Huawei IP Phone eSpace 6805&6810&6830&6850&6870 V100R001

Administrator Guide

Issue 01

Date 2011-12-21

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

About This Document

Intended Audience

1 Overview describes the functions, service features, and networking of the eSpace 6805, eSpace 6810, eSpace 6830, eSpace 6850, and eSpace 6870;

2 Configuration and Loading Files describes how to configure an IP phone;

3 Configuring and Upgrading IP Phones in Batches describes how to configure and upgrade IP phones in batches;

4 Troubleshooting describes the troubleshooting of the eSpace 6805, eSpace 6810, eSpace 6830, eSpace 6850, and eSpace 6870.

This document is intended for:

- Technical support engineers
- Maintenance engineers

Change History

Updates between document issues are cumulative. Therefore, the latest document issue contains all updates made in previous issues.

Issue 01 (2011-12-21)

First commercial release.

Contents

1 Overview

1.1 Principle Introduction

The IP phone product adopts the digitalized transmission technology in packets based on the IP technology. The basic principle is as follows:

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

In this way, 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 for voices.

1.2 Functions

In terms of the orientation, eSpace 6870 and eSpace 6850 are high-end-oriented products, eSpace 6805, eSpace 6810,eSpace 6830 is a low-end-oriented product. eSpace 6805, eSpace 6810,eSpace 6830, eSpace 6850, and eSpace 6870 are a series of products.

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

Codec Function

eSpace 6805, eSpace 6810, eSpace 6830, eSpace 6850, and eSpace 6870 support G.711A, G.711U, G.726, G.729, G.723, G.722, GSM, 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.

- If the network is in a good condition, G.711 is recommended to ensure high voice quality.
- If the network is not in a good condition, G.729 or G.723 is recommended.

PoE Function

eSpace 6805, eSpace 6810,eSpace 6830, eSpace 6850, and eSpace 6870 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 Quidway S3900 Series) to work normally. eSpace 6805, eSpace 6810, eSpace 6830, eSpace 6850, and eSpace 6870 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 6805, eSpace 6810,eSpace 6830, eSpace 6850, and eSpace 6870 support the bridging function. The device connected to the PC interface 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 6805, eSpace 6810,eSpace 6830, eSpace 6850, or eSpace 6870 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 **Yes** in **Silence Suppression** on the **ACCOUNT** page of the Web configuration interface.

VLAN Functions

eSpace 6805, eSpace 6810,eSpace 6830, eSpace 6850, and eSpace 6870 support the VLAN function. The packets sent by an IP phone are labeled with tags. In this case, the packets can be transmitted through a separate voice VLAN so that the stability of VOIP packets is ensured.

QoS Functions

The eSpace-series IP phones support the Layer 2 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 6805, eSpace 6810,eSpace 6830, eSpace 6850, and eSpace 6870 support the PPPoE dialing function. By using the PPPoE user name and password that are preset on an IP phone, the IP phone can initiate the PPPoE dialing and set up a connection with the softswitch through ADSL. In this way, the VoIP conversation is set up successfully.

TR-069 Function

eSpace 6805, eSpace 6810,eSpace 6830, eSpace 6850, and eSpace 6870 support Technical Report 069 (TR-069). TR-069 is a DSL Forum technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices. As a bidirectional SOAP/HTTP-based protocol, it provides the communication between customer-premises equipment (CPE) and Auto Configuration

Servers (ACS). It includes both a safe auto configuration and the control of other CPE management functions within an integrated framework.

In the course of the broadband market boom, the number of different Internet access possibilities grew as well (for example, modems, routers, gateways, set-top box, and VoIP-phones). At the same time, the configuration of the equipment became more complicated (too complicated for end users). For this reason, the TR-069 standard was developed. It provides the possibility of auto configuration of these access types. Using TR-069, the terminals can get in contact with the ACS and establish the configuration automatically.

After IP phones are connected to the ACS through TR-069, you can perform the following operations on the IP phones on the ACS:

- Configuration management

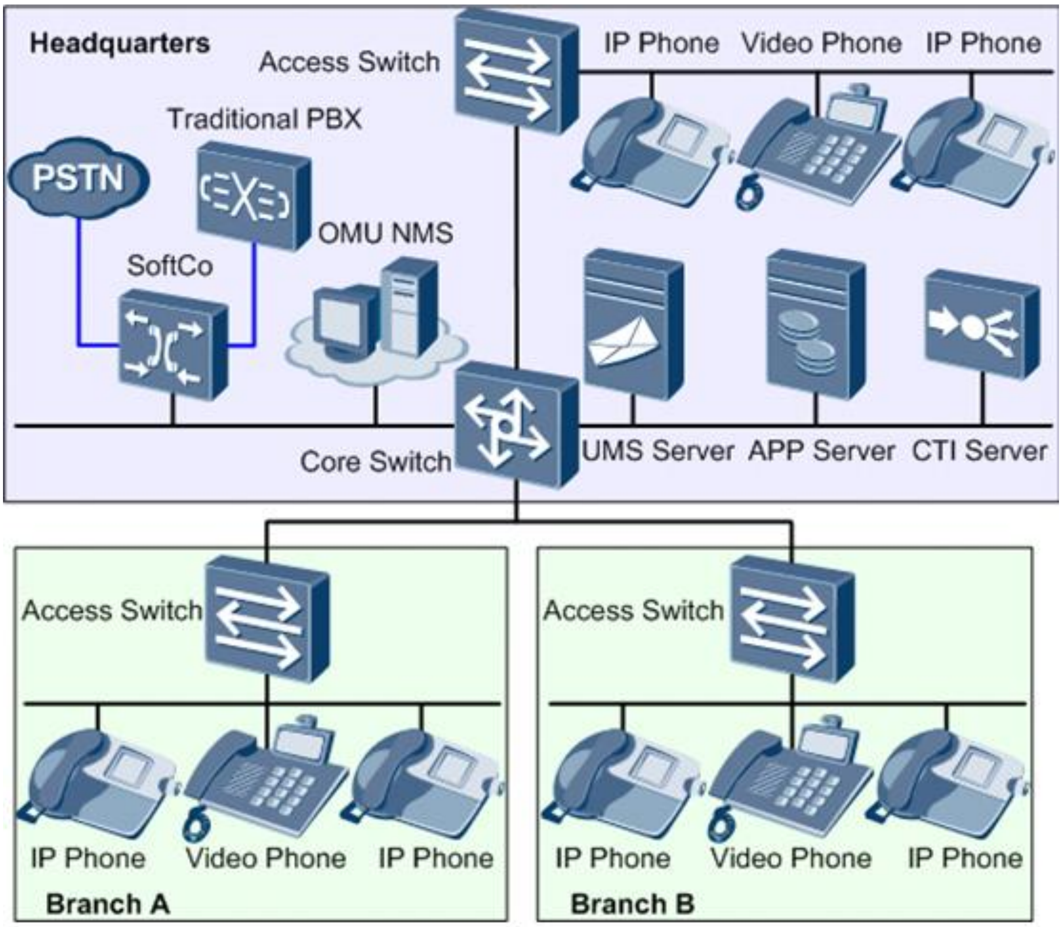
  They can configure and upgrade the IP phones in batches.
- Remote monitoring

  They can monitor the phone status and performance, and query the phone status in real time.

1.3 Network

In terms of networking features, eSpace-series IP phones can be deployed on enterprise networks to interoperate with application servers such as the IPPBX and UMS servers, implementing the functions such as the basic call functions, additional service functions, unified message functions, and phone book display functions. The communication efficiency of enterprises is improved.

Figure 1-1 Network diagram



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 Configuration and Loading Files

If the number of IP phones is small or the environment for centralized upgrade is not provided on site, configure and upgrade IP phones one by one.

CAUTION

This chapter uses eSpace 6870 to illustrate the procedures for configuring an IP phone. The procedures for configuring eSpace 6805, eSpace 6810,eSpace 6830, eSpace 6850, and eSpace 6870 are similar. The procedure for setting the network parameters such as the IP address for eSpace 6870 through the button is typical. The differences between eSpace 6805, eSpace 6810,eSpace 6830, eSpace 6850 and eSpace 6870 are described independently.

2.1 Configuring Network Parameters Using Buttons

If the DHCP server exists on site, an eSpace 6870 IP phone can obtain an IP address through DHCP. By default, eSpace-series IP phones obtain IP addresses through DHCP. If the eSpace 6870 IP phone obtains an IP address successfully, the IP address is displayed. You can use the displayed IP address to log in to the Web page of the IP phone to set the other parameters.

If the DHCP server does not exist on site, you must set the network parameters for the eSpace 6870 IP phone separately. The procedures for setting the IP address, SIP server, and SIP account through the keypad for eSpace 6870 are complicated. Therefore, it is recommended that you set the IP address through the keypad, and log in to the Web page to set the other parameters.

To set a static IP address through the keyboard in the English system, proceed as follows:

1. Press the **MENU** key on eSpace 6870 to enter the configuration page.
2. Press the Up or Down key to select **Network**, and press the **MENU** key.
3. Press the Up or Down key to select **IP Setting**, and press the **MENU** key.
4. Press the Up or Down key to select **Static IP**, and press the **MENU** key.
5. Press the Up or Down key to select **IP**, and press the **MENU** key. Press the **BackSpace** key to delete an IP address, enter the required IP address, and press the **OK** key.
6. Repeat step 5 to set **Netmask** and **Gateway**.

7. Press the left key or Back soft key to return to the Menu page.
8. Press the Up or Down key to select **Reboot**, and press the **MENU** key to make the configurations take effect.

----End

CAUTION

- When using the **BackSpace** soft key to delete an IP address, press the Left or Right key to move the cursor on the left of the number that you want to delete, and press the **BackSpace** soft key.
- The **MENU** key indicates the round key in the middle of the Up, Down, Left, and Right navigation keys. A white dot is in the middle of this button on the eSpace 6805, eSpace 6810, eSpace 6830 IP phones.

2.2 Setting Basic Parameters on the Web Page

The web server embedded in IP phones responds to HTTP GET/POST requests. Embedded HTML pages allow a user to configure the IP phone through any web browser.

The functions available for the administrator are as follows:

- **Status**

  Display the network status, account status, software version, and MAC address of the phone.
- **Basic**

  Basic preferences such as date and time settings, IP address, multi-purpose keys and LCD settings are included.
- **Advanced Settings**

  Set advanced network settings, firmware/provisioning path and XML configuration settings.
- **Account (1-6)**

  Configure each of the four SIP accounts.
- **EXT1, EXT2**

  Configure the extension module if the extension board is connected. The eSpace 6805, eSpace 6810, eSpace6830 IP phones do not support this function.

2.2.1 Accessing the Web Configuration Page

Connect the phone and computer on a reachable network. Proceed as follows:

Connect the computer to the same hub or switch as the phone is connected to. In absence of a hub/switch (or free ports on the hub/switch), connect the computer directly to the phone by using the PC port on the phone. Make sure that the phone is powered on and displays the IP address.

To access the Web configuration menu of the phone, proceed as follows:

1. Start the web browser on your computer.
2. Enter the phones IP-address in the address bar of the browser and press Enter.
3. Enter the administrator's password to access the web configuration menu. The default administrator password is **admin**.

----End

Figure 2-1 Login page

NOTE

- After changing the settings, click **Update** on the bottom of the page to save the change. Reboot the phone to have the changes take effect.
- If the settings are saved and you must perform other modifications, click **Continue** and access the required tab page to perform modifications. Then click **Reboot** to restart the phone for the modifications to take effect.

2.2.2 Displaying Phone Status

After logging in to the IP phone, click the **STATUS** tab page to view the status of the IP phone, as shown in Figure 2-2.

Figure 2-2 Status tab page

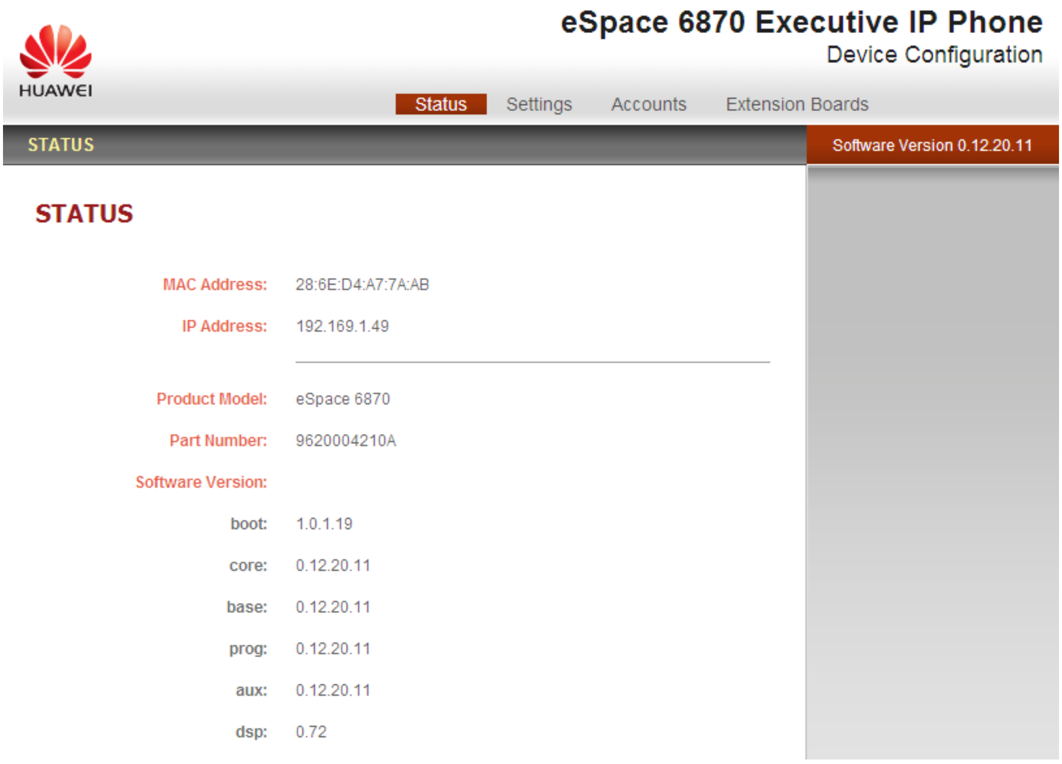


Table 2-1 describes the parameters on the **STATUS** tab page.

Table 2-1 Parameters on the STATUS tab page

Field	Description
MAC Address	Device ID in hexadecimal notation.
IP Address	IP address of the phone.
Product Model	Product model information.
Part Number	Production batch number.
Software Version	Displays the software version information about the current phone. The value of prog is the main version number of the software.
System Up Time	Power-on duration since the last restart.
System Time	Current system time.
Registered	Indicates whether accounts are registered with the related SIP servers. The eSpace 6870,eSpace 6850,eSpace 6830, eSpace 6810 and eSpace 6805 IP phones support six, four,four,two and two independent SIP accounts respectively.
PPPoE Link Up	Indicates whether the PPPoE connection is enabled when the phone is connected to a DSL modem.
Service Status	Running status of the GUI and PHONE processes for the phone. The

Field	Description
	options are: • **RUNNING**: The process is running properly. • **STOP**: The process is not running properly.
Core Dump	Link for the core file that is generated when the GUI or PHONE process does not work properly. You can download the core file and provide it to the R&D engineers to locate causes of the fault.

2.2.3 Basic Configuration

For details of Basic Configuration, see *Huawei IP Phone eSpace 68XX UserManual*, **XX** represents different models.

2.2.4 Advanced Configuration

In addition to performing basic settings for an IP phone, the administrator can perform advanced settings.

Choose **Settings** > **ADVANCED SETTINGS** to enter the **ADVANCED SETTINGS** page, as shown in Figure 2-3.

Figure 2-3 ADVANCED SETTINGS page (1)

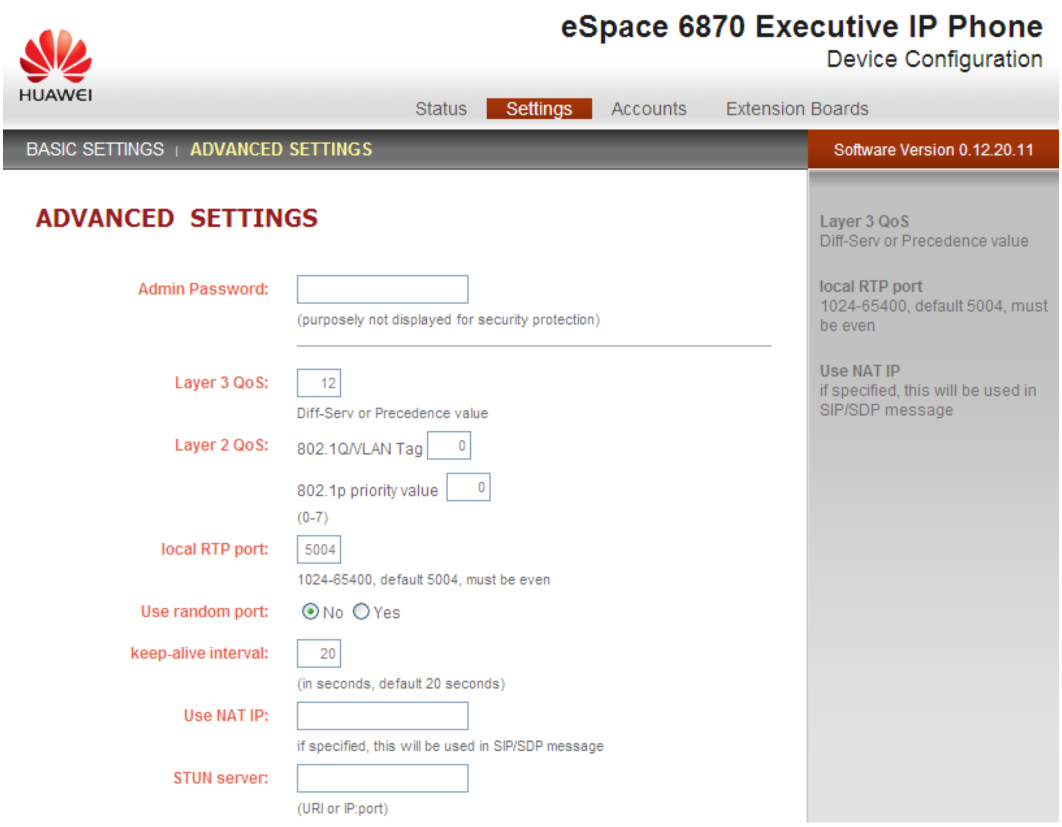


Table 2-2 describes the parameters on the **ADVANCED SETTINGS** page.

Table 2-2 Parameters on the ADVANCED SETTINGS page

Field	Description
Admin Password	Administrator password. Only the administrator can configure the **ADVANCED SETTINGS** tab page. The **Password** field is blank for security reasons after updating and saving. The password contains a maximum of 30 characters.
Layer 3 QoS	Layer 3 QoS parameter, which is used for the IP precedence, Diff-Serv value, or EXP priority of MPLS packets. The default value is **12**.
Layer 2 QoS	Layer 2 QoS parameter, which is used to set the 802.1q VLAN flag value and 802.1p priority value. The default value is **0**.
Local RTP port	This parameter defines the local RTP port pair used to listen and transmit messages. It is the base RTP port for channel 0. When an application initiates an RTP session, two ports are used. One is used for RTP, and the other is used for RTCP. When the parameter is set, channel 0 takes **port_value** as the RTP port value, and **port_value+1** as the RTCP port value; channel 1 takes **port_value+2** as the RTP port value and **port_value+3** as the RTCP port value. The default value is **5004**.
Use Random Port	When this parameter is set to **Yes**, the phone forces the random generation of both the local SIP and RTP ports. This is necessary when multiple phones are behind the same NAT. The default value is **No**.
Keep-alive interval	This parameter specifies how often the phone sends a blank UDP packet to the SIP server in order to keep **hole** on the NAT router open. The default value is **20** and the minimum value is **10**.
Use NAT IP	NAT IP address used in the SIP/SDP message. By default, this parameter is left blank.
STUN Server	IP address or domain name of the STUN server.
Firmware Upgrade and Provisioning	This parameter is used to set the time for upgrading the firmware. The default mode is **Always Check for New Firmware**. • **Always Check for New Firmware**: The phone always checks whether there is a new software version of the server. • **Check New Firmware only when F/W pre/suffix changes**: The phone checks the prefix and suffix of the upgrade file name. This mode is specifically for the ITSP. • **Always Skip the Firmware Check**: The phone skips the version check and retains the current version.
XML Config File Password	If you have used the XML Provision mode to update the configuration file and have used encryption tools such as the Openssl to encrypt the file, this parameter specifies a password for the phone to decrypt the downloaded XML file.
HTTP/HTTPS User Name	If the HTTP or HTTPS firmware or configuration server adopts the user authentication mode, set this parameter to the authorized user name.

Field	Description
HTTP/HTTPS Password	If the HTTP or HTTPS firmware or configuration server adopts the user authentication mode, set this parameter to the authorized password.
Upgrade Via	Mode of upgrading the firmware or configuration file. The options are TFTP, HTTP, and HTTPS. The default value is **HTTP**.
Firmware Server Path	IP address or domain name of the firmware server.
Config Server Path	IP address or domain name of the configuration server.
Firmware File Prefix	By default, this parameter is left blank. If the parameter is set, the phone requests the firmware file with the prefix to be upgraded. This setting is useful for ITSPs. Users must keep it blank.
Firmware File Postfix	By default, this parameter is left blank. Users must keep it blank.
Config File Prefix	By default, this parameter is left blank. Users must keep it blank.
Config File Postfix	By default, this parameter is left blank. Users must keep it blank.
Allow DHCP Option 43 and Option 66 to override server	The default value is **Yes**. If the parameter is set to **Yes**, the phone is allowed to obtain the firmware upgrade server address when obtaining an IP address through the DHCP server. The configuration is performed on the DHCP server. The obtained firmware upgrade server address overwrites the value of **Firmware Server Path**. The automatic deployment is complete.
Disable DHCP Option248	The default value is **No**. If the parameter is set to **Yes**, the DHCP Option248 function is disabled. If this happens, the unified upgrade and centralized configuration are supported.
Automatic Upgrade	This function is for the ITSP. The default value is **Yes**. • If the parameter is set to **Yes**, the automatic upgrade and configuration function is enabled. Enter the interval for checking the software upgrade or configuration changes. • When the parameter is set to **No**, the phone only performs HTTP upgrade and configuration check once at boot up.
Authenticate Conf File	If No is selected, the configuration file is authenticated before it is applied to the phone for ITSP.
Enable TR-069	• If this parameter is set to **Yes**, the phone will send session connection requests to the ACS. To enable TR-069, you must enable the ACS. For details on how to enable the ACS, see the ACS configuration guide. • If this parameter is set to **No**, the phone will not send session connection requests to the ACS.
ACS URL	ACS URL. The URL can be in either of the following formats: • http://IP address:9090

Field	Description
	For example, http://10.10.10.1:9090. • http://domain name:9090 For example, http://huawei.acs.com:9090. Here, **9090** is the port number of the ACS. This parameter is mandatory when TR-069 is enabled.
TR-069 Username	User name for authenticating a TR-069 client (phone) when the client attempts to connect to the ACS. The user name must be the same as that configured on the ACS.
TR-069 Password	Password for authenticating a TR-069 client (phone) when the client attempts to connect to the ACS. The password must be the same as that configured on the ACS.
Periodic Inform Enable	Indicates whether to periodically initiate sessions to the ACS.
Periodic Inform Interval	Interval for initiating sessions to the ACS, in seconds.
Connection Request 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.
Connection Request Password	Password for authenticating the ACS when the ACS attempts to connect to a phone. The password must be the same as that configured on the ACS.
Authentication Method	Mode of authenticating the ACS when the ACS attempts to connect to a phone. The options are: • No Authentication The ACS is not authenticated. That is, the user name and password are not required. • Basic The ACS is authenticated using its user name and password in plain texts. • Digest The user name and password are encrypted before authentication.
Connection Request Port	Port number for the ACS to send connection requests to a phone. This port cannot be occupied by another application of the phone. The default value is **7547**.
Phonebook XML Download	Indicates whether to enable the download of XML phonebook through HTTP or TFTP. Define the XML server path and download interval: • Phonebook downloading server path: IP address or domain name of the phonebook XML download server, which can be either the same as or different from the f/w server. • Phonebook XML download interval: interval of download. • Remove manually-edited items after download. The default value is **Yes**. If the parameter is set to Yes, the personal

Field	Description
	phonebook through keypad will be overwritten.
LDAP Directory	This function is not supported currently. By default, this parameter is left blank.
Idle Screen XML Download	Indicates whether to use HTTP or TFTP to download the screen saver file that is in XML format. • If **Download Screen XML At Boot up** is set to **Yes**, the phone automatically downloads the screen saver file when it restarts. If **Download Screen XML At Boot up** is set to **No**, the phone downloads the screen saver file only when you select Download SCR XML on the Preference page. • If **Use custom filename** is set to **Yes**, you must add the screen saver file name to the storage path on the XML server. If **Use custom filename** is set to **No**, you do not need to add the screen saver file name to the storage path. • In **Idle Screen XML Server Path**, enter the storage path of the screen saver file on the XML server.
XML Application	IP phone and the server are interacted through XML files to implement LCD display and change the soft key labels. This function is not supported currently.
Offhook Auto Dial	Supported for only primary account or Account 1 or Line 1. When the feature is enabled, the phone functions as a one-line phone. The remaining lines are not active.
Syslog Server	IP address or URL of the Syslog server. This feature is useful for ITSPs.
Syslog Level	Log level reported by the selected ATA. The default value is **NONE**. The level is one of **DEBUG**, **INFO**, **WARNING** and **ERROR**. Syslog messages are sent based on the following events: • Product model or version on startup (INFO level) • NAT-related information (INFO level) • Sent or received SIP messages (DEBUG level) • SIP message summary (INFO level) • Incoming and outgoing calls (INFO level) • Registration status change (INFO level) • Negotiated code (INFO level) • Ethernet connection (INFO level) • SLIC chip exception (WARNING and ERROR levels) • Memory exception (ERROR level) The Syslog uses USER function. In addition to standard Syslog payload, the following components are contained: HW_LOG: [device MAC address][error code] error message. Example: May 19 02:40:38 192.168.1.14 HW_LOG: [00:0b:82:00:a1:be][000]. Ethernet is connected.
Send SIP Log	Indicates whether to add SIP message receiving and processing information to the **Syslog.log** file.

Field	Description
NTP Server	URI or IP address of the NTP server, which is used to display the current date and time on the phone.
Allow DHCP Option 42 to override NTP server	If this parameter is enabled, the DHCP server can override the NTP server configured in the phone. This is used for ITSP or system administrator. Users can ignore this parameter.
Public Mode	Indicates whether to enable the public mode. If this parameter is set to **Yes**, the login window is displayed after a phone is powered on. Enter the correct user name and password to enter the standby mode. The user name and password are those of the corresponding SIP account. If this parameter is set to **No**, a phone directly enters the standby mode after being powered on.
SSL Certificate	SSL certificate required for accessing some resources.
SSLPrivate Key	Private key for SSL verification.
SSLPrivate Key Password	Private key password for SSL verification.
Distinctive Ring Tone	Three customized ring tones can be configured. Therefore, distinctive ring tone is played when an incoming call from a specified user comes. Enter a specific ID in the text box. When a ring tone is selected and a calling party ID is set, the device only plays this ring tone when the incoming call is the number of the preset calling party ID. The device will use the system ring tone for all other calls.
System Ring Tone	System ring tone: the North American standard is adopted by default. The user can adjust the system ring tones frequencies and cadences based on their countries telecom standard.
Call Progress Tones	These settings can be configured through various call progress tone frequencies and cadences according to the standard of country where the phone is located. By default, call progress tones are set to North American standard. Frequencies must be configured with known values to avoid uncomfortable high pitch sounds. **ON** is the period of ringing (the unit of **On time** is **ms**) while **OFF** is the period of silence. In order to set a continuous ring, **OFF** must set be to zero. Otherwise, it rings **ON** ms and a pause of **OFF** ms and repeats the pattern. A maximum three cadences are supported.
Disable Call Waiting	The default value is **No**. If the parameter is set to **Yes**, the call waiting function is disabled.
Disable Call-Waiting Tone	The default value is **No**. If the parameter is set to **Yes**, the call waiting tone is not played to remind user when there is an incoming call, and only the LED blinks as the reminder.
Disable	The default value is **No**. If the parameter is set to **Yes**, the three-party

Field	Description
Conference	conference function of eSpace 6870 is disabled.
Enable MPK Sending DTMF	The default value is **No**. If the parameter is set to **Yes**, multi-purpose keys can be set as DTMF.
Disable DND	The default value is **No**. If the parameter is set to **Yes**, the DND button on keypad as DND shortcut is disabled.
Disable Transfer	The default value is **No**. If the parameter is set to **Yes**, the transfer function is disabled.
Configuration via Keypad Menu	Specify the menus that can be used on the eSpace 6870 through the **MENU** menu. The default value is **Unrestricted**. • **Unrestricted**: indicates that all menus are available. • **Basic settings only**: indicates that all menus except Config are available. • **Constraint Mode**: indicates that all menus except **New Entry** in **Phone Book**, **Config, Factory Functions**, and **Network** are available. If a user selects **Admin Login** on the main menu, enters the administrator password, and logs in, the user can use all menus that are available in **Unrestricted** mode.
Display Language	Select the language that is displayed on the Web and LCD. You can select English, simplified or traditional Chinese, Japanese, Korean, Italian, French, Spanish, or German, or download other languages through the server.

2.2.5 Individual Account Configuration

The eSpace 6870, eSpace 6850, eSpace 6830, eSpace 6810 and eSpace 6805 provide 6-channel, 4-channel,4-channel, 2-channel and 2-channel and each channel can be configured with an independent SIP account. Each SIP account can be configured on the corresponding configuration page and the configuration method is similar.

