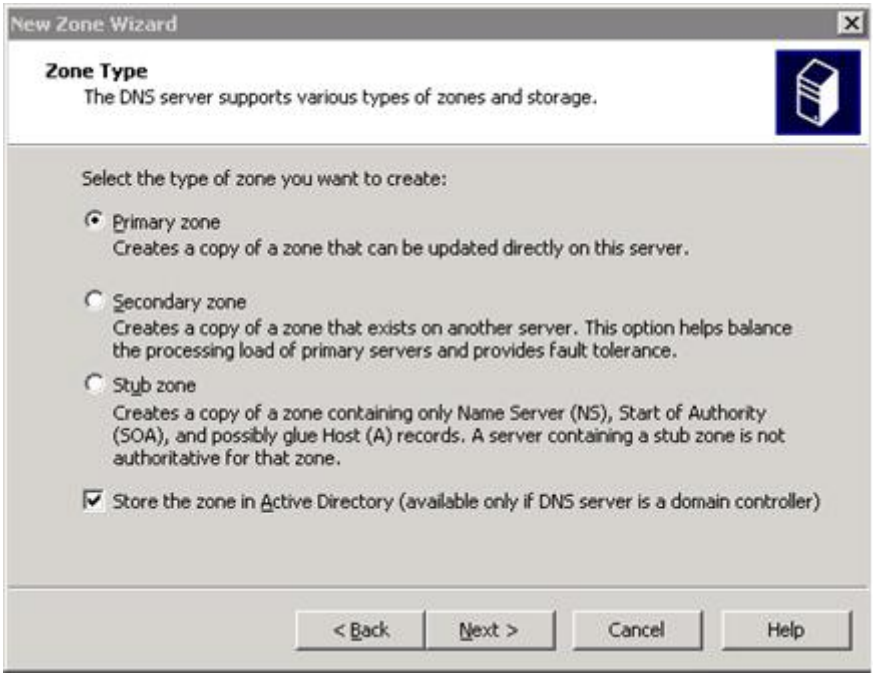
Step 1 Right click **Forward Lookup Zones**, and then choose **New Zone** to start **New Zone Wizard**.As shown in Figure 7-8.

Figure 7-8 New Zone Wizard



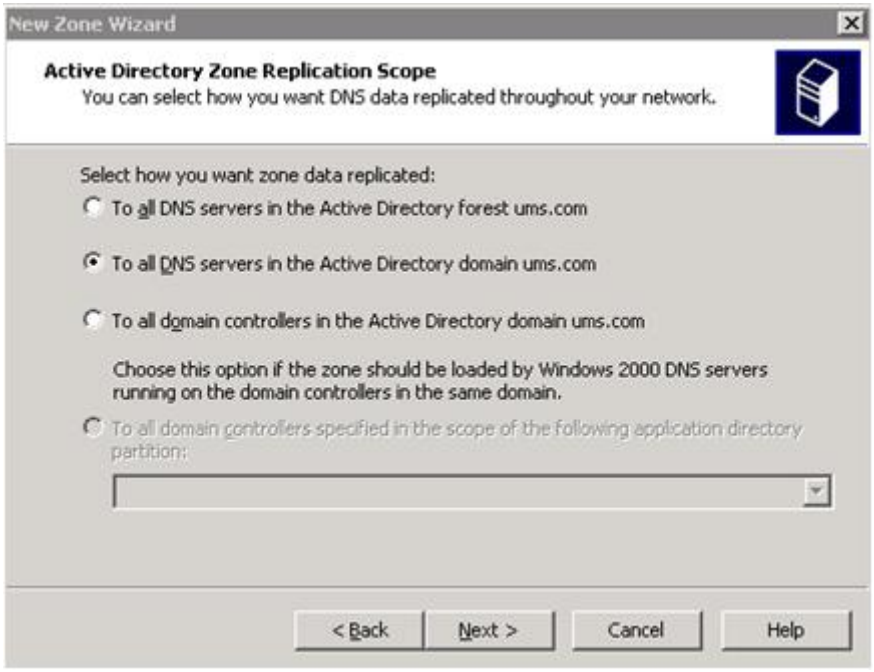
Step 2 Click **Next**, and then select **Primary zone** to create a primary zone.As shown in Figure 7-9.

Figure 7-9 Zone Type



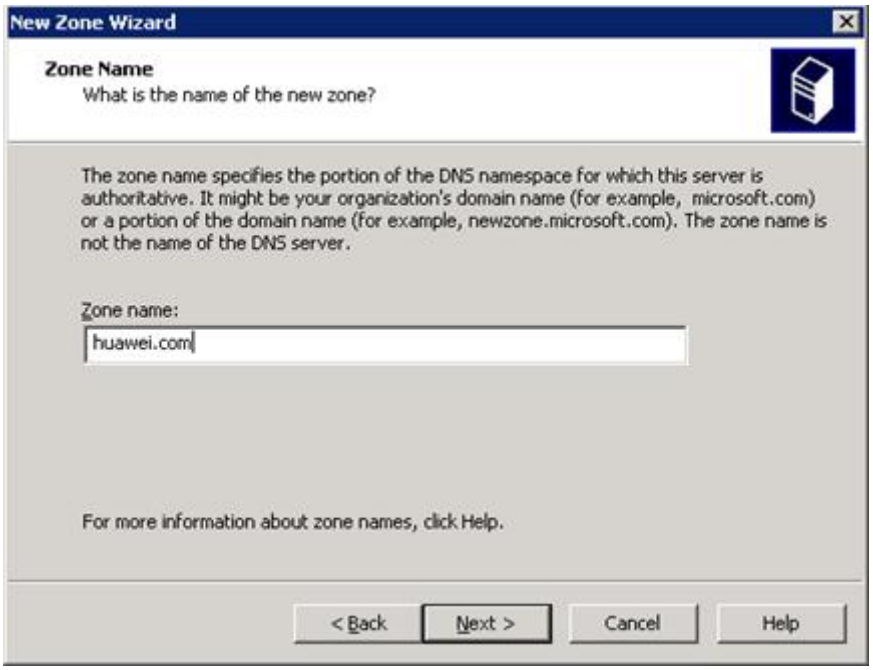
Step 3 Select an option for Select how you want zone data replicated, and click **Next**.As shown in Figure 7-10.

Figure 7-10 Active Directory Zone Replication Scope



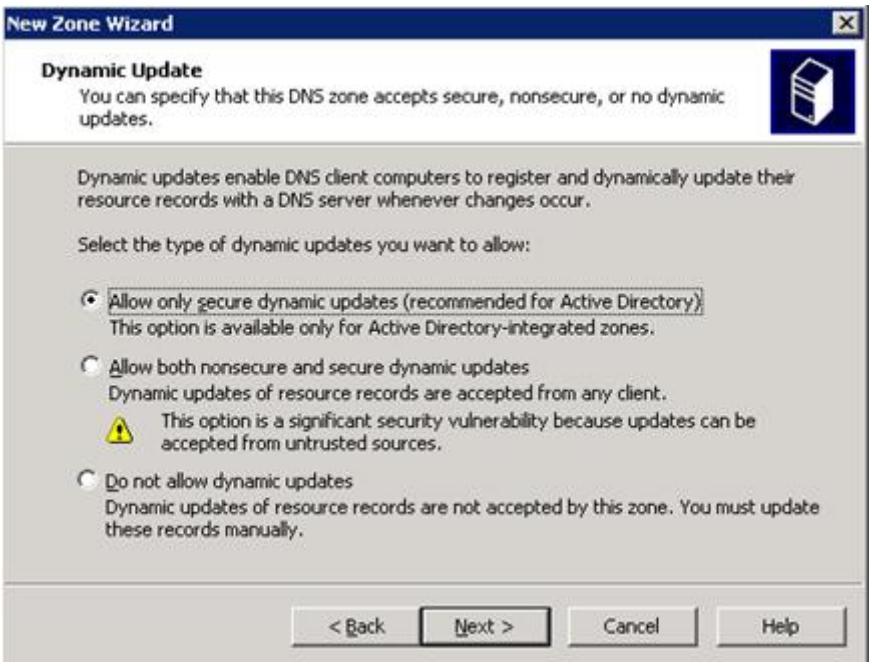
Step 4 Enter the name of the DNS zone, for example, huawei.com. Then click **Next**.As shown in Figure 7-11.

Figure 7-11 Zone Name



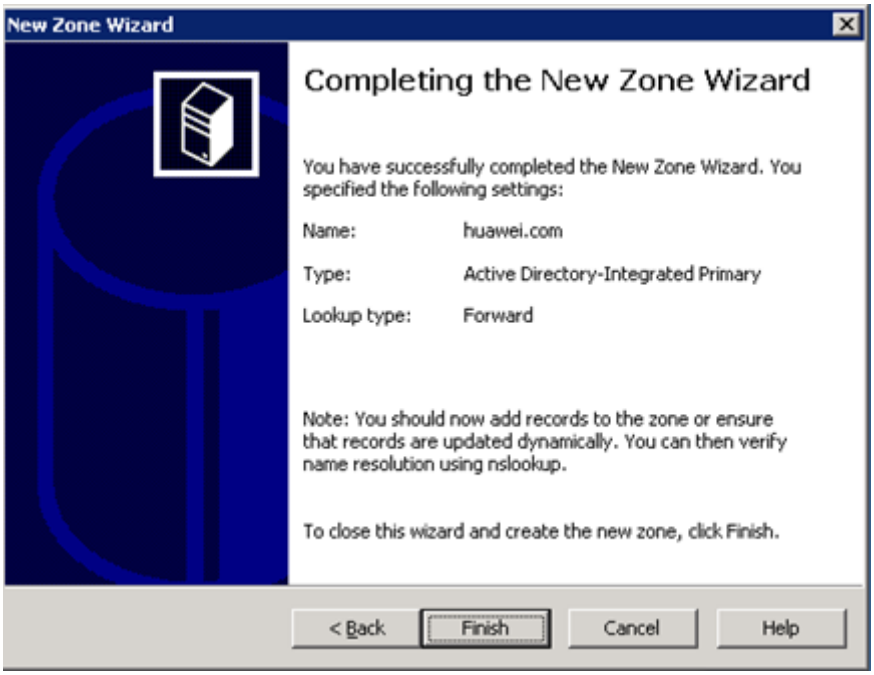
Step 5 Select a dynamic update type, and then click **Next**.As shown in Figure 7-12.

Figure 7-12 Dynamic Update



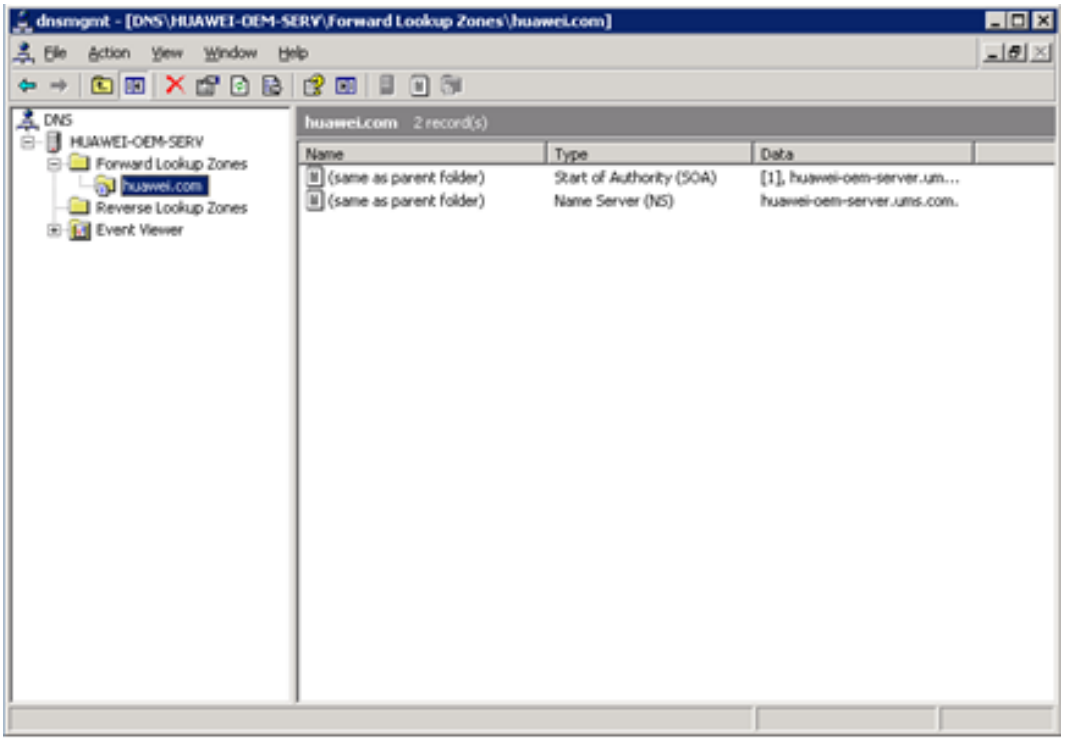
Step 6 After the zone is created, click **Finish**.As shown in Figure 7-13.

Figure 7-13 Finish New Zone Wizard



Step 7 A new zone is displayed.As shown in Figure 7-14.

Figure 7-14 New Zone



Step 8 Click the zone to display the resource records in detail. You can find that each zone has records **Start of Authority (SOA)** and **Name Server (NS)**, which can be used to determine your DNS server. The SOA indicates the account name that is used.

----End

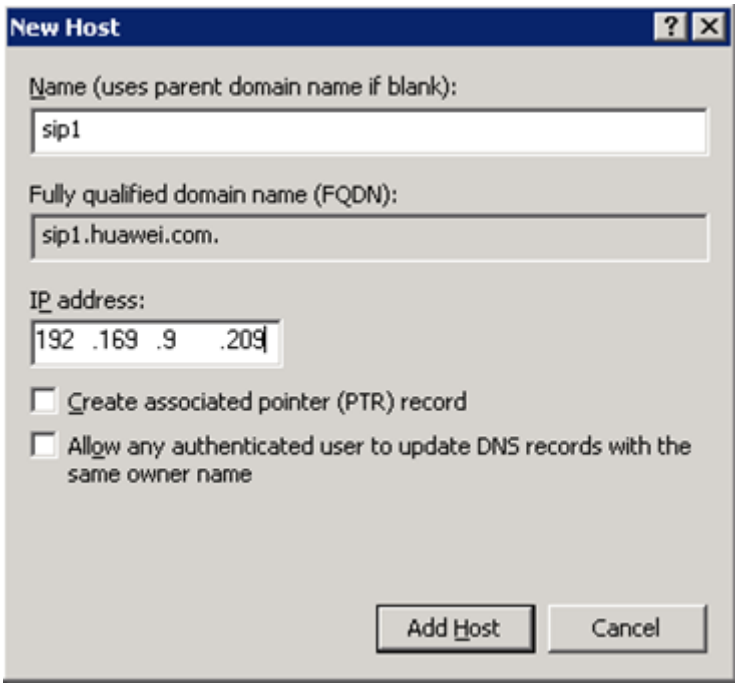
Creating a Record of Type A

A record of Type A provides the mapping between standard host names and IP addresses. In the following figure, Name indicates the host name and the value is the IP address of the host. For example, {relay1.bar.foo com,145.37.93.126,A} is a record of Type A.

To create a record of Type A, do as follows:

Step 1 Right-click **Huawei.com** and choose **New Host(A)**. After setting the host name and IP address, click **Add Host**.As shown in Figure 7-15.

Figure 7-15 New Host



Step 2 Repeat the preceding operation to create multiple records of Type A.

----End

7.4 Setting Up the DHCP Server

7.4.1 Setting Up the DHCP Server in the Window 2003 Server

Basics Concepts

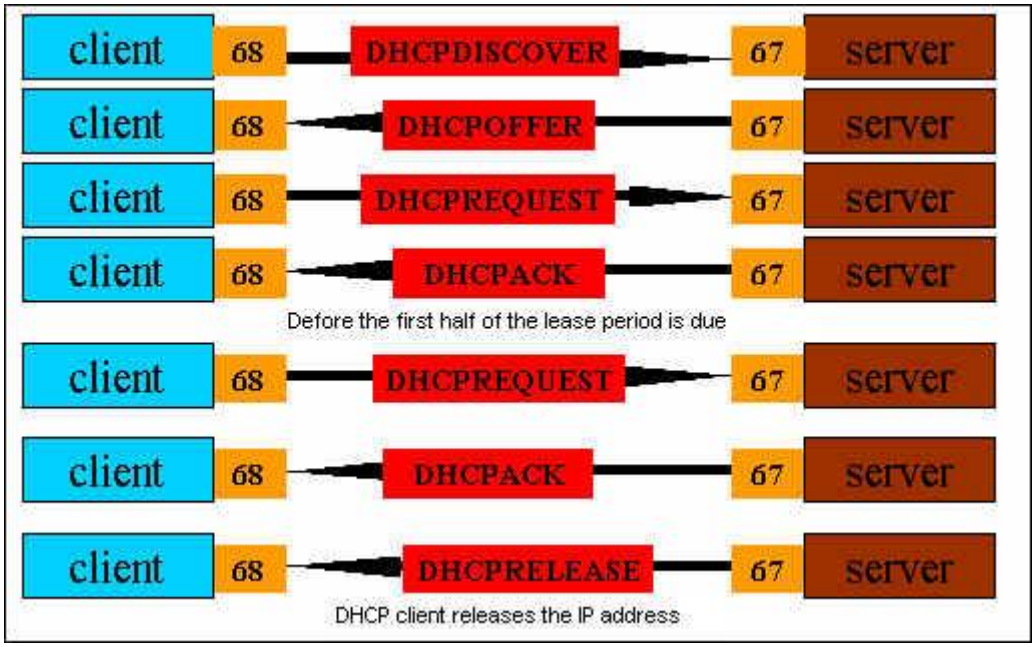
The Dynamic Host Configuration Protocol (DHCP) is mainly used to allocate dynamic IP addresses to terminals on the same network. When DHCP is used, a DHCP server needs to be deployed on the network and IP phones function as DHCP clients.

When a DHCP client sends a request for a dynamic IP address, the DHCP server provides an available IP address and subnet mask for the DHCP client according to the preserved IP address set.

The DHCP has two port numbers, that is, port 67 for the DHCP server and port 68 for the DHCP client. This means that the DHCP client selects only port 68, rather than a temporary port that is not used.

Here, the two ports are selected because a response from the DHCP server can be broadcast. The Figure 7-16 shows the process for an IP phone to obtain the IP address through DHCP.

Figure 7-16 Obtain the IP address through DHCP

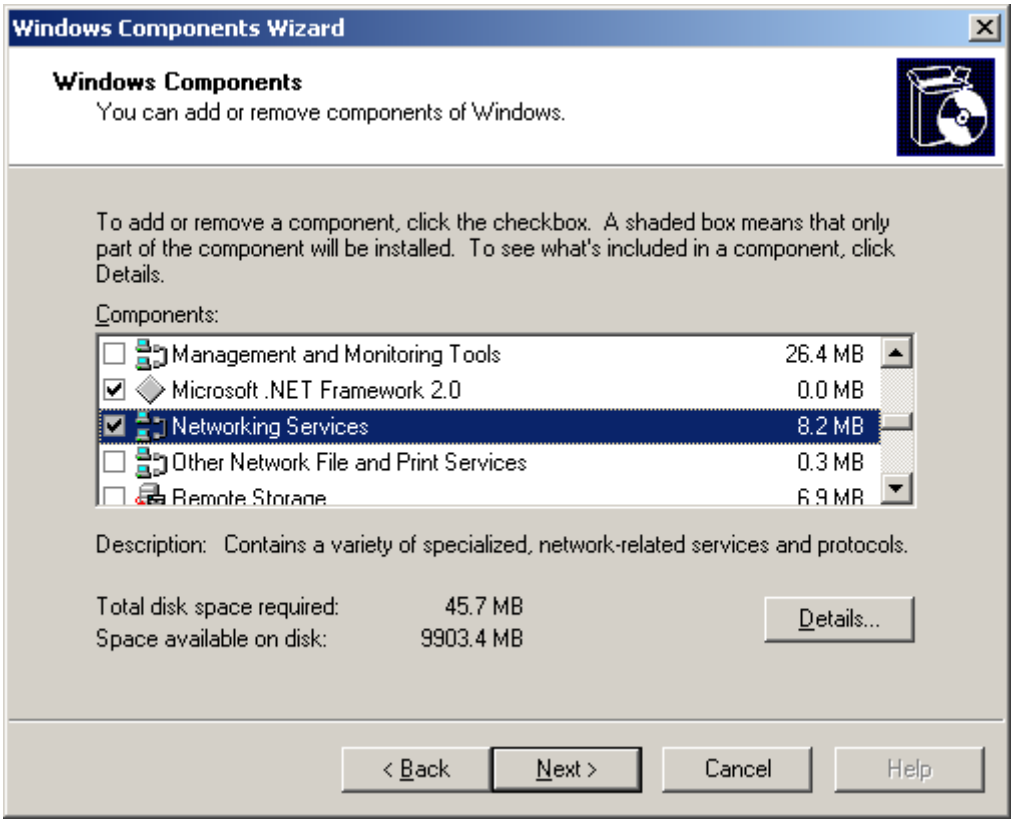


Installing the DHCP Service

Generally, the DHCP service component is installed by default during the installation of the Window 2003 Server. If the DHCP service component is already installed, go to Starting the DHCP Service and Setting DHCP Parameters. If the DHCP service component is not installed, do as follows to install it:

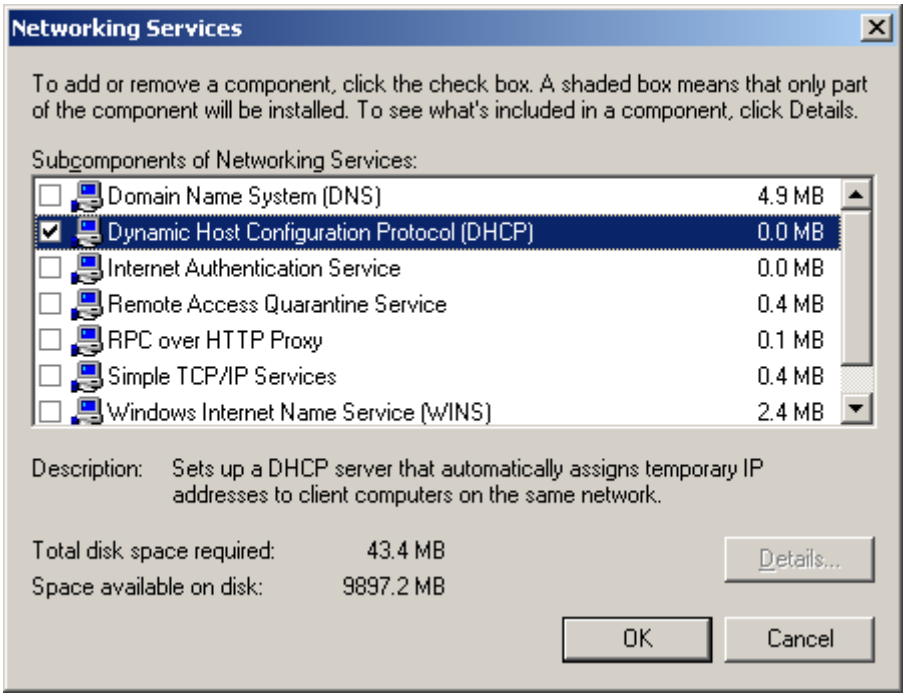
Step 1 Choose **Start** > **Settings** > **Control Panel**, click **Add or Remove Programs**, and click **Add/Remove Windows Components**.The **Windows Components Wizard** dialog box is displayed. as shown in Figure 7-17.

Figure 7-17 Windows Components Wizard



Step 2 Select **Networking Services**, and click **Details** to display the **Networking Services** dialog box. as shown in Figure 7-18.

Figure 7-18 Networking Services



Step 3 Select the DHCP service and click **OK** to exit the page of network service. Click **Next** repeatedly until the installation is complete. After the installation is successful, the dialog box shown in the following figure is displayed. as shown in Figure 7-19.

Figure 7-19 Completing the Windows Components Wizard

----End

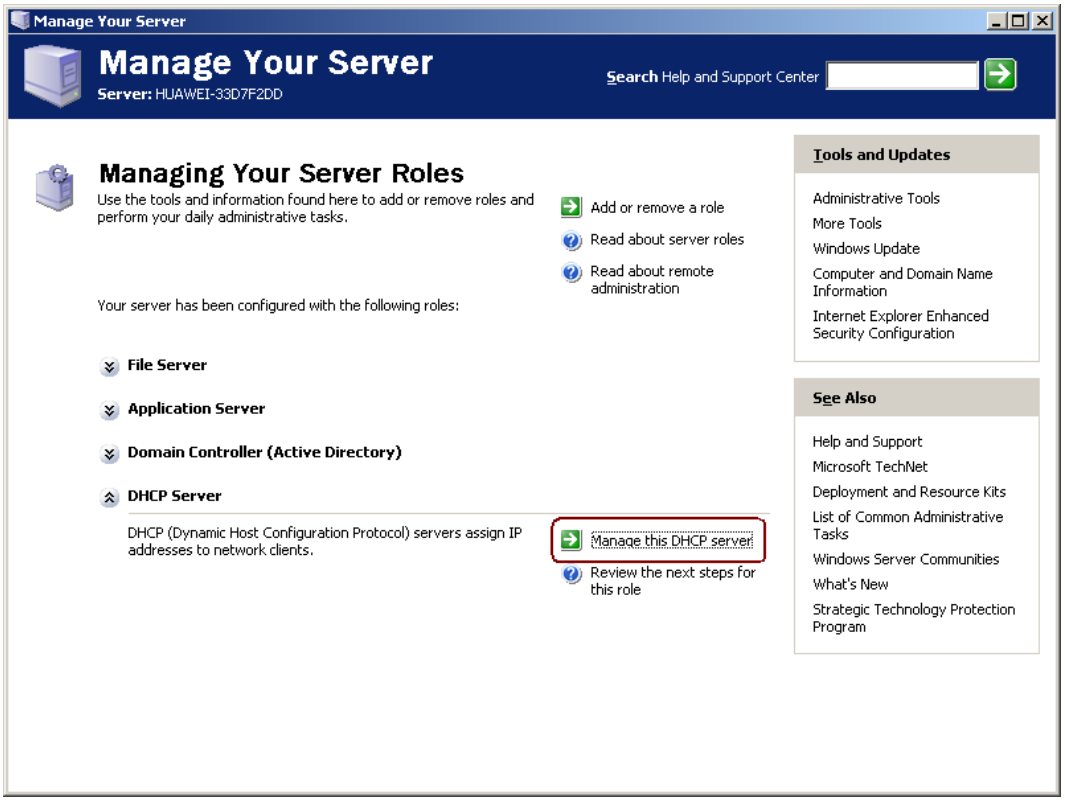
Starting the DHCP Service and Setting DHCP Parameters

After the DHCP service component is installed, do as follows to start the DHCP service:

Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **Manage Your Server**.

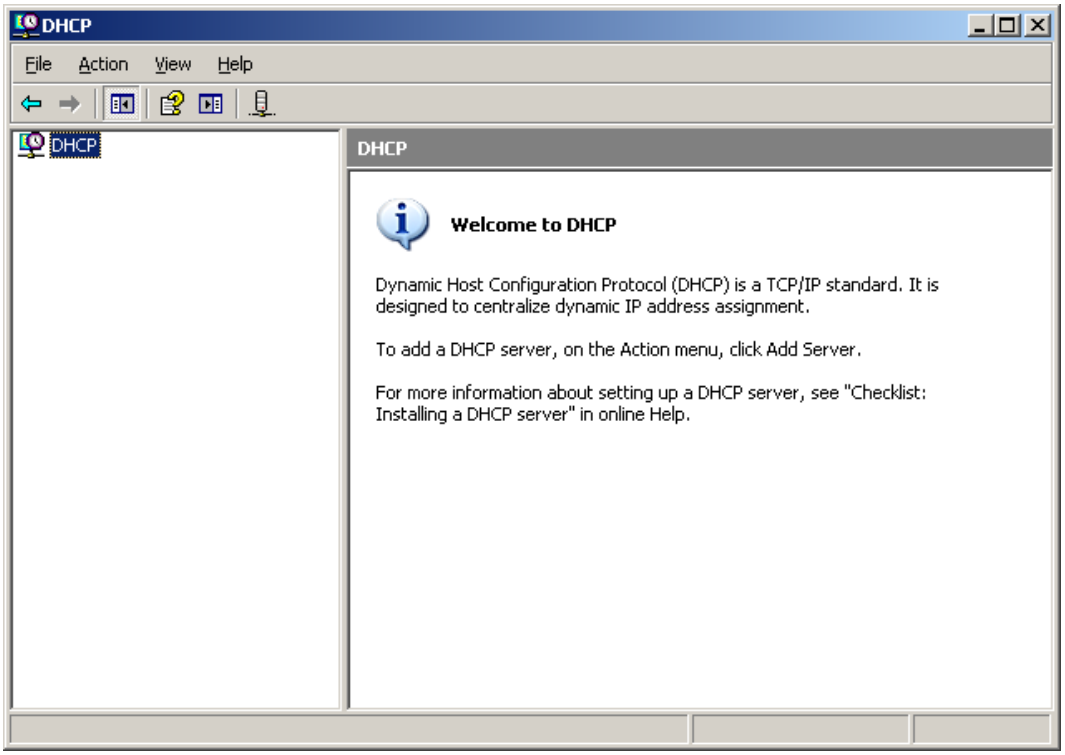
Step 2 In the **Manage Your Server** dialog box that is displayed, select **Manage this DHCP** server. as shown in Figure 7-20.

Figure 7-20 Manage Your Server



Step 3 Enter the main page of the DHCP, as shown in the following figure. as shown in Figure 7-21.

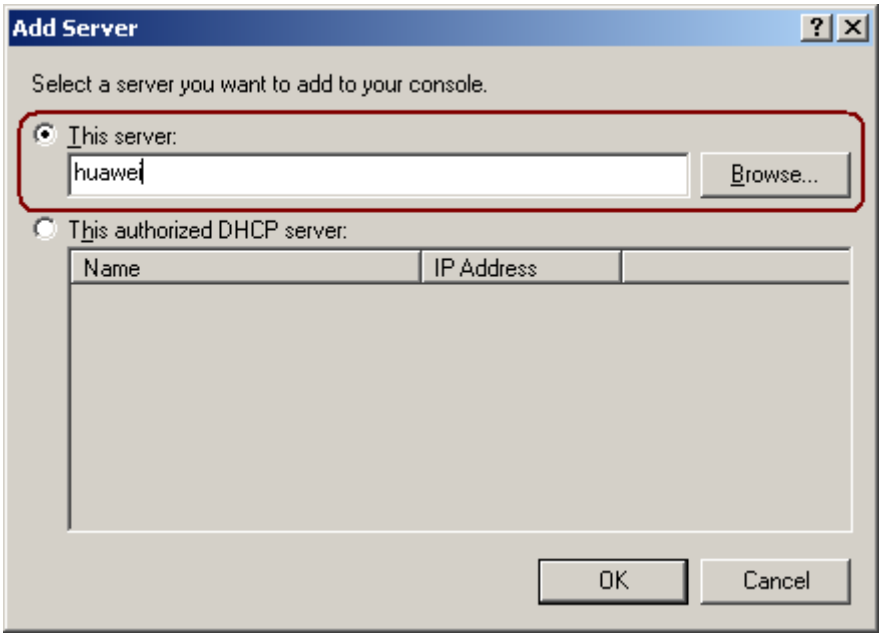
Figure 7-21 The main page of the DHCP



Step 4 Right-click **DHCP** and choose **Add Server**.

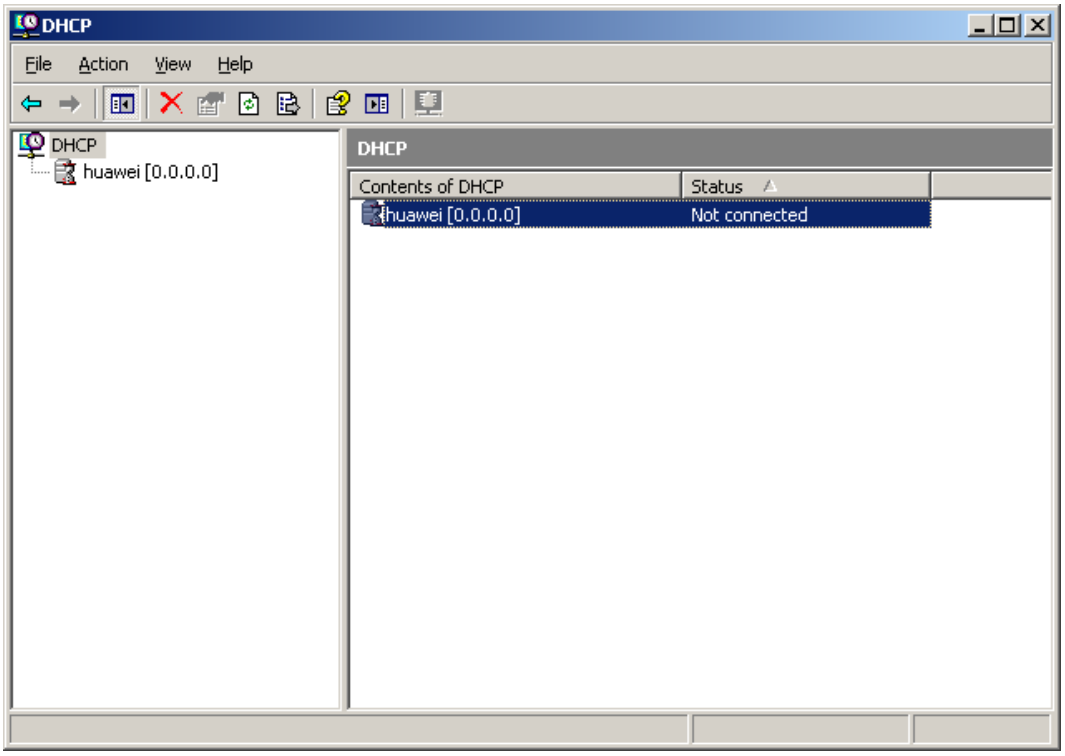
The **Add Server** dialog box is displayed. as shown in Figure 7-22.

