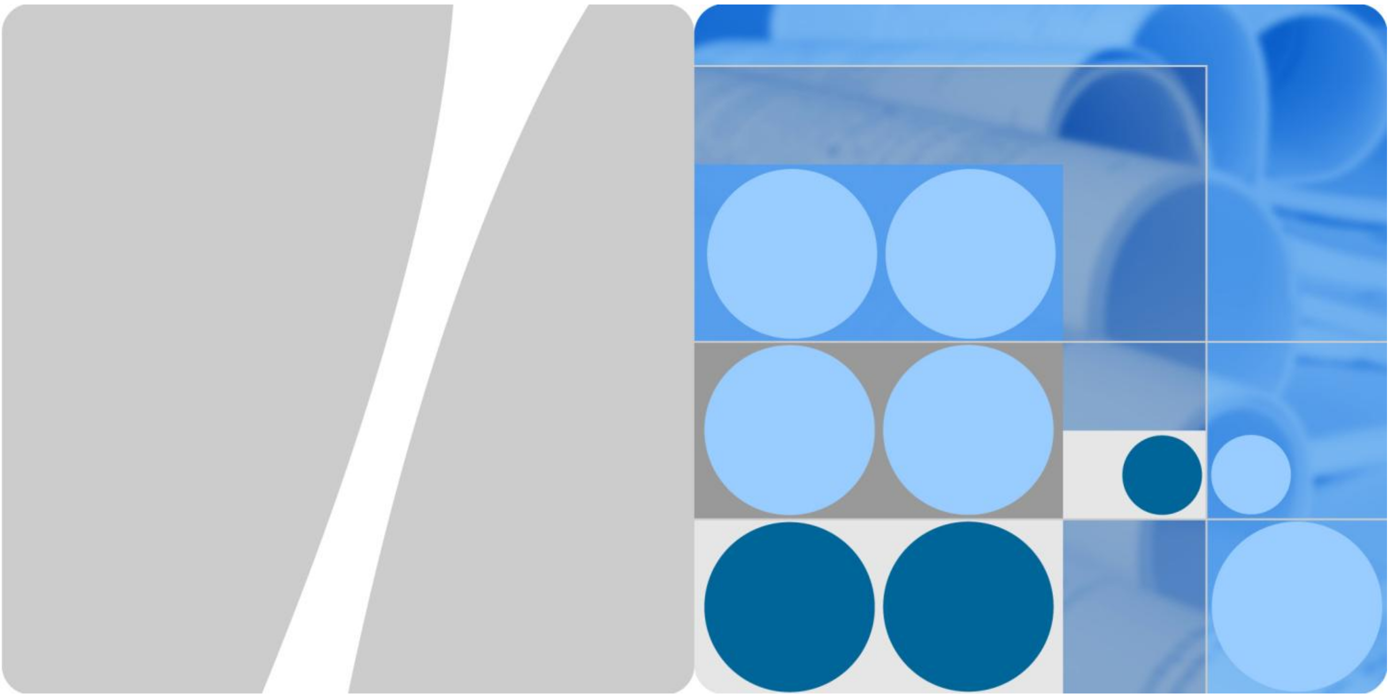


Huawei IP Phone eSpace 6805&6810&6830&6850&6870 V100R001C02SPC100

Administrator Guide

Issue	**01**
Date	**2012-06-20**

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: http://www.huawei.com

Email: support@huawei.com

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 (2012-06-20)

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

- If the network is in a good condition, G.711 A-law/μ-law is recommended to ensure high voice quality.
- If the network is not in a good condition, G.729AB or G.723.1 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

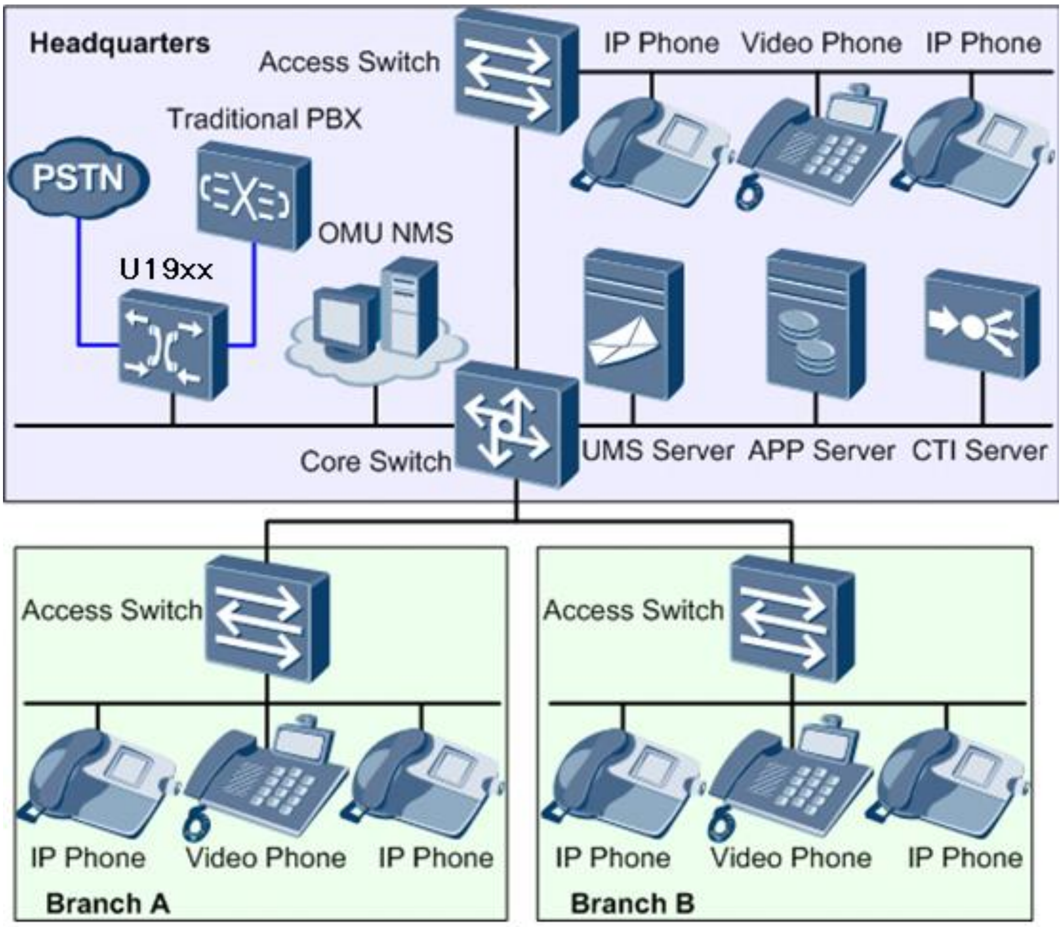
Servers (ACS). It includes both a safe auto configuration and the control of other CPE management functions within an integrated framework.

After IP phones are connected to the ACS through TR-069, you can reboot the IP phone on the ACS.

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:

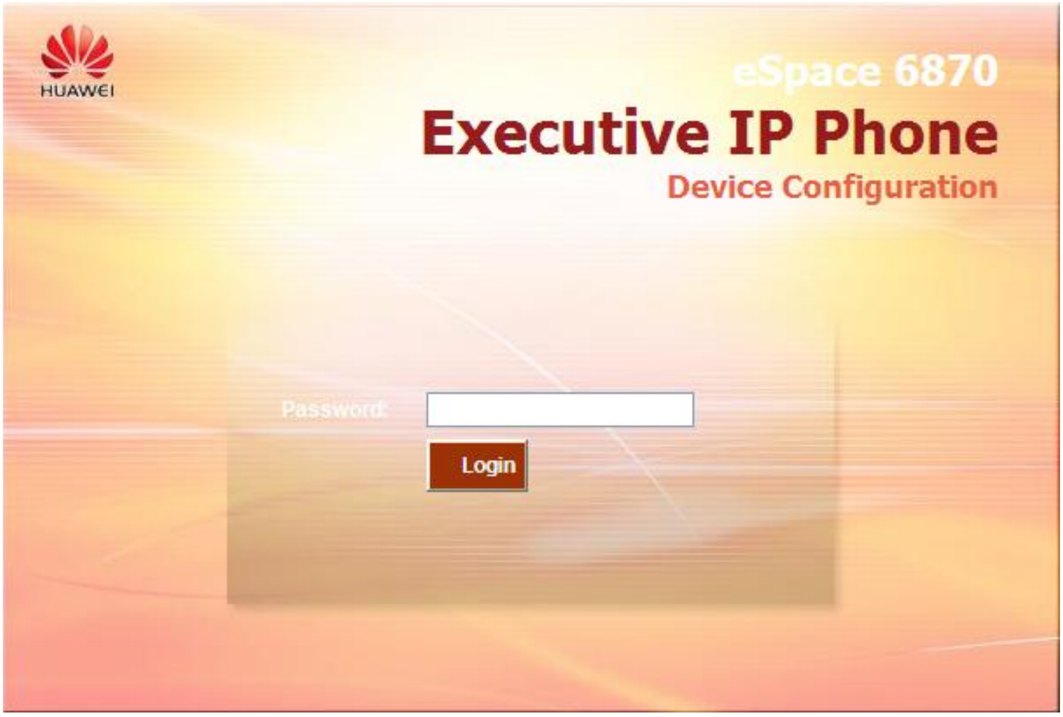
Connect the computer to the same hub or switch as the phone is connected to. In absence of a hub/switch (or free ports on the hub/switch), connect the computer directly to the phone by using the PC port on the phone. Make sure that the phone is powered on and displays the IP address.

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



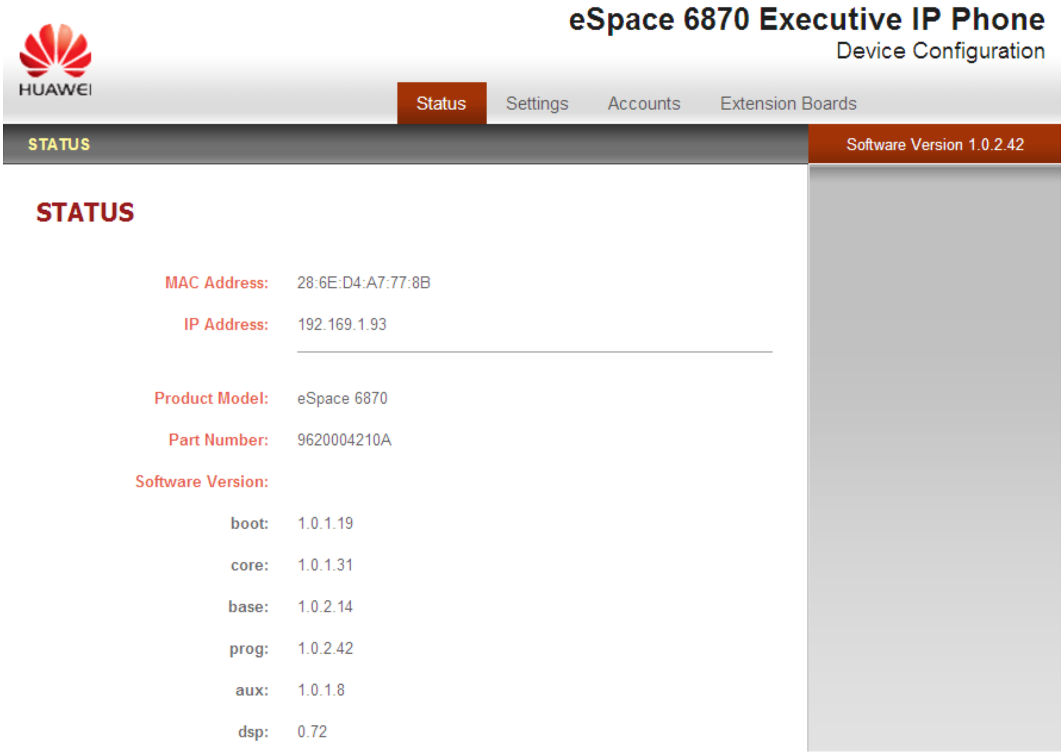
NOTE

- 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



eSpace 6870 Executive IP Phone
Device Configuration

STATUS

Software Version 1.0.2.42

STATUS

MAC Address: 28:6E:D4:A7:77:8B
IP Address: 192.169.1.93

Product Model: eSpace 6870
Part Number: 9620004210A
Software Version:
boot: 1.0.1.19
core: 1.0.1.31
base: 1.0.2.14
prog: 1.0.2.42
aux: 1.0.1.8
dsp: 0.72

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

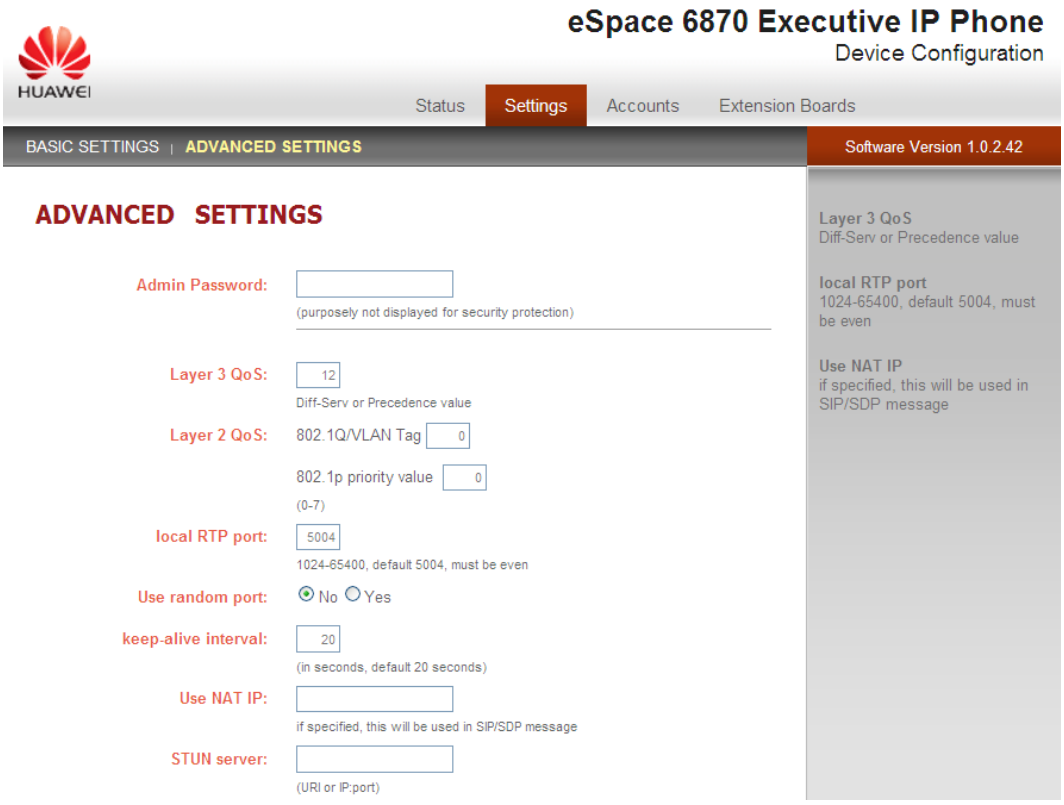
For details of Basic Configuration, see *Huawei IP Phone eSpace 68XX UserManual*, **XX** represents different models.

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)



eSpace 6870 Executive IP Phone
Device Configuration

Software Version 1.0.2.42

ADVANCED SETTINGS

Admin Password:
(purposely not displayed for security protection)

Layer 3 QoS: 12
Diff-Serv or Precedence value

Layer 2 QoS: 802.1Q/VLAN Tag 0
802.1p priority value 0
(0-7)

local RTP port: 5004
1024-65400, default 5004, must be even

Use random port: ● No ○ Yes

keep-alive interval: 20
(in seconds, default 20 seconds)

Use NAT IP:
if specified, this will be used in SIP/SDP message

STUN server:
(URI or IP:port)

Layer 3 QoS
Diff-Serv or Precedence value

local RTP port
1024-65400, default 5004, must be even

Use NAT IP
if specified, this will be used in SIP/SDP message

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.
HTTP/HTTPS Password	If the HTTP or HTTPS firmware or configuration server adopts the user authentication mode, set this parameter to the authorized password.

Field	Description
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 For example, http://10.10.10.1:9090. • http://domain name:9090

Field	Description
	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 phonebook through keypad will be overwritten.
LDAP	This function is not supported currently. By default, this parameter is left

Field	Description
Directory	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.
NTP Server	URI or IP address of the NTP server, which is used to display the current date and time on the phone.

Field	Description
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 Conference	The default value is **No**. If the parameter is set to **Yes**, the three-party conference function of eSpace 6870 is disabled.
Enable MPK	The default value is **No**. If the parameter is set to **Yes**, multi-purpose keys

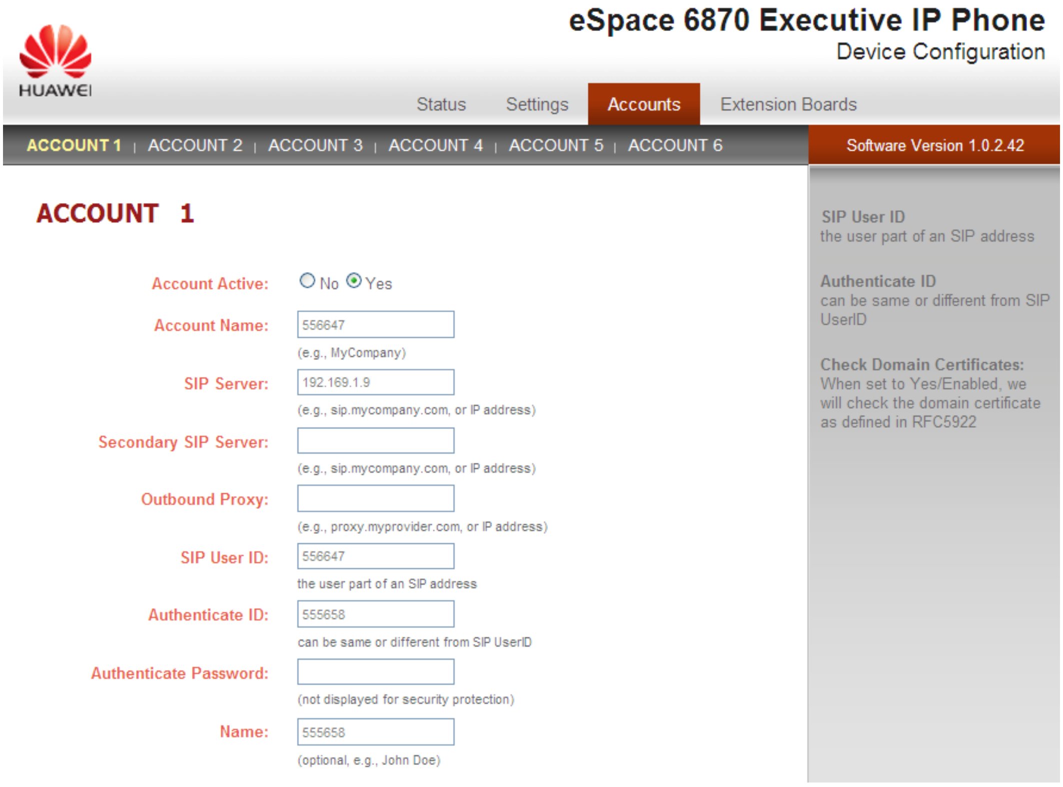
Field	Description
Sending DTMF	can be set as DTMF.
Disable DND	The default value is **No**. If the parameter is set to **Yes**, the DND button on keypad as DND shortcut is disabled.
Disable Transfer	The default value is **No**. If the parameter is set to **Yes**, the transfer function is disabled.
Configuration 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)



eSpace 6870 Executive IP Phone

Device Configuration

ACCOUNT 1 | ACCOUNT 2 | ACCOUNT 3 | ACCOUNT 4 | ACCOUNT 5 | ACCOUNT 6

Software Version 1.0.2.42

ACCOUNT 1

Account Active: ○ No ● Yes

Account Name: 556647
(e.g., MyCompany)

SIP Server: 192.169.1.9
(e.g., sip.mycompany.com, or IP address)

Secondary SIP Server:
(e.g., sip.mycompany.com, or IP address)

Outbound Proxy:
(e.g., proxy.myprovider.com, or IP address)

SIP User ID: 556647
the user part of an SIP address

Authenticate ID: 555658
can be same or different from SIP UserID

Authenticate Password:
(not displayed for security protection)

Name: 555658
(optional, e.g., John Doe)

SIP User ID
the user part of an SIP address

Authenticate ID
can be same or different from SIP UserID

Check Domain Certificates:
When set to Yes/Enabled, we will check the domain certificate as defined in RFC5922

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. It is used for the firewall or NAT penetration in different network

Field	Description
	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 Failure Retry Wait	The default value is **20**. Configure the option to allow resending registration packet once the registration fails due to multiple possible

Field	Description
Time	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.
PUBLISH for	The default value is **No**. If the parameter is enabled, the SIP server

Field	Description
Presence	must support the Presence function before the function works.
Proxy-Require	The SIP extension informs the SIP server that the unit is behind the NAT/firewall.
Voice Mail UserID	When this option is configured, the user can access messages by pressing MSG. This ID is the VM portal access number.
Send DTMF	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
Early Dial	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.
Dial Plan Prefix	Set the prefix added to each dialed number. This prefix string is added to each dialed number
Dial Plan	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.
BLF Call-pickup Prefix	The default value is ******. This prefix is used when answering call with BLF event calls.

Field	Description
Delayed Call Forward Wait Time	This parameter adjusts the time delay before calls are forwarded. The default value is **20**. 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.

Field	Description
	Three customer ring tones: When this option is selected, incoming calls corresponding to designated accounts will play the selected ring 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

Field	Description
	connected using SRTP or not.
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.723.1 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.723.1 voice frame contains 30 ms of audio. Similarly, if this parameter is set to **2** and the first codec is G.729AB, G.711 A-law/μ-law 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.
G723 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:

Field	Description
	• The iLBC audio CODEC frame size is 30 ms in the case of 13.3 kbit/s. • 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.	

2. Click **Yes** for **Account Active** to activate the account.
3. Enter the IP address of the registration server in the **SIP Server** text box.
4. Enter the account ID of the SIP user in the **SIP User ID** text box.
5. If the SIP server has authentication information, enter the authentication ID and password in the **Authenticate ID** and **Authenticate Password** text boxes.
6. 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 eSpace U19xx and the called IP phone. If the version of the eSpace U19xx is V100R001C03 or later and the called IP phone is an SIP phone, the name can be displayed.
7. 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 eSpace U19xx.
8. 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.
9. 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.
10. Click **Update** to save the configuration, and click **Reboot** to restart the IP phone to make the configuration take effect.
11. 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

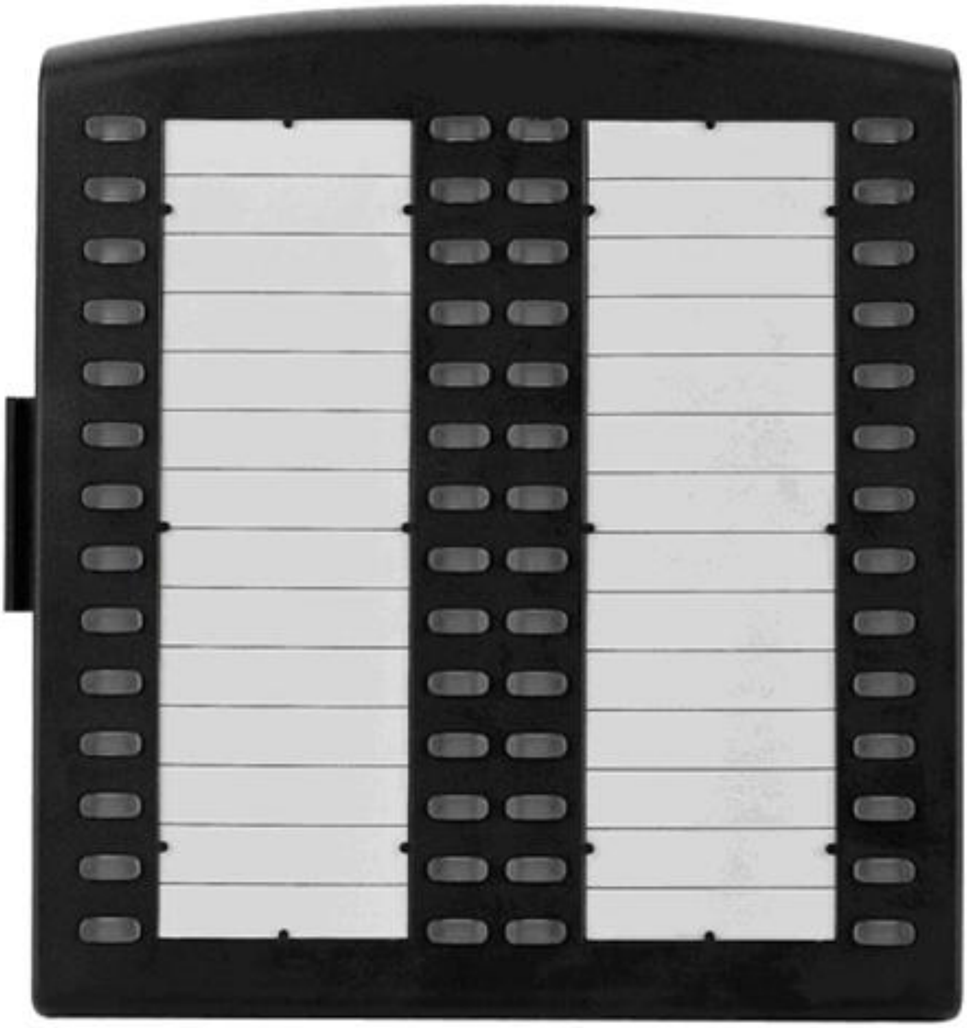
Only the first three parameters are mandatory. You are recommended not to change the parameter values unless otherwise required.

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

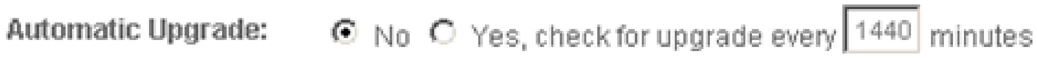
- Ensure the power supply of an IP phone during the upgrade. Otherwise, result in upgrade failed.
- The file lists contained in the programs for software upgrade and new installation are the same. Use the compressed package for upgrade. Upgrade the software after decompressing the package in the actual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

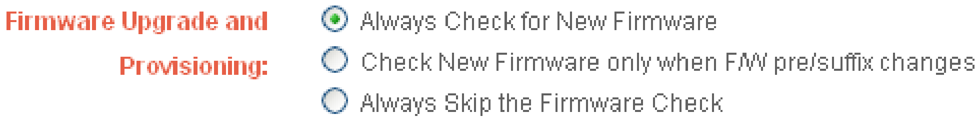
Figure 2-6 Set Automatic Upgrade



Automatic Upgrade: ● No ○ Yes, check for upgrade every 1440 minutes

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

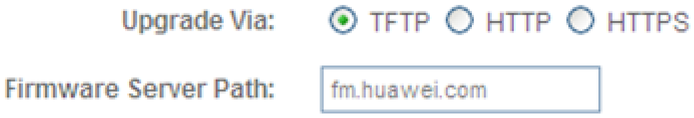
Figure 2-7 Firmware Upgrade and Provisioning



Firmware Upgrade and Provisioning: ● Always Check for New Firmware ○ Check New Firmware only when F/W pre/suffix changes ○ Always Skip the Firmware Check

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



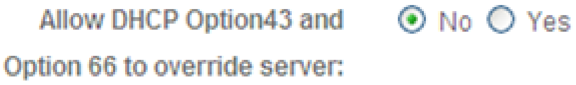
Upgrade Via: ● TFTP ○ HTTP ○ HTTPS

Firmware Server Path: fm.huawei.com

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



Allow DHCP Option43 and Option 66 to override server: ● No ○ Yes

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

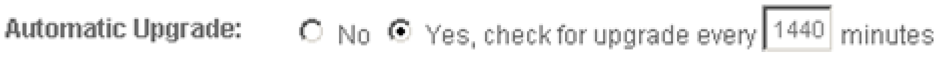
Automatic Upgrade

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.

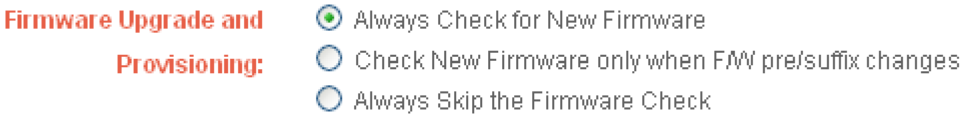
Figure 2-10 Automatic Upgrade



Automatic Upgrade: ○ No ● Yes, check for upgrade every 1440 minutes

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

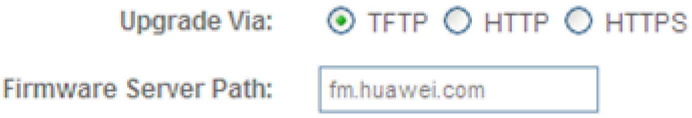
Figure 2-11 Firmware Upgrade and Provisioning



Firmware Upgrade and Provisioning:
● Always Check for New Firmware
○ Check New Firmware only when F/W pre/suffix changes
○ Always Skip the Firmware Check

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

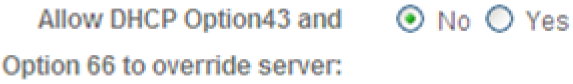


Upgrade Via: ● TFTP ○ HTTP ○ HTTPS
Firmware Server Path: fm.huawei.com

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



Allow DHCP Option43 and Option 66 to override server: ● No ○ Yes

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.

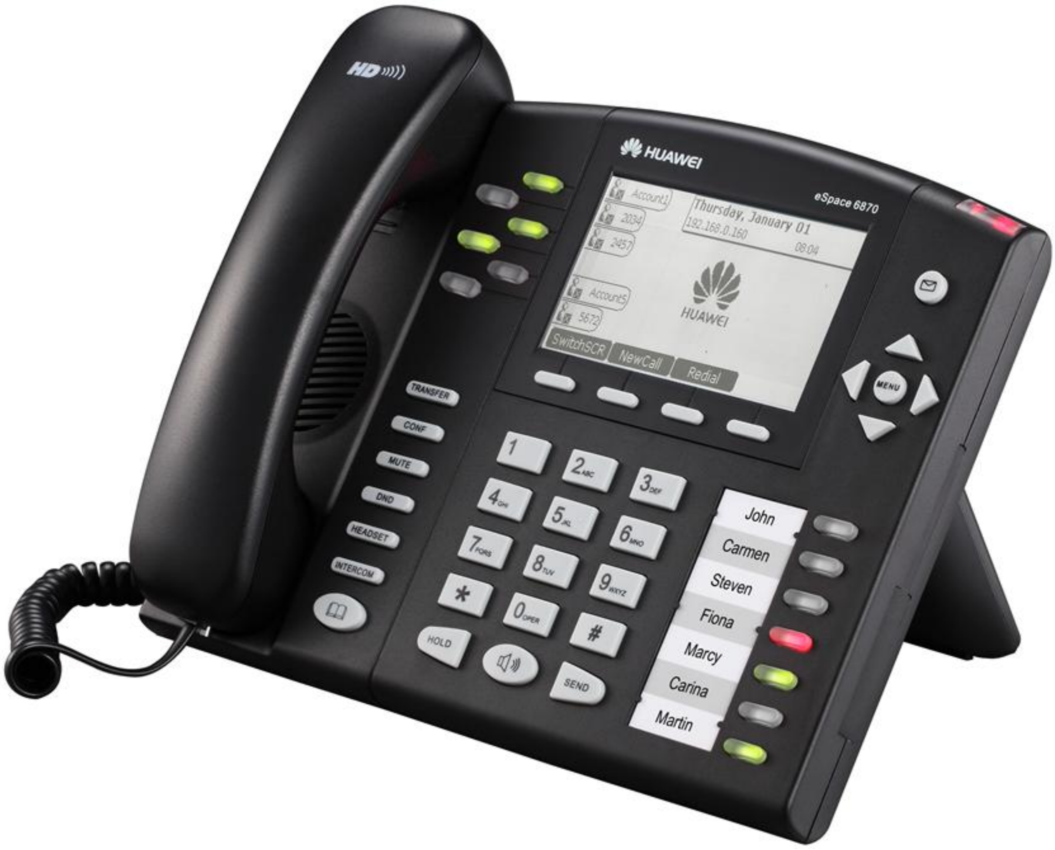
   ----End

2.2.8 Common Operation Configurations

Configuring Multi-Purpose Keys on an IP Phone

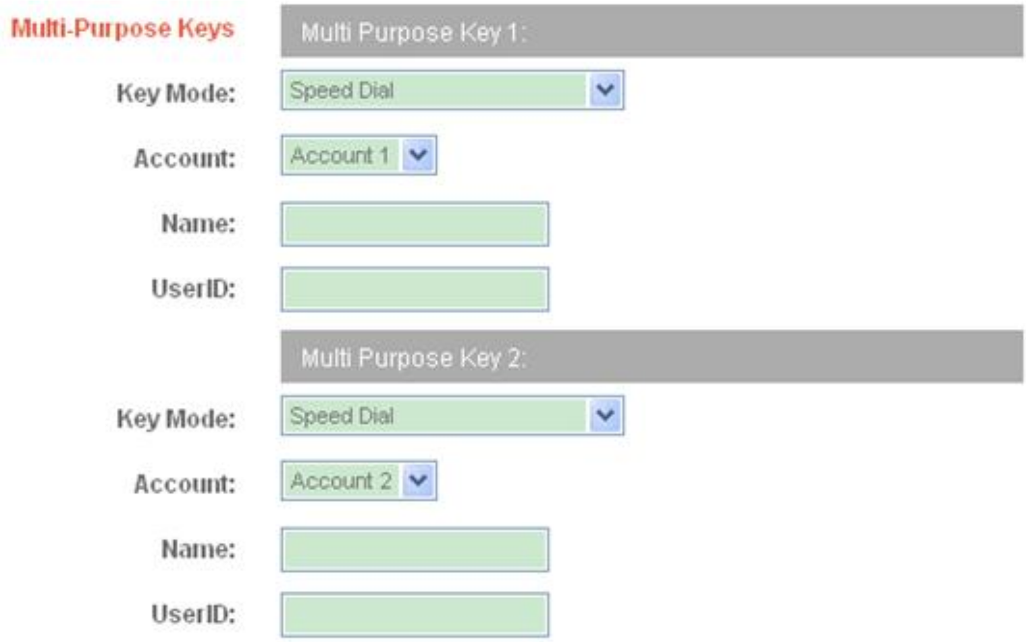
eSpace 6870 provides seven multi-purpose keys. The multi-purpose keys of an IP phone can be set as the keys for the functions such as fast dialing and BLF. The multi-purpose keys can be used to implement only the fast dialing function when the keys are used with the eSpace U19xx.