1. Choose **Account**>**ACCOUNT 1** to set the SIP parameters, as shown in Figure 2-4.

Figure 2-4 ACCOUNT 1 page (1)

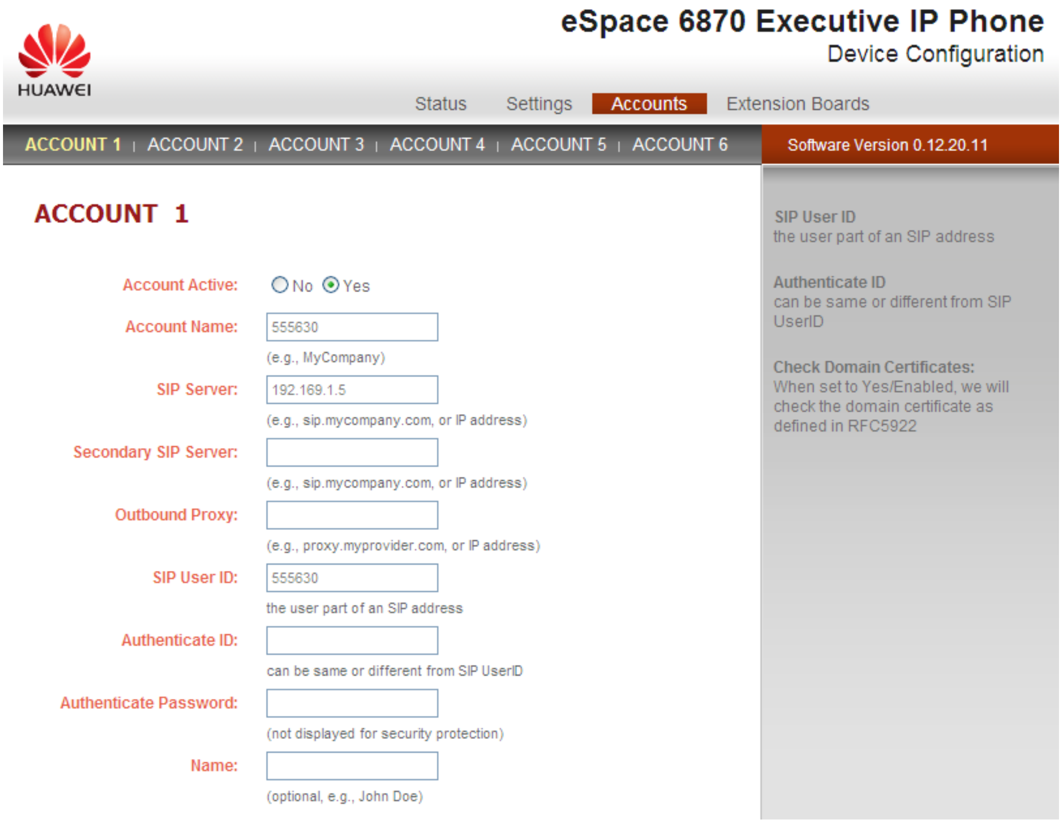


Table 2-3 describes the parameters on the **ACCOUNT 1** page.

Table 2-3 Parameters on the ACCOUNT 1 page

Field	Description
Account Active	This field indicates whether the account is active. The default value for each account is **Yes**.
Account Name	The name corresponding to each account. Only the primary account (Account 1) is displayed on the LCD. The account name is shown on the LCD of eSpace 6870 when you answer a call, or in the hand-free and off-hook modes.
SIP Server	IP address or domain name of the SIP server, which is provided by the VoIP service provider.
Secondary SIP Server	IP address or domain name of the secondary SIP server to which an IP phone connects when the primary SIP server fails. When both **SIP Server** and **Secondary SIP Server** are set, an IP phone registers with both SIP servers. After the registration is successful, the IP phone connects to the secondary SIP server if the primary SIP server fails. This parameter has no default value, indicating that IP phones do not register with a secondary SIP server.
Outbound Proxy	IP address or domain name of outbound proxy server, media gateway, or session border controller.

Field	Description
	It is used for the firewall or NAT penetration in different network environment. If the system detects that the symmetric NAT and STUN cannot work. Only the outbound proxy server can provide solution for symmetric NAT.
SIP User ID	User account information provided by the VoIP service provider (ITSP). This parameter can be digits in a phone number format or an actual phone number.
Authenticate ID	Authentication ID used by SIP service users.
Authenticate Password	SIP service users account password for the eSpace 6870 IP phone to register with SIP servers of the ITSP.
Name	SIP service users name that is used as the calling party ID and displayed on the called party's LCD (this feature needs to be supported by the SIP server). When the phone is in idle mode, the account name of Account 1 is displayed on the LCD. The LCDs on the eSpace 6830 IP phones do not display the account name.
DNS Mode	Record type that the DNS can query. The default value is **A Record**. • **A Record**: A phone queries a domain name and parses it to an IP address. • **DNS SRV**: Dialing by domain names allows an SIP user to obtain an SIP address to relocate the IP address of the current SIP server. Service records (SRV records) maintain stability. • **NAPTR/SRV**: The phone attempts to perform a Name Authority Pointer (NAPTR) query and to perform an SRV record query on the NAPTR query result. This ensures the stability and reliability of registration. • **Use Configured IP**: When the server address is a domain name, the phone parses the server address to this IP address.
TEL URI	If the phone has an assigned PSTN phone number, this parameter must be set to **Yes**. Otherwise, set it to **No**. If the parameter is set to **Yes**, the **user=phone** parameter will be attached to the **From** header in SIP request.
SIP Registration	This parameter controls the sending of register messages to the proxy server. The default value is **Yes**.
Unregister on Reboot	The default value is **No**. If the parameter is set to **Yes**, the SIP users registration information is cleared on restart. The "*" will be sent in the SIP header to request bidding removal. Some servers do not support this function.
Register Expiration	This parameter allows users to specify the time frequency (in minutes) that the eSpace 6870 IP phone refreshes its registration. The default interval is **60**. The maximum interval is 65535 minutes (about 45 days) and the minimum expiration is 2 minutes.
Local SIP Port	This parameter defines the local SIP port used to listen and transmit.
SIP Registration	The default value is **20**. Configure the option to allow resending

Field	Description
Failure Retry Wait Time	registration packet once the registration fails due to multiple possible reasons.
SIP T1 Timeout	The default value is **0.5**.
SIP T2 Interval	The default value is **4**.
SIP Transport	Select the SIP transport either through UDP or TCP. The default value is **UDP**.
Check Domain Certificates	Indicates whether to check the domain name certificate based on the definition in RFC 5922.
Remove OBP from Route	The default value is **No**. If **Outbound Proxy** is selected, the routing information is added as the first field to an SIP message sent by a phone by default. If **Remove OBP from Route** is set to **Yes**, the routing information is deleted from an SIP message sent by a phone.
Validate Incoming Messages	This parameter verifies the received SIP information.
Support SIP Instance ID	Indicates whether to add an instance ID to a REGISTER message initiated by a phone. The default value is **Yes**.
NAT Traversal	This parameter activates the NAT traversal mechanism. • The default value is **No**, indicating that the NAT traversal is not used. The mode is used in the situation that the SIP server and the terminal are on the same private network, or the NAT traversal of the RTP media stream is implemented by the SIP server. • When you enable the parameter by selecting **STUN**, and when a STUN server is also specified, the phone works according to the STUN client specifications. In this mode, the embedded STUN client detects if and what type of NAT/Firewall configuration is used. If the detected NAT type is Full Cone, Restricted Cone, or Port-Restricted Cone, the phone uses its mapped public IP address and port number in all SIP and SDP messages. • If you select **Keep-alive**, the eSpace 6870 IP phone periodically (every 20 seconds) sends a blank UDP packet (with no payload data) to the SIP server to keep **hole** on the NAT open. • If the parameter is set to **UPnP**, eSpace 6870 sends the mapping request to the built-in UpNP server of the NAT before using the SIP or RTP port. In addition, eSpace 6870 maps the result port in the SIP or RTP message to implement the NAT traversal. • If the parameter is set to **Auto**, eSpace 6870 sets the NAT solution according to the detected upper-level NAT type. If the outbound proxy server is used, this parameter must be set to **No**.
Subscribe for MWI	The default value is **No**. If the parameter is set to **Yes**, a SUBSCRIBE for message waiting indication is sent periodically.
SUBSCRIBE for Registration	The default value is **No**. If this parameter is set to **Yes**, a phone sends a SUBSCRIBE message when sending a REGISTER message.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>PUBLISH for Presence</td><td>The default value is No. If the parameter is enabled, the SIP server must support the Presence function before the function works.</td></tr>
<tr><td>Proxy-Require</td><td>The SIP extension informs the SIP server that the unit is behind the NAT/firewall.</td></tr>
<tr><td>Voice Mail UserID</td><td>When this option is configured, the user can access messages by pressing MSG. This ID is the VM portal access number.</td></tr>
<tr><td>Send DTMF</td><td>Mechanism to transmit DTMF digits during the call.
The following modes are supported:
In audio: Indicates DTMF is combined in audio signals (not reliable for low-bit-rate codec)
Via RTP (RFC2833)
Via SIP INFO</td></tr>
<tr><td>Early Dial</td><td>The default value is No. This parameter is used only when the proxy server supports 484 responses. The phone sends every dialed number until the digit string is sent wholly and successfully.</td></tr>
<tr><td>Dial Plan Prefix</td><td>Set the prefix added to each dialed number. This prefix string is added to each dialed number</td></tr>
<tr><td>Dial Plan</td><td>The dialing rule specifies the number range allowed by eSpace 6870 and the abbreviated dialing numbers. The default value is { [*#x]+ }. The rules are as follows:
The valid values are as follows: 1,2,3,4,5,6,7,8,9,0,*,#
Dialing rule:
x -: indicates a numeral ranging from 0 to 9.
xx -: indicates a two-digit numeral ranging from 00 to 99.
^ -: indicates that a call cannot be made.
[3-5] -: indicates that the number 3, 4, or 5 can be dialed.
[147] -: indicates that the number 1, 4, or 7 can be dialed.
<2=011> -: indicates that the dialing number 2 is replaced with 011.
Instances:
Instance 1: {[369]11 | 1617xxxxxxx} -: indicates that the numbers 311, 611, and 911, and any eleven-digit numerals starting with 1617 are allowed to be dialed.
Instance 2: {^1900x+ | <=1617>xxxxxxx} -: indicates that any number starting with 1900 is rejected to be dialed, and all seven-digit numerals are prefixed with 1617 when being dialed. Set {x+} and allow all numbers to be dialed.</td></tr>
<tr><td>BLF Call-pickup Prefix</td><td>The default value is **. This prefix is used when answering call with BLF event calls.</td></tr>
<tr><td>Delayed Call Forward Wait</td><td>This parameter adjusts the time delay before calls are forwarded. The default value is 20.</td></tr>
</table>

Field	Description
Time	For example, **delayed call forwarding** specifies the time before a call is sent to a forwarded number or sent to the voice mailbox.
Enable Call Features	If the parameter is set to **Yes**, the call transfer, call forwarding and Do-Not-Disturb (DND) functions are supported locally.
Call Log	There are three options, and the default value is **Log All Calls**. • Log All Calls: record all calls. • Log Incoming/Outgoing only: The missed call records are not displayed. • Disable Call Log: disable call records.
Session Expiration	Session Expiration is the time (in seconds) that is considered as the duration for timeout, when no successful session refresh transaction occurs beforehand. The default value is **180**. The SIP Session Timer extension enables SIP sessions to be periodically refreshed through a SIP request (UpDATE or re-INVITE). Once the session interval expires and there is no refresh through the UpDATE or re-INVITE message, the session is terminated.
Min-SE	This parameter defines the minimum session expiration (in seconds). The default value is **90**.
Caller Request Timer	If the parameter is set to **Yes**, the phone uses the Session Timer when an outgoing call is made and the remote party supports the Session Timer.
Callee Request Timer	If the parameter is set to **Yes**, the phone uses the Session Timer when an incoming call is received with Session Timer requests.
Force Timer	If the parameter is set to **Yes**, the phone uses the Session Timer even if the remote party does not support this feature. If the parameter is set to **No**, the Session Timer is enabled only when the remote party supports this feature. To disable the Session Timer, select **No** for **Caller Request Timer**, **Callee Request Timer**, and **Force Timer**.
UAC Specify Refresher	As a calling party, select UAC to use the phone as the refresher, or UAS to use the called party or proxy server as the refresher.
UAS Specify Refresher	As a called party, select UAC to use calling party or proxy server as the refresher, or UAS to use the phone as the refresher.
Force INVITE	Session Timer can be refreshed in the INVITE or UpDATE method. Select **Yes** to adopt the INVITE method to refresh the Session Timer.
Enable 100rel	The PRACK method enables reliability to SIP provisional responses (1xx series). This is necessary for supporting the PSTN network.
Account Ring Tone	There are four different ring tones: One system ring tone: When this option is selected, all calls will ring with the system ring tone. Three customer ring tones: When this option is selected, incoming calls corresponding to designated accounts will play the selected ring

Field	Description
	tone.
Ring Timeout	Period of time when a phone rings upon an incoming call and times out.
Line-seize Timeout	Timeout duration when a phone enters the dialing state after a user presses the **SeizeLine** soft key. This parameter is valid only when the shared line is enabled.
Send Anonymous	If this parameter is set to **Yes**, the INVITE message starting with **From** is set to anonymous, essentially blocking the calling party ID from displaying.
Anonymous Call Rejection	The default value is **No**. If the parameter is set to **Yes**, the anonymous call is rejected.
Auto Answer	The default value is **No**. If the parameter is set to **Yes**, the eSpace 6870 IP phone automatically switches to the speaker to answer the incoming call.
Allow Auto Answer by Call-Info	Set the parameter to **Yes** if the paging function is used. The IP phone answers the call automatically based on Call-info in the SIP message. The default value is **No**.
Refer-To Use Target Contact	The default value is **No**. If the parameter is enabled and the server supports this feature, the phone checks the **Refer-To** header to process the call.
Transfer on Conference Hangup	After this function is enabled, the remaining two parties continue the conference if the creator of the three-party conference hangs up the phone first.
Preferred Vocoder	The eSpace 6870 IP phone supports a maximum of five different Vocoder types, including G.711(a/μ)(PCMU/PCMA), GSM, G.726-32, G.723.1, G.729A/B, and iLBC. Configure Vocoders in a preference list that is in the same preference order as the SDP message. Enter the first Vocoder in this list by selecting the proper option for **Choice 1**. Similarly, enter the last Vocoder in this list by selecting the proper option for **Choice 8**. In **Choice 1**, the default value **PCMA** is recommended. If you select the others, some conversation transaction errors may occur.
SRTP Mode	The default value is **Disabled**. • **Enabled but not forced**: indicates that only SAVP voice encryption information is contained in the SDP messages when a phone makes a call, and that the call can be connected using SRTP or not. • **Enabled and forced**: indicates that a call must be connected using SRTP. • **Optional**: indicates that both SAVP voice encryption information and non-encryption AVP voice information are contained in SDP messages when a phone makes a call, and that the call can be connected using SRTP or not.

Field	Description
Symmetric RTP	Indicates whether the eSpace 6870 supports the symmetric RTP. If this parameter is set to **Yes**, a phone ignores the host address in the RTP stream contained in SDP messages, and sends RTP messages to the host address in the RTP stream that is received.
Silence Suppression	This parameter controls the silence suppression or VAD feature of the audio codec G.711. • If the parameter is set to **Yes** and there is no call, a small number of CNG packets are sent, and then a small number of VAD packets (instead of audio packets) are sent. • If the parameter is set to **No**, this feature is disabled.
Voice Frames per TX(unit: 10 ms)	Number of voice frames to be transmitted in a single Ethernet packet. When setting this value, you must pay attention to the requested packet time (**ptime** used in SDP message). This parameter is associated with the first codec in the preceding codec preference list or the actual used payload type negotiated between the two conversation parties at the running time. For example, if the first codec is configured as G.723 and **Voice Frames per TX** is set to **2**, the value of **ptime** in the SDP message of an INVITE request is **60** because each G.723 voice frame contains 30 ms of audio. Similarly, if this parameter is set to **2** and the first codec is G.729, G.711, or G.726, the value of ptime in the SDP message of an INVITE request is **20**. If the configured voice frames per TX exceed the maximum value, the IP phone uses and saves the maximum permitted value for the corresponding first codec choice. The maximum value of all the codec is **90** ms. Pay attention to the parameter modifications. The parameter adjustment also changes the dynamic jitter buffer. The phone has a patent dynamic jitter buffer for the handling algorithm. The jitter buffer ranges from 20 to 200 ms. You are advised to use the default settings and not to change the parameters as a common user because incorrect settings will affect the voice quality.
No Key Entry Timeout	The default value is **6**. The dialed number is sent after this preset duration without pressing the **SEND** soft key.
Use # as Dial Key	This parameter allows users to set the pound key (#) as **SEND**. If the parameter is set to **Yes**, the call can be sent immediately by pressing the pound key. If the parameter is set to **No**, the pound key is included as part of the dial string.
G.723 Rate	G.723 audio codec encoding rate, either 6.3 kbit/s or 5.3 kbit/s. Check the ITSP.
G.726-32 Packing Mode	The parameter is invalid.
iLBC frame size	iLBC audio CODEC frame size, which is either 20 ms or 30 ms: • The iLBC audio CODEC frame size is 30 ms in the case of 13.3 kbit/s.

Field	Description
	• The iLBC audio CODEC frame size is 20 ms in the case of 15.2 kbit/s.
iLBC payload type	iLBC audio CODEC payload type. The value ranges from **96** to **127**. The default value is **98**.
Eventlist BLF URI	The IP or domain name for the event list BLF. The SIP sever is required to support this feature.
Special Feature	The default value is **Standard**. Select the value to meet special requirements of softswitch vendors.
NOTE RTT is short for round-trip time. PRACK is short for Provisional Acknowledgment.	

1. Click **Yes** for **Account Active** to activate the account.
2. Enter the IP address of the registration server in the **SIP Server** text box.
3. Enter the account ID of the SIP user in the **SIP User ID** text box.
4. If the SIP server has authentication information, enter the authentication ID and password in the **Authenticate ID** and **Authenticate Password** text boxes.
5. Enter the user name that is displayed on the called IP phone in the **Name** text box.

   Whether the called IP phone can display the name depends on the types of the SoftCo and the called IP phone. If the version of the SoftCo is V100R001C03 or later and the called IP phone is an SIP phone, the name can be displayed.
6. Enter the registration duration in the **Register Expiration** text box according to the requirements of the server. Generally, the registration duration is set to 5 minutes when the IP phone works with the SoftCo.
7. Enter the port number for transmitting SIP messages in the **local SIP port** text box. The default port number is 5056. If the IP phone uses multiple lines at the same time, ensure that the values of **local SIP port** for account 1 and account 2 are different. Otherwise, the registration may fail.
8. If you want to set the codec that is used by the IP phone, enter the codec in the **Preferred Vocoder: (in listed order)** text box at the bottom.
9. Click **Update** to save the configuration, and click **Reboot** to restart the IP phone to make the configuration take effect.
10. After the IP phone is restarted successfully, log in to the Web page of the IP phone and click **STATUS** to view the registration status of the account in the Registered area.

    ----End

CAUTION

Only the first three parameters are mandatory. You are recommended not to change the parameter values unless otherwise required.

In general, the IP phone can be used for conversation normally after the preceding steps. For the detailed configuration of parameters of eSpace 6870, see the user manual of eSpace 6870.

2.2.6 Configuring the Expansion Module

Figure 2-5 shows the view of the eSpace 6870 expansion module.

Figure 2-5 eSpace 6870 expansion module

eSpace 6850 and eSpace 6870 support the connection expansion module for the situation that the functional keys of the phone are insufficient. Each expansion module can expand 56 functional keys. eSpace 6850 and eSpace 6870 can connect to a maximum of two expansion modules. That is, eSpace 6850 and eSpace 6870 can expand a maximum of 112 functional keys.

The setting of functional keys on the expansion module is the same as that on the IP phone. For details, see Configuring Multi-Purpose Keys on an IP Phone.

2.2.7 Loading Files

On the IP phone, you can load version upgrade files, .xml phone book and screen saver files, and distinctive ring tone files.

For details on how to load .xml phone book, see the 5.3 Making a Personal Phone Book on IP Phone.

For details on how to load distinctive ring tone files, see the 5.4 Setting Personal Ring Tones for an IP Phone.

Upgrading a Single IP Phone

The upgrade through HTTP is the same as the upgrade through TFTP. Here takes upgrade through HTTP as an example.

CAUTION

- Ensure the power supply of an IP phone during the upgrade. Otherwise, result in upgrade failed.
- The file lists contained in the programs for software upgrade and new installation are the same. Use the compressed package for upgrade. Upgrade the software after decompressing the package in the actual situation.

Manual Upgrade

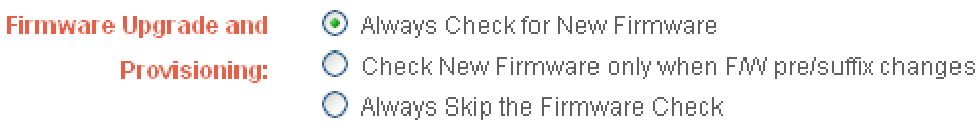
When you manually upgrade the IP phone version on the Web configuration page, do as follows:

1. Select **No** in **Automatic Upgrade** on the **ADVANCED SETTINGS** page.

Figure 2-6 Set Automatic Upgrade

2. Enable the version detection switch. Select **Always Check for New Firmware** in **Firmware Upgrade** and Provisioning on the **ADVANCED SETTINGS** page.

Figure 2-7 Firmware Upgrade and Provisioning



3. Set the mode of eSpace 6805&6810&6830&6850&6870and the upgrade server. Select **TFTP** in **Upgrade Via** and enter the TFTP server address in the **Firmware Server Path**

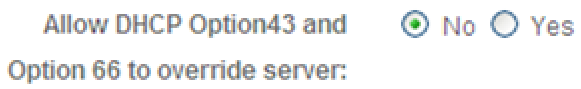
text box, namely, IP address of the computer where loading files are stored. The domain name and IP address are supported.

Figure 2-8 Upgrade Via

4. Set **Allow DHCP Option43 and Option 66 to override server** to **No**.

   If the parameter is set to Yes, the phone is allowed to obtain the firmware upgrade server address when obtaining an IP address through the DHCP server. The configuration is performed on the DHCP server. The obtained firmware upgrade server address overwrites the value of **Firmware Server Path** set in Step 3.

Figure 2-9 Set DHCP Option43 and Option66 to override server



5. Click **Update** to save the setting and click **Reboot** to restart the IP phone. After being restarted, the IP phone upgrades the version automatically.

   ----End

Automatic Upgrade

eSpace 6805, eSpace 6810,eSpace 6830, eSpace 6850, and eSpace 6870 support automatic upgrade.

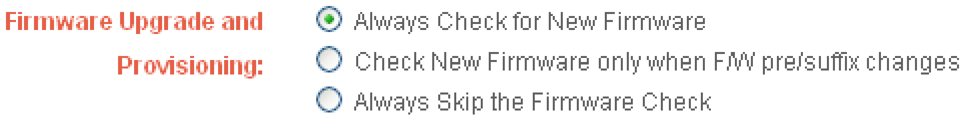
1. Set **Automatic Upgrade** to **Yes** in on the **ADVANCED SETTINGS** page and set the proper interval for checking the version.

   The default value is **1440**, and the minimum value is **60**, in minutes.

Figure 2-10 Automatic Upgrade

2. Enable the version detection switch. Select **Always Check for New Firmware** in **Firmware Upgrade** and **Provisioning** on the **ADVANCED SETTINGS** page.

Figure 2-11 Firmware Upgrade and Provisioning



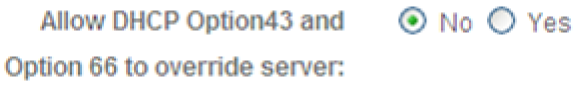
3. Set the mode of eSpace 6805&6810&6830&6850&6870and the upgrade server. Select **TFTP** in **Upgrade Via** and enter the TFTP server address in the **Firmware Server Path** text box, namely, IP address of the computer where loading files are stored. The domain name and IP address are supported.

Figure 2-12 Upgrade Via

4. Set **Allow DHCP Option43 and Option 66 to override server** to **No**.

   If the parameter is set to Yes, the phone is allowed to obtain the firmware upgrade server address when obtaining an IP address through the DHCP server. The configuration is performed on the DHCP server. The obtained firmware upgrade server address overwrites the value of **Firmware Server Path** set in Step 3.

Figure 2-13 Set DHCP Option43 and Option66 to override server



5. Click **Update** to save the setting and click **Reboot** to restart the IP phone. After being restarted, the IP phone upgrades the version automatically.

   If a new version is detected, the IP phone automatically upgrades the version.

   ----End

2.2.8 Common Operation Configurations

Configuring Multi-Purpose Keys on an IP Phone

eSpace 6870 provides seven multi-purpose keys. The multi-purpose keys of an IP phone can be set as the keys for the functions such as fast dialing and BLF. The multi-purpose keys can be used to implement only the fast dialing function when the keys are used with the SoftCo.

Figure 2-14 Multi-purpose keys

You can assign a function to a multi-purpose key on eSpace 6870, as shown in Figure 2-15

Figure 2-15 Configuring multi-purpose keys

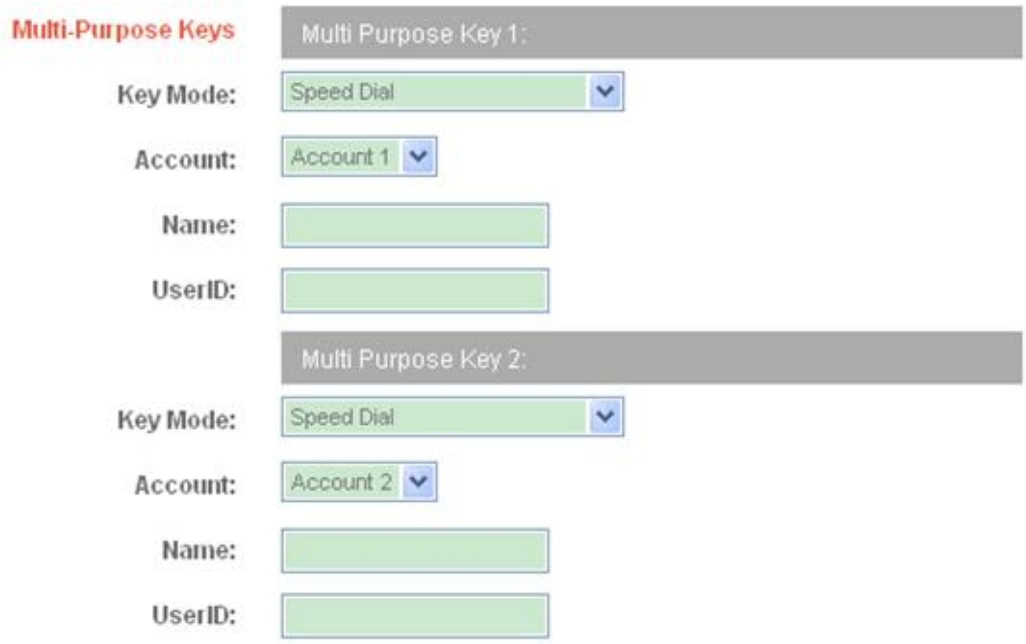


Table 2-4 describes the functions that can be assigned to multi-purpose keys.

Table 2-4 Multi-purpose keys

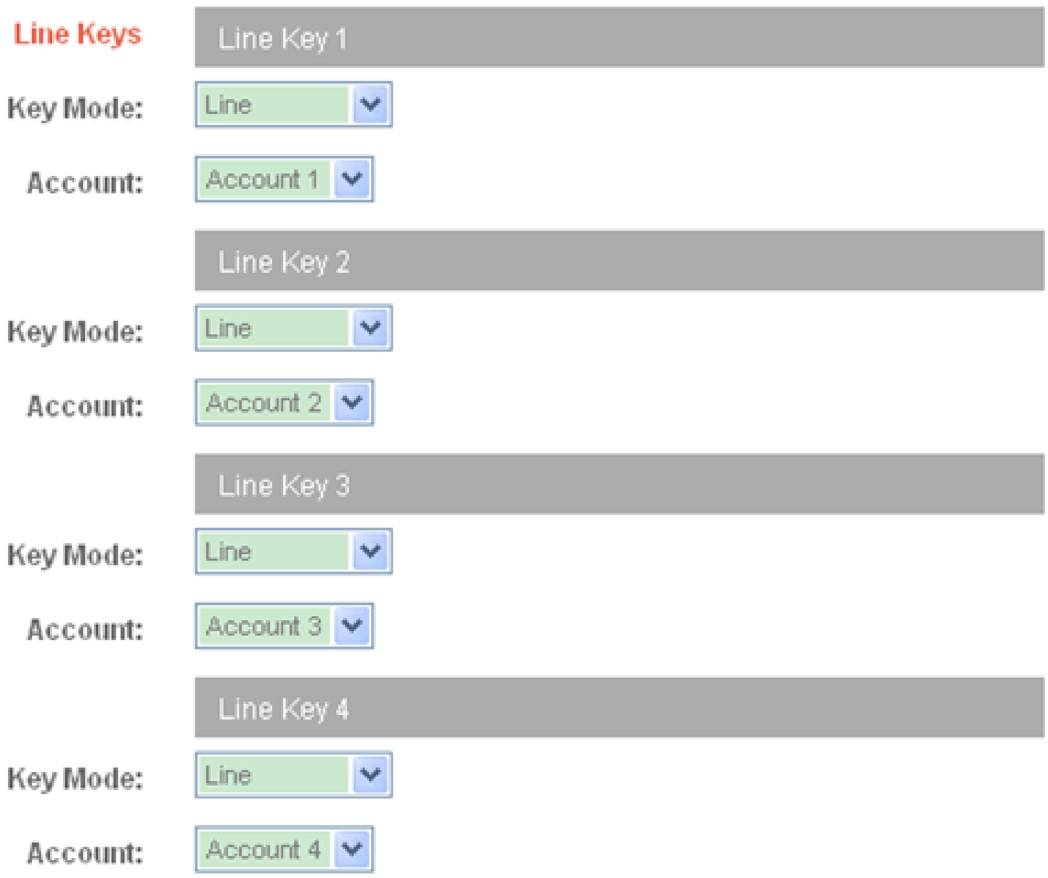
Function	Description	Setting		
		Account	Name	UserID
Speed dial	After pressing the key that is assigned with this function, you can directly make a call to the speed dial number.	Account dedicated for speed dial. The default account is **ACCOUNT 1**.	User name of the called party.	Phone number of the called party.
BLF	You can press this key to view the account status of a monitored account and directly make a call to the monitored account if it is idle. The BLF function must have been enabled on the SIP server. For details, see the SoftCo documentation.	Account that is used to make a call to a monitored account.	User name correspondi ng to the monitored account.	Phone number of the monitored party.
eventlist BLF	You can press this key to view the account status of a monitored account in a	Account that is used to make a call to	User name correspondi ng to the	Phone number of the

Function	Description	Setting		
		Account	Name	UserID
	group and directly make a call to the monitored account if it is idle. The **eventlist BLF URI** parameter on **ACCOUNT** page must be set to the group name. The group name must be the same as that configured during group creation on the SoftCo server. The BLF function must have been enabled on the SIP server. For details, see the SoftCo documentation.	a monitored number.	monitored phone.	monitored party.
Speed Dial via active account	By switching line keys to an available account, you can directly press the key that is assigned with this function to make a call to the specified number.	Account that is used to make a call.	User name of the called party.	Phone number of the called party.
DTMF	You can press this key to enable a phone to display a configured number in the phone main window instead of directly making a call to the number. You can supplement the number or retain the number and then directly press the **SEND key** to make a call.	Account dedicated for speed dial. The default account is account 1.	This parameter is dimmed.	Phone number that is automatically displayed on a phone.

Configuring Line Keys

eSpace 6870 has six line keys that normally map six independent accounts. eSpace 6870 supports the BroadSoft SCA function that is used to implement the line sharing function by interacting with the server. That is, two or more numbers in different area can be bound. If one line is in use, other lines are disabled. When an incoming call comes, all phones that share the line, however, ring at the same time. To enable this function, you must set the line key mode. Select a required line key on the **Settings**>**BASIC SETTING** page. Set **Key mode** to **Shared Line** and specify an account for sharing, as shown in Figure 2-16.