Figure 7-22 Add Server



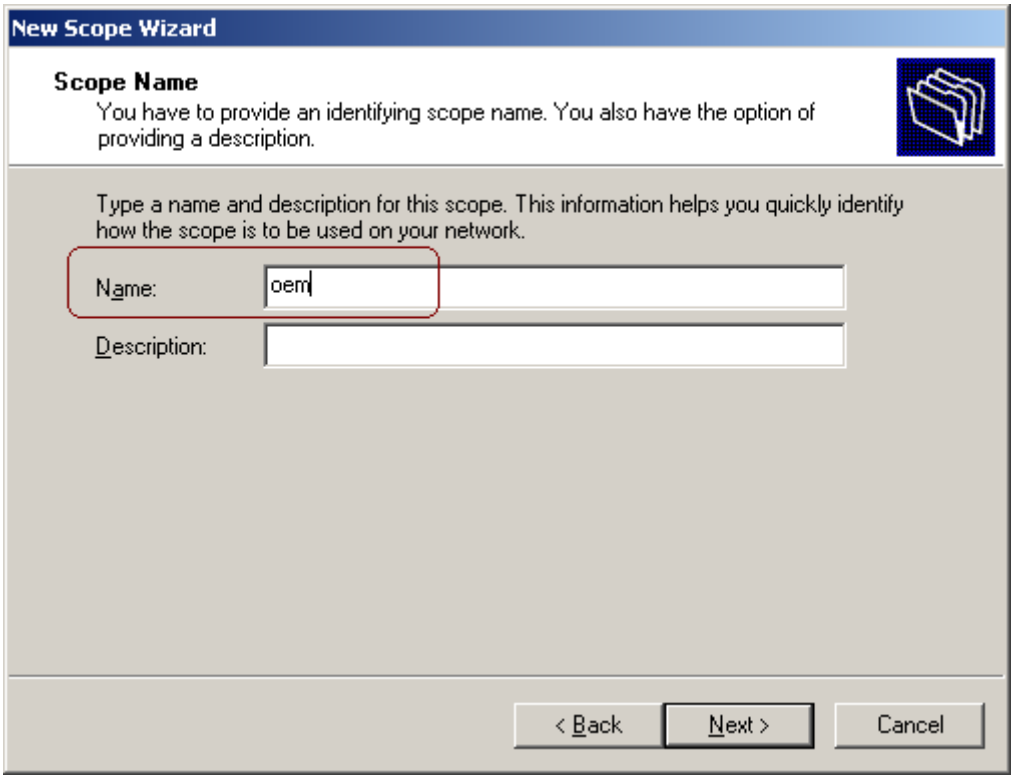
Step 5 Set the name of the DHCP server randomly, and then click **OK**. If the setting is successful, the page shown in the following figure is displayed. as shown in Figure 7-23.

Figure 7-23 Setting Server



Step 6 Right-click **Huawei[10.10.10.2]** and choose **New Scope**. In the **New Scope Wizard** dialog box that is displayed, click **Next**.A dialog box is displayed, as shown in the following figure. as shown in Figure 7-24.

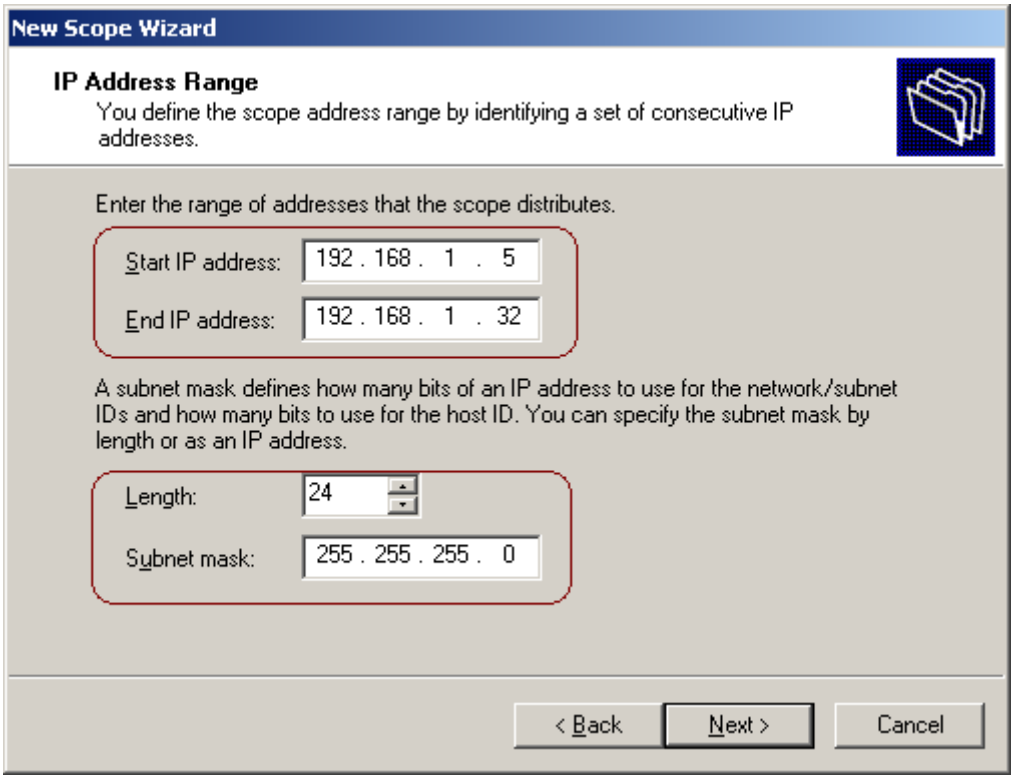
Figure 7-24 New Scope Wizard



Step 7 Set the name of the new function domain randomly, and then click **Next**.

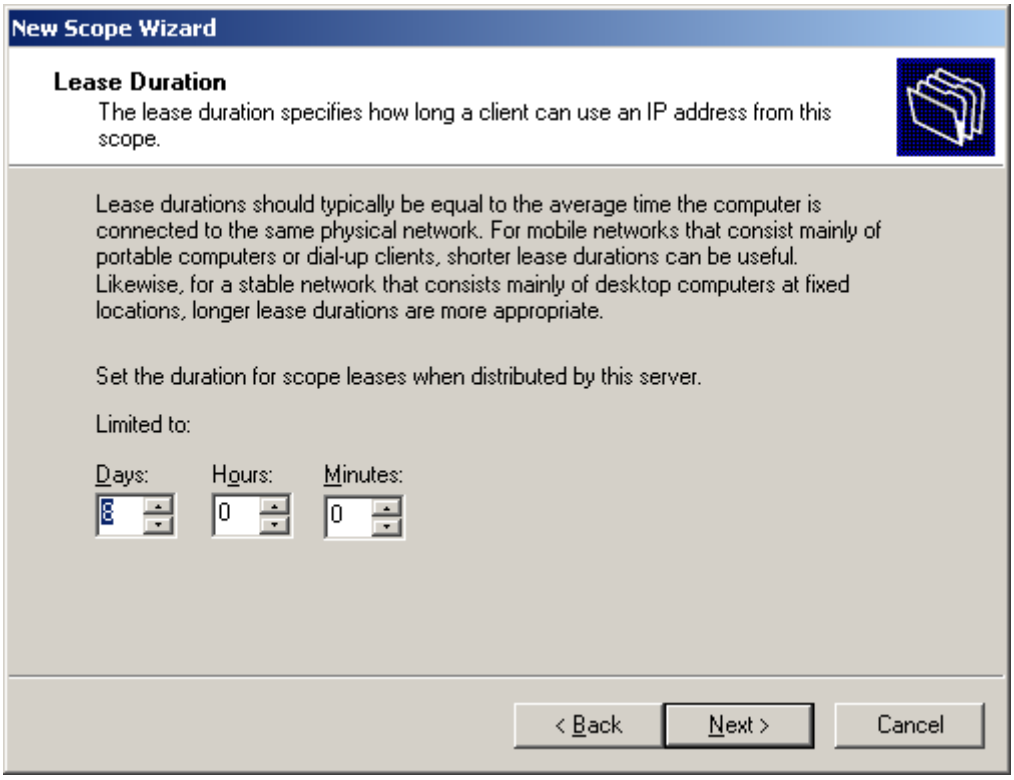
The following dialog box is displayed. as shown in Figure 7-25.

Figure 7-25 Set the name of the new function domain



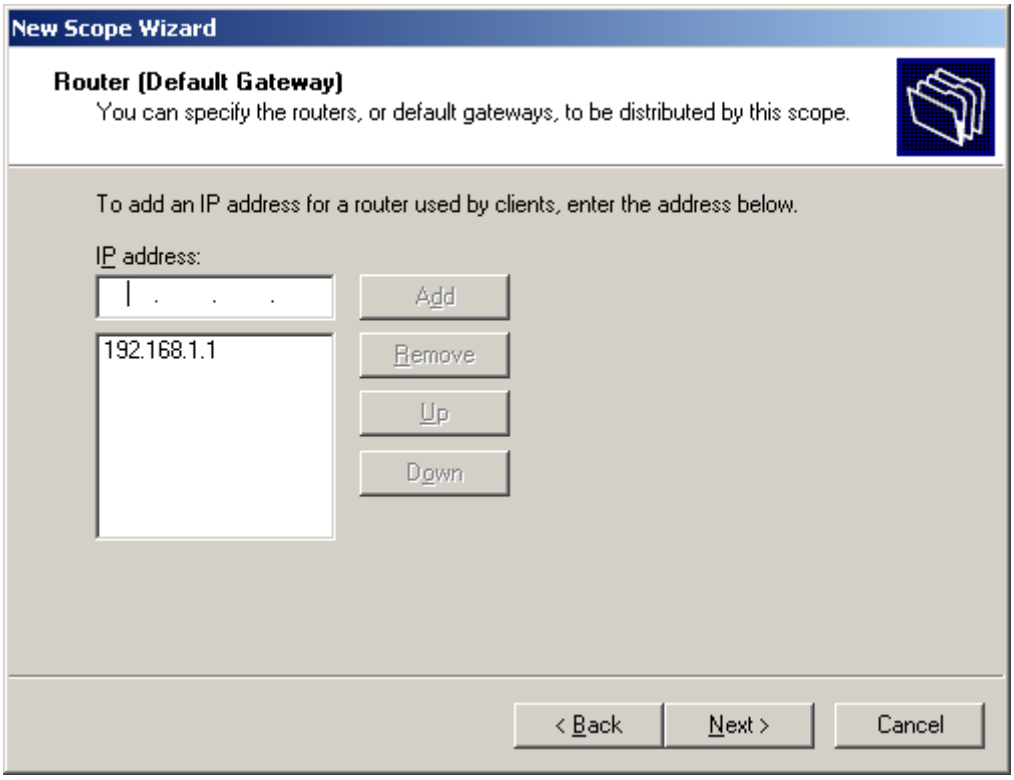
Step 8 In the preceding dialog box, set the start and end IP addresses provided by the DHCP server, and set the subnet mask. Then click **Next** repeatedly until the **Lease Duration** dialog box is displayed, as shown in the following figure. as shown in Figure 7-26.

Figure 7-26 Lease Duration



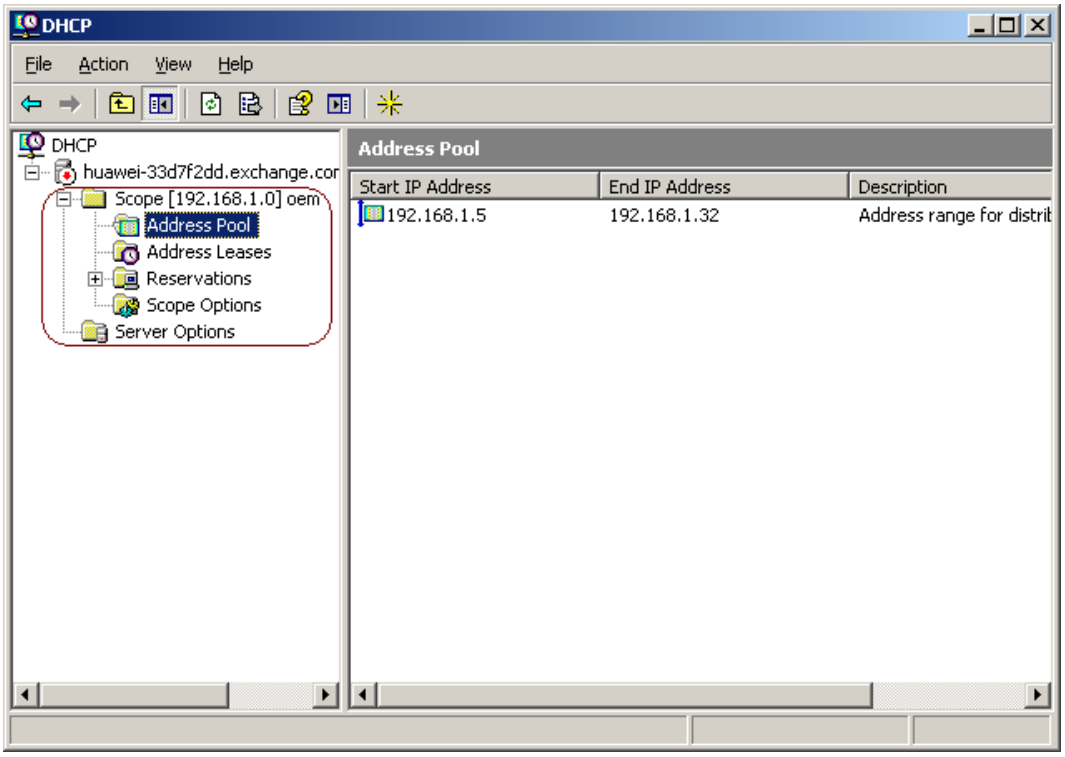
Step 9 In the **Lease Duration** dialog box, you can set the lease period of the DHCP server. By default, the lease period of the DHCP server is eight days. After the setting, click **Next** repeatedly until the **Router(Default Gateway)** dialog box is displayed, as shown in the following figure. as shown in Figure 7-27.

Figure 7-27 Router(Default Gateway)



Step 10 Set the gateway address provided by the DHCP server. When an IP phone obtains the IP address from the DHCP server, the DHCP server provides the IP address and gateway address for the IP phone. After the setting is complete, click **Next** repeatedly until the setting is complete. Then the page shown in the following figure is displayed. You can view the IP address pool information on it. as shown in Figure 7-28.

Figure 7-28 Complete the DHCP server



After the setting is complete, if some IP phones are set to obtain IP addresses through DHCP, the DHCP server allocates the IP addresses in the IP address pool to the IP phones one by one. If the lease of IP addresses is not renewed, the DHCP server withdraws the IP addresses for use of other devices.

----End

7.4.2 Setting Up the DHCP Server on Router AR-28

The configuration scripts and remarks for logging in to router AR-28 and enabling the DHCP server function are as follows:

```
<Quidway>system-view                //Enter the configuration mode.
[Quidway]dhcp enable                 //Enable the DHCP server function of the
router.
[Quidway]dhcp server detect           //Verify the DHCP server function.
[Quidway]interface Ethernet 0/1       //Connect to network port 1 on board 0.
```

NOTE

You must make sure that the network cable is inserted into network port 1 of board 0 on router AR-28. In the rear panel of the router, you can view the board slots and enable DHCP function on network port 1.

```
[Quidway-Ethernet0/1]ip address 192.168.2.1 255.255.255.0   //Set the IP
address of network port 0/1. The router also uses the IP address as the gateway
address and allocates the IP address to the DHCP client.
```

```
[Quidway-Ethernet0/1]dhcp select interface        //If the DHCP server mode
is selected based on the interface, the router can also set the DHCP server
based on other modes.
[Quidway-Ethernet0/1]dhcp server dns-list 192.168.2.20   //Set the DNS server
IP address delivered to the DHCP client when the DHCP server delivers an IP
address to the DHCP client. The DNS server IP address is optional.
[Quidway-Ethernet0/1]dhcp server option ****   //Set the DHCP options as
required.
[Quidway-Ethernet0/1]dhcp server expired ****  //Set the DHCP lease period.
You can set to unlimited or several days. The maximum lease period is 365 days.
The default lease period is 24 hours.
[Quidway-Ethernet0/1]quit     //Return to the configuration mode.
[Quidway]quit    //Exit the configuration mode.
<Quidway>save   //Save the setting.
```

After the setting is complete, save the setting. Otherwise, the data is lost after restart.

NOTE

In the preceding scripts, *** indicates the parameters followed. The parameter names can be set according to the actual situation. For which parameter names can be set, press **Shift + ?**.

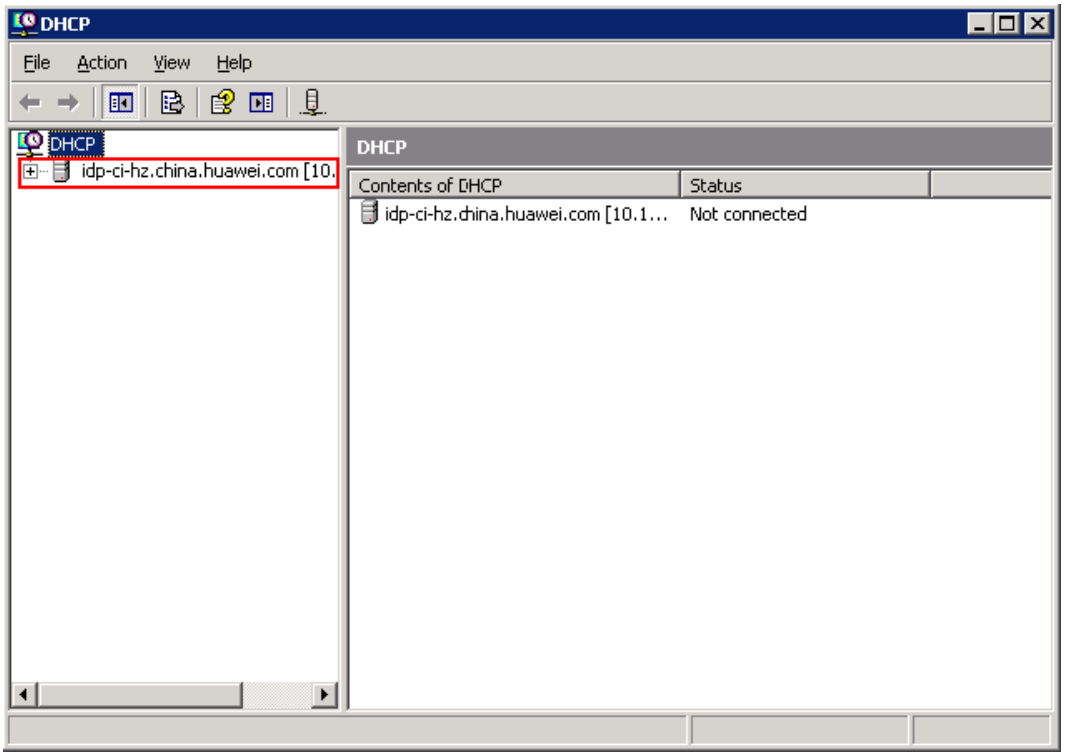
7.5 Setting the Option246 Parameter

This document describes how to set the **Option246** parameter.

Procedure

1. Choose **Start** > **Administrative Tools** > **DHCP**.
   The **DHCP** window is displayed.
2. Click on the left pane to expand the navigation tree, as shown in Figure 7-29.

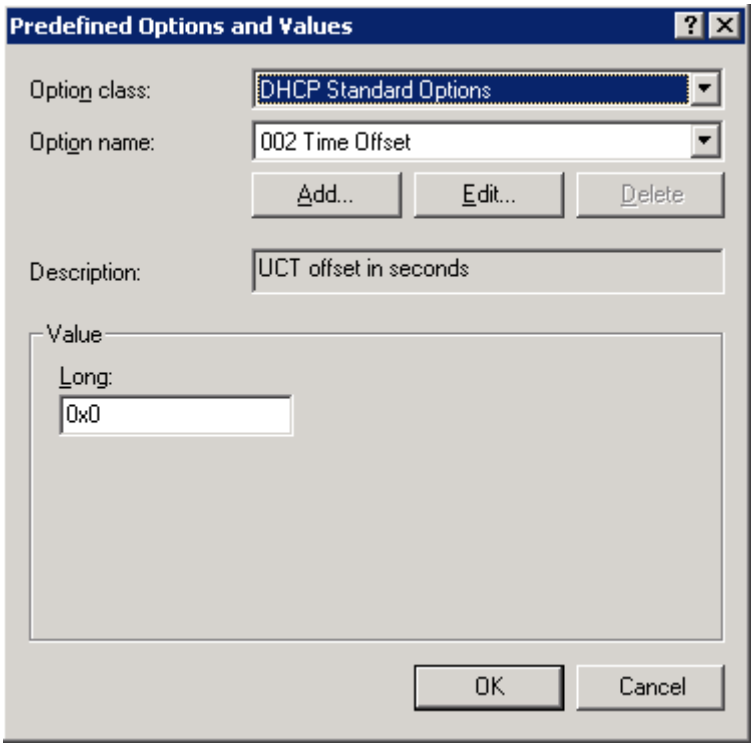
Figure 7-29 DHCP window



3. Right-click the record framed in red in Figure 7-29 and choose **Configure the Predefined Options** from the shortcut menu.

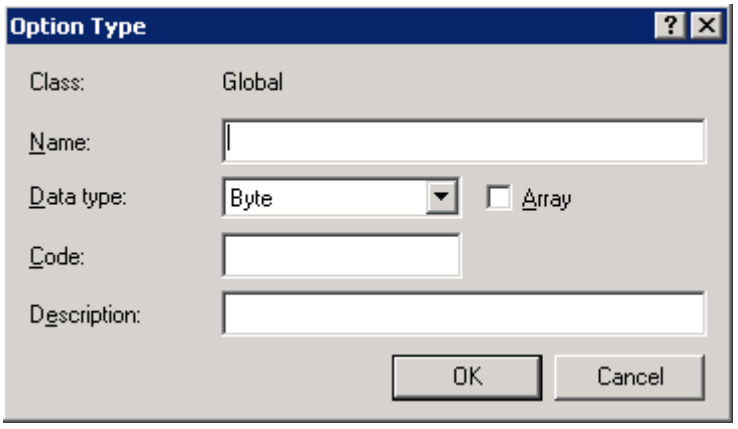
   The **Predefined Options and Values** dialog box is displayed, as shown in Figure 7-30.

Figure 7-30 Predefined Options and Values dialog box



4. Click **Add**.
   The **Option Type** dialog box is displayed, as shown in Figure 7-31.

Figure 7-31 Option Type dialog box



5. Set related parameters according to Table 7-1.

Table 7-1 Parameter settings

Parameter	Example
Name	ip phone

Parameter	Example
Data type	String
Code	246
Description	ip phone auto provision

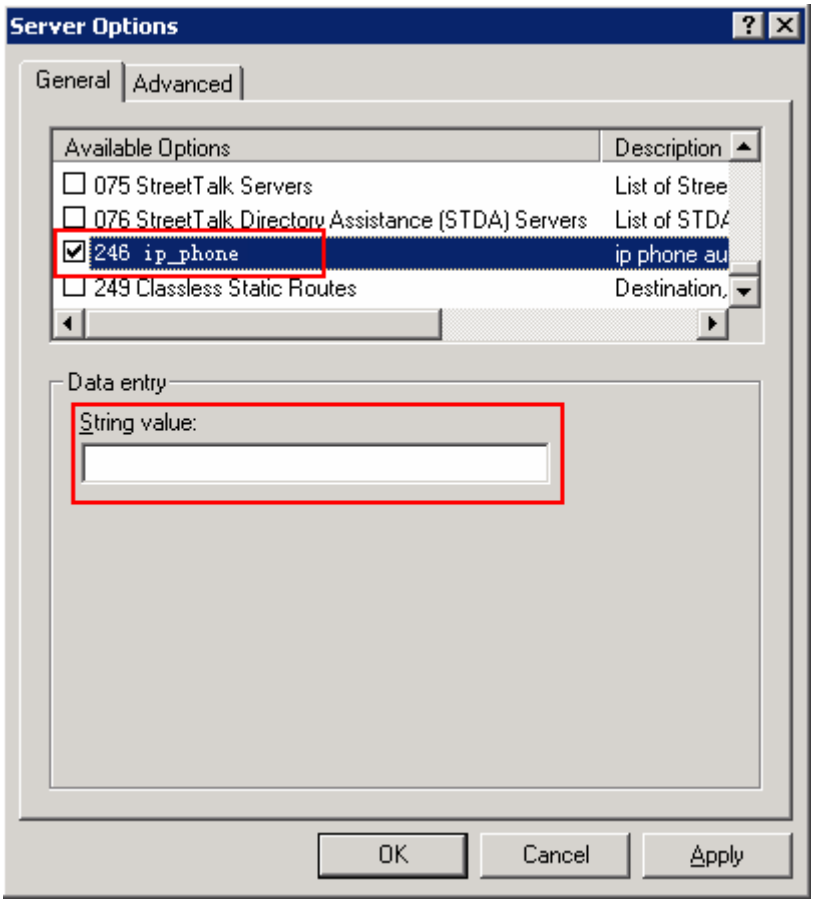
6. Click **OK**.

   The system returns to the **Predefined Options and Values** dialog box.
7. Click **OK**.

   The system returns to the **DHCP** window.
8. Select and right-click **Server Options** in the navigation tree and choose **Configure the Options** from the shortcut menu.

   The **Server Options** dialog box is displayed.
9. Select the **246 ip_phone** check box under **Available Options**, as shown in Figure 7-32.

Figure 7-32 Server Options



10. Set **String value** in the **Data entry** area.

    For example, set it to http://10.1.1.10

11. Click **OK**.

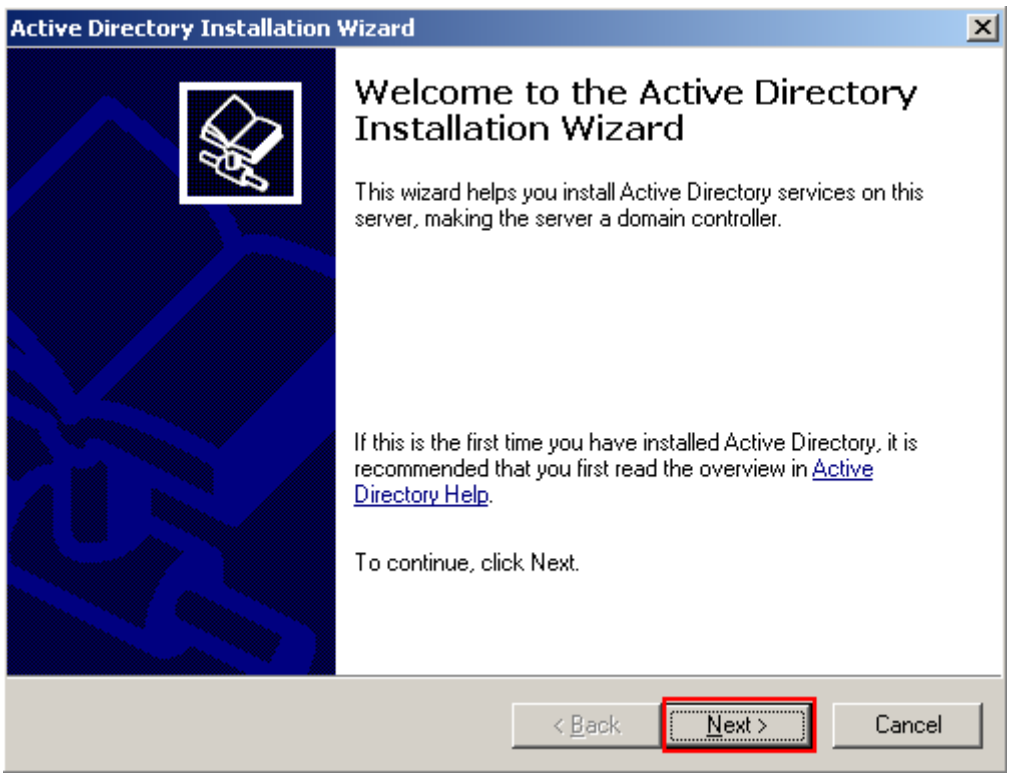
    The server information is displayed in the **DHCP** window.

7.6 Using Windows 2003 Server AD

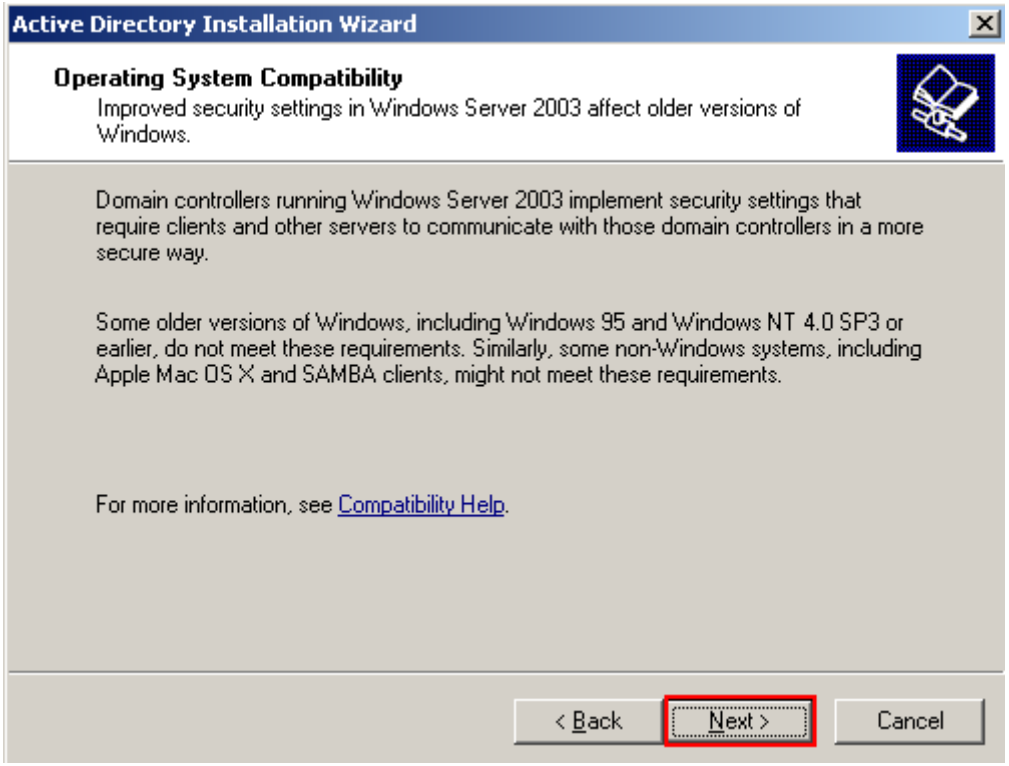
7.6.1 Installing Windows 2003 Server AD

1. Insert the Service Pack 2 CD-ROM to CD-ROM drive of a PC running Windows 2003 Server.
2. Choose **Start** > **Run in Windows 2003 Server**, enter **dcpromo**, and click **OK**.

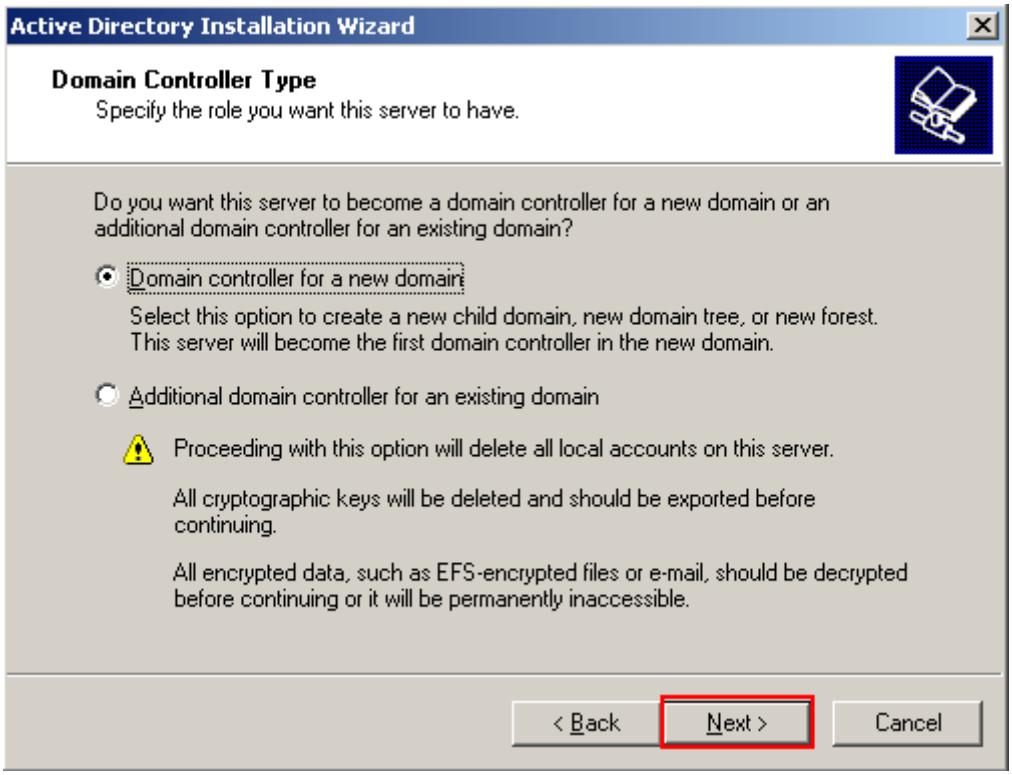
   The **Active Directory Installation Wizard** page is displayed.
3. Click **Next**.