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



Multi-Purpose Keys

Multi Purpose Key 1:

Key Mode: Speed Dial

Account: Account 1

Name:

UserID:

Multi Purpose Key 2:

Key Mode: Speed Dial

Account: Account 2

Name:

UserID:

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

Table 2-4 Multi-purpose keys

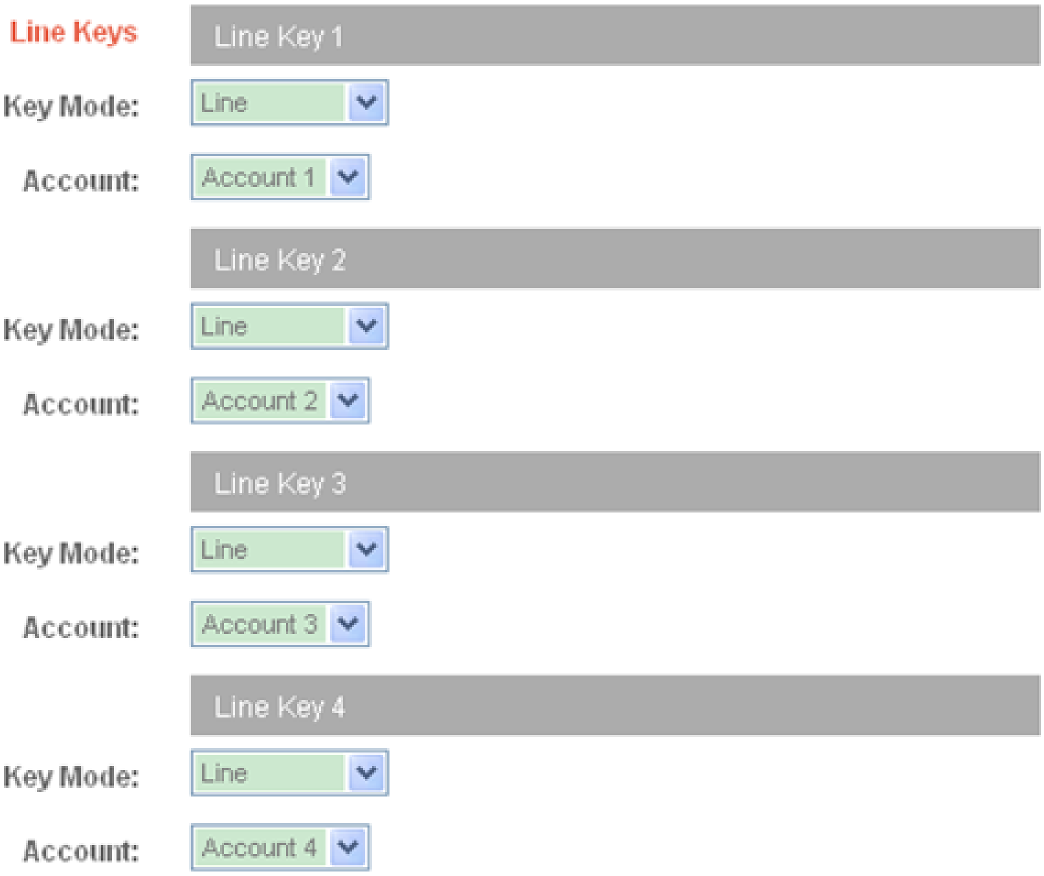
Function	Description	Setting		
		Account	Name	UserID
Speed dial	After pressing the key that is assigned with this function, you can directly make a call to the speed dial number.	Account dedicated for speed dial. The default account is **ACCOUNT 1**.	User name of the called party.	Phone number of the 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 eSpace U19xx documentation.	Account that is used to make a call to a monitored account.	User name corresponding to the monitored account.	Phone number of the monitored party.
eventlist BLF	You can press this key to view the account status of a	Account that is used to	User name correspondi	Phone number of

Function	Description	Setting		
		Account	Name	UserID
	monitored account in a 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 eSpace U19xx server. The BLF function must have been enabled on the SIP server. For details, see the eSpace U19xx documentation.	make a call to a monitored number.	ng to the monitored phone.	the 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



Line Keys

Line Key 1

Key Mode: Line

Account: Account 1

Line Key 2

Key Mode: Line

Account: Account 2

Line Key 3

Key Mode: Line

Account: Account 3

Line Key 4

Key Mode: Line

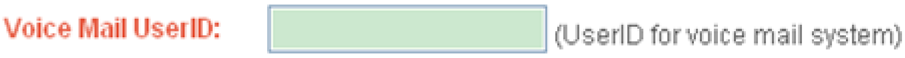
Account: Account 4

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 eSpace U19xx.

Figure 2-17 Voice Mail UserID



Voice Mail UserID: (UserID for voice mail system)

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

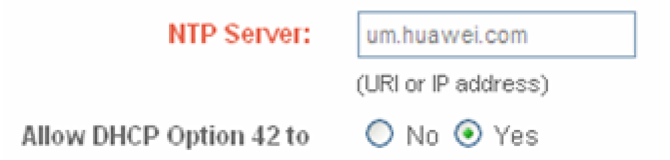
Perform the following steps to obtain the network time through NTP:

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 eSpace U19xx, or a router can act as an NTP server to provide the time for IP phones.

Figure 2-18 NTP Server



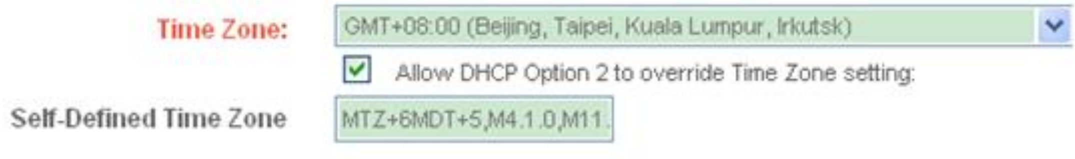
NTP Server: um.huawei.com

(URI or IP address)

Allow DHCP Option 42 to ○ No ● Yes

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



Time Zone: GMT+08:00 (Beijing, Taipei, Kuala Lumpur, Irkutsk)

☑ Allow DHCP Option 2 to override Time Zone setting:

Self-Defined Time Zone MTZ+6MDT+5,M4.1.0,M11.

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 *eSpace U19xx Unified Gateway Product Documentation*.

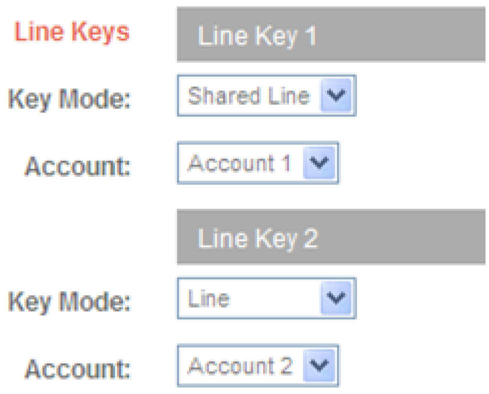
Configuring the Manager's Phone

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



Line Keys

Line Key 1

Key Mode: Shared Line

Account: Account 1

Line Key 2

Key Mode: Line

Account: Account 2

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

   ----End

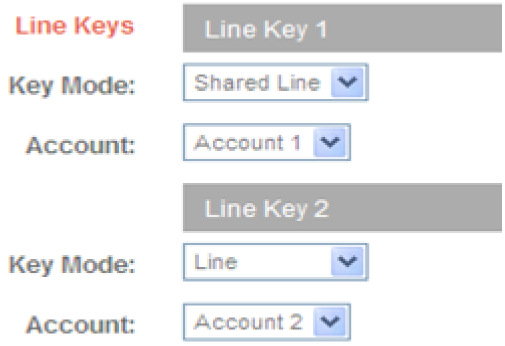
Configuring the Secretary's Phone

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



Line Keys

Line Key 1

Key Mode: Shared Line

Account: Account 1

Line Key 2

Key Mode: Line

Account: Account 2

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.

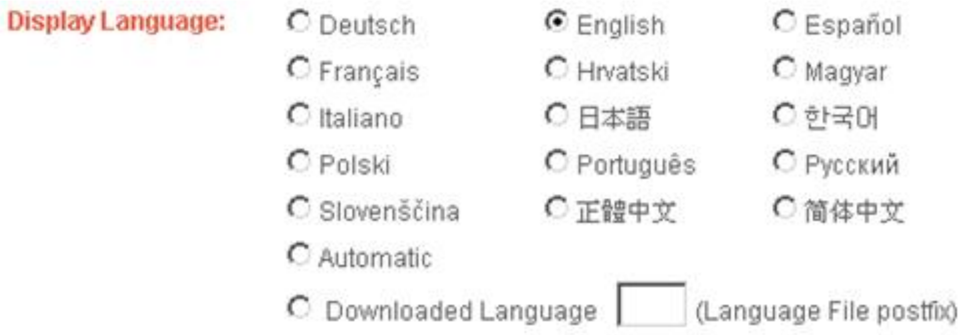
⚠ **CAUTION**

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



Display Language:

○ Deutsch ● English ○ Español
○ Français ○ Hrvatski ○ Magyar
○ Italiano ○ 日本語 ○ 한국어
○ Polski ○ Português ○ Русский
○ Slovenščina ○ 正體中文 ○ 简体中文
○ Automatic
○ Downloaded Language □ (Language File postfix)

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

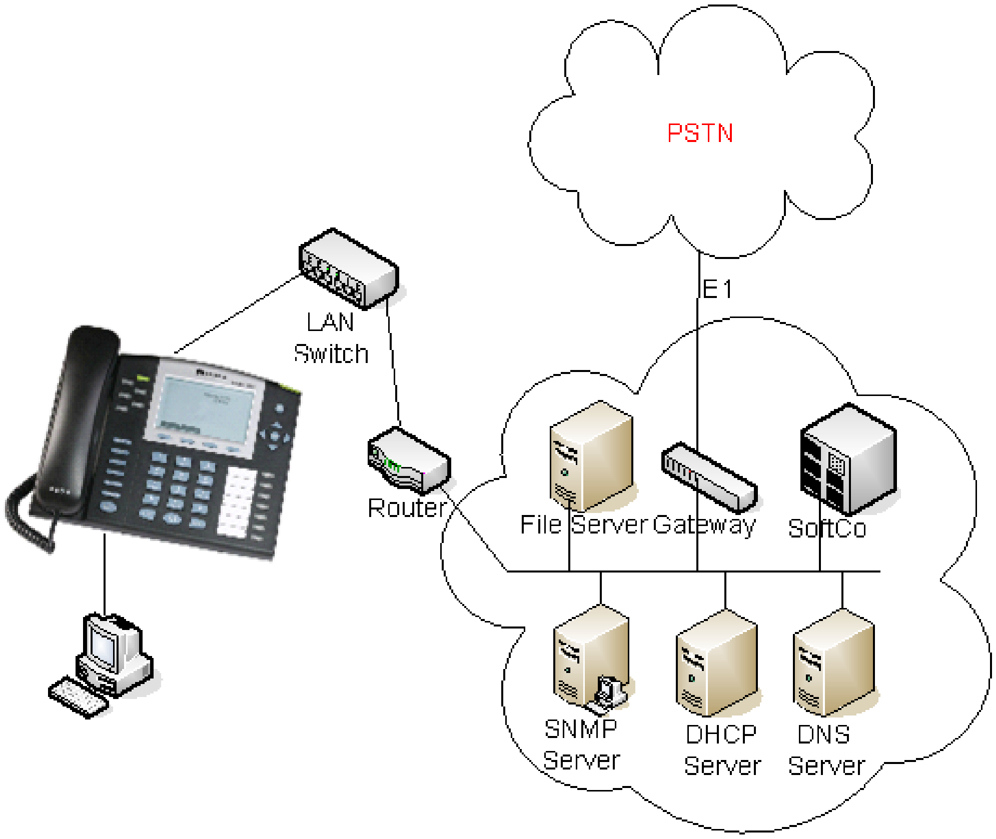
  When configuring the DHCP server, define a Option248 parameter as the file server URL. After this parameter is set, the DHCP server sends the file server URL to the IP phone that applies for an IP address. The phone downloads the version files and configuration file from this URL.
- DNS server

  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 5.2.2 Using the Apache Server.

4. Store the phone version files and configuration file in the HTTP server root directory **C:\Program Files\Apache Software Foundation\Apache2.2\htdocs**.

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

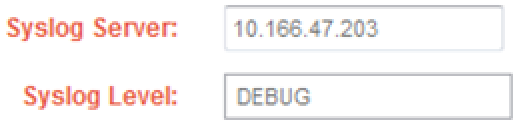
To locate the cause of the fault on an IP phone or learn the operation of an IP phone, you often need to use logs of the IP phone. The logs of the IP phone including the SIP information during the call and key debugging information of the IP phone can be displayed on the server so that maintenance personnel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



Syslog Server: 10.166.47.203

Syslog Level: DEBUG

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

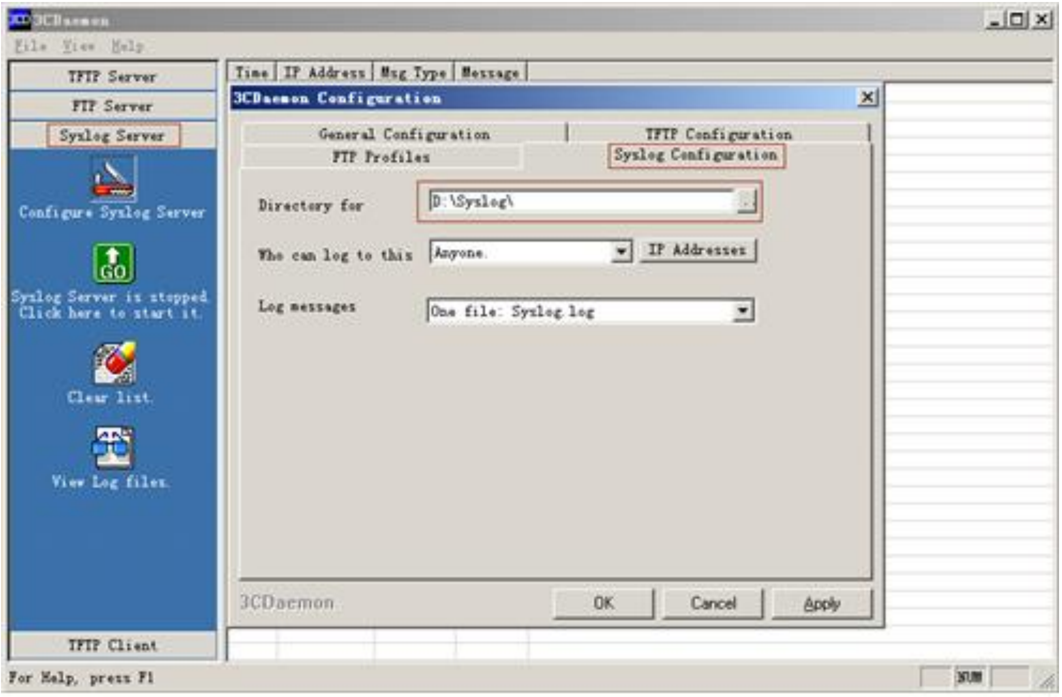
Setting the Log Server

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



Directory for: D:\Syslog\

Who can log to this: Anyone.

Log messages: One file: Syslog.log

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.

For details on how to capture and analyze packets, see 5.9 Wireshark User Guide.

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.

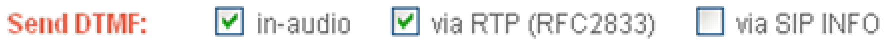
Cause

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



Send DTMF: ☑ in-audio ☑ via RTP (RFC2833) □ via SIP INFO

NOTE

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

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

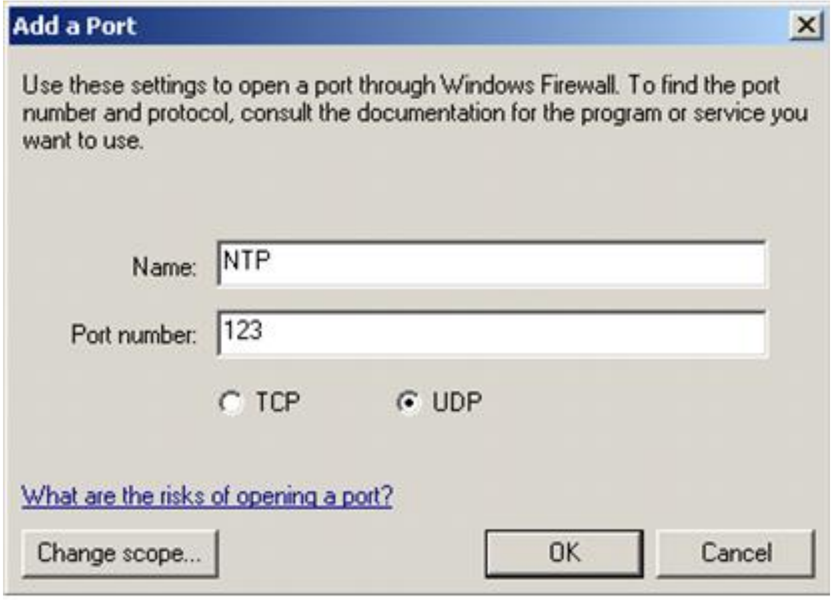
The firewall is installed on the computer; therefore, NTP packets sent by the IP phone are intercepted.

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



Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.

Name: NTP

Port number: 123

○ TCP ● UDP

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.711 A-law/μ-law. If the network quality is low, you can set the codec to G.729AB or G.723.1.

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

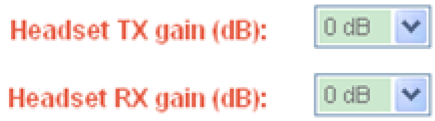
The volume of the IP phone is excessively low.

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)



Headset TX gain (dB): 0 dB

Headset RX gain (dB): 0 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.

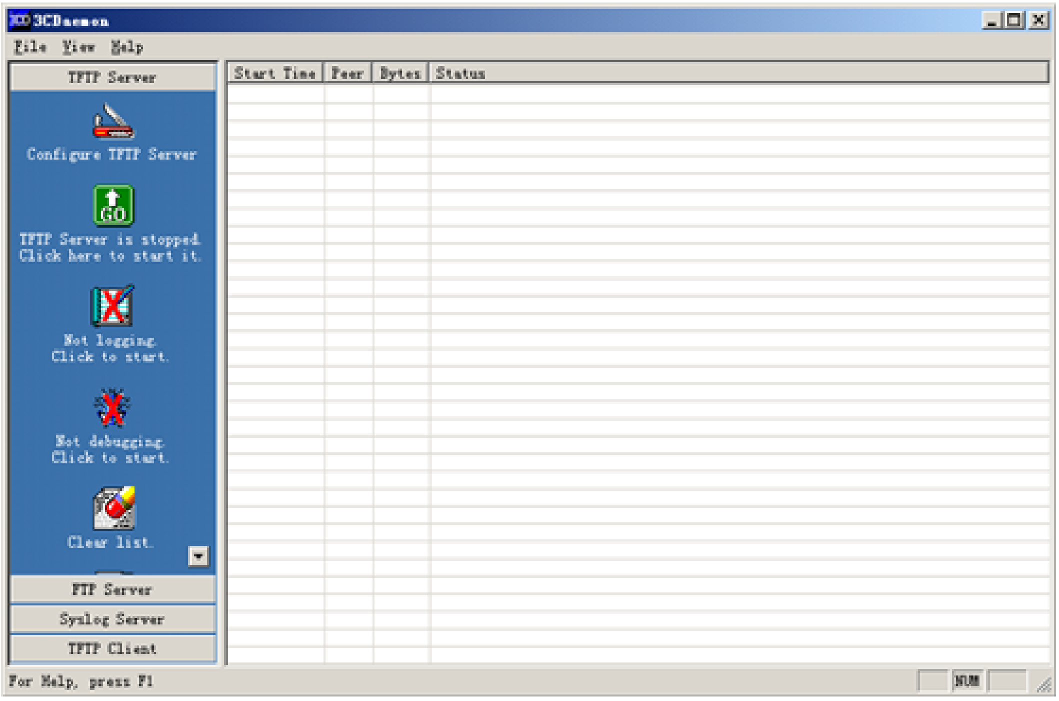
5 Appendix

5.1 Configuring the TFTP Server

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

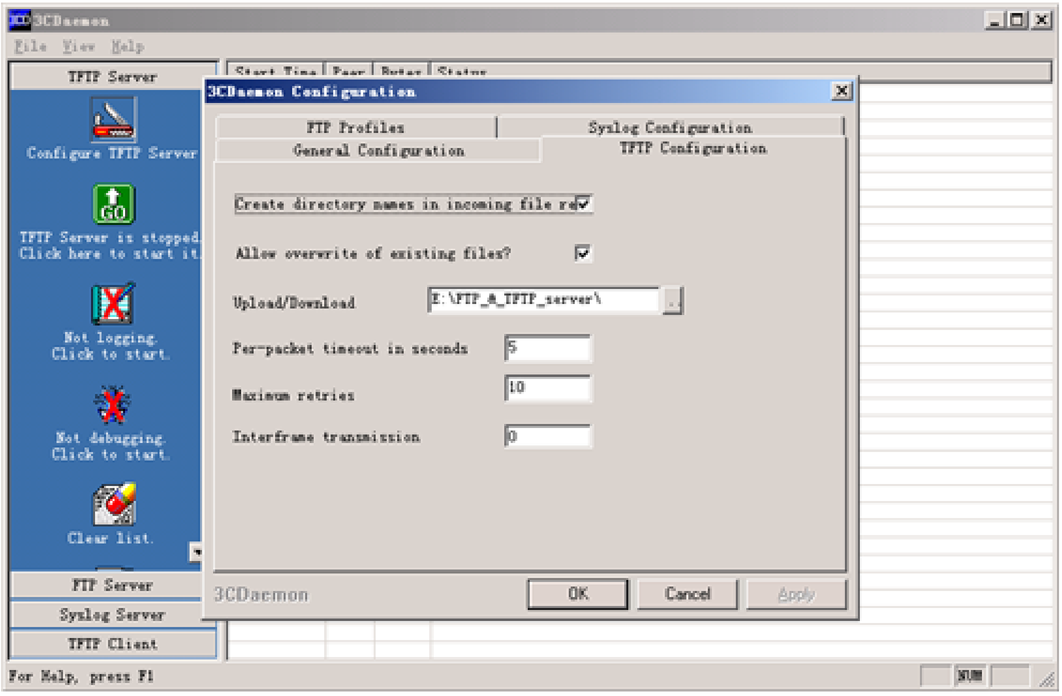
1. Start the TFTP server.

Figure 5-1 Starting the TFTP server



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

Figure 5-2 Configure TFTP Server



Create directory names in incoming file re ☑

Allow overwrite of existing files? ☑

Upload/Download E:\FTP_&_TFTP_server\

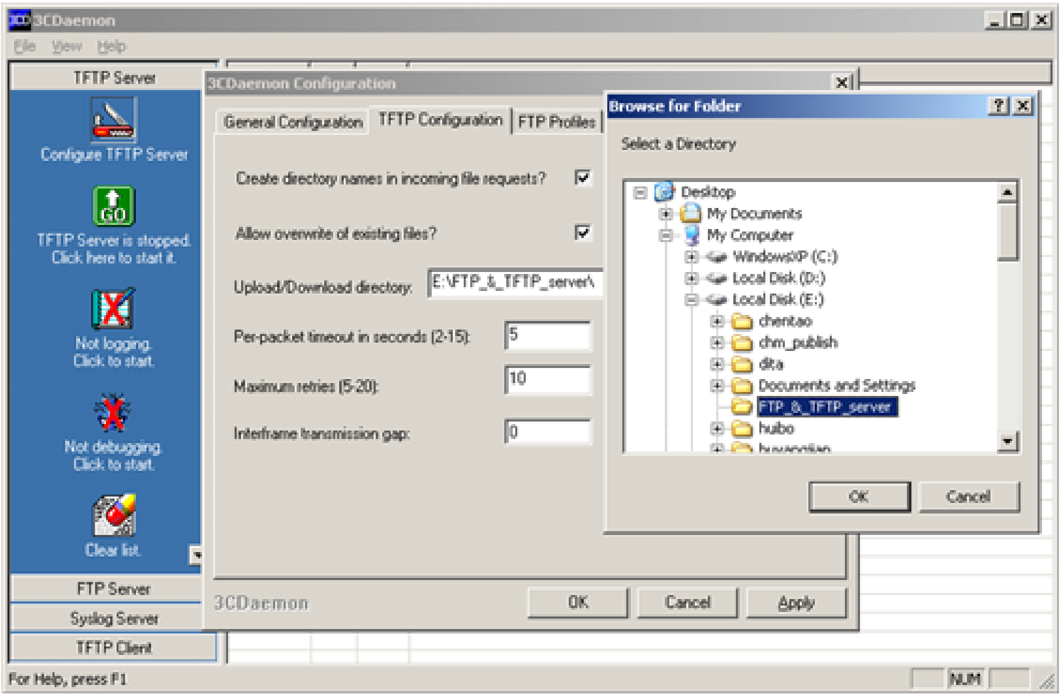
Per-packet timeout in seconds 5

Maximum retries 10

Interframe transmission 0

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



Create directory names in incoming file requests? ☑

Allow overwrite of existing files? ☑

Upload/Download directory: E:\FTP_&_TFTP_server\

Per-packet timeout in seconds (2-15): 5

Maximum retries (5-20): 10

Interframe transmission gap: 0

----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 Setting Up the HTTP Server

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

Stopping and Disabling Windows IIS

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

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

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

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

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

5.2.1 Using the Windows IIS Component

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

Context

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

Procedure

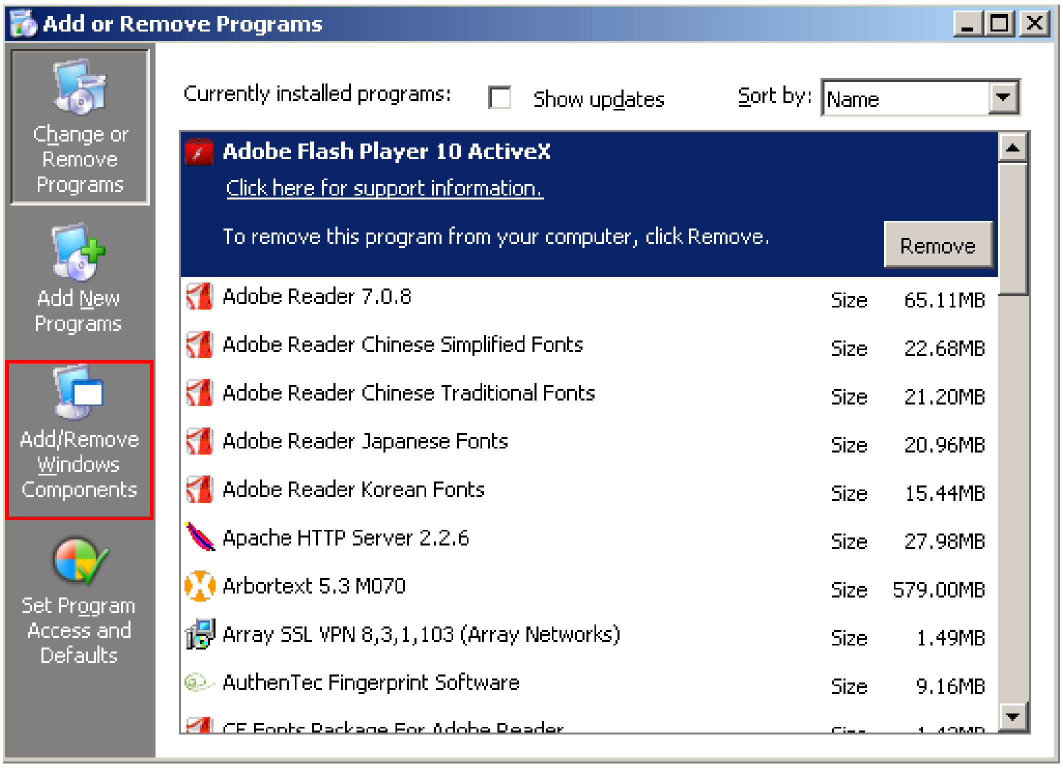
Step 1 Choose **Start** > **Control Panel**.

The **Control Panel** window is displayed.

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

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

Figure 5-4 Add or Remove Programs window


Add or Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Set Program Access and Defaults
Currently installed programs:
□ Show updates
Sort by: Name
Remove

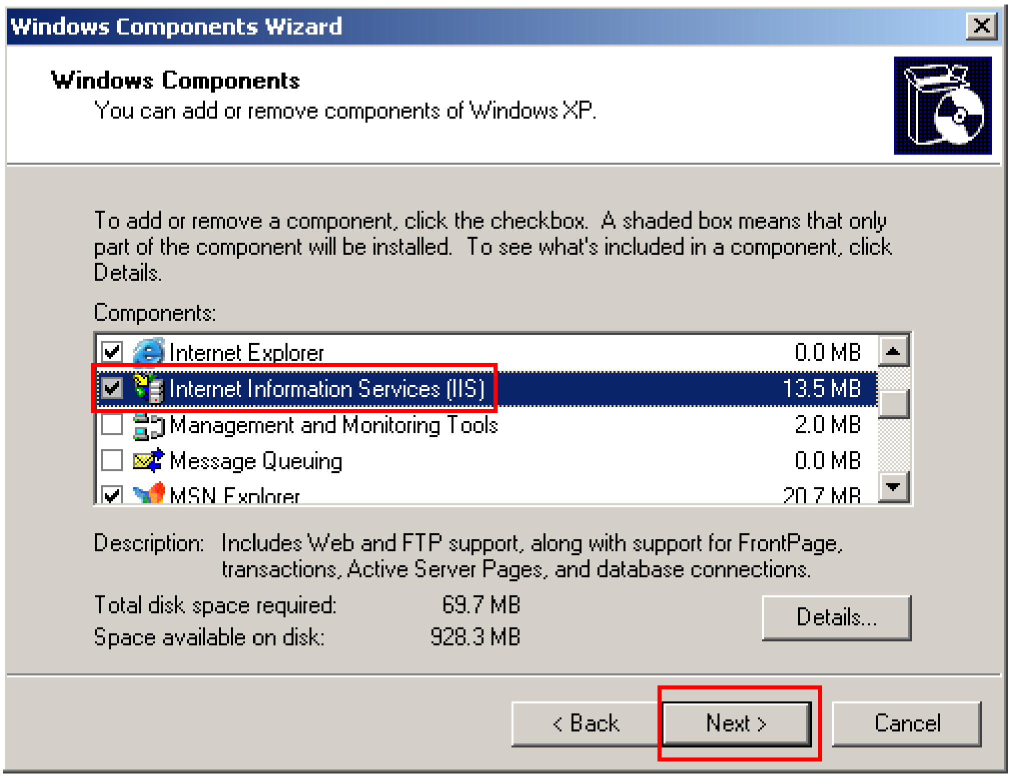
Adobe Flash Player 10 ActiveX
Click here for support information.
To remove this program from your computer, click Remove.

Adobe Reader 7.0.8	Size	65.11MB
Adobe Reader Chinese Simplified Fonts	Size	22.68MB
Adobe Reader Chinese Traditional Fonts	Size	21.20MB
Adobe Reader Japanese Fonts	Size	20.96MB
Adobe Reader Korean Fonts	Size	15.44MB
Apache HTTP Server 2.2.6	Size	27.98MB
Arbortext 5.3 M070	Size	579.00MB
Array SSL VPN 8,3,1,103 (Array Networks)	Size	1.49MB
AuthenTec Fingerprint Software	Size	9.16MB
CE Fonts Package For Adobe Reader	Size	

Step 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



Windows Components Wizard

Windows Components
You can add or remove components of Windows XP.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑	Internet Explorer	0.0 MB
☑	Internet Information Services (IIS)	13.5 MB
□	Management and Monitoring Tools	2.0 MB
□	Message Queuing	0.0 MB
☑	MSN Explorer	20.7 MB

Description: Includes Web and FTP support, along with support for FrontPage, transactions, Active Server Pages, and database connections.

Total disk space required: 69.7 MB
Space available on disk: 928.3 MB

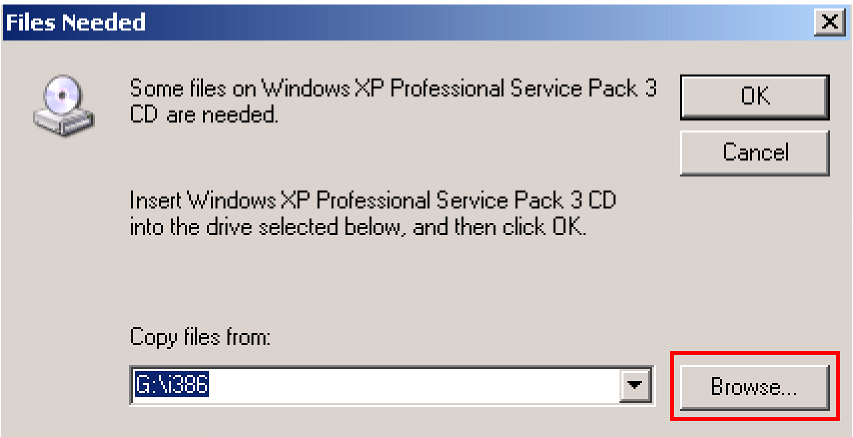
Step 4 Select the **Internet Information Services (IIS)** check box in the **Components** area and click **Next**.

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

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

The Files Needed dialog box is displayed, as shown in Figure 5-6.

Figure 5-6 Files Needed dialog box



Files Needed

Some files on Windows XP Professional Service Pack 3 CD are needed.

Insert Windows XP Professional Service Pack 3 CD into the drive selected below, and then click OK.

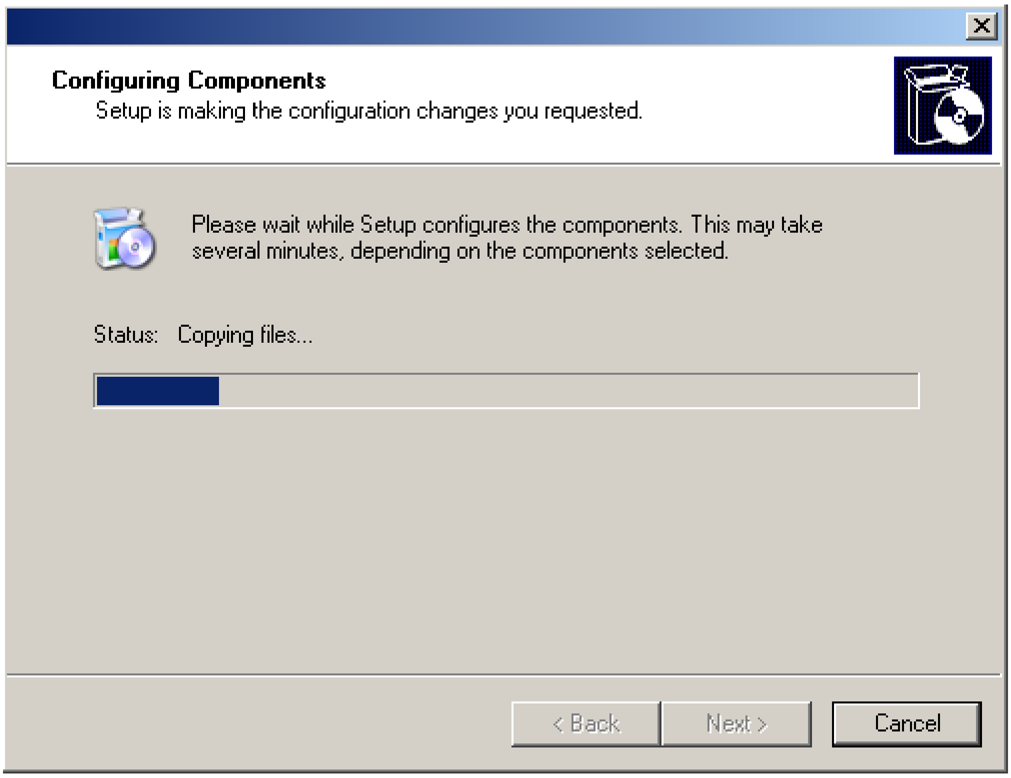
Copy files from:
G:\i386

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

Step 7 Click OK.