Figure 2-16 Configuring line keys



Configuring the Voice Mailbox Key

The **MSG** keys on eSpace 6870 are voice mailbox keys. By using the voice mailbox key, you can enter the voice mailbox and retrieve voice messages according to the IVP prompt messages.

1. Configure the voice mailbox key on the Web page of IP phones according to the number for retrieving voice messages in the voice leave system. For the number for retrieving voice messages, see the prefix for retrieving voice messages configured on the SoftCo.

Figure 2-17 Voice Mail UserID

2. When a new voice message is received, the message waiting indicator (MWI) on an IP phone becomes on if you have subscribed to the MWI service. Then you can press the voice mailbox key to log in to the voice mailbox.

----End

CAUTION

Before you use the MWI service, make sure that **SUBSCRIBE for MWI** on the Accounts tab page of the IP phone is enabled.

Configuring the Time on an IP Phone

Perform the following steps to obtain the network time through NTP:

1. Access the **ADVANCED SETTINGS** tab page on the Web page. Set the NTP server address in the corresponding field.

NOTE

In general, a computer using the Windows XP operating system, the SoftCo, or a router can act as an NTP server to provide the time for IP phones.

Figure 2-18 NTP Server

2. If the deployed site is not in Beijing time zone, you can select a required time zone on the **BASIC SETTINGS** tab page.

Figure 2-19 Time Zone

CAUTION

eSpace 6805, eSpace 6810,eSpace 6830, eSpace 6850, and eSpace 6870 support the function of obtaining time through DHCP. At this time, enable this function on the DHCP server. That is, select Yes for the parameters following the parameters for setting the NTP server and for setting the time zone.

Configuring the Manager and Secretary Service

eSpace 6805, eSpace 6810, eSpace 6830, eSpace 6850, and eSpace 6870 support the manager and 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.

Prerequisite

- Two lines have been configured for the manager's phone. For details, see 2.2.5 Individual Account Configuration.
  - 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. For details, see 2.2.5 Individual Account Configuration.

  When a secretary needs to serve four managers, at least four lines must be configured for the secretary's phone, and each line is bound to the external number of each manager.
- The manager and secretary service has been configured for both the manager's phone and the secretary's phone. For details, see the *SoftCo VoIP Integrated Exchange Product Documentation*.

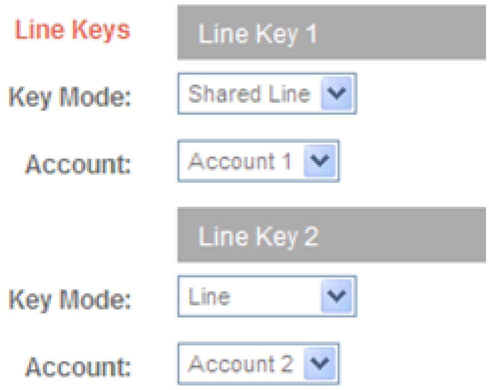
Configuring the Manager's Phone

1. Access the Web configuration page of the manager's phone.
2. Click the **Settings** tab and set **Key Mode** to **Shared Line** for line 1 under **BASIC SETTINGS**, as shown in Figure 2-20.

NOTE

If the manager needs to be configured with two secretaries, the lines bound to both secretaries must be set to shared lines.

Figure 2-20 Setting the shared line for the manager's phone



3. Click **Update** and restart the phone to make settings take effect.

----End

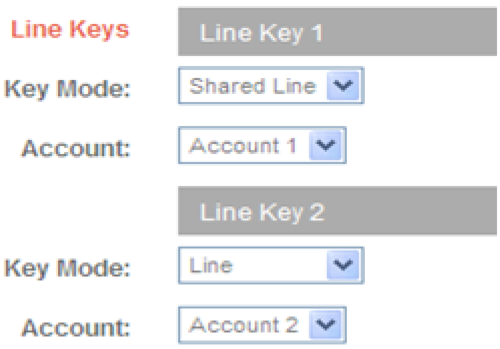
Configuring the Secretary's Phone

1. Access the Web configuration page of the secretary's phone.
2. Click the **Settings** tab and set **Key Mode** to **Shared Line** for line 1 under Basic Settings, as shown in Figure 2-21.

NOTE

If a secretary serves more than one manager, the lines bound to all managers must be set to shared lines.

Figure 2-21 Setting the shared line for the secretary's phone



3. Click **Update** and restart the phone to make settings take effect.

Restoring Factory Settings

If you want to clear the settings on an IP phone and reconfigure the IP phone, restore factory settings. The following uses eSpace 6870 to illustrate how to restore factory settings:

1. Press the **MENU** key to access the configuration menu on the IP phone, and select Config.
2. Press the **MENU** key, and select **Factory Reset** on the submenu.

3. Enter the MAC address that is printed at the bottom of the IP phone. The rule is as follows:
   - 0-9: 0-9
   - A: 22 (If you press **2** two times, **A** is displayed on the LCD.)
   - B: 222
   - C: 2222
   - D: 33 (If you press **3** three times, **D** is displayed on the LCD.)
   - E: 333
   - F: 3333

   For example, if the MAC address is 0018820E3956, enter **00188203333956**. Then **0018820E3956** is displayed on the LCD.
4. Press the **OK** soft key. If the MAC address is correct, the IP phone is restarted and factory settings are restored. If the MAC address is incorrect, return to the previous menu.

CAUTION

For eSpace 6805, eSpace 6810, eSpace 6830, eSpace 6850, and eSpace 6870, you can restore factory settings only by pressing keys and cannot restore factory settings on the Web page.

Switching Between Different Languages

The eSpace 6805, eSpace 6810, eSpace 6830, eSpace 6850, and eSpace 6870 IP phones support the display of Chinese, English, and other 13 languages on the LCD and Web page. By default, English is selected. If Chinese display is required for the customer during the deployment, you can access the **ADVANCED SETTINGS** tab page on the Web page, and set the language to Chinese. The configuration takes effect after being saved without restart.

Figure 2-22 Setting the language

3 Configuring and Upgrading IP Phones in Batches

3.1 Technique Introduction

In the technology of configuring and upgrading IP phones in batches, an IP phone uses the configuration file downloaded from the server through HTTP. The auto provisioning system (APS) has the following features:

- All IP phones use the same configuration file.

  The configuration file applies to all IP phones. The administrator does not need to configure a unique configuration file for each IP phone.
- An IP phone determines whether to perform upgrade according to the verification mechanism.

  The verification mechanism is designed for an IP phone before the IP phone downloads the configuration file and upgrades the version file. If the configuration file and version file on the server are different from that on the IP phone, the IP phone synchronizes the files from the server. If the configuration file and version file of the IP phone on the server are the same as that on the IP phone, the IP phone skips upgrade and is started normally.

3.2 Configuring and Upgrading IP Phones

CAUTION

- Ensure the power supply of an IP phone during the upgrade. Otherwise, result in upgrade failed.
- The file lists contained in the programs for software upgrade and new installation are the same. Use the compressed package for upgrade. Upgrade the software after decompressing the package in the actual situation.

eSpace 6805, eSpace 6810, eSpace 6830, eSpace 6850 and eSpace 6870 IP phones can be configured and upgraded in batches. The basic principle is as follows:

- Unified upgrade

  When an IP phone is powered on or restarted, it obtains the version file URL from the DHCP server, and compares the version file that is stored on the file server and its own version. If the versions are different, the IP phone automatically upgrades and starts. If the versions are the same, the IP phone starts normally.

- Centralized configuration

  When an IP phone is powered on or restarted, it obtains the configuration file URL from the DHCP server, and compares the configuration in the configuration file that is stored on the file server and its own configuration. If the configurations are different, the IP phone automatically upgrades and starts. If the configurations are the same, the IP phone starts normally.

3.2.1 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 an .xml file. You can change the parameter values in the template based on the site scenarios.

- File server

  The HTTP server is used.

- DHCP server

  When configuring the DHCP server, define a Option248 parameter as the file server URL. After this parameter is set, the DHCP server sends the file server URL to the IP phone that applies for an IP address. The phone downloads the version files and configuration file from this URL.

- DNS server

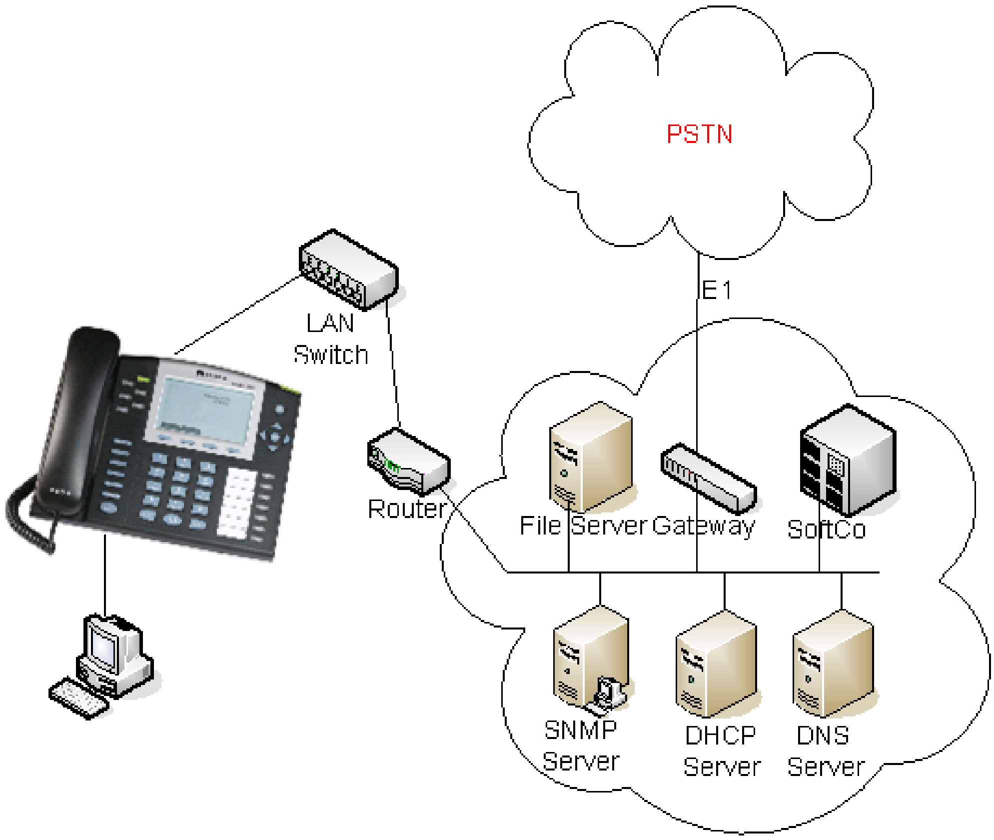
  A DNS server is required when you use domain names to configure the configuration file URL.

- Version software

  The version software is not required if you only want to configure IP phones in batches.

Figure 3-1 shows the general networking diagram for deployment.

Figure 3-1 Network diagram



3.2.2 Procedure for Configuring and Upgrading IP Phones in Batches

1. Modify the configuration file template.

CAUTION

After an IP phone obtains a modified configuration file, it only updates the modified parameter settings. The parameters that are not set or commented out are ignored.

2. Set up the DNS server environment.

   For the procedure for setting up the DNS server environment, see 5.6 Guidelines for Setting Up the DNS Server

3. Set up the HTTP server environment.

   For details on how to set up the HTTP server environment, see Method 1: Apache Server.

4. Store the phone version files and configuration file in the HTTP server root directory **C:\inetpub\wwwroot**.

NOTE

- If the version file is compressed, decompress it and obtain the .bin files. If IP phone upgrade is not required, do not store the version file in **C:\inetpub\wwwroot** if you only configure IP phones.
- If the IP phones to be configured belong to different sites, store the configuration files in two independent folders (for example, **configA** and **configB**) in the root directory. The folder name cannot contain spaces; otherwise, files in the folder cannot be downloaded. Set the Option248 parameter of the DHCP server in each site to the configuration file URL, for example, **config=http://server IP/congfigA/filename.xml**.

5. Set up the DHCP server environment.

   For the procedure for setting up the DHCP server environment, see 5.7 Setting Up the DHCP Server

6. Change the Option248 parameter value of the DHCP server to the version file URL and configuration file URL.How to set the Option248 parameter, see 5.8 Setting the Option248 Parameter

   – If the upgrade and configuration URL in 2.2.3 Basic Configuration.

     For details of Basic Configuration, see *Huawei IP Phone eSpace 68XX UserManual*, **XX** represents different models.

   – 2.2.4 Advanced Configuration is also set, the URL specified by the Option248 parameter prevails.

   – Use a semicolon (;) to separate the version file URL and the configuration file URL. Their sequence can be changed You can enter only a version file URL or a configuration file URL.

   Table 3-1 describes the Option248 parameter settings.

Table 3-1 Option 248 parameter settings

Setting Format	Example
IP	firmware=http://**server IP**;config=http://**server IP**/filename.xml
IP/path	firmware=http://**server IP/path**;config=http://**server IP/path**/filename.xml
IP:port	firmware=http://**server IP**:port;config=http://**server IP:port**/filename.xml
IP:port/path	firmware=http://**server IP:port/path**;config=http://**server IP:port/path**/filename.xml
Domain	firmware=http://**domain**;config=http://**domain**/filename.xml
Domain/path	firmware=http://**domain/path**;config=http://**domain/path** /filename.xml
Domain:port	firmware=http://**domain:port**;config=http://**domain:port**/filename.xml
Domain:port/path	firmware=http://**domain:port/path**;config=http://**domain:port/path**/filename.xml

   In Parameters in the configuration file template, **firmware** indicates the version file URL, and **config** indicates the configuration file URL.

7. 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 version file URL and configuration file URL to the phone using the **Option248** parameters. After obtaining the URLs, the phone searches the file server for the version file and configuration file and compares them with those on the phone. If The settings in the files are different, the phone configurations automatically update.

----End

After you complete the preceding procedure, the IP phones can download software version files and configuration files from the server and can run normally after being restarted. You are advised to test on certain IP phones to ensure that the IP phones run normally.

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

4 Troubleshooting

4.1 Methods of Locating Faults

4.1.1 Displaying Debugging Logs

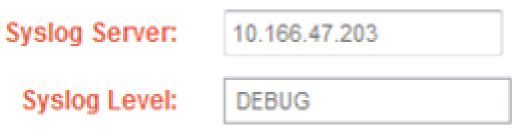
To locate the cause of the fault on an IP phone or learn the operation of an IP phone, you often need to use logs of the IP phone. The logs of the IP phone including the SIP information during the call and key debugging information of the IP phone can be displayed on the server so that maintenance personnel can query the logs.

Setting the IP Phone

Log in to the Web configuration page and proceed as follows:

1. Access the **ADVANCED SETTINGS** page.
2. Enter the log server address (IP address or domain name) in the **Syslog Server** text box and select the output log information level from **Syslog Level**. By default, the syslog level is debug.

Figure 4-1 Setting Syslog Server and Syslog Level



3. Click **Update** to save the setting.
4. Click **Reboot** to reboot the IP phone. The setting takes effect after the IP phone reboots.

----End

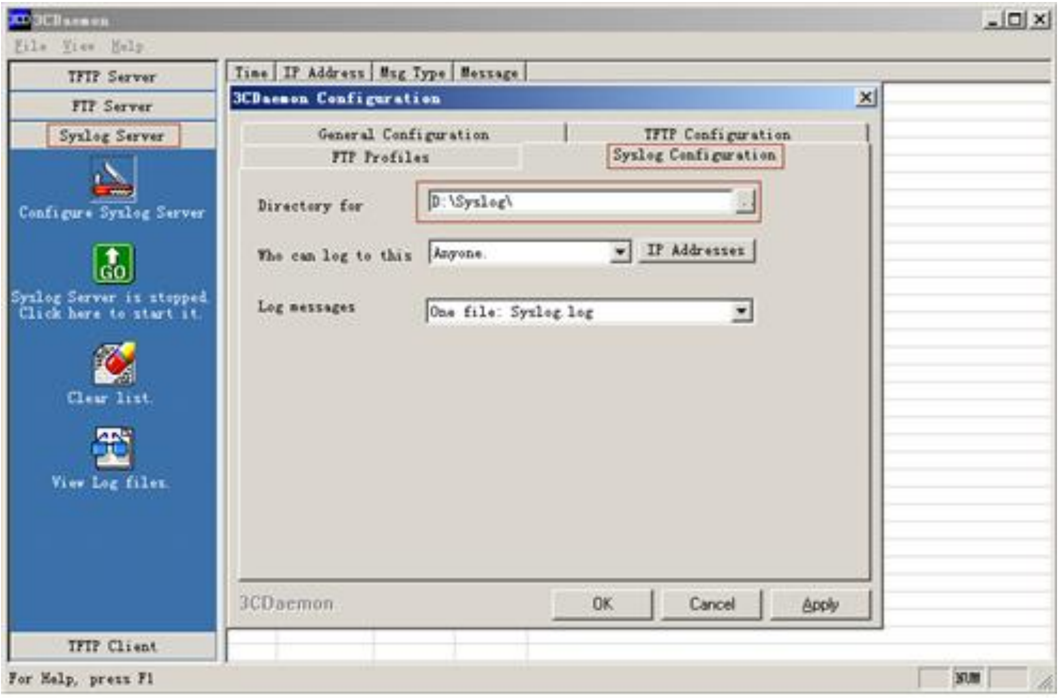
Setting the Log Server

Enable the log server (a common file server can function as a log server and 3CDaemon is recommended) and proceed as follows:

1. Choose **Syslog Server** and click **Configure Syslog Server** to set the storage path of the log server.

2. In the displayed **Syslog Configuration** dialog box, click **Browse** to set the directory for saving logs in **Directory for**. In the following figure, the logs are saved in D:\syslog. By default, a log server saves device logs displayed on the log server into D:\syslog, with the log file named **syslog.log**.

Figure 4-2 Syslog Configuration



3. After the setting, test whether the log file can be saved.

   Access the directory and verify that the **syslog.log** file exists and that the information in the file is the same as the information displayed on the log server.

4. Set the IP address of log servers of other IP phones to the IP address of this computer if the setting is successful.

   ----End

NOTE

If you do not want to trace debugging information, select **NONE** from **Syslog Level** and do not set any IP phone number. In this case, the impacts on IP phones and the network are reduced.

4.1.2 Capturing Packets Through the Packet Capture Tool

You can connect the LAN interface of an IP phone and a computer to the same hub, and use the packet capture software such as the Sniffer, Ethereal, or Wireshark to capture packets. Alternatively, you can configure mirroring on the interface connected to the IP phone. You can locate faults quickly by analyzing the captured packets. You are advised to use the Wireshark-0.99.6a software to capture and analyze packets.

For details on how to capture and analyze packets, see 5.9 Capturing Packets Through the Packet Capture Tool.

4.1.3 Obtaining Device Information by Observing the Status Indicators and Screen

Observing the Status Indicators

The status indicators on eSpace 6805, eSpace 6810, eSpace 6830, eSpace 6850, and eSpace 6870 IP phones are the LINE, LAN, PC, Message, and SPEEDDIAL/BLF/Presence indicators. Table 4-1 describes the status indicators.

Table 4-1 Description of IAD101(102)E status indicators

Indicator	Color	Status	Description
LINE	Green	On	The IP phone line is in use.
		Blink	The call of this IP phone line is held.
		Off	The IP phone is in hang-off state.
	Red	On	The IP phone line is unavailable.
		Blink	The IP phone is ringing.
LAN	Green	Blink	The IP phone is sending or receiving data.
		On	A LAN connection is set up.
		Off	No LAN connection is set up.
PC	Green	Blink	The computer is sending or receiving data.
		On	A PC connection is set up.
		Off	No PC connection is set up.
Message Indicator	Green	Blink	A new message to the IP phone exists on the server.
		Off	No new message to the IP phone exists.
SPEEDDIAL Indicator	Green	On	The fast dialing function is in use.
		Off	The fast dialing function is not used.

4.2 Common Faults and Fault Analysis

4.2.1 Obtaining the MAC Address When the IP Phone Is Powered Off

You can obtain the MAC address through either of the following ways:

- According to the corresponding purchase order (PO), you can request the supplier to provide the delivery information table that contains the MAC address.

- A label on the large package box of IP phones, where MAC addresses of all the IP phones are contained, is specially designed for MAC addresses.
- The MAC address of the IP phone is pasted on the small package box of each IP phone. In addition, the MAC address of an IP phone is pasted in the rear of the IP phone.

4.2.2 Causes of Unidirectional Communication

In the case of unidirectional communication on the PSTN network, you can determine the upper-level office fault or the internal office fault by making a call on a specified trunk circuit.

If no fault is found after making calls 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 settings are correct. The internal office fault may be the hardware or software fault:

- Hardware faults can be often detected. According to the symptom, a fault occurs in an office direction or a fault often occurs. To locate the 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, analyze the causes one by one, and locate the actual cause.
- To locate the software fault, trace the call information when the fault occurs step by step and describe the scenario and recurrence conditions carefully. Then send the information to the R&D personnel for further analysis.

Common faults are as follows:

- Media streams cannot be transmitted. Check the network setting.
- eSpace 6805, eSpace 6810, eSpace 6830, eSpace 6850, and eSpace 6870 receive extra RTP messages. That is, two devices send RTP messages to an IP phone simultaneously.
- The IP phone or headset is incorrectly connected to an interface. The headset interfaces of eSpace 6830, adopt RJ-9 and the IP phone interfaces also adopt RJ-9. Verify that the IP phone or headset is correctly connected to an interface.
- eSpace 6805, eSpace 6810,eSpace 6830, eSpace 6850, and eSpace 6870 support RTP encryption. If RTP encryption is enabled on the IP phone but encryption is disabled on the peer end, unidirectional communication may occur. Check that RTP encryption is enabled or disabled simultaneously on the two parties.

4.2.3 Causes of Crosstalk

- The MAC addresses of the IP phone conflict. There is a small possibility of this cause.
- The session is not synchronized on the lower-level NAT firewall when the SBC is used.

4.2.4 Causes of Disconnection

- The network runs abnormally. As a result, the connection is interrupted.
- SoftCo media resources are insufficient.

4.2.5 IP Phone Is Disconnected from the Network

Problem

The IP phone screen is abnormally displayed. For example, **0.0.0.0** is displayed on the screen.

Cause

- The LAN port is incorrectly connected to the switch.
- Network parameters such as IP addresses are set incorrectly.

Solution

Verify that the LAN port is correctly connected to the switch. If the LAN port is correctly connected to the switch, verify that network parameters such as IP addresses are set correctly.

4.2.6 IP Phone Cannot Be Registered

Problem

An IP phone cannot be registered. For example, the cross icon is displayed at the account position in the upper-left area of the eSpace 6870 IP phone screen.

Cause

- For the eSpace 6870 IP phone,**SIP Transport** is set to **TCP/TLS**.
- The device ID of the IP phone is not set on the SoftCo, or the SIP server configured on the IP phone is not the SoftCo.
- Different values of authentication parameters are set on the SoftCo and the IP phone.
- The device ID of this IP phone is registered by another IP phone.

Solution

- For the eSpace 6870, log in to the Web page and access the **ACCOUNT** tab page. Then check whether the value of **SIP Transport** is set to **TCP/TLS**. If yes, change it to **UDP**.
- On the IP phone, check whether the IP address of the SIP server is the IP address of the SoftCo (for the eSpace 6870, check the value of **SIP Server**). If not, change the IP address of the SIP server to the IP address of the SoftCo.
- Check the device ID of the IP phone (for the eSpace 6870, check the value of **SIP User ID**). On the SoftCo, run the **show sipue eid***phone-id* command to check whether the device ID of the IP phone exists. If not, configure the IP phone as a SIP user on the SoftCo.
- Run the **show sipue eid***phone-id* command on the SoftCo to check the value of **Status**. If the value of **Status** is **OK/LOGIN**, the device ID of the IP phone is registered by another IP phone.
- Run the **show sipue eid***phone-id* command to check how the SoftCo authenticates the IP phone (that is, the value of **AuthorizationType**). According to the value, check whether the authentication parameter settings on the two devices are the same. If not, change the settings on either device to ensure that the settings are the same on the two devices.
  - If the value of **AuthorizationType** is **authbyeid**, verify that the authentication password is the same on the two devices.
  - If the value of **AuthorizationType** is **authbyip**, verify that the IP address of the IP phone is the same on the two devices.
  - If the value of **AuthorizationType** is **authbyeidandip**, verify that the authentication passwords are the same and the IP addresses of the IP phones are the same on the two devices.

4.2.7 IP Phone Cannot Be Registered After the IP Address of the IP Phone Changes

If the IP address of the IP phone changes or a new IP address is obtained through DHCP, the IP phone cannot be registered.

1. Set up the packet capture environment, capture the SIP packets of the IP phone, and log in to the SoftCo to view the SIPUE status of the IP phone.
   - If the SIPUE registers the original IP address, the SoftCo rejects the request when the IP phone requests to be registered with the new IP address.
   - When the previous registration of the IP phone times out and the SIPUE status becomes FAULT, the IP phone can be registered successfully again.
2. Before the timeout of registration, delete users from the SoftCo, and add users again.
3. Restart the IP phone. The IP phone can be registered successfully.

CAUTION

Generally, you are advised to set the registration duration to the default value of 60 minutes.

----End

The problem occurs when the IP phone is used with the SoftCo of V100R001C03 or earlier one. When the IP phone is used with the SoftCo of later version of V100R001C03, such a problem does not occur.

NOTE

After the eSpace 6805, eSpace 6810, eSpace 6830, eSpace 6850 and eSpace 6870 IP phone receives Forbidden (403) messages, the IP phone sends the re-registration request 30 minutes later if the setting is not changed.

4.2.8 IP Phone Cannot Provide Two-Stage Dialing When the IP Phone Is Used with the SoftCo

Problem

An IP phone cannot provide the two-stage dialing.

Cause

The SoftCo supports two dual-tone multi-frequency (DTMF) signal collection modes. That is, in-audio and Info; therefore, the DTMF signal sending modes of the IP phone must be set to in-audio and Info modes.

Solution

Check DTMF signal sending modes of the IP phone and ensure that in-audio and Info modes are selected. For the eSpace 6870, access the SIP configuration page (that is, the **ACCOUNT** page), and select **in-audio** and **via SIP INFO** in **Send DTMF**.

Figure 4-3 Send DTMF

NOTE

When the IP phone supports G.711A codec, it is recommended that you set the highest priority for G.711A, that is, set **choice 1** in the **Preferred Vocoder** area to **G.711A**.

4.2.9 IP Phone Cannot Transfer a Call

Problem

Other terminals can transfer calls, but the eSpace 6870 cannot transfer a call.

Cause

When you press another LINE key to transfer an ongoing call on the eSpace 6870, the account that is displayed is not the account carrying the ongoing call.

Solution

The correct steps are as follows:

1. User A sets up a call on a line of an eSpace 6870 with user B.
2. User A presses any other LINE key on the eSpace 6870. When the account of the ongoing call is displayed, user A dials the destination number C.
3. User C hooks off, and users A and C are connected.
4. User A presses the Transfer key. User B can talk with user C. That is, the call is transferred successfully.

----End

4.2.10 IP Phone Can Make Outgoing Calls but Cannot Receive Incoming Calls

Problem

The eSpace 6870 can make outgoing calls but cannot receive incoming calls.

Cause

When the do-not-disturb (DND) function is enabled on the eSpace 6870, the incoming calls are rejected.

Solution

Check the DND icon. If the icon blinks, you can infer that the DND function is enabled. When the eSpace 6870 is not used, press **DND** to disable the DND function.

4.2.11 IP Phone Rings When Receiving a Call, but Nothing Is Heard When the IP Phone Is Picked Up

Problem

The IP phone rings when receiving a call, but nothing is heard when the IP phone is picked up.

Cause

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

Solution

Check the network configuration to ensure that the devices between which the RTP channel is set up are interconnected.

4.2.12 IP Phone Cannot Obtain Time from the NTP Server

Problem

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

Cause

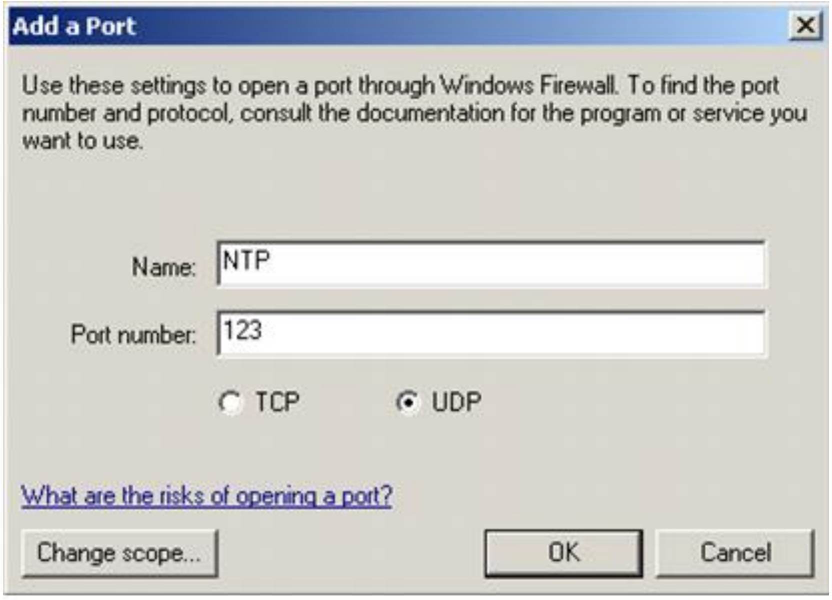
The firewall is installed on the computer; therefore, NTP packets sent by the IP phone are intercepted.

Solution

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. On the Exception tab page of the firewall, add a port with the number being 123 (a port number frequently used by the NTP server) and the protocol being UDP. The port name is customized.

Figure 4-4 Exception tab page of the firewall



If an IP phone cannot obtain the time from the computer, it is recommended that the SoftCo be used as the NTP server so that the IP phone obtains the time from the SoftCo. The SoftCo of V100R001C03 and later one provides the NTP function.

Configuration command on the SoftCo: [%SoftCo9500(config)]$start sntpserver

4.2.13 Voice on the IP Phone Is Intermittent

Problem

The voice on the IP phone is intermittent.

Cause

This fault is caused by the packet loss and jitter:

- Packet loss is caused by network congestion or insufficient device capabilities.
- The jitter is caused by packet reassembling on the transmission device or receiving device, such as the timeout processing, retransmission mechanism, and insufficient buffer.

Solution

- Improve the network quality.
- Change the codec of the IP phone. Generally, the default codec of an IP phone is G.711A. If the network quality is low, you can set the codec to G.729 or G.723.

4.2.14 When Subscribers Talk on the IP Phone, the Voice Heard Is Excessively Low

Problem

When subscribers talk on the eSpace 6805, eSpace 6810, eSpace 6830, eSpace 6850 and eSpace 6870, the voice heard is excessively low.

Cause

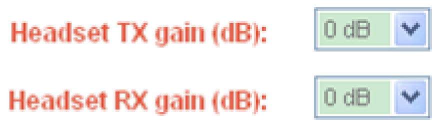
The volume of the IP phone is excessively low.