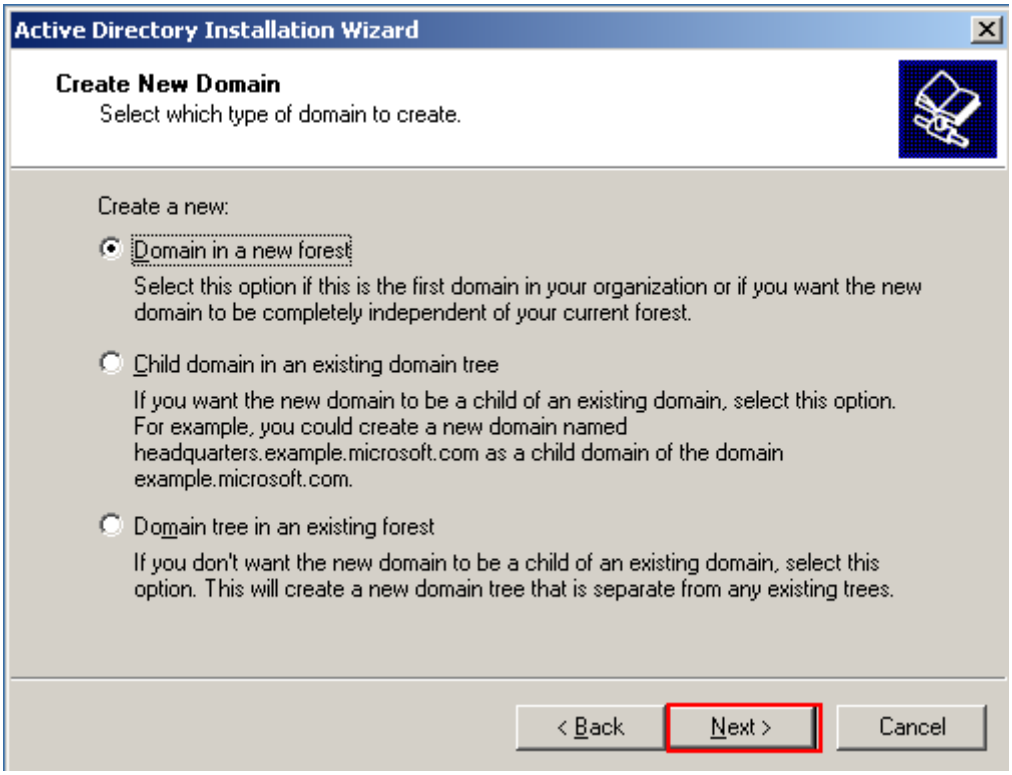
4. Click **Next**.



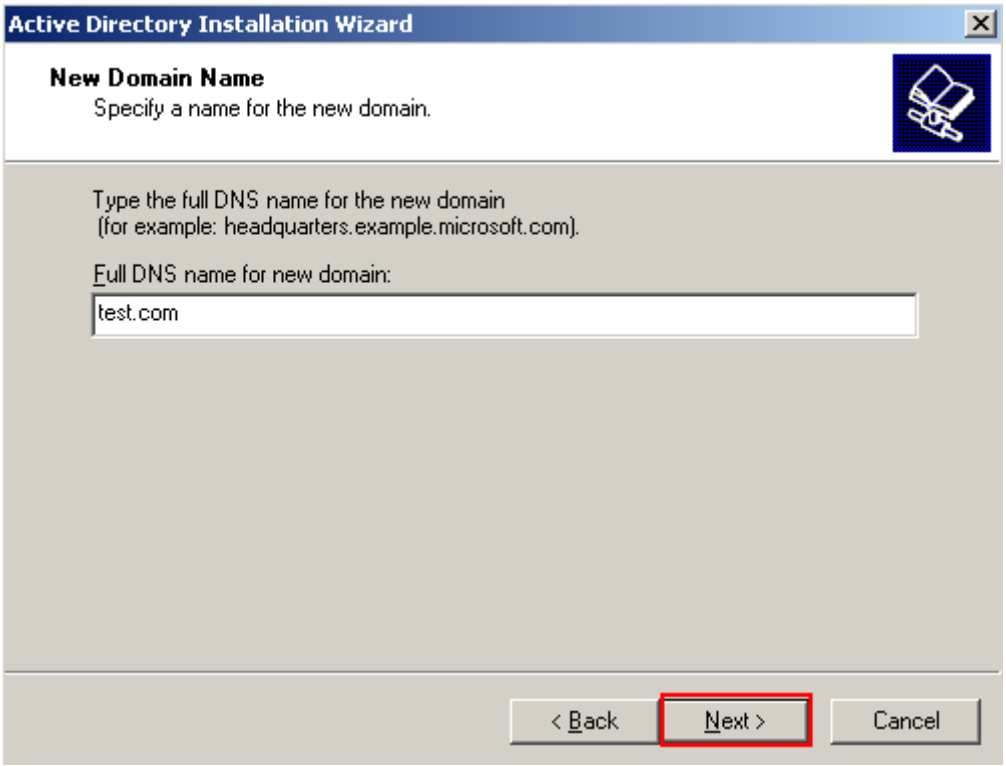
5. Select **Domain controller for a new domain** to specify the local PC running Windows 2003 Server as the domain controller (DC).



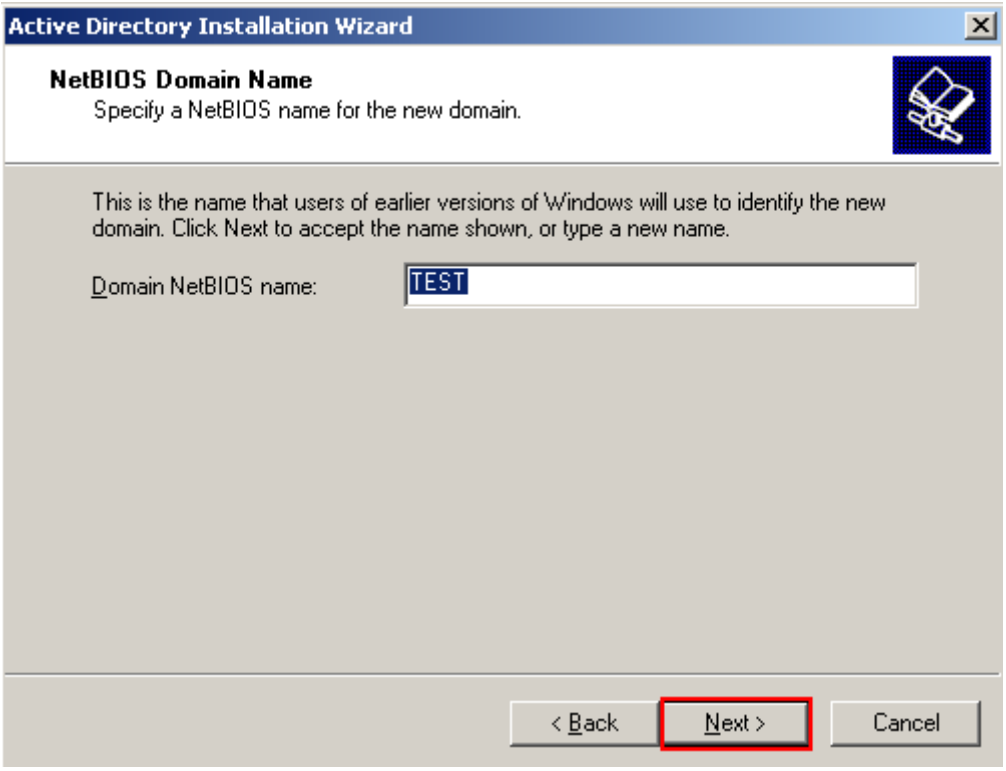
6. Select **Domain in a new forest**, and click **Next**.



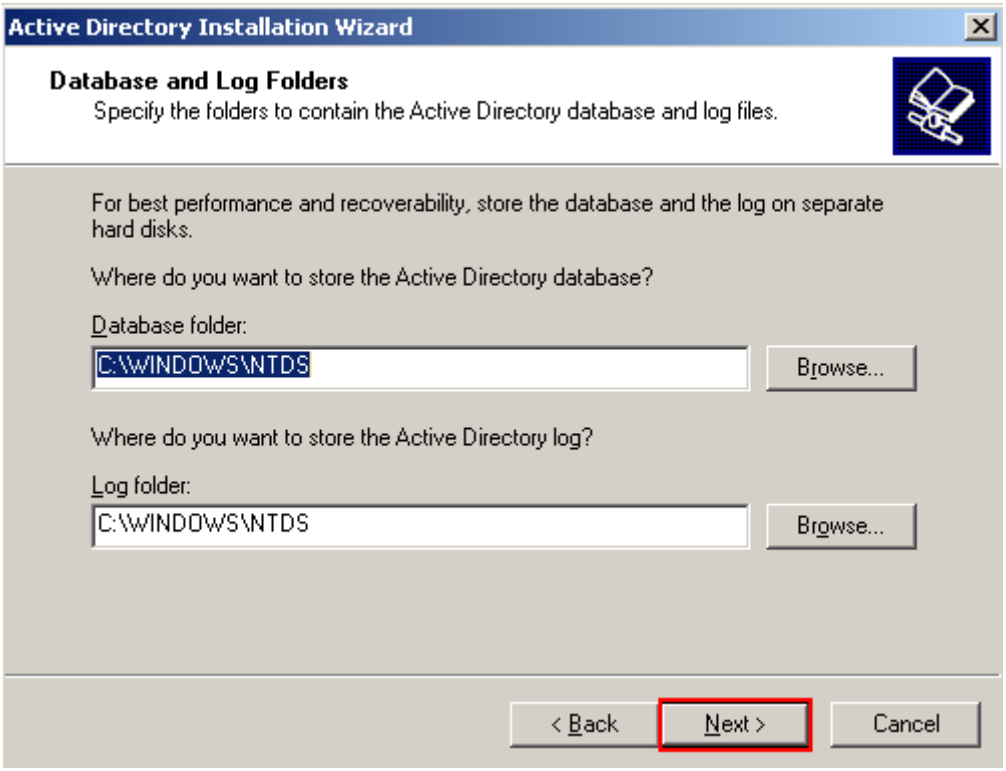
7. Enter **test.com** as the new domain name, and click **Next**.



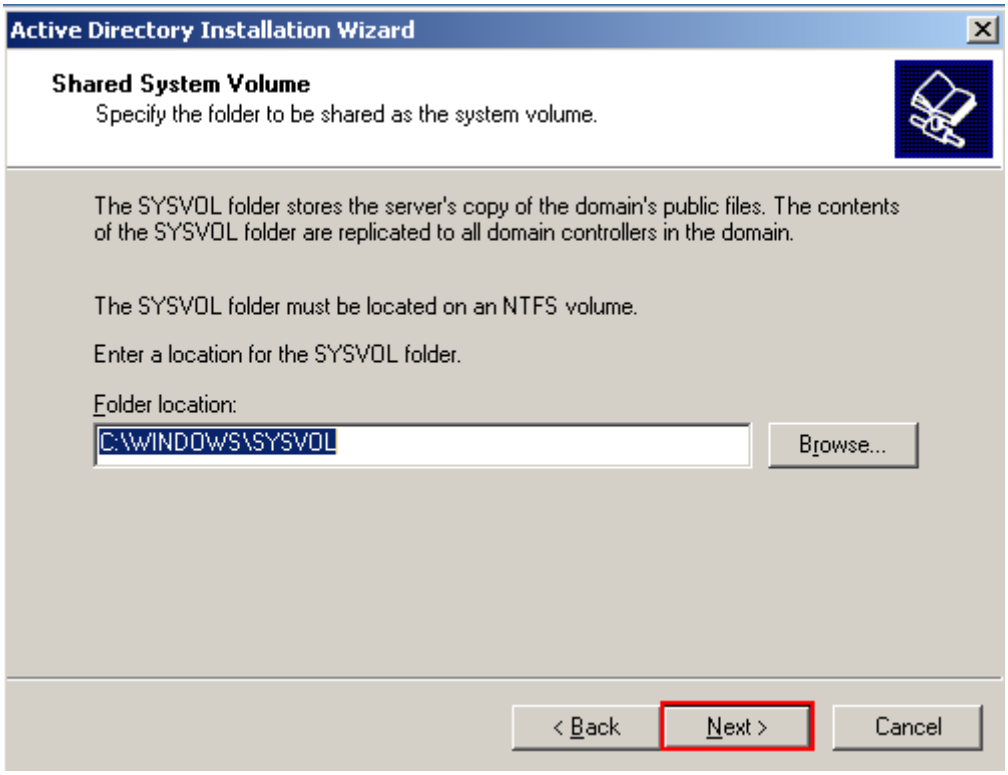
8. Retain the default value **TEST** as the **Domain NetBIOS name**, and click **Next**.



9. Retain the default values of paths for saving database and log folders, and click **Next**.



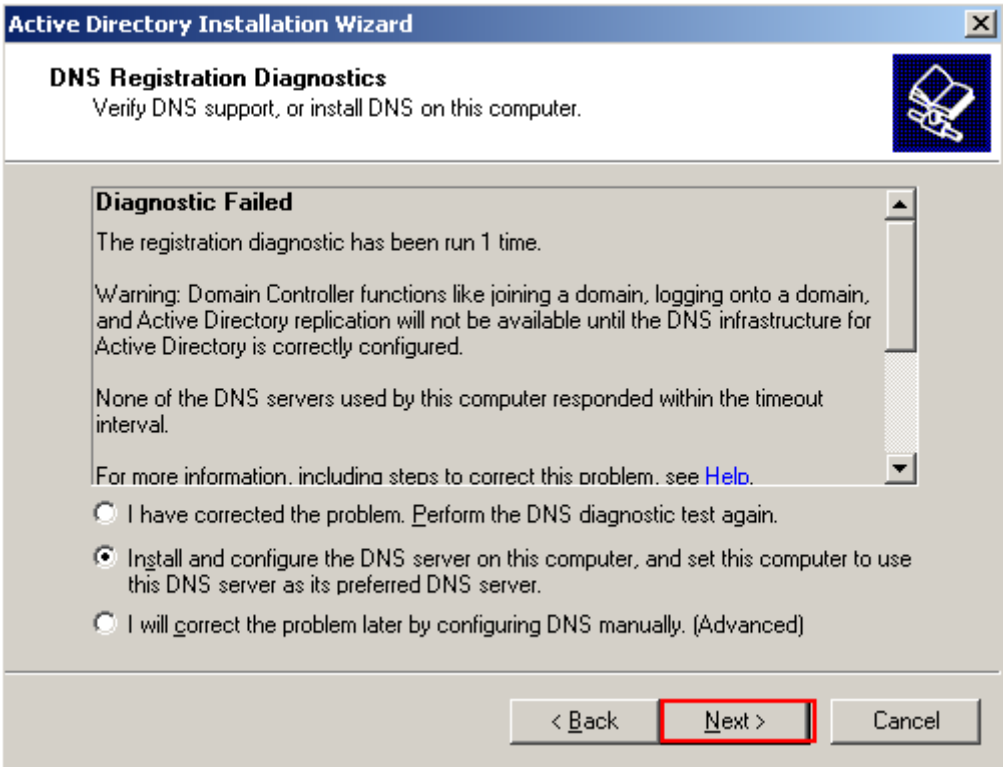
10. Retain the default path for saving the folder to be shared as the system volume, and click **Next**.



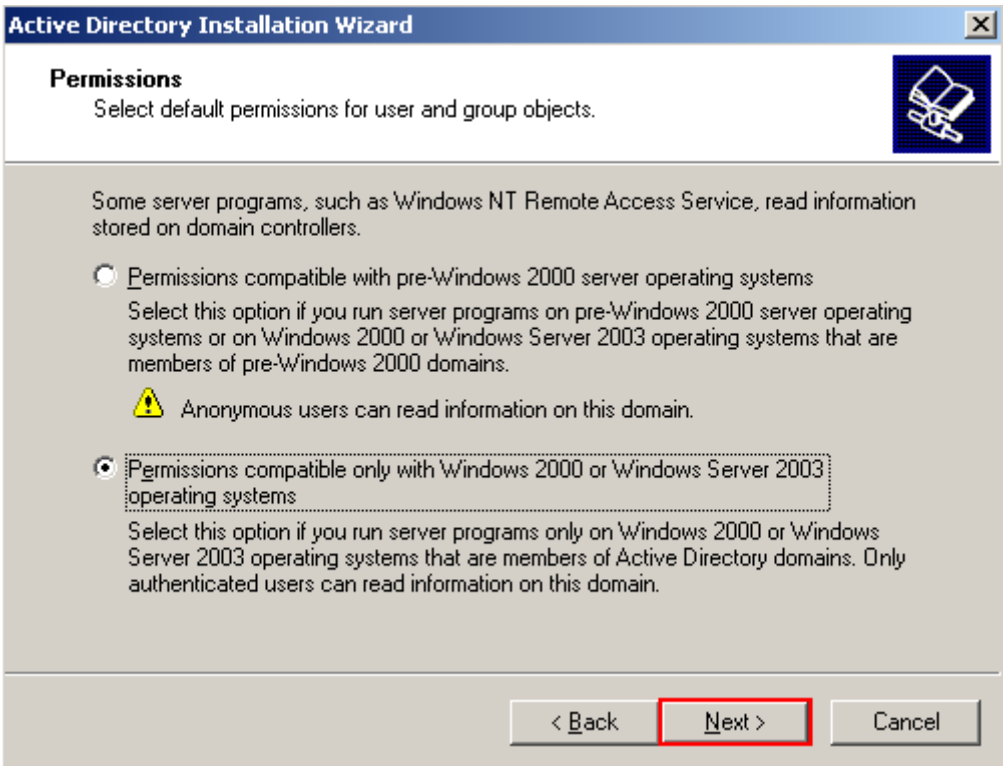
11. Diagnose DNS registration.

    DNS service components are not installed on the PC running Windows 2003 Server so the diagnosis fails.

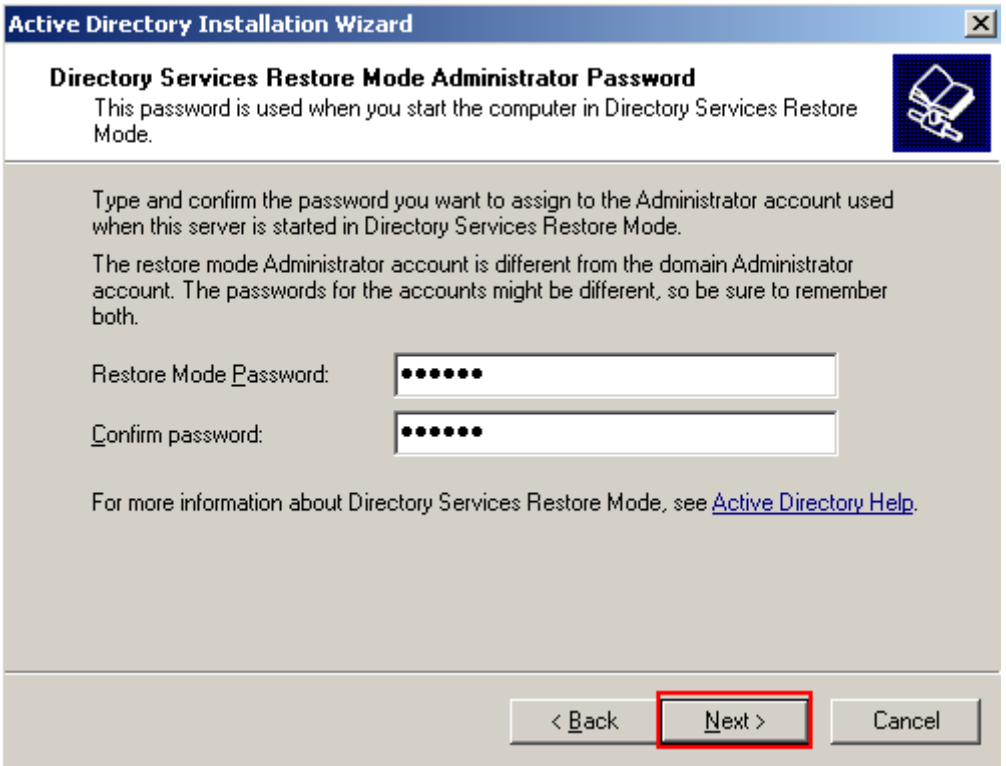
12. Select **Install and configure the DNS server on this computer, and set this computer to use this DNS server as its preferred DNS server**, and click **Next**.



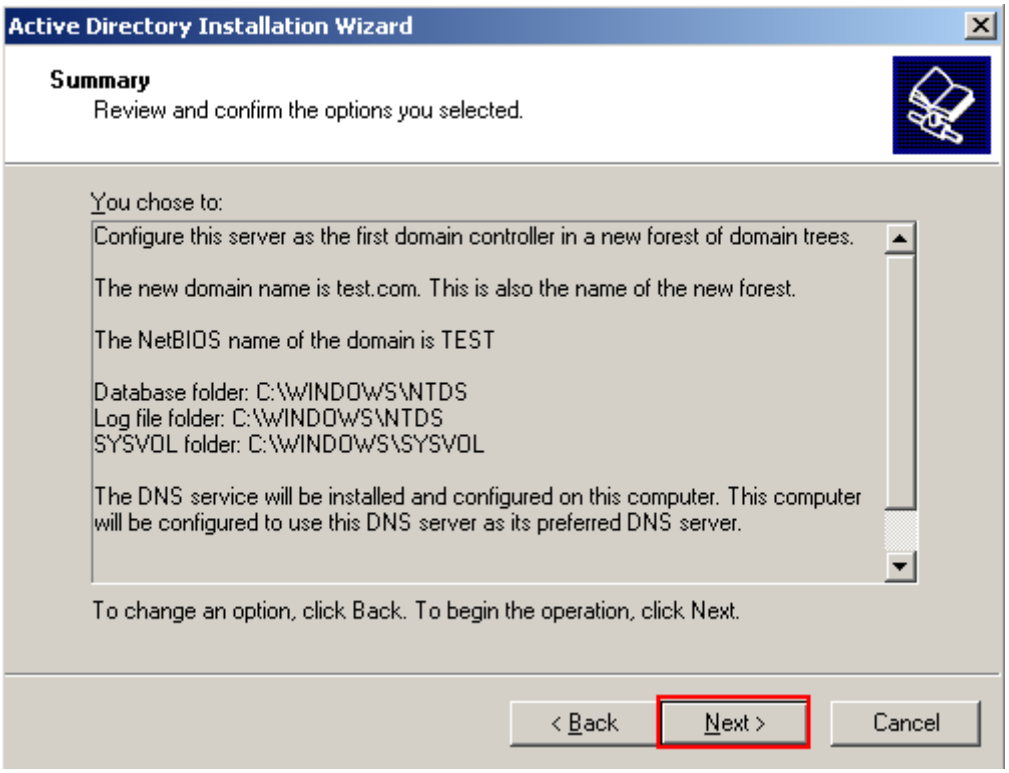
13. Retain the default value when setting default permissions for users and group objects, and click **Next**.



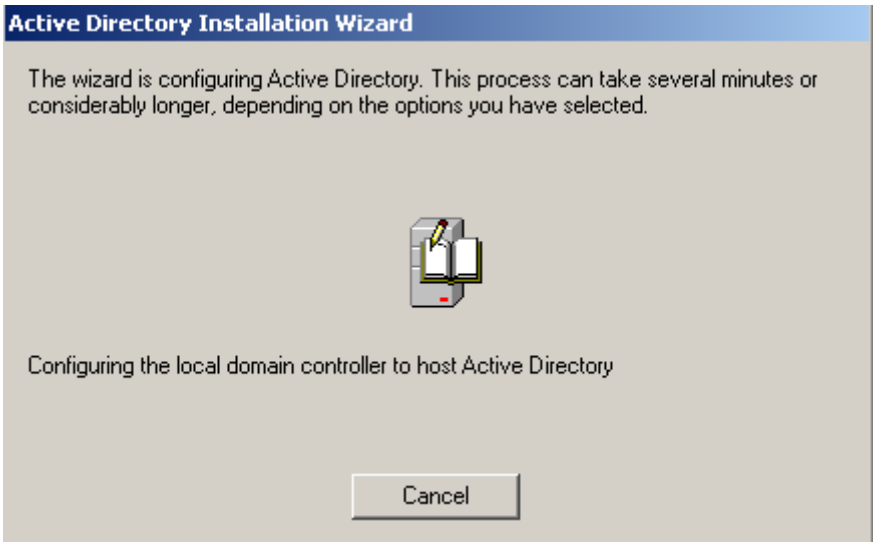
14. Set the administrator password for the restore mode, for example, 123456, and click **Next**.



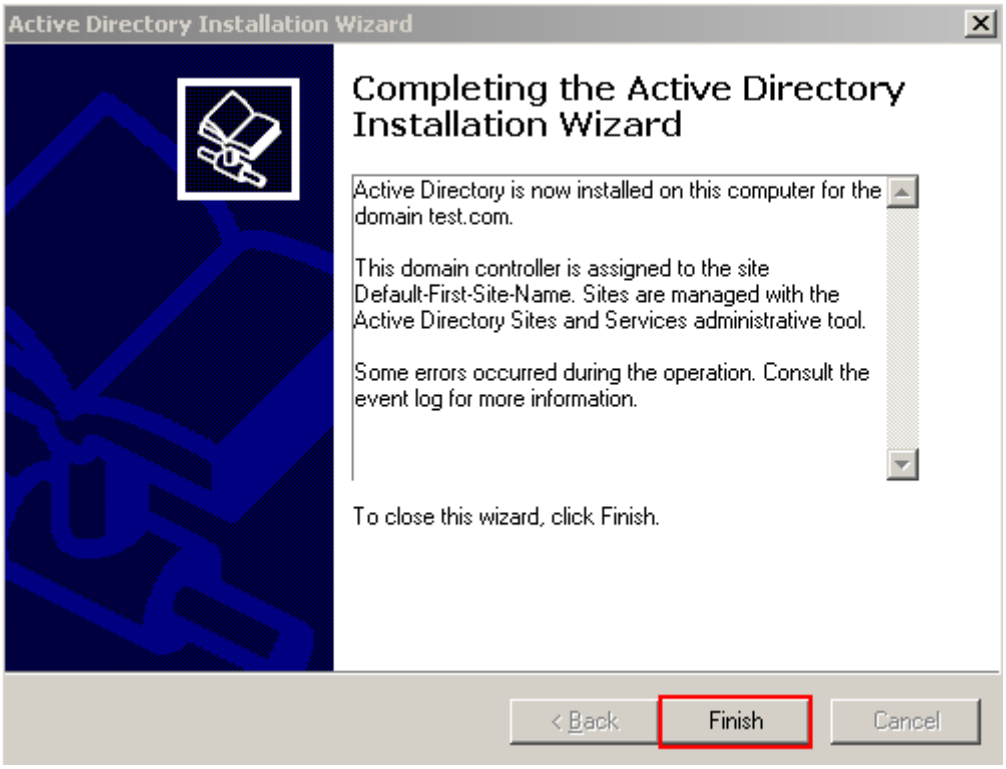
15. Verify the configurations and click **Next**.



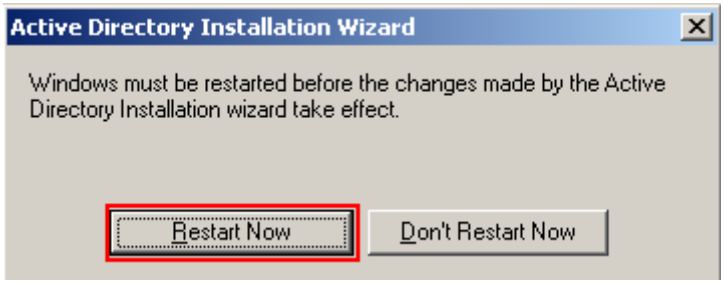
16. Wait for the AD to be installed and configured.



17. Click **Finish** after the AD is installed.

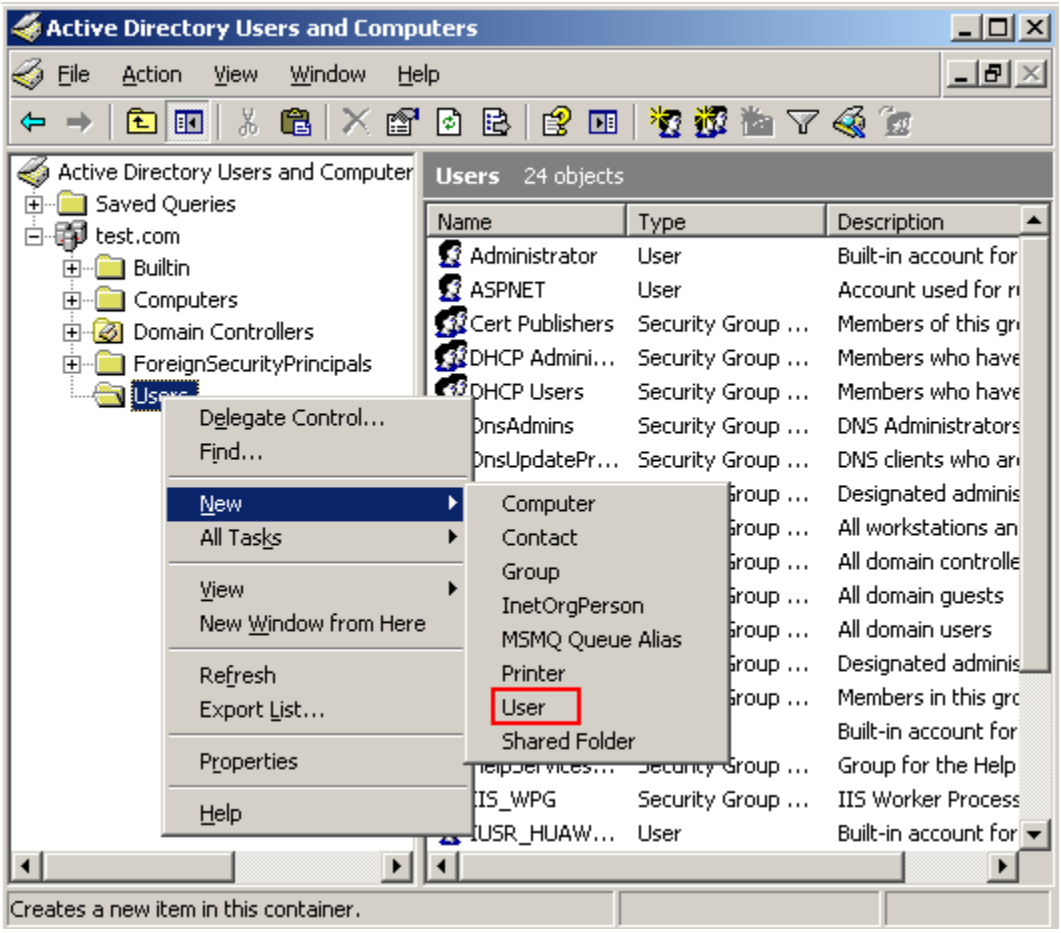


18. Click **Restart** to make the settings take effect.

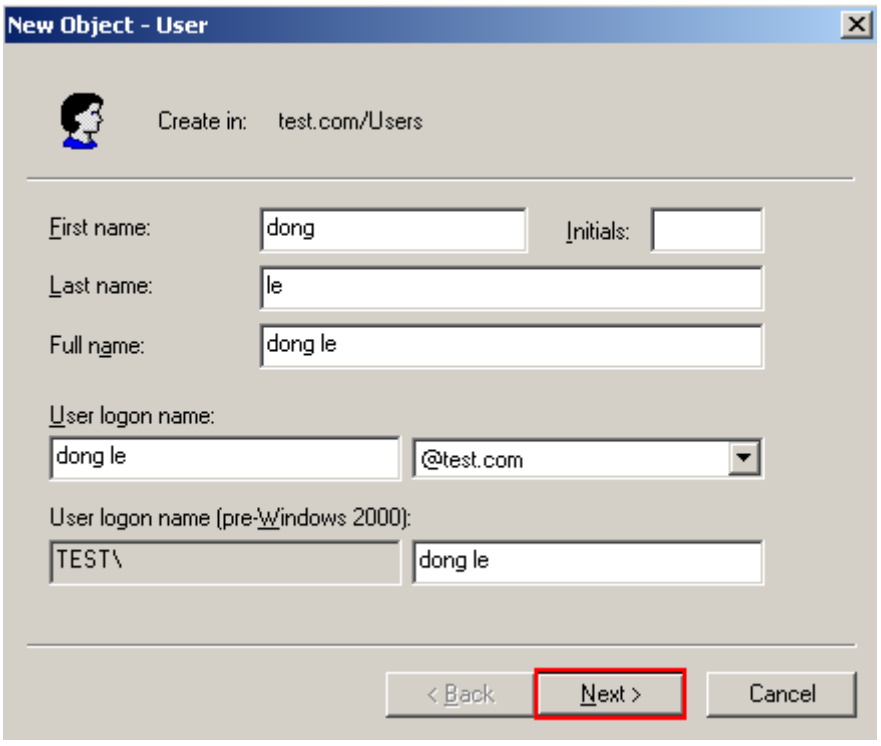


7.6.2 Creating a Domain User

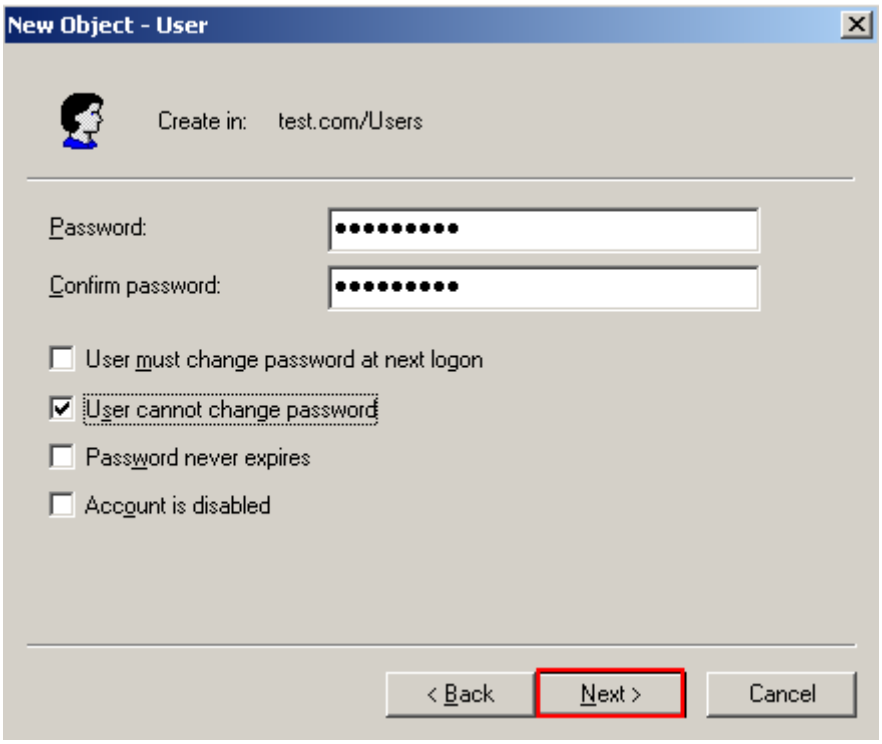
1. Choose **Start** > **Program** > **Administrative Tools** > **Active Directory Users and Computer**.
2. Right-click User and choose **New** > **User**.