The system starts copying the files and installing the component, as shown in Figure 5-7.

Figure 5-7 Configuring Components dialog box



Configuring Components

Setup is making the configuration changes you requested.

Please wait while Setup configures the components. This may take several minutes, depending on the components selected.

Status: Copying files...

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

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

----End

5.2.2 Using the Apache Server

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

Context

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

Procedure

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

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

NOTE

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

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

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

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

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

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

NOTE

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

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

----End

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://enterprise.huawei.com/en/support/** to download **PhoneBook.exe**.

NOTE

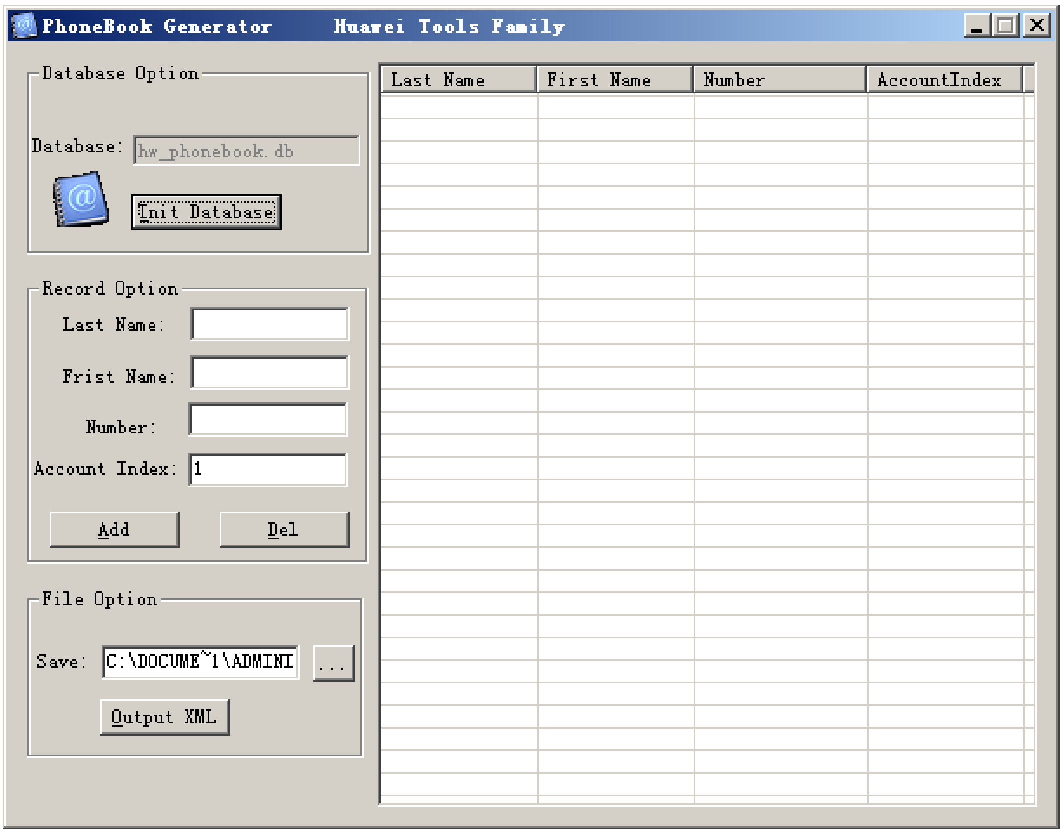
You must apply for permission to download **PhoneBook.exe** from the website. If you need to download the tool, contact system or service providers.

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

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

Figure 5-8 shows the **PhoneBook Generator** page.

Figure 5-8 PhoneBook Generator page



Database: hw_phonebook.db

Last Name:

Frist Name:

Number:

Account Index: 1

Save: C:\DOCUME~1\ADMINI

Last Name	First Name	Number	AccountIndex

- 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**.

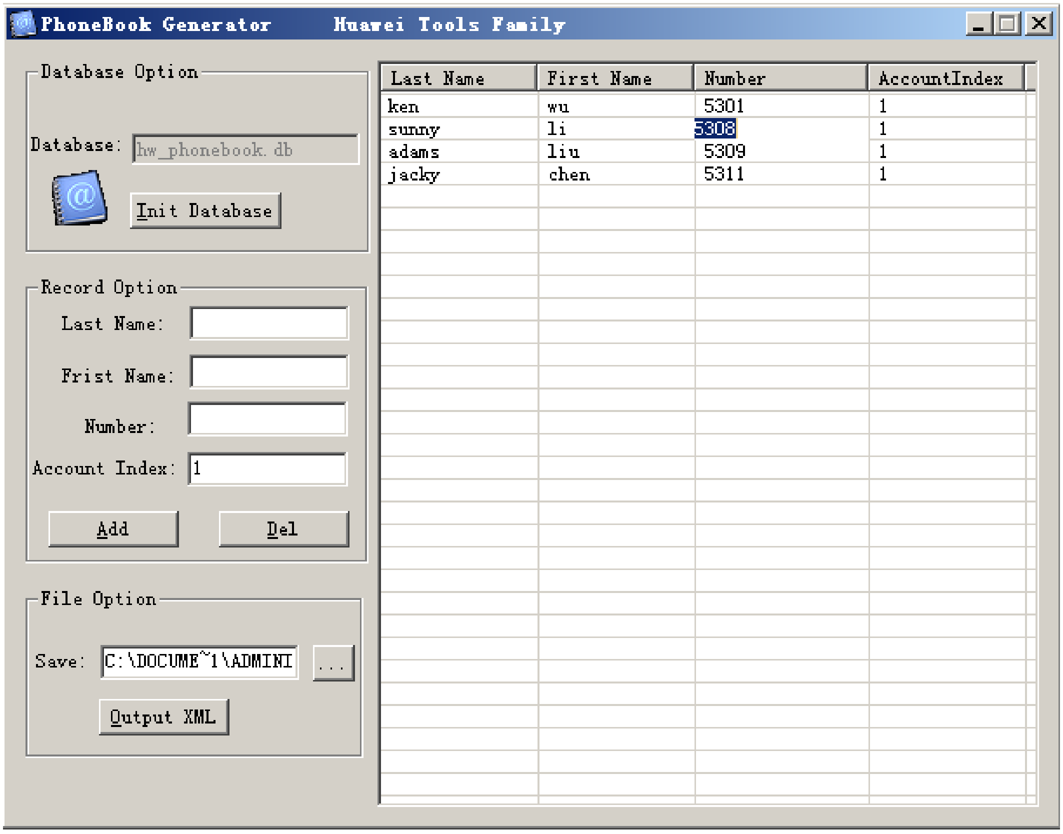
After entering the parameter values in the preceding table, click **Add**. The new record is displayed on the right of the page.

- 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 5-9 Changing a phone number



Database: hw_phonebook.db

Account Index: 1

Save: C:\DOCUME~1\ADMINI

Last Name	First Name	Number	AccountIndex
ken	wu	5301	1
sunny	li	5308	1
adams	liu	5309	1
jacky	chen	5311	1

- 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

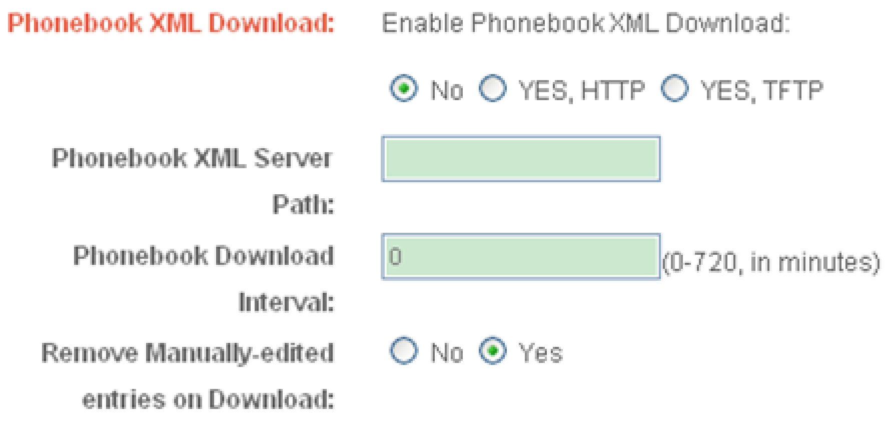
- The **Upgrade** button displayed after you click … is used only to select the destination path. The **Output XML** button is used to export an .xml file.
- Do not change the name of the phone book file. Otherwise, it cannot be imported. The default phone book file is **named hw_phonebook.xml**.

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 5-10 Advanced settings



Phonebook XML Download: Enable Phonebook XML Download:

● No ○ YES, HTTP ○ YES, TFTP

Phonebook XML Server Path:

Phonebook Download Interval: 0 (0-720, in minutes)

Remove Manually-edited entries on Download: ○ No ● Yes

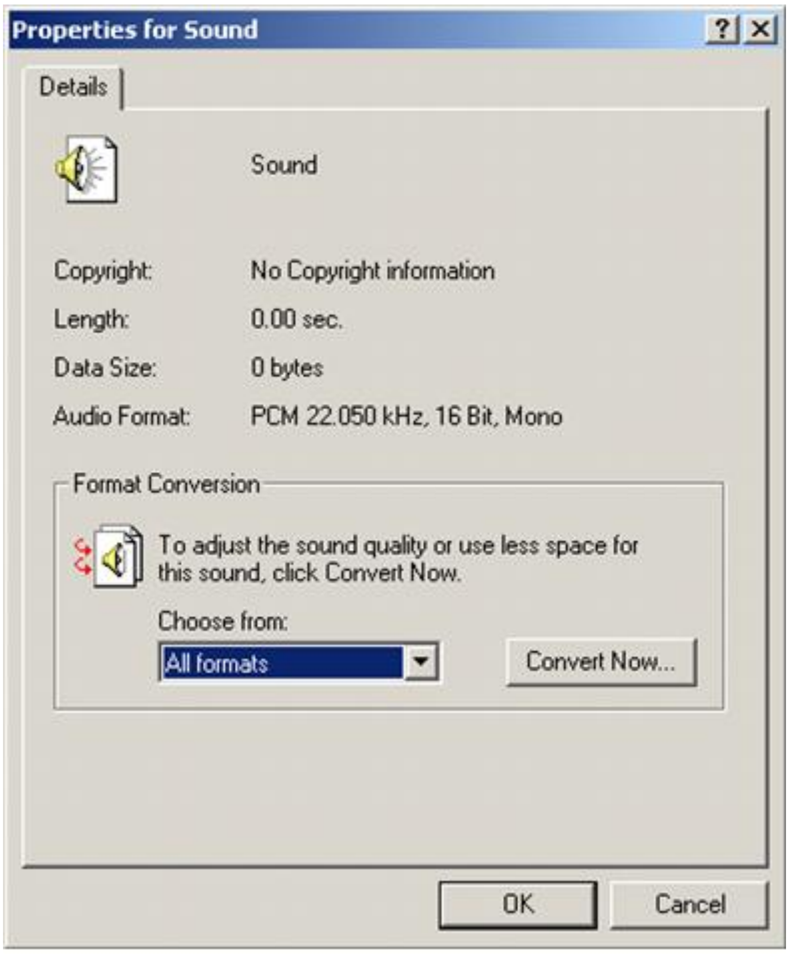
5.4 Setting Personal Ring Tones for an IP Phone

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 5-11 Properties for Sound dialog box



Properties for Sound

Sound

Copyright: No Copyright information

Length: 0.00 sec.

Data Size: 0 bytes

Audio Format: PCM 22.050 kHz, 16 Bit, Mono

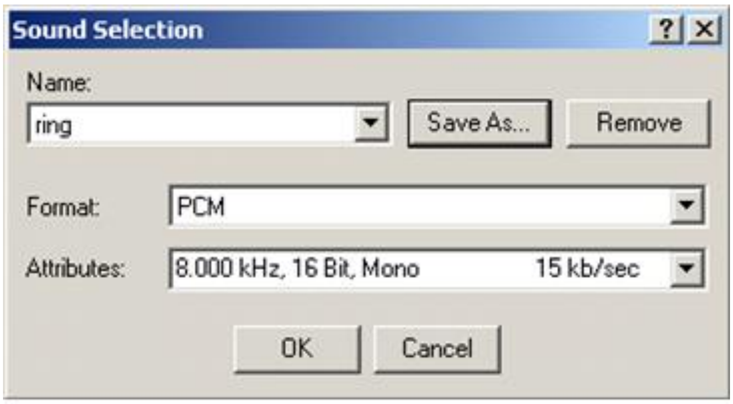
Format Conversion

To adjust the sound quality or use less space for this sound, click Convert Now.

Choose from: All formats

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 5-12 Sound Selection dialog box



Name: ring

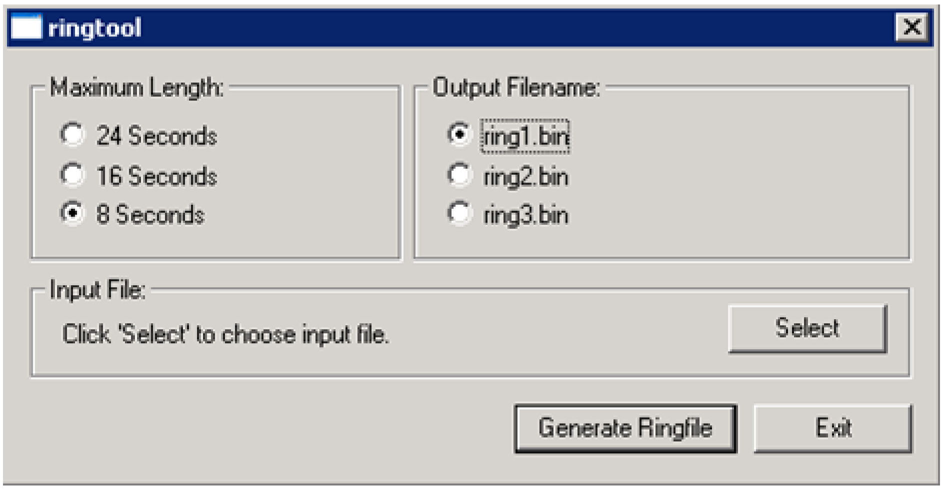
Format: PCM

Attributes: 8.000 kHz, 16 Bit, Mono 15 kb/sec

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 5-13 Ringtool dialog box



Maximum Length:
○ 24 Seconds
○ 16 Seconds
● 8 Seconds

Output Filename:
● ring1.bin
○ ring2.bin
○ ring3.bin

Input File:
Click 'Select' to choose input file.

   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.

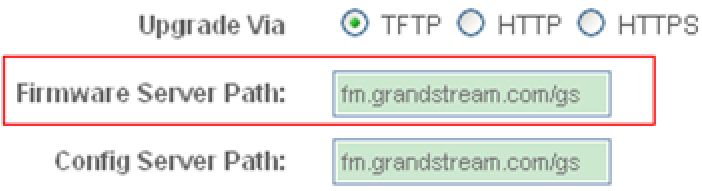
   ----End

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 5-14 Firmware server path

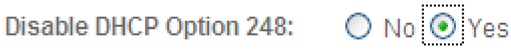


Upgrade Via ● TFTP ○ HTTP ○ HTTPS

Firmware Server Path: fm.grandstream.com/gs

Config Server Path: fm.grandstream.com/gs

3. Disable DHCP Option 248.



Disable DHCP Option 248: ○ No ● Yes

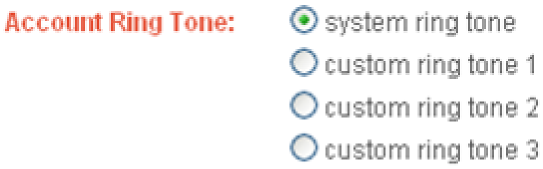
4. Restart the IP phone. The IP phone downloads the three files when the time for automatic upgrade comes.

----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 5-15 Account Ring Tone



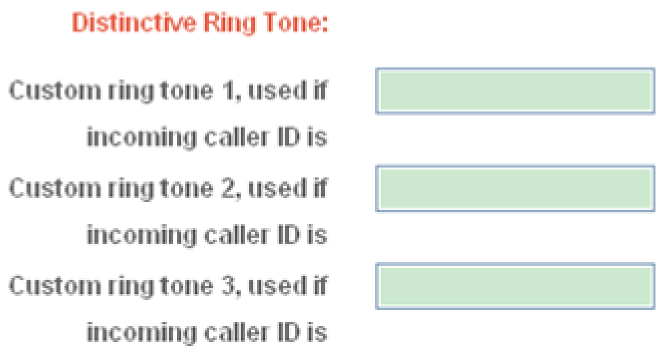
Account Ring Tone: ● system ring tone
○ custom ring tone 1
○ custom ring tone 2
○ custom ring tone 3

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 5-16 Distinctive Ring Tone



Distinctive Ring Tone:

Custom ring tone 1, used if incoming caller ID is

Custom ring tone 2, used if incoming caller ID is

Custom ring tone 3, used if incoming caller ID is

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://enterprise.huawei.com/en/support/**.

NOTE

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

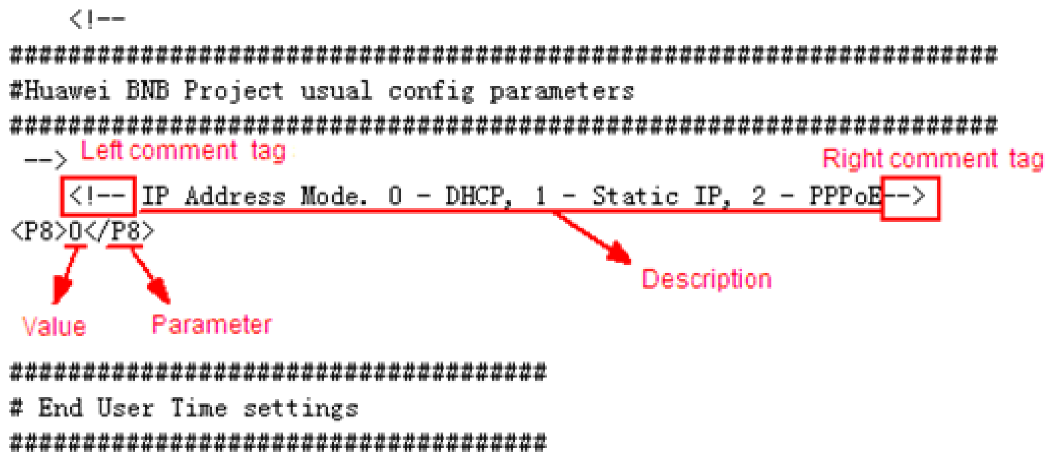
The path is **Software Downloads** > **Unified Communication** > **IP Phone** > **Version (For example, IP Phone V100R001C02)** > **software**.

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 5-17 shows the configuration file template.

Figure 5-17 Configuration file template



```
  <!--
######################################################################
#Huawei BNB Project usual config parameters
######################################################################
 -->
   <!--IP Address Mode. 0 - DHCP, 1 - Static IP, 2 - PPPoE-->
<P8>0</P8>

######################################
# End User Time settings
######################################
```

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

NOTE

- For parameter description, see Table 2-2 in the 2.2.4 Advanced Configuration and Table 2-3 in the 2.2.5 Individual Account Configuration.
- 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.

ID	Parameter	Setting Example	Description
			- 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. 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	1	Indicates whether to enable the Option43 and Option66 settings on the DHCP server. - 0: No - 1: Yes The default value is **1**.

ID	Parameter	Setting Example	Description
	server		
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. 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.

ID	Parameter	Setting Example	Description
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 • 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

ID	Parameter	Setting Example	Description
			- 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**. 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**.

ID	Parameter	Setting Example	Description
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 • 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

ID	Parameter	Setting Example	Description
			• 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**.
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**.

ID	Parameter	Setting Example	Description
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**

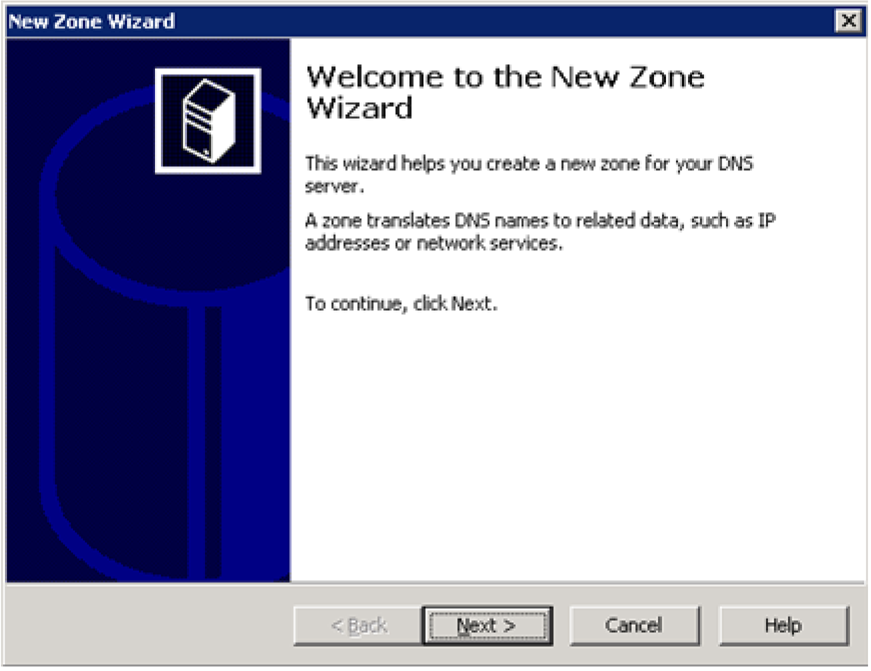
If the DNS service is not installed on the PC, install the DNS component firstly.

Creating a Zone

To create a zone, do as follows:

Step 1 Right click **Forward Lookup Zones**, and then choose **New Zone** to start **New Zone Wizard**.As shown in Figure 5-18.

Figure 5-18 New Zone Wizard



New Zone Wizard

Welcome to the New Zone Wizard

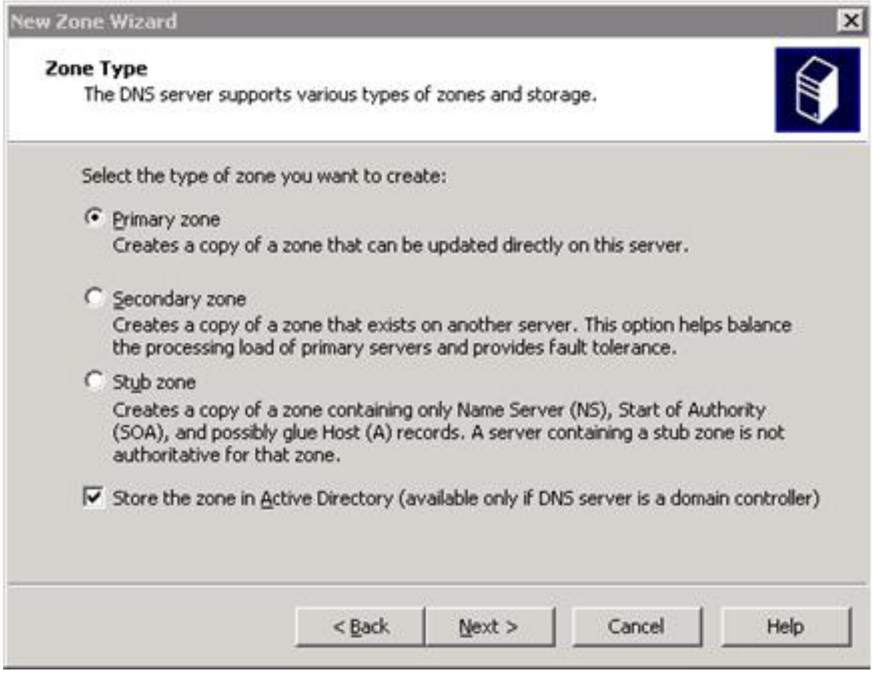
This wizard helps you create a new zone for your DNS server.

A zone translates DNS names to related data, such as IP addresses or network services.

To continue, click Next.

Step 2 Click **Next**, and then select **Primary zone** to create a primary zone.As shown in Figure 5-19.

Figure 5-19 Zone Type



New Zone Wizard

Zone Type

The DNS server supports various types of zones and storage.

Select the type of zone you want to create:

● Primary zone
Creates a copy of a zone that can be updated directly on this server.

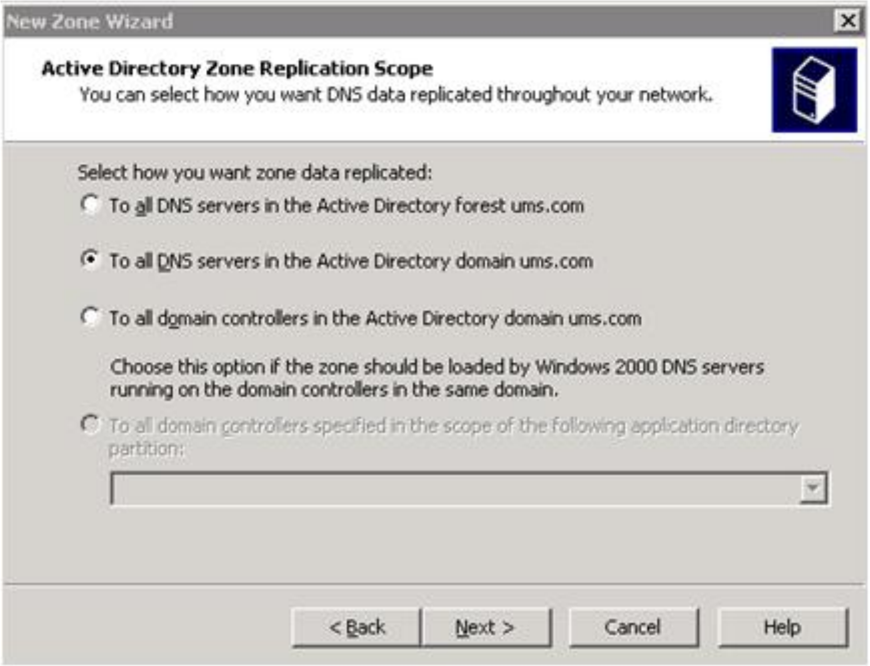
○ Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.

○ Stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.

☑ Store the zone in Active Directory (available only if DNS server is a domain controller)

Step 3 Select an option for Select how you want zone data replicated, and click **Next**.As shown in Figure 5-20.

Figure 5-20 Active Directory Zone Replication Scope



New Zone Wizard

Active Directory Zone Replication Scope
You can select how you want DNS data replicated throughout your network.

Select how you want zone data replicated:

○ To all DNS servers in the Active Directory forest ums.com

● To all DNS servers in the Active Directory domain ums.com

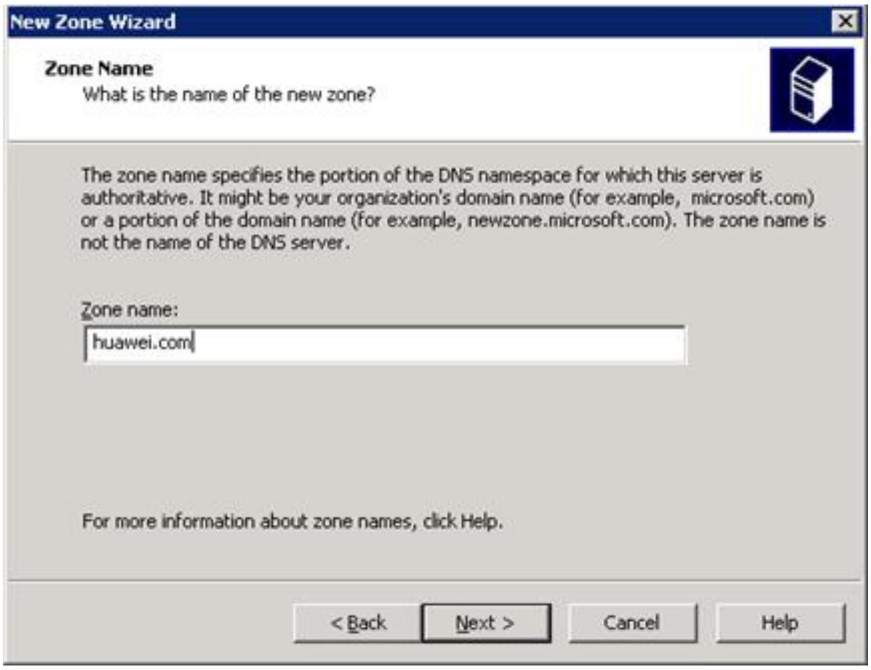
○ To all domain controllers in the Active Directory domain ums.com

Choose this option if the zone should be loaded by Windows 2000 DNS servers running on the domain controllers in the same domain.

○ To all domain controllers specified in the scope of the following application directory partition:

Step 4 Enter the name of the DNS zone, for example, huawei.com. Then click **Next**.As shown in Figure 5-21.

Figure 5-21 Zone Name



New Zone Wizard

Zone Name
What is the name of the new zone?

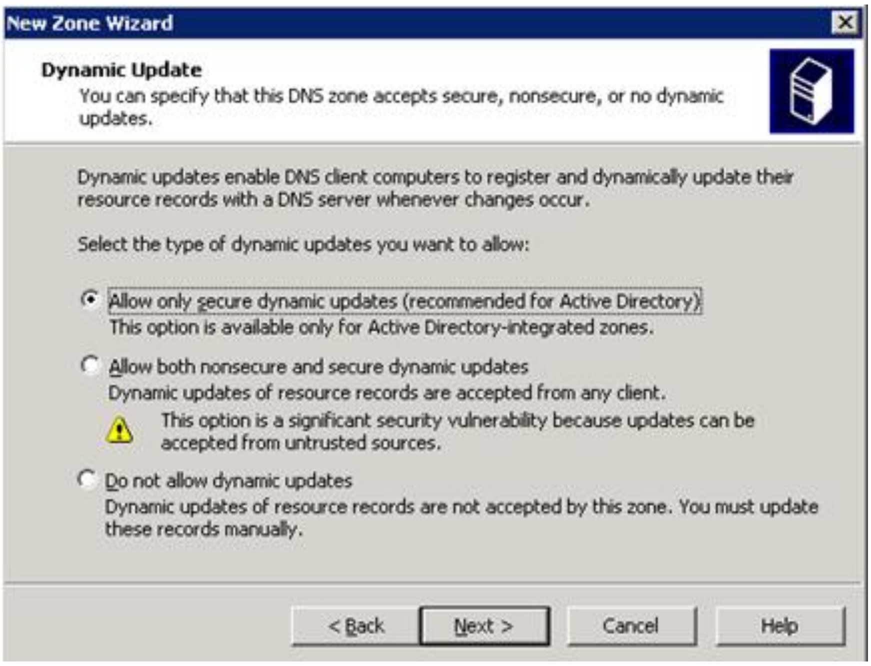
The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.

Zone name: huawei.com

For more information about zone names, click Help.

Step 5 Select a dynamic update type, and then click **Next**.As shown in Figure 5-22.

Figure 5-22 Dynamic Update



New Zone Wizard

Dynamic Update

You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.

Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.

Select the type of dynamic updates you want to allow:

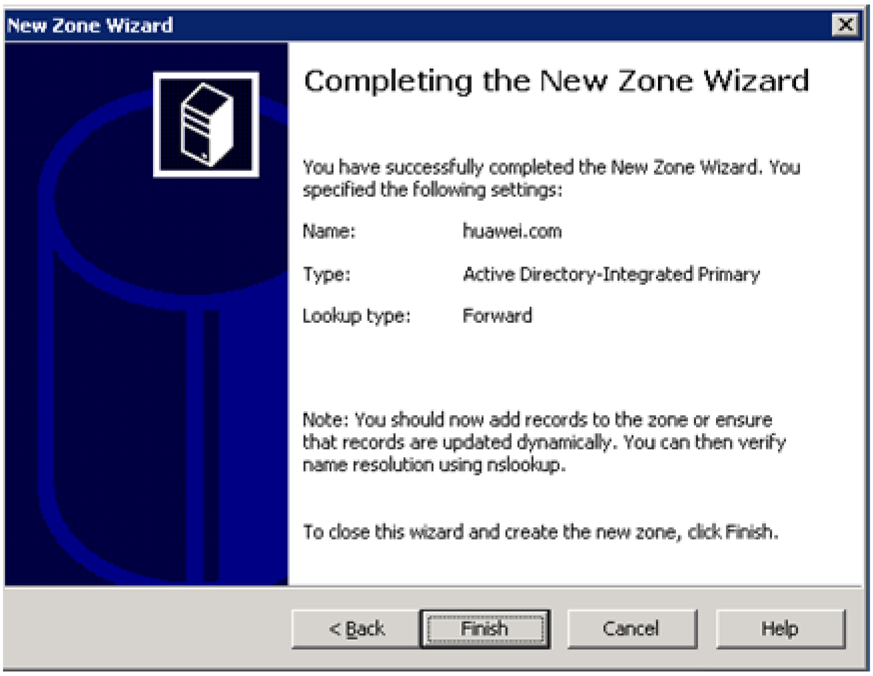
● Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.

○ Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
⚠ This option is a significant security vulnerability because updates can be accepted from untrusted sources.

○ Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.

Step 6 After the zone is created, click **Finish**.As shown in Figure 5-23.