Solution

The volumes of the eSpace 6805, eSpace 6810, eSpace 6830, eSpace 6850 and eSpace 6870 include the microphone volume of the IP phone, hand-free speaker volume, earphone volume, and microphone volume of the earphone. The preceding volumes are output volumes and the microphone volume of the earphone is the input volume. The input volume of the IP phone and hand-free speaker cannot be adjusted. The adjustment of the volumes is independent, that is, adjusting the microphone volume of the IP phone does not affect the volume of the speaker.

- Adjustment of the microphone volume of the IP phone: Press the Up or Down arrow key to adjust the volume after the IP phone is picked up. The default volume is four blocks. The maximum volume is seven blocks.
- Adjustment of the hand-free speaker volume: Press the Up or Down arrow key to adjust the volume after the **hand-free** key is pressed. The default volume is four blocks. The maximum volume is seven blocks.
- Adjustment of the earphone volume: Press the Up or Down arrow key to adjust the volume after the **HEADSET** key is pressed. The default volume is four blocks. The maximum volume is seven blocks. For certain earphones, if the volume is low after the volume of the IP phone is set to seven blocks. In this case, you can access the **BASIC SETTINGS** page and set the value of **Headset RX gain (dB)** to +6 dB. Then the volume of about one block is increased.
- Adjustment of the microphone volume of the earphone: On the IP phone, the microphone volume cannot be adjusted. You can access the **BAISC SETTINGS** page and adjust the value of **Headset TX gain (dB)**. Then the microphone volume is adjusted.

Figure 4-5 Headset TX gain (dB)



NOTE

- Up and Down keys in hook-off state can be used to adjust the microphone volume of the IP phone, the hand-free speaker volume, and the earphone volume.
- The parameters **Headset RX gain (dB)** and **Headset TX gain (dB)** on the Web configuration page can be used to adjust only the speaker volume of the earphone and the microphone volume of the earphone.

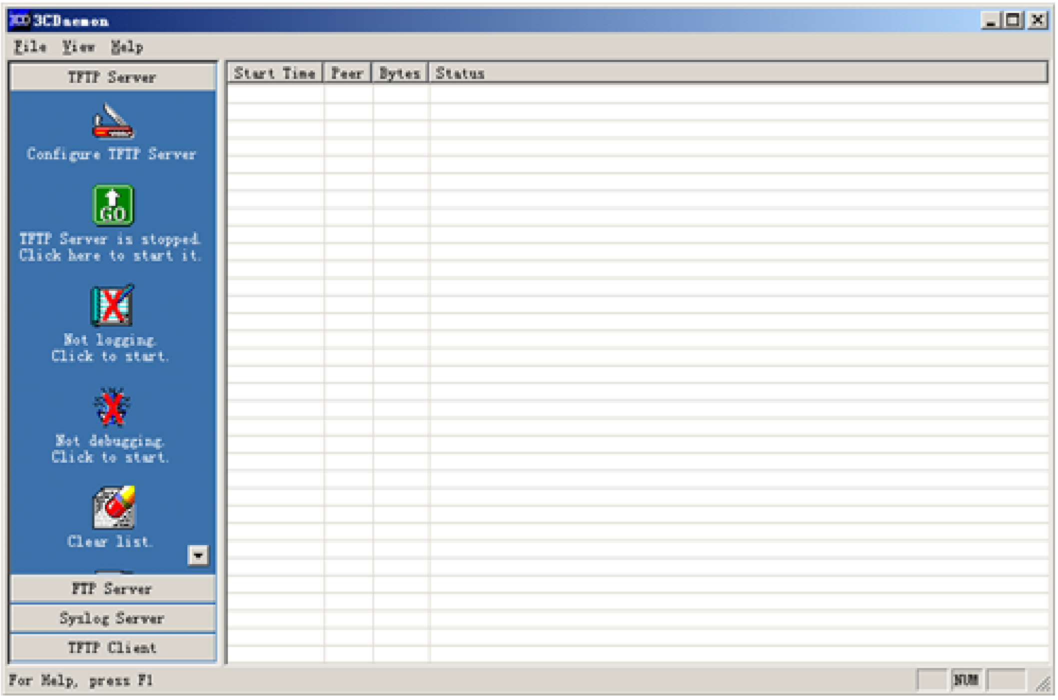
5 Appendix

5.1 Configuring the TFTP Server

Download the TFTP server from the official website.Here takes 3CDaemon TFTP server as an example.

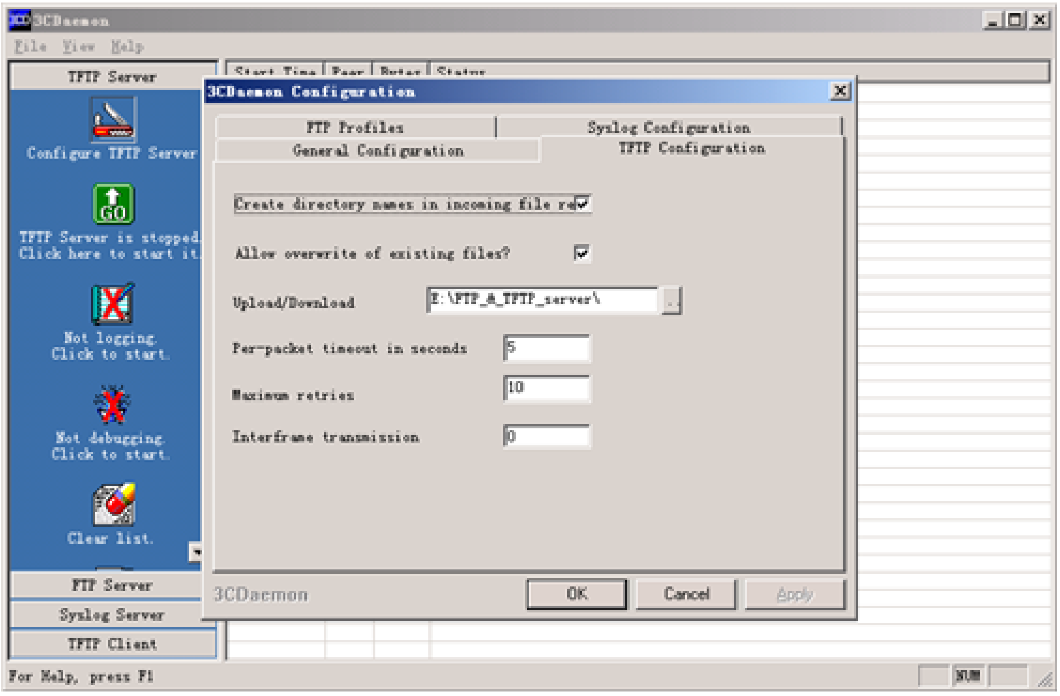
1. Start the TFTP server.

Figure 5-1 Starting the TFTP server



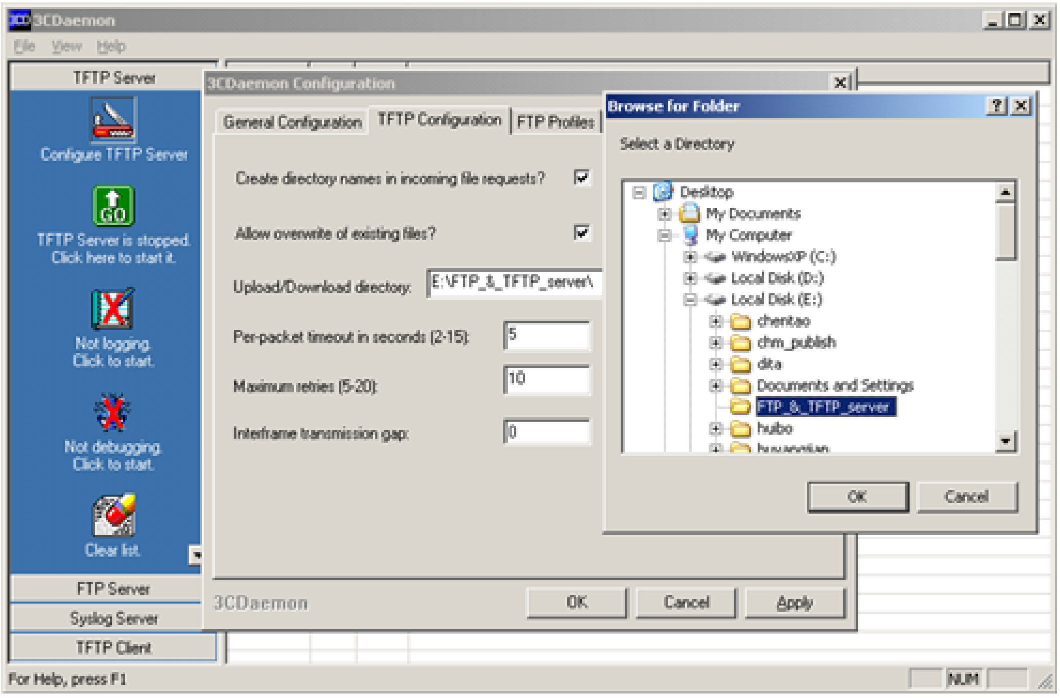
2. Click **Configure TFTP Server** in the **TFTP Server** area.

Figure 5-2 Configure TFTP Server



3. Select the directory where the file to be upgraded exists in the **Upload/Download** text box on the **TFTP Configuration** tab page.

Figure 5-3 Selecting a directory



----End

CAUTION

- This software is green software that does not need to be installed.
- The version file in the directory server is a .bin file.

5.2 Configuring the HTTP Server

Method 1: Apache Server

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

Assume that Apache HTTP Server2.2 has been installed in the Windows XP operating system. Perform the following steps to start the Apache Server and place the required files:

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

   If icon  is shown on the taskbar, the Apache server has been started. If icon  is shown on the task bar, right-click the icon and choose **Start** from the shortcut menu.

2. Place the required files in the installation path, for example,**Apache Software Foundation\Apache2.2\htdocs.**

NOTE

- If the required files are placed directly in the**htdocs** folder, type 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://10.10.10.9:8088/serviceagenthttp://192.169.1.51**.
- If the required files are placed under a subfolder of the **htdocs** folder, type 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**.

Method 2: Using the Windows IIS Component

The Windows Internet Information Service (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 IIS component.

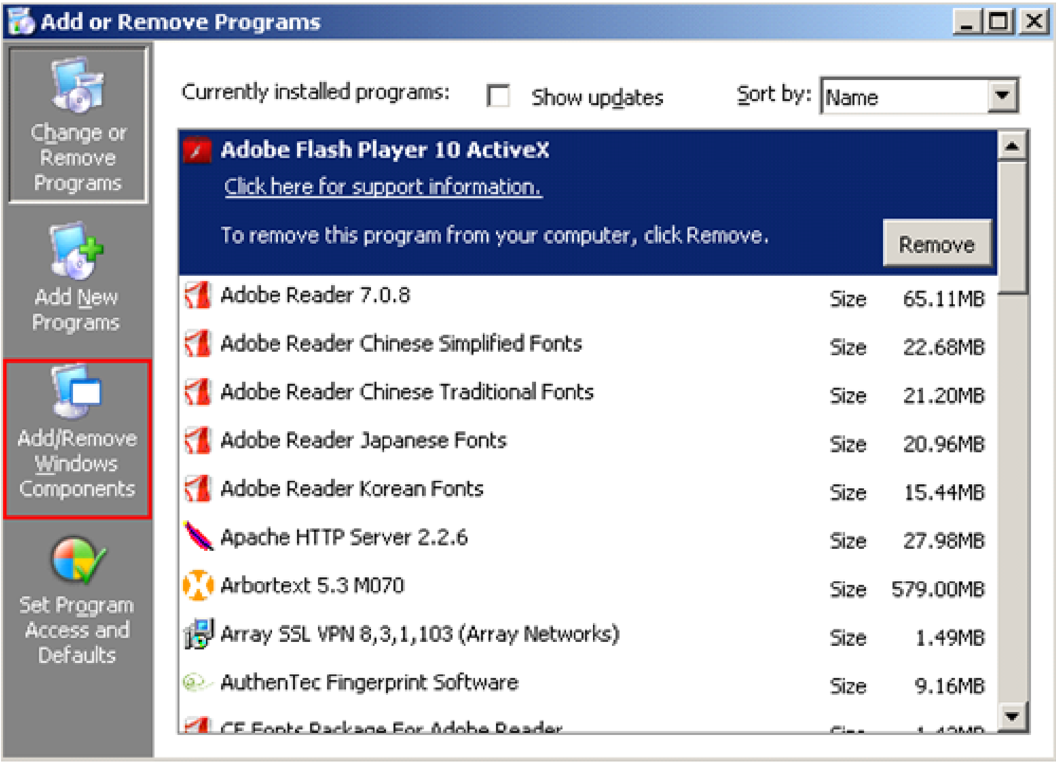
To install the IIS component in the Windows XP operating system, proceed as follows:

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

   The **Control Panel** window is displayed.
2. Double-click **Add or Remove Programs**.

   The **Add or Remove Programs** window is displayed, as shown in Figure 5-4.

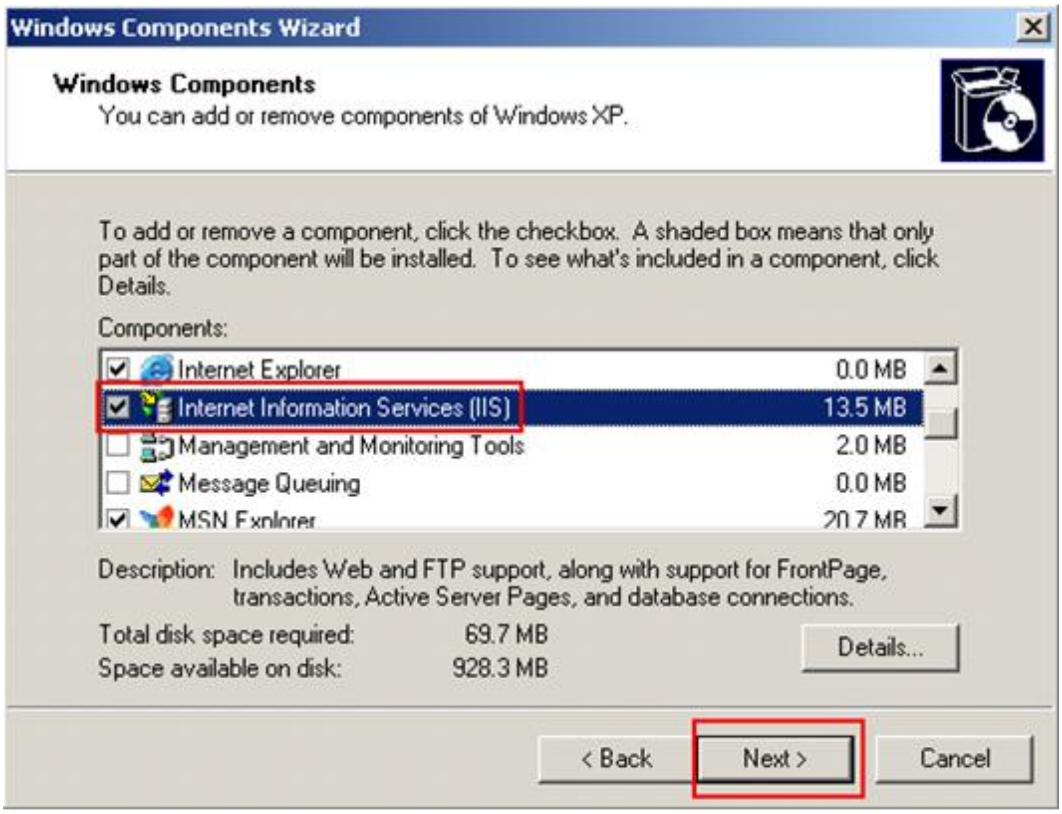
Figure 5-4 Add or Remove Programs window



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

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

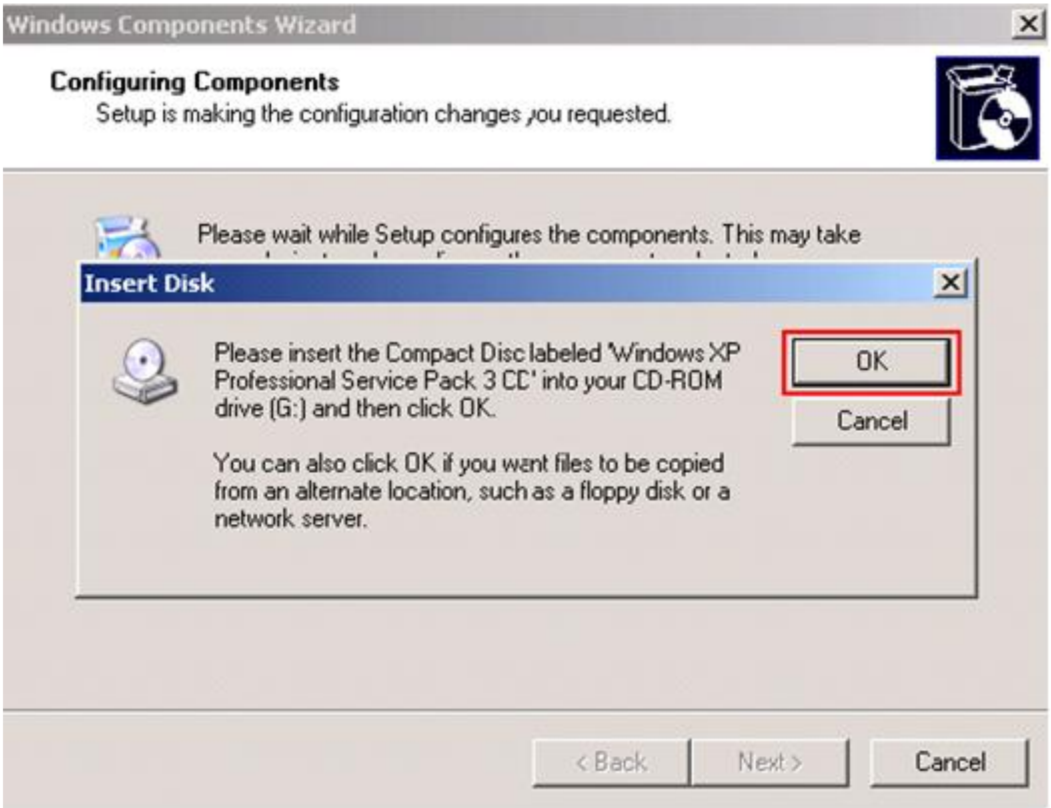
Figure 5-5 Windows Components Wizard window



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, as shown in Figure 5-6.

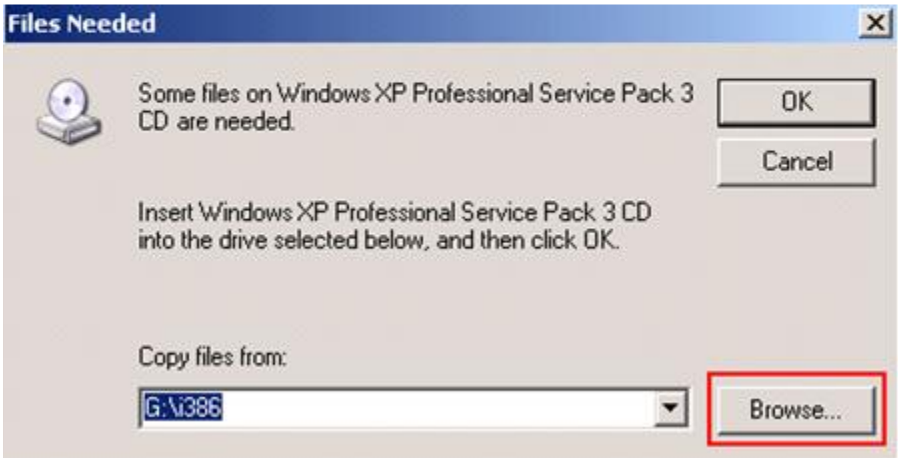
Figure 5-6 Insert Disk dialog box



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

   The **Files Needed** dialog box is displayed, as shown in Figure 5-7.

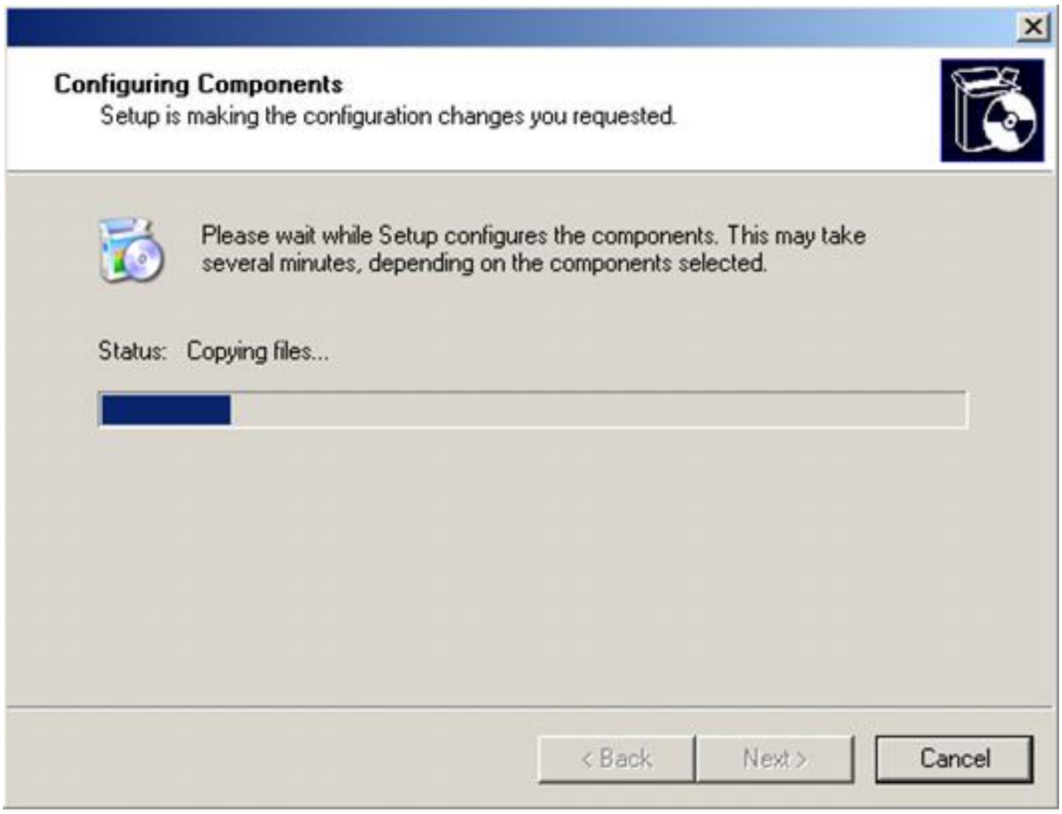
Figure 5-7 Files Needed dialog box



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

The system starts copying the files and installing the component, as shown in Figure 5-8.

Figure 5-8 Configuring Components dialog box



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

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

----End

5.3 Making a Personal Phone Book on IP Phone

Making a Phone Book

Making personal phone books on an IP phone is difficult because of the restrictions of keys and input modes of the IP phone. You can make a personal phone book on a computer, and import the phone book to the IP phone.

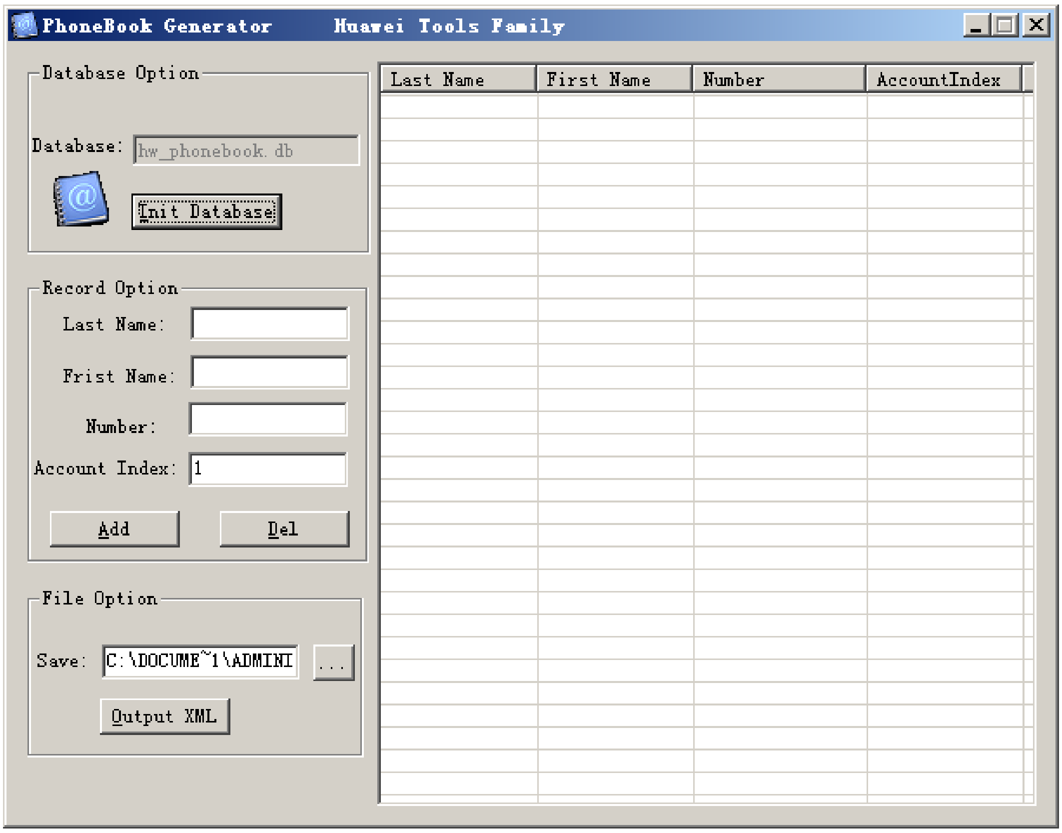
Phone Book Generator is a tool for generating phone books based on the development mode of a mini-database. This tool can be used to generate **.xml** files conveniently, quickly, and effectively for the IP phones to download. By using this tool, you can quickly modify an existing record.

Log in to **http://support.huawei.com/** to download **PhoneBook.exe**.The path is **SUPPORT** > **Software Center** > **Version Software** > **Application and Software Product Line** > **Application and Software Solution** > **Enterprise UC>IP Phone**.

After decompressing the preceding package, double-click **PhoneBook.exe**.

Figure 5-9 shows the **PhoneBook Generator** page.

Figure 5-9 PhoneBook Generator page



- Creating a phone book

  Start the software and clear the existing records in the database. Click **Init Database** to create a phone book.

- Adding a record

  Table 5-1 describes the parameters in each new record.

Table 5-1 Parameters in each new record

Parameter	Description	Value Range
Last Name	Name	The value cannot be blank.
First Name	First name.	The value cannot be blank.
Number	Phone number.	The value must be a numeral.
Account Index	Account index of the IP phone.	The value must be a numeral ranging from **1** to **4**. The default value is **1**.

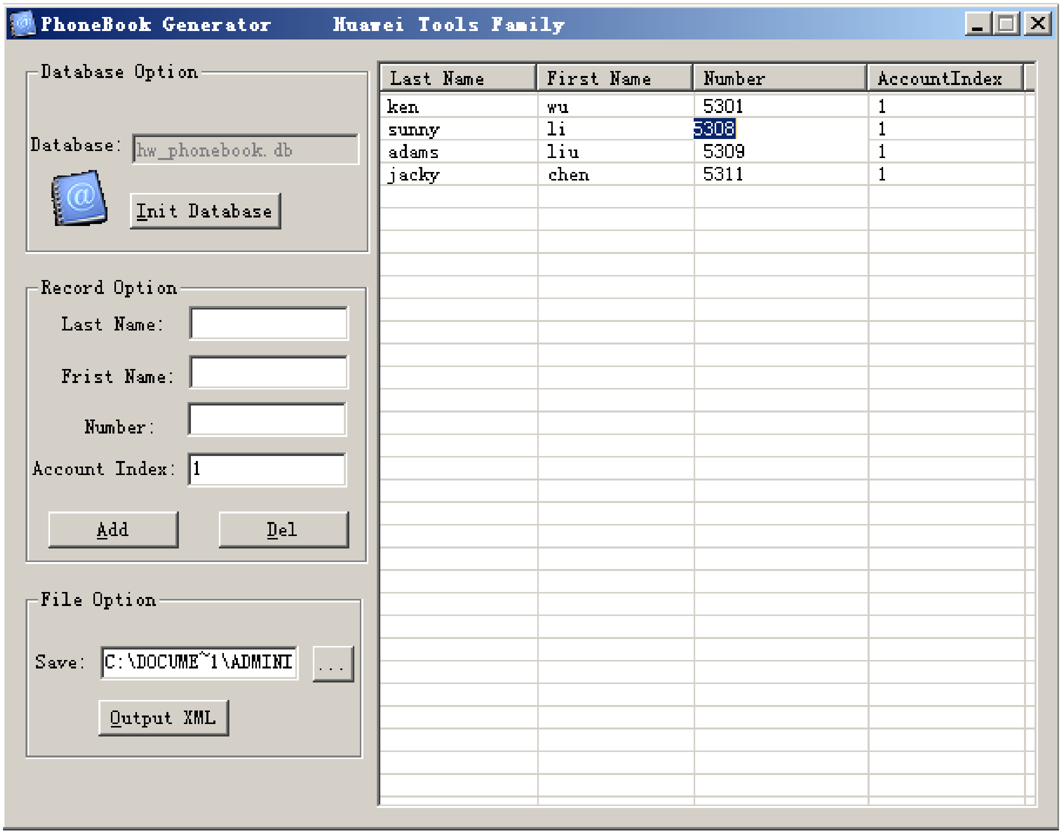
After entering the parameter values in the preceding table, click **Add**. The new record is displayed on the right of the page.

- Modifying a record

  To modify an existing record, change the value directly on the right of the page. The database automatically saves the new value and discards the old value.

  Assume that the phone number of Sunny is changed to 5310. Click **5308**, and enter 5310.

Figure 5-10 Changing a phone number



- Deleting a record

  You can delete a useless record by using the following method:

  Click the record that you want to delete on the right of the page, and click **Del**.

CAUTION

If you delete a record, the records with the same phone number are also deleted. You are recommended to ensure that each phone number is unique when you add records. Actually, each phone number is unique.

- Exporting a phone book

Verify that the records on the right of the page are complete and correct, and export the phone book. To export a phone book, you can click **...** to select the destination path, and enter the file name. The default destination path is the same as the path of the PhoneBook Generator. Click **Output XML** to generate a phone book in .**xml** format in the corresponding path.