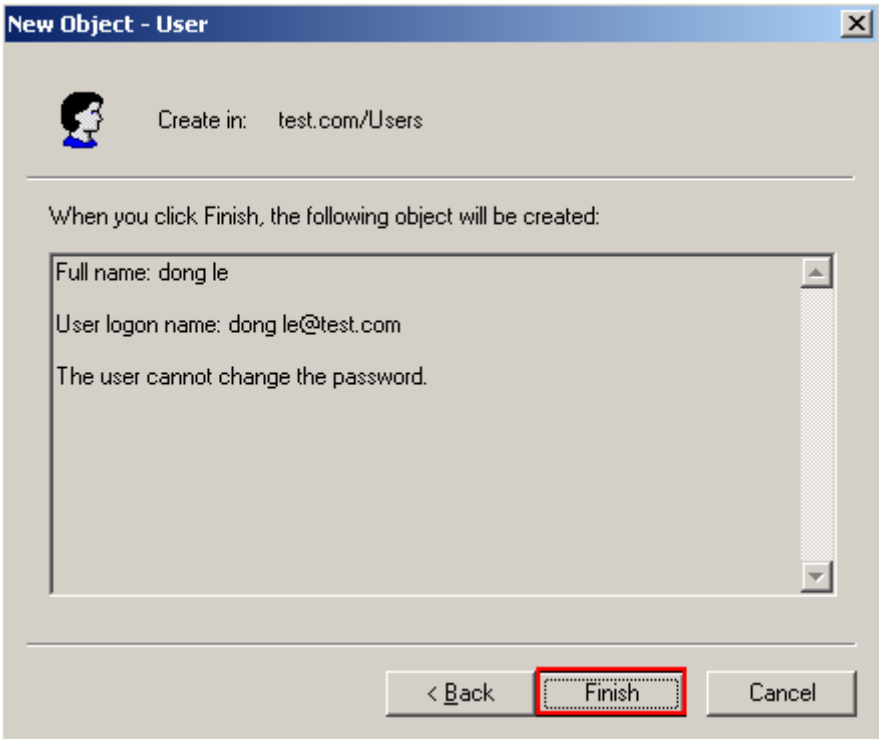
3. Create a login user account **dongle**.



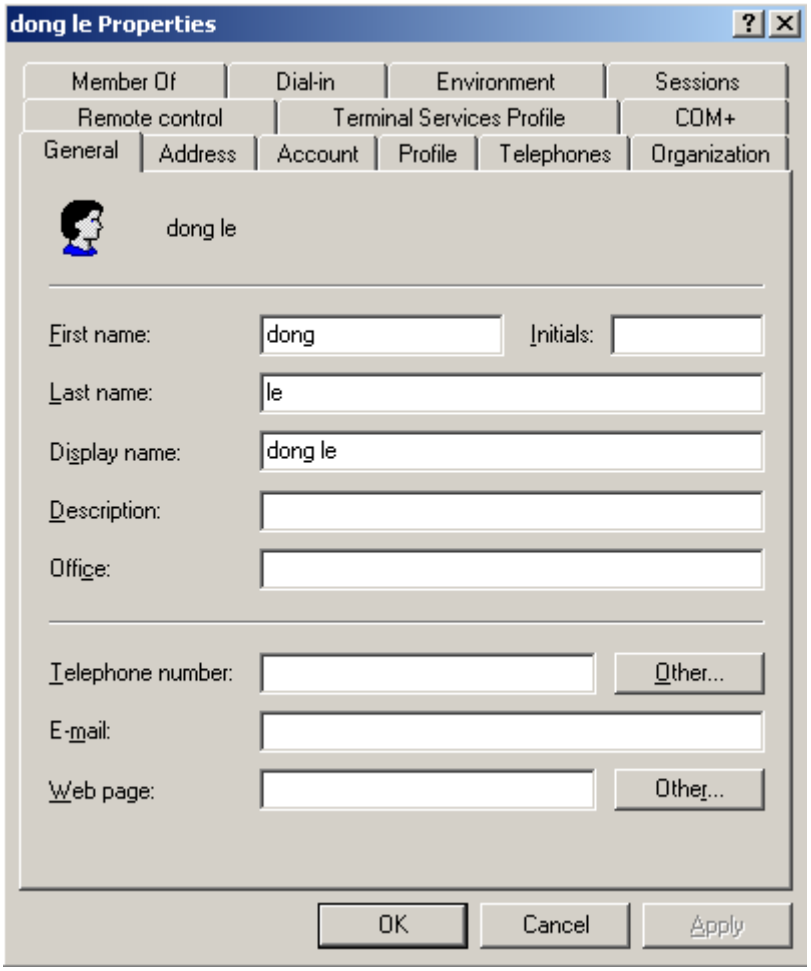
4. Create a password (Huawei123) for the **dongle** user, and select **User cannot change password**. Click **Next**.



5. The login user account **dongle** is created.
6. Click **Finish**.



7. Double-click the **dongle** user's avatar and set the user's phone number and other information.



7.7 Wireshark User Guide

7.7.1 Tool Introduction

Obtaining Method

Obtain the Wireshark installation file according to operating system as follows:

- R&D area: Access **\\lg-fs\Rnd\Software\2.ITapply** and download the Wireshark installation file.
- Non-R&D area: Access http://www.wireshark.com and download the Wireshark installation file.

User

Onsite engineers and R&D personnel.

Function

Analyze the Call Access Function (CAF) or service control point (SCP) signaling.

Application Scenario

Analyzing the CAF or SCP signaling is required.

Function Description

The Wireshark can run in various operating systems, such as the UNIX, Linux, and Windows operating systems.

The Wireshark provides the following functions:

- Captures messages on running nodes.
- Analyzes data that is captured from the network.
- Analyzes hard disk data that is captured by other tools.

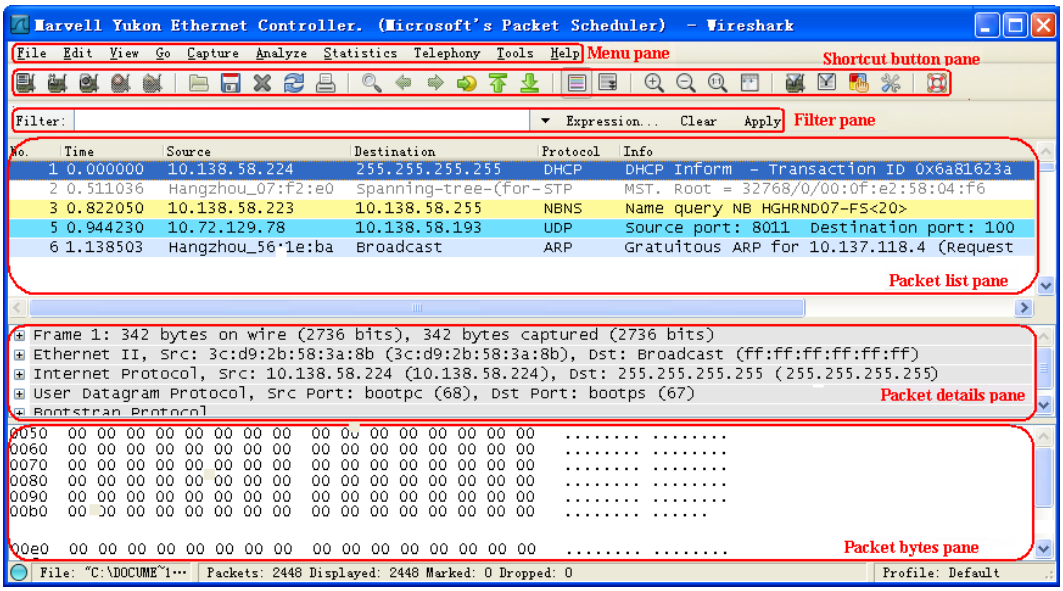
7.7.2 Common Operations and Menus

This topic describes the menus of the Wireshark and common operations. For details about the menu functions, see the Wireshark online help.

Wireshark Main Page

The Wireshark main page consists of six panes: menu pane, shortcut button pane, filter pane, packet list pane, packet details pane, and packet bytes pane, as shown in Figure 7-33.

Figure 7-33 Wireshark main page



Menu Pane

The menu pane contains the following menus:

- File

  Contains items to open and merge capture files, save, print, or export capture files in whole or in part, and to exit the Wireshark.

- Edit

  Contains items to find a packet, mark one or more packets, and set your preferences (such as fonts, color, time format, and parsing application), and then save the preferences as default settings.
- View

  Controls the display of the captured data, such as time format and color of packets transmitted using different protocols.
- Go

  Contains items to go to a specific packet.
- Capture

  Allows you to set capture parameters, including selecting network adapters, starting and stopping captures.
- Analyze

  Allows you to enable or disable protocol dissectors.
- Statistics

  Contains items to display various statistic windows, including a summary of the packets that have been captured and displaying protocol hierarchy statistics.
- Telephony

  Contains items to provide telephony communication mode, such as G or LTE.
- Tools

  Contains two items: Firewall ACL Rules and Lua.
- Help

  Contains items to help users, such as access to some basic help, a list of supported protocols, and user guides.

Shortcut Button Pane

Lists the shortcut buttons for common functions.

When the pointer is moved to a button, its function is displayed.

Filter Pane

Specifies the filter expression. You can set the filter expression to filter out only the required packets for analysis. For details about the filter expression usage, see SIP Protocol Analysis.

Packet List Pane

Lists all packets according to the time, address, and protocol.

- The Wireshark displays the protocols and types of the packets that can be parsed.
- The Wireshark marks the packets whose formats or processes are faulty with colors.

NOTE

Because the Wireshark is not entirely intelligent, the marks can be used only for reference, not as the analysis basis. For detailed analysis, view the packet content and analyze the packet based on the signaling process.

Packet Details Pane

Displays packet contents by protocol or network layer. The Wireshark parses all fields if a packet can be parsed. The Wireshark analyzes TCP packets based on packet serial numbers to check the signaling process.

Packet Bytes Pane

Displays the original packet contents in the hexadecimal format on the left, with the matching ASCII characters on the right.

Common Operations

Context

CAUTION

The Wireshark can be used only after it is bound to a network adapter. After being installed on a PC, the Wireshark can capture only the packets passing through this network adapter. Therefore, before using the Wireshark to capture packets, configure the network to ensure that packets can be sent to the network adapter to which the Wireshark is bound.

Procedure

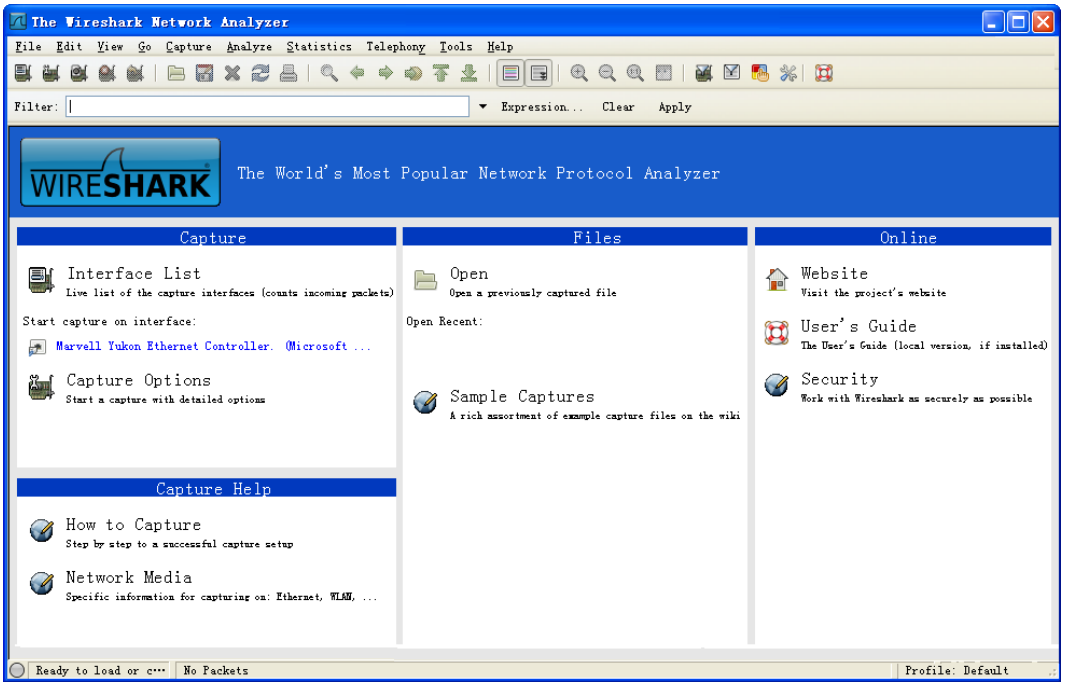
Step 1 Set monitoring and mirroring ports on the switch.

1. Access port one of the switch and set it as the monitoring port.
2. Access other ports and set them as mirroring ports.
3. Connect the PC installed with Wireshark to port one of the switch.

Step 2 Double-click  to start the Wireshark.

The Wireshark main page is displayed, as shown in Figure 7-34.

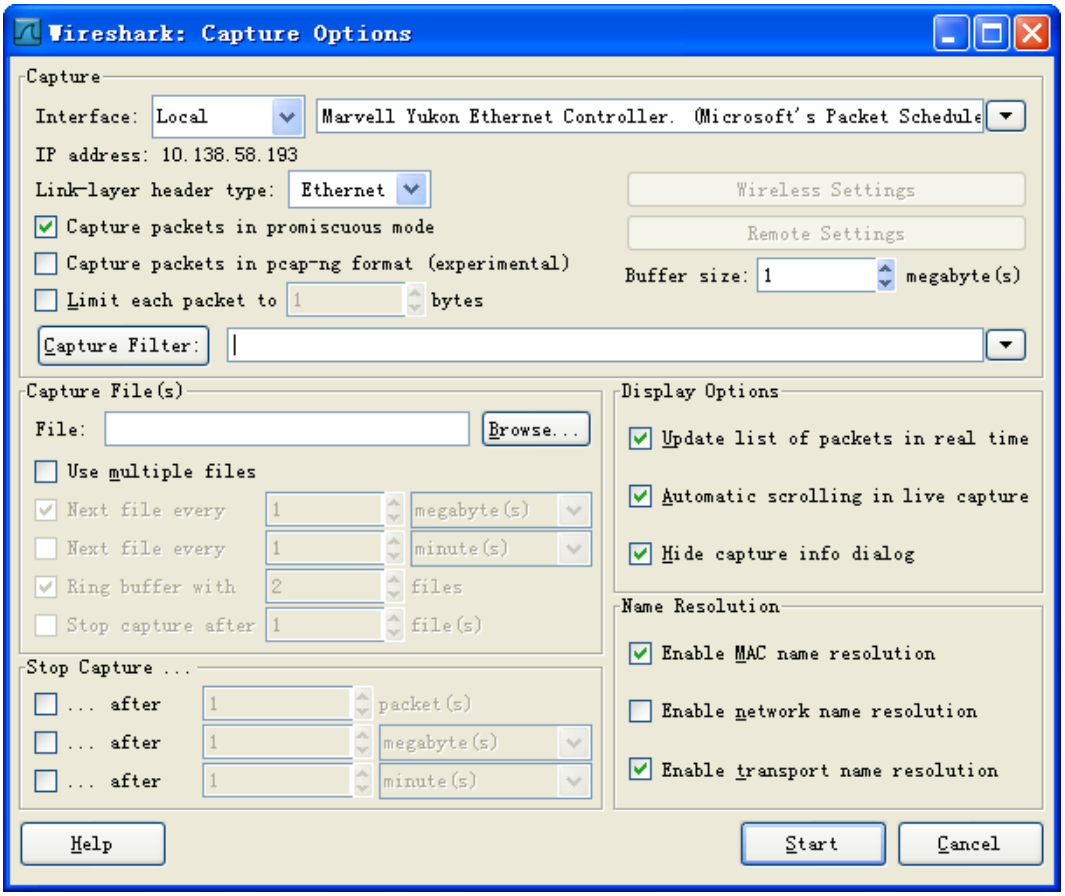
Figure 7-34 Wireshark main page



Step 3 Choose **Capture** > **Option**.

The **Capture Options** page is displayed, as shown in Figure 7-35.

Figure 7-35 Wireshark: Capture Options page



Main areas on the **Wireshark: Capture Options** page are described as follows:

- Capture
  - Interface

    Specifies the network adapter for capturing packets.

CAUTION

After the Wireshark is installed, the system automatically generates a logical network adapter. In addition to the logical network adapter, a physical network adapter is required, as shown in Figure 7-35. During the actual packet capture, select a correct physical network adapter, especially for a host with multiple network adapters. A physical network adapter will be displayed in the drop-down list box only after the WinPcap is installed.

  - Capture Filter

    Specifies the filter criteria. The Wireshark captures only the packets that comply with the filter criteria. For example, if **Capture Filter** is set to **host 10.138.5.10**, only packets sent and received by the host whose IP address is 10.138.5.10 will be captured.

    Table 7-2 describes the filter criteria categories specified by **Capture Filter**.

Table 7-2 Filter criteria categories specified by Capture Filter

Filter Criteria Category	Example
Capture the packets passing through the MAC address 08:00:08:15:ca:fe	ether host 08:00:08:15:ca:fe
Capture the packets passing through the MAC address 08:00:08:15:ca:fe or 08:00:08:15:ca:ee	ether host 08:00:08:15:ca:fe or ether host 08:00:08:15:ca:ee
Capture the packets passing through the IP address 192.168.0.10	host 192.168.0.10
Capture the packets passing through the IP address 192.168.0.10 or 192.168.0.11	host 192.168.0.10 or host 192.168.0.11
Capture the packets passing through the TCP port 80	tcp port 80
Capture the packets sent and received by the IP address 192.168.0.10, excluding the HTTP packets (packets passing through the TCP port 80)	host 192.168.0.10 and not tcp port 80

- Capture File(s)

  Specifies the path for automatically saving the captured packets as files. Ensure that the destination hard disk has sufficient free space.

  - File

    Click **Browse** and select a path for storing captured data packets.

  - Use multiple files

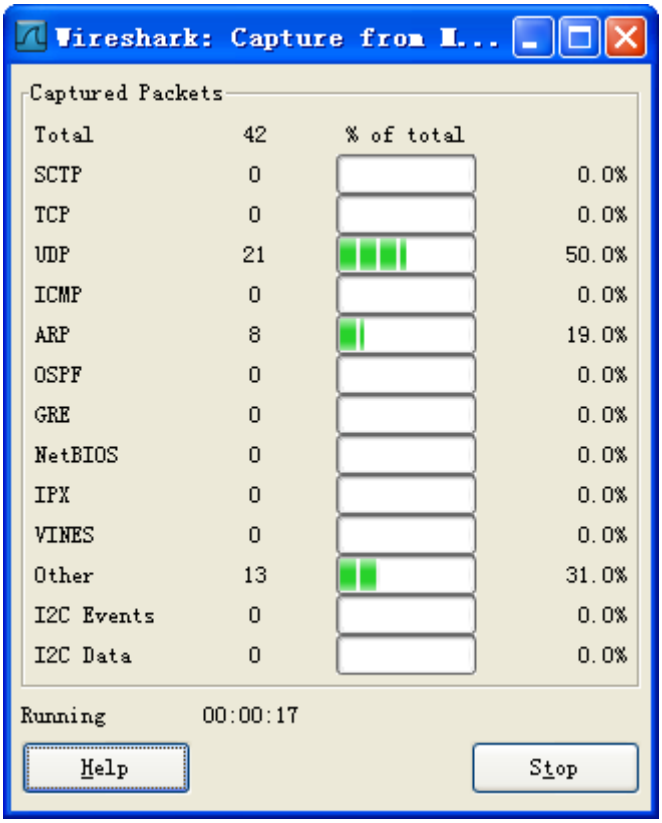
    Set the parameters to specify the way of creating files for saving captured data packets.

- Display Options

  Specifies whether to display the real-time capture results during the packet capture.

  - Select **Update list of packets in real time**. The packet list is displayed on the Wireshark main page.
  - Select **Automatic scrolling in live capture**. If the captured results exceed one screen, the results are displayed in automatic scrolling mode.
  - Deselect **Hide capture info dialog**. The **Captured Packets** page shown in Figure 7-36 is displayed during the packet capture, with the real-time information about the numbers of captured packets of various protocols.

Figure 7-36 Captured Packets page



Step 4 Setting the options as request, and click **Start**.

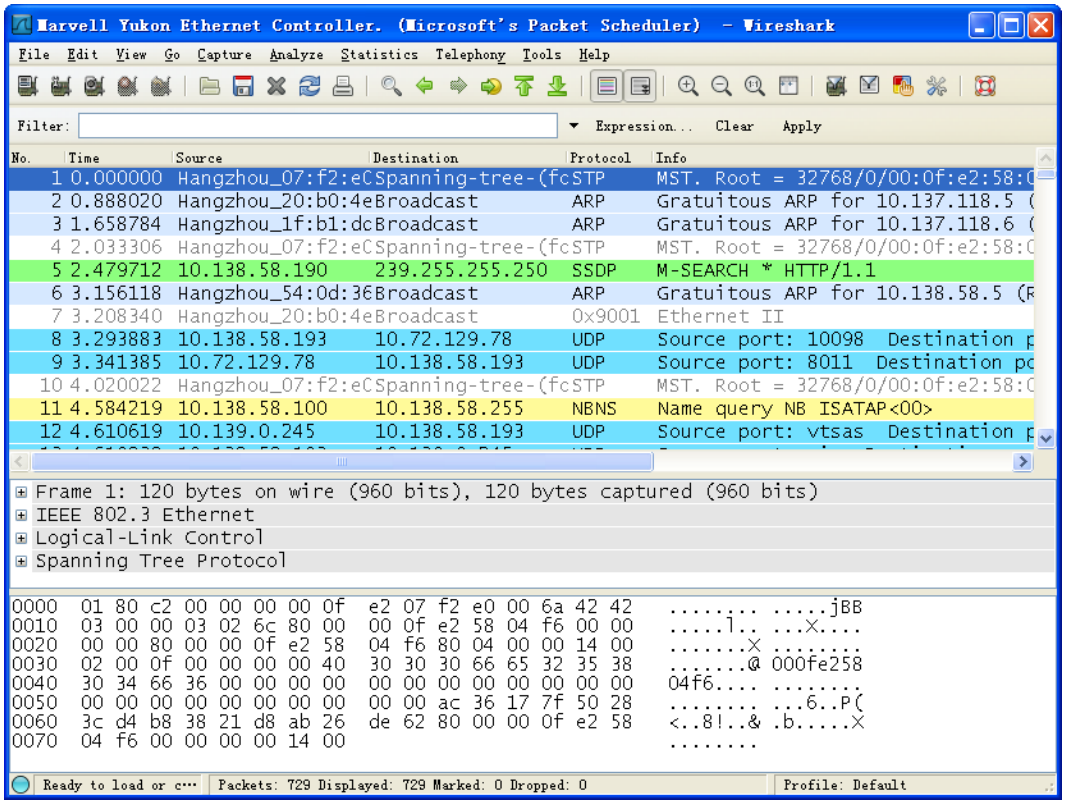
The Wireshark starts to capture packets.

Step 5 Recur the operation scene that needs to be captured packets.

Step 6 Choose **Capture** > **Stop** or click **Stop** in Figure 7-36.

The **Capture result** page is displayed, as show in Figure 7-37.

Figure 7-37 Capture result



NOTE

You can verify the result of capturing data packets based on the data flow. For example, enter **sip** in **Filter pane** and click **Apply**. If "packet list pane, packet details pane and packet bytes pane" is displayed, data packets are captured successfully.

Step 7 Save the data packet capturing results.

1. Choose **File** > **Save As**.

   The **Wireshark: Save file as** page is displayed.

2. Name the file, select the save type and the save path as prompted, and then click **Save**.

NOTE

Add a file name extension when specifying the file name. To save data packets numbered 1 to 1000, select **Range** and enter **1 to 1000**.

Step 8 Choose **File** > **Quit** to exit the Wireshark.

----End

7.7.3 Filter Rules

This topic describes the filter Rules, including filter expression rules and filter expression construction tips.

NOTE

Different from **Capture Filter** under the **Option** submenu of **Capture**, the filter rule specifies the packet capture results .

Filter Expression Rules

The Wireshark uses simple expressions to implement the powerful filtering function. A user can specify the source IP address, destination IP address, and packet field contained in a protocol or packet, or combine any of the preceding filter criteria. The Wireshark supports various logical operations, such as **==**, **!=**, **>**, **<**, **and**, **or**, **not**.

Comparison Symbols

The Wireshark can use comparison symbols (English words or operators) to form filter expressions. Table 7-3 describes the comparison symbols used in filter expressions.

Table 7-3 Comparison symbols used in filter expressions

English	Operator	Description and Setting
eq	==	Equal to ip.addr==10.138.21.5 ip.addr eq 10.138.21.5
ne	!=	Not equal to !(ip.addr == 10.138.21.5) !(ip.addr eq 10.138.21.5)
gt	>	Greater than frame.pkt_len > 10 frame.pkt_len gt 10
lt	<	Smaller than frame.pkt_len < 128 frame.pkt_len lt 128
ge	>=	Equal to or greater than frame.pkt_len >= 0x100 frame.pkt_len ge 0x100
le	<=	Smaller than or equal to frame.pkt_len <= 0x20 frame.pkt_len le 0x20

Logical Operators

The Wireshark can use logical operators to combine multiple filter expressions. For example, if you want to filter out packets that are transmitted using the GPRS tunneling protocol (GTP) and through the IP address 10.138.21.5, use the filter expression gtp && ip.addr==10.138.21.5. Table 7-4 describes the logical operators used in filter expressions.

Table 7-4 Logical operators used in filter expressions

English	Operator	Description and Setting
and	&&	And ip.addr==10.0.0.5 and tcp.flags.fin
or	||	Or ip.addr==10.0.0.5 or ip.addr==192.1.1.1
not	!	Not not llc

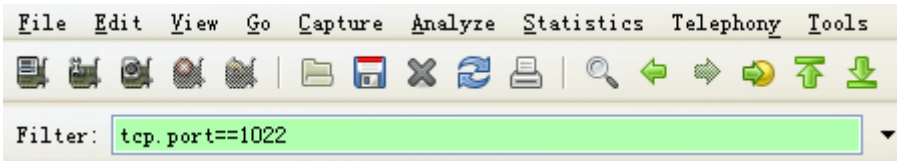
Setting Protocol Fields

To set the protocol fields, proceed as follows:

1. Set filter criteria.
   - Enter the protocol fields in the **Filter** text box.

     For example, if you want to filter out TCP packets that are transmitted through port 1022, enter **tcp.port==1022**, as shown in Figure 7-38.

Figure 7-38 Protocol field example

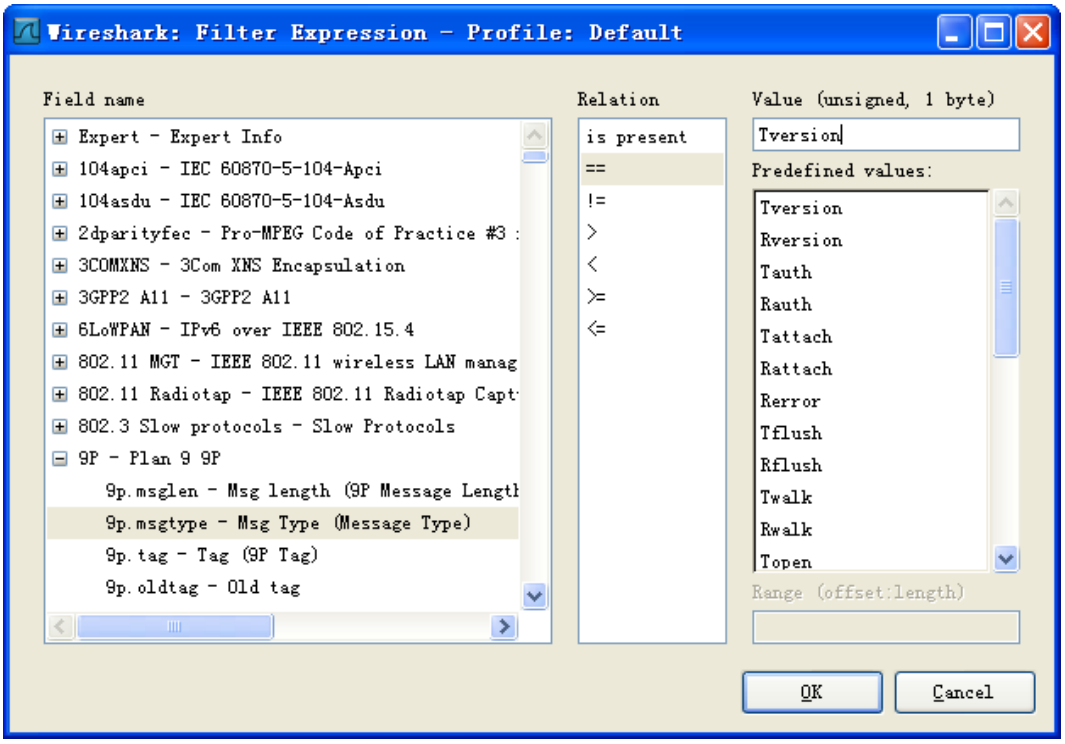


   - Customize filter expressions.

   a. Click **Expression** next to **Filter**.

      The **Wireshark: Filter Expression** dialog box is displayed, as shown in Figure 7-39.

Figure 7-39 Wireshark: Filter Expression



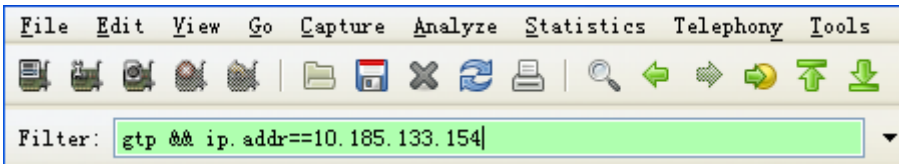
b. Select a field, select a relation, and then enter a value in the **Value (IPv4 address)** test box, as shown in Figure 7-39.

c. Click **OK**.