Figure 5-23 Finish New Zone Wizard



New Zone Wizard

Completing the New Zone Wizard

You have successfully completed the New Zone Wizard. You specified the following settings:

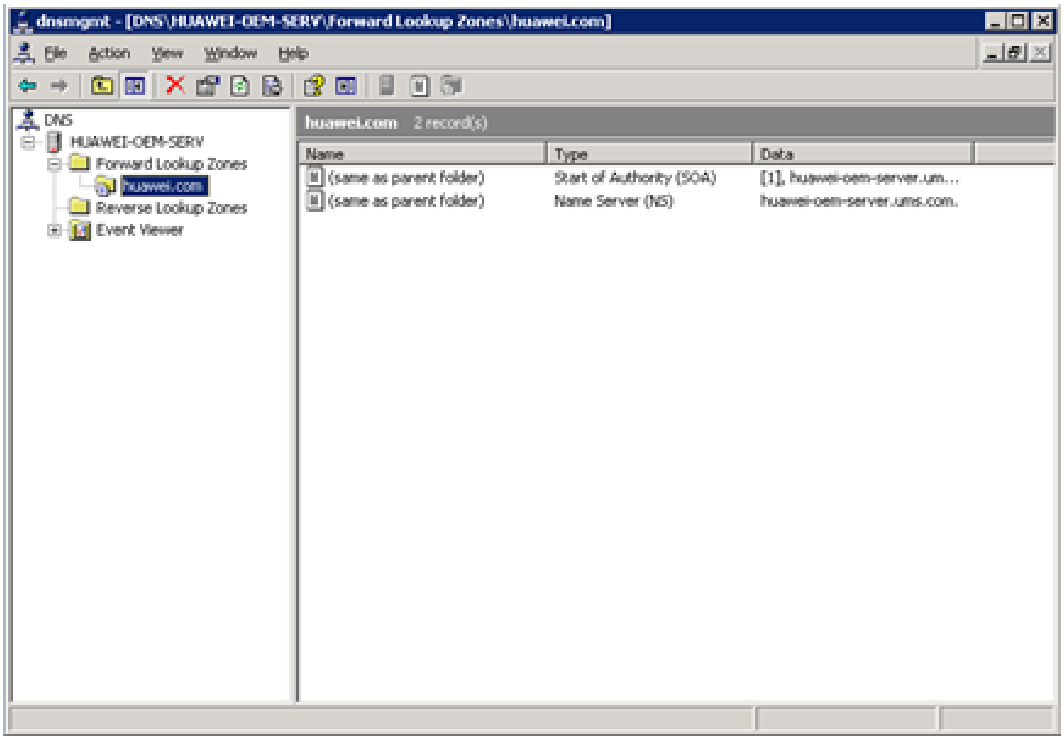
Name:	huawei.com
Type:	Active Directory-Integrated Primary
Lookup type:	Forward

Note: You should now add records to the zone or ensure that records are updated dynamically. You can then verify name resolution using nslookup.

To close this wizard and create the new zone, click Finish.

Step 7 A new zone is displayed.As shown in Figure 5-24.

Figure 5-24 New Zone



Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[1], huawei-oem-server.um...
(same as parent folder)	Name Server (NS)	huawei-oem-server.ums.com.

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

----End

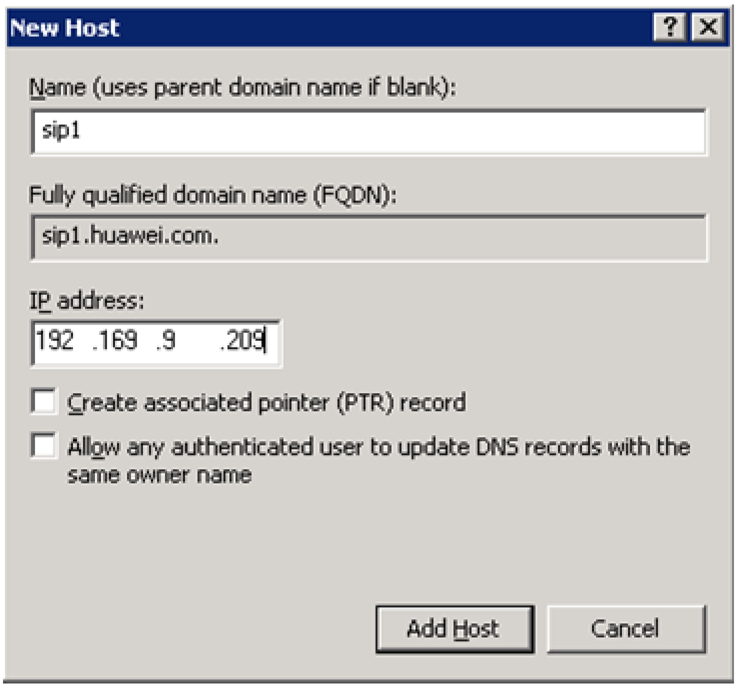
Creating a Record of Type A

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

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

Step 1 Right-click **Huawei.com** and choose **New Host(A)**. After setting the host name and IP address, click **Add Host**.As shown in Figure 5-25.

Figure 5-25 New Host



Name (uses parent domain name if blank):
sip1

Fully qualified domain name (FQDN):
sip1.huawei.com.

IP address:
192 .169 .9 .209

□ Create associated pointer (PTR) record

□ Allow any authenticated user to update DNS records with the same owner name

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

----End

5.7 Setting Up the DHCP Server

5.7.1 Setting Up the DHCP Server in the Window 2003 Server

Basics Concepts

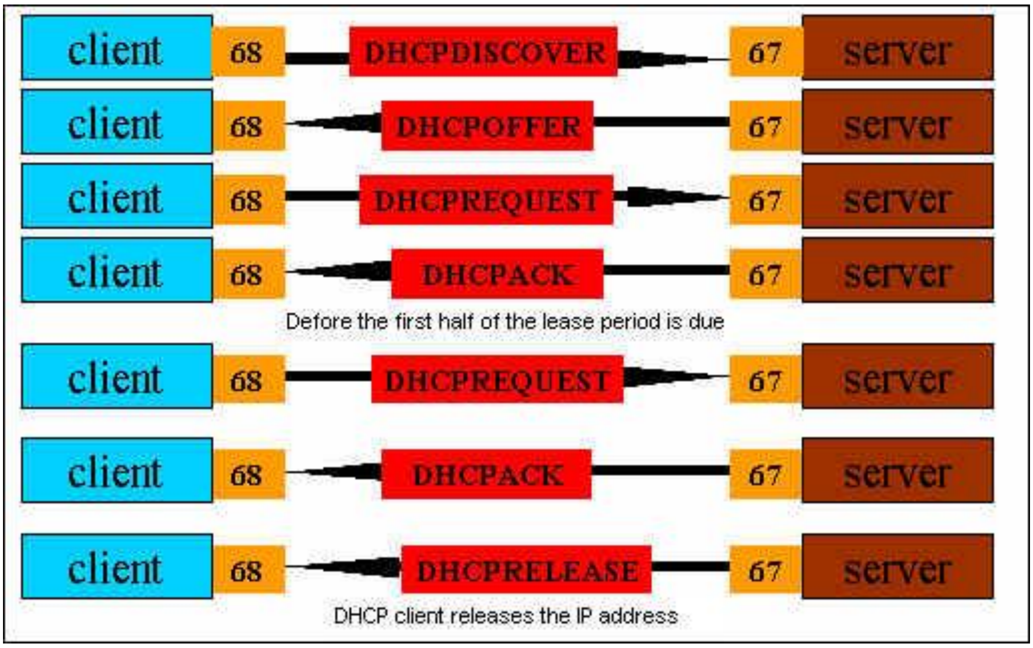
The Dynamic Host Configuration Protocol (DHCP) is mainly used to allocate dynamic IP addresses to terminals on the same network. When DHCP is used, a DHCP server needs to be deployed on the network and IP phones function as DHCP clients.

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 Figure 5-26 shows the process for an IP phone to obtain the IP address through DHCP.

Figure 5-26 Obtain the IP address through DHCP

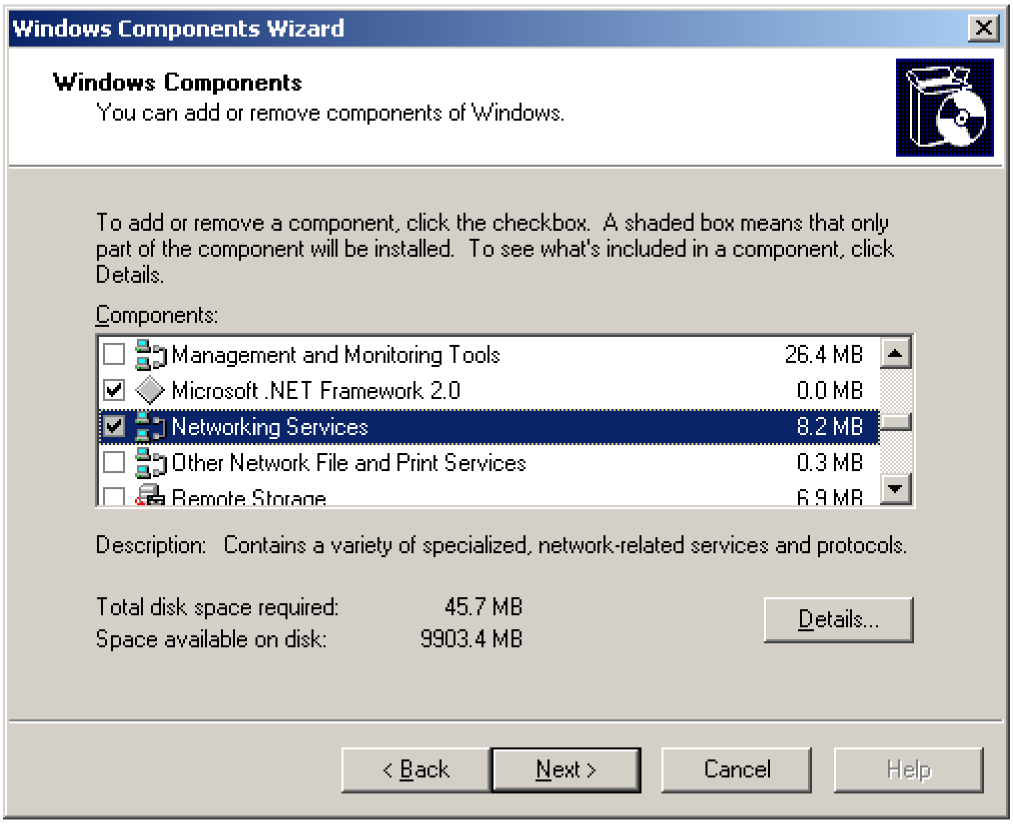


Installing the DHCP Service

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

Step 1 Choose **Start** > **Settings** > **Control Panel**, click **Add or Remove Programs**, and click **Add/Remove Windows Components**.The **Windows Components Wizard** dialog box is displayed. as shown in Figure 5-27.

Figure 5-27 Windows Components Wizard



Windows Components Wizard

Windows Components

You can add or remove components of Windows.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

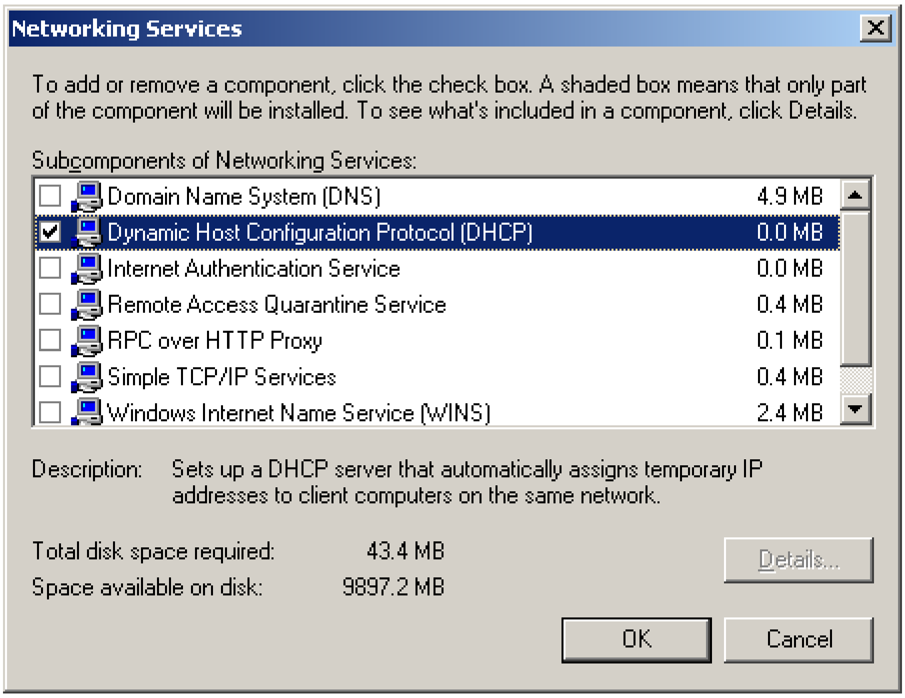
□	Management and Monitoring Tools	26.4 MB
☑	Microsoft .NET Framework 2.0	0.0 MB
☑	Networking Services	8.2 MB
□	Other Network File and Print Services	0.3 MB
□	Remote Storage	6.9 MB

Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 45.7 MB
Space available on disk: 9903.4 MB

Step 2 Select **Networking Services**, and click **Details** to display the **Networking Services** dialog box. as shown in Figure 5-28.

Figure 5-28 Networking Services



To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Networking Services:

□	Domain Name System (DNS)	4.9 MB
☑	Dynamic Host Configuration Protocol (DHCP)	0.0 MB
□	Internet Authentication Service	0.0 MB
□	Remote Access Quarantine Service	0.4 MB
□	RPC over HTTP Proxy	0.1 MB
□	Simple TCP/IP Services	0.4 MB
□	Windows Internet Name Service (WINS)	2.4 MB

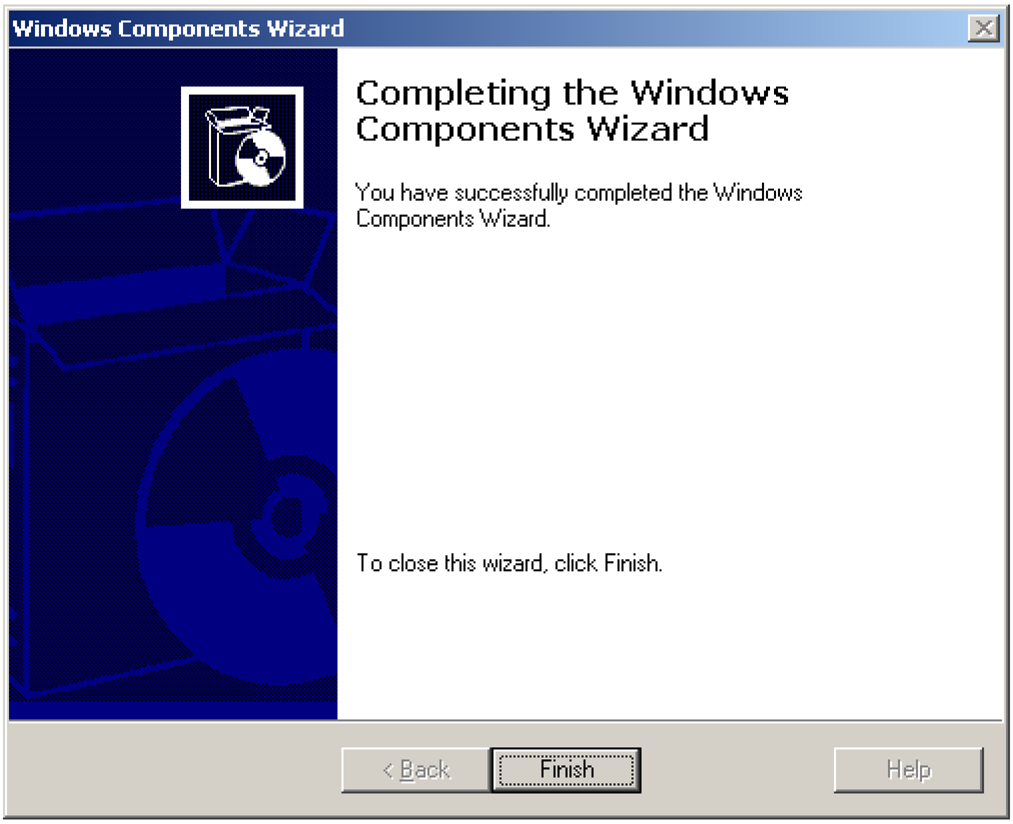
Description: Sets up a DHCP server that automatically assigns temporary IP addresses to client computers on the same network.

Total disk space required: 43.4 MB

Space available on disk: 9897.2 MB

Step 3 Select the DHCP service and click **OK** to exit the page of network service. Click **Next** repeatedly until the installation is complete. After the installation is successful, the dialog box shown in the following figure is displayed. as shown in Figure 5-29.

Figure 5-29 Completing the Windows Components Wizard



Completing the Windows Components Wizard

You have successfully completed the Windows Components Wizard.

To close this wizard, click Finish.

----End

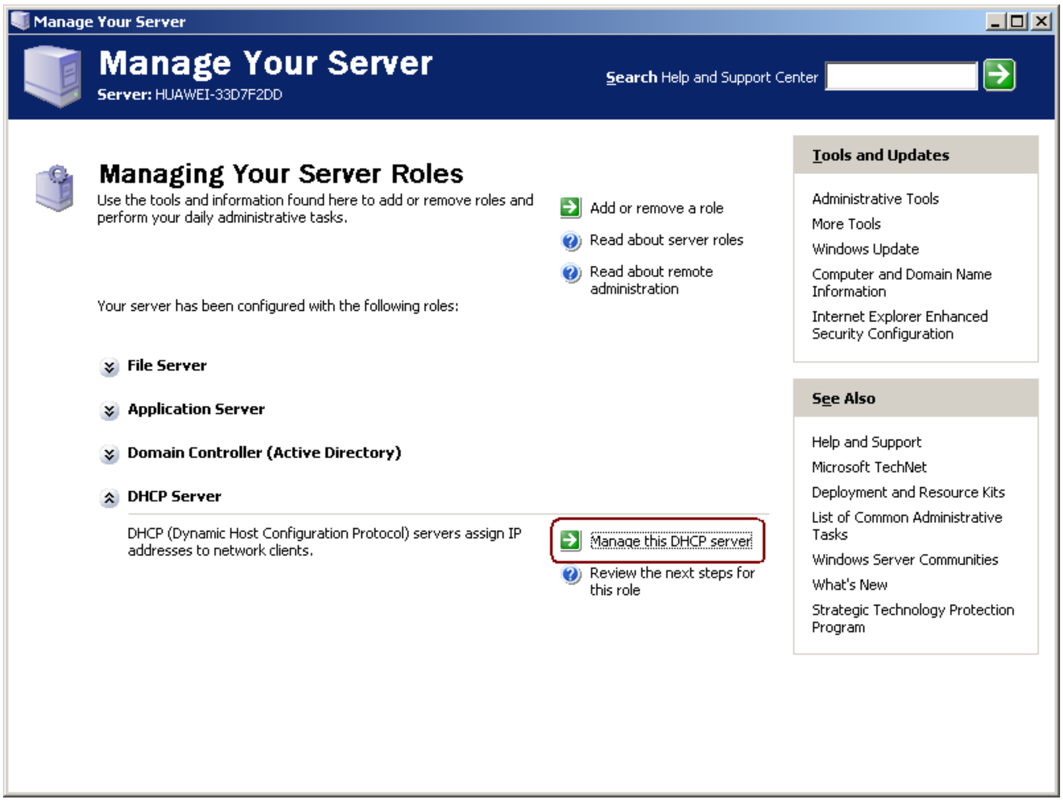
Starting the DHCP Service and Setting DHCP Parameters

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

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

Step 2 In the **Manage Your Server** dialog box that is displayed, select **Manage this DHCP** server. as shown in Figure 5-30.

Figure 5-30 Manage Your Server



Manage Your Server

Server: HUAWEI-33D7F2DD

Search Help and Support Center

Managing Your Server Roles

Use the tools and information found here to add or remove roles and perform your daily administrative tasks.

Add or remove a role

Read about server roles

Read about remote administration

Your server has been configured with the following roles:

File Server

Application Server

Domain Controller (Active Directory)

DHCP Server

DHCP (Dynamic Host Configuration Protocol) servers assign IP addresses to network clients.

Manage this DHCP server

Review the next steps for this role

Tools and Updates

Administrative Tools

More Tools

Windows Update

Computer and Domain Name Information

Internet Explorer Enhanced Security Configuration

See Also

Help and Support

Microsoft TechNet

Deployment and Resource Kits

List of Common Administrative Tasks

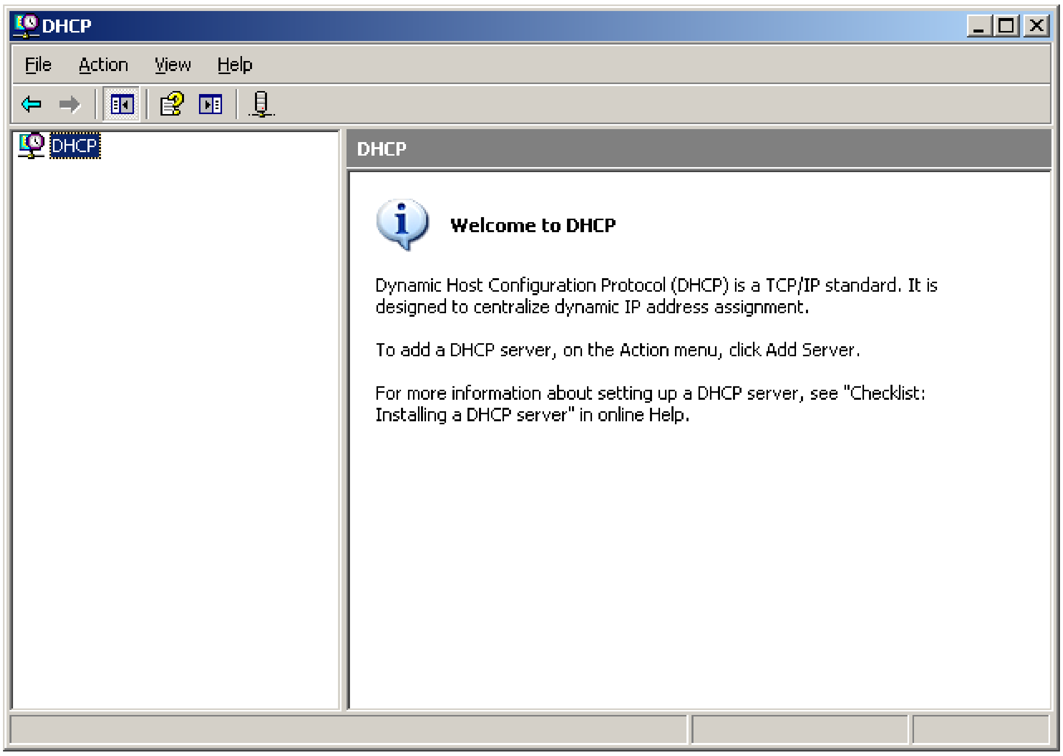
Windows Server Communities

What's New

Strategic Technology Protection Program

Step 3 Enter the main page of the DHCP, as shown in the following figure. as shown in Figure 5-31.

Figure 5-31 The main page of the DHCP



Welcome to DHCP

Dynamic Host Configuration Protocol (DHCP) is a TCP/IP standard. It is designed to centralize dynamic IP address assignment.

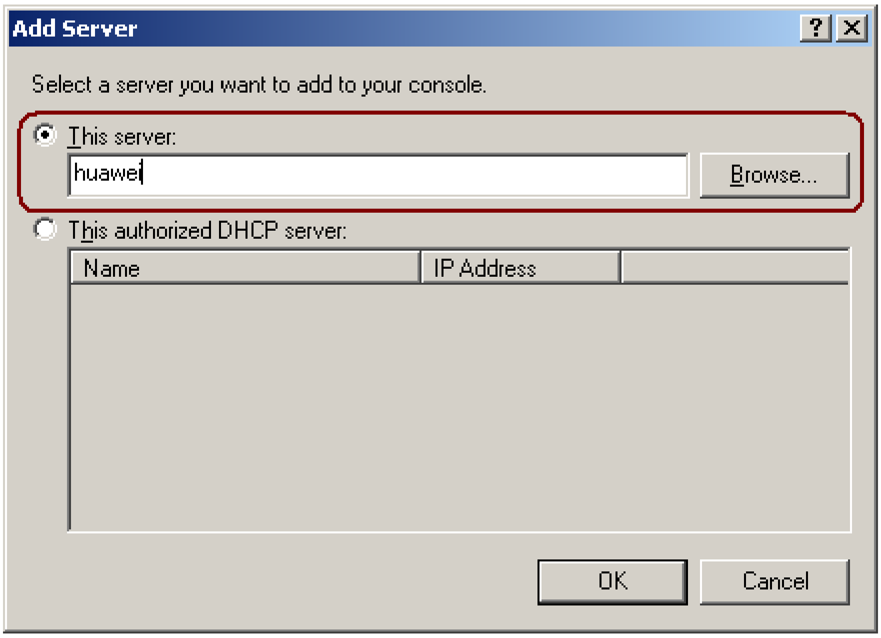
To add a DHCP server, on the Action menu, click Add Server.

For more information about setting up a DHCP server, see "Checklist: Installing a DHCP server" in online Help.

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

The **Add Server** dialog box is displayed. as shown in Figure 5-32.

Figure 5-32 Add Server



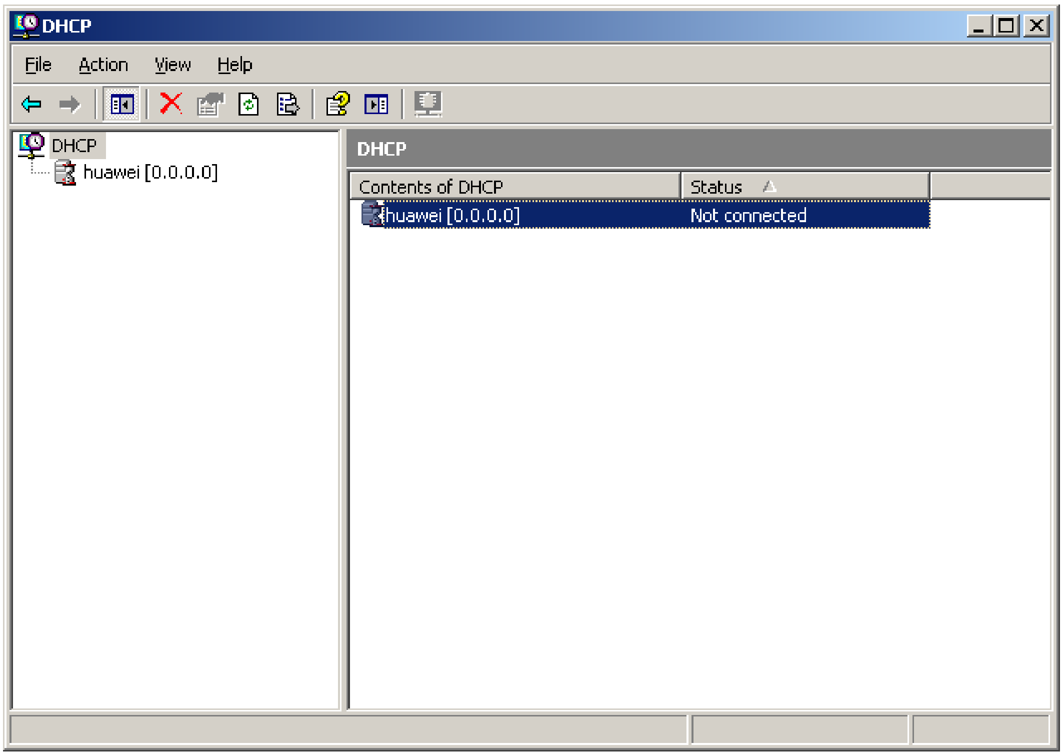
Select a server you want to add to your console.

● This server: huawei

○ This authorized DHCP server:

Step 5 Set the name of the DHCP server randomly, and then click **OK**. If the setting is successful, the page shown in the following figure is displayed. as shown in Figure 5-33.

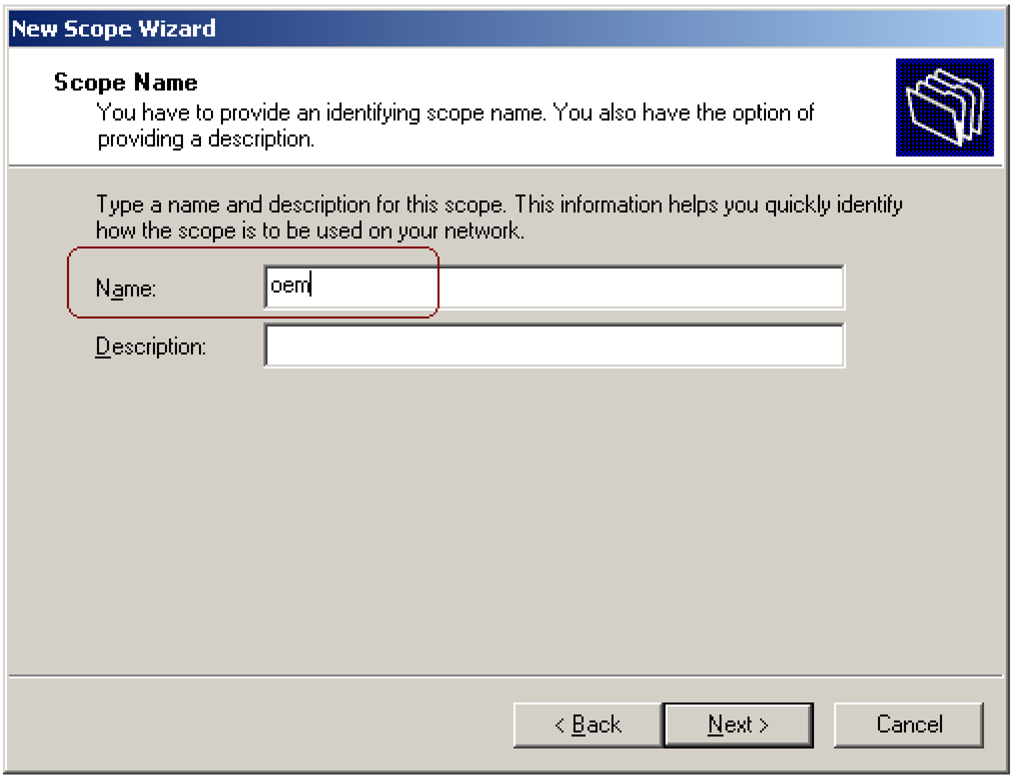
Figure 5-33 Setting Server



Contents of DHCP	Status
huawei [0.0.0.0]	Not connected

Step 6 Right-click **Huawei[10.10.10.2]** and choose **New Scope**. In the **New Scope Wizard** dialog box that is displayed, click **Next**.A dialog box is displayed, as shown in the following figure. as shown in Figure 5-34.

Figure 5-34 New Scope Wizard



Scope Name

You have to provide an identifying scope name. You also have the option of providing a description.

Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

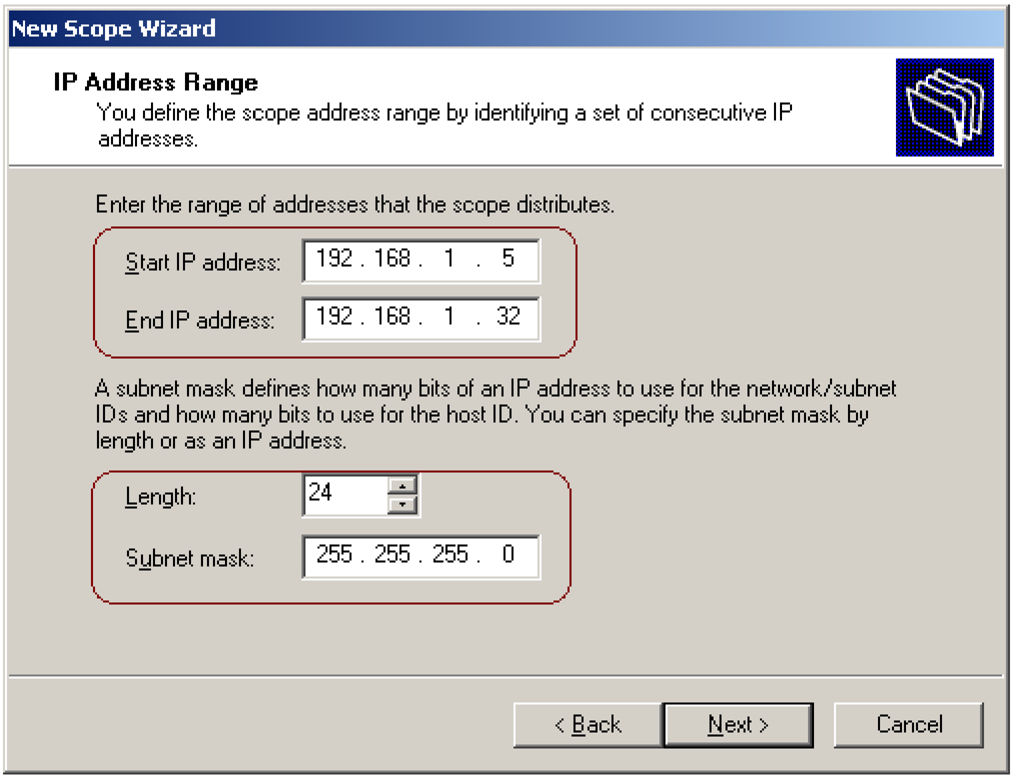
Name: oem

Description:

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

The following dialog box is displayed. as shown in Figure 5-35.

Figure 5-35 Set the name of the new function domain



IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.

Enter the range of addresses that the scope distributes.

Start IP address: 192 . 168 . 1 . 5

End IP address: 192 . 168 . 1 . 32

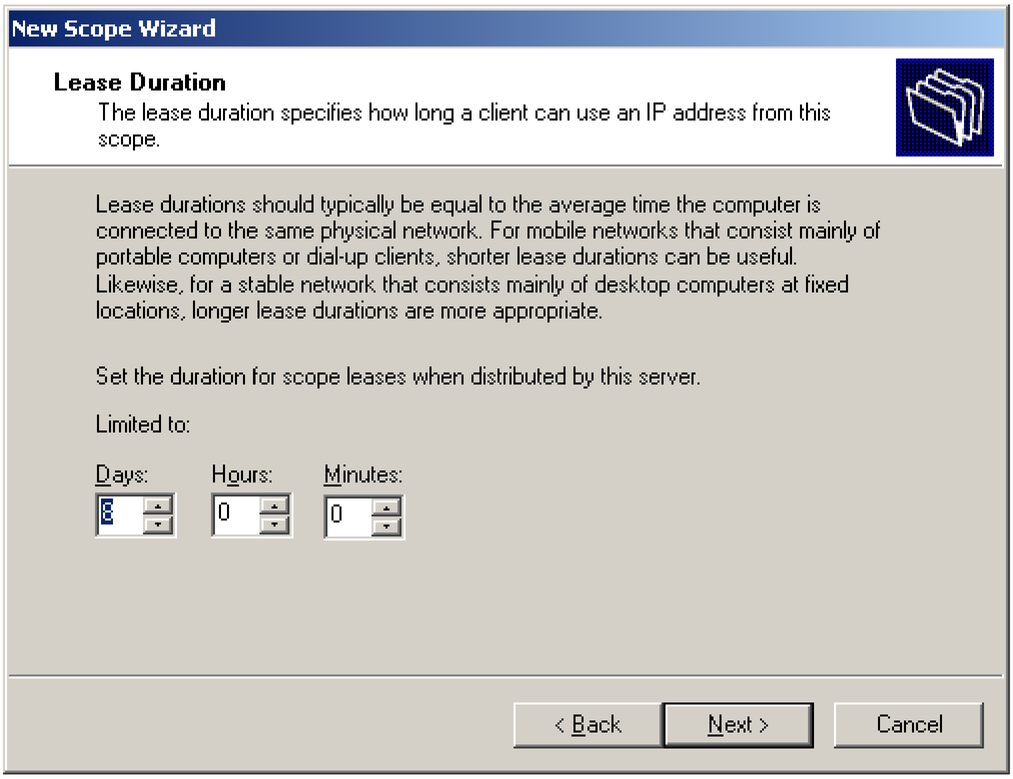
A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.