CAUTION

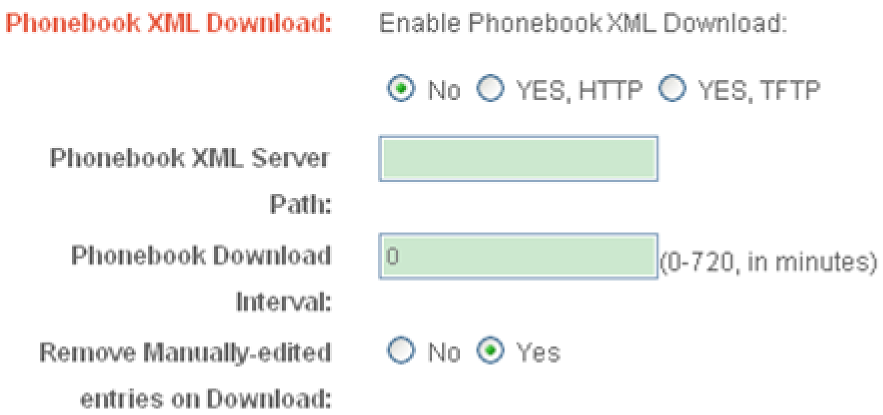
- The **Upgrade** button displayed after you click … is used only to select the destination path. The **Output XML** button is used to export an .xml file.
- Do not change the name of the phone book file. Otherwise, it cannot be imported. The default phone book file is **named hw_phonebook.xml**.

Importing a Phone Book to an IP Phone

To download a ring tone file to an IP phone through HTTP or TFTP, proceed as follows:

1. Store the generated .xml files to the version path of the upgrade server, and configure the TFTP server or HTTP server.
2. Access the **ADVANCED SETTINGS** tab page on the Web page, set the path for downloading a phone book, select whether to remove the phone book that is added manually. Generally, set the interval for downloading a phone book, and select not to remove the phone book that is added manually.

Figure 5-11 Advanced settings



5.4 Setting Personal Ring Tones for an IP Phone

eSpace 6805, eSpace 6810, eSpace 6830, eSpace 6850 and eSpace 6870 can be used to make personal ring tones. The personal ring tones can be used as the default ring tone of an IP phone or as one of the three distinctive ring tones for calling numbers.

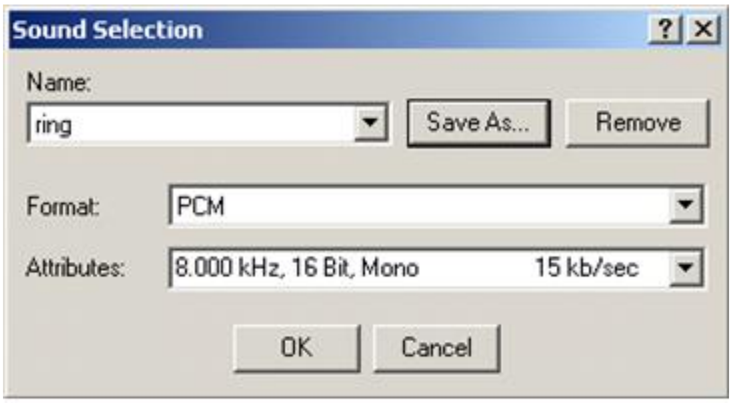
Making a Ring Tone

1. Select three favorite songs in .mp3, .wma, or .rm format which can be converted through an audio conversion tool. Download an audio conversion tool such as the Audio Converter, and convert the three songs to **.wav** format.
2. Choose **File** > **Open**, and select a song of **.wav** format.
3. If the Windows Sound Recorder is used, choose **File** > **Properties** to display the Properties for Sound dialog box.

Figure 5-12 Properties for Sound dialog box

4. Click **Convert Now** to convert the file in .wav format generated in step 1 to the 16-bit linear PCM audio file in .wav format.

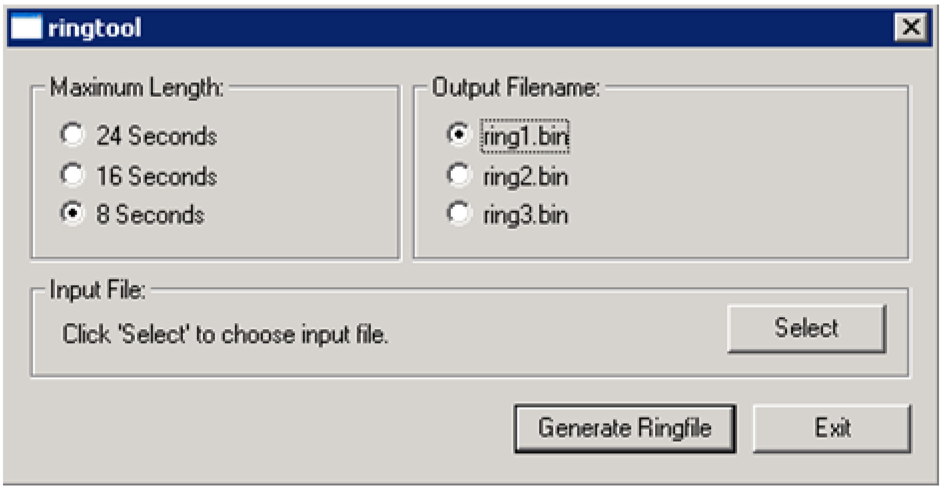
Figure 5-13 Sound Selection dialog box



5. Click **OK** to close the **Sound Selection** dialog box.
6. Click **OK** to close the **Properties for Sound** dialog box.
7. Choose **File** > **Save** as to convert the song to the 16-bit linear PCM .wav format.
8. Run the **ringtool.exe** tool for generating ring tones.

   The GUI is displayed as follows:

Figure 5-14 Ringtool dialog box



   Click select to load the audio files in .wav format. Select values for **Maximum Length** and **Output Filename**, and click **Generate Ringfile** to generate a ring tone file.

   Download the **ringtool.exe** software from the official website.

9. Click **Select** to load the song (**.wav** format) converted in Step 7.
10. Choose **Maximum Length** as **8 Seconds** and Choose the **Output Filename**.
11. Click **Generate Ringfile** to make the ring tones.

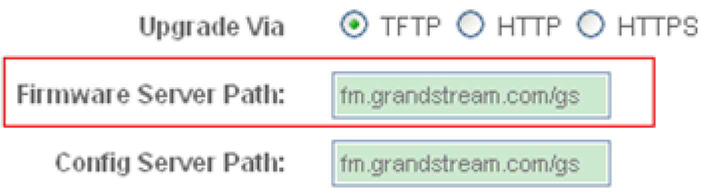
   ----End

Downloading the Ring Tone File to the IP Phone Through HTTP or TFTP

To download the ring tone file to the IP phone, proceed as follows:

1. Store the **ring1.bin**, **ring2.bin**, and **ring3.bin** files to the version path of the upgrade server.
2. Log in to the **ADVANCED SETTINGS** page of the Web page of the IP phone and set the upgrade mode and path (firmware server path) of the IP phone.

Figure 5-15 Firmware server path



3. Disable DHCP Option 248.

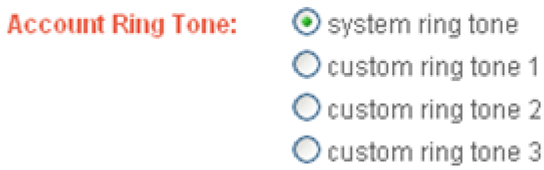
4. Restart the IP phone. The IP phone downloads the three files when the time for automatic upgrade comes.

----End

Replacing the Original Ring Tone with a Personal Ring Tone

Access the **Account** tab page on the Web page of an IP phone. You can select three customized ring tones and one system ring tone as the default ring tone.

Figure 5-16 Account Ring Tone

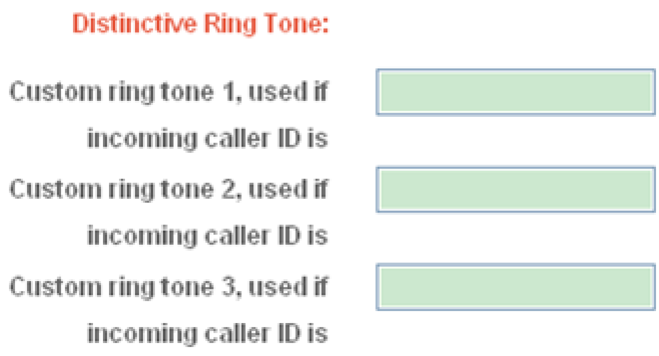


Setting Distinctive Ring Tones for Phone Numbers

You can set distinctive ring tones for three phone numbers on eSpace 6805, eSpace 6810, eSpace 6830, eSpace 6850, or eSpace 6870 IP phones.

You can set distinctive ring tones for three phone numbers on the **ADVANCED SETTINGS** tab page on the Web page of an IP phone.

Figure 5-17 Distinctive Ring Tone



NOTE

When a phone number that is not set with a distinctive ring tone calls, the default ring tone will be used.

5.5 Making Configuration File Templates

A global configuration file template is provided for deployment. The template may not meet onsite requirements. 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://support.huawei.com/**.

Double-click the **config.xml** file, and modify parameter settings.

Each configuration file parameter is in .xml format and consists of multiple items. Each item consists of the parameter name, value, and description.

Figure 5-18 shows the configuration file template.

Figure 5-18 Configuration file template

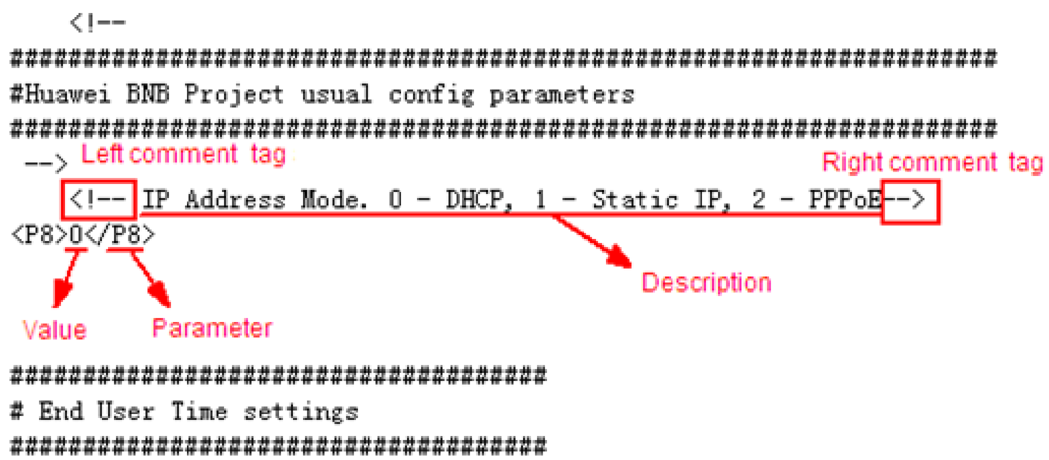


Table 5-2 lists the commonly used parameters and their settings.

NOTE

- For parameter description, see Table 2-2 in the and Table 2-3 in the #IP_Phone_68xx_Appendix_00006/IP_Phone_68xx_SingleConfig_00008.xml.
- When modifying the template, you are advised to comment out unnecessary parameters. If you want to use these parameters again, delete the comment characters.

Table 5-2 Parameters in the configuration file template

ID	Parameter	Setting Example	Description
P8	IP Address	0	Mode of obtaining the phone's IP address. • 0: Obtain the IP address through DHCP • 1: Use a static IP address. • 2: Obtain the IP address through PPPoE The default value is **0**.
P64	Time Zone	TZY-8	Time zone of a phone. If the phone is not located in a defined time zone, set this parameter to **customize**, and set the **P246** parameter at the same time. The default value is **TZY-8**.
P246	Self-Defined Time Zone	MTZ+6MDT+5,M4.1.0,M11.1.0	User-defined time zone including the DST. For example, MTZ+6MDT+5, M4.1.0, M11.1.0. **MTZ+6MDT+5** specifies the time zone, **M4.1.0** specifies the DST start time, and **M11.1.0** specifies the DST end time. • In the parameter value, + indicates that the time zone is on the west of the Prime Meridian; **-** indicates that the time zone is on the east of the Prime Meridian. • In the DST, the first part specifies the month, the second part specifies the week, and the third part specifies the day. For example, **M4.1.0**, **M11.1.0** indicates that the DST starts from the second Sunday in March to the first Sunday in November. • Within the DST, the MDT time is used; otherwise, the MTZ time is used. The default value is **MTZ+6MDT+5,M4.1.0,M11.1.0**.
P1312	HEADSET Key Mode	0	Headset key mode. • 0: No headset is used. • 1: A headset is used. The default value is **0**.
P2	Admin Password	Admin	Password for the administrator to access the Web configuration page.

ID	Parameter	Setting Example	Description
			The default value is **admin**.
P38	Layer 3 QoS	12	Value of Layer-3 QoS. The default value is **12**.
P51	802.1Q/VLAN Tag	0	802.1Q VLAN tag. The default value is **0**.
P87	802.1p priority value	0	802.1P priority value. The default value is **0**.
P212	Upgrade Via	1	Protocol used for upgrade. • 0: TFTP • 1: HTTP • 2: HTTPS The default value is **1**.
P192	Firmware Server Path	10.10.10.1	Firmware server address. The default value is **um.huawei.com/etphone**.
P237	Config Server Path	10.10.10.1	Config server address. The default value is **um.huawei.com/etphone**.
P145	Allow DHCP Option 43 and Option 66 to override server	1	Indicates whether to enable the Option43 and Option66 settings on the DHCP server. • 0: No • 1: Yes The default value is **1**.
P1408	Disable DHCP Option248	0	Indicates whether to disable DHCP Option248. • 0: No • 1: Yes The default value is **0**.
P194	Automatic Upgrade	0	Indicates whether to automatically upgrade phone software. • 0: No • 1: Yes The default value is **0**.
P193	Automatic Upgrade	1440	Interval for checking new versions. This parameter is valid only when **Automatic Upgrade** is set to 1. The unit is minute.

ID	Parameter	Setting Example	Description
			The default value is **1440**.
PEnableTR069	Enable TR-069	0	Indicates whether to enable TR-069. • 0: No • 1: Yes The default value is **0**.
P4504	TR-069 Username	User	TR-069 user name. There is no default value.
P4505	TR-069 Password	User	Password of the TR-069 user. There is no default value.
P4503	ACS URL	10.10.10.1:8089	URL of the ACS server. There is no default value.
P4506	Periodic Inform Enable	0	Indicates whether to enable scheduled connection. • 0: No • 1: Yes The default value is **0**.
P4507	Periodic Inform Interval	3600	Scheduled connection interval. The unit is second. There is no default value.
P4511	Connection Request Username	Admin123	User name used for a phone to authenticate the connection to the ACS. There is no default value.
P4512	Connection Request Password	Admin123	Password for a phone to authenticate the ACS. There is no default value.
P4519	Authentication Method	0	Mode of authenticating the ACS when the ACS attempts to connect to a phone. • 0: No Authentication • 1: Basic • 2: Digest The default value is **0**.
P4518	Connection Request Port	7080	Port number for the ACS to send connection requests to a phone. There is no default value.
P207	Syslog Server	10.10.10.2	IP address or URL of the Syslog server. There is no default value.
P208	Syslog Level	0	Log level. • 0: None

ID	Parameter	Setting Example	Description
			• 1: Debug • 2: Info • 3: Warning • 4: Error The default value is **0**.
P1387	Send SIP Log	0	Indicates whether to send SIP logs. • 0: No • 1: Yes The default value is **0**.
P30	NTP Server	10.10.10.3	NTP server address. It can be a domain name or an IP address. The default value is **us.pool.ntp.org**.
P1345	Public Mode	0	Indicates whether to enable the public mode. If this parameter is set, **SIP Server** is mandatory. • 0: No • 1: Yes The default value is **0**.
P1362	Display Language	auto	Phone language. The default value is **auto**.
P47	SIP Server	10.10.10.4	IP address of the SIP server. There is no default value.
P103	DNS Mode	0	DNS mode. • 0: A Record • 1: SRV • 2: NAPTR/SRV • 3: User-defined mode The default value is **0**.
P2308	Primary IP	10.10.10.5	Primary IP address. This parameter is valid only when **DNS Mode** is set to **3**. There is no default value.
P2309	Backup IP1	10.10.10.6	Backup IP address 1. This parameter is valid only when **DNS Mode** is set to **3**. There is no default value.
P2310	Backup IP2	10.10.10.7	Backup IP address 2. This parameter is valid only when **DNS Mode** is set to **3**. There is no default value.
P32	Register Expiration	60	Registration expiration time, in minutes. The maximum value is **64800**.

ID	Parameter	Setting Example	Description
			The default value is **60**.
P130	SIP Transport	0	SIP transmission mode. • 0: UDP • 1: TCP • 2: TLS/TCP The default value is **0**.
P99	SUBSCRIBE for MWI	0	Indicates whether to subscribe to the voice message service. • 0:No • 1:Yes The default value is **0**.
P33	Voice Mail UserID	90000	ID of a voice mailbox. There is no default value.
P2301	Send DTMF	0	Indicates whether to send DTMF streams in the in-audio mode. • 0:No • 1:Yes The default value is **0**.
P2302	Send DTMF	1	Indicates whether to use RFC2833 to send DTMF streams. • 0:No • 1:Yes The default value is **1**.
P2303	Send DTMF	0	Indicates whether to send DTMF streams in the SIP-INFO mode. • 0:No • 1:Yes The default value is **0**.
P290	Dial Plan	{x+}	Dialing rule. The default value is **{ [*#x]+ }**.
P57	Preferred Vocoder (choice 1)	0	Voice coding type 1. • 0: PCMU • 2: G.726-32 • 4: G.723.1 • 8: PCMA • 9: G.722 • 18: G.729A/B

ID	Parameter	Setting Example	Description
			• 98: iLBC The default value is **0**.
P58	Preferred Vocoder (choice 2)	8	Voice coding type 2. • 0: PCMU • 2: G.726-32 • 4: G.723.1 • 8: PCMA • 9: G.722 • 18: G.729A/B • 98: iLBC The default value is **8**.
P59	Preferred Vocoder (choice 3)	4	Voice coding type 3. • 0: PCMU • 2: G.726-32 • 4: G.723.1 • 8: PCMA • 9: G.722 • 18: G.729A/B • 98: iLBC The default value is **4**.
P60	Preferred Vocoder (choice 4)	18	Voice coding type 4. • 0: PCMU • 2: G.726-32 • 4: G.723.1 • 8: PCMA • 9: G.722 • 18: G.729A/B • 98: iLBC The default value is **18**.
P61	Preferred Vocoder (choice 5)	9	Voice coding type 5. • 0: PCMU • 2: G.726-32 • 4: G.723.1 • 8: PCMA • 9: G.722 • 18: G.729A/B • 98: iLBC The default value is **9**.

ID	Parameter	Setting Example	Description
P62	Preferred Vocoder (choice 6)	98	Voice coding type 6. • 0: PCMU • 2: G.726-32 • 4: G.723.1 • 8: PCMA • 9: G.722 • 18: G.729A/B • 98: iLBC The default value is **98**.
P46	Preferred Vocoder (choice 7)	2	Voice coding type 7. • 0: PCMU • 2: G.726-32 • 4: G.723.1 • 8: PCMA • 9: G.722 • 18: G.729A/B • 98: iLBC The default value is **2**.
P183	SRTP Mode	0	Whether to enable SRTP. • 0: disabled • 1: enabled (optional) • 2: enabled (mandatory) • 3: optional The default value is **0**.
P50	Silence SuPPression	0	Indicates whether to enable the silence suppression function. • 0: No • 1: Yes The default value is **0**.
P72	Use # as Dial Key	0	Indicates whether to set the pound key (#) as the **SEND** key. • 0: No • 1: Yes The default value is **0**.

5.6 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

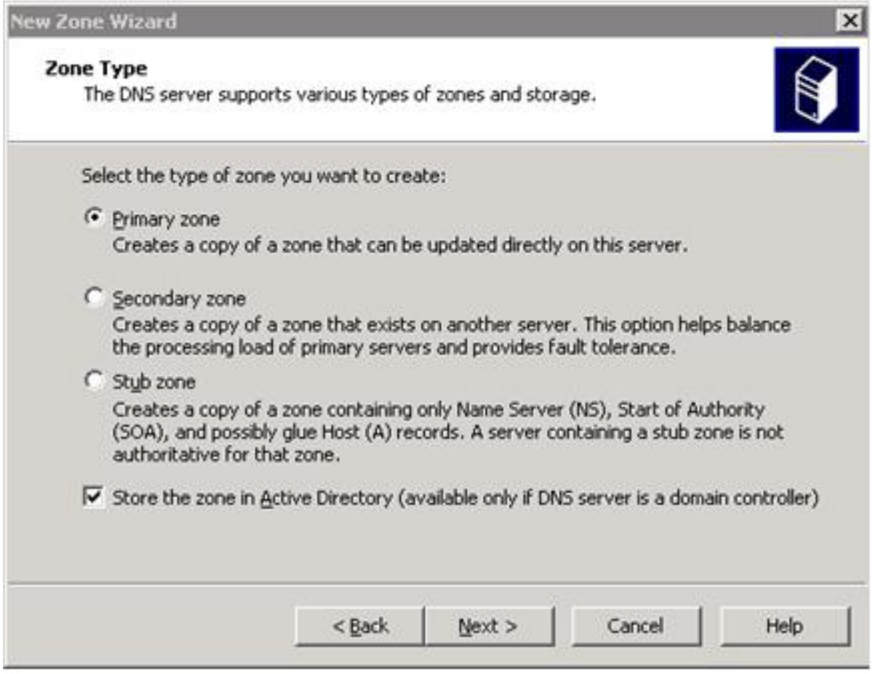
If the DNS service is not installed on the PC, install the DNS component firstly.

Creating a Zone

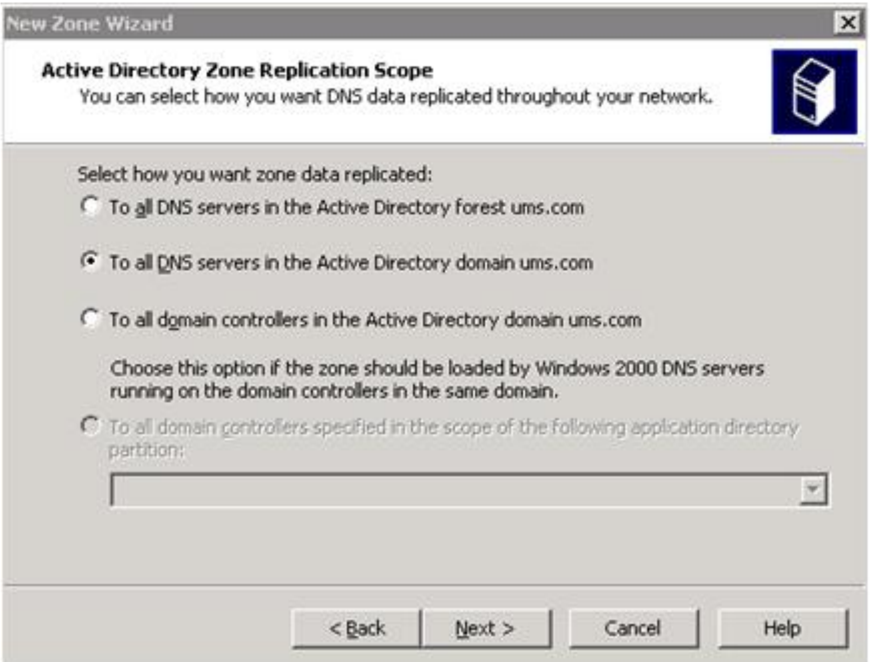
To create a zone, do as follows:

1. Right click **Forward Lookup Zones**, and then choose **New Zone** to start **New Zone Wizard**.

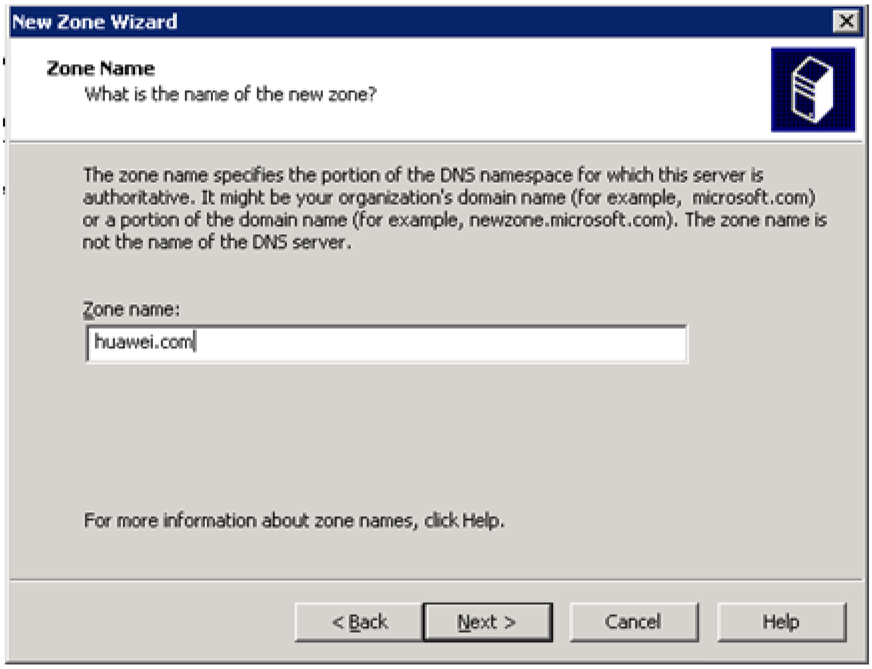
2. Click **Next**, and then select **Primary zone** to create a primary zone.



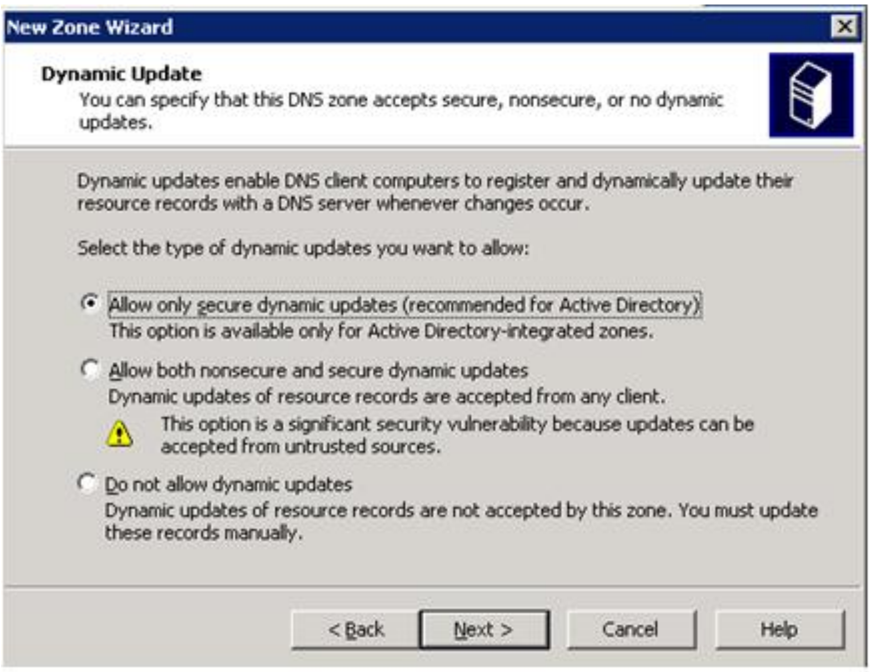
3. Select an option for Select how you want zone data replicated, and click **Next**.



4. Enter the name of the DNS zone, for example, huawei.com. Then click **Next**.

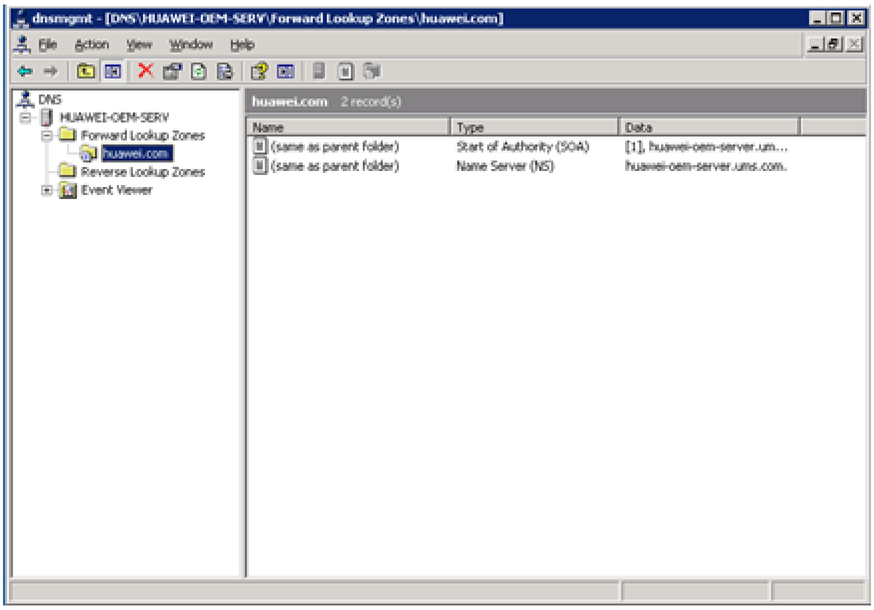


5. Select a dynamic update type, and then click **Next**.



6. After the zone is created, click **Finish**.

7. A new zone is displayed.



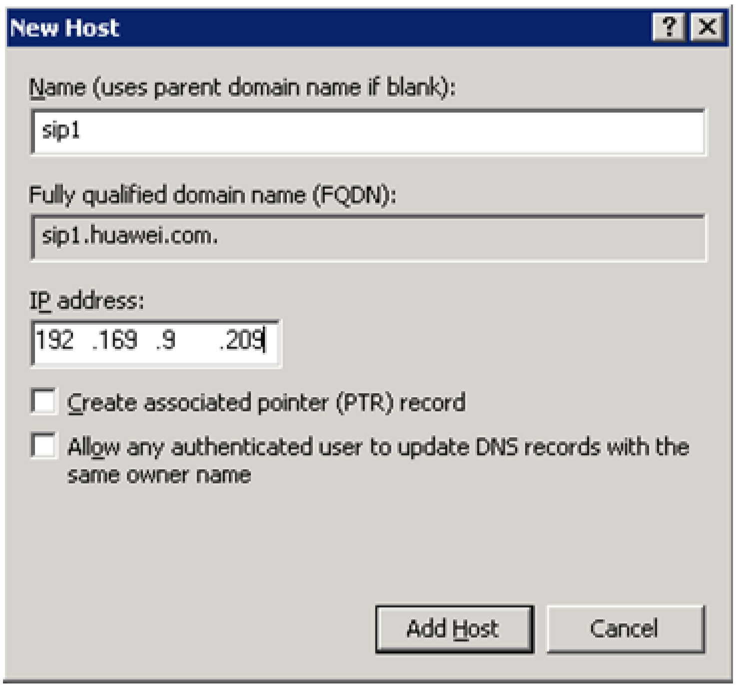
8. Click the zone to display the resource records in detail. You can find that each zone has records **Start of Authority (SOA)** and **Name Server (NS)**, which can be used to determine your DNS server. The SOA indicates the account name that is used.

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:

1. Right-click **Huawei.com** and choose **New Host(A)**. After setting the host name and IP address, click **Add Host**.