Check whether a filter expression is correct.

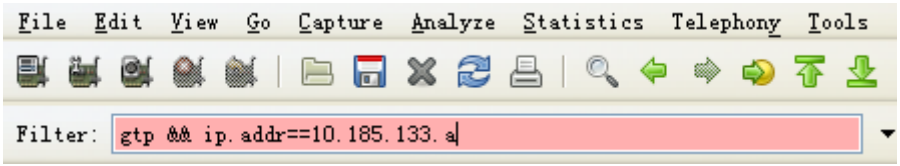
- If the filter expression is correct, the background color of the **Filter** text box is green, as shown in Figure 7-40.

Figure 7-40 Displayed Filter text box if the filter expression is correct



- If the filter expression is incorrect, the background color of the **Filter** text box is dark pink, as shown in Figure 7-41.

Figure 7-41 Displayed Filter text box if the filter expression is incorrect



2. Press **Enter** or click **Apply**.
   The packets that meet the filter criteria are displayed.

Common Filter Expressions

Common filter expressions used to filter out packets are as follows:

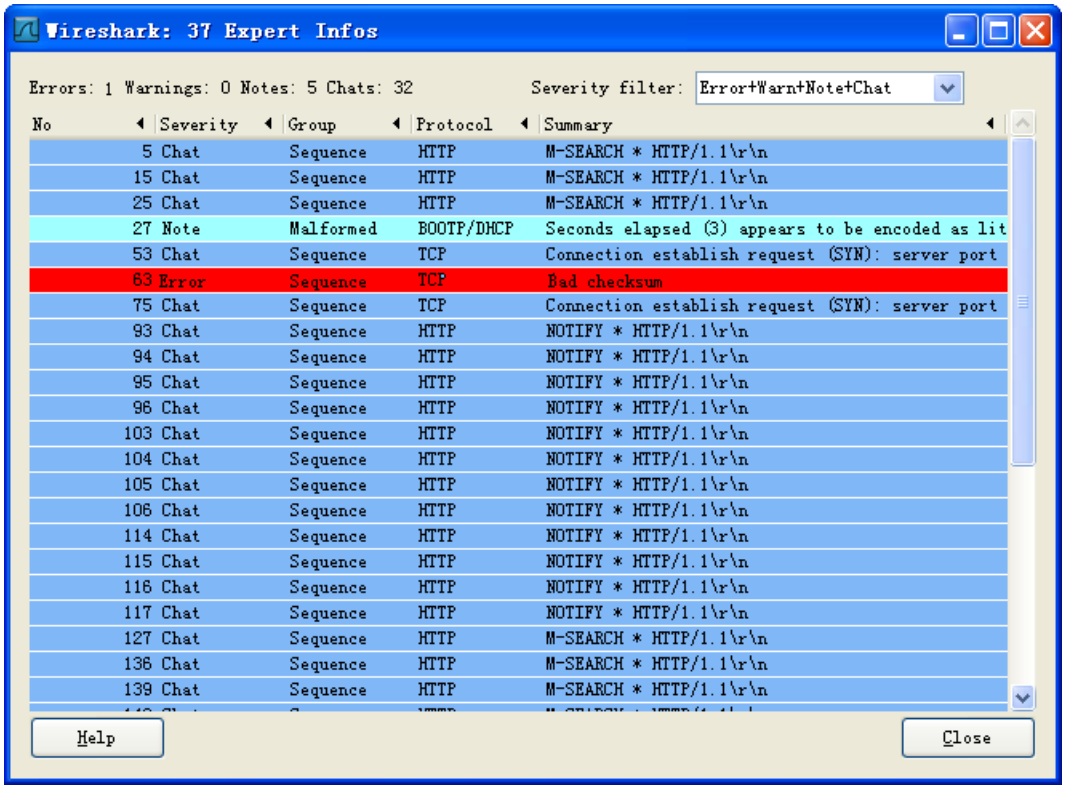
- Filter expressions that specify protocols
  - ip
  - icmp
  - tcp
  - gtp
  - gre
  - http
- Filter expressions that specify addresses
  - IP address
    ip.addr==10.161.225.1
  - Source IP address
    ip.src==10.161.225.1
  - Destination IP address
    ip.dst==10.161.225.1
  - Source Media Access Control (MAC) address
    eth.src == 00:e0:fc:44:5e:a1
  - Source User Datagram Protocol (UDP) port
    udp.srcport == 2123
- Filter expressions that specify fields (message types)
  - GTP Echo Request messages
    gtp.message == 0x01
  - Remote authentication dial-in user service (RADIUS) accounting request or response messages
    radius.code == 4 || radius.code == 5

Filtering Segment Packets

Use the filter criteria !(ip.frag_offset == 0) to check whether segment packets exist.

Choose **Analyze** > **Expert Info**. If `TCP Bad checksum` is displayed, segment packets may exist, as shown in Figure 7-42. The Wireshark does not combine segment packets or verify that `Checksum` is correct. Therefore, `Bad checksum` is displayed.

Figure 7-42 Suspicious packets displayed on the Expert Infos



NOTE

The Ethernet allows a maximum data frame length of 1,500 bytes and the IEEE 802.3 allows a maximum data frame length of 1492 bytes. Maximum data frame length at the link layer is called a Max Transfer Unit (MTU). Most networks have an MTU. If a packet sent from the IP layer is greater in size than the MTU at the link layer, the packet must be divided into fragments whose sizes are smaller than the MTU.

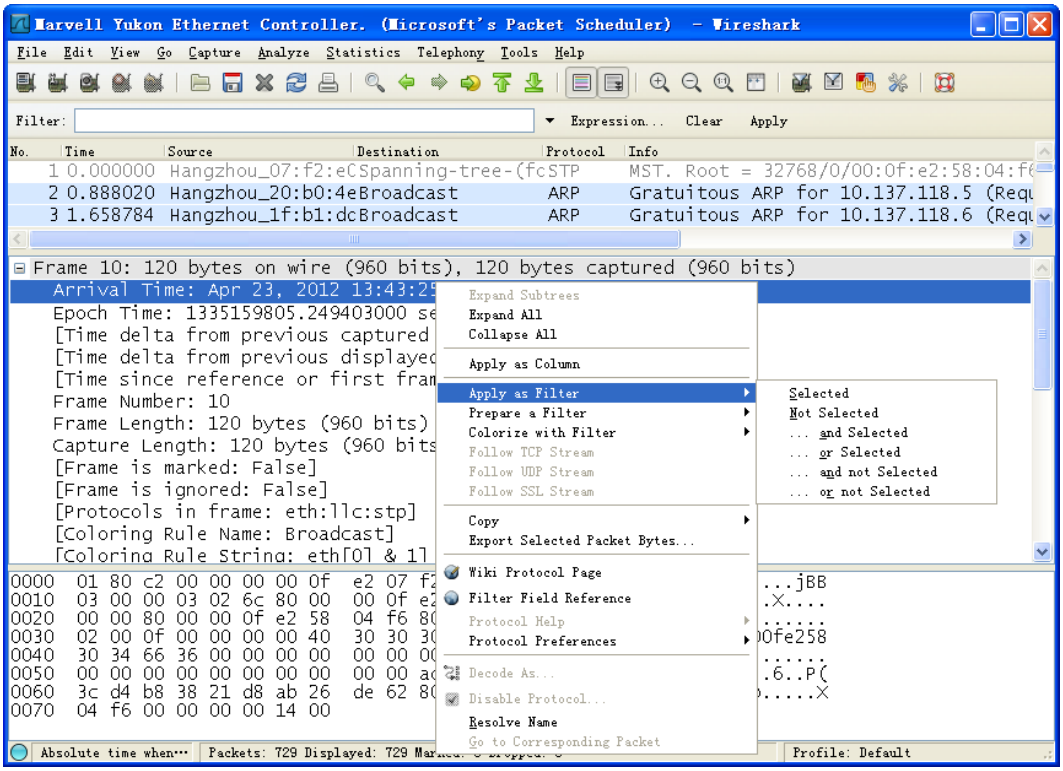
Filter Expression Construction Tips

To use the application filter to construct a filter expression, proceed as follows:

1. Expand the message parsing contents.
2. Right-click a field in packet list pane or packet details pane, and then choose **Apply as Filter** > **Selected**.

   The field is set as a filter criterion and displayed in the **Filter** text box, and the corresponding data packets are displayed based on this expression, as shown in Figure 7-43.

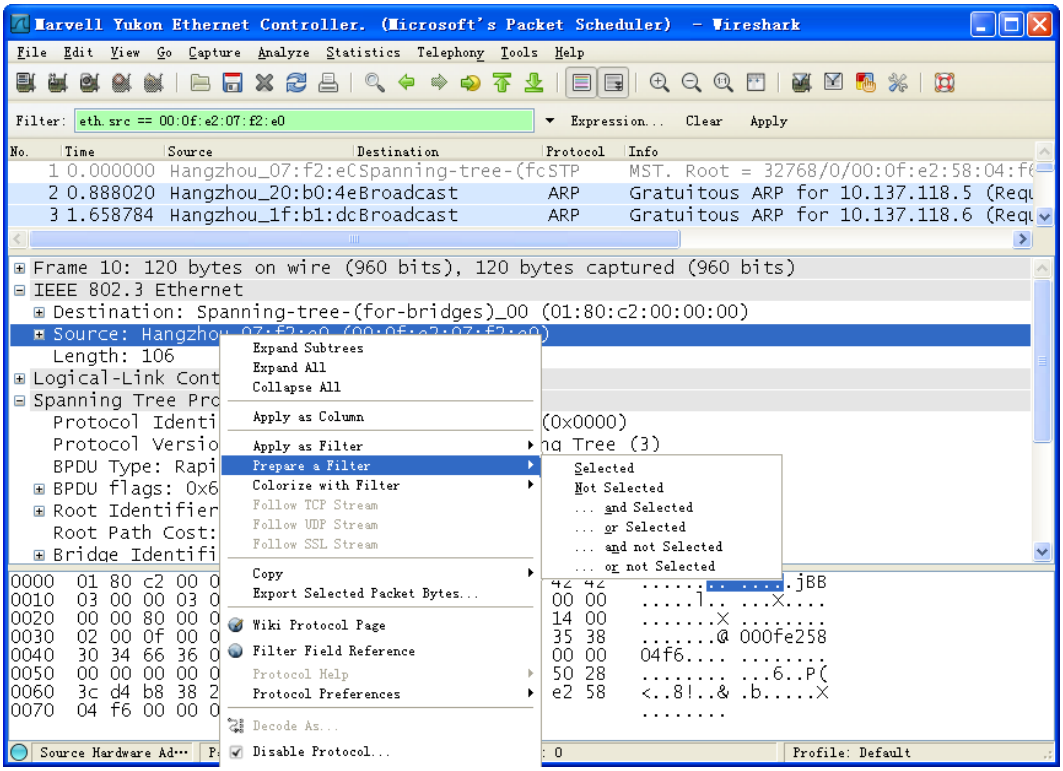
Figure 7-43 Setting a field as a filter criterion and starting the filtering immediately



The differences between the **Prepare a Filter** menu and the **Apply as Filter** menu are as follows:

- After you choose **Apply as Filter** > **Selected**, the selected field is set as the filter criterion directly and the data packets that meet the filter criterion are displayed immediately.
- After you choose **Prepare a Filter** > **Selected**, the selected field is displayed in the **Filter** text box but no filter is performed. You can modify the filter criterion as required. After you click **Apply**, data packets that meet the filter criterion are displayed, as shown in Figure 7-44.

Figure 7-44 Preparing to set a field as a filter criterion



7.7.4 Typical Scenario

SIP Protocol Analysis

This topic describes how to use the Wireshark to analyze SIP signaling.

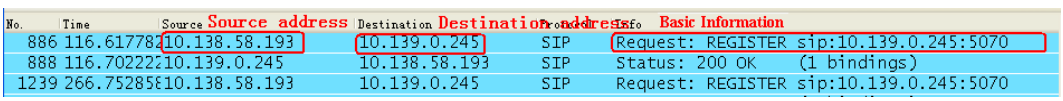
After starting the Wireshark, enter **sip** in the **Filter** text box. Then all SIP signaling that passes through the network adapter is filtered out.

Information in the Captured Packet List Window

Figure 7-45 shows the information in the captured packet list window.

- Source address from which a signaling record is sent
  IP address of the host that sends the signaling record
- Destination address to which a signaling record is sent
- Basic information about a signaling record
  Whether the signaling is a request or a status message.

Figure 7-45 Information in the captured packet list window



After a signaling record is selected, the protocol layer information about the signaling record is displayed in the protocol layer description window.

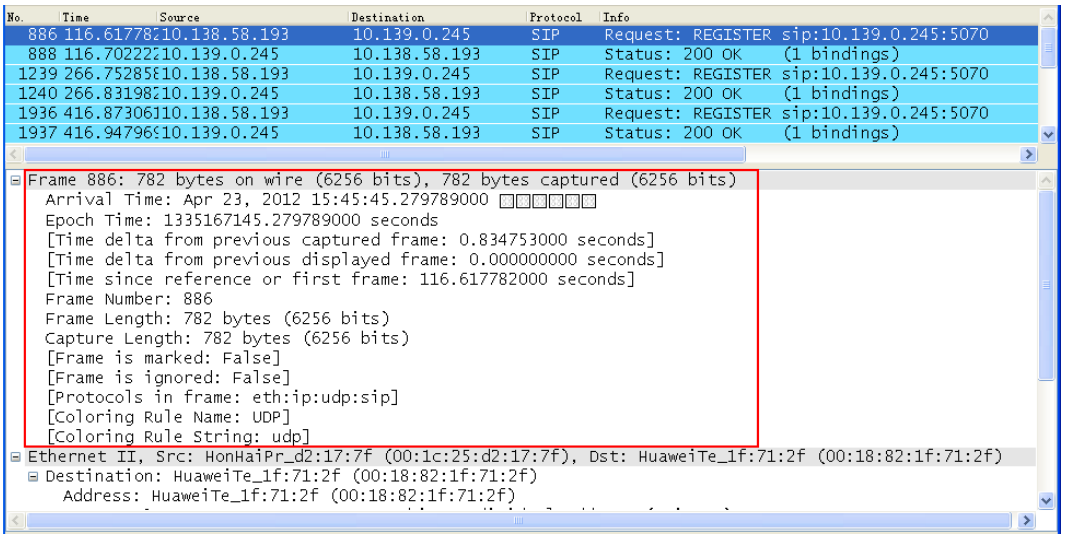
Information in the Protocol Layer Description Window

Pay attention to the information at the application layer.

- Physical layer

  The first layer in the protocol layer description window is the physical layer, which contains **Frame Number** and **Packet Length**, as shown in Figure 7-46.

Figure 7-46 Physical layer of the SIP protocol



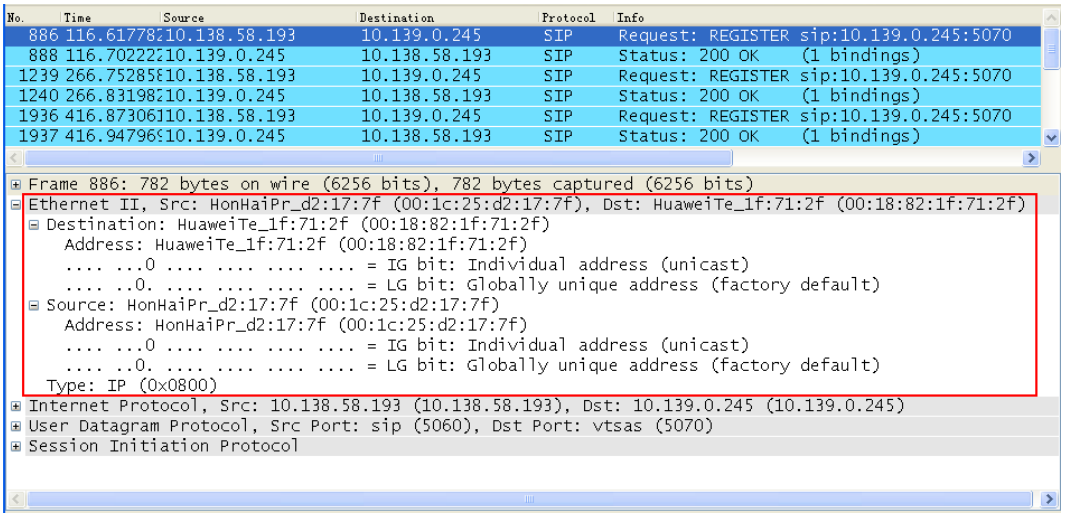
- Data link layer

  The second layer in the protocol layer description window is the data link layer, which contains the MAC address of the sender (**Source**), MAC address of the receiver (**Destination**), and packet type (**Type**), as shown in Figure 7-47.

NOTE

At the data link layer, ensure that the MAC addresses are correct. If the MAC addresses are incorrect, the network device cannot send the packet to the expected destination address.

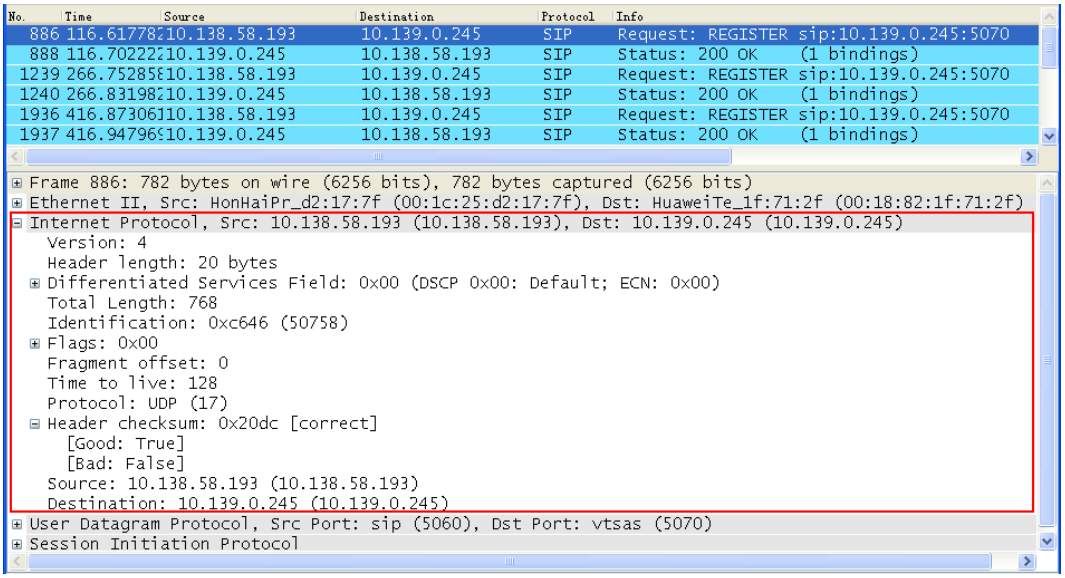
Figure 7-47 Data link layer of the SIP protocol



- Network layer

  The third layer in the protocol layer description window is the network layer, which contains the source IP address (**Source**), destination IP address (**Destination**), packet length (**Total length**), and checksum (**Header checksum**), as shown in Figure 7-48.

Figure 7-48 Network layer of the SIP protocol



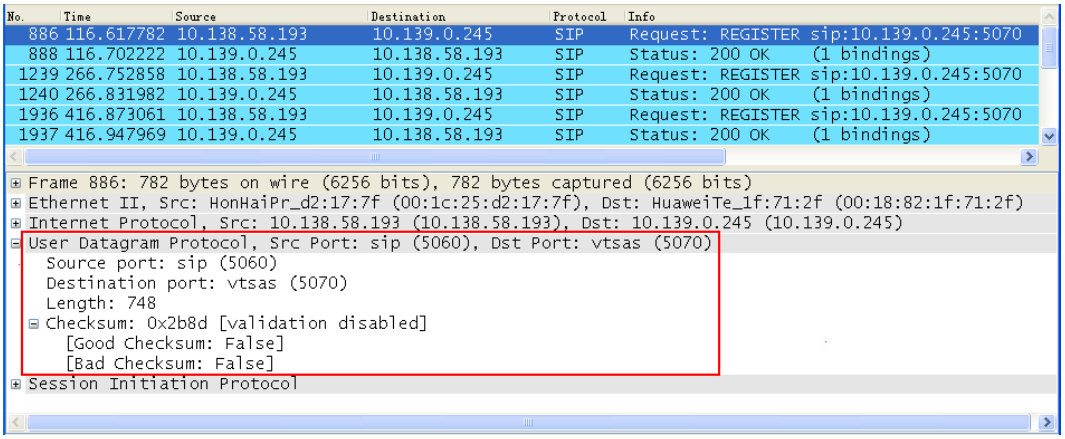
  At the network layer, check whether:

  - The source IP address and destination address are correct.
  - The length of a packet exceeds the maximum length allowed by a certain device.

- Transport control layer

  The fourth layer in the protocol layer description window is the transport control layer, which contains **Source port**, **Destination port**, packet length (**Length**), and **Checksum**, as shown in Figure 7-49.

Figure 7-49 Transport control layer of the SIP protocol



At the transport control layer, check whether:

- The destination port is correct.
- The application process port is correct.
- The checksum information is correct.

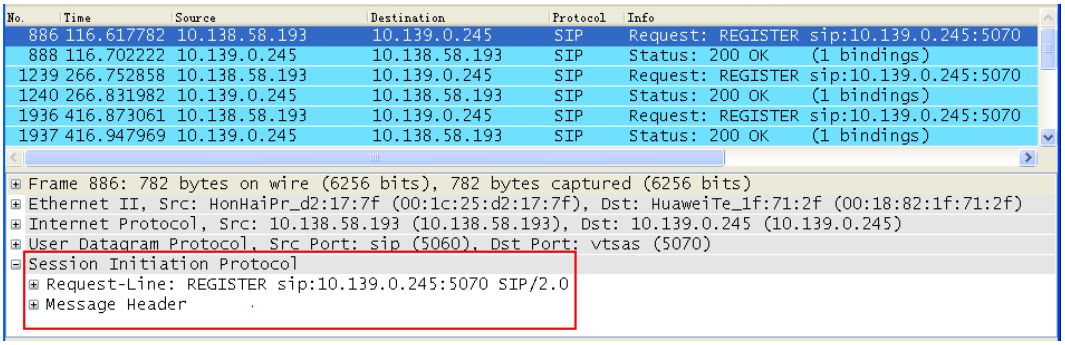
  The network adapters of certain devices may calculate the checksum of the User Datagram Protocol (UDP) layer. If the checksum is incorrect, the network adapter of the device may discard the packet.

- Application layer

  The fifth layer in the protocol layer description window is the application layer, which contains the SIP protocol details.

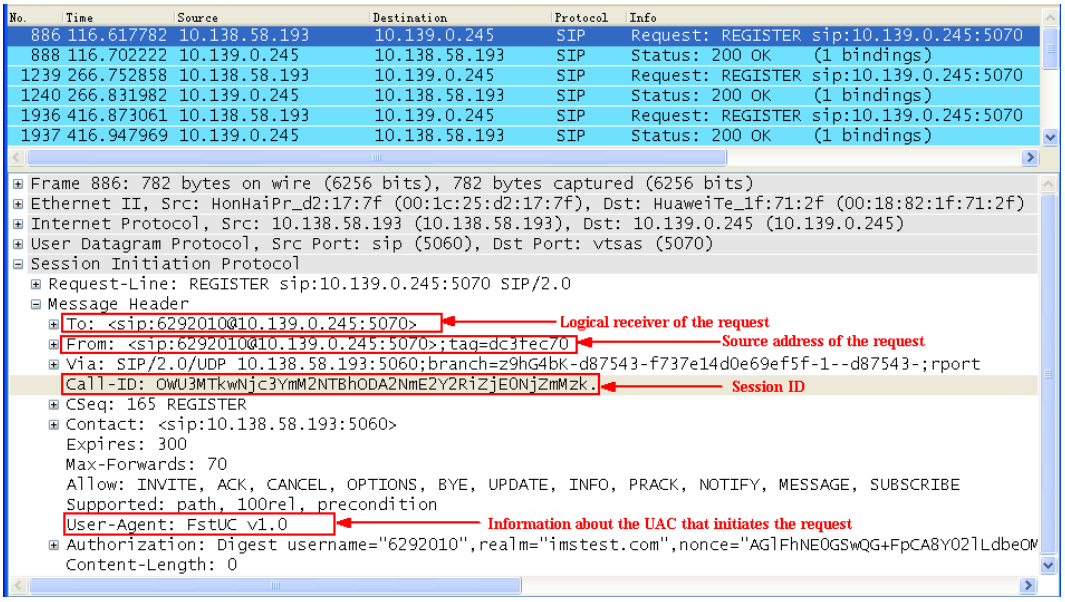
  The signaling record consists of Request-Line and Message Header. If a message includes a message body, Message Body is also included, as shown in Figure 7-50.

Figure 7-50 Request messages at the application layer of the SIP protocol



The message header information can be used to locate faults, as shown in Figure 7-51.

Figure 7-51 Message header information



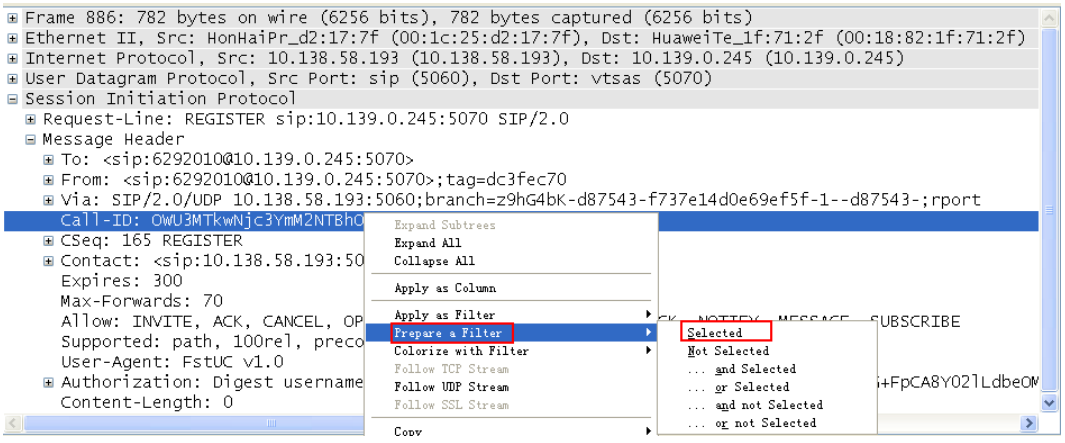
In the message header, pay attention to the following information:

- Call-ID

  Unique identifier of a group of messages. The requests and responses of a UA in a session share the same Call-ID. Therefore, you can obtain the information about the requests and responses of a session by querying the Call-ID.

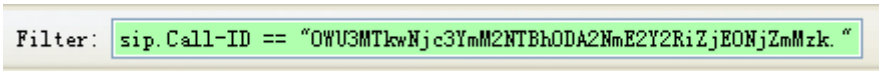
  Right-click a Call-ID to be queried, and then choose **Apply as Filter** > **Selected**, as shown in Figure 7-52.

Figure 7-52 Filtering a Call-ID out



Then the signaling records that share the same Call-ID are displayed in the captured packet list window. The Call-ID that is filtered out is displayed in the **Filter** text box on the toolbar, as shown in Figure 7-53.

Figure 7-53 Value of Filter on the toolbar



- From

  Source address of the request.
- To

  Logical receiver of the request.
- User-Agent

  Information about the User Agent Client (UAC) that initiates the request.

  If the value of **User-Agent** is **Conf-serv/3GPP**, the request is initiated by a personal computer (PC).

SOAP Protocol Analysis

This topic describes how to use the Wireshark to analyze SOAP packets.

Background

To capture a Simple Object Access Protocol (SOAP) packet, pay attention to the following information:

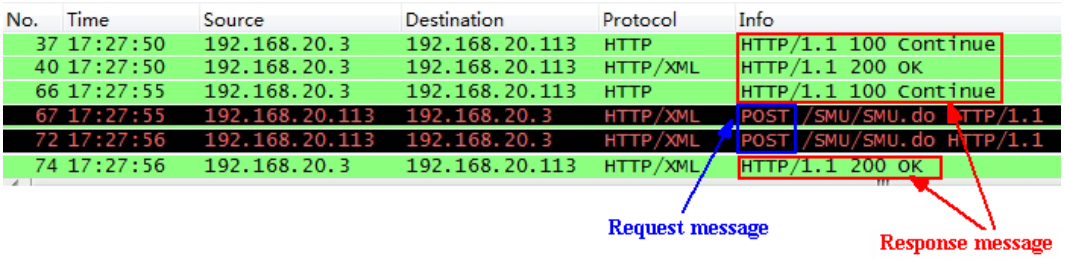
- Capture the packet on the AS.
  - Install the Wireshark of the Linux operating system on the AS.
  - After capturing a SOAP packet using a command on the AS, use the Wireshark to analyze the captured SOAP packet on the Windows host.

    tcpdump -i eth0(actual network adapter name) -w Packet name -s 1200
- After choosing **Capture** > **Options** to set parameters, do not enter any information in the **Capture Filter** text box.
- Enter **http** in the **Filter** text box when capturing SOAP packets, as shown in Figure 7-54.

Figure 7-54 Filter criteria

After capturing the SOAP packet is completed, the Hypertext Transfer Protocol (HTTP) signaling that passes through the network adapter with the IP address of the host is displayed, as shown in Figure 7-55.

Figure 7-55 Filtered HTTP signaling



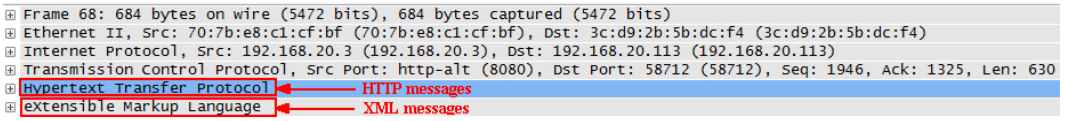
To query signaling details, proceed as follows:

1. Right-click the signaling to be queried.
2. Choose **Show Packet in New Window** from the shortcut menu. A dialog box is displayed, containing the signaling details.

Protocol Analysis

A SOAP message includes HTPP and Extensible Markup Language (XML) messages. Pay attention to the contents at the following layers in the red box, as shown in Figure 7-56.

Figure 7-56 Protocol layers that you need to pay attention to



- HTTP messages

  An HTTP message contains the name and operation of a SOAP request, as shown in Figure 7-57 and Figure 7-58.

  You must pay attention to the method name in the request and the response code in the response.

Figure 7-57 HTTP request

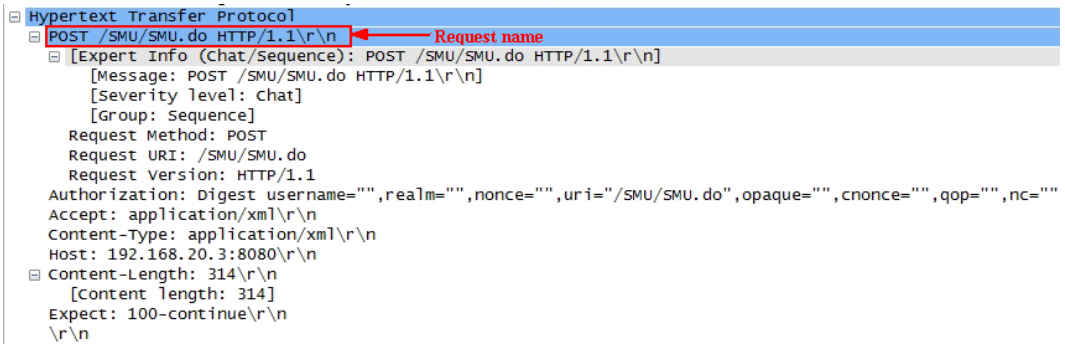
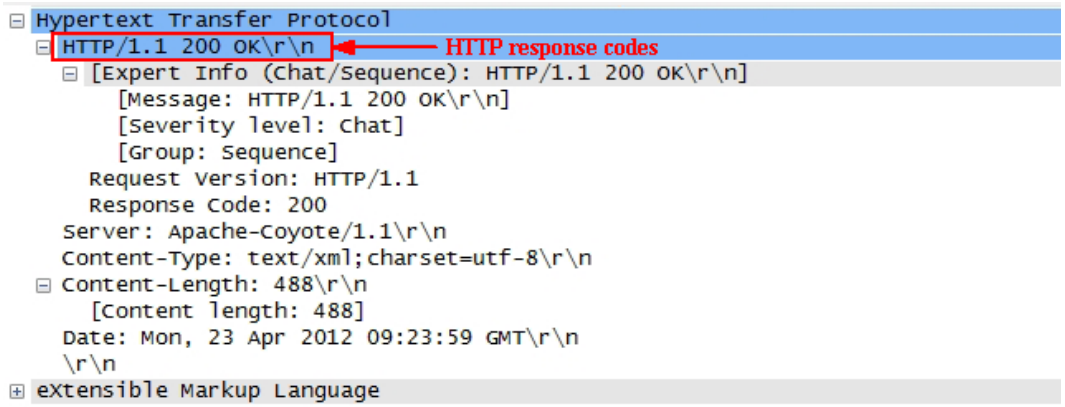


Figure 7-58 HTTP response



- XML messages

  An XML messages contains a message type and a message content.