Length: 24

Subnet mask: 255 . 255 . 255 . 0

Step 8 In the preceding dialog box, set the start and end IP addresses provided by the DHCP server, and set the subnet mask. Then click **Next** repeatedly until the **Lease Duration** dialog box is displayed, as shown in the following figure. as shown in Figure 5-36.

Figure 5-36 Lease Duration



New Scope Wizard

Lease Duration

The lease duration specifies how long a client can use an IP address from this scope.

Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

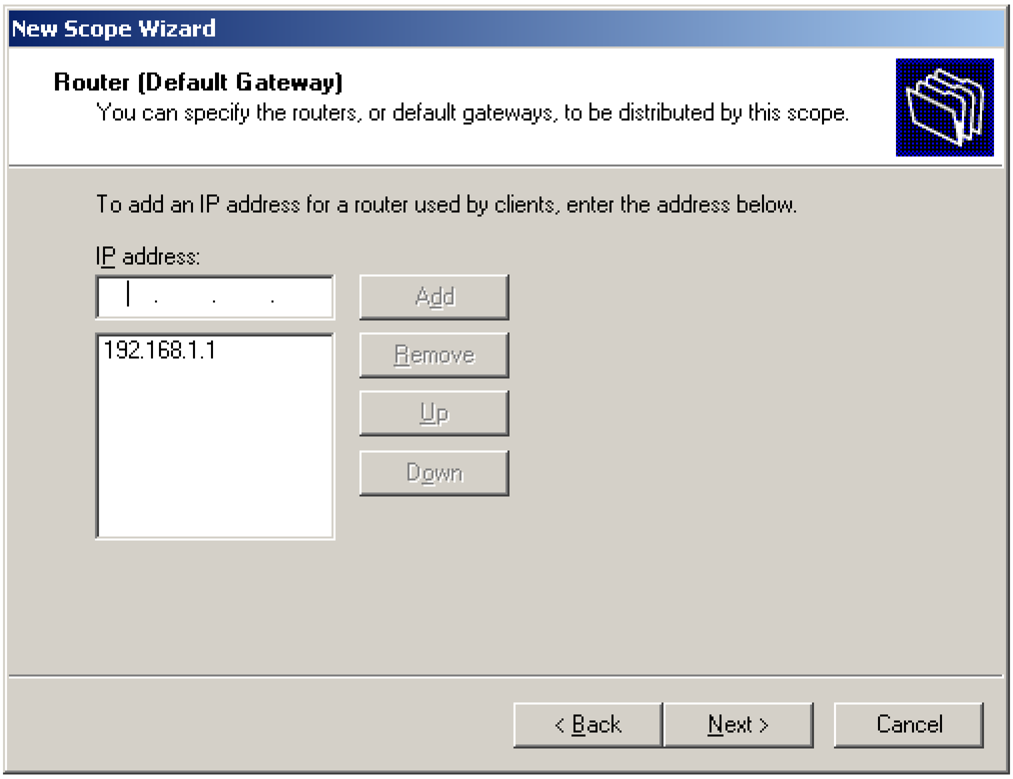
Set the duration for scope leases when distributed by this server.

Limited to:

Days: 8 Hours: 0 Minutes: 0

Step 9 In the **Lease Duration** dialog box, you can set the lease period of the DHCP server. By default, the lease period of the DHCP server is eight days. After the setting, click **Next** repeatedly until the **Router(Default Gateway)** dialog box is displayed, as shown in the following figure. as shown in Figure 5-37.

Figure 5-37 Router(Default Gateway)



New Scope Wizard

Router (Default Gateway)

You can specify the routers, or default gateways, to be distributed by this scope.

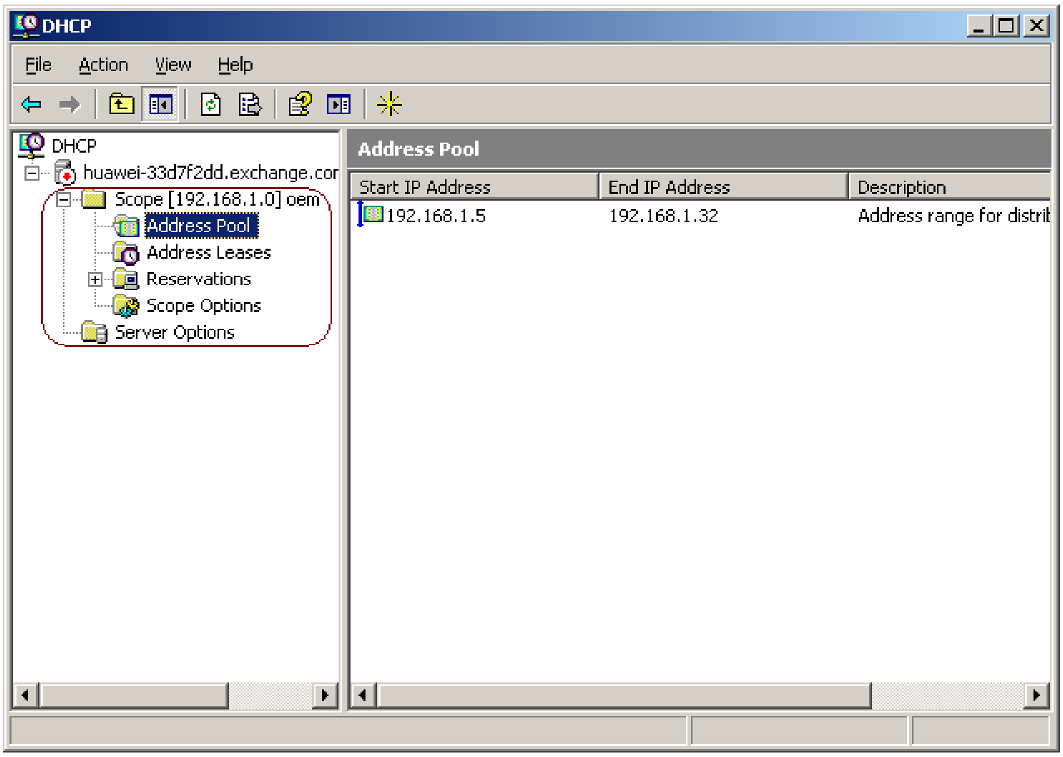
To add an IP address for a router used by clients, enter the address below.

IP address:

192.168.1.1

Step 10 Set the gateway address provided by the DHCP server. When an IP phone obtains the IP address from the DHCP server, the DHCP server provides the IP address and gateway address for the IP phone. After the setting is complete, click **Next** repeatedly until the setting is complete. Then the page shown in the following figure is displayed. You can view the IP address pool information on it. as shown in Figure 5-38.

Figure 5-38 Complete the DHCP server



DHCP
huawei-33d7f2dd.exchange.cor
Scope [192.168.1.0] oem
Address Pool
Address Leases
Reservations
Scope Options
Server Options

Address Pool

Start IP Address	End IP Address	Description
192.168.1.5	192.168.1.32	Address range for distrit

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

----End

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.

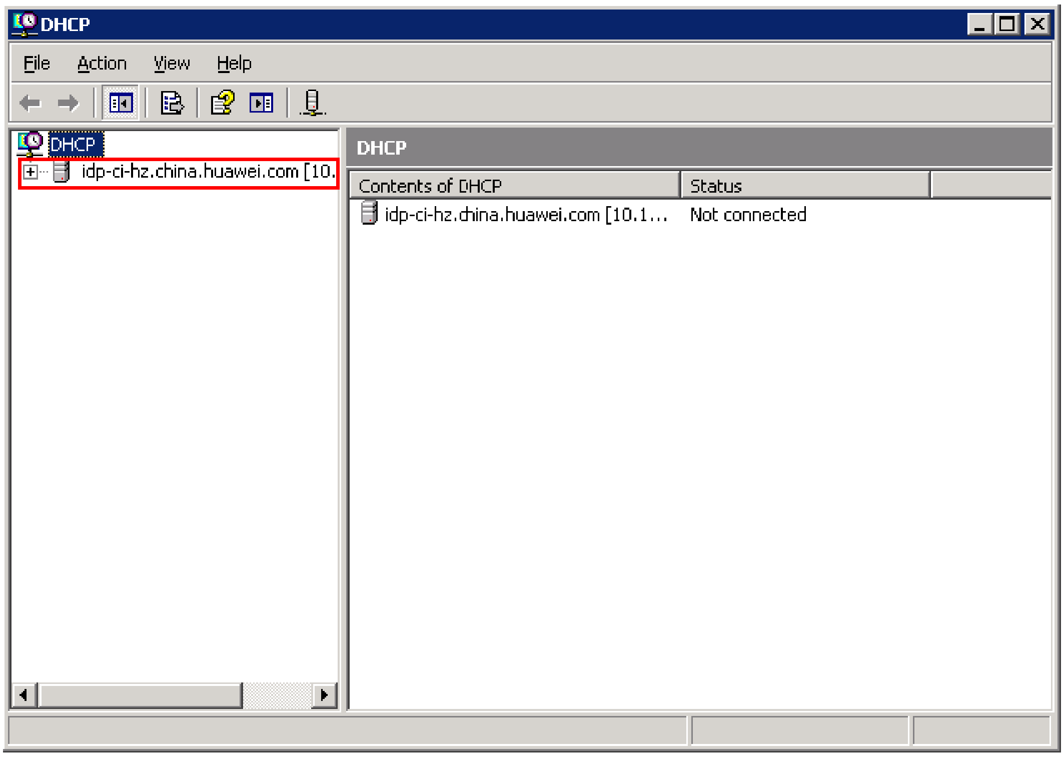
Procedure

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 5-39.

Figure 5-39 DHCP window

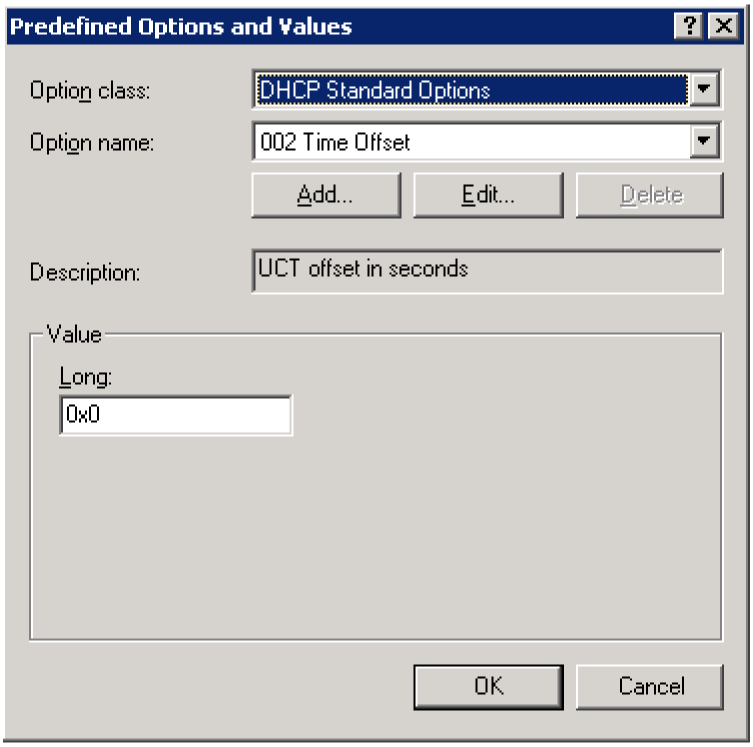


Contents of DHCP	Status
idp-ci-hz.china.huawei.com [10.1...	Not connected

3. Right-click the record framed in red in Figure 5-39 and choose **Configure the Predefined Options** from the shortcut menu.

   The **Predefined Options and Values** dialog box is displayed, as shown in Figure 5-40.

Figure 5-40 Predefined Options and Values dialog box



Option class: DHCP Standard Options

Option name: 002 Time Offset

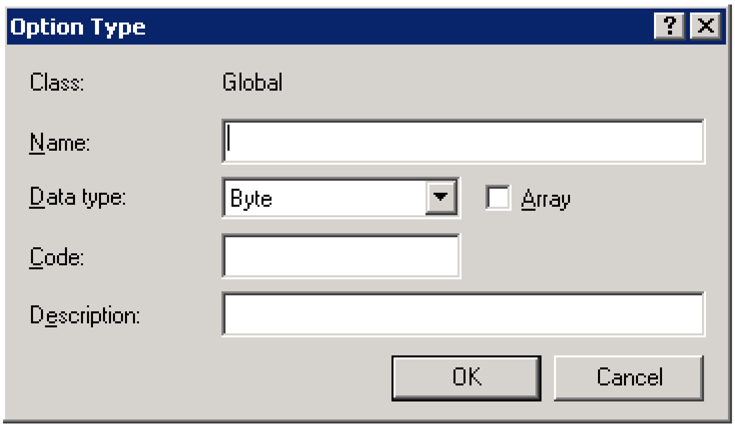
Description: UCT offset in seconds

Long: 0x0

4. Click **Add**.

   The **Option Type** dialog box is displayed, as shown in Figure 5-41.

Figure 5-41 Option Type dialog box



Class: Global

Name:

Data type: Byte □ Array

Code:

Description:

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**.

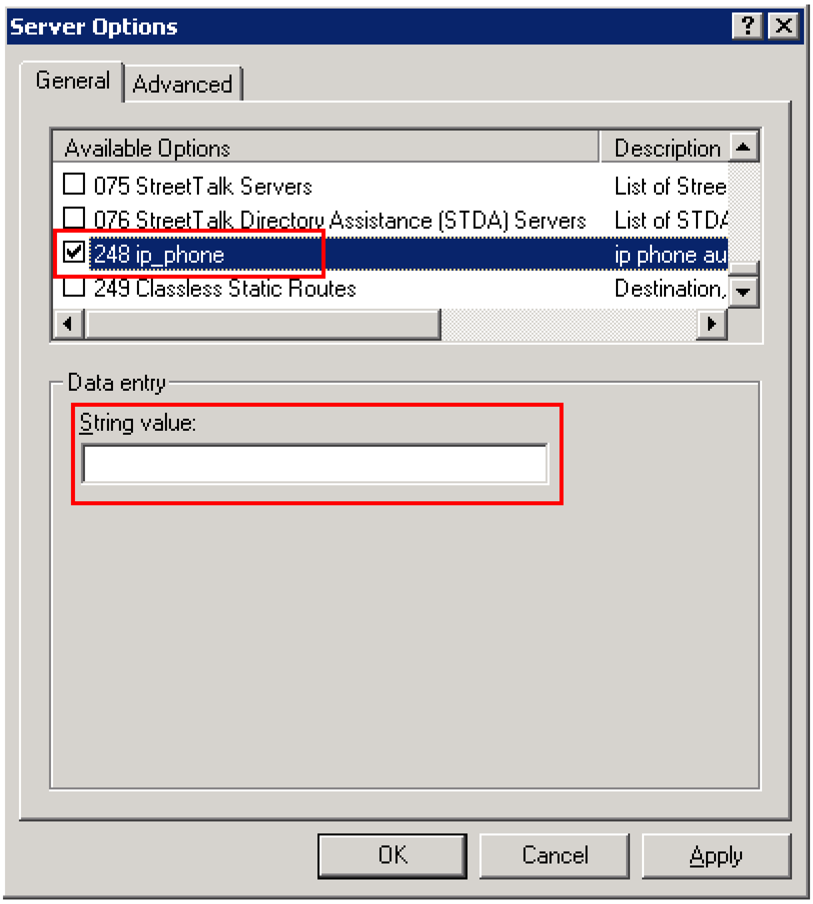
   The system returns to the **DHCP** window.

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 5-42.

Figure 5-42 Server Options



Available Options	Description
□ 075 StreetTalk Servers	List of Stree
□ 076 StreetTalk Directory Assistance (STDA) Servers	List of STDA
☑ 248 ip_phone	ip phone au
□ 249 Classless Static Routes	Destination,

Data entry

String value:

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 Wireshark User Guide

5.9.1 Tool Introduction

Obtaining Method

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

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

User

Onsite engineers and R&D personnel.

Function

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

Application Scenario

Analyzing the CAF or SCP signaling is required.

Function Description

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

The Wireshark provides the following functions:

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

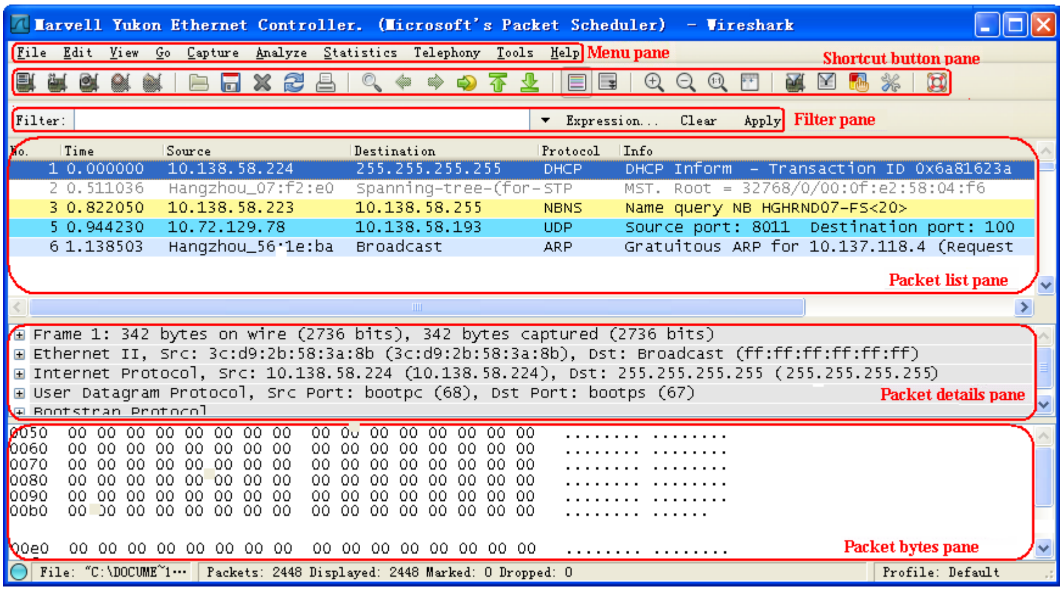
5.9.2 Common Operations and Menus

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

Wireshark Main Page

The Wireshark main page consists of six panes: menu pane, shortcut button pane, filter pane, packet list pane, packet details pane, and packet bytes pane, as shown in Figure 5-43.

Figure 5-43 Wireshark main page


Marvell Yukon Ethernet Controller. (Microsoft's Packet Scheduler) - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Menu pane
Shortcut button pane
Filter:
Expression... Clear Apply
Filter pane
Packet list pane
Packet details pane
Packet bytes pane

```
No.   Time       Source              Destination          Protocol  Info
    1 0.000000   10.138.58.224       255.255.255.255      DHCP      DHCP Inform  - Transaction ID 0x6a81623a
    2 0.511036   Hangzhou_07:f2:e0   Spanning-tree-(for-  STP       MST. Root = 32768/0/00:0f:e2:58:04:f6
    3 0.822050   10.138.58.223       10.138.58.255        NBNS      Name query NB HGHRND07-FS<20>
    5 0.944230   10.72.129.78        10.138.58.193        UDP       Source port: 8011  Destination port: 100
    6 1.138503   Hangzhou_56:1e:ba   Broadcast            ARP       Gratuitous ARP for 10.137.118.4 (Request

⊞ Frame 1: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
⊞ Ethernet II, Src: 3c:d9:2b:58:3a:8b (3c:d9:2b:58:3a:8b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol, Src: 10.138.58.224 (10.138.58.224), Dst: 255.255.255.255 (255.255.255.255)
⊞ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
⊞ Bootstrap Protocol

0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ......

00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........

File: "C:\DOCUME~1…   Packets: 2448 Displayed: 2448 Marked: 0 Dropped: 0   Profile: Default
```

Menu Pane

The menu pane contains the following menus:

- File

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

- Edit

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

- View

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

- Go

  Contains items to go to a specific packet.

- Capture

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

- Analyze

  Allows you to enable or disable protocol dissectors.

- Statistics

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

- Telephony

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

- Tools

Contains two items: Firewall ACL Rules and Lua.

- Help

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

Shortcut Button Pane

Lists the shortcut buttons for common functions.

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

Filter Pane

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

Packet List Pane

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

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

NOTE

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

Packet Details Pane

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

Packet Bytes Pane

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

Common Operations

Context

CAUTION

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

Procedure

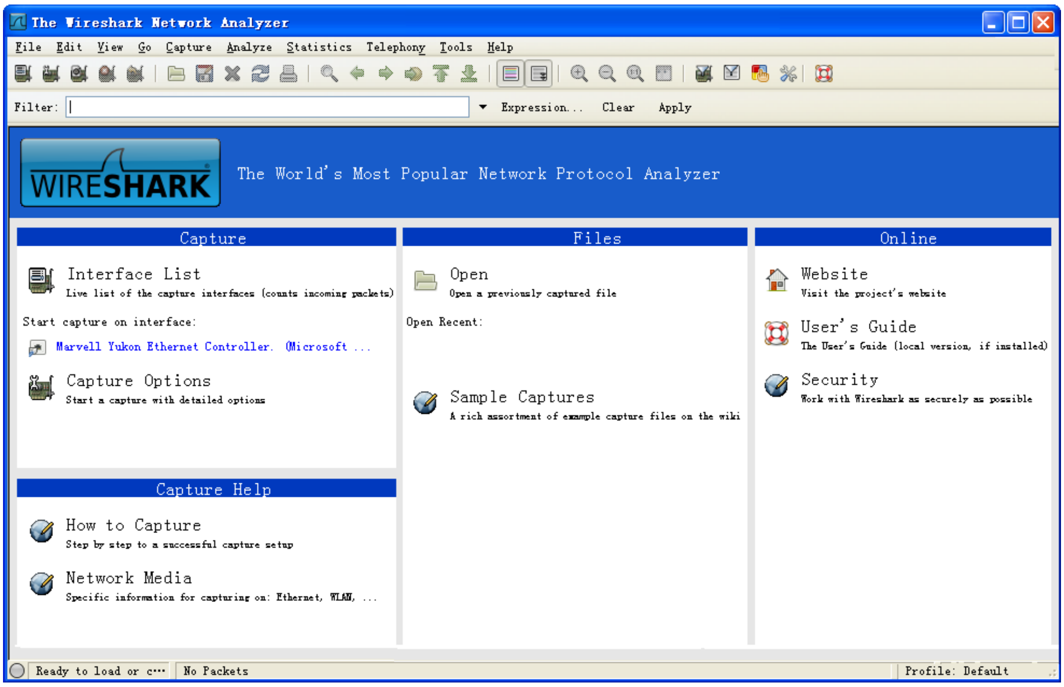
Step 1 Set monitoring and mirroring ports on the switch.

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

Step 2 Double-click to start the Wireshark.

The Wireshark main page is displayed, as shown in Figure 5-44.

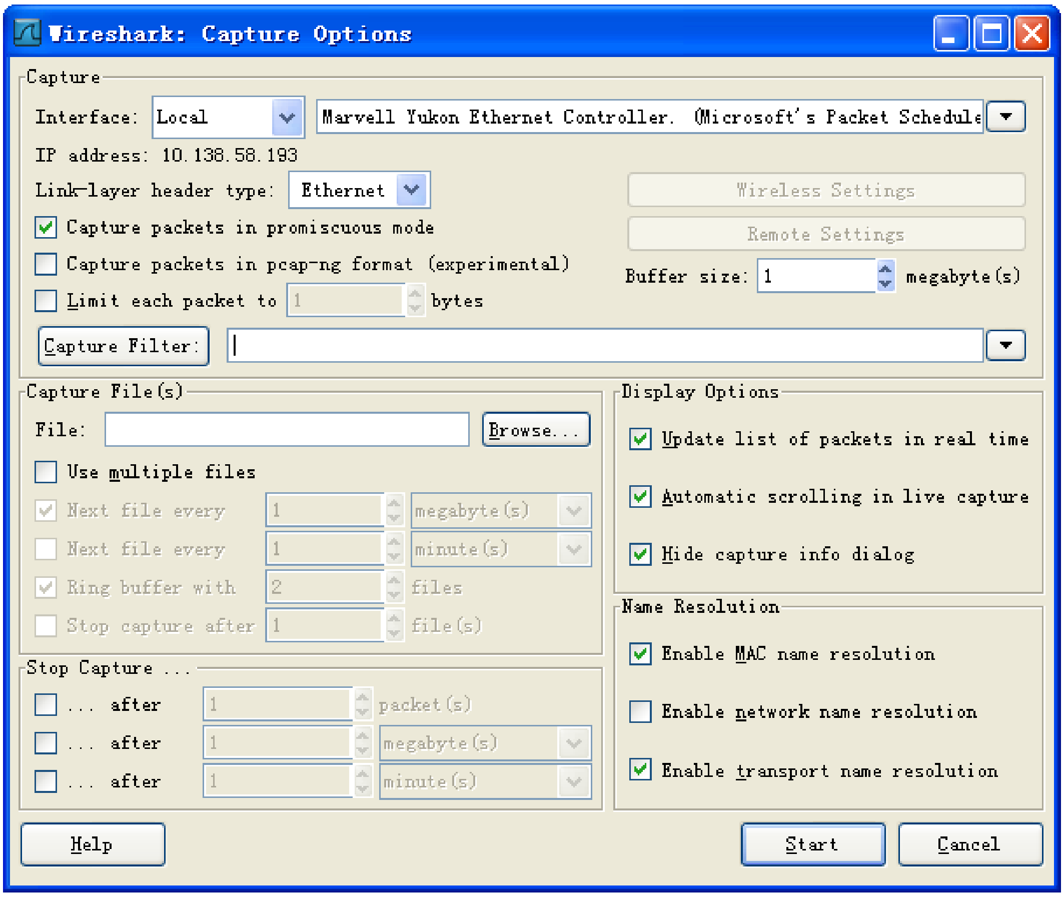
Figure 5-44 Wireshark main page


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Capture
Interface List
Live list of the capture interfaces (counts incoming packets)
Start capture on interface:
Marvell Yukon Ethernet Controller. (Microsoft ...
Capture Options
Start a capture with detailed options
Files
Open
Open a previously captured file
Open Recent:
Sample Captures
A rich assortment of example capture files on the wiki
Online
Website
Visit the project's website
User's Guide
The User's Guide (local version, if installed)
Security
Work with Wireshark as securely as possible
Capture Help
How to Capture
Step by step to a successful capture setup
Network Media
Specific information for capturing on: Ethernet, WLAN, ...
Ready to load or c···
No Packets
Profile: Default

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

The **Capture Options** page is displayed, as shown in Figure 5-45.

Figure 5-45 Wireshark: Capture Options page



Wireshark: Capture Options

Capture

Interface: Local | Marvell Yukon Ethernet Controller. (Microsoft's Packet Schedule

IP address: 10.138.58.193

Link-layer header type: Ethernet

☑ Capture packets in promiscuous mode

□ Capture packets in pcap-ng format (experimental)

□ Limit each packet to 1 bytes

Capture Filter: |

Buffer size: 1 megabyte(s)

Capture File(s)

File:

□ Use multiple files

☑ Next file every 1 megabyte(s)

□ Next file every 1 minute(s)

☑ Ring buffer with 2 files

□ Stop capture after 1 file(s)

Stop Capture ...

□ ... after 1 packet(s)

□ ... after 1 megabyte(s)

□ ... after 1 minute(s)

Display Options

☑ Update list of packets in real time

☑ Automatic scrolling in live capture

☑ Hide capture info dialog

Name Resolution

☑ Enable MAC name resolution

□ Enable network name resolution

☑ Enable transport name resolution

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

- Capture
  - Interface

    Specifies the network adapter for capturing packets.

CAUTION

After the Wireshark is installed, the system automatically generates a logical network adapter. In addition to the logical network adapter, a physical network adapter is required, as shown in Figure 5-45. During the actual packet capture, select a correct physical network adapter, especially for a host with multiple network adapters. A physical network adapter will be displayed in the drop-down list box only after the WinPcap is installed.

  - Capture Filter

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

    Table 5-4 describes the filter criteria categories specified by **Capture Filter**.

Table 5-4 Filter criteria categories specified by Capture Filter

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

- Capture File(s)

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

  - File

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

  - Use multiple files

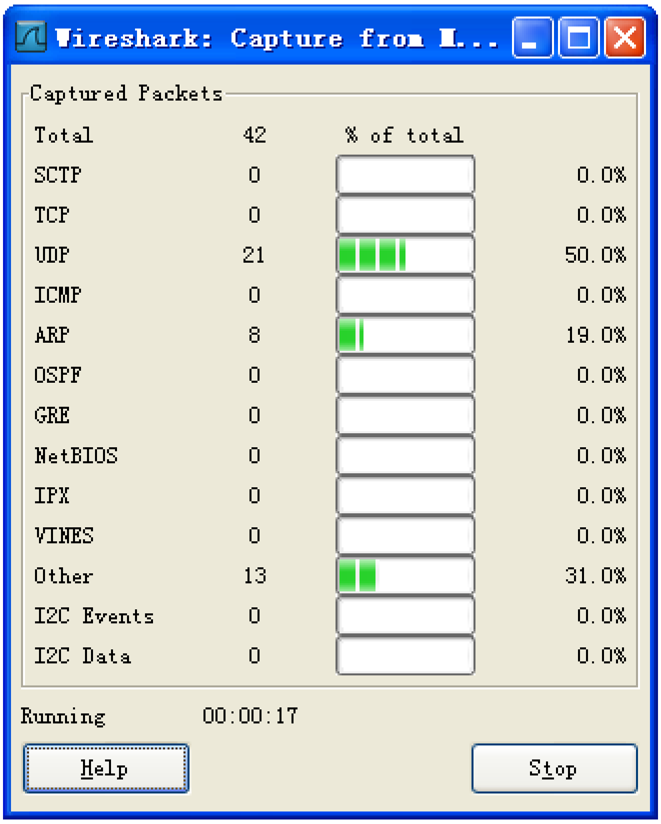
    Set the parameters to specify the way of creating files for saving captured data packets.

- Display Options

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

  - Select **Update list of packets in real time**. The packet list is displayed on the Wireshark main page.
  - Select **Automatic scrolling in live capture**. If the captured results exceed one screen, the results are displayed in automatic scrolling mode.
  - Deselect **Hide capture info dialog**. The **Captured Packets** page shown in Figure 5-46 is displayed during the packet capture, with the real-time information about the numbers of captured packets of various protocols.

Figure 5-46 Captured Packets page



Captured Packets

Total	42	% of total
SCTP	0	0.0%
TCP	0	0.0%
UDP	21	50.0%
ICMP	0	0.0%
ARP	8	19.0%
OSPF	0	0.0%
GRE	0	0.0%
NetBIOS	0	0.0%
IPX	0	0.0%
VINES	0	0.0%
Other	13	31.0%
I2C Events	0	0.0%
I2C Data	0	0.0%

Running 00:00:17

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

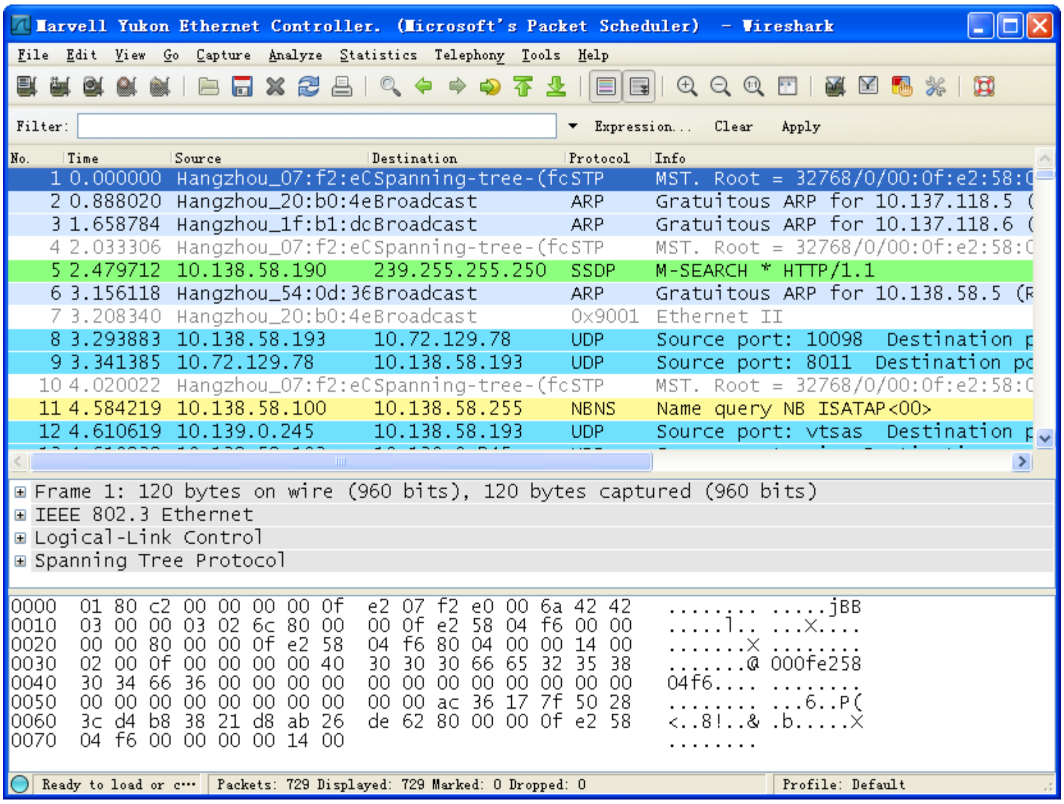
The Wireshark starts to capture packets.

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

Step 6 Choose **Capture** > **Stop** or click **Stop** in Figure 5-46.

The **Capture result** page is displayed, as show in Figure 5-47.

Figure 5-47 Capture result


Marvell Yukon Ethernet Controller. (Microsoft's Packet Scheduler) - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression...
Clear
Apply

```
No.  Time     Source              Destination         Protocol Info
   1 0.000000 Hangzhou_07:f2:eCSpanning-tree-(fcSTP     MST. Root = 32768/0/00:0f:e2:58:0
   2 0.888020 Hangzhou_20:b0:4eBroadcast          ARP      Gratuitous ARP for 10.137.118.5 (
   3 1.658784 Hangzhou_1f:b1:dcBroadcast          ARP      Gratuitous ARP for 10.137.118.6 (
   4 2.033306 Hangzhou_07:f2:eCSpanning-tree-(fcSTP     MST. Root = 32768/0/00:0f:e2:58:0
   5 2.479712 10.138.58.190     239.255.255.250   SSDP     M-SEARCH * HTTP/1.1
   6 3.156118 Hangzhou_54:0d:36Broadcast          ARP      Gratuitous ARP for 10.138.58.5 (R
   7 3.208340 Hangzhou_20:b0:4eBroadcast          0x9001   Ethernet II
   8 3.293883 10.138.58.193     10.72.129.78      UDP      Source port: 10098  Destination p
   9 3.341385 10.72.129.78      10.138.58.193     UDP      Source port: 8011  Destination po
  10 4.020022 Hangzhou_07:f2:eCSpanning-tree-(fcSTP     MST. Root = 32768/0/00:0f:e2:58:0
  11 4.584219 10.138.58.100     10.138.58.255     NBNS     Name query NB ISATAP<00>
  12 4.610619 10.139.0.245      10.138.58.193     UDP      Source port: vtsas  Destination p
```

```
⊞ Frame 1: 120 bytes on wire (960 bits), 120 bytes captured (960 bits)
⊞ IEEE 802.3 Ethernet
⊞ Logical-Link Control
⊞ Spanning Tree Protocol
```

```
0000  01 80 c2 00 00 00 00 0f  e2 07 f2 e0 00 6a 42 42   ........ .....jBB
0010  03 00 00 03 02 6c 80 00  00 0f e2 58 04 f6 00 00   .....l.. ...X....
0020  00 00 80 00 00 0f e2 58  04 f6 80 04 00 00 14 00   .......X ........
0030  02 00 0f 00 00 00 00 40  30 30 30 66 65 32 35 38   .......@ 000fe258
0040  30 34 66 36 00 00 00 00  00 00 00 00 00 00 00 00   04f6.... ........
0050  00 00 00 00 00 00 00 00  00 00 ac 36 17 7f 50 28   ........ ...6..P(
0060  3c d4 b8 38 21 d8 ab 26  de 62 80 00 00 0f e2 58   <..8!..& .b.....X
0070  04 f6 00 00 00 00 14 00                            ........
```

Ready to load or c... Packets: 729 Displayed: 729 Marked: 0 Dropped: 0 Profile: Default

NOTE

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

Step 7 Save the data packet capturing results.