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

5.7 Setting Up the DHCP Server

5.7.1 Setting Up the DHCP Server in the Window 2003 Server

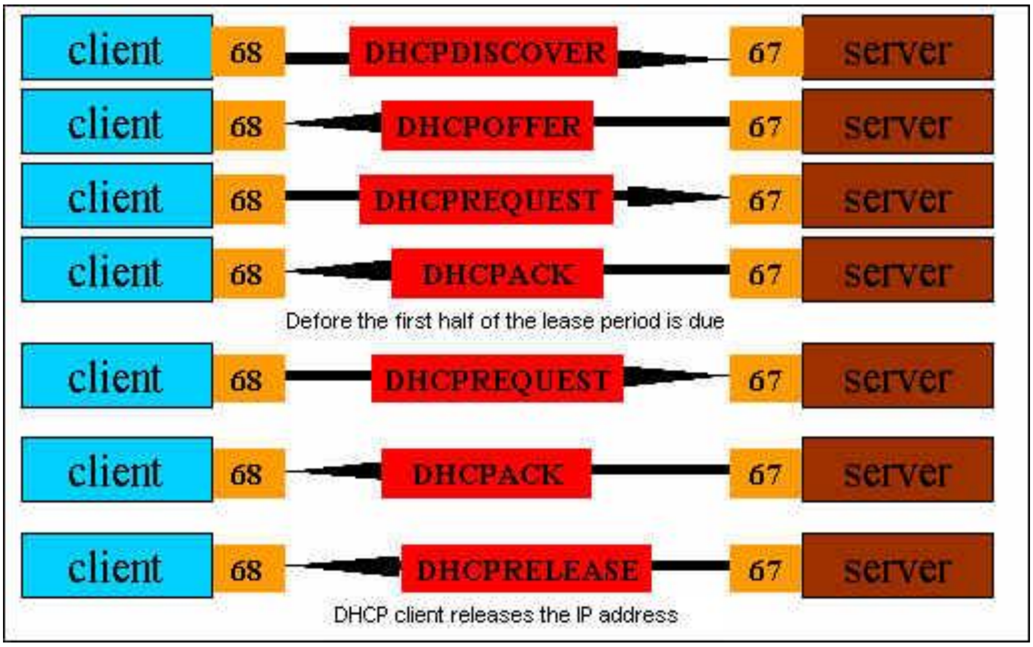
Basics Concepts

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 following figure shows the process for an IP phone to obtain the IP address through DHCP.

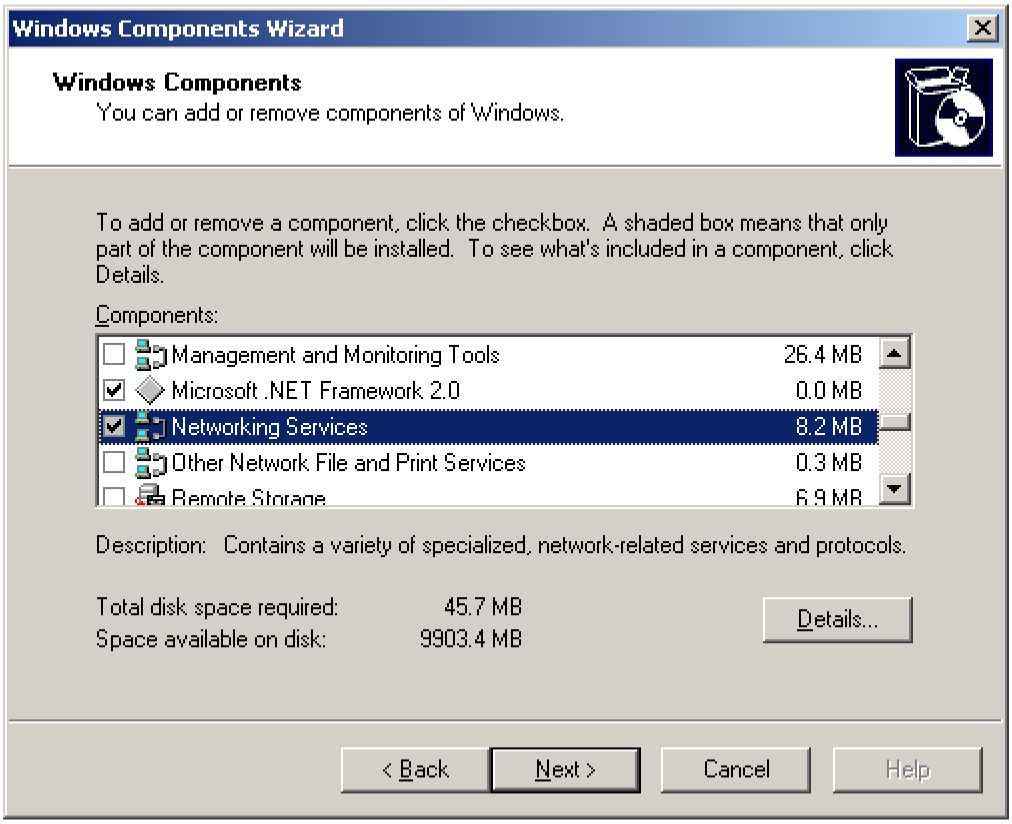


Installing the DHCP Service

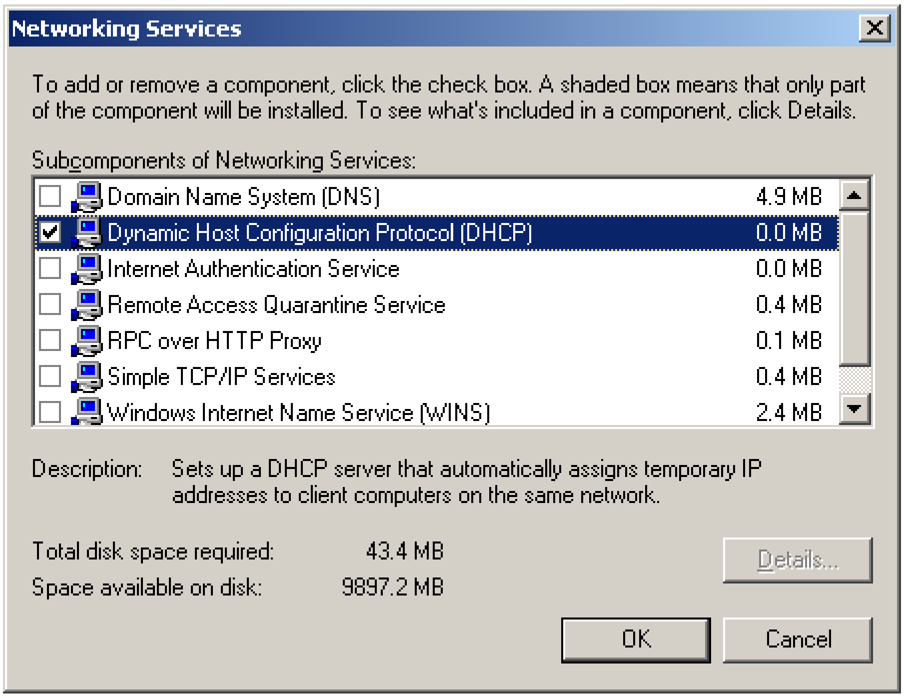
Generally, the DHCP service component is installed by default during the installation of the Window 2003 Server. If the DHCP service component is already installed, go to Starting the DHCP Service and Setting DHCP Parameters. If the DHCP service component is not installed, do as follows to install it:

1. Choose **Start** > **Settings** > **Control Panel**, click **Add or Remove Programs**, and click **Add/Remove Windows Components**.

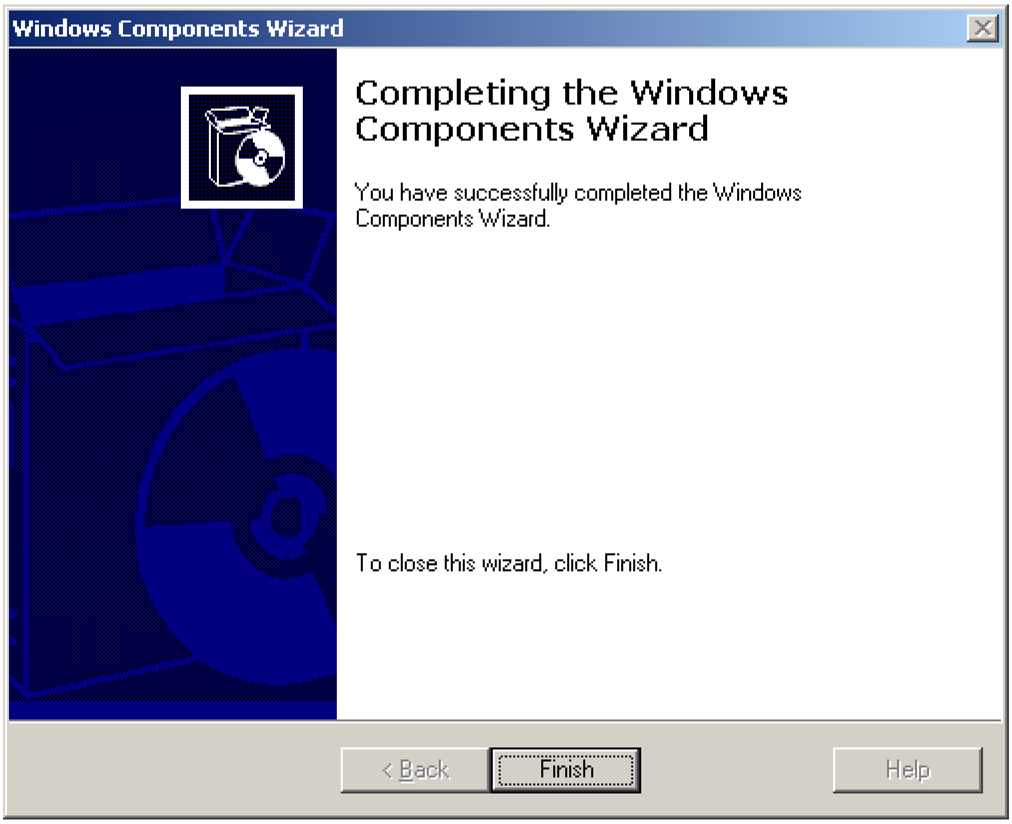
   The **Windows Components Wizard** dialog box is displayed.



2. Select **Networking Services**, and click **Details** to display the **Networking Services** dialog box.



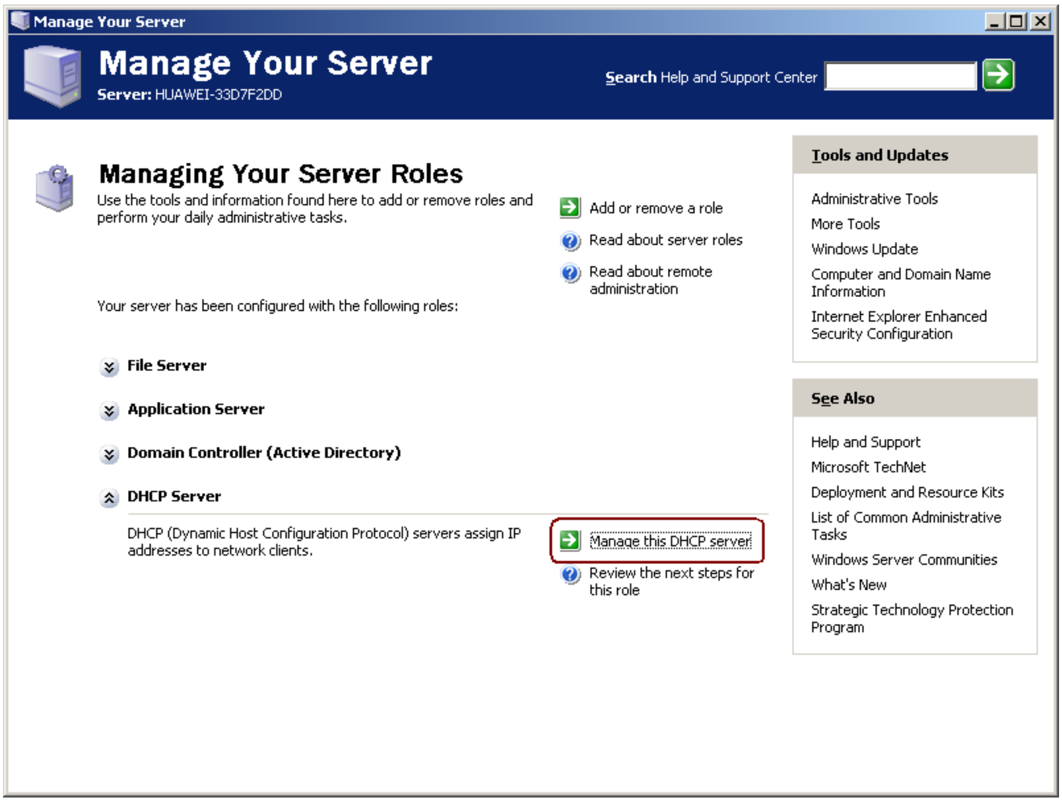
3. Select the DHCP service and click **OK** to exit the page of network service. Click **Next** repeatedly until the installation is complete. After the installation is successful, the dialog box shown in the following figure is displayed.



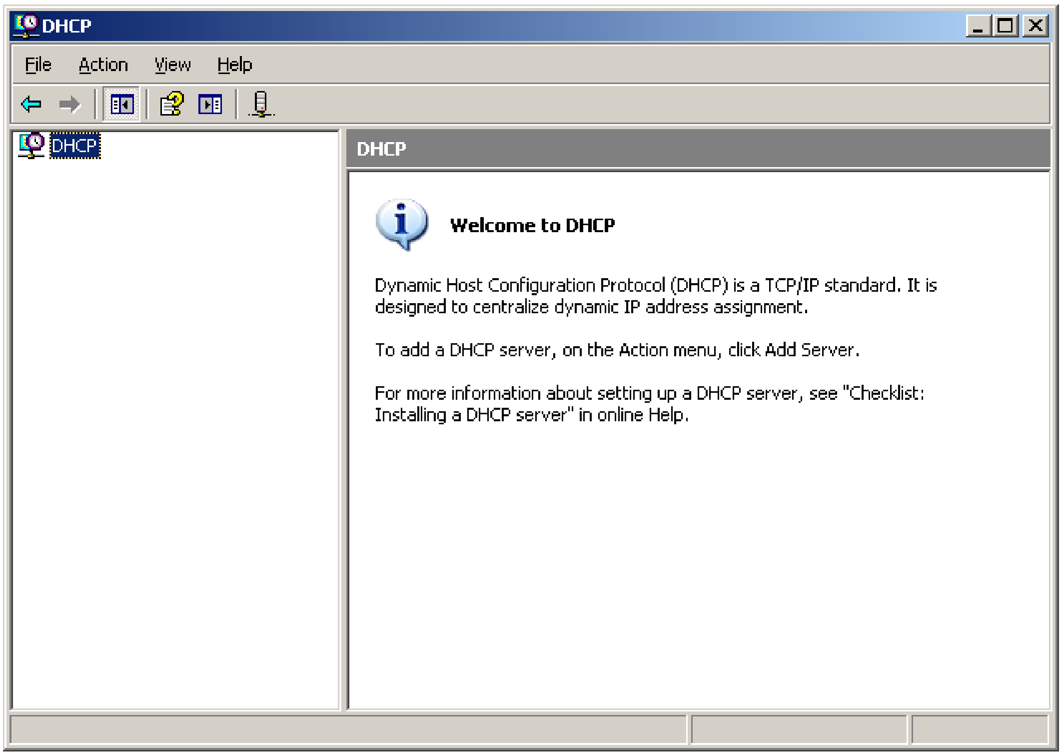
Starting the DHCP Service and Setting DHCP Parameters

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

1. Choose **Start** > **Programs** > **Administrative Tools** > **Manage Your Server**.
2. In the **Manage Your Server** dialog box that is displayed, select **Manage this DHCP** server.

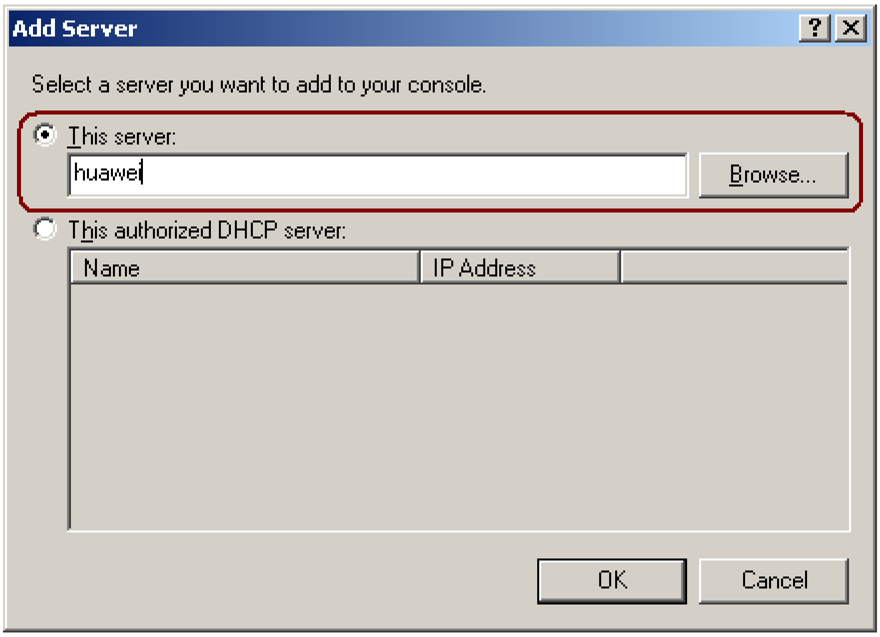


3. Enter the main page of the DHCP, as shown in the following figure.

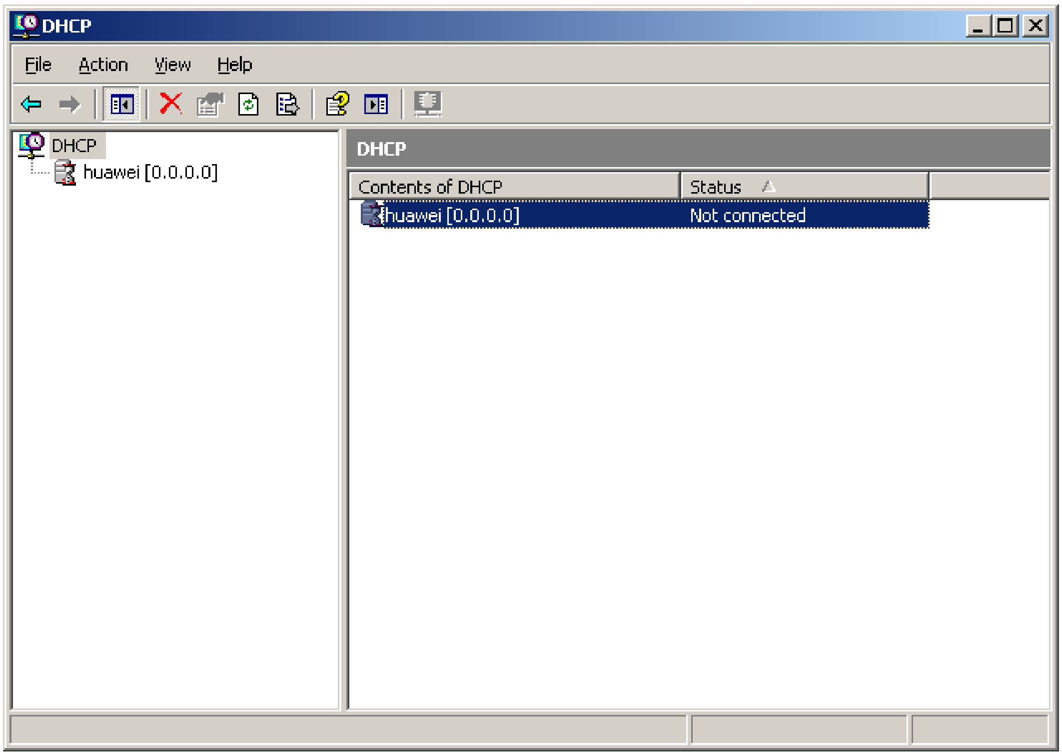


4. Right-click **DHCP** and choose **Add Server**.

   The **Add Server** dialog box is displayed.

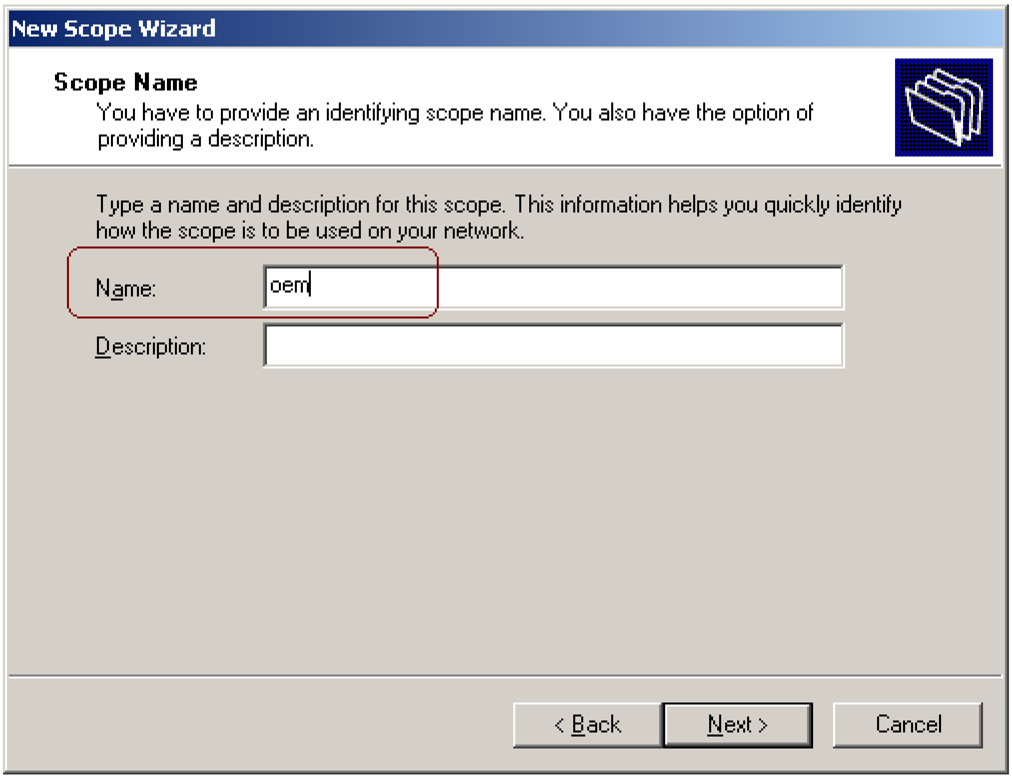


5. Step 5 Set the name of the DHCP server randomly, and then click **OK**. If the setting is successful, the page shown in the following figure is displayed.



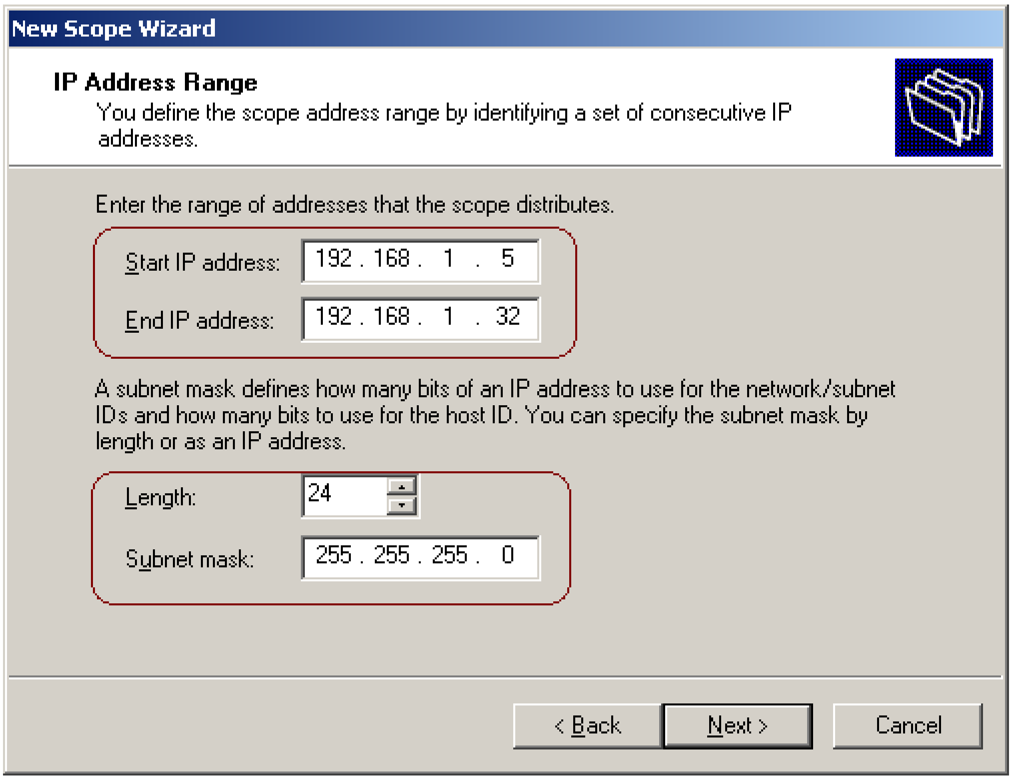
6. Right-click **Huawei[10.10.10.2]** and choose **New Scope**. In the **New Scope Wizard** dialog box that is displayed, click **Next**.

   A dialog box is displayed, as shown in the following figure.

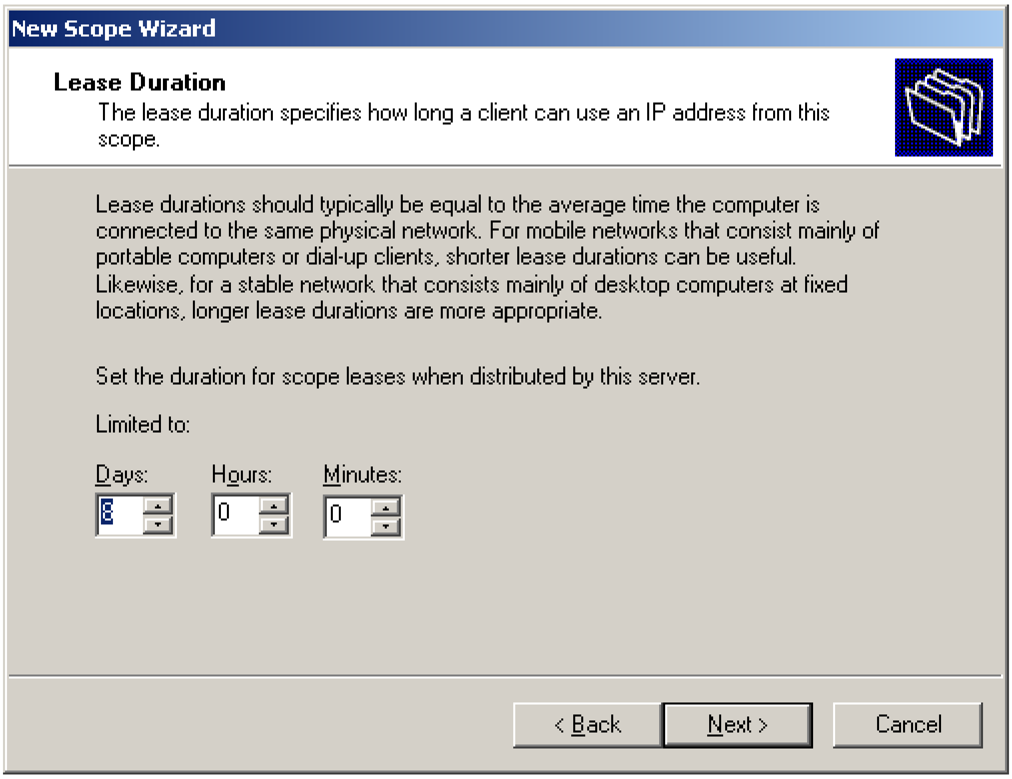


7. Set the name of the new function domain randomly, and then click **Next**.

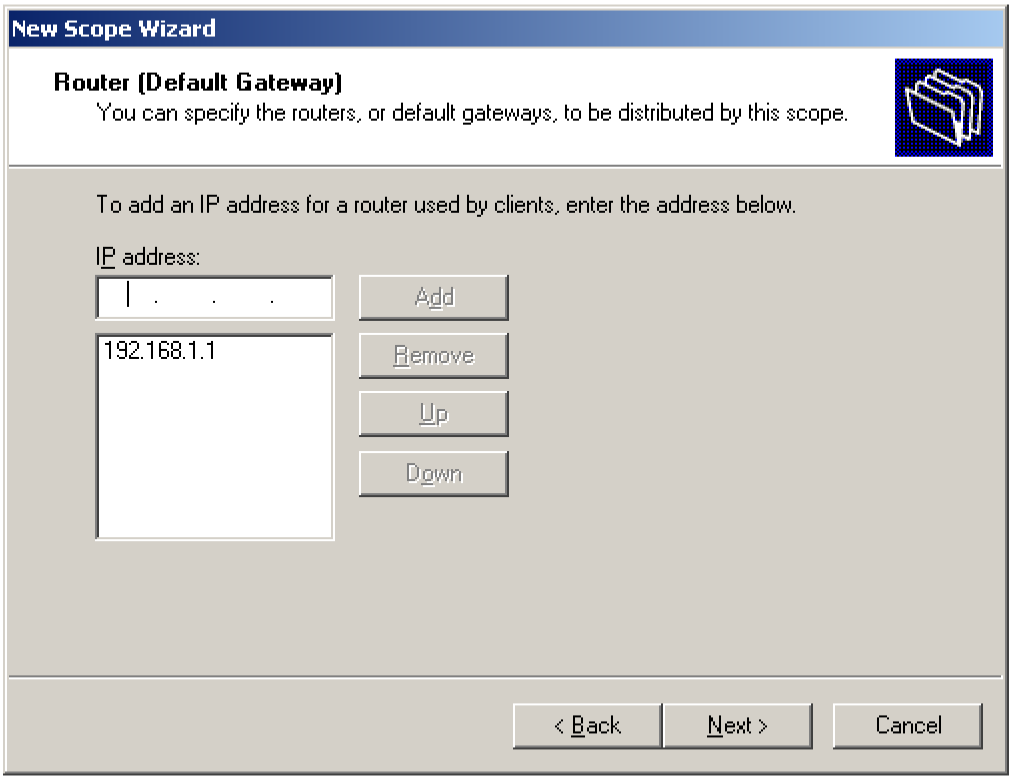
   The following dialog box is displayed.



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.