  – MSG_TYPE presents a message type declaration.

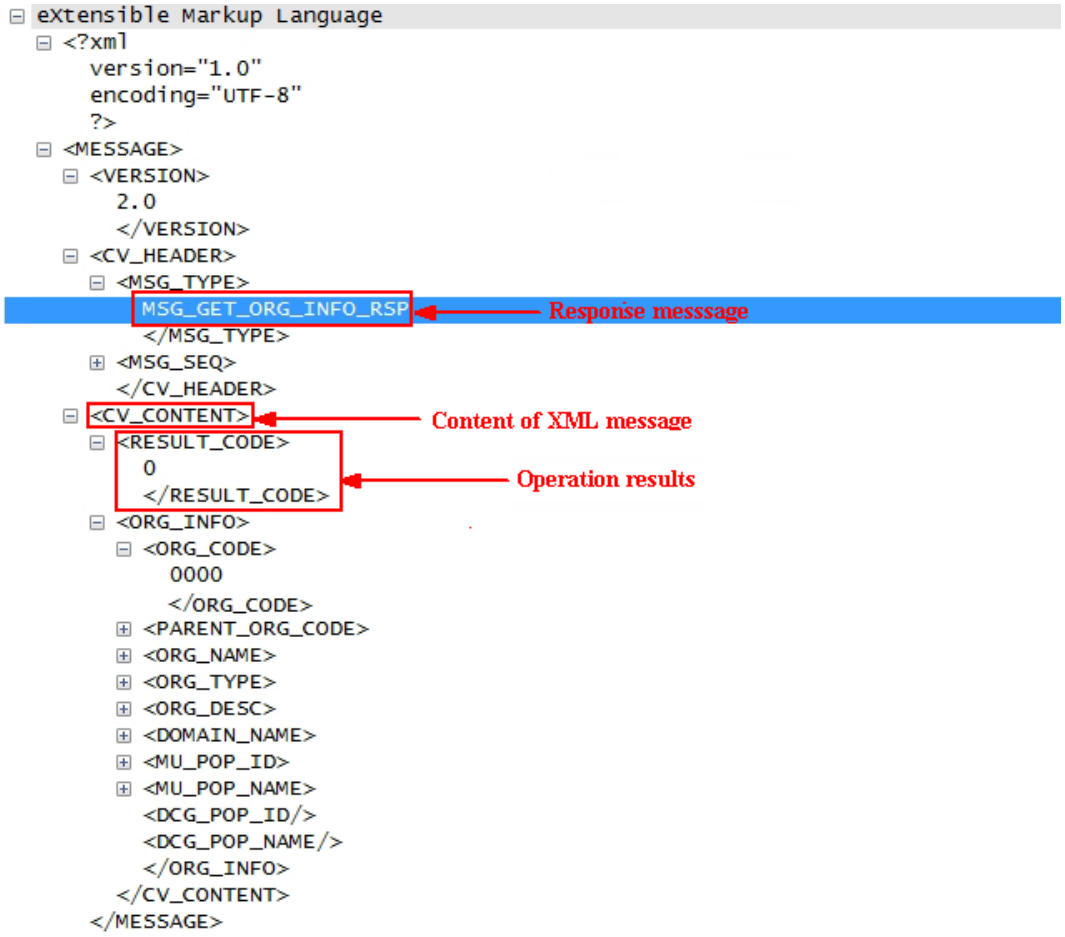
  – CV_CONTENT presents a message content declaration.

  Figure 7-59shows the XML messages in a request for a login in scene.

  Figure 7-60shows the XML messages in a response for a login in scene.

Figure 7-59 XML messages in a request for a login in scene

Figure 7-60 XML messages in a response for a login in scene



7.7.5 Common Tips

Changing the Time Display Mode

CAUTION

The absolute time generated after the gateway GPRS support node (GGSN) users use the tmf2cap to convert .tmf files to .cap files may be incorrect. You can use the relative time to view the packet delay information.

Generally, data packets are displayed by relative time in the program, which is the interval between a subsequent packet and the initial packet.

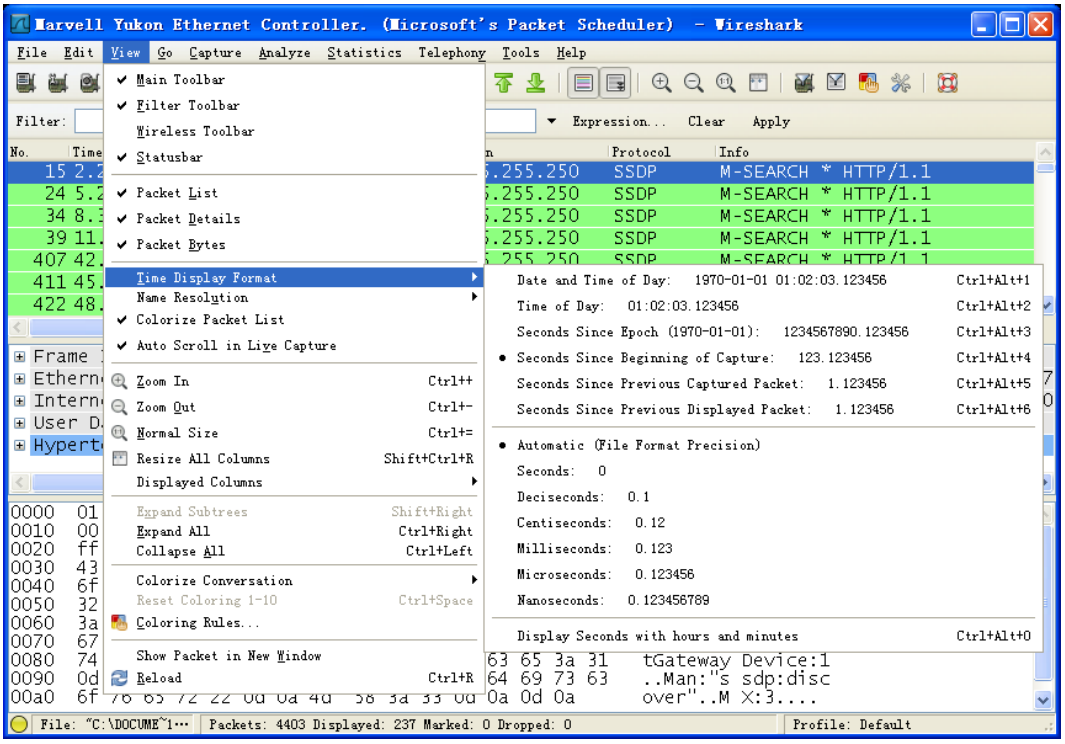
You can choose **View** > **Time Display Format** to change the time display mode.

The **Time Display Format** menu contains four options, as shown in Figure 7-61.

- **Time of Day**: for example, 18:23:01.852876.

- **Date and Time of a Day**
- **Seconds Since Beginning of Capture**
- **Seconds Since Previous Captured Packet**, which is used for viewing the time delay between packets.

Figure 7-61 Changing the time display mode

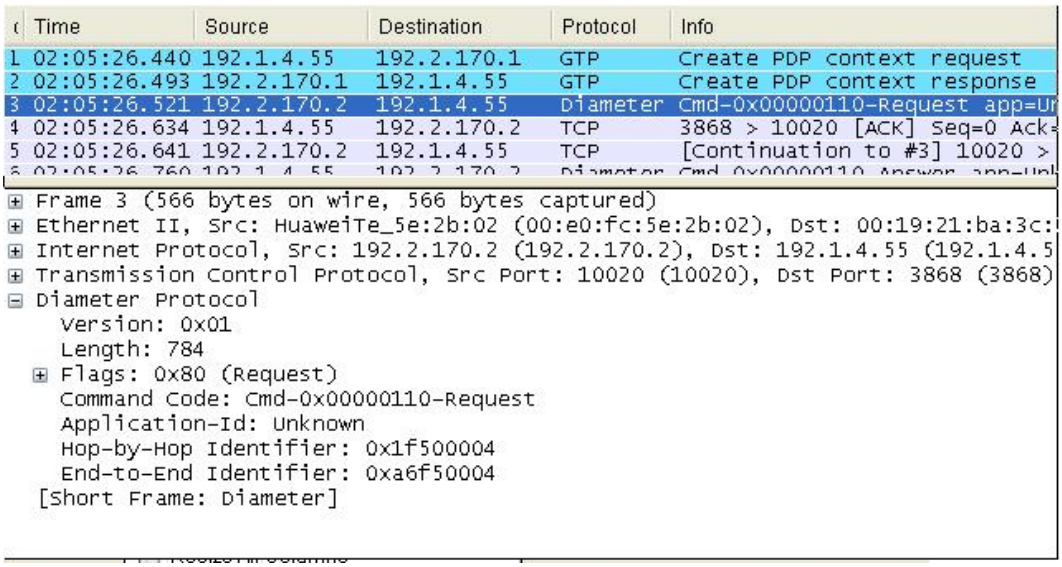


Loading the Custom Format Library

You can download or customize a format library for an application protocol that cannot be parsed by the Wireshark, and then load the format library to the Wireshark. Then the Wireshark can parse the application protocol, as shown in Figure 7-62.

For example, after you decompress the **libxml2.rar** file and copy the .dll file in the decompressed directory to the Wireshark installation directory, the Wireshark can parse the diameter protocol. The default Wireshark installation path is **C:\Program Files\Wireshark**.

Figure 7-62 Parsed diameter protocol after the diameter format library is loaded

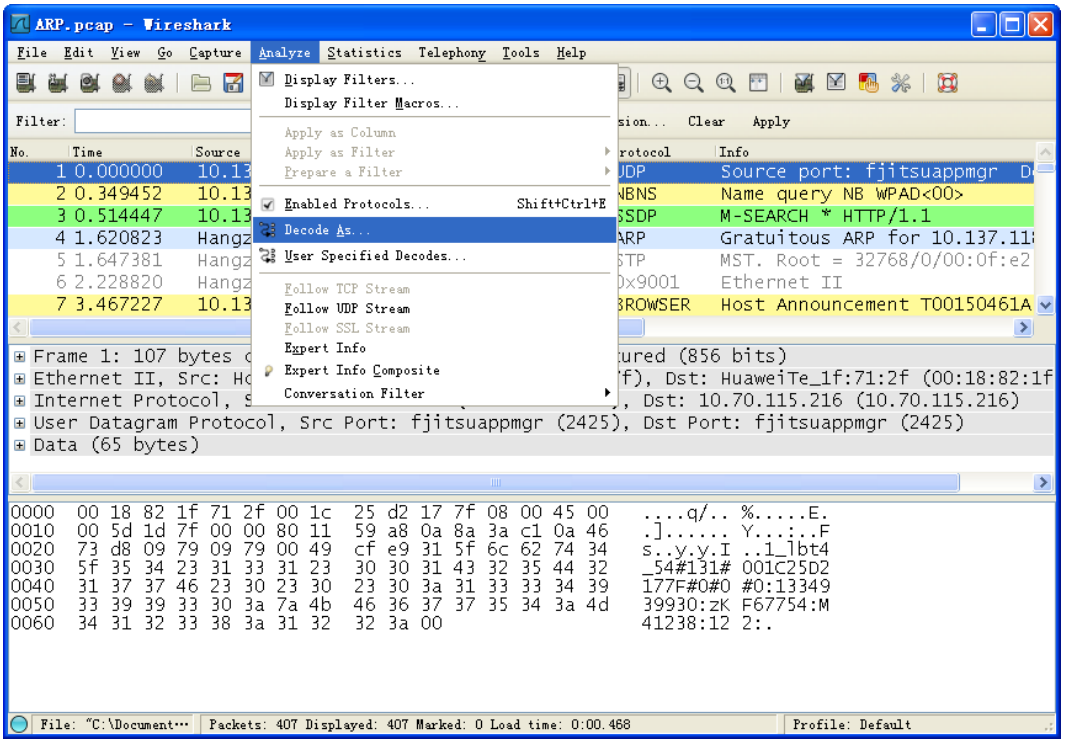


Customizing the Non-Standard Port Applications

The Wireshark cannot identify the type of an application protocol that uses a non-standard port. Users can customize a protocol for parsing the non-standard port application protocol.

1. If the HTTP application has been enabled on port 1031 in an office, select the data packet on port 1031.
2. Choose **Analyze** > **Decode As...**, as shown in Figure 7-63.

Figure 7-63 Decode As

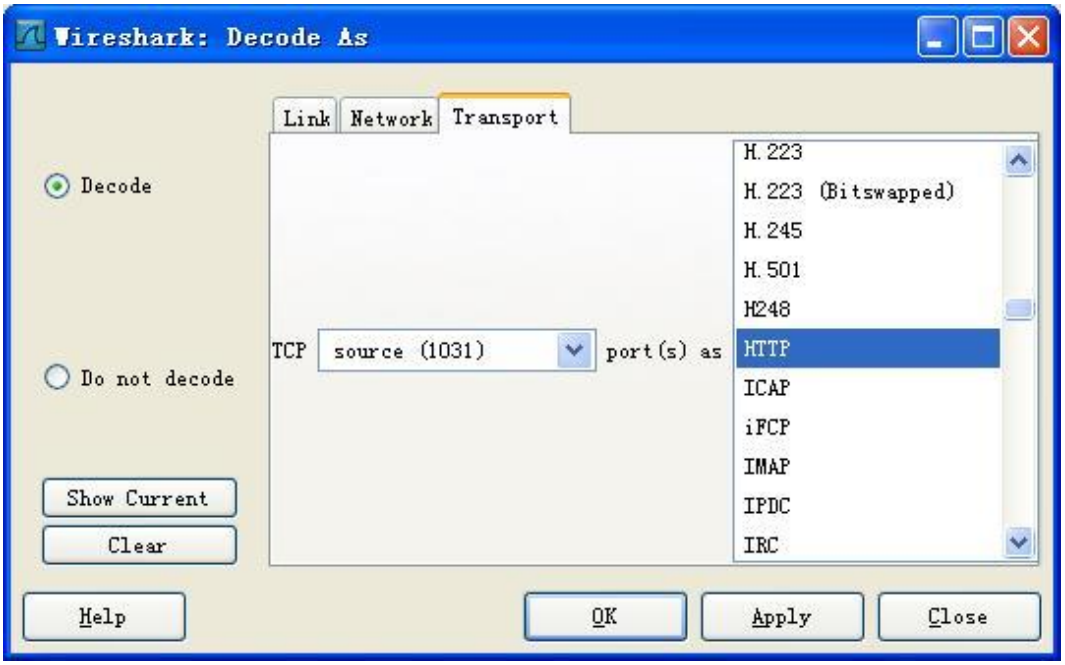


CAUTION

You must choose **Analyze** > **Decode As** and select a protocol each time when you start the Wireshark to parse a non-standard port application protocol.

3. Select an application protocol, and then click **Apply**, as shown in Figure 7-64.

Figure 7-64 Customizing a protocol for parsing the non-standard port application protocol



4. Click **OK**.

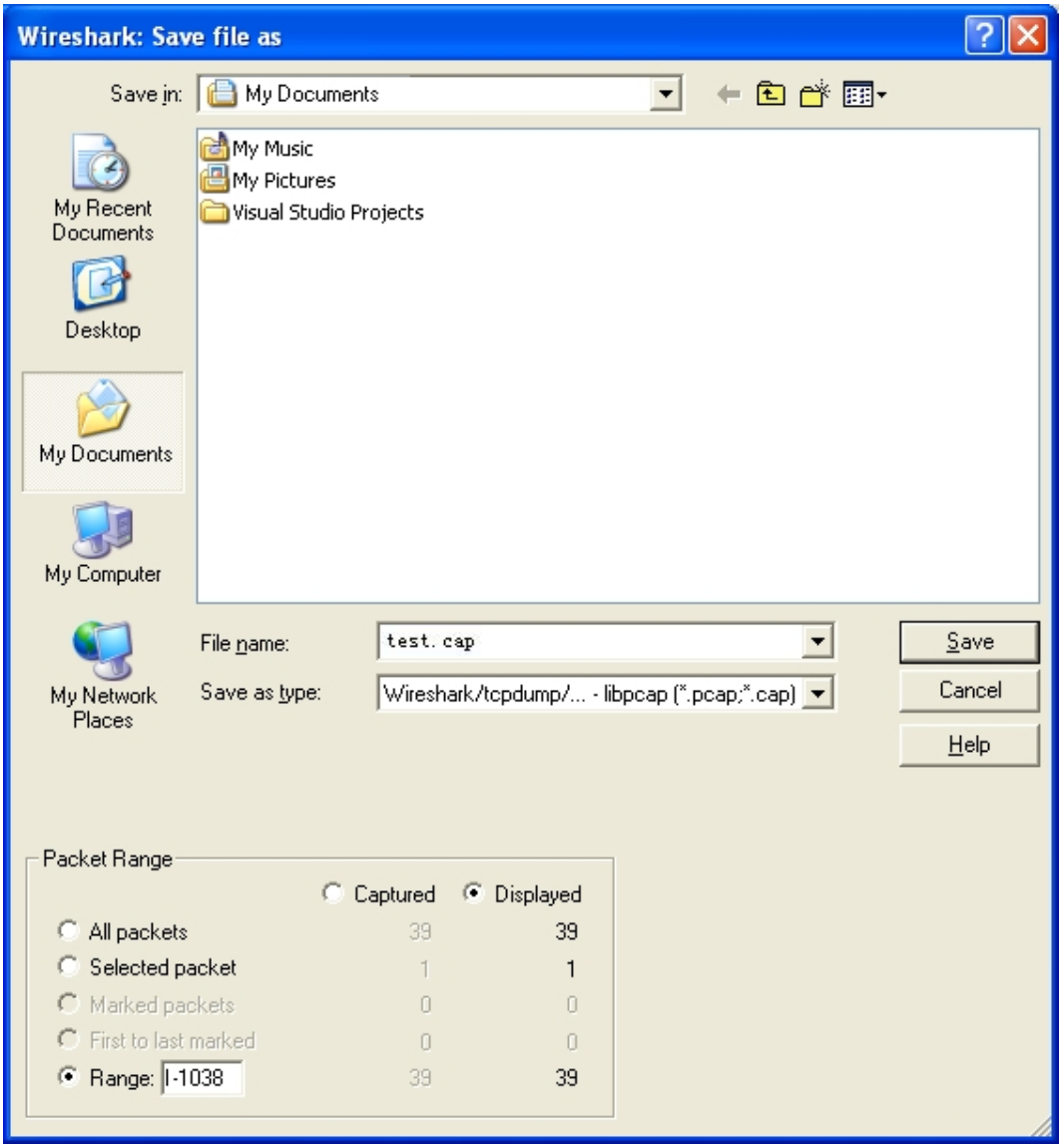
Splitting and Merging Result Files

1. Split a result file.

   Choose **File** > **save as**, and then split a result file, as shown in Figure 7-65.

   - Use the filter to display the information that you want to save as files separately, and then choose **displayed** in the **Packet Range** area.
   - Choose**Range**, and then enter a number range, for example **1-1038**. Then packets numbered from 1 to 1038 are saved as a file.

Figure 7-65 Save file as



2. Merge a result file.

   Choose **File** > **Merge**.

   The system prompts you to save the result file before merging it.

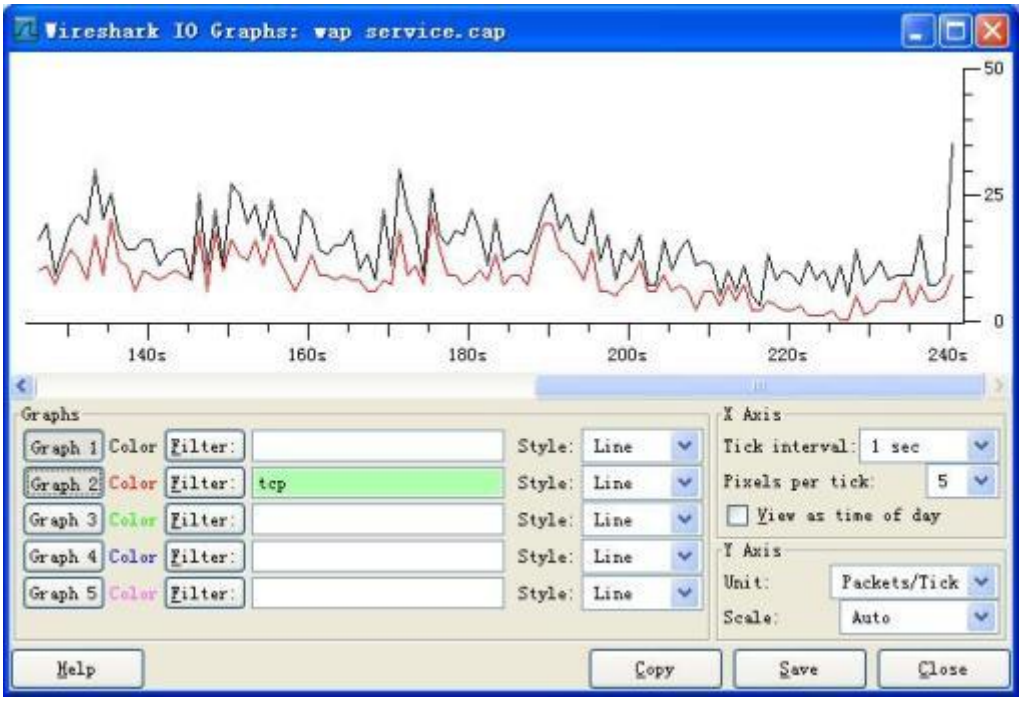
   - Enter the name of the result file to be merged, and then click **Save**.
   - Select the file to which you will merge the result file, and then click **Open**.

Displaying Traffic Waveform Chart

The Wireshark can generate traffic waveform charts based on the captured data packets. You can set filter criteria to display the waveform charts of certain protocol traffic or user traffic in a certain period.

Choose **Statistics** > **IO Graphs**. The **Wireshark IO Graphs** dialog box is displayed, as shown in Figure 7-66.

Figure 7-66 Wireshark IO Graphs



By default, all traffic waveform charts are displayed. After you set the filter criteria in the filter, only traffic waveform charts that meet the filter criteria are displayed.

Calculating the Packet Traffic

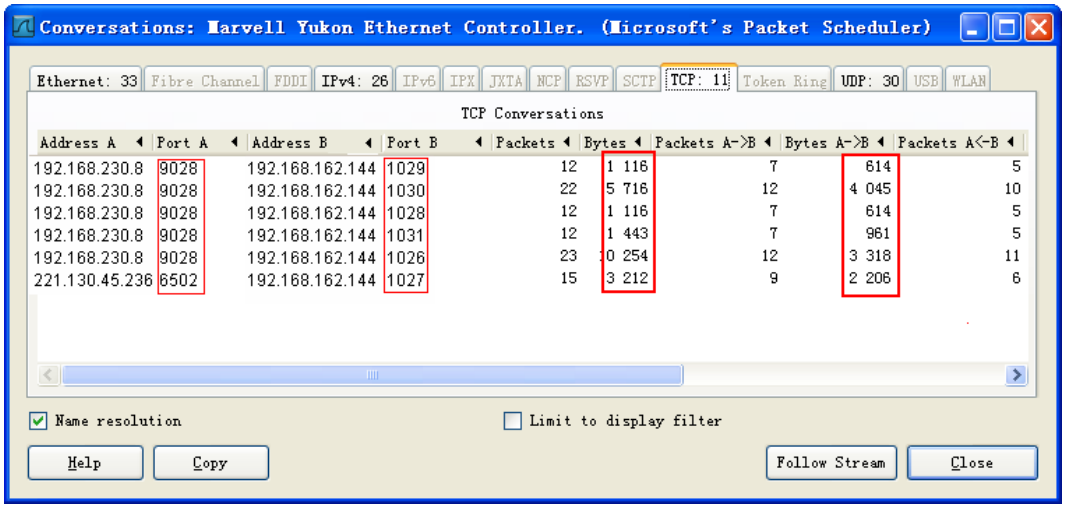
The following describes the common method for calculating the packet traffic.

When receiving a request for calculating the packet traffic, you must verify that the extended field statistics in the Call Detail Records (CDRs) are correct.

- Choose **Statistics** > **Conversations** in the Wireshark.

  The **Conversations** page is displayed, as shown in Figure 7-67.

Figure 7-67 Conversations



In the basic packet information, such as all types of packets generated during mobile phone conversions, the **TCP** and **UDP** tab pages are displayed. On the **TCP** tab page, the following columns are included: **Address A**, **Port A**, **Address B**, **Port B**, **Bytes**, **Bytes A->B**, and **Bytes A<-B**.

On the **TCP** and **UDP** tab pages shown in Figure 7-67, packets that have same address but different port numbers are displayed in different columns but are calculated together.

- Choose **Statistics** > **Summary** to calculate the total packet bytes. Before calculating the total packet bytes, ensure that the filter criteria are set.

  After the preceding packet length is calculated, subtract 14 bytes (layer 2 information) and packet encapsulation added to the original packets by GGSN or Serving GPRS Support Node (SGSN), such as generic routing encapsulation (GRE) or GPRS tunneling protocol (GTP) encapsulation. The various encapsulation lengths are as follows:

  – GTP V0 header 20 bytes

    GTP V1 header: The fixed part is 8 bytes and the common part is 12 bytes.

  – UDP header

    8 bytes

  – IP header

    20 bytes

  – GRE header

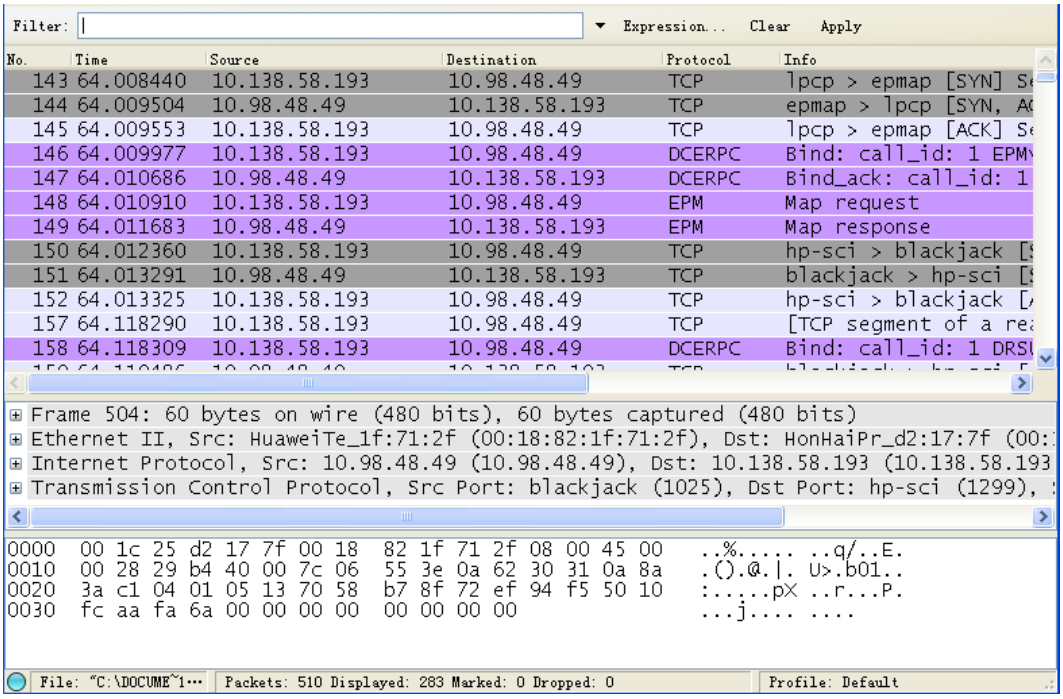
    4 bytes

The window for parsing packets in the Wireshark includes:

- Upper part: area for obtaining packet serial numbers
- Middle part: area for parsing the selected packet
- Lower part: area for displaying the original code streams for the selected packet

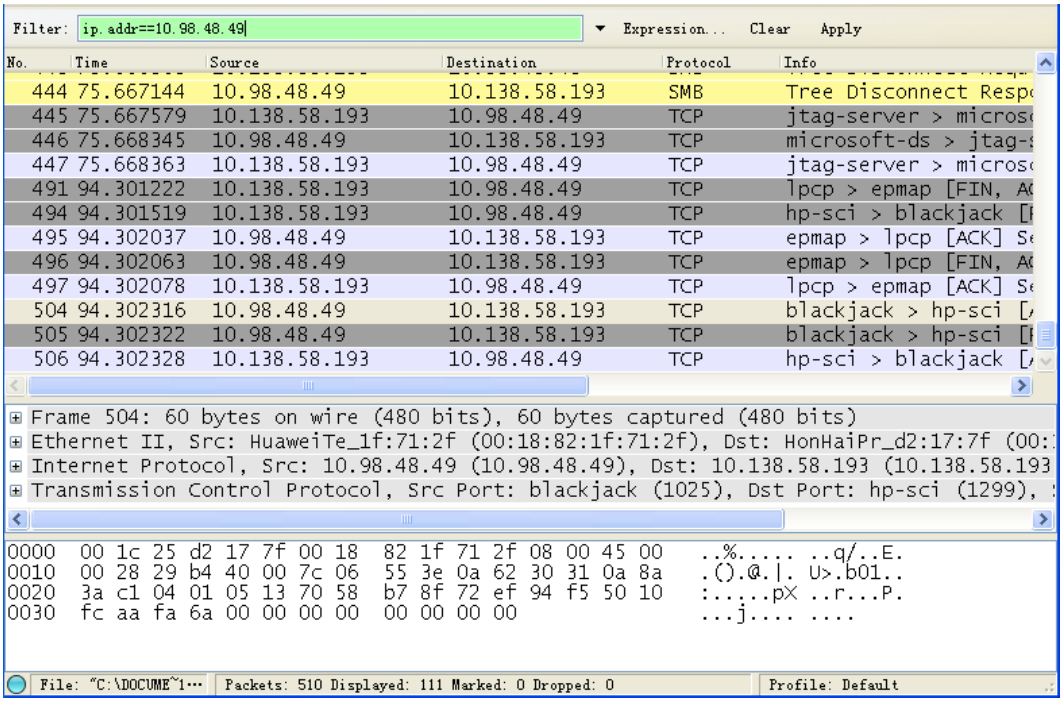
In the Wireshark, you can enter filter criteria in the **Filter** text box shown in Figure 7-68; the packets that meet the filter criteria are displayed.

Figure 7-68 Parsing packets in the Wireshark



For example, to query the packets that are sent from or to the IP address 10.0.0.1, enter **ip.addr==10.0.0.1** in the **Filter** text box shown in Figure 7-68, and then click **Apply**. The packets that are sent from or to the IP address 10.0.0.1 are displayed, as shown Figure 7-69.

Figure 7-69 Filtering out the captured packets



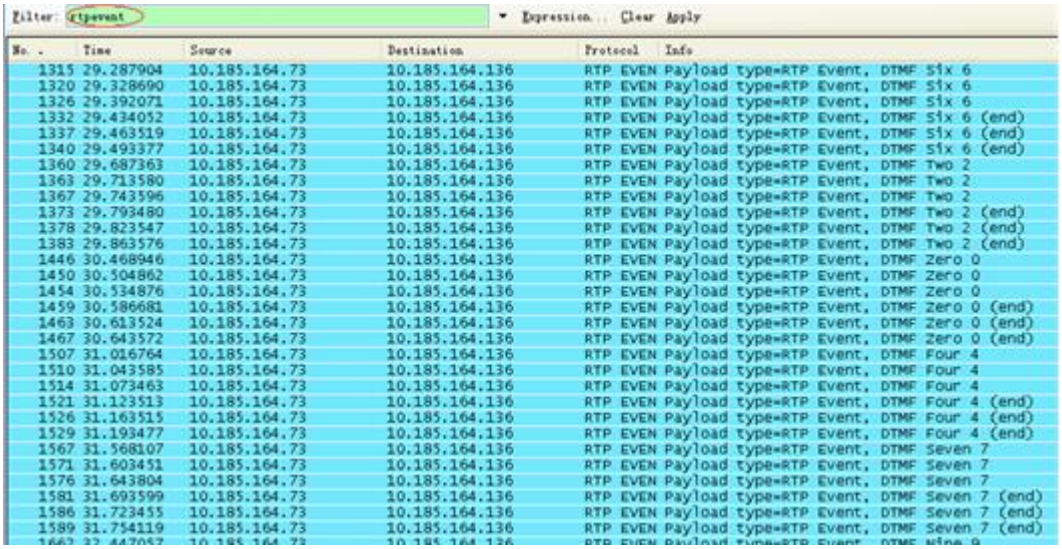
Using the RTP to Analyze 2833 Packets

To use the RTP to analyze 2833 packets, proceed as follows:

1. Use the Wireshark to open the bearer network port captured file in .pcap or .cap format.
2. Enter **(rtp) && (rtp.p_type > 34)** or **rtpevent** in the **Filter** text box.
3. Press **Enter**.

   All files that are transferred using RFC 2833 in the captured information are filtered out, as shown in Figure 7-70.