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

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

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

NOTE

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

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

----End

5.9.3 Filter Rules

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

NOTE

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

Filter Expression Rules

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

Comparison Symbols

The Wireshark can use comparison symbols (English words or operators) to form filter expressions. Table 5-5 describes the comparison symbols used in filter expressions.

Table 5-5 Comparison symbols used in filter expressions

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

Logical Operators

The Wireshark can use logical operators to combine multiple filter expressions. For example, if you want to filter out packets that are transmitted using the GPRS tunneling protocol (GTP) and through the IP address 10.138.21.5, use the filter expression gtp && ip.addr==10.138.21.5. Table 5-6 describes the logical operators used in filter expressions.

Table 5-6 Logical operators used in filter expressions

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

Setting Protocol Fields

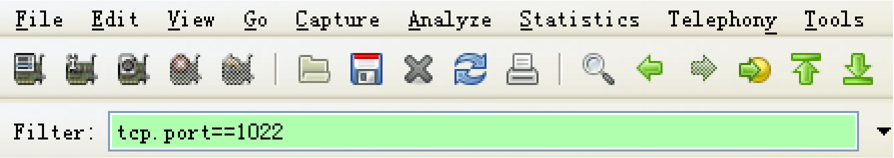
To set the protocol fields, proceed as follows:

1. Set filter criteria.

   - Enter the protocol fields in the **Filter** text box.

     For example, if you want to filter out TCP packets that are transmitted through port 1022, enter **tcp.port==1022**, as shown in Figure 5-48.

Figure 5-48 Protocol field example


File Edit View Go Capture Analyze Statistics Telephony Tools

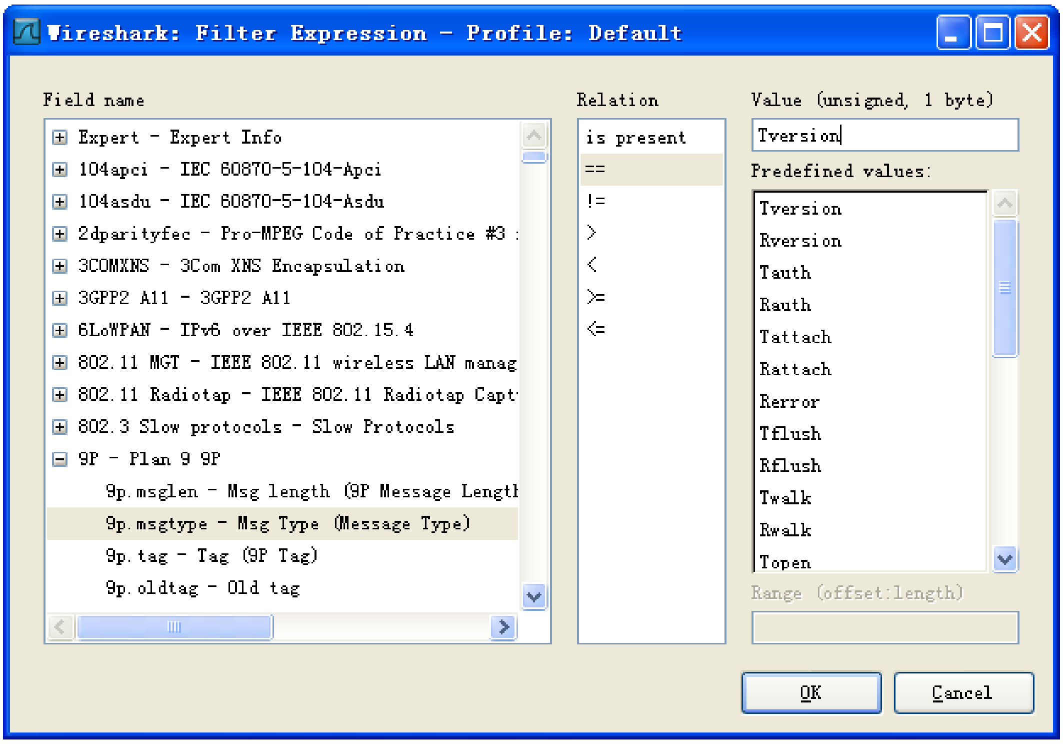
Filter: tcp.port==1022

   - Customize filter expressions.

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

   The **Wireshark: Filter Expression** dialog box is displayed, as shown in Figure 5-49.

Figure 5-49 Wireshark: Filter Expression



Wireshark: Filter Expression - Profile: Default

Field name: 9p.msgtype - Msg Type (Message Type)

Relation: ==

Value (unsigned, 1 byte): Tversion

Expert - Expert Info
104apci - IEC 60870-5-104-Apci
104asdu - IEC 60870-5-104-Asdu
2dparityfec - Pro-MPEG Code of Practice #3 :
3COMXNS - 3Com XNS Encapsulation
3GPP2 A11 - 3GPP2 A11
6LoWPAN - IPv6 over IEEE 802.15.4
802.11 MGT - IEEE 802.11 wireless LAN manag
802.11 Radiotap - IEEE 802.11 Radiotap Capt
802.3 Slow protocols - Slow Protocols
9P - Plan 9 9P
9p.msglen - Msg length (9P Message Lengtl
9p.msgtype - Msg Type (Message Type)
9p.tag - Tag (9P Tag)
9p.oldtag - Old tag
is present
==
!=
>
<
>=
<=
Predefined values:
Tversion
Rversion
Tauth
Rauth
Tattach
Rattach
Rerror
Tflush
Rflush
Twalk
Rwalk
Topen
Range (offset:length)
OK
Cancel

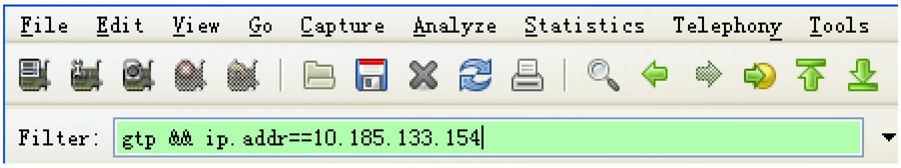
b. Select a field, select a relation, and then enter a value in the **Value (IPv4 address)** test box, as shown in Figure 5-49.

c. Click **OK**.

Check whether a filter expression is correct.

– If the filter expression is correct, the background color of the **Filter** text box is green, as shown in Figure 5-50.

Figure 5-50 Displayed Filter text box if the filter expression is correct

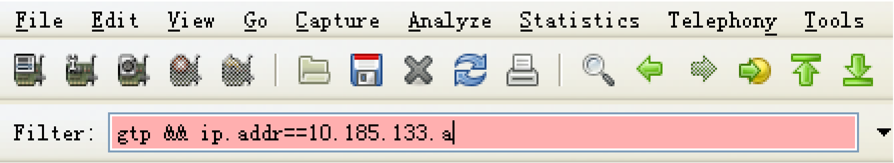


Filter: gtp && ip.addr==10.185.133.154

File Edit View Go Capture Analyze Statistics Telephony Tools

– If the filter expression is incorrect, the background color of the **Filter** text box is dark pink, as shown in Figure 5-51.

Figure 5-51 Displayed Filter text box if the filter expression is incorrect



Filter: gtp && ip.addr==10.185.133.a

File Edit View Go Capture Analyze Statistics Telephony Tools

2. Press **Enter** or click **Apply**.

   The packets that meet the filter criteria are displayed.

Common Filter Expressions

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

- Filter expressions that specify protocols
  - ip
  - icmp
  - tcp
  - gtp
  - gre
  - http
- Filter expressions that specify addresses
  - IP address

    ip.addr==10.161.225.1
  - Source IP address

    ip.src==10.161.225.1
  - Destination IP address

    ip.dst==10.161.225.1
  - Source Media Access Control (MAC) address

    eth.src == 00:e0:fc:44:5e:a1
  - Source User Datagram Protocol (UDP) port

    udp.srcport == 2123
- Filter expressions that specify fields (message types)
  - GTP Echo Request messages

    gtp.message == 0x01
  - Remote authentication dial-in user service (RADIUS) accounting request or response messages

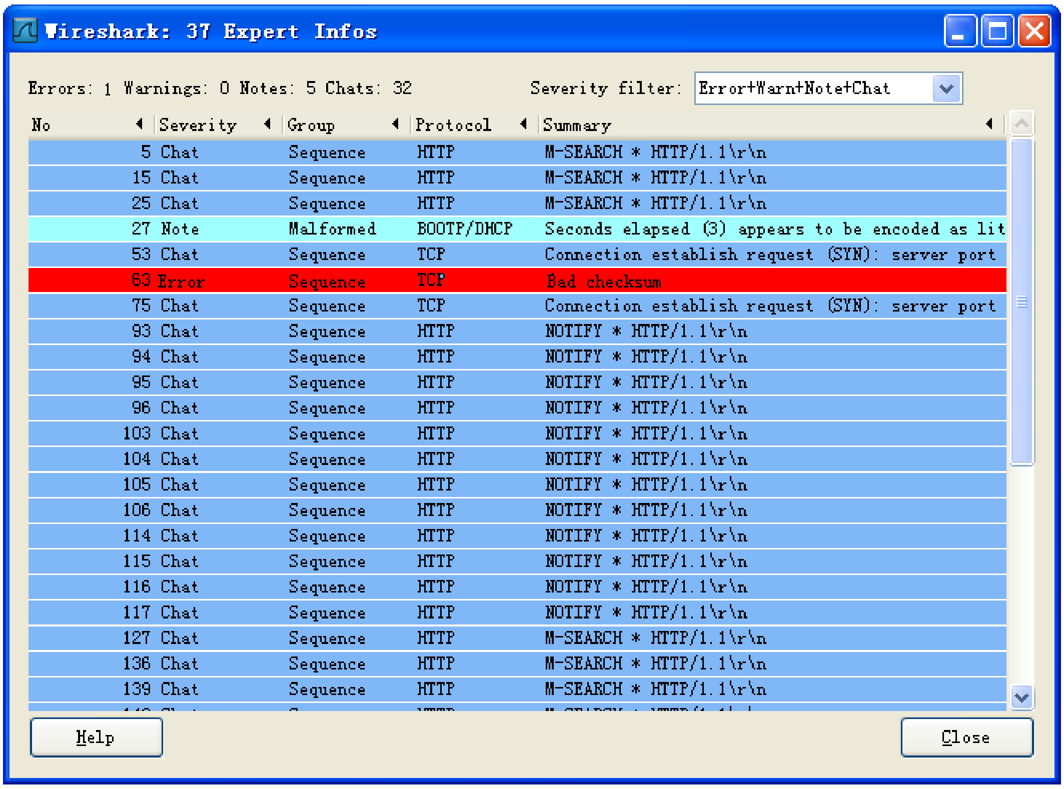
    radius.code == 4 || radius.code == 5

Filtering Segment Packets

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

Choose **Analyze** > **Expert Info**. If `TCP Bad checksum` is displayed, segment packets may exist, as shown in Figure 5-52. The Wireshark does not combine segment packets or verify that `Checksum` is correct. Therefore, `Bad checksum` is displayed.

Figure 5-52 Suspicious packets displayed on the Expert Infos



Errors: 1 Warnings: 0 Notes: 5 Chats: 32

Severity filter: Error+Warn+Note+Chat

No	Severity	Group	Protocol	Summary
5	Chat	Sequence	HTTP	M-SEARCH * HTTP/1.1\r\n
15	Chat	Sequence	HTTP	M-SEARCH * HTTP/1.1\r\n
25	Chat	Sequence	HTTP	M-SEARCH * HTTP/1.1\r\n
27	Note	Malformed	BOOTP/DHCP	Seconds elapsed (3) appears to be encoded as lit
53	Chat	Sequence	TCP	Connection establish request (SYN): server port
63	Error	Sequence	TCP	Bad checksum
75	Chat	Sequence	TCP	Connection establish request (SYN): server port
93	Chat	Sequence	HTTP	NOTIFY * HTTP/1.1\r\n
94	Chat	Sequence	HTTP	NOTIFY * HTTP/1.1\r\n
95	Chat	Sequence	HTTP	NOTIFY * HTTP/1.1\r\n
96	Chat	Sequence	HTTP	NOTIFY * HTTP/1.1\r\n
103	Chat	Sequence	HTTP	NOTIFY * HTTP/1.1\r\n
104	Chat	Sequence	HTTP	NOTIFY * HTTP/1.1\r\n
105	Chat	Sequence	HTTP	NOTIFY * HTTP/1.1\r\n
106	Chat	Sequence	HTTP	NOTIFY * HTTP/1.1\r\n
114	Chat	Sequence	HTTP	NOTIFY * HTTP/1.1\r\n
115	Chat	Sequence	HTTP	NOTIFY * HTTP/1.1\r\n
116	Chat	Sequence	HTTP	NOTIFY * HTTP/1.1\r\n
117	Chat	Sequence	HTTP	NOTIFY * HTTP/1.1\r\n
127	Chat	Sequence	HTTP	M-SEARCH * HTTP/1.1\r\n
136	Chat	Sequence	HTTP	M-SEARCH * HTTP/1.1\r\n
139	Chat	Sequence	HTTP	M-SEARCH * HTTP/1.1\r\n

NOTE

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

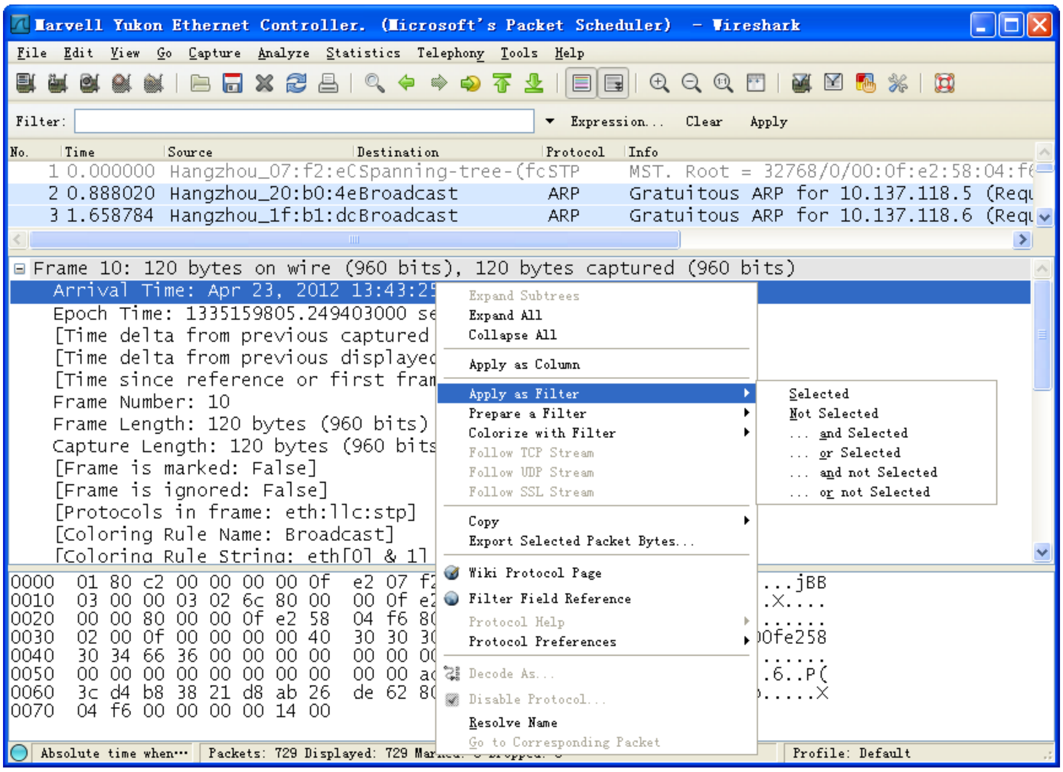
Filter Expression Construction Tips

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

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

   The field is set as a filter criterion and displayed in the **Filter** text box, and the corresponding data packets are displayed based on this expression, as shown in Figure 5-53.

Figure 5-53 Setting a field as a filter criterion and starting the filtering immediately



```
No.  Time       Source                  Destination            Protocol  Info
  1 0.000000   Hangzhou_07:f2:eCSpanning-tree-(fcSTP      MST. Root = 32768/0/00:0f:e2:58:04:f6
  2 0.888020   Hangzhou_20:b0:4eBroadcast          ARP      Gratuitous ARP for 10.137.118.5 (Requ
  3 1.658784   Hangzhou_1f:b1:dcBroadcast          ARP      Gratuitous ARP for 10.137.118.6 (Requ
```

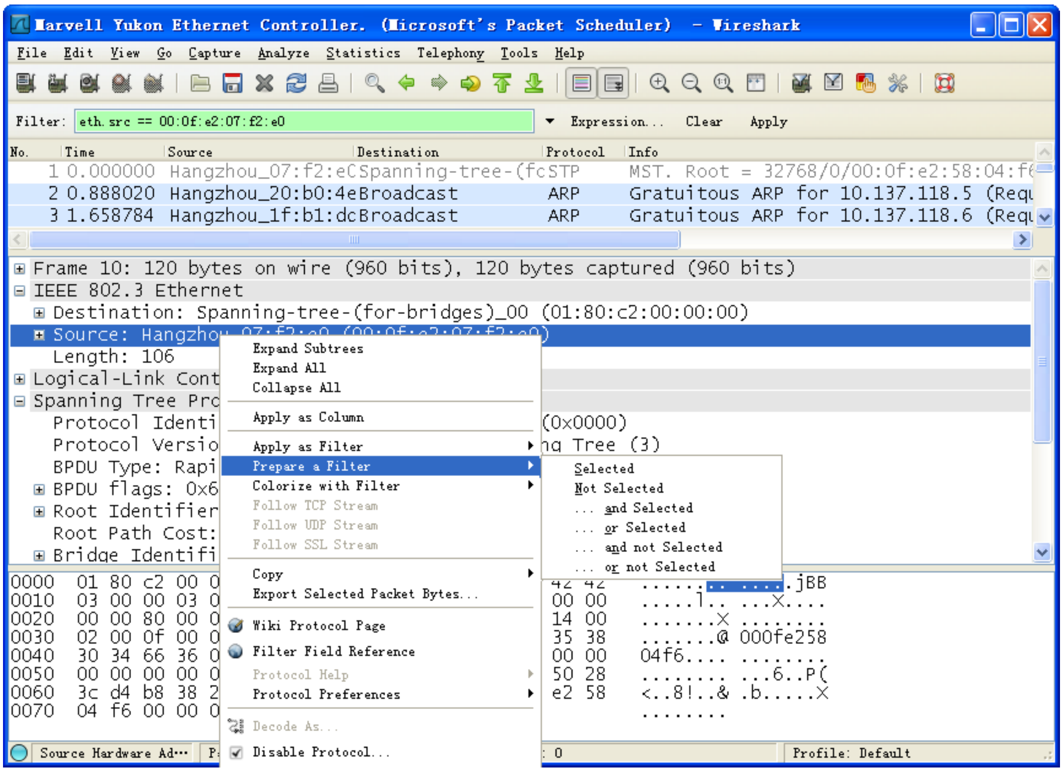
```
⊟ Frame 10: 120 bytes on wire (960 bits), 120 bytes captured (960 bits)
    Arrival Time: Apr 23, 2012 13:43:25
    Epoch Time: 1335159805.249403000 se
    [Time delta from previous captured
    [Time delta from previous displayed
    [Time since reference or first fran
    Frame Number: 10
    Frame Length: 120 bytes (960 bits)
    Capture Length: 120 bytes (960 bits
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:llc:stp]
    [Coloring Rule Name: Broadcast]
    [Coloring Rule String: eth[0] & 1]
```

```
0000  01 80 c2 00 00 00 00 0f  e2 07 f2             ...jBB
0010  03 00 00 03 02 6c 80 00  00 0f e2             .X....
0020  00 00 80 00 00 0f e2 58  04 f6 80             ......
0030  02 00 0f 00 00 00 00 40  30 30 30             )0fe258
0040  30 34 66 36 00 00 00 00  00 00 00             ......
0050  00 00 00 00 00 00 00 00  00 00 ac             .6..P(
0060  3c d4 b8 38 21 d8 ab 26  de 62 80             ).....X
0070  04 f6 00 00 00 00 14 00
```

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

- After you choose **Apply as Filter** > **Selected**, the selected field is set as the filter criterion directly and the data packets that meet the filter criterion are displayed immediately.
- After you choose **Prepare a Filter** > **Selected**, the selected field is displayed in the **Filter** text box but no filter is performed. You can modify the filter criterion as required. After you click **Apply**, data packets that meet the filter criterion are displayed, as shown in Figure 5-54.

Figure 5-54 Preparing to set a field as a filter criterion



Filter: eth.src == 00:0f:e2:07:f2:e0

```
No.  Time      Source              Destination         Protocol Info
   1 0.000000  Hangzhou_07:f2:eCSpanning-tree-(fcSTP      MST. Root = 32768/0/00:0f:e2:58:04:f6
   2 0.888020  Hangzhou_20:b0:4eBroadcast         ARP      Gratuitous ARP for 10.137.118.5 (Requ
   3 1.658784  Hangzhou_1f:b1:dcBroadcast         ARP      Gratuitous ARP for 10.137.118.6 (Requ
```

```
⊞ Frame 10: 120 bytes on wire (960 bits), 120 bytes captured (960 bits)
⊟ IEEE 802.3 Ethernet
  ⊞ Destination: Spanning-tree-(for-bridges)_00 (01:80:c2:00:00:00)
  ⊞ Source: Hangzhou_07:f2:e0 (00:0f:e2:07:f2:e0)
    Length: 106
⊞ Logical-Link Cont
⊟ Spanning Tree Pro
    Protocol Identi                                  (0x0000)
    Protocol Versio                                  ng Tree (3)
    BPDU Type: Rapi
  ⊞ BPDU flags: 0x6
  ⊞ Root Identifier
    Root Path Cost:
  ⊞ Bridge Identifi
```

```
0000  01 80 c2 00 0   42 42   ..............jBB
0010  03 00 00 03 0   00 00   .....l.. ...X....
0020  00 00 80 00 0   14 00   .......X ........
0030  02 00 0f 00 0   35 38   .......@ 000fe258
0040  30 34 66 36 0   00 00   04f6.... ........
0050  00 00 00 00 0   50 28   ........ ...6..P(
0060  3c d4 b8 38 2   e2 58   <..8!..& .b.....X
0070  04 f6 00 00 0           ........
```

5.9.4 Typical Scenario

SIP Protocol Analysis

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

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

Information in the Captured Packet List Window

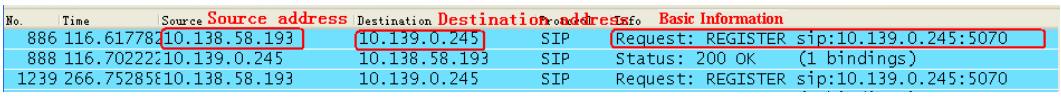
Figure 5-55 shows the information in the captured packet list window.

- Source address from which a signaling record is sent

  IP address of the host that sends the signaling record
- Destination address to which a signaling record is sent
- Basic information about a signaling record

  Whether the signaling is a request or a status message.

Figure 5-55 Information in the captured packet list window



```
No.  Time        Source         Destination    Protocol Info
 886 116.61778210.138.58.193   10.139.0.245   SIP      Request: REGISTER sip:10.139.0.245:5070
 888 116.70222210.139.0.245    10.138.58.193  SIP      Status: 200 OK      (1 bindings)
1239 266.75285810.138.58.193   10.139.0.245   SIP      Request: REGISTER sip:10.139.0.245:5070
```

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

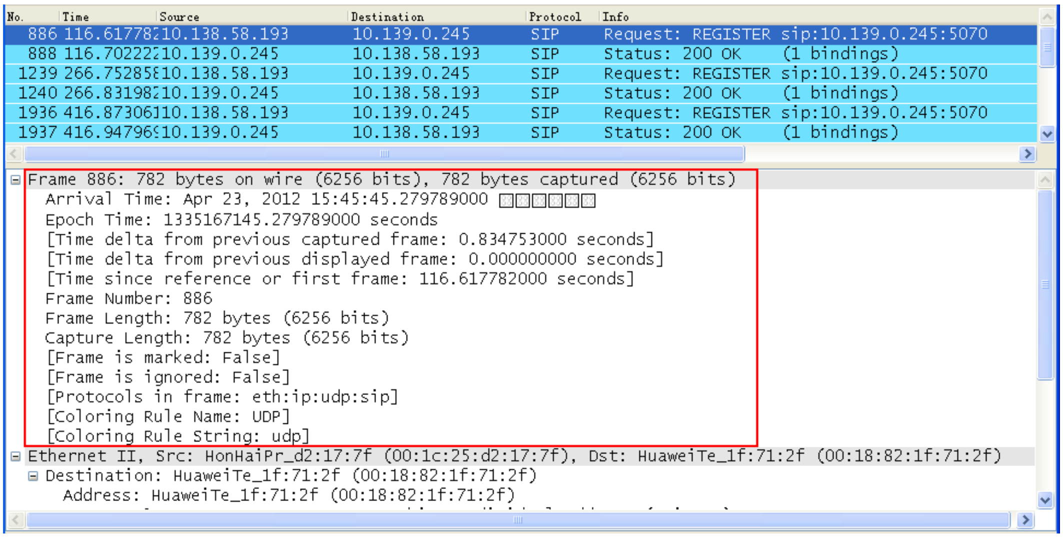
Information in the Protocol Layer Description Window

Pay attention to the information at the application layer.

- Physical layer

  The first layer in the protocol layer description window is the physical layer, which contains **Frame Number** and **Packet Length**, as shown in Figure 5-56.

Figure 5-56 Physical layer of the SIP protocol



```
No.  Time          Source          Destination     Protocol Info
 886 116.61778 10.138.58.193   10.139.0.245    SIP      Request: REGISTER sip:10.139.0.245:5070
 888 116.70222 10.139.0.245    10.138.58.193   SIP      Status: 200 OK     (1 bindings)
1239 266.75285 10.138.58.193   10.139.0.245    SIP      Request: REGISTER sip:10.139.0.245:5070
1240 266.83198 10.139.0.245    10.138.58.193   SIP      Status: 200 OK     (1 bindings)
1936 416.87306 10.138.58.193   10.139.0.245    SIP      Request: REGISTER sip:10.139.0.245:5070
1937 416.94796 10.139.0.245    10.138.58.193   SIP      Status: 200 OK     (1 bindings)

⊟ Frame 886: 782 bytes on wire (6256 bits), 782 bytes captured (6256 bits)
    Arrival Time: Apr 23, 2012 15:45:45.279789000 □□□□□□
    Epoch Time: 1335167145.279789000 seconds
    [Time delta from previous captured frame: 0.834753000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 116.617782000 seconds]
    Frame Number: 886
    Frame Length: 782 bytes (6256 bits)
    Capture Length: 782 bytes (6256 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ip:udp:sip]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
⊟ Ethernet II, Src: HonHaiPr_d2:17:7f (00:1c:25:d2:17:7f), Dst: HuaweiTe_1f:71:2f (00:18:82:1f:71:2f)
  ⊟ Destination: HuaweiTe_1f:71:2f (00:18:82:1f:71:2f)
      Address: HuaweiTe_1f:71:2f (00:18:82:1f:71:2f)
```

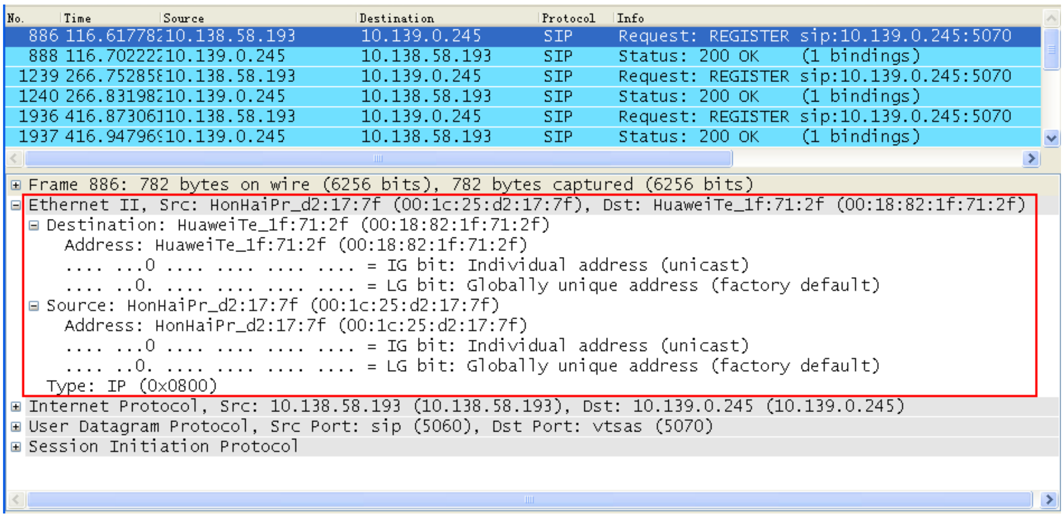
- Data link layer

  The second layer in the protocol layer description window is the data link layer, which contains the MAC address of the sender (**Source**), MAC address of the receiver (**Destination**), and packet type (**Type**), as shown in Figure 5-57.

NOTE

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

Figure 5-57 Data link layer of the SIP protocol

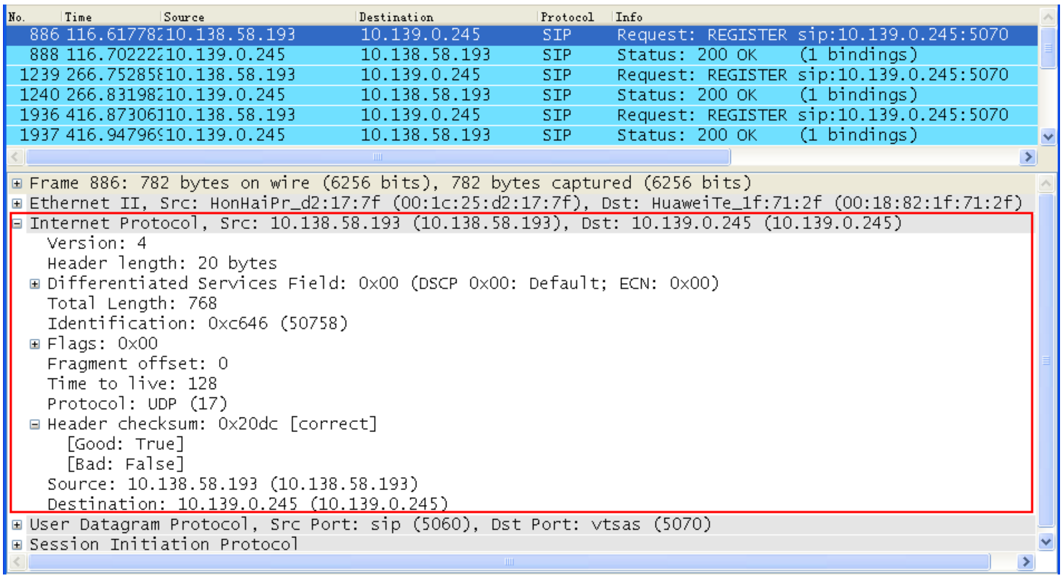


```
No.   Time      Source          Destination     Protocol  Info
  886 116.61778 10.138.58.193   10.139.0.245    SIP       Request: REGISTER sip:10.139.0.245:5070
  888 116.70222 10.139.0.245    10.138.58.193   SIP       Status: 200 OK    (1 bindings)
 1239 266.75285 10.138.58.193   10.139.0.245    SIP       Request: REGISTER sip:10.139.0.245:5070
 1240 266.83198 10.139.0.245    10.138.58.193   SIP       Status: 200 OK    (1 bindings)
 1936 416.87306 10.138.58.193   10.139.0.245    SIP       Request: REGISTER sip:10.139.0.245:5070
 1937 416.94796 10.139.0.245    10.138.58.193   SIP       Status: 200 OK    (1 bindings)

⊞ Frame 886: 782 bytes on wire (6256 bits), 782 bytes captured (6256 bits)
⊟ Ethernet II, Src: HonHaiPr_d2:17:7f (00:1c:25:d2:17:7f), Dst: HuaweiTe_1f:71:2f (00:18:82:1f:71:2f)
  ⊟ Destination: HuaweiTe_1f:71:2f (00:18:82:1f:71:2f)
      Address: HuaweiTe_1f:71:2f (00:18:82:1f:71:2f)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
  ⊟ Source: HonHaiPr_d2:17:7f (00:1c:25:d2:17:7f)
      Address: HonHaiPr_d2:17:7f (00:1c:25:d2:17:7f)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Type: IP (0x0800)
⊞ Internet Protocol, Src: 10.138.58.193 (10.138.58.193), Dst: 10.139.0.245 (10.139.0.245)
⊞ User Datagram Protocol, Src Port: sip (5060), Dst Port: vtsas (5070)
⊞ Session Initiation Protocol
```

- Network layer

  The third layer in the protocol layer description window is the network layer, which contains the source IP address (**Source**), destination IP address (**Destination**), packet length (**Total length**), and checksum (**Header checksum**), as shown in Figure 5-58.