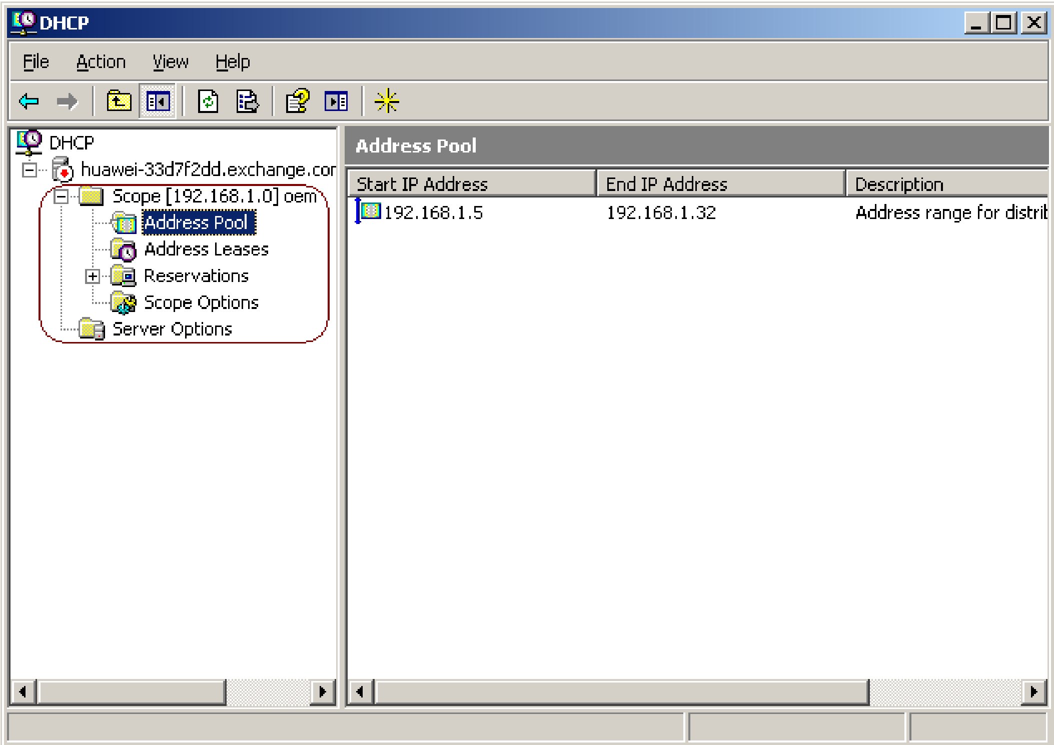


9. In the **Lease Duration** dialog box, you can set the lease period of the DHCP server. By default, the lease period of the DHCP server is eight days. After the setting, click **Next** repeatedly until the **Router(Default Gateway)** dialog box is displayed, as shown in the following figure.



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.



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.

5.7.2 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 + ?**.

5.8 Setting the Option248 Parameter

This document describes how to set the **Option248** parameter.

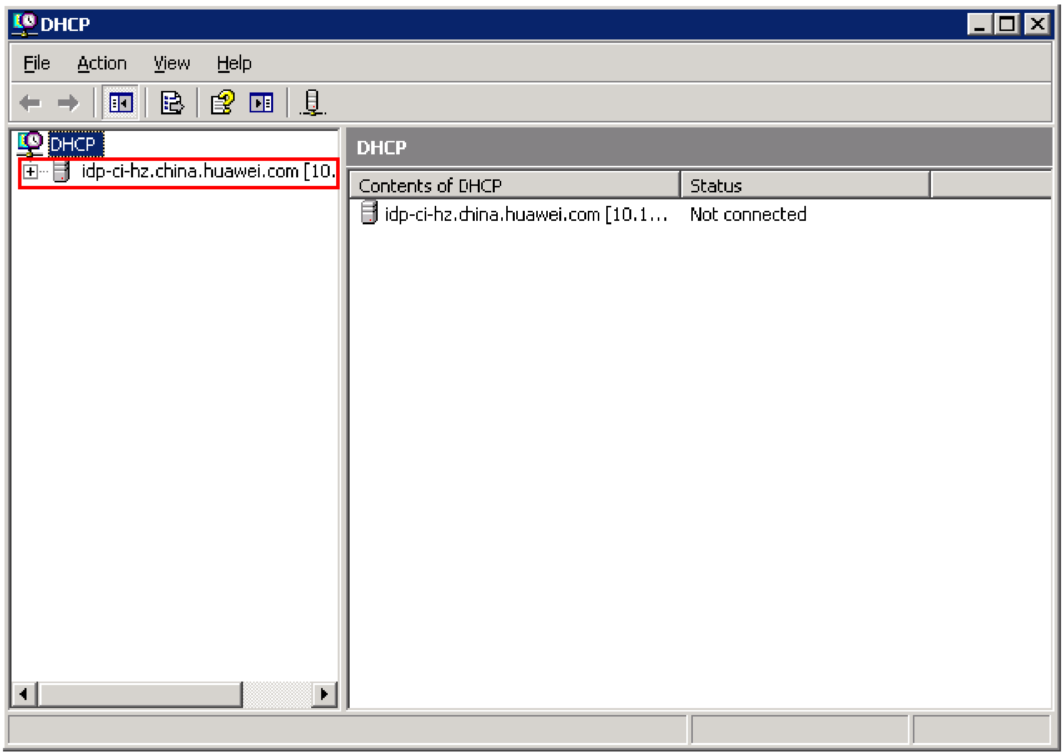
Procedure

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 5-19.

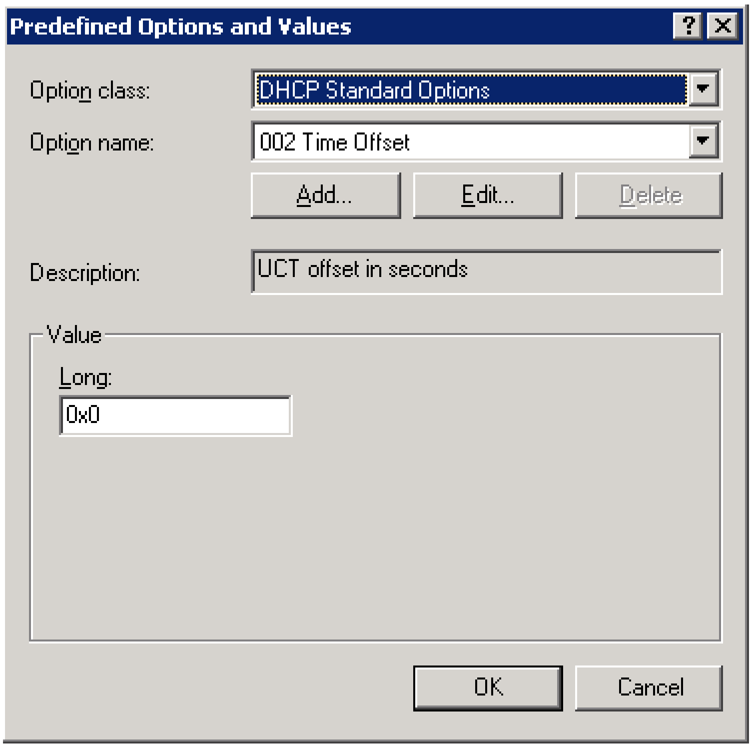
Figure 5-19 DHCP window



3. Right-click the record framed in red in Figure 5-19 and choose **Configure the Predefined Options** from the shortcut menu.

   The **Predefined Options and Values** dialog box is displayed, as shown in Figure 5-20.

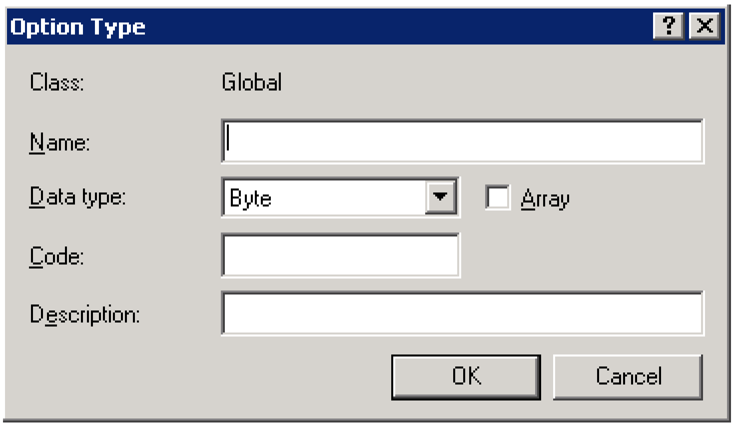
Figure 5-20 Predefined Options and Values dialog box



4. Click **Add**.

   The **Option Type** dialog box is displayed, as shown in Figure 5-21.

Figure 5-21 Option Type dialog box



5. Set related parameters according to Table 5-3.

Table 5-3 Parameter settings

Parameter	Example
Name	ip phone

Parameter	Example
Data type	String
Code	248
Description	ip phone auto provision

6. Click **OK**.

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

7. Click **OK**.

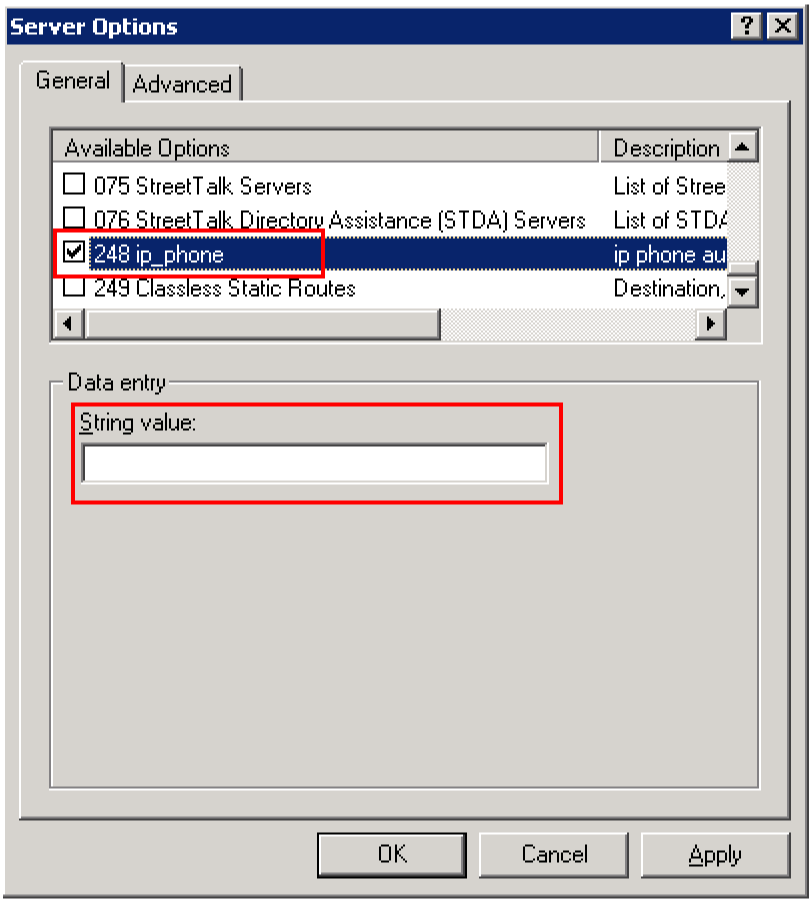
   The system returns to the **DHCP** window.

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 **248 ip_phone** check box under **Available Options**, as shown in Figure 5-22.

Figure 5-22 Server Options



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

    For example, set it to firmware=http://10.1.1.10/;config=http://10.1.1.10/config.xml.

11. Click **OK**.

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

5.9 Capturing Packets Through the Packet Capture Tool

You can connect the LAN interface of an IP phone and a computer to the same hub, and use the packet capture software such as the Sniffer, Ethereal, or Wireshark to capture packets. Alternatively, you can configure mirroring on the interface connected to the IP phone. You can locate faults quickly by analyzing the captured packets. You are advised to use the Wireshark-0.99.6a software to capture and analyze packets.

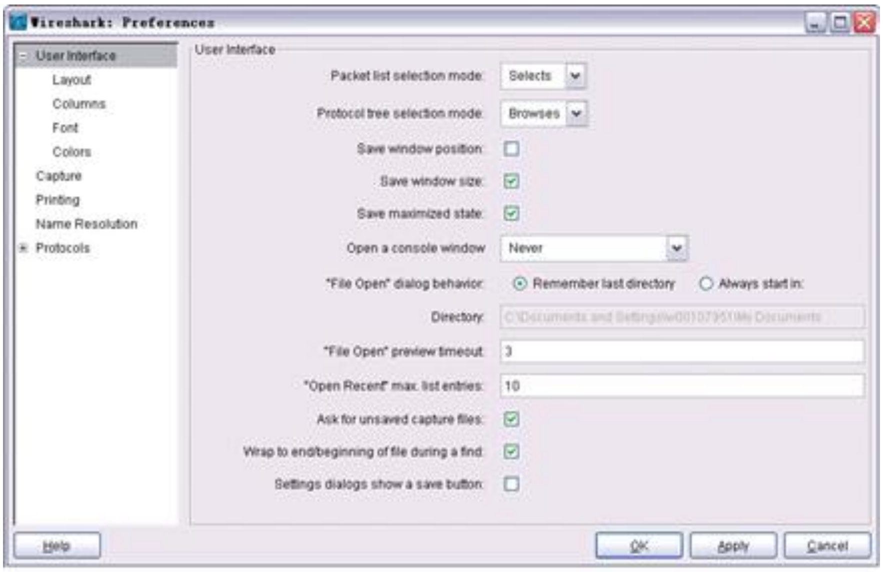
For details on how to capture and analyze packets, see the following document:

Packet Capture Setting

Generally, you do not need to perform special setting before using Wireshark to capture and analyze packets. To modify settings, do as follows:

1. Select **Preferences** on the **Edit** menu.

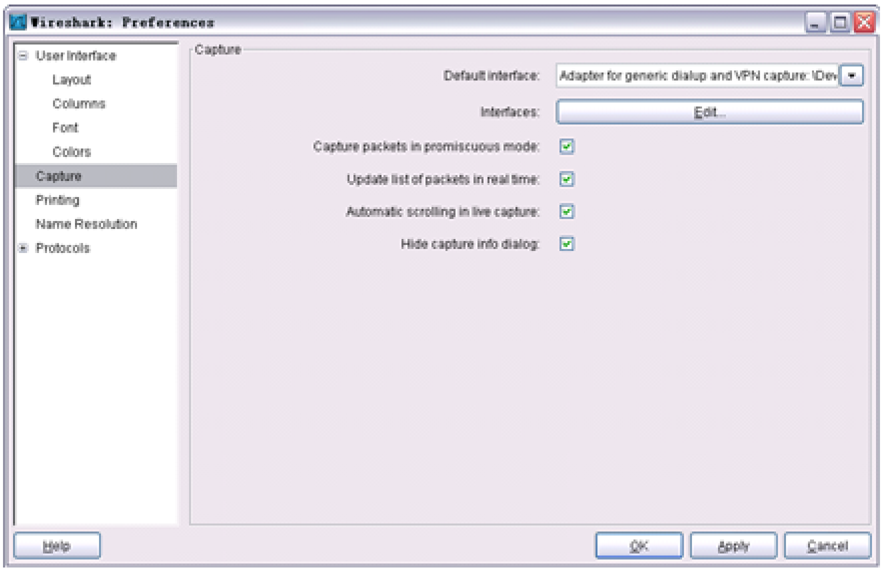
Figure 5-23 Setting parameters on the Preferences dialog box



2. Set parameters on the displayed **Preferences** dialog box according to the actual situation.
3. Choose **Capture** to modify the packet capture setting.

   On the **Capture** dialog box, you can specify the network adapter where packets need to be captured, and determine whether to capture packets in promiscuous mode. (capture all the packets passing through the network adapter, whether to update packets in real time, whether to scroll packets automatically, and whether to hide the packet capture dialog box.)

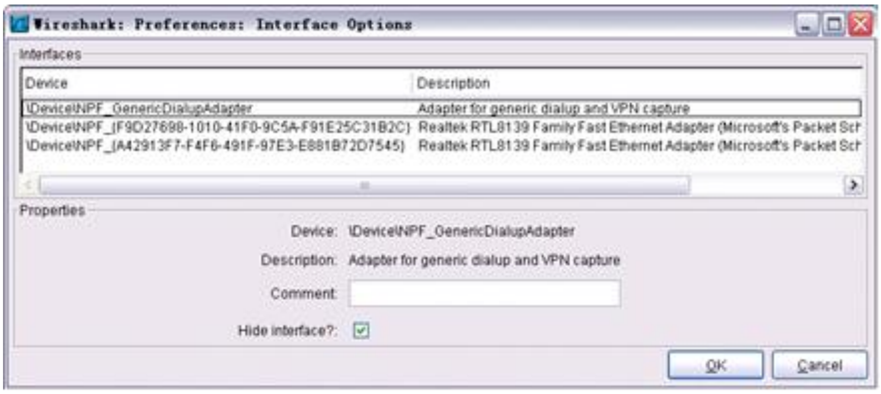
Figure 5-24 Setting on the Capture dialog box



4. Click **Edit** to change the interface properties.

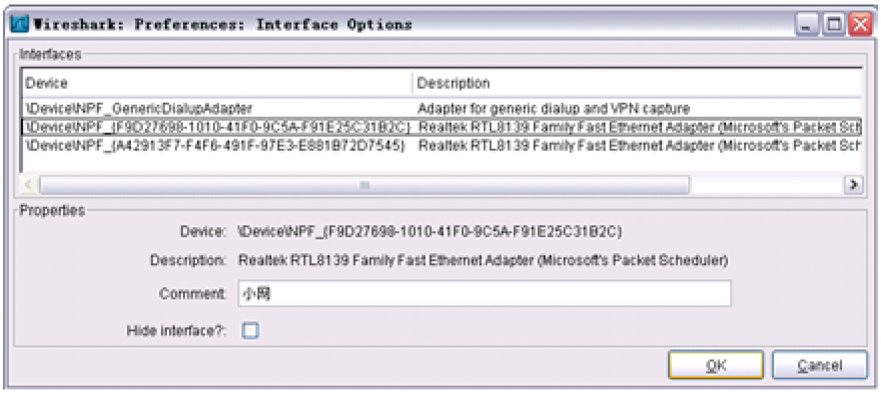
   You are advised to **hide Adapter for generic dialup and VPN capture**; otherwise, packets cannot be captured because the interface is set to the default one. Operation procedure: Choose **Adapter for generic dialup and VPN capture** and select **Hide interface**.

Figure 5-25 Setting on the Interface Options page



5. If multiple network adapters are available, you are advised to add a comment to each network adapter so that you can distinguish the network adapter where packets are captured. Operation procedure: Choose the network adapter to be modified and add the contents in the **Comment** text box.

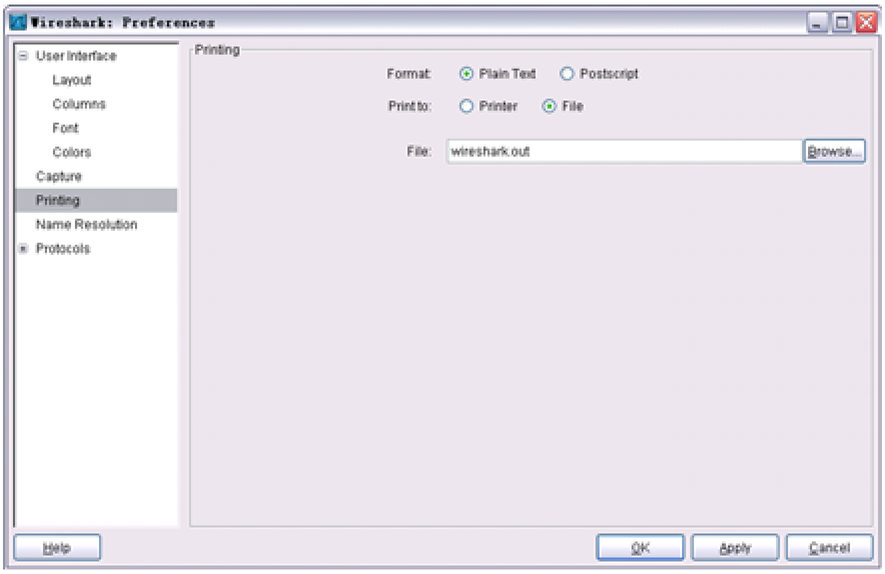
Figure 5-26 Adding contents to the Comment text box



6. Choose Printing to modify the printing setting.

   You can select **File** or **Printer** in **Print to**. The format can be plain text or postscript. Generally, the format is plain text.

Figure 5-27 Setting on the Printing page



Methods of Capturing Packets

You can use the Wireshark to start capturing packets from multiple ingresses. The details are as follows.

- Capturing Packets Directly

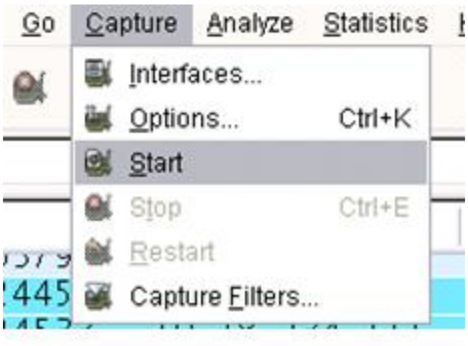
  You can start capturing packets directly. That is, you use the default setting without setting packet capture options. You can use either of the following methods:

1. Click **Start** button the toolbar to start capturing packets, as shown in Figure 5-28

Figure 5-28 Starting capturing packets through the toolbar

2. Choose **Capture** > **Start**>, as shown in Figure 5-29.

Figure 5-29 Capturing packets through the menu



- Capturing Packets by Specifying an Interface

  You need to select an interface, and then start capturing packets.

  You can set options after opening the **Capture Interfaces** dialog box. The method is as follows: Select **Interfaces** from the **Capture** menu and **open the Capture Interfaces** dialog box, as shown in Figure 5-30.

Figure 5-30 Selecting an interface for capturing packets

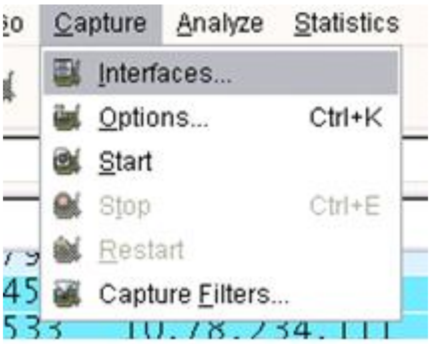
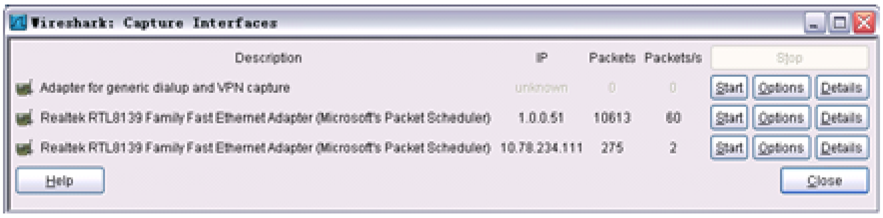


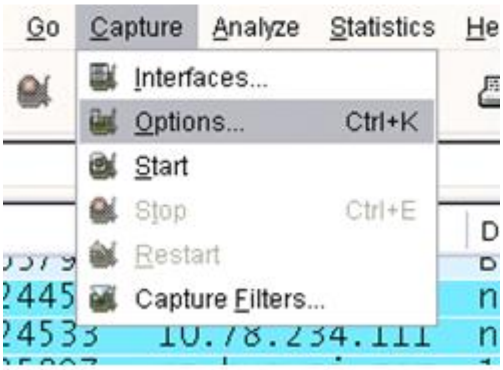
Figure 5-31 Capture Interfaces dialog box



You can start capturing packets by clicking **Start** corresponding to the interface. You can click **Options** to modify the option setting, and then start capturing packets. See the following steps.

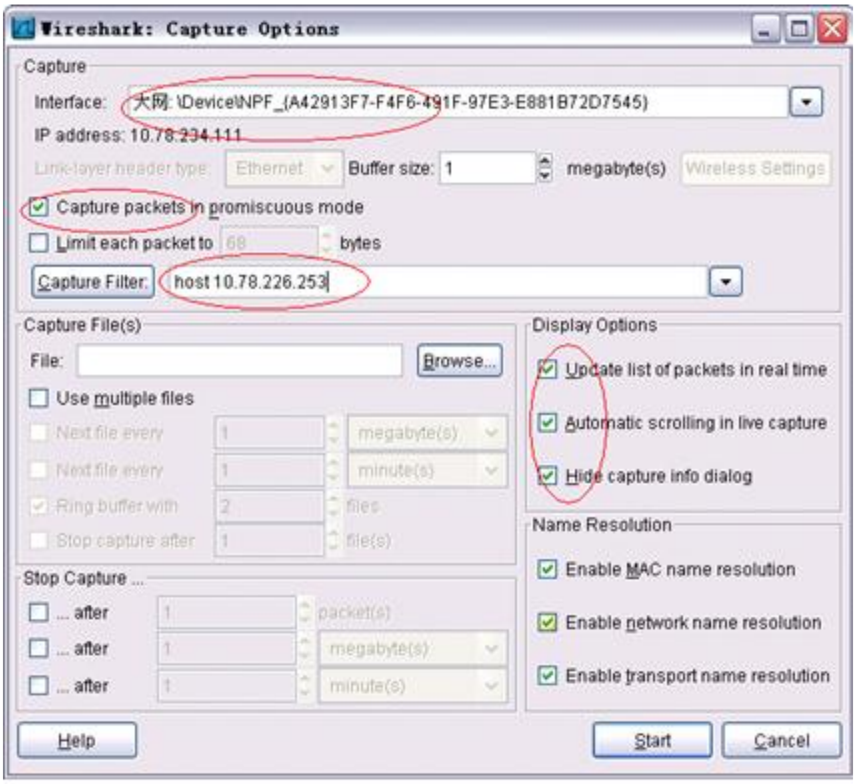
1. Set options for capturing packets.

Figure 5-32 Selecting Options



2. On the **Capture Options** dialog box, you need to select the network adapter where packets need to be captured to filter out packets. You need to capture packets in promiscuous mode and automatically updating and scrolling packets in packet capture, as shown in Figure 5-33.

Figure 5-33 Setting packet capture options



Sometimes you need to capture packets cyclically or capture packets with the fixed size (for example, capture packets of 10 M, and then stop capturing packets), or capture packets with a fixed interval (stop capturing packets after capturing packets for 10 minutes). You can set related options in **capture File(s)**.

Before capturing packets, you can filter packets. The expression used to filter packets is host<IP address>.Only the packets with the specified IP address are captured. Common expressions used to filter packets are as follows:

```
[src|dst] host <host>
ether [src|dst] host <ehost>
gateway host <host>
[src|dst] net <net>[{mask <mask>}|{len <len>}]
[tcp|udp] [src|dst] port <port>
less|greater <length>
ip|ether proto <protocol>
ether|ip broadcast|multicast
<expr>relop<expr>
```

Packet Analysis

1. Packet Filtering

   In actual applications, there is a large amount of data in packet capture. To rapidly locate the required packets, you need to use the packet filtering function.

   To filter packets, enter the expression in the **Filter** text box and click **Apply**. For example, to filter TCP packets, enter **tcp** in the **Filter** text box and click **Apply**.

Figure 5-34 Packets that are not filtered

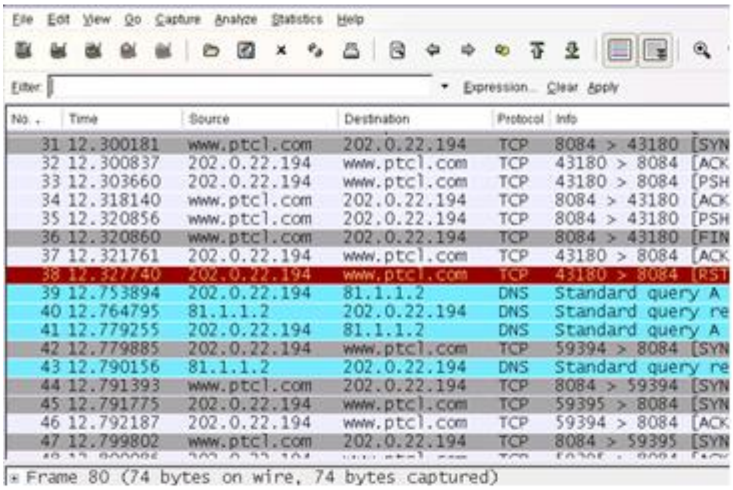
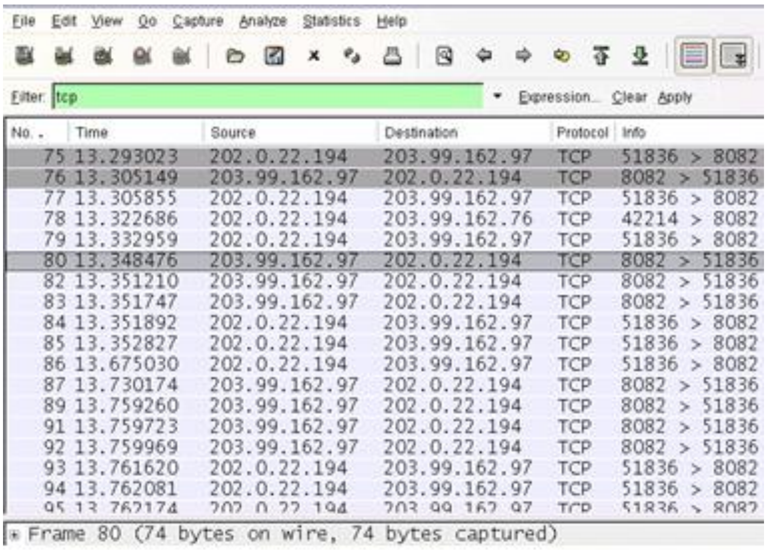


Figure 5-35 Filtered packets



In addition to entering the expression manually, you can use other shortcut methods. On the **Packet List** window, right-click the source or destination address of any packet and choose **Apply as Filter** > **Selected**, as shown in Figure 5-36.Figure 5-37 shows the filtering effect.

Figure 5-36 Filtering packets (1)

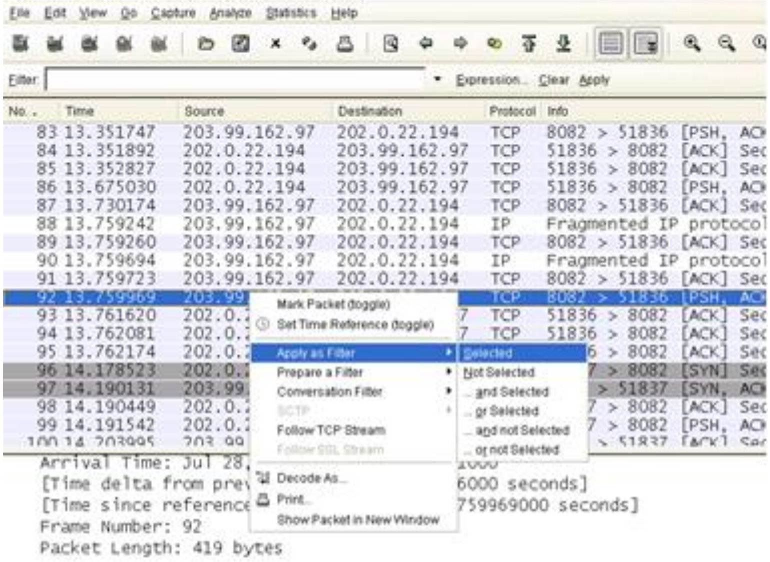
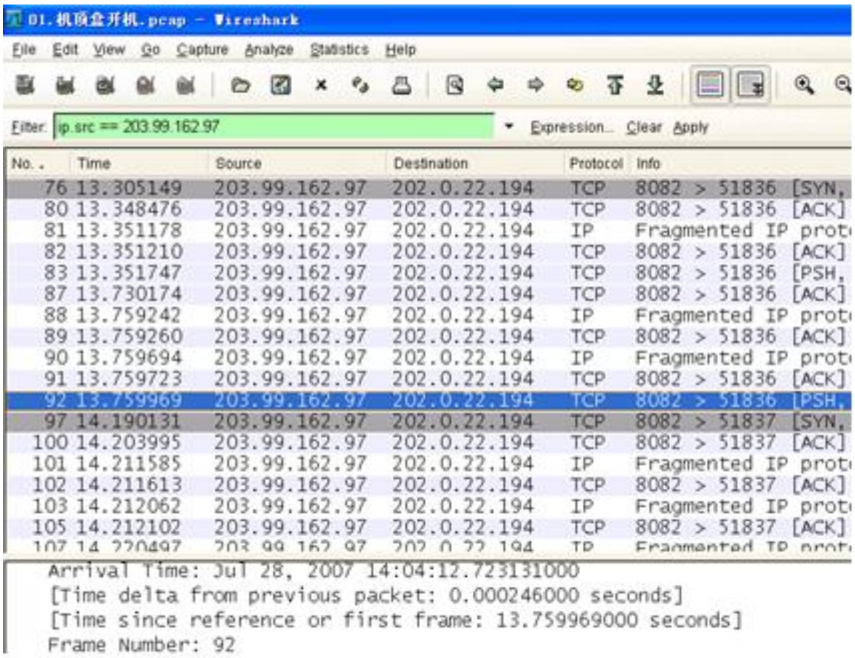


Figure 5-37 Filtering packets (2)



This filtering method is simple. In addition to the **Packet List** window, you can use the similar method on the **Packet Details** window.