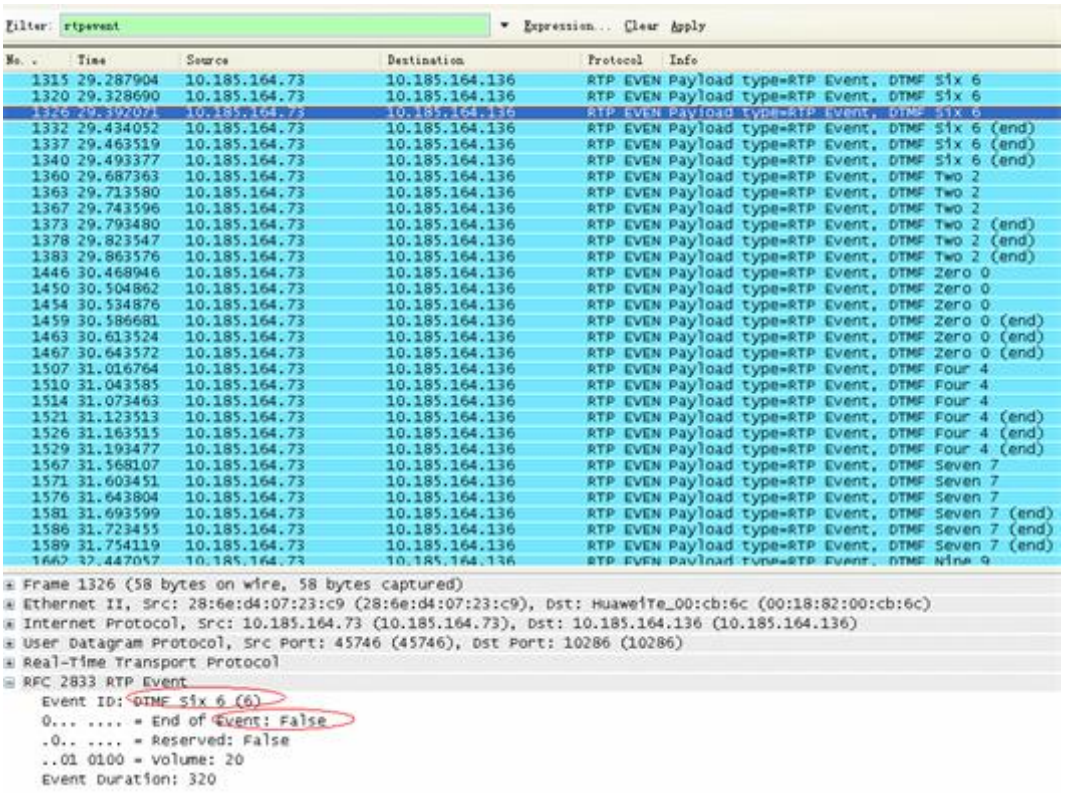
Figure 7-70 RTP information



2833 packets use the sampling mode to send a number for multiple times. Numbers are separated by RTP packets whose **Event** is **TRUE**, as shown in Figure 7-71. The procedure for sending the number 6 is used as an example.

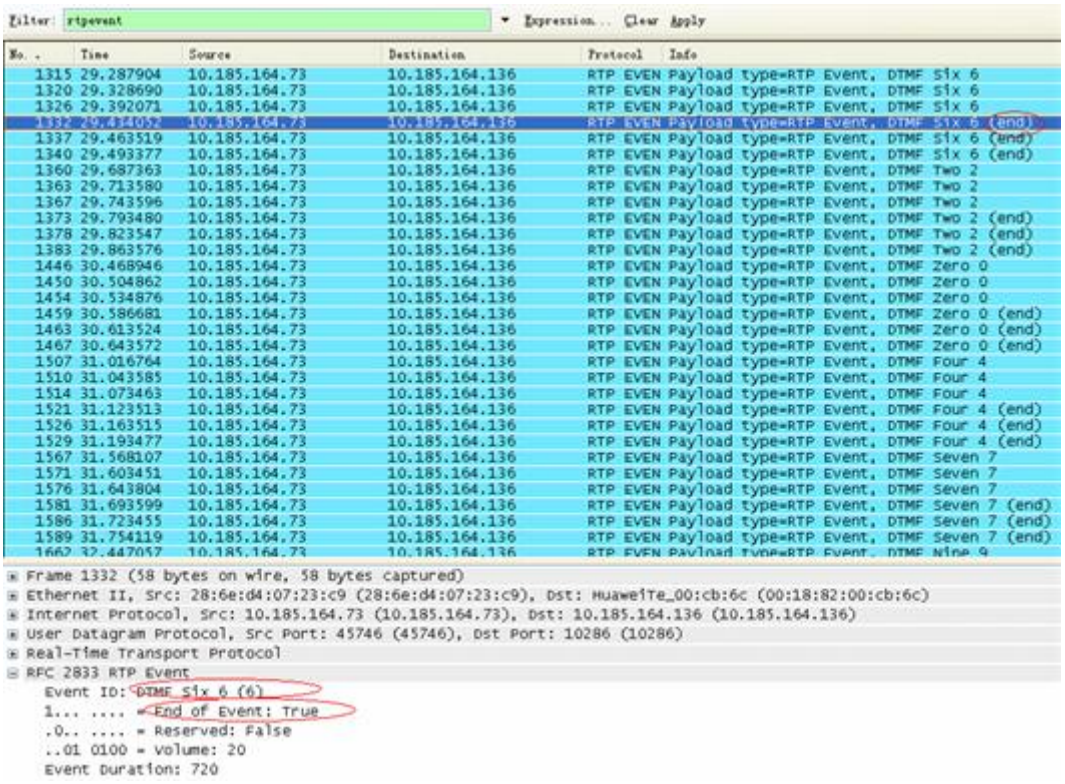
- The message "End of Event: False" in the packet parsing area indicates that the number 6 has not been sent completely.

Figure 7-71 Message "End of Event: False"



- The message "End of Event: True" in the packet parsing area indicates that the number 6 has been sent to the media stream. Then the number collection process is complete.

Figure 7-72 Message "End of Event: True"

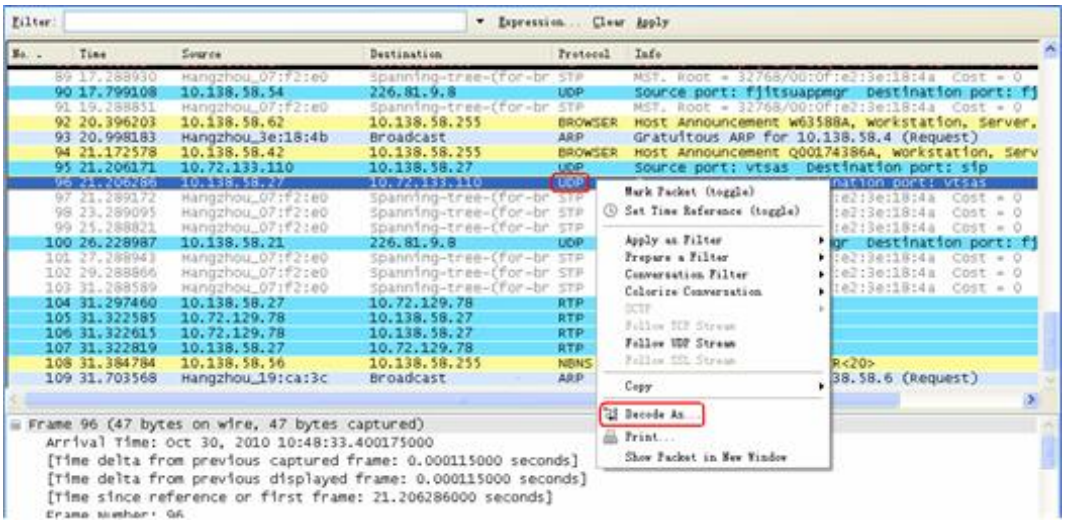


To convert the captured UDP packets to RTP packets, go to 4.

4. Right-click a signaling record in the **UDP** column.

   A shortcut menu is displayed, as shown in Figure 7-73.

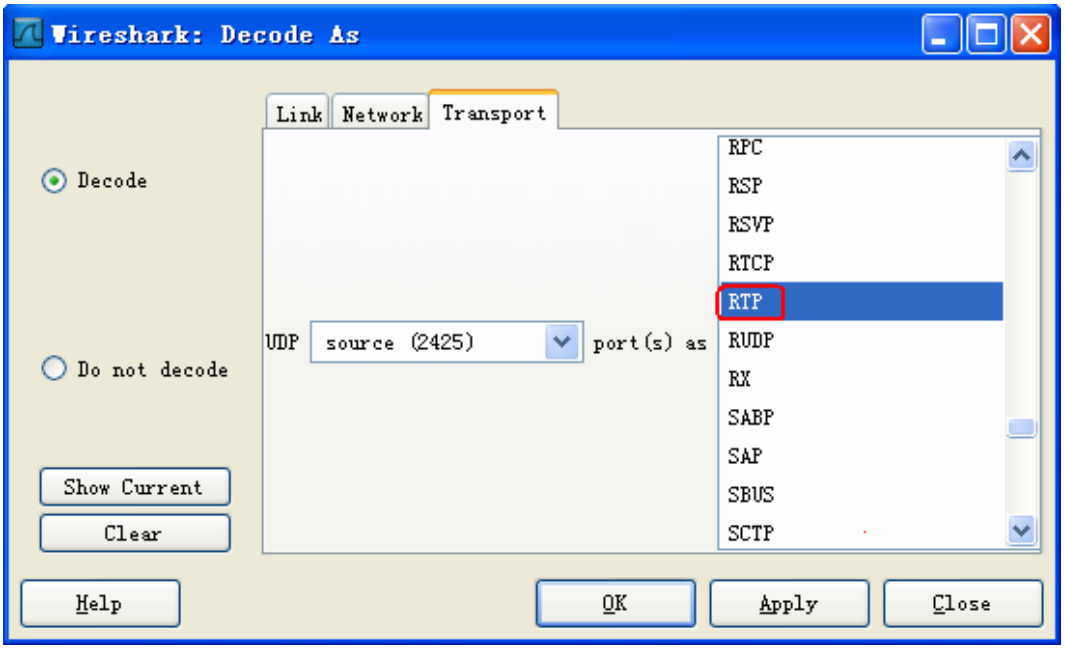
Figure 7-73 Displayed shortcut menu



5. Choose **Decode As...**.

   The **Decode As** dialog box is displayed, as shown in Figure 7-74.

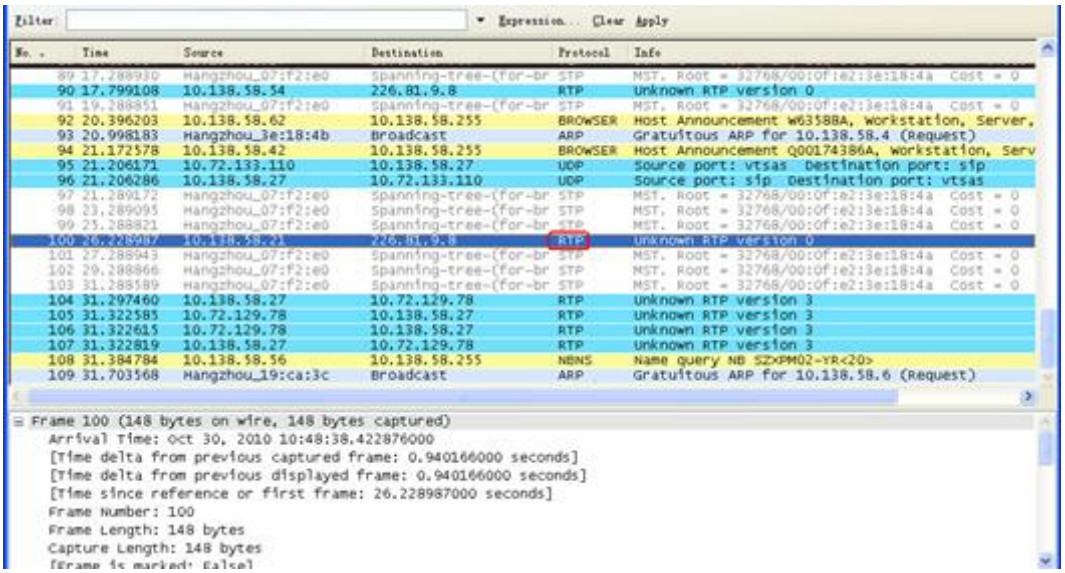
Figure 7-74 Decode As



6. Select **RTP** on the right pane.
7. Click **OK**.

   A page shown in Figure 7-75 is displayed. The captured UDP packets have been converted to RTP packets. Then perform 1 through 3 to verify that the packet information has been transmitted to the media stream.

Figure 7-75 Converting UDP packets to RTP packets



Viewing Call Processes

The Wireshark allows you to view call processes and play voice recordings. The procedure is as follows:

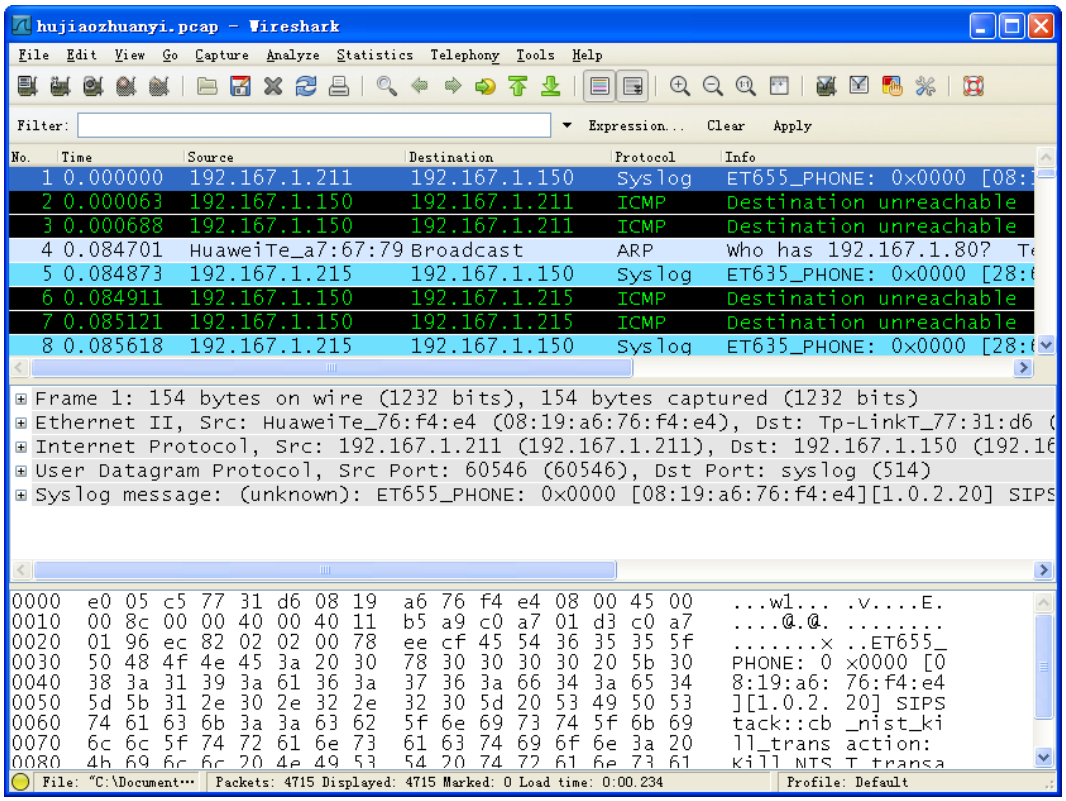
NOTE

This topic describes how to view the call forwarding process. First you need to capture the data packets related to call forwarding and save the captured packets as a .pcap file, such as **hujiaozhuanyi.pcap**.

1. Double-click **hujiaozhuanyi.pcap** on the PC.

   The system shows the call forwarding data, as shown in Figure 7-76.

Figure 7-76 Call forwarding



2. Select a data packet record and choose **Telephony** > **VoIP Calls**.

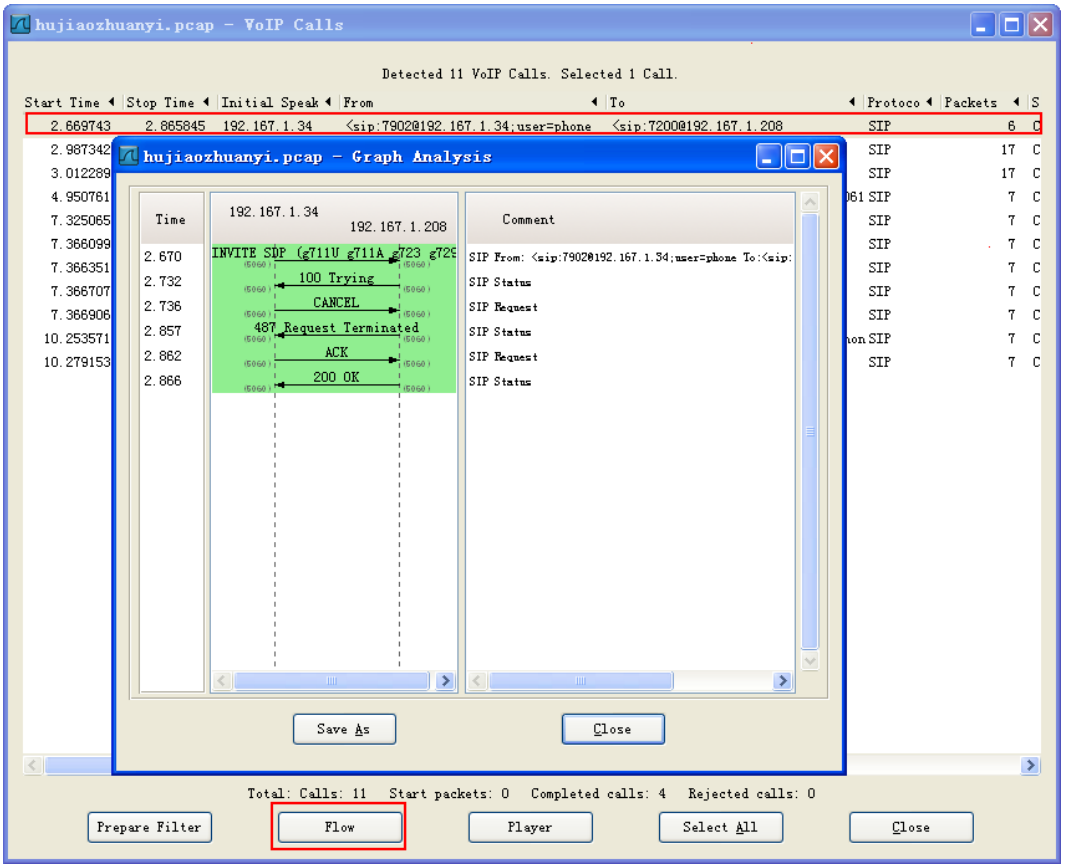
   The **VoIP Calls** page is displayed.

3. View the call process.

   a. Select a call record and click **Flow**.

      The **Graph Analysis** page is displayed, as shown in Figure 7-77.

Figure 7-77 Call process



NOTE

To select all call records, click **Select All**.

b. (Optional) Click **Save as**.

Specify a path and file type, and enter the file name in the **Save file as** dialog box, and then click **Save**.

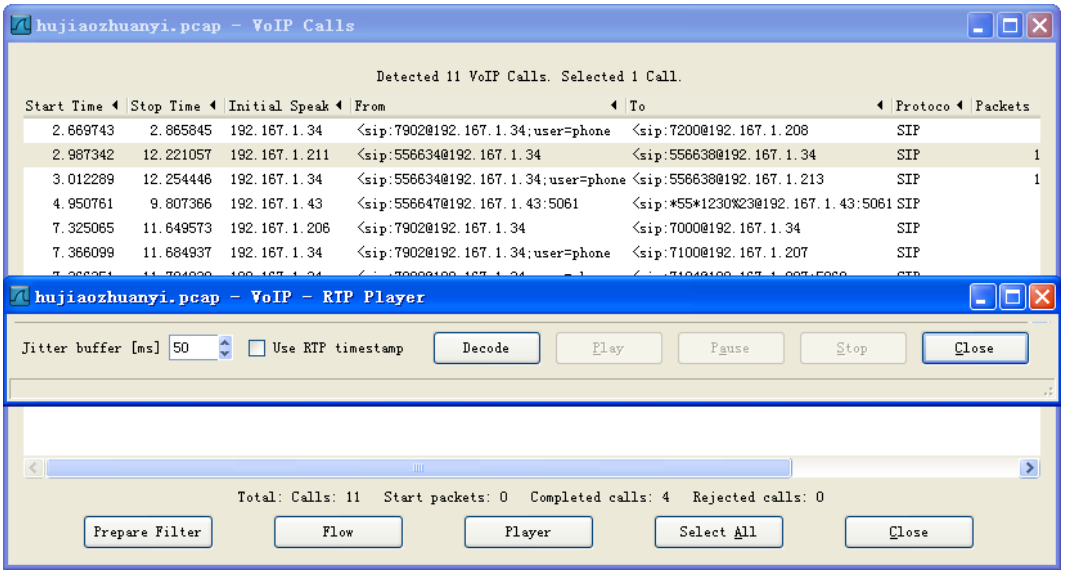
c. Click **Close**.

4. Play the voice recording.

a. Select a call record and click **Player**.

The **VoIP-RTP Player** page is displayed, as shown in Figure 7-78.

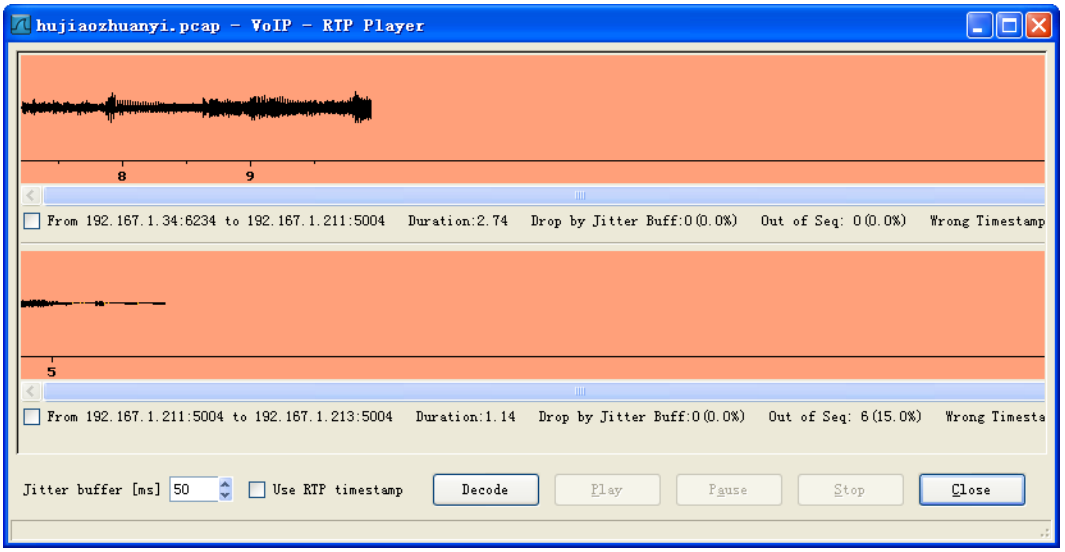
Figure 7-78 VoIP-RTP Player



b. Click **Decode**.

The voice recording page is played is displayed, as shown in Figure 7-79.

Figure 7-79 Voice recordings



c. Select one or more voice recordings, and click **Play**.

The system plays the recordings one by one.

NOTE

You can click **Pause** or **Stop** to stop the play.

d. Click **Close**.

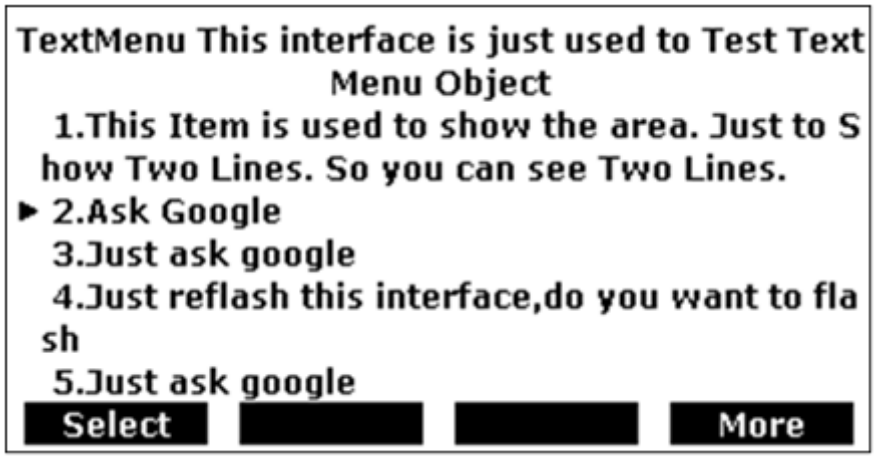
7.8 XML Files Supported by the XML Browser

The XML browser supports seven types of XML files. This section describes the parameters in the files.

7.8.1 TextMenu

Figure 7-80 shows the page of the TextMenu type, which displays menu items in text.

Figure 7-80 Page of the TextMenu type



An example of the XML file of the TextMenu type is as follows:

```
<****TextMenu
defaultIndex = "some integer"
style = "numbered/none/radio"
Beep = "yes/no"
Timeout = "some integer"
LockIn = "yes/no"
WrapList = "yes/no"
>
<Title wrap = "yes/no">Menu Title</Title>
<MenuItem>
    <Prompt>First Choice</Prompt>
    <URI>http://somepage.xml</URI>
    <Dial>Number to dial</Dial>
    <Selection>Selection</Selection>
</MenuItem>
<SoftKey index = "1-6">
    <Label>TextLabel</Label>
    <URI>http://someserver/somepage OR SoftKey:someaction</URI>
</SoftKey>
</****TextMenu >
```

Table 7-5 lists the parameters in the XML file of the TextMenu type.

Table 7-5 Parameters in the XML file of the TextMenu type

Parameter	Mandatory	Value Type	Description
****TextMenu	Yes	The string **** can be any value, including a blank character string.	Root element.
defaultIndex	No	Integer	Default index for accessing the menu page. Default value: 1
style	No	numbered none radio	Style of the icon to the left of a menu. • **numbered**: number icon. • **none**: no icon. • **radio**: radio icon.
Beep	No	yes no	Indicates whether the IP phone plays a beep tone when accessing the menu. Default value: no
Timeout	No	Integer Unit: second	Timeout interval. If a user does not perform any operations within the interval, the IP phone returns to the standby page. Default value: 45
LockIn	No	yes no	If the parameter is set to **yes**, the IP phone responds only to the defined soft keys. For example, when a user picks up the IP phone, the dialing page is not displayed. If the **Dial** menu item is set to a value, a user can make a call after picking up the phone. Default value: no
WrapList	No	yes no	Indicates whether to display the menu item specified by **Prompt** in multiple lines if the menu item is too long. Default value: no
Title	Yes	Character string	Title on the menu page.
wrap	No	yes no	Indicates whether to display the title in multiple lines if the title is too long. Default value: no
MenuItem	Yes	None	Menu item. A maximum of 30 menu items

Parameter	Mandatory	Value Type	Description
			can be set.
Prompt	Yes	Character string	Menu item title, which is controlled by **wrapList**.
URI	Yes	URI	Operation corresponding to the menu item.
Dial	No	Phone number	When this menu item is selected, the IP phone makes a call to the phone number if a user picks up the phone, presses the account key, or presses the handsfree key.
Selection	No	Character string	If the URI of a soft key is an HTTP address, the IP phone suffixes **?selection**=*Preset parameter* to the HTTP address.
SoftKey	No	XML object	For details, see 7.8.8 Soft Keys.

Table 7-6 lists the default soft keys if no soft keys are defined in the XML file of the TextMenu type.

Table 7-6 Default soft keys on the page of the TextMenu type

Soft Key Index	Name	URI
1	Exit	SoftKey:Exit
4	Select	SoftKey:Select

Table 7-7 lists the functions of keys on the page of the TextMenu type.

Table 7-7 Functions of keys on the page of the TextMenu type

Key Name	Key	Function
UP/DOWN	Up and down arrow keys	Moves the cursor up or down.
Digitkey	Number keys 1 to 9	Moves the cursor to the menu item indicated by the same number. If the number key that a user presses is larger than the number of menu items, the IP phone moves the cursor to the last menu item.
Select	Soft key. URI="SoftKey:Select"	Invokes a command (for example, the **http** or **Dial** command) to access the URI in the menu item.
Exit	Soft key. URI="SoftKey:E	Displays the previous XML page. If the current page is the first page that a user views, the IP phone displays the

Key Name	Key	Function
	xit"	standby page.
OffHook/Linekey/Handfree	Off-hook/Account key/Handsfree key	If the **Dial** menu item is not blank, the IP phone makes a call to the number specified by the **Dial** menu item. If the menu item is blank and the value of **LockIn** is **yes**, the IP phone does not respond to the keys; if the menu item is blank and the value of **LockIn** is **no**, the IP phone displays the dialing page.
Cancel	X key on an IP phone	Returns to the standby page.
Ok	OK key on an IP phone	If the value of LockIn is no, the **OK** key functions as the **Select** key; if the value of **LockIn** is **yes**, the IP phone does not respond to this key.
DSS key except the key assigned the SIP account function	DSS key, including keys on expansion modules	If the value of **LockIn** is **no**, the IP phone performs the function specified by the DSS key; if the value of **LockIn** is **yes**, the IP phone does not respond to this key.

7.8.2 TextScreen

Figure 7-81 shows the page of the TextScreen type, which displays a text note.

Figure 7-81 Page of the TextScreen type

An example of the XML file of the TextScreen type is as follows:

```
<****TextScreen
doneAction = "some URI"
Beep = "yes/no"
Timeout = "some integer"
LockIn = "yes/no"
>
<Title wrap = "yes/no">Screen Title</Title>
<Text>The screen text goes here</Text>
```

```
</****TextScreen>
```

Table 7-8 lists the parameters in the XML file of the TextScreen type.

Table 7-8 Parameters in the XML file of the TextScreen type

Parameter	Mandatory	Value Type	Description
****TextScreen	Yes	The string **** can be any value, including a blank character string.	Root element.
Beep	No	yes no	Indicates whether the IP phone plays a beep tone when accessing the menu. Default value: no
doneAction	No	URI	URI that an IP phone accesses when a user presses the **done** soft key.
Timeout	No	Integer Unit: second	Timeout interval. If a user does not perform any operations within the interval, the IP phone returns to the standby page. Default value: 45
LockIn	No	yes no	If the parameter is set to yes, the IP phone responds only to the defined soft keys. For example, when a user picks up the IP phone, the dialing page is not displayed. Default value: no
Title	Yes	Character string	Title of the text note.
Wrap	No	yes no	Indicates whether to display the title in multiple lines if the title is too long. Default value: yes
Text	Yes	Character string	Title of the text note.
SoftKey	No	XML object	For details, see 5.3.8 Soft Keys.

Table 7-9 lists the default soft key if no soft keys are defined in the XML file of the TextScreen type.

Table 7-9 Default soft key on the page of the TextScreen type

Soft Key Index	Name	URI
1	Exit	SoftKey:Exit

Table 7-10 lists the functions of keys on the page of the TextScreen type.

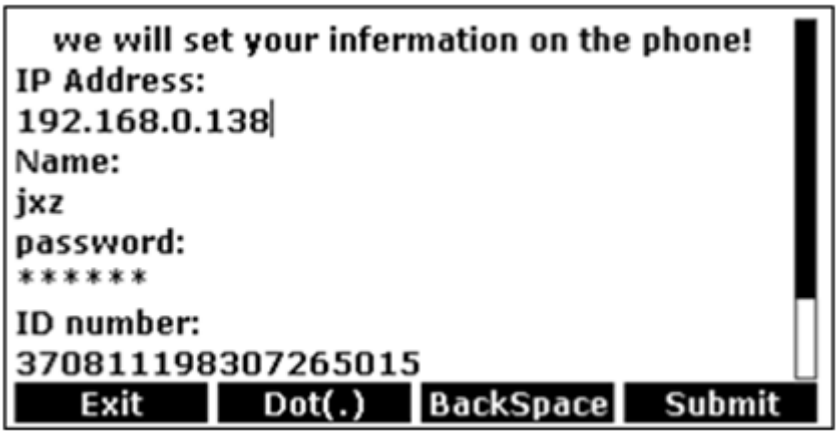
Table 7-10 Functions of keys on the page of the TextScreen type

Key Name	Key	Function
UP/DOWN	Up and down arrow keys	Scrolls through the text.
Digitkey	Number keys 1 to 9	The IP phone has no response when users press number keys.
Exit	Soft key. URI="SoftKey:Exit"	Displays the previous XML page. If the current page is the first page that a user views, the IP phone displays the standby page.
OffHook/Linekey /Handfree/DSSkey	Off-hook/Account key/Handsfree key/DSS key	If the value of **LockIn** is **no**, the IP phone displays the dialing page or performs the function specified by the DSS key; if the value of **LockIn** is **yes**, the IP phone does not respond to the keys.
Cancel	X key on an IP phone	Returns to the standby page.
Ok	OK key on an IP phone	Accesses the URI specified by **doneAction**.

7.8.3 InputScreen

Figure 7-82 shows the page of the InputScreen type, which asks a user to enter information and sends the information to the server.