Figure 5-58 Network layer of the SIP protocol



```
No.   Time      Source          Destination     Protocol  Info
  886 116.61778 10.138.58.193   10.139.0.245    SIP       Request: REGISTER sip:10.139.0.245:5070
  888 116.70222 10.139.0.245    10.138.58.193   SIP       Status: 200 OK    (1 bindings)
 1239 266.75285 10.138.58.193   10.139.0.245    SIP       Request: REGISTER sip:10.139.0.245:5070
 1240 266.83198 10.139.0.245    10.138.58.193   SIP       Status: 200 OK    (1 bindings)
 1936 416.87306 10.138.58.193   10.139.0.245    SIP       Request: REGISTER sip:10.139.0.245:5070
 1937 416.94796 10.139.0.245    10.138.58.193   SIP       Status: 200 OK    (1 bindings)

⊞ Frame 886: 782 bytes on wire (6256 bits), 782 bytes captured (6256 bits)
⊞ Ethernet II, Src: HonHaiPr_d2:17:7f (00:1c:25:d2:17:7f), Dst: HuaweiTe_1f:71:2f (00:18:82:1f:71:2f)
⊟ Internet Protocol, Src: 10.138.58.193 (10.138.58.193), Dst: 10.139.0.245 (10.139.0.245)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 768
    Identification: 0xc646 (50758)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
  ⊟ Header checksum: 0x20dc [correct]
      [Good: True]
      [Bad: False]
    Source: 10.138.58.193 (10.138.58.193)
    Destination: 10.139.0.245 (10.139.0.245)
⊞ User Datagram Protocol, Src Port: sip (5060), Dst Port: vtsas (5070)
⊞ Session Initiation Protocol
```

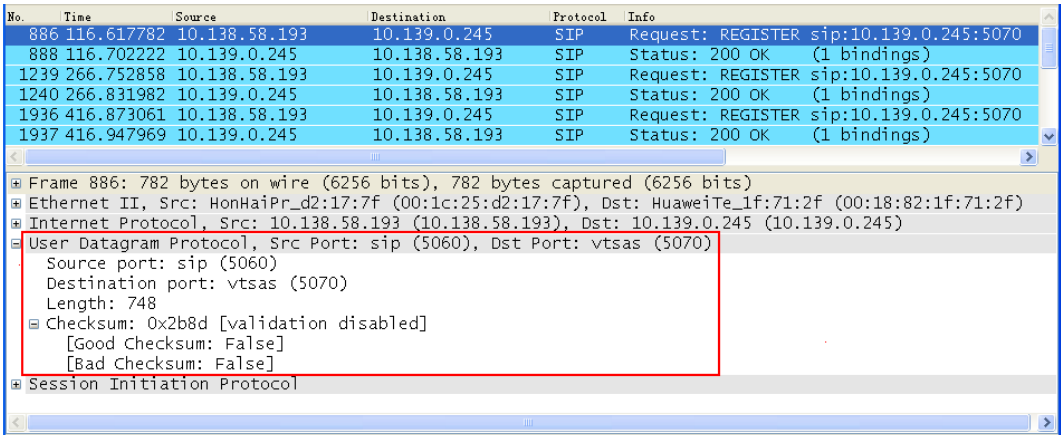
At the network layer, check whether:

- The source IP address and destination address are correct.
- The length of a packet exceeds the maximum length allowed by a certain device.

- Transport control layer

  The fourth layer in the protocol layer description window is the transport control layer, which contains **Source port**, **Destination port**, packet length (**Length**), and **Checksum**, as shown in Figure 5-59.

Figure 5-59 Transport control layer of the SIP protocol



```
No.    Time        Source          Destination     Protocol  Info
  886 116.617782 10.138.58.193   10.139.0.245    SIP       Request: REGISTER sip:10.139.0.245:5070
  888 116.702222 10.139.0.245    10.138.58.193   SIP       Status: 200 OK    (1 bindings)
 1239 266.752858 10.138.58.193   10.139.0.245    SIP       Request: REGISTER sip:10.139.0.245:5070
 1240 266.831982 10.139.0.245    10.138.58.193   SIP       Status: 200 OK    (1 bindings)
 1936 416.873061 10.138.58.193   10.139.0.245    SIP       Request: REGISTER sip:10.139.0.245:5070
 1937 416.947969 10.139.0.245    10.138.58.193   SIP       Status: 200 OK    (1 bindings)

⊞ Frame 886: 782 bytes on wire (6256 bits), 782 bytes captured (6256 bits)
⊞ Ethernet II, Src: HonHaiPr_d2:17:7f (00:1c:25:d2:17:7f), Dst: HuaweiTe_1f:71:2f (00:18:82:1f:71:2f)
⊞ Internet Protocol, Src: 10.138.58.193 (10.138.58.193), Dst: 10.139.0.245 (10.139.0.245)
⊟ User Datagram Protocol, Src Port: sip (5060), Dst Port: vtsas (5070)
    Source port: sip (5060)
    Destination port: vtsas (5070)
    Length: 748
  ⊟ Checksum: 0x2b8d [validation disabled]
      [Good Checksum: False]
      [Bad Checksum: False]
⊞ Session Initiation Protocol
```

At the transport control layer, check whether:

- The destination port is correct.
- The application process port is correct.
- The checksum information is correct.

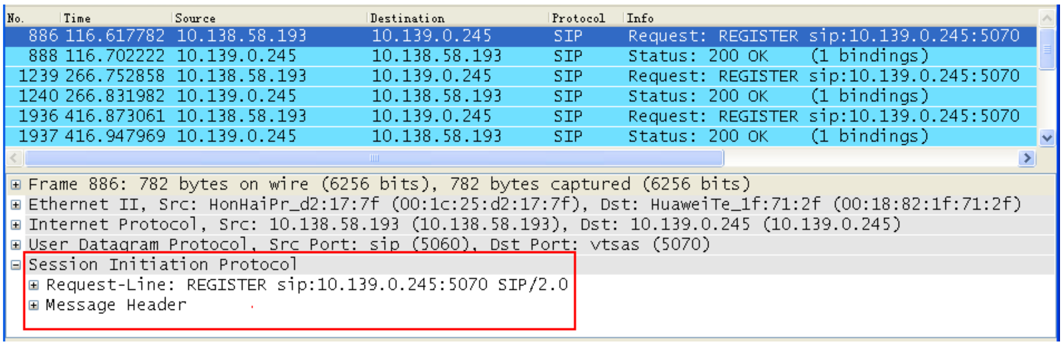
  The network adapters of certain devices may calculate the checksum of the User Datagram Protocol (UDP) layer. If the checksum is incorrect, the network adapter of the device may discard the packet.

- Application layer

  The fifth layer in the protocol layer description window is the application layer, which contains the SIP protocol details.

  The signaling record consists of Request-Line and Message Header. If a message includes a message body, Message Body is also included, as shown in Figure 5-60.

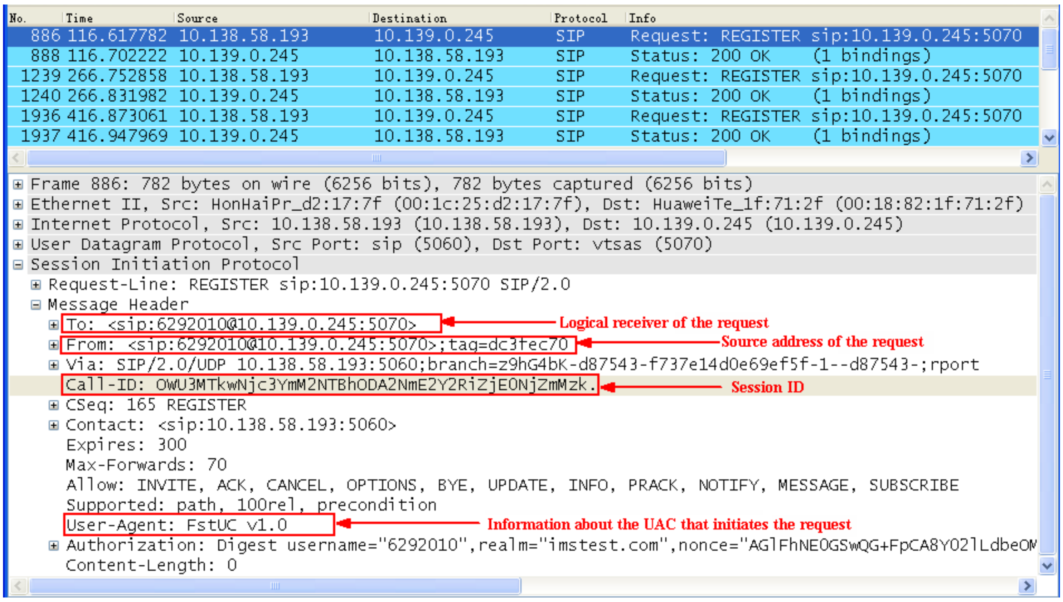
Figure 5-60 Request messages at the application layer of the SIP protocol



```
No.    Time        Source          Destination     Protocol  Info
  886 116.617782 10.138.58.193   10.139.0.245    SIP       Request: REGISTER sip:10.139.0.245:5070
  888 116.702222 10.139.0.245    10.138.58.193   SIP       Status: 200 OK    (1 bindings)
 1239 266.752858 10.138.58.193   10.139.0.245    SIP       Request: REGISTER sip:10.139.0.245:5070
 1240 266.831982 10.139.0.245    10.138.58.193   SIP       Status: 200 OK    (1 bindings)
 1936 416.873061 10.138.58.193   10.139.0.245    SIP       Request: REGISTER sip:10.139.0.245:5070
 1937 416.947969 10.139.0.245    10.138.58.193   SIP       Status: 200 OK    (1 bindings)

⊞ Frame 886: 782 bytes on wire (6256 bits), 782 bytes captured (6256 bits)
⊞ Ethernet II, Src: HonHaiPr_d2:17:7f (00:1c:25:d2:17:7f), Dst: HuaweiTe_1f:71:2f (00:18:82:1f:71:2f)
⊞ Internet Protocol, Src: 10.138.58.193 (10.138.58.193), Dst: 10.139.0.245 (10.139.0.245)
⊞ User Datagram Protocol, Src Port: sip (5060), Dst Port: vtsas (5070)
⊟ Session Initiation Protocol
  ⊞ Request-Line: REGISTER sip:10.139.0.245:5070 SIP/2.0
  ⊞ Message Header
```

The message header information can be used to locate faults, as shown in Figure 5-61.

Figure 5-61 Message header information



```
No.   Time        Source          Destination    Protocol Info
  886 116.617782 10.138.58.193   10.139.0.245   SIP      Request: REGISTER sip:10.139.0.245:5070
  888 116.702222 10.139.0.245    10.138.58.193  SIP      Status: 200 OK    (1 bindings)
 1239 266.752858 10.138.58.193   10.139.0.245   SIP      Request: REGISTER sip:10.139.0.245:5070
 1240 266.831982 10.139.0.245    10.138.58.193  SIP      Status: 200 OK    (1 bindings)
 1936 416.873061 10.138.58.193   10.139.0.245   SIP      Request: REGISTER sip:10.139.0.245:5070
 1937 416.947969 10.139.0.245    10.138.58.193  SIP      Status: 200 OK    (1 bindings)

⊞ Frame 886: 782 bytes on wire (6256 bits), 782 bytes captured (6256 bits)
⊞ Ethernet II, Src: HonHaiPr_d2:17:7f (00:1c:25:d2:17:7f), Dst: HuaweiTe_1f:71:2f (00:18:82:1f:71:2f)
⊞ Internet Protocol, Src: 10.138.58.193 (10.138.58.193), Dst: 10.139.0.245 (10.139.0.245)
⊞ User Datagram Protocol, Src Port: sip (5060), Dst Port: vtsas (5070)
⊟ Session Initiation Protocol
  ⊞ Request-Line: REGISTER sip:10.139.0.245:5070 SIP/2.0
  ⊟ Message Header
    ⊞ To: <sip:6292010@10.139.0.245:5070>
    ⊞ From: <sip:6292010@10.139.0.245:5070>;tag=dc3fec70
    ⊞ Via: SIP/2.0/UDP 10.138.58.193:5060;branch=z9hG4bK-d87543-f737e14d0e69ef5f-1--d87543-;rport
      Call-ID: OWU3MTkwNjc3YmM2NTBhODA2NmE2Y2RiZjE0NjZmMzk.
    ⊞ CSeq: 165 REGISTER
    ⊞ Contact: <sip:10.138.58.193:5060>
      Expires: 300
      Max-Forwards: 70
      Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, UPDATE, INFO, PRACK, NOTIFY, MESSAGE, SUBSCRIBE
      Supported: path, 100rel, precondition
      User-Agent: FstUC v1.0
    ⊞ Authorization: Digest username="6292010",realm="imstest.com",nonce="AGlFhNEOGSwQG+FpCA8Y02lLdbeOM
      Content-Length: 0
```

Logical receiver of the request
Source address of the request
Session ID
Information about the UAC that initiates the request

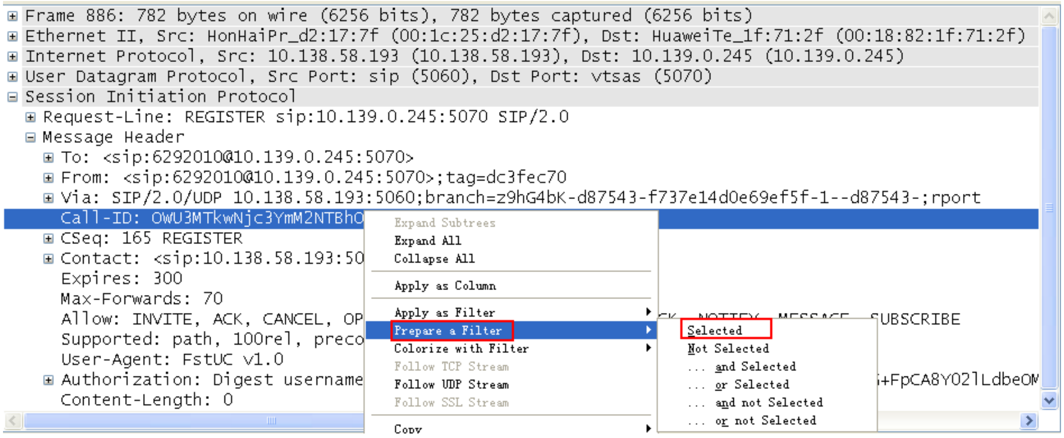
In the message header, pay attention to the following information:

- Call-ID

  Unique identifier of a group of messages. The requests and responses of a UA in a session share the same Call-ID. Therefore, you can obtain the information about the requests and responses of a session by querying the Call-ID.

  Right-click a Call-ID to be queried, and then choose **Apply as Filter** > **Selected**, as shown in Figure 5-62.

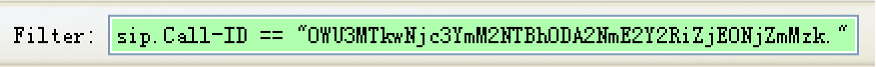
Figure 5-62 Filtering a Call-ID out



```
⊞ Frame 886: 782 bytes on wire (6256 bits), 782 bytes captured (6256 bits)
⊞ Ethernet II, Src: HonHaiPr_d2:17:7f (00:1c:25:d2:17:7f), Dst: HuaweiTe_1f:71:2f (00:18:82:1f:71:2f)
⊞ Internet Protocol, Src: 10.138.58.193 (10.138.58.193), Dst: 10.139.0.245 (10.139.0.245)
⊞ User Datagram Protocol, Src Port: sip (5060), Dst Port: vtsas (5070)
⊟ Session Initiation Protocol
  ⊞ Request-Line: REGISTER sip:10.139.0.245:5070 SIP/2.0
  ⊟ Message Header
    ⊞ To: <sip:6292010@10.139.0.245:5070>
    ⊞ From: <sip:6292010@10.139.0.245:5070>;tag=dc3fec70
    ⊞ Via: SIP/2.0/UDP 10.138.58.193:5060;branch=z9hG4bK-d87543-f737e14d0e69ef5f-1--d87543-;rport
      Call-ID: OWU3MTkwNjc3YmM2NTBhO
    ⊞ CSeq: 165 REGISTER
    ⊞ Contact: <sip:10.138.58.193:50
      Expires: 300
      Max-Forwards: 70
      Allow: INVITE, ACK, CANCEL, OP
      Supported: path, 100rel, preco
      User-Agent: FstUC v1.0
    ⊞ Authorization: Digest username
      Content-Length: 0
```

Then the signaling records that share the same Call-ID are displayed in the captured packet list window. The Call-ID that is filtered out is displayed in the **Filter** text box on the toolbar, as shown in Figure 5-63.

Figure 5-63 Value of Filter on the toolbar



Filter: sip.Call-ID == “OWU3MTkwNjc3YmM2NTBhODA2NmE2Y2RiZjE0NjZmMzk.”

- From

  Source address of the request.

- To

  Logical receiver of the request.

- User-Agent

  Information about the User Agent Client (UAC) that initiates the request.

  If the value of **User-Agent** is **Conf-serv/3GPP**, the request is initiated by a personal computer (PC).

SOAP Protocol Analysis

This topic describes how to use the Wireshark to analyze SOAP packets.

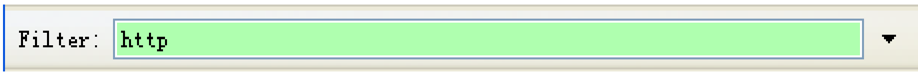
Background

To capture a Simple Object Access Protocol (SOAP) packet, pay attention to the following information:

- Capture the packet on the AS.
  - Install the Wireshark of the Linux operating system on the AS.
  - After capturing a SOAP packet using a command on the AS, use the Wireshark to analyze the captured SOAP packet on the Windows host.

    tcpdump -i eth0(actual network adapter name) -w Packet name -s 1200
- After choosing **Capture** > **Options** to set parameters, do not enter any information in the **Capture Filter** text box.
- Enter **http** in the **Filter** text box when capturing SOAP packets, as shown in Figure 5-64.

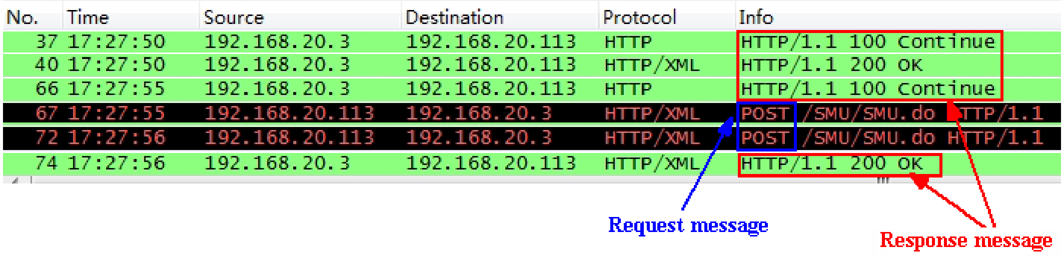
Figure 5-64 Filter criteria



Filter: http

After capturing the SOAP packet is completed, the Hypertext Transfer Protocol (HTTP) signaling that passes through the network adapter with the IP address of the host is displayed, as shown in Figure 5-65.

Figure 5-65 Filtered HTTP signaling



```
No.  Time      Source          Destination     Protocol  Info
  37 17:27:50  192.168.20.3    192.168.20.113  HTTP      HTTP/1.1 100 Continue
  40 17:27:50  192.168.20.3    192.168.20.113  HTTP/XML  HTTP/1.1 200 OK
  66 17:27:55  192.168.20.3    192.168.20.113  HTTP      HTTP/1.1 100 Continue
  67 17:27:55  192.168.20.113  192.168.20.3    HTTP/XML  POST /SMU/SMU.do HTTP/1.1
  72 17:27:56  192.168.20.113  192.168.20.3    HTTP/XML  POST /SMU/SMU.do HTTP/1.1
  74 17:27:56  192.168.20.3    192.168.20.113  HTTP/XML  HTTP/1.1 200 OK
```

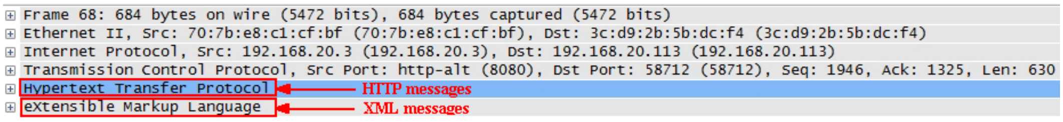
To query signaling details, proceed as follows:

1. Right-click the signaling to be queried.
2. Choose **Show Packet in New Window** from the shortcut menu. A dialog box is displayed, containing the signaling details.

Protocol Analysis

A SOAP message includes HTPP and Extensible Markup Language (XML) messages. Pay attention to the contents at the following layers in the red box, as shown in Figure 5-66.

Figure 5-66 Protocol layers that you need to pay attention to



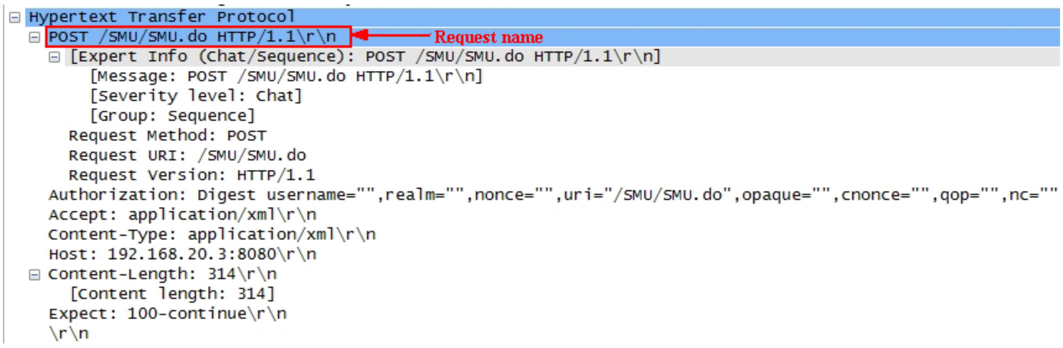
```
⊞ Frame 68: 684 bytes on wire (5472 bits), 684 bytes captured (5472 bits)
⊞ Ethernet II, Src: 70:7b:e8:c1:cf:bf (70:7b:e8:c1:cf:bf), Dst: 3c:d9:2b:5b:dc:f4 (3c:d9:2b:5b:dc:f4)
⊞ Internet Protocol, Src: 192.168.20.3 (192.168.20.3), Dst: 192.168.20.113 (192.168.20.113)
⊞ Transmission Control Protocol, Src Port: http-alt (8080), Dst Port: 58712 (58712), Seq: 1946, Ack: 1325, Len: 630
⊞ Hypertext Transfer Protocol
⊞ eXtensible Markup Language
```

- HTTP messages

  An HTTP message contains the name and operation of a SOAP request, as shown in Figure 5-67 and Figure 5-68.

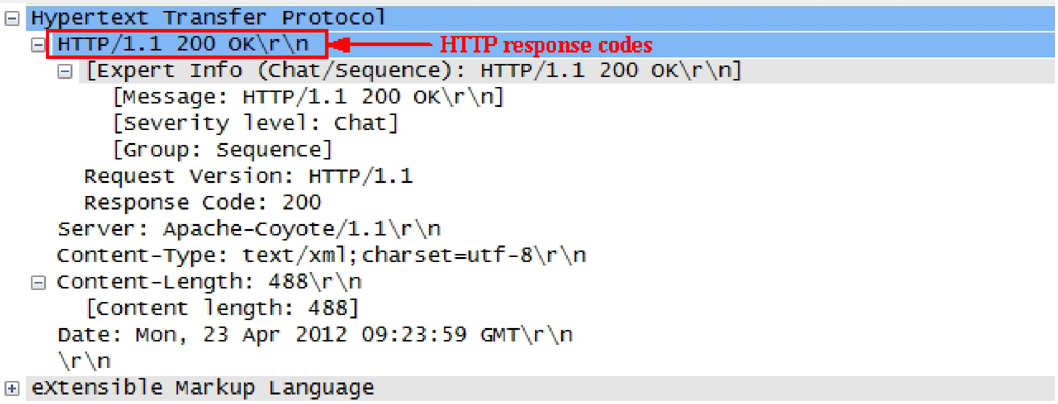
  You must pay attention to the method name in the request and the response code in the response.

Figure 5-67 HTTP request



```
⊟ Hypertext Transfer Protocol
  ⊟ POST /SMU/SMU.do HTTP/1.1\r\n
    ⊟ [Expert Info (Chat/Sequence): POST /SMU/SMU.do HTTP/1.1\r\n]
        [Message: POST /SMU/SMU.do HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: POST
      Request URI: /SMU/SMU.do
      Request Version: HTTP/1.1
    Authorization: Digest username="",realm="",nonce="",uri="/SMU/SMU.do",opaque="",cnonce="",qop="",nc=""
    Accept: application/xml\r\n
    Content-Type: application/xml\r\n
    Host: 192.168.20.3:8080\r\n
  ⊟ Content-Length: 314\r\n
      [Content length: 314]
    Expect: 100-continue\r\n
    \r\n
```

Figure 5-68 HTTP response



```
⊟ Hypertext Transfer Protocol
  ⊟ HTTP/1.1 200 OK\r\n
    ⊟ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        [Message: HTTP/1.1 200 OK\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Version: HTTP/1.1
      Response Code: 200
    Server: Apache-Coyote/1.1\r\n
    Content-Type: text/xml;charset=utf-8\r\n
  ⊟ Content-Length: 488\r\n
      [Content length: 488]
    Date: Mon, 23 Apr 2012 09:23:59 GMT\r\n
    \r\n
⊞ eXtensible Markup Language
```

HTTP response codes

- XML messages

  An XML messages contains a message type and a message content.

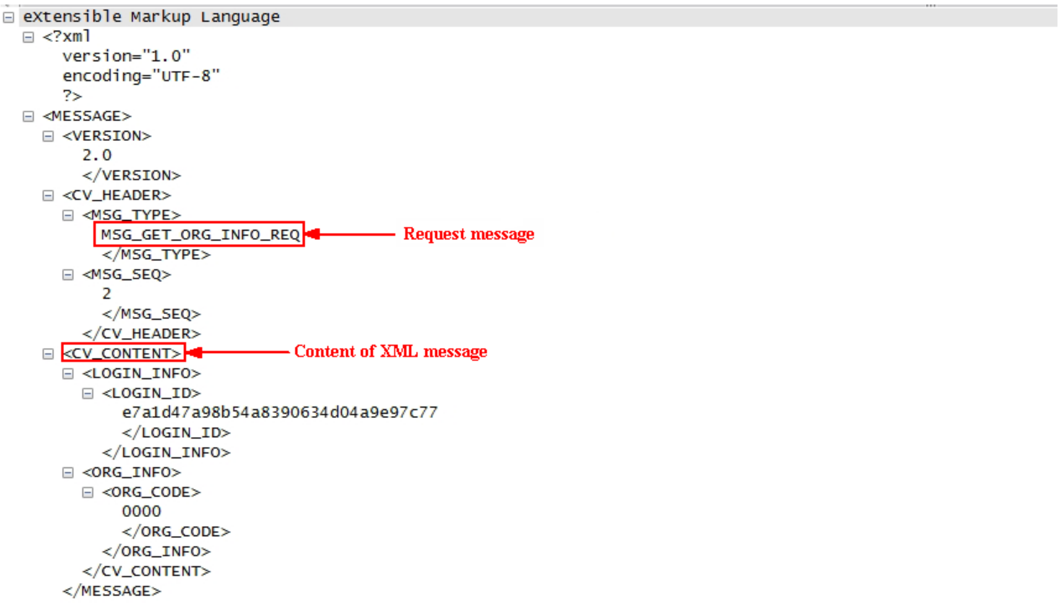
  – MSG_TYPE presents a message type declaration.

  – CV_CONTENT presents a message content declaration.

  Figure 5-69shows the XML messages in a request for a login in scene.

  Figure 5-70shows the XML messages in a response for a login in scene.

Figure 5-69 XML messages in a request for a login in scene

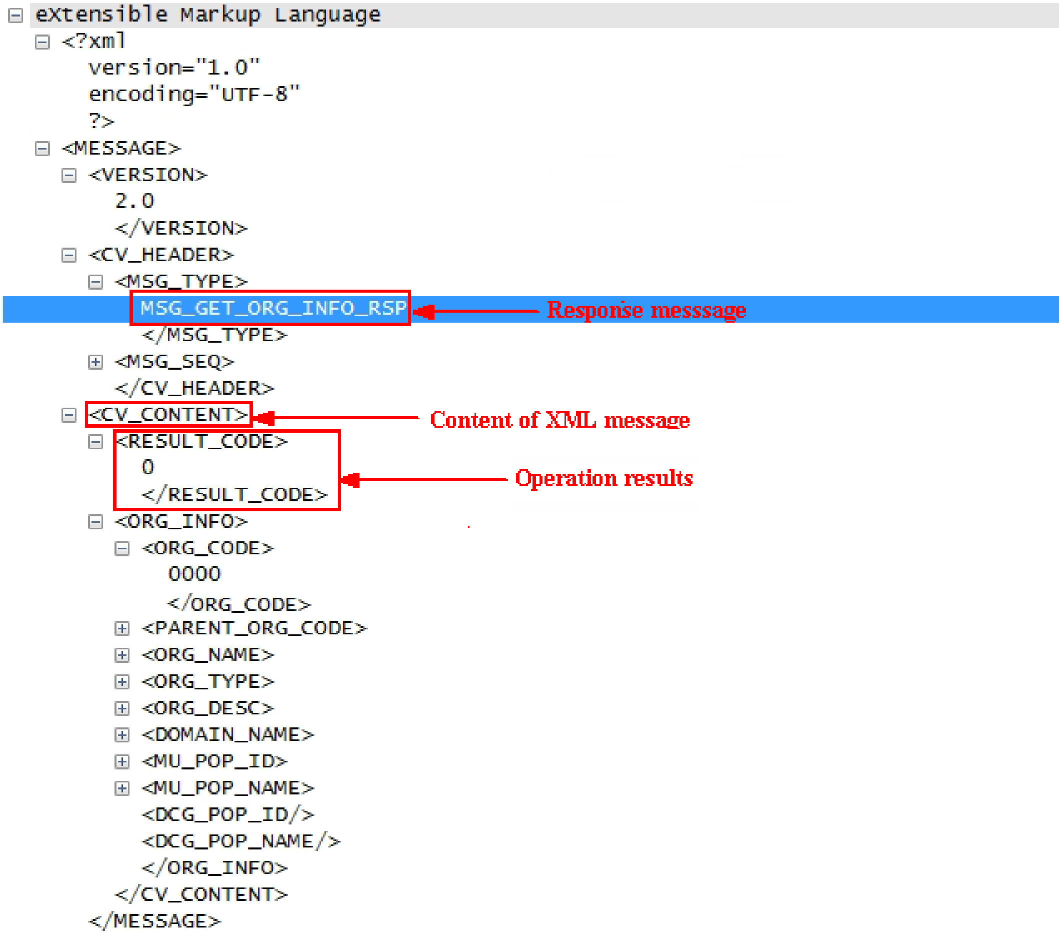


```
⊟ eXtensible Markup Language
  ⊟ <?xml
      version="1.0"
      encoding="UTF-8"
      ?>
  ⊟ <MESSAGE>
    ⊟ <VERSION>
        2.0
        </VERSION>
    ⊟ <CV_HEADER>
      ⊟ <MSG_TYPE>
          MSG_GET_ORG_INFO_REQ
          </MSG_TYPE>
      ⊟ <MSG_SEQ>
          2
          </MSG_SEQ>
        </CV_HEADER>
    ⊟ <CV_CONTENT>
      ⊟ <LOGIN_INFO>
        ⊟ <LOGIN_ID>
            e7a1d47a98b54a8390634d04a9e97c77
            </LOGIN_ID>
          </LOGIN_INFO>
      ⊟ <ORG_INFO>
        ⊟ <ORG_CODE>
            0000
            </ORG_CODE>
          </ORG_INFO>
        </CV_CONTENT>
    </MESSAGE>
```

Request message

Content of XML message

Figure 5-70 XML messages in a response for a login in scene



```
⊟ eXtensible Markup Language
  ⊟ <?xml
      version="1.0"
      encoding="UTF-8"
      ?>
  ⊟ <MESSAGE>
    ⊟ <VERSION>
        2.0
        </VERSION>
    ⊟ <CV_HEADER>
      ⊟ <MSG_TYPE>
          MSG_GET_ORG_INFO_RSP
          </MSG_TYPE>
      ⊞ <MSG_SEQ>
        </CV_HEADER>
    ⊟ <CV_CONTENT>
      ⊟ <RESULT_CODE>
          0
          </RESULT_CODE>
      ⊟ <ORG_INFO>
        ⊟ <ORG_CODE>
            0000
            </ORG_CODE>
        ⊞ <PARENT_ORG_CODE>
        ⊞ <ORG_NAME>
        ⊞ <ORG_TYPE>
        ⊞ <ORG_DESC>
        ⊞ <DOMAIN_NAME>
        ⊞ <MU_POP_ID>
        ⊞ <MU_POP_NAME>
          <DCG_POP_ID/>
          <DCG_POP_NAME/>
          </ORG_INFO>
        </CV_CONTENT>
      </MESSAGE>
```

Response messsage

Content of XML message

Operation results

5.9.5 Common Tips

Changing the Time Display Mode

CAUTION

The absolute time generated after the gateway GPRS support node (GGSN) users use the tmf2cap to convert .tmf files to .cap files may be incorrect. You can use the relative time to view the packet delay information.

Generally, data packets are displayed by relative time in the program, which is the interval between a subsequent packet and the initial packet.

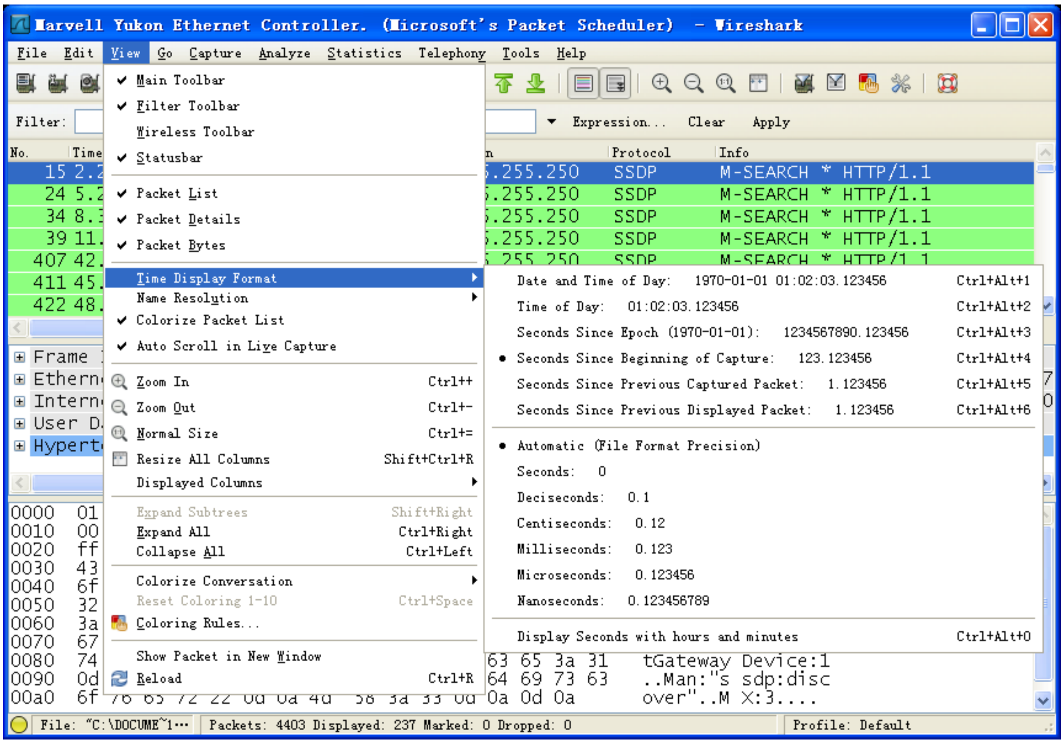
You can choose **View** > **Time Display Format** to change the time display mode.