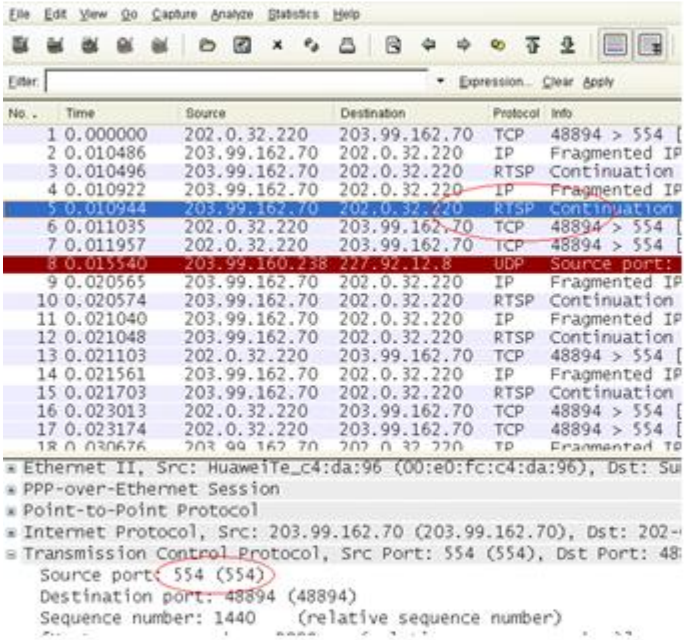
2. Decoding

Generally, the Wireshark uses the port number to parse application layer protocols. If applications do not use standard port numbers or default port numbers of application layer protocols, the Wireshark cannot parse the application layer protocols. Instead, it can parse only transport layer protocols (TCP or UDP).

For example, the Web application using HTTP uses port 80 as the default port number. If an application uses port 80, the application layer HTTP in the captured packets is parsed by the Wireshark. Otherwise, TCP in the packets is parsed.

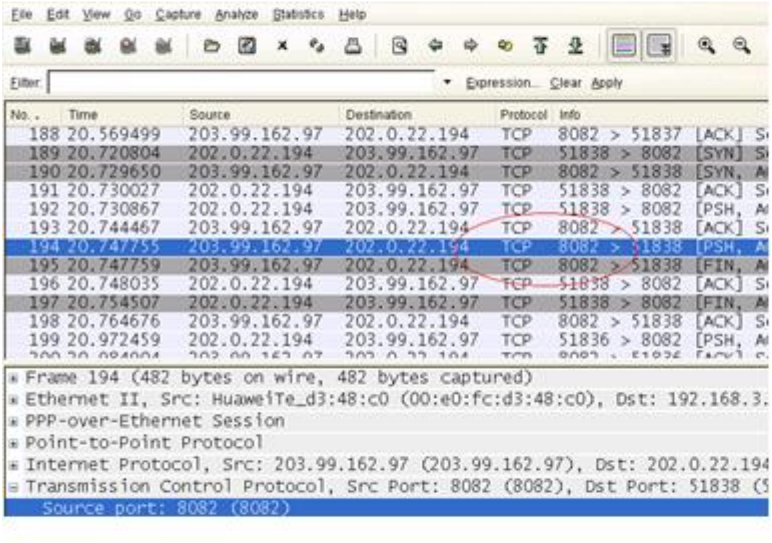
The default port of the application that uses RTSP for communication is port 554; therefore; the packets containing port 554 are RSTP packets, as shown in .

Figure 5-38 Parsing RTSP packets



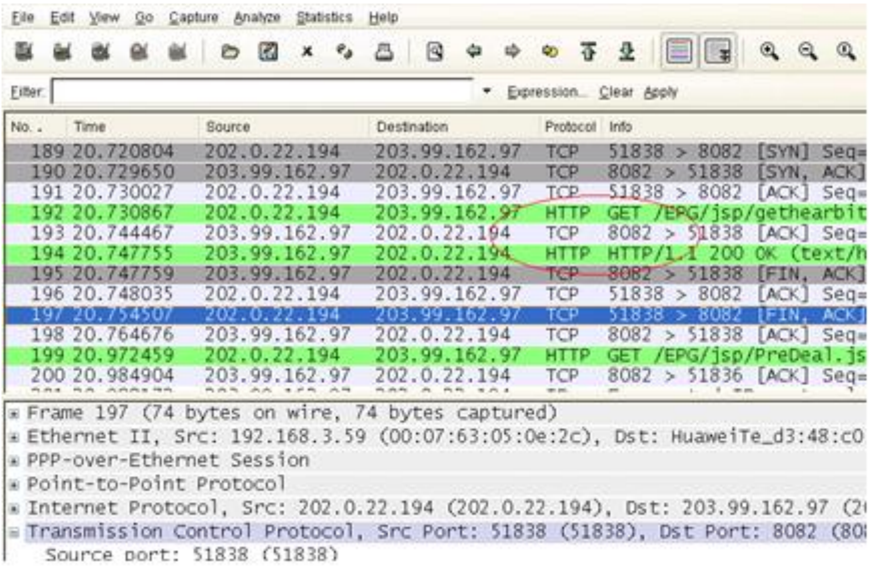
If the Web application does not use port 80, for example, port 8082, HTTP cannot be parsed. It is difficult to analyze the captured packets.

Figure 5-39 Packet whose HTTP is not parsed



To analyze packets easily, you can use the encoding function of the Wireshark to parse the HTTP protocol. The packet whose HTTP is parsed is as follows.

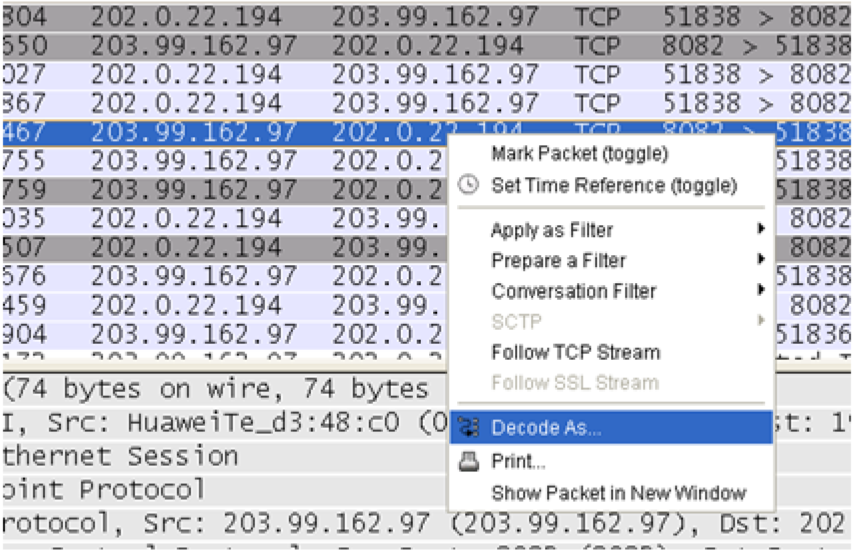
Figure 5-40 Packet whose HTTP is parsed



The steps are as follows:

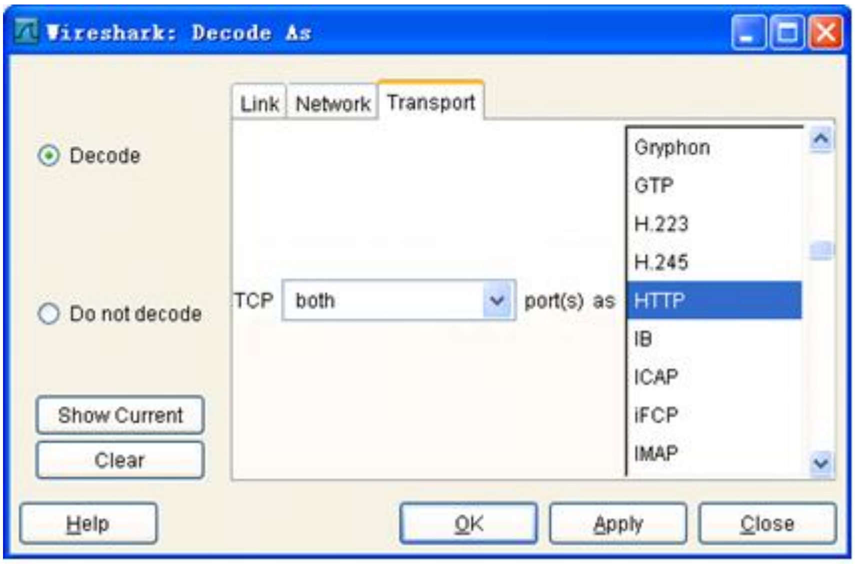
a. Right-click any packet containing port 8082 and select **Decode As…**.

Figure 5-41 Parsing packet a through the non-standard HTTP port



b. On the displayed **Decode As** dialog box, click **Decode**, select **both** in **TCP** on the **Transport** page, and set the parsing protocol to **HTTP**.

Figure 5-42 Parsing packet b through the standard HTTP port



c. After the options are set, click **OK**.

To remove the customized decoding mode, click **Do not decode** on the **Decode As** dialog box.

3. Follow TCP Stream

To analyze data flows based on TCP, you can use the Follow TCP Stream function of the Wireshark. This function allows you to analyze the exchange process of data flows.

On the **Packet List** window, choose any packet and right-click to choose **Follow TCP streams**, as shown in Figure 5-43.

Figure 5-43 Follow TCP Stream

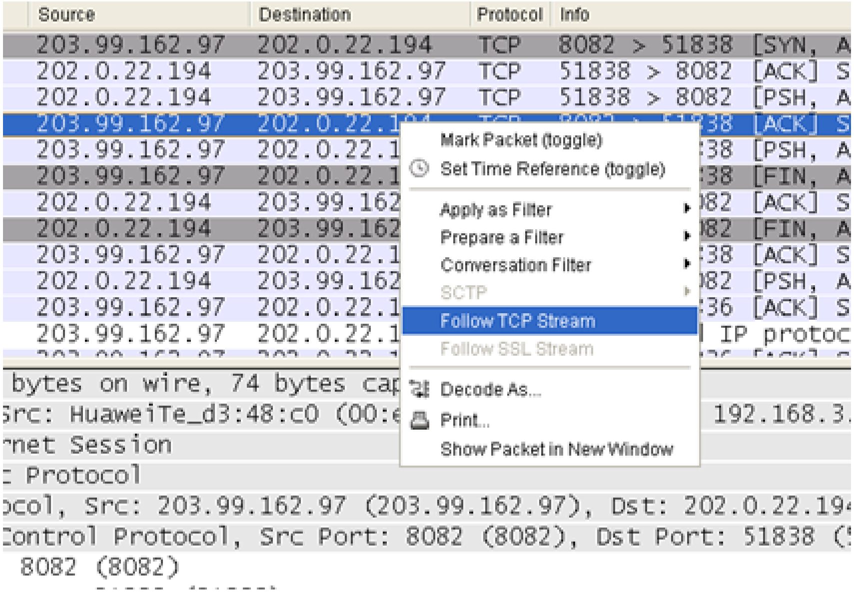
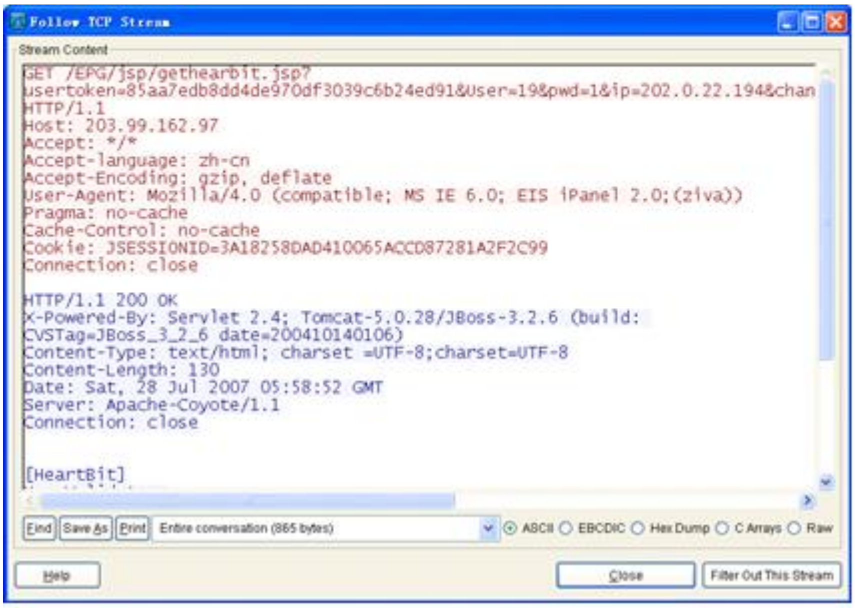


Figure 5-44shows the operation result from which you can view the detailed exchange process and data.

Figure 5-44 Operation result



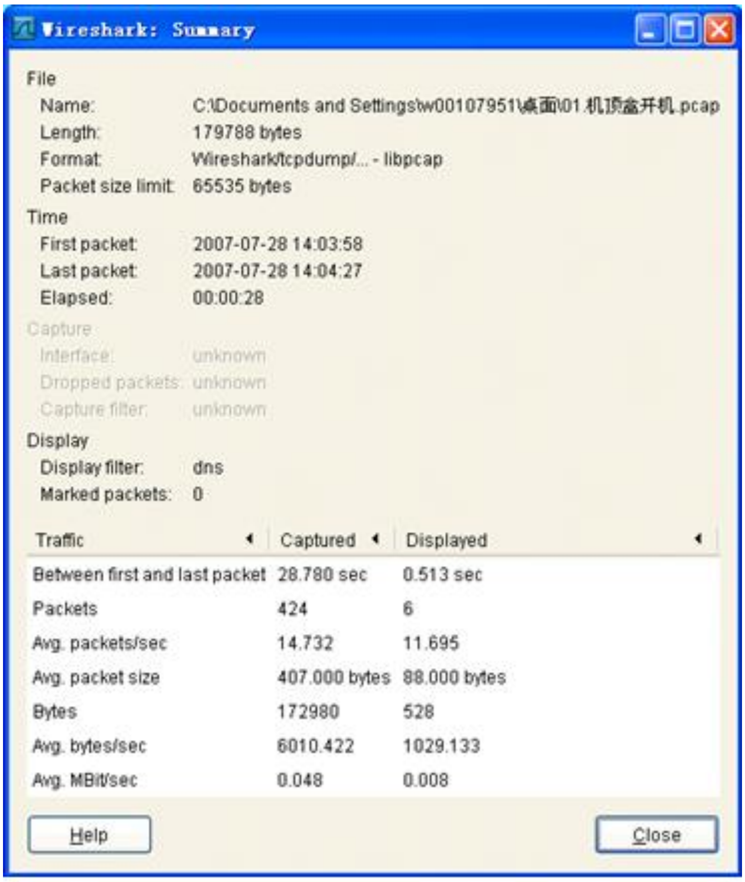
Statistics Function

- Summary Information

  The Wireshark provides powerful statistics functions, including the statistics on the summary of the traffic.

  Choose **Statistics** > **Summary**, and you can view the summary of the traffic. On the **Summary** page, the statistics on all the packets can be displayed or the statistics on the packets matching a filtering condition can be displayed.

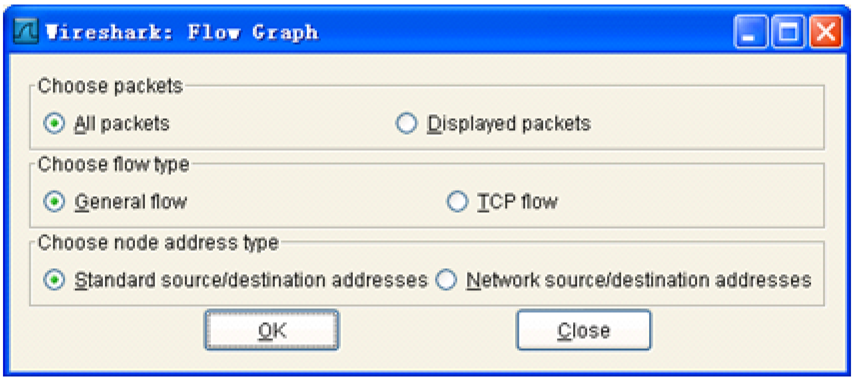
Figure 5-45 Statistics function



- Call Process

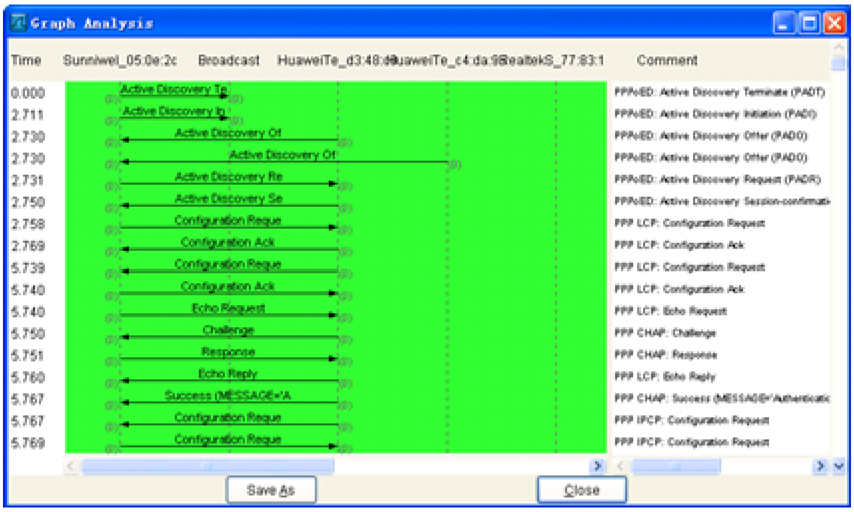
  When using the Wireshark to analyze packets, you can choose **Statistics** > **Flow Graph** to learn the exchange process of each component.

Figure 5-46 Flow Graph



After choosing **Flow Graph**, a dialog box is displayed. After performing the setting as required, click **OK** to display the **Graph Analysis** dialog box.

Figure 5-47 Graph Analysis dialog box



To use the preceding figure in other documents, you can copy the screenshot or click **Save as** to save the figure as the flowchart in text format. The format is as follows:

```
|Time     | Sunniwel_05:0e:2c | Broadcast   | HuaweiTe_d3:48:c0 | HuaweiTe_c4:da:96
|
|0.000    |        Active Discovery Te     |                 |                |
|         |(0)     ------------------>  (0)|                 |                |
|2.711    |        Active Discovery In     |                 |                |
|         |(0)     ------------------>  (0)|                 |                |
|2.730    |        Active Discovery Of     |                 |                |
|         |(0)     <--------------------------------  (0)      |                |
|2.730    |        Active Discovery Of     |                 |                |
|         |(0)     <---------------------------------------------------  (0)
|
|2.731    |        Active Discovery Re     |                 |                |
|         |(0)     -------------------------------->  (0)      |                |
```

```
|2.750    |        Active Discovery Se    |                |                |
|        |(0)     <--------------------------------  (0)     |                |
|2.758    |        Configuration Reque    |                |                |
|        |(0)     -------------------------------->  (0)     |                |
|2.769    |        Configuration Ack      |                |                |
|        |(0)     <--------------------------------  (0)     |                |
|5.739    |        Configuration Reque    |                |                |
|        |(0)     <--------------------------------  (0)     |                |
|5.740    |        Configuration Ack      |                |                |
|        |(0)     -------------------------------->  (0)     |                |
|5.740    |        Echo Request          |                |                |
|        |(0)     -------------------------------->  (0)     |                |
|5.750    |        Challenge |           |                |                |
|        |(0)     <--------------------------------  (0)     |                |
|5.751    |        Response  |           |                |                |
|        |(0)     -------------------------------->  (0)     |                |
|5.760    |        Echo Reply|           |                |                |
|        |(0)     <--------------------------------  (0)     |                |
|5.767    |        Success (MESSAGE='A    |                |                |
```

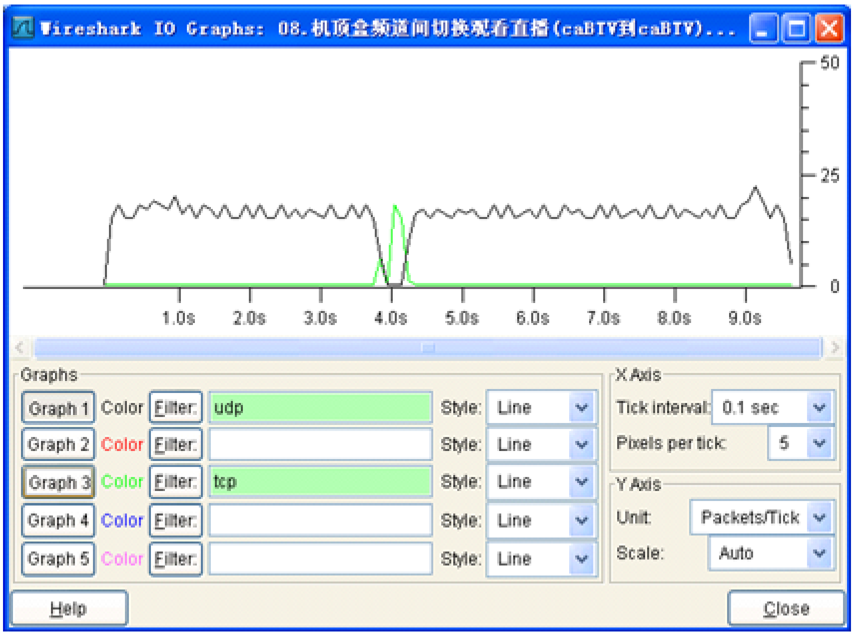
- Analyzing Burst Traffic

  You can use the Wireshark to analyze the burst traffic. The steps are as follows:

1. Choose **Statistics** > **IO Graphs** to display the **IO Graphs** dialog box.
2. Adjust the values of parameters in **X Axis** and **Y Axis**.In **Graphs**, the five columns indicate the modes of displaying the traffic figure according to five filtering conditions. You can select one or multiple modes.

   For example, set the filtering condition to udp in column 1 and click **Graph1**. The UDP traffic is displayed in black curve. Set the filtering condition to tcp in column 3 and click **Graph3**. The TCP traffic is displayed in green curve.

Figure 5-48 Analysis on burst traffic

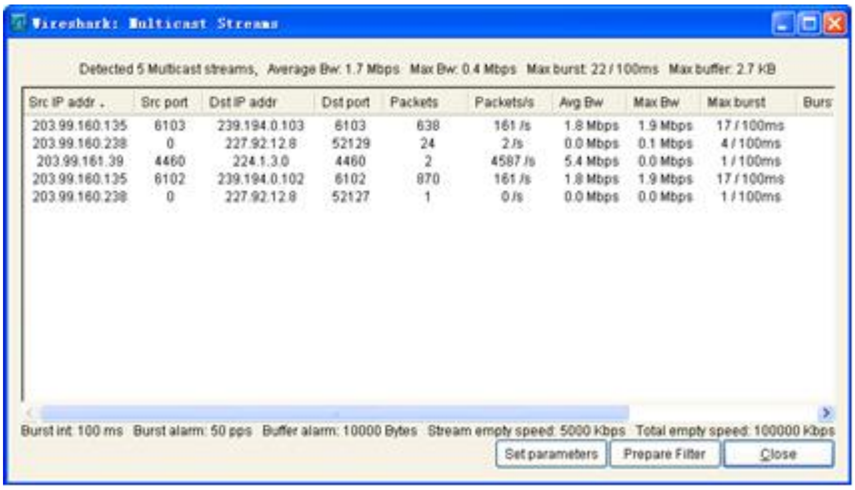


- Multicast Traffic

  You can use the Wireshark to view the statistics on multicast flows among the captured packets, including the source address, source port, multicast address, multicast port, and average traffic.

  Operation procedure: Choose **Statistics** > **Multicast Streams**, as shown in Figure 5-49.

Figure 5-49 Analysis on multicast traffic



File Exporting

You can use the Wireshark to export the packet analysis result to other file formats.

For example, to display the hierarchical structure of a packet in a Word document, you can export the analysis result on the **Packet Detail** window to the text format. Then paste the contents to the Word document.

The Wireshark can export packets in the following formats:

- Plain text: The document can contain the contents of the **Packet List**, **Packet Details**, or **Packet Bytes** window, which are analyzed by the Wireshark.
- Comma Separated Values Summary (CSV): The document contains only the summary of packets on the **Packet List** window, without the hierarchical structure of packets and packet contents in hexadecimal notation on the **Packet Details** window.
- The documents in XML Packet Summary (PSML) and XML Packet Detail (PDML) formats are documents in .xml format. Their difference is as follows:
  - The document in PSML format contains the contents on the **Packet List** window of the Wireshark, that is, summary of packets.
  - The document in PDML format contains the contents on the **Packet Detail** window of the Wireshark, that is, details on packets.

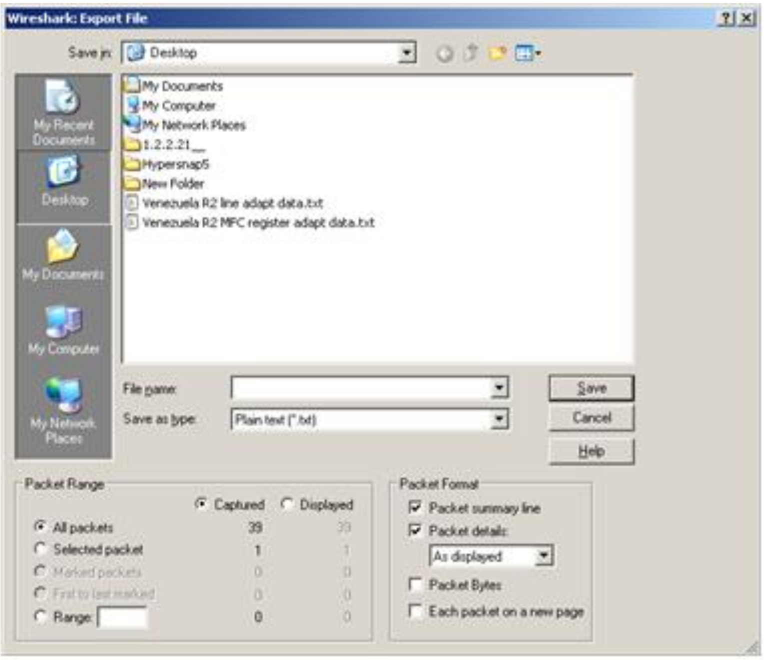
The file can be exported in two ways, which are described as follows.

- Exporting Files Through Export

  The steps are as follows:

1. Choose **Export** > **File** to display the Export File dialog box, as shown in Figure 5-50.

Figure 5-50 Export File dialog box



2. Select the format of saving files (.txt, .ps, .CSV, PSML, PDML) in **Save as type**.

3. Enter the file name to be saved.
4. Select the output packet range in **Packet Range**.
5. Select the output packet format in **Packet Format**.

CAUTION

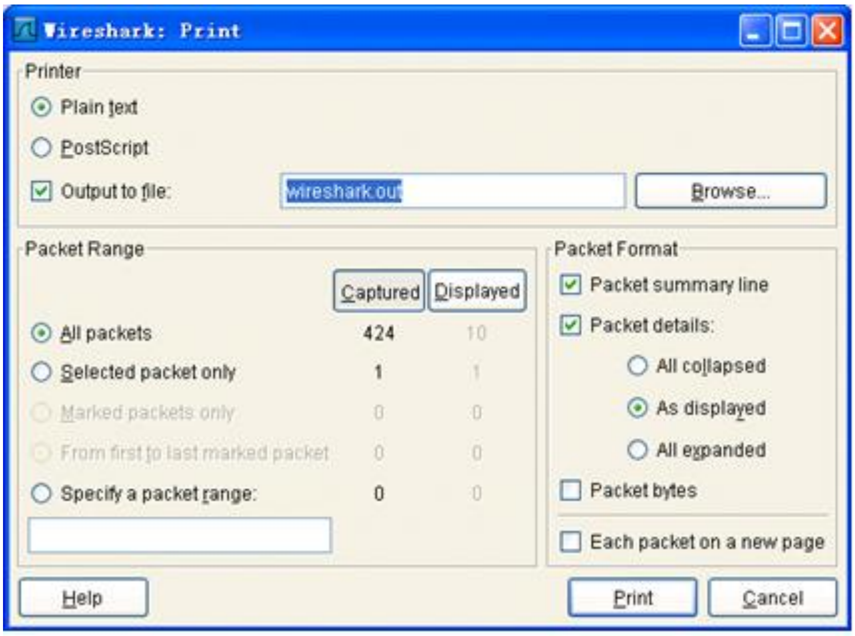
When entering the file name to be saved, you must add the extension name. This is because the Wireshark does not add the extension name when exporting files. If the file in Plain text format is exported, you must add the extension name **.txt**. If the file in Post Script format is exported, you must add the extension name **.ps**. If the file in CSV format is exported, you must add the extension name **.csv**. If the file in PSML or PDML format is exported, you must add the extension name **.xml**. This is because the extension name PSML or PDML cannot be recognized.

- Exporting Files Through Print

  Exporting files through **Print** is similar to exporting files through **Export**, but there is a slight difference. The steps are as follows:

1. Choose **File** > **Print** to display the Print dialog box, as shown in Figure 5-51.

Figure 5-51 Print dialog box



2. Select the output packet format in **Printer**.
3. Select **Output to file** and enter the file name to be saved in the text box. Adjust the extension name according to the actual situation.
4. The settings in **Packet Range** and **Packet Format** are the same as those in Exporting Files Through Export.

CAUTION

You can only export files in Plain text or Post Script format through this method.