Figure 7-82 Page of the InputScreen type



An example of the XML file of the InputScreen type is as follows:

```
<****InputScreen
type = "IP/string/number/timeUS/timeInt/dateUS/dateInt"
password = "yes/no"
editable = "yes/no"
Beep = "yes/no"
Timeout = "some integer"
LockIn = "yes/no"
defaultIndex = "some integer 1 to 6"
displayMode = "normal/condensed"
inputLanguage = "English/French/German/Italian/Spanish"
>
<Title wrap = "yes/no">Title string</Title>
<Prompt>Guidance for the input</Prompt>
<URL>Target receiving the input</URL>
<Parameter>name of the parameter add to URL</Parameter>
<Default>Default Value (1)</Default>
<InputField
type = "IP/string/number/timeUS/timeInt/dateUS/dateInt/empty"
password = "yes/no"
editable = "yes/no"
>
<Prompt>Guidance for the input</Prompt>
<URL>Target receiving the input</URL>
<Parameter>parameter name add to URL</Parameter>
<Default>Default Value</Default>
<Selection>Selection</Selection>
</InputField>
</****InputScreen>
```

Table 7-11 lists the parameters in the XML file of the InputScreen type.

Table 7-11 Parameters in the XML file of the InputScreen type

Parameter	Mandatory	Value Type	Description
****InputScreen	Yes	The string **** can be any value, including a blank character string.	Root element.
Type	Yes	IP string number timeUS timeInt dateUS dateInt empty	Data type. • **IP**: IP address • **string**: character string • **number** • **timeUS**: time in 12-hour format. AM indicates a time in the morning, and PM indicates a time in the afternoon. • **timeInt**: time in 24-hour format • **dateUS**: date in the format

Parameter	Mandatory	Value Type	Description
			MM/DD/YYYY • **dateInt**: date in the format DD/MM/YYYY • **empty**: blank lines. The number of lines is specified by **displayMode**. Default value: string (Currently, only the value **string** is supported.)
Beep	No	yes no	Indicates whether the IP phone plays a beep tone when accessing the menu. Default value: no
Password	No	yes no	An asterisk (*) is displayed when a user enters a character. Default value: no
Timeout	No	Integer Unit: second	Timeout interval. If a user does not perform any operations within the interval, the IP phone returns to the standby page. Default value: 45
LockIn	No	yes no	If the parameter is set to **yes**, the IP phone responds only to the defined soft keys after the page of the InputScreen type is displayed. For example, when a user picks up the IP phone, the dialing page is not displayed. Default value: no
inputLanguage	No	English French German Italian Spanish	Language of the content that a user enters. Default value: English
displayMode	No	normal condensed	• **Normal**: indicates that the field and text box are displayed in two lines. • **Condensed**: indicates that the field and text box are displayed in one line. Default value: Normal
defaultIndex	No	Integer	Default text box index if multiple text boxes exist. Default value: 1
Title	Yes	Character string	Title of the entered object.
Wrap	No	yes	Indicates whether to display the title in

Parameter	Mandatory	Value Type	Description
		no	multiple lines if the title is too long. Default value: yes
Prompt	No	Character string	Prompt information entered by a user.
URL	Yes	URL	URL to which the IP phone sends the information entered by a user.
Parameter	Yes	Character string	Name of the parameter that the IP phone suffixes to an URI. The new URI is in the format *old URI?Parameter=information entered by a user*.
Default	No	Character string	Information that is entered by default.
InputField	No	None.	A maximum of six text boxes can be set.
Type	No	IP string number timeUS timeInt dateUS dateInt empty	Data type. • **IP**: IP address • **string**: character string • **number** • **timeUS**: time in 12-hour format. AM indicates a time in the morning, and PM indicates a time in the afternoon. • **timeInt**: time in 24-hour format • **dateUS**: date in the format MM/DD/YYYY • **dateInt**: date in the format DD/MM/YYYY • **empty**: blank lines. The number of lines is specified by **displayMode**. Currently, only the value **string** is supported.
password	No	yes no	An asterisk (*) is displayed when a user enters a character. Default value: no
editable	No	yes no	Indicates whether a user can enter information. The value **no** indicates that a user cannot enter information or modify the default information. Default value: yes
Prompt	No	Character string	Prompt information entered by a user.

Parameter	Mandatory	Value Type	Description
Default	No	Character string	Information that is entered by default.
Selection	No	Character string	If the URI of a soft key is an HTTP address, the IP phone suffixes **?selection**=*Preset parameter* to the HTTP address. Example: http://10.1.0.105/input.php?selection=1
Softkey	No	XML object	Soft key to be added, for example, the soft key for adding input methods. A maximum of six soft keys are added.
SoftKey	No	XML object	For details, see 7.8.8 Soft Keys.

Table 7-12 lists the formats of the timeUS, timeInt, dateUS, and dateInt types.

Table 7-12 Description of the timeUS, timeInt, dateUS, and dateInt types

Type	Format	Example
timeUS	HH:MM:SS AM/PM HH: 1 to 12, MM: 0 to 59, SS: 0 to 59	02:00:23 AM 12:59:00 PM
timeInt	HH:MM:SS HH: 0 to 23, MM: 0 to 59, SS: 0 to 59	23:25:00
dateUS	MM/DD/YYYY MM: 1 to 12, DD: 1 to 31, YYYY: 0000 to 9999	12/31/2009
dateInt	MM/DD/YYYY MM: 1 to 12, DD: 1 to 31, YYYY: 0000 to 9999	31/01/2010

Table 7-13 lists the default soft keys that are used when no soft keys are set and **Type** is set to **IP** in the XML file of the InputScreen type.

Table 7-13 Default soft keys when Type is set to IP

Soft Key Index	Name	URI
1	Exit	SoftKey:Exit
2	Dot	SoftKey:Dot
3	Backspace	SoftKey: BackSpace
4	Submit	SoftKey: Submit

Table 7-14 lists the default soft keys that are used when no soft keys are set and **Type** is set to **Number** in the XML file of the InputScreen type.

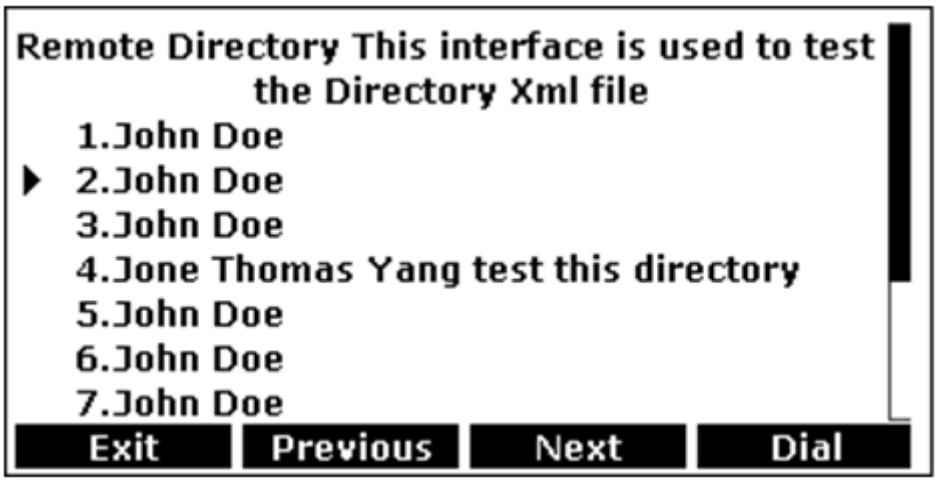
Table 7-14 Default soft keys when Type is set to Number

Soft Key Index	Name	URI
1	Exit	SoftKey:Exit
3	Backspace	SoftKey: BackSpace
4	Submit	SoftKey: Submit

7.8.4 Directory

Figure 7-83 shows the page of the Directory type, which is used for downloading phone books from the server and displays phone books on the LCD.

Figure 7-83 Page of the Directory type



An example of the XML file of the Directory type is as follows:

```
<****Directory
Next = "some URI"
Previous = "some URI"
Beep = "yes/no"
Timeout = "some integer"
LockIn = "yes/no"
>
<Title wrap = "yes/no">Directory Title</Title>
<MenuItem>
    <Prompt>Contact Name</Prompt>
    <URI>number</URI>
</MenuItem>
```

```
</****Directory>
```

Table 7-15 lists the parameters in the XML file of the Directory type.

Table 7-15 Parameters in the XML file of the Directory file

Parameter	Mandatory	Value Type	Description
****Directory	Yes	None.	Root element.
Next	No	URI	URI corresponding to the **Next** soft key.
Previous	No	URI	URI corresponding to the **Previous** soft key.
Beep	No	yes no	Indicates whether the IP phone plays a beep tone when accessing the menu. Default value: no
Timeout	No	Integer Unit: second	Timeout interval. If a user does not perform any operations within the interval, the IP phone returns to the standby page. Default value: 45
LockIn	No	yes no	If the parameter is set to **yes**, the IP phone responds only to the defined soft keys. For example, when a user picks up the IP phone, the dialing page is not displayed. Default value: no
Title	Yes	Character string	Title of an phone book.
Wrap	No	yes no	Indicates whether to display the title in multiple lines if the title is too long. Default value: yes
MenuItem	Yes	None	Address book at a lower level. A maximum of 15 address books can be added.
Prompt	Yes	Character string	Title of an address book.
URI	Yes	URI	Operation on an item in an address book. For example, the IP phone dials a phone number.
Softkey	No	xml object	For details, see 7.8.8 Soft Keys.

Table 7-16 lists the default soft keys if no soft keys are defined in the XML file of the Directory type.

Table 7-16 Default soft keys on the page of the Directory type

Soft Key Index	Name	URI
1	Exit	SoftKey: Exit
2	Previous	SoftKey: Previous
3	Next	SoftKey: Next
4	Call	SoftKey: Dial

Table 7-17 lists the functions of keys on the page of the Directory type.

Table 7-17 Functions of keys on the page of the Directory type

Key Name	Key	Function
UP/DOWN	Up and down arrow keys	Moves the cursor up or down.
Digitkey	Number keys 1 to 9	Moves the cursor to the menu item indicated by the same number. If the number key that a user presses is larger than the number of menu items, the IP phone moves the cursor to the last menu item.
Dial	Soft key. URI="SoftKey: Dial"	Calls the number in the selected address book.
Previous	Soft key. URI="SoftKey: Previous"	Accesses the URI (such as an HTTP address) specified by **Previous**.
Next	Soft key. URI="SoftKey: Next"	Accesses the URI (such as an HTTP address) specified by **Next**.
Exit	Soft key. URI="SoftKey: Exit"	Displays the previous page.
OffHook/Lineke y/Handfree	Off-hook/Acco unt key/Handsfree key	Calls the number in the selected address book.
Cancel	X key on an IP phone	Returns to the standby page.
Ok	OK key on an IP phone	If the value of **LockIn** is **no**, the **OK** key functions as the **Dial** key; if the value of **LockIn** is **yes**, the IP phone does not respond to this key.
DSS key except the key assigned	DSS key, including keys	If the value of **LockIn** is **no**, the IP phone performs the function specified by the DSS key; if the value of

Key Name	Key	Function
the SIP account function	on expansion modules	**LockIn** is **yes**, the IP phone does not respond to this key.

7.8.5 Execute

The page of the Execute type is used to request an IP phone to run commands in a specified sequence. When the IP phone runs the command, no prompt message is displayed.

An example of the XML file of the Execute type is as follows:

```
<****Execute Beep = "yes/no">
<ExecuteItem URI = "URI"/>
</****Execute>
```

Table 7-18 lists the parameters in the XML file of the Execute type.

Table 7-18 Parameters in the XML file of the Execute type

Parameter	Mandatory	Value Type	Description
****Execute	Yes	The string **** can be any value, including a blank character string.	Root element.
Beep	No	yes no	Indicates whether to play a beep tone when the IP phone starts to run commands. Default value: no
ExecuteItem	Yes	None.	Command item. A maximum of 30 commands can be added.
URI	No	URI	Operation corresponding to a command, for example, calling a user or downloading data from the server based on the URI.

Table 7-19 lists the common commands that are configured in the XML file of the Execute type.

Table 7-19 Common commands that are configured in the XML file of the Execute type

Name	URI	Function
Any Supported uri	http(s)://myserver.com/myscript.pl	Accesses the URI.
	Dial:XXXXX	Calls the phone number.
	Led:XXXX=on/off/slowflash/fastfl	Controls the indicator.

Name	URI	Function
	ash	
	Key:XXXX	Presses the keys XXXX.
	Wav.Play:[tftp|http://[username[:password]@] <host>[:port][/<Path>]/<file> Wav.Stop:	Plays or stops a WAV file.
Phone Reboot	Command:Reset	Restores factory settings.
Phone Fast Reboot	Command:Reboot	Restarts the IP phone.
Phone Lock	Command:Lock	Enables the talk only function.
Phone Unlock	Command:Unlock	Unlocks all keys.
Clear	Command:ClearCallersList	Clears the local call history.
	Command:ClearDirectory	Clears the local contact list.
	Command:ClearRedialList	Clears the call history.
Do nothing	None.	None.

Table 7-20 lists the settings of XXXX in the URI Led:XXXX=on/off/slowflash/fastflash.

Table 7-20 Settings of XXXX in the URI Led:XXXX=on/off/slowflash/fastflash

Setting	Indicator	Example
EXP-%d-%d2-%s	%d: %dth expansion module. The value ranges from 1 to 6. %d2: %d2th key on an expansion module. The value ranges from 1 to 20. %s: color of the indicator. The value is **RED** or **GREEN**.	Led:EXP38-2-3-RED=on: indicates that the indicator corresponding to the third key on the second expansion module is turned on in red.
LINE%d	%d: number of the indicator corresponding to a line key. The value ranges from 1 to 6.	Led:LINE3=on: indicates that the indicator corresponding to the line3 key is turned on.
MEMO%d_%s	%d: number of the DSS key. The value ranges from 1 to 10. %s: color of the indicator. The value is **RED** or **GREEN**.	Led: MEMO5_GREEN =on: indicates that the indicator corresponding to DSS key 5 is turned on in green.
HEADSET	Headset status indicator.	Led:HEADSET=off: indicates that the headset status indicator is turned off.
BACKLIGHT	Backlight.	N/A

Setting	Indicator	Example
HANDFREE	Handsfree status indicator.	N/A
POWER	Power supply indicator.	N/A

Table 7-21 lists the settings of XXXX in the URI Key:XXXX.

Table 7-21 Settings of XXXX in the URI Key:XXXX

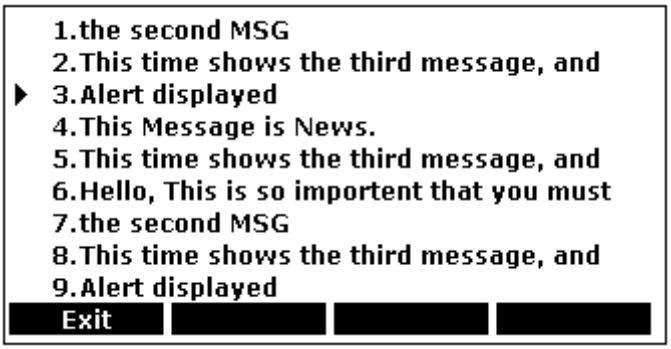
Setting	Key
EXP-%d-%d	%d: %dth expansion module. The value ranges from 1 to 6. %d2: %d2th key on an expansion module. The value ranges from 1 to 20. An example is as follows: Key:EXP-2-3: indicates that the third key on the second expansion module.
OFF_HOOK	Off-hook key Example: Key:OFF_HOOK
ON_HOOK	On-hook
OK	OK key
CANCEL	X key
UP	Up arrow key
DOWN	Down arrow key
LEFT	Left arrow key
RIGHT	Right arrow key
INCREASE	Key for increasing the volume
DECREASE	Key for decreasing the volume
REDIAL	Redial key
HOLD	Hold key
MUTE	Mute key
CONFERENCE	Conference key
TRANSFER	Transfer key
FWD	Forward key
PHONEBOOK	Key for accessing a remote address book
SWITCH	Switch key
HEADSET	Headset key
HANDFREE	Handsfree key

Setting	Key
LINE%d	Account keys. The value of %d ranges from 1 to 6.
HOTKEY%d	Soft keys. The value of %d ranges from 1 to 4.
MEMORY%d	Memory keys. The value of %d ranges from 1 to 10.
KEY_%d	Number keys. The value of %d ranges from 0 to 9.
STAR	Star key (*)
POUND	Pound key (#)
GROUP_LISTEN	Group listening key.
HOLD_PUBLIC	Public Hold key when the SCA function is enabled.
HOLD_PRIVATE	Private Hold key when the SCA function is enabled.

7.8.6 Status

Figure 7-84 shows the page of the Status type, which displays the IP phone's state.

Figure 7-84 Page of the Status type.



An example of the XML file of the Status type is as follows:

```
<****Status Beep = "yes/no">
<Session>Session ID</Session>
<Message
                  Index = "index"
                  Type = "alert"
                  Timeout = "timeout"
>Message</Message>
</****Status>
```

Table 7-22 lists the parameters in the XML file of the Status type.

Table 7-22 Parameters in the XML file of the Status type

Parameter	Mandatory	Value Type	Description
****Status	Yes	The string **** can be any value, including a blank character string.	Root element.
Beep	No	yes no	Indicates whether to play a beep tone when displays status information. Default value: no
Session	No	Character string	Session ID, identifying different display objects. The minimum value is **0**.
Message	Yes	None.	Information displayed on the LCD. The value ranges from 0 to 10.
Index	Yes	Integer	Index of status information in a session. The value ranges from 1 to 10. Default value: 1
Type	No	alert	Currently only the value **alert** is supported. If no type is specified, status information is always displayed in turn on the LCD until a user presses a key or the IP phone exits the page as required. Default value: alert
Timeout	No	Integer Unit: second	Timeout interval for displaying status information. Default value: 3
Softkey	No	XML object	For details, see 7.8.8 Soft Keys.

Table 7-23 lists the functions of keys on the page of the Status type.

Table 7-23 Functions of keys on the page of the Status type

Key Name	Key	Function
UP/DOWN	Up and down arrow keys	Moves the cursor up or down.
Digitkey	Number keys 1 to 9	Moves the cursor to the message item indicated by the same number. If the number key that a user presses is larger than the number of message items, the IP phone moves the cursor to the last message item.
Exit	Soft key. URI="SoftKey:E	Displays the previous XML page. If the current page is the first page that a user views, the IP phone displays the

Key Name	Key	Function
	xit"	standby page.
OffHook/Linekey/Handfree/DSSkey	Off-hook/Account key/Handsfree key/DSSkey	If the value of **LockIn** is **no**, the IP phone displays the dialing page or performs the function specified by the DSS key; if the value of **LockIn** is **yes**, the IP phone does not respond to the keys.
Cancel	X key on an IP phone	Returns to the standby page.
Ok	OK key on an IP phone	Accesses the URI specified by **doneAction**.

7.8.7 Configuration

The XML file of the Configuration type is used for modifying IP phone settings. No page is displayed on the LCD for this file.

An example of the XML file of the Configuration type is as follows:

```
<****Configuration
Beep = "yes/no"
setType = "config/boot"
>
<ConfigurationItem>
    <Path>path</Path>
    <Session>session</Session>
<Parameter>parameter</Parameter>
<Value>value</Value>
</ConfigurationItem>
</****Configuration>
```

Table 7-24 lists the parameters in the XML file of the Configuration type.

Table 7-24 Parameters in the XML file of the Configuration type

Parameter	Mandatory	Value Type	Description
****Configuration	Yes	The string **** can be any value, including a blank character string.	Root element for setting IP phone parameters.
Beep	No	yes no	Indicates whether to play a beep tone when a user sets IP phone parameters. Default value: no
setType	No	config boot	• **config**: indicates that the modification takes effect, and the IP phone does not restart. • **boot**: indicates that the modification

Parameter	Mandatory	Value Type	Description
			takes effect, and the IP phone restarts.
ConfigurationItem	Yes	None.	Configuration item. The value ranges from 0 to 1000.
Path	Yes	Character string	Path where parameters are stored.
Session	Yes	Character string	Node where parameters are stored.
Parameter	Yes	Character string	Parameter name.
Value	Yes	Character string	Parameter value.

7.8.8 Soft Keys

A user can define four soft keys on an IP phone. The format of the file for configuring soft keys is as follows:

```
<SoftKey index = "1-6">
<Label>Text</Label>
<URI>http://someserver/somepage OR SoftKey:someaction</URI>
</SoftKey>
```

Table 7-25 lists parameters for configuring soft keys.

Table 7-25 Parameters for configuring soft keys

Parameter	Mandatory	Value Type	Description
SoftKey	Yes	None.	Root element for configuring a soft key.
index	Yes	Integer	Index value of the soft key. The values for soft keys from left to right are 1 to 4. If more than four soft keys are configured, the fourth soft key is automatically changed to **More** for displaying the next page of keys. The value ranges from 1 to 6.
Label	Yes	Character string	Name of the soft key.
URI	Yes	Character string	Operation corresponding to the soft key.

Table 7-26 lists available soft keys.

Table 7-26 Available soft keys

Key Value	Description
Exit	Displays the previous page.

Key Value	Description
Dial	Calls the selected phone number.
Submit	Submits information.
Select	Displays the selected item.
Next	Displays the next page.
Previous	Displays the previous page.
Dot	Enters a dot.
BackSpace	Deletes the character to the left of the cursor.
ChangeMode	Switches the input methods.

7.9 Creating a Logo

1. Prepare an image in .bmp format.
2. Download the logo creation tool.

   The tool is available at http://enterprise.huawei.com/en/support/.

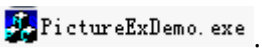
   The path is **Software Downloads** > **Unified Communication** > **IP Phone** > **Version (For example, IP Phone V100R001C02)** > **software**.

NOTE

You must apply for permission to download **PictureExDemo.exe** from the website. If you need to download the tool, contact system or service providers.

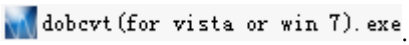
CAUTION

- Do not directly change the extension of an image file in other format (for example, .png) to .bmp.
- Image pixels for eSpace 7820 and 7830 cannot exceed 132 x 64. Image pixels for eSpace 7850 cannot exceed 236 x 82.
- eSpace 7820 and 7830 only support mono or grayscale images.

3. Decompress the logo creation tool, and double-click 

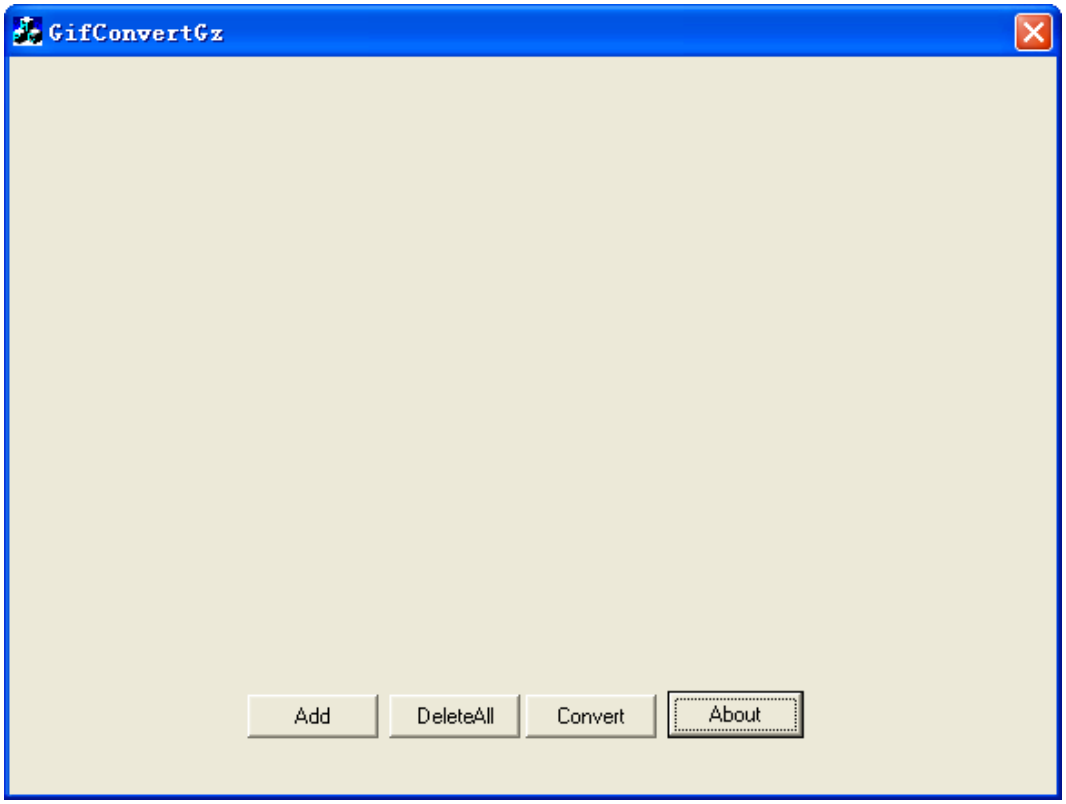
.

NOTE

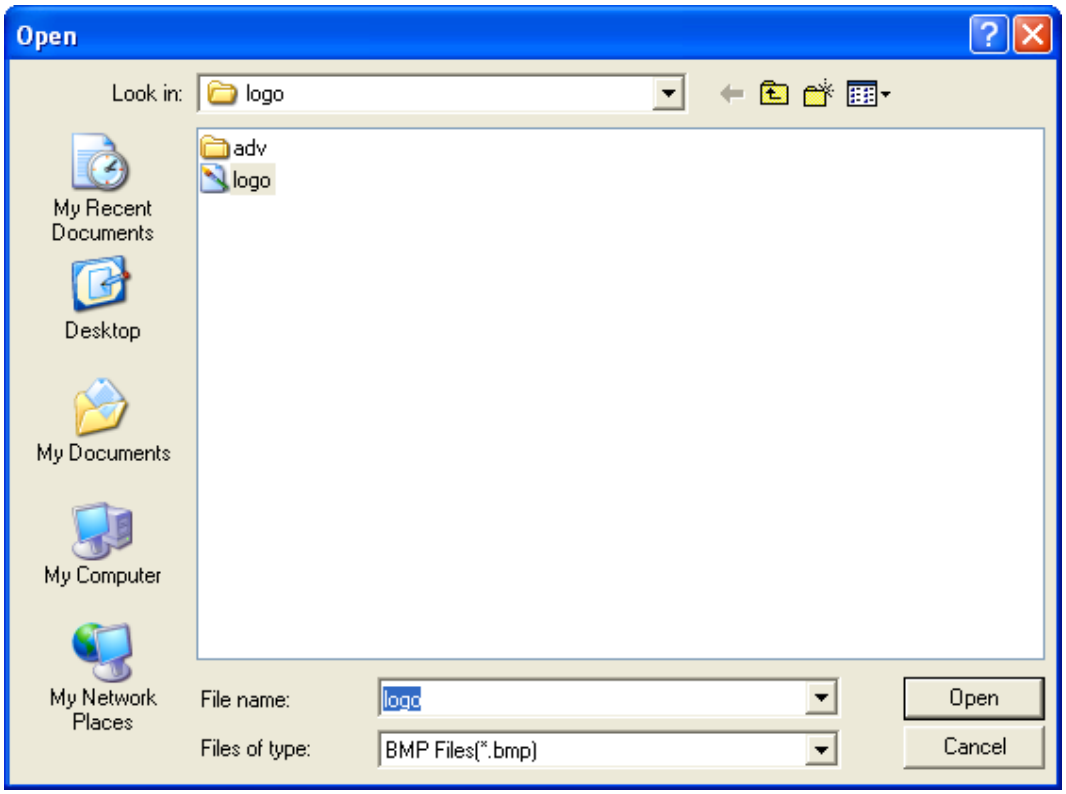
On Windows Vista or Windows 7, double-click 

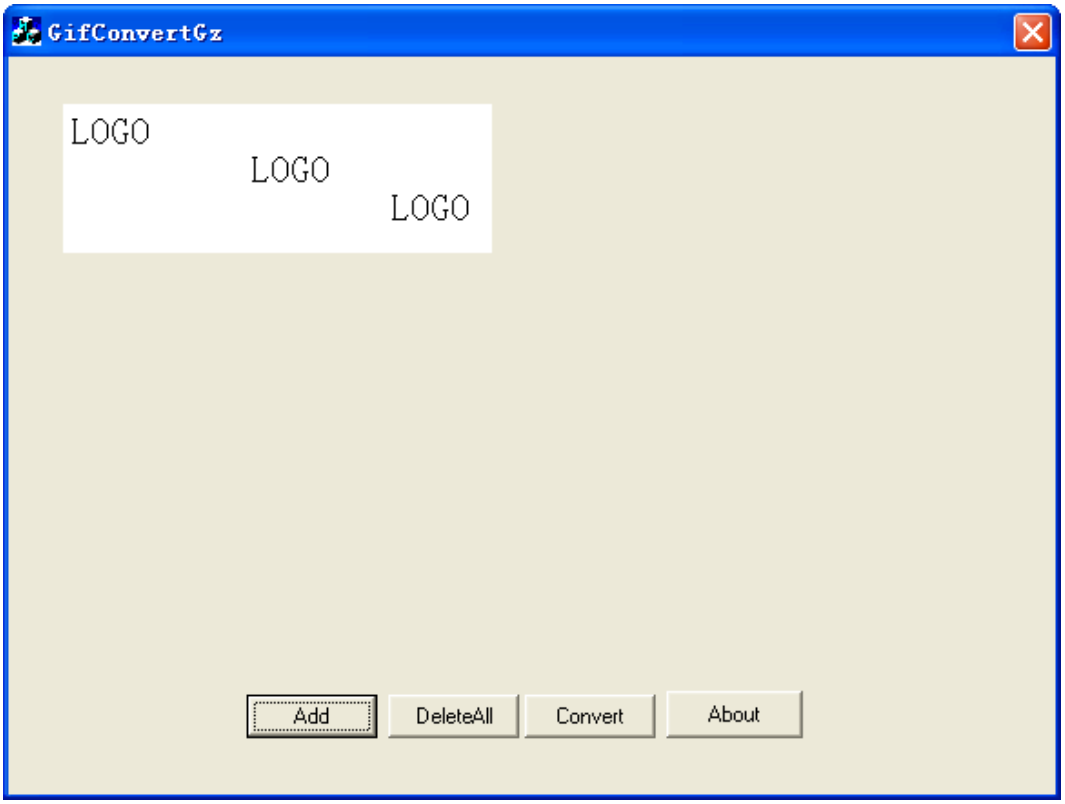
. The following describes how to create a logo on Windows XP.

A dialog box is displayed as follows.



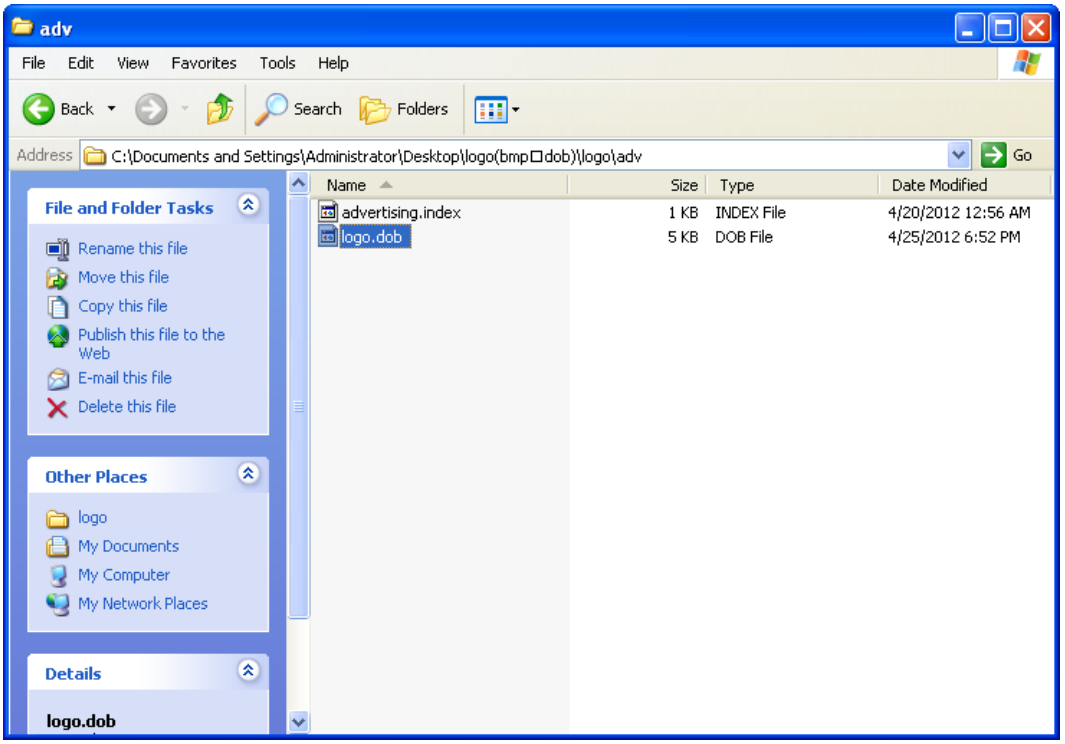
4. Click **Add** and select an image in the dialog box that is displayed, as shown in the following figure.





5. Click **Convert**.

   An image in .dob format is generated in the **adv** folder, as shown in the following figure.



Upload the **logo.dob** file to use it a customized logo.