The **Time Display Format** menu contains four options, as shown in Figure 5-71.

- **Time of Day**: for example, 18:23:01.852876.

- **Date and Time of a Day**
- **Seconds Since Beginning of Capture**
- **Seconds Since Previous Captured Packet**, which is used for viewing the time delay between packets.

Figure 5-71 Changing the time display mode

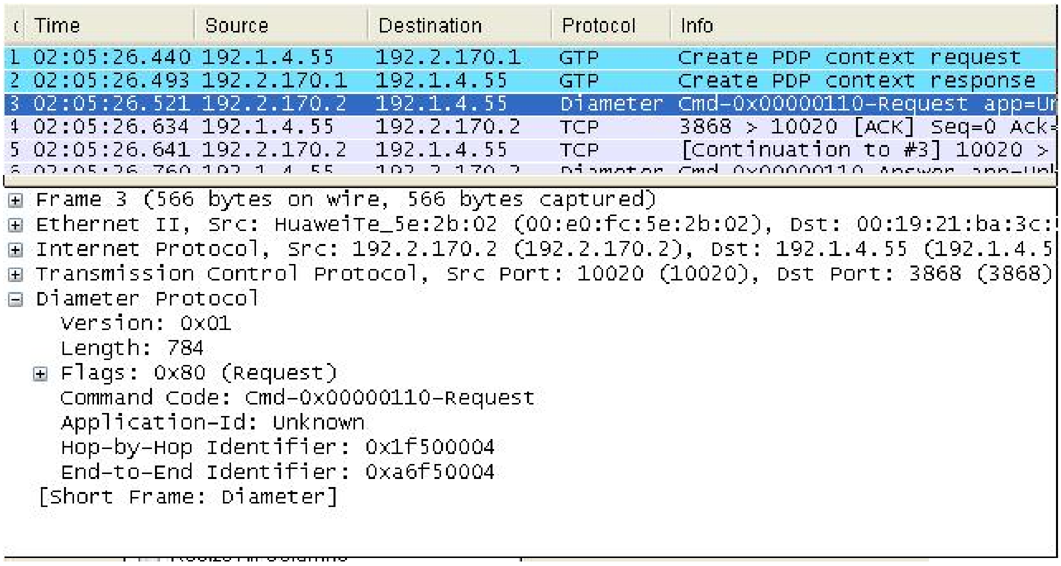

Marvell Yukon Ethernet Controller. (Microsoft's Packet Scheduler) - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply
No. Time
Protocol Info
SSDP M-SEARCH * HTTP/1.1
✓ Main Toolbar
✓ Filter Toolbar
Wireless Toolbar
✓ Statusbar
✓ Packet List
✓ Packet Details
✓ Packet Bytes
Time Display Format
Name Resolution
✓ Colorize Packet List
✓ Auto Scroll in Live Capture
Zoom In Ctrl++
Zoom Out Ctrl+-
Normal Size Ctrl+=
Resize All Columns Shift+Ctrl+R
Displayed Columns
Expand Subtrees Shift+Right
Expand All Ctrl+Right
Collapse All Ctrl+Left
Colorize Conversation
Reset Coloring 1-10 Ctrl+Space
Coloring Rules...
Show Packet in New Window
Reload Ctrl+R
Date and Time of Day: 1970-01-01 01:02:03.123456 Ctrl+Alt+1
Time of Day: 01:02:03.123456 Ctrl+Alt+2
Seconds Since Epoch (1970-01-01): 1234567890.123456 Ctrl+Alt+3
● Seconds Since Beginning of Capture: 123.123456 Ctrl+Alt+4
Seconds Since Previous Captured Packet: 1.123456 Ctrl+Alt+5
Seconds Since Previous Displayed Packet: 1.123456 Ctrl+Alt+6
● Automatic (File Format Precision)
Seconds: 0
Deciseconds: 0.1
Centiseconds: 0.12
Milliseconds: 0.123
Microseconds: 0.123456
Nanoseconds: 0.123456789
Display Seconds with hours and minutes Ctrl+Alt+0
Frame
Ethern
Intern
User D
Hypert
File: "C:\DOCUME~1... Packets: 4403 Displayed: 237 Marked: 0 Dropped: 0
Profile: Default

Loading the Custom Format Library

You can download or customize a format library for an application protocol that cannot be parsed by the Wireshark, and then load the format library to the Wireshark. Then the Wireshark can parse the application protocol, as shown in Figure 5-72.

For example, after you decompress the **libxml2.rar** file and copy the .dll file in the decompressed directory to the Wireshark installation directory, the Wireshark can parse the diameter protocol. The default Wireshark installation path is **C:\Program Files\Wireshark**.

Figure 5-72 Parsed diameter protocol after the diameter format library is loaded



```
( Time            Source          Destination     Protocol   Info
1 02:05:26.440 192.1.4.55      192.2.170.1     GTP        Create PDP context request
2 02:05:26.493 192.2.170.1     192.1.4.55      GTP        Create PDP context response
3 02:05:26.521 192.2.170.2     192.1.4.55      Diameter   Cmd-0x00000110-Request app=Un
4 02:05:26.634 192.1.4.55      192.2.170.2     TCP        3868 > 10020 [ACK] Seq=0 Ack=
5 02:05:26.641 192.2.170.2     192.1.4.55      TCP        [Continuation to #3] 10020 >
6 02:05:26.760 192.1.4.55      192.2.170.2     Diameter   Cmd-0x00000110-Answer app=Unk
```

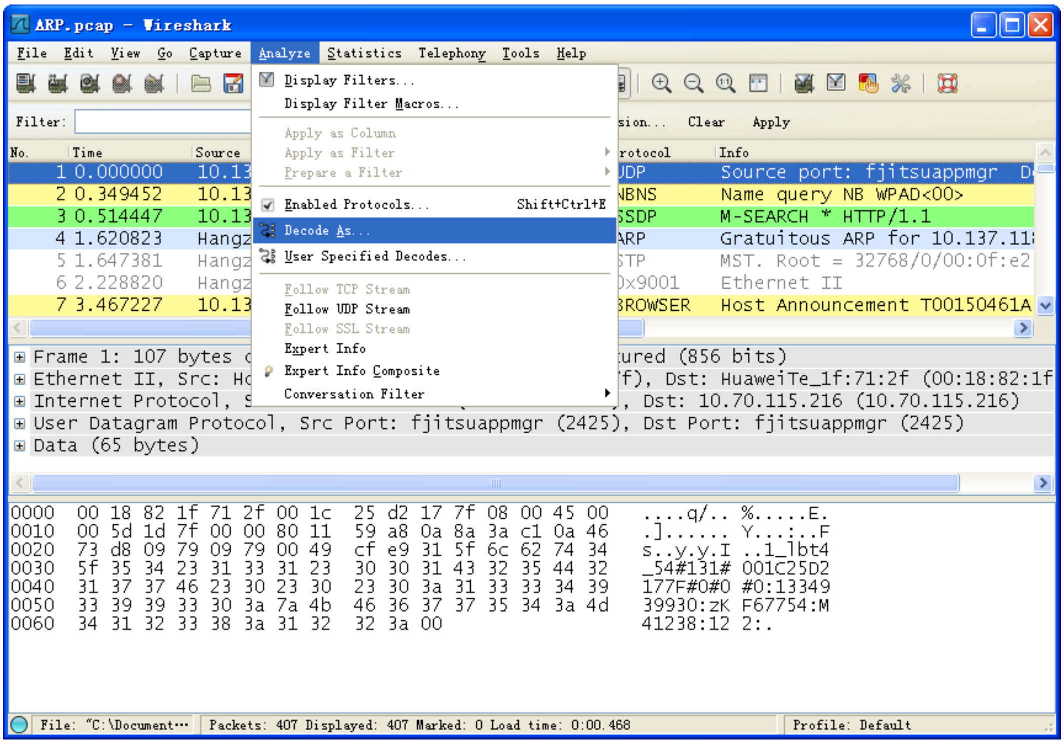
```
⊞ Frame 3 (566 bytes on wire, 566 bytes captured)
⊞ Ethernet II, Src: HuaweiTe_5e:2b:02 (00:e0:fc:5e:2b:02), Dst: 00:19:21:ba:3c:
⊞ Internet Protocol, Src: 192.2.170.2 (192.2.170.2), Dst: 192.1.4.55 (192.1.4.5
⊞ Transmission Control Protocol, Src Port: 10020 (10020), Dst Port: 3868 (3868)
⊟ Diameter Protocol
    Version: 0x01
    Length: 784
  ⊞ Flags: 0x80 (Request)
    Command Code: Cmd-0x00000110-Request
    Application-Id: Unknown
    Hop-by-Hop Identifier: 0x1f500004
    End-to-End Identifier: 0xa6f50004
   [Short Frame: Diameter]
```

Customizing the Non-Standard Port Applications

The Wireshark cannot identify the type of an application protocol that uses a non-standard port. Users can customize a protocol for parsing the non-standard port application protocol.

1. If the HTTP application has been enabled on port 1031 in an office, select the data packet on port 1031.
2. Choose **Analyze** > **Decode As...**, as shown in Figure 5-73.

Figure 5-73 Decode As



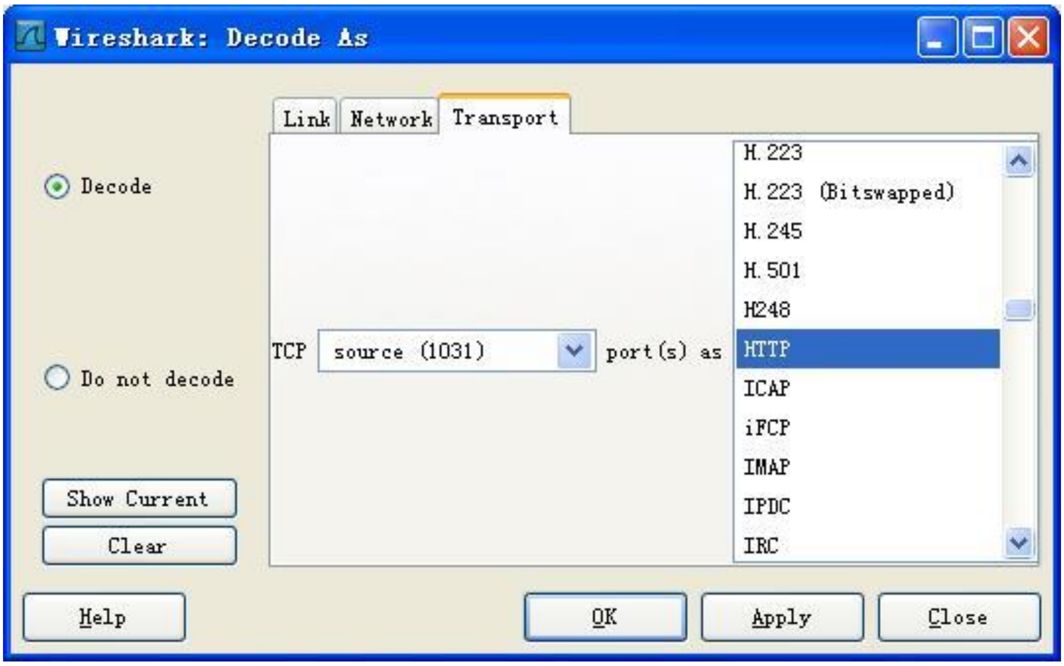
```
No.  Time        Source   rotocol   Info
  1 0.000000     10.13    UDP       Source port: fjitsuappmgr  D
  2 0.349452     10.13    NBNS      Name query NB WPAD<00>
  3 0.514447     10.13    SSDP      M-SEARCH * HTTP/1.1
  4 1.620823     Hangz    ARP       Gratuitous ARP for 10.137.11
  5 1.647381     Hangz    STP       MST. Root = 32768/0/00:0f:e2
  6 2.228820     Hangz    0x9001    Ethernet II
  7 3.467227     10.13    BROWSER   Host Announcement T00150461A

⊞ Frame 1: 107 bytes c                        ured (856 bits)
⊞ Ethernet II, Src: Hc                        f), Dst: HuaweiTe_1f:71:2f (00:18:82:1f
⊞ Internet Protocol, S                        , Dst: 10.70.115.216 (10.70.115.216)
⊞ User Datagram Protocol, Src Port: fjitsuappmgr (2425), Dst Port: fjitsuappmgr (2425)
⊞ Data (65 bytes)

0000  00 18 82 1f 71 2f 00 1c  25 d2 17 7f 08 00 45 00   ....q/.. %.....E.
0010  00 5d 1d 7f 00 00 80 11  59 a8 0a 8a 3a c1 0a 46   .]...... Y...:..F
0020  73 d8 09 79 09 79 00 49  cf e9 31 5f 6c 62 74 34   s..y.y.I ..1_lbt4
0030  5f 35 34 23 31 33 31 23  30 30 31 43 32 35 44 32   _54#131# 001C25D2
0040  31 37 37 46 23 30 23 30  23 30 3a 31 33 33 34 39   177F#0#0 #0:13349
0050  33 39 39 33 30 3a 7a 4b  46 36 37 37 35 34 3a 4d   39930:zK F67754:M
0060  34 31 32 33 38 3a 31 32  32 3a 00                  41238:12 2:.

File: "C:\Document…   Packets: 407 Displayed: 407 Marked: 0 Load time: 0:00.468   Profile: Default
```

CAUTION

You must choose **Analyze** > **Decode As** and select a protocol each time when you start the Wireshark to parse a non-standard port application protocol.

3. Select an application protocol, and then click **Apply**, as shown in Figure 5-74.

Figure 5-74 Customizing a protocol for parsing the non-standard port application protocol



Wireshark: Decode As

● Decode

○ Do not decode

Link | Network | Transport

TCP source (1031) port(s) as HTTP

4. Click **OK**.

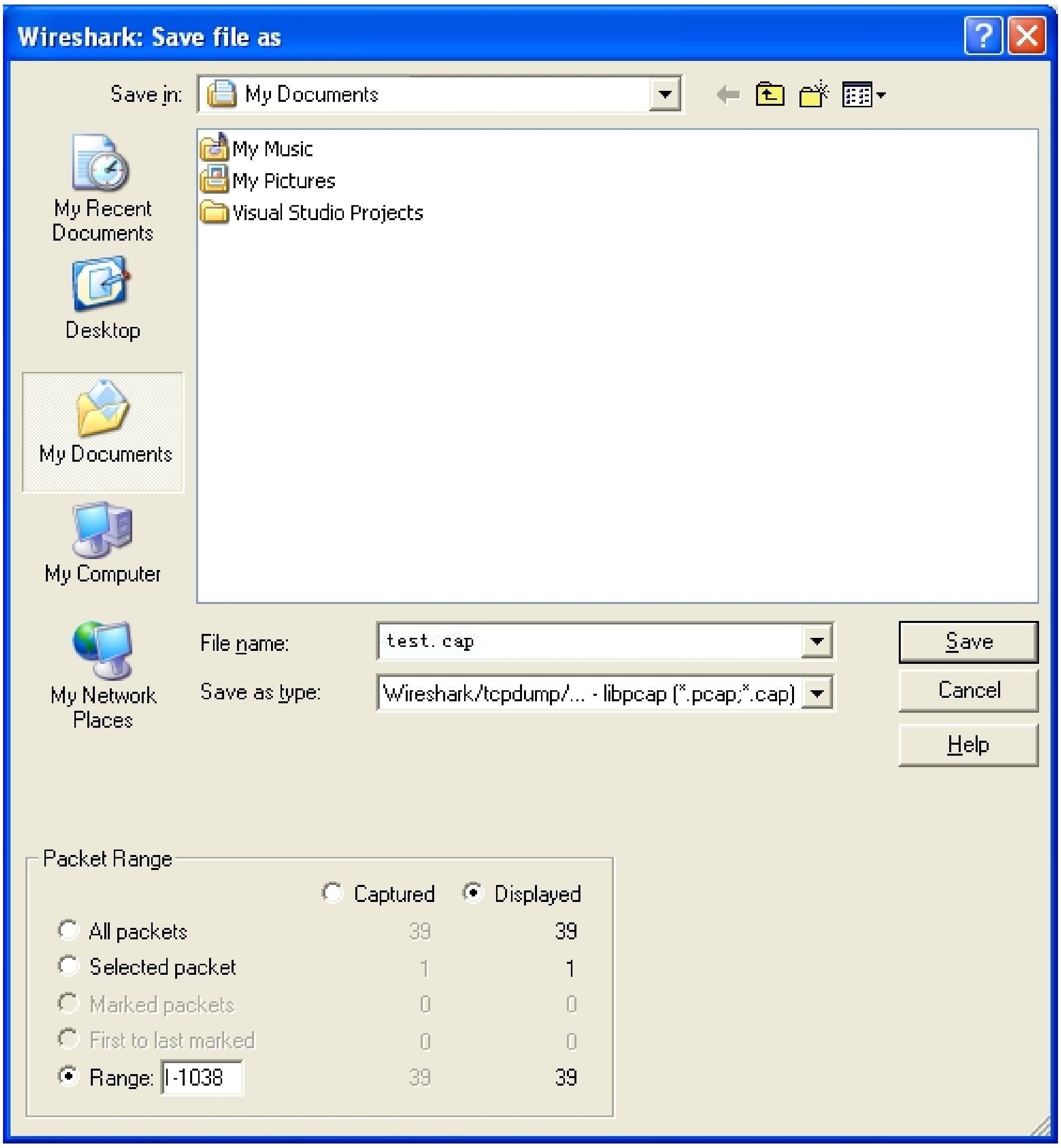
Splitting and Merging Result Files

1. Split a result file.

   Choose **File** > **save as**, and then split a result file, as shown in Figure 5-75.

   - Use the filter to display the information that you want to save as files separately, and then choose **displayed** in the **Packet Range** area.
   - Choose**Range**, and then enter a number range, for example **1-1038**. Then packets numbered from 1 to 1038 are saved as a file.

Figure 5-75 Save file as



Save in: My Documents

File name: test. cap

Save as type: Wireshark/tcpdump/... - libpcap (*.pcap;*.cap)

Packet Range

	○ Captured	● Displayed
○ All packets	39	39
○ Selected packet	1	1
○ Marked packets	0	0
○ First to last marked	0	0
● Range: 1-1038	39	39

2. Merge a result file.

   Choose **File** > **Merge**.

   The system prompts you to save the result file before merging it.

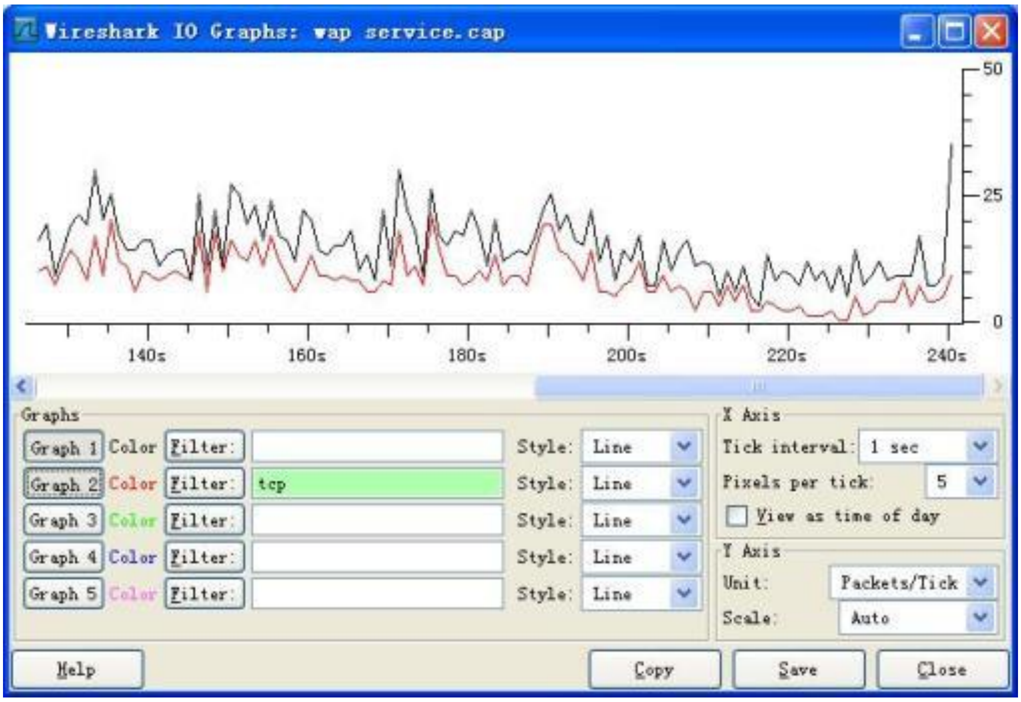
   - Enter the name of the result file to be merged, and then click **Save**.
   - Select the file to which you will merge the result file, and then click **Open**.

Displaying Traffic Waveform Chart

The Wireshark can generate traffic waveform charts based on the captured data packets. You can set filter criteria to display the waveform charts of certain protocol traffic or user traffic in a certain period.

Choose **Statistics** > **IO Graphs**. The **Wireshark IO Graphs** dialog box is displayed, as shown in Figure 5-76.

Figure 5-76 Wireshark IO Graphs



Graph 1	Color	Filter:		Style:	Line
Graph 2	Color	Filter:	tcp	Style:	Line
Graph 3	Color	Filter:		Style:	Line
Graph 4	Color	Filter:		Style:	Line
Graph 5	Color	Filter:		Style:	Line

Tick interval: 1 sec
Pixels per tick: 5
□ View as time of day
Unit: Packets/Tick
Scale: Auto

By default, all traffic waveform charts are displayed. After you set the filter criteria in the filter, only traffic waveform charts that meet the filter criteria are displayed.

Calculating the Packet Traffic

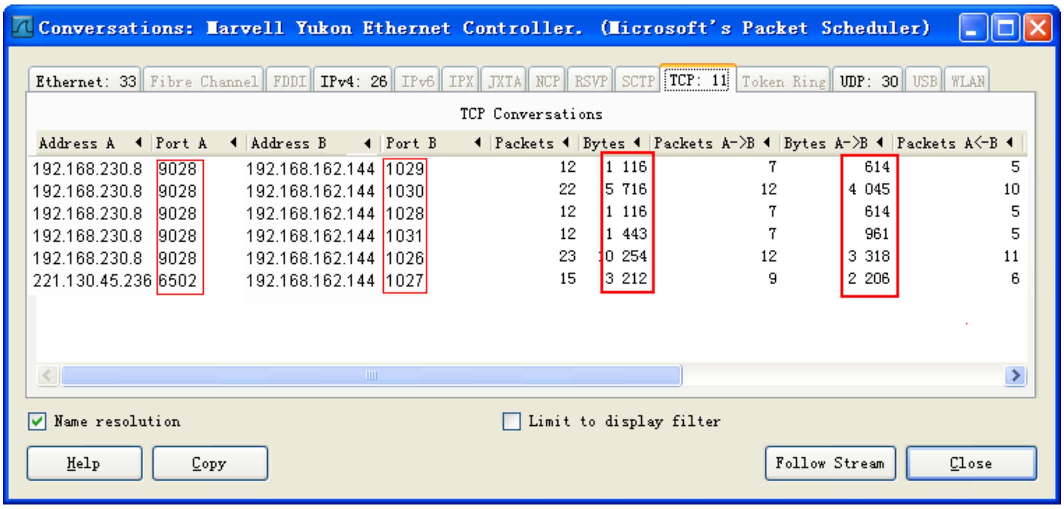
The following describes the common method for calculating the packet traffic.

When receiving a request for calculating the packet traffic, you must verify that the extended field statistics in the Call Detail Records (CDRs) are correct.

- Choose **Statistics** > **Conversations** in the Wireshark.

  The **Conversations** page is displayed, as shown in Figure 5-77.

Figure 5-77 Conversations



TCP Conversations

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B
192.168.230.8	9028	192.168.162.144	1029	12	1 116	7	614	5
192.168.230.8	9028	192.168.162.144	1030	22	5 716	12	4 045	10
192.168.230.8	9028	192.168.162.144	1028	12	1 116	7	614	5
192.168.230.8	9028	192.168.162.144	1031	12	1 443	7	961	5
192.168.230.8	9028	192.168.162.144	1026	23	10 254	12	3 318	11
221.130.45.236	6502	192.168.162.144	1027	15	3 212	9	2 206	6

☑ Name resolution ☐ Limit to display filter

In the basic packet information, such as all types of packets generated during mobile phone conversions, the **TCP** and **UDP** tab pages are displayed. On the **TCP** tab page, the following columns are included: **Address A**, **Port A**, **Address B**, **Port B**, **Bytes**, **Bytes A->B**, and **Bytes A<-B**.

On the **TCP** and **UDP** tab pages shown in Figure 5-77, packets that have same address but different port numbers are displayed in different columns but are calculated together.

- Choose **Statistics** > **Summary** to calculate the total packet bytes. Before calculating the total packet bytes, ensure that the filter criteria are set.

  After the preceding packet length is calculated, subtract 14 bytes (layer 2 information) and packet encapsulation added to the original packets by GGSN or Serving GPRS Support Node (SGSN), such as generic routing encapsulation (GRE) or GPRS tunneling protocol (GTP) encapsulation. The various encapsulation lengths are as follows:

  - GTP V0 header 20 bytes

    GTP V1 header: The fixed part is 8 bytes and the common part is 12 bytes.

  - UDP header

    8 bytes

  - IP header

    20 bytes

  - GRE header

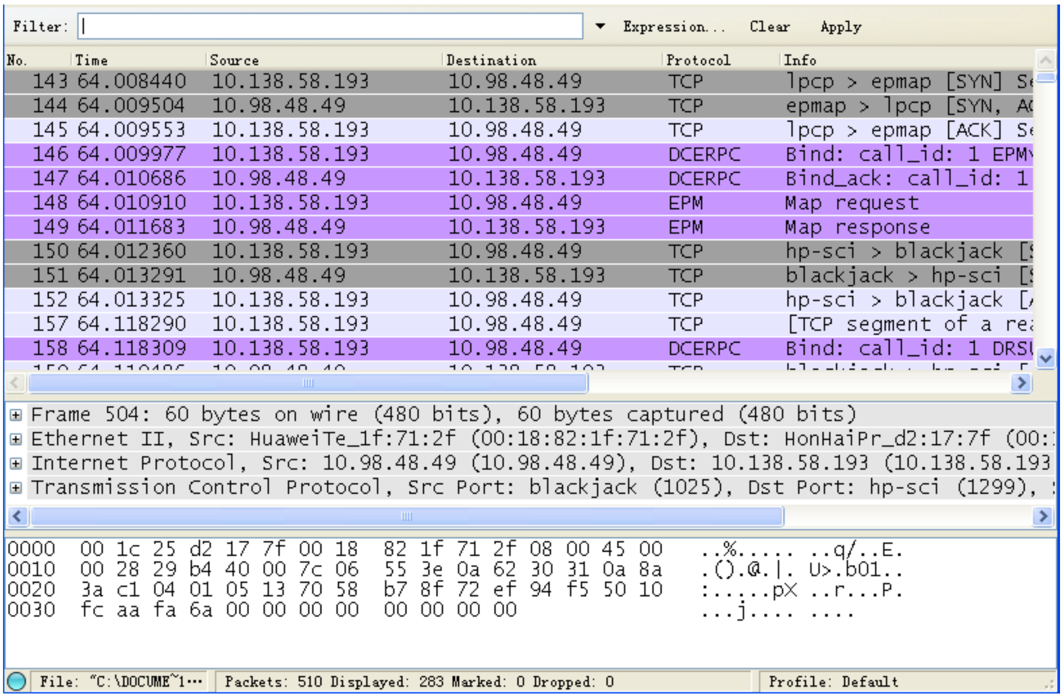
    4 bytes

The window for parsing packets in the Wireshark includes:

- Upper part: area for obtaining packet serial numbers
- Middle part: area for parsing the selected packet
- Lower part: area for displaying the original code streams for the selected packet

In the Wireshark, you can enter filter criteria in the **Filter** text box shown in Figure 5-78; the packets that meet the filter criteria are displayed.

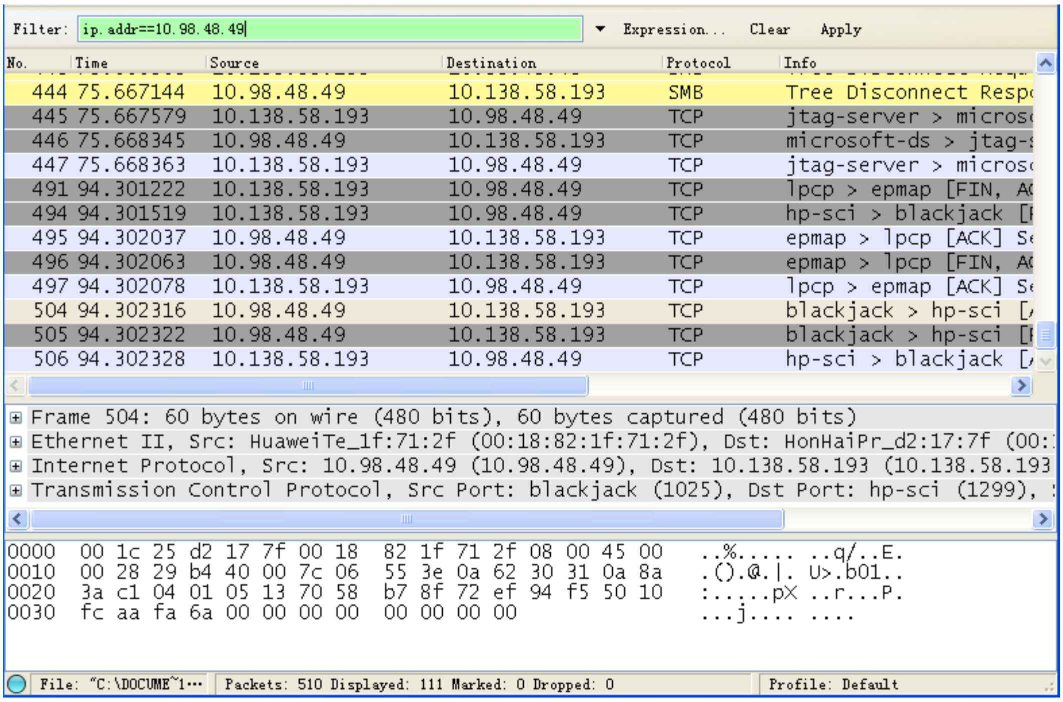
Figure 5-78 Parsing packets in the Wireshark



```
Filter: |                                   ▼ Expression...  Clear  Apply
No.  Time       Source         Destination    Protocol  Info
 143 64.008440  10.138.58.193  10.98.48.49    TCP       lpcp > epmap [SYN] Se
 144 64.009504  10.98.48.49    10.138.58.193  TCP       epmap > lpcp [SYN, AC
 145 64.009553  10.138.58.193  10.98.48.49    TCP       lpcp > epmap [ACK] Se
 146 64.009977  10.138.58.193  10.98.48.49    DCERPC    Bind: call_id: 1 EPMv
 147 64.010686  10.98.48.49    10.138.58.193  DCERPC    Bind_ack: call_id: 1
 148 64.010910  10.138.58.193  10.98.48.49    EPM       Map request
 149 64.011683  10.98.48.49    10.138.58.193  EPM       Map response
 150 64.012360  10.138.58.193  10.98.48.49    TCP       hp-sci > blackjack [S
 151 64.013291  10.98.48.49    10.138.58.193  TCP       blackjack > hp-sci [S
 152 64.013325  10.138.58.193  10.98.48.49    TCP       hp-sci > blackjack [A
 157 64.118290  10.138.58.193  10.98.48.49    TCP       [TCP segment of a rea
 158 64.118309  10.138.58.193  10.98.48.49    DCERPC    Bind: call_id: 1 DRSU

⊞ Frame 504: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
⊞ Ethernet II, Src: HuaweiTe_1f:71:2f (00:18:82:1f:71:2f), Dst: HonHaiPr_d2:17:7f (00:
⊞ Internet Protocol, Src: 10.98.48.49 (10.98.48.49), Dst: 10.138.58.193 (10.138.58.193
⊞ Transmission Control Protocol, Src Port: blackjack (1025), Dst Port: hp-sci (1299),

0000  00 1c 25 d2 17 7f 00 18  82 1f 71 2f 08 00 45 00   ..%..... ..q/..E.
0010  00 28 29 b4 40 00 7c 06  55 3e 0a 62 30 31 0a 8a   .().@.|. U>.b01..
0020  3a c1 04 01 05 13 70 58  b7 8f 72 ef 94 f5 50 10   :.....pX ..r...P.
0030  fc aa fa 6a 00 00 00 00  00 00 00 00               ...j.... ....

File: "C:\DOCUME~1…  Packets: 510 Displayed: 283 Marked: 0 Dropped: 0  Profile: Default
```

For example, to query the packets that are sent from or to the IP address 10.0.0.1, enter **ip.addr==10.0.0.1** in the **Filter** text box shown in Figure 5-78, and then click **Apply**. The packets that are sent from or to the IP address 10.0.0.1 are displayed, as shown Figure 5-79.

Figure 5-79 Filtering out the captured packets



```
Filter: ip.addr==10.98.48.49|               ▼ Expression...  Clear  Apply
No.  Time       Source         Destination    Protocol  Info
 444 75.667144  10.98.48.49    10.138.58.193  SMB       Tree Disconnect Respo
 445 75.667579  10.138.58.193  10.98.48.49    TCP       jtag-server > micros
 446 75.668345  10.98.48.49    10.138.58.193  TCP       microsoft-ds > jtag-s
 447 75.668363  10.138.58.193  10.98.48.49    TCP       jtag-server > micros
 491 94.301222  10.138.58.193  10.98.48.49    TCP       lpcp > epmap [FIN, AC
 494 94.301519  10.138.58.193  10.98.48.49    TCP       hp-sci > blackjack [F
 495 94.302037  10.98.48.49    10.138.58.193  TCP       epmap > lpcp [ACK] Se
 496 94.302063  10.98.48.49    10.138.58.193  TCP       epmap > lpcp [FIN, AC
 497 94.302078  10.138.58.193  10.98.48.49    TCP       lpcp > epmap [ACK] Se
 504 94.302316  10.98.48.49    10.138.58.193  TCP       blackjack > hp-sci [A
 505 94.302322  10.98.48.49    10.138.58.193  TCP       blackjack > hp-sci [F
 506 94.302328  10.138.58.193  10.98.48.49    TCP       hp-sci > blackjack [A

⊞ Frame 504: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
⊞ Ethernet II, Src: HuaweiTe_1f:71:2f (00:18:82:1f:71:2f), Dst: HonHaiPr_d2:17:7f (00:
⊞ Internet Protocol, Src: 10.98.48.49 (10.98.48.49), Dst: 10.138.58.193 (10.138.58.193
⊞ Transmission Control Protocol, Src Port: blackjack (1025), Dst Port: hp-sci (1299),

0000  00 1c 25 d2 17 7f 00 18  82 1f 71 2f 08 00 45 00   ..%..... ..q/..E.
0010  00 28 29 b4 40 00 7c 06  55 3e 0a 62 30 31 0a 8a   .().@.|. U>.b01..
0020  3a c1 04 01 05 13 70 58  b7 8f 72 ef 94 f5 50 10   :.....pX ..r...P.
0030  fc aa fa 6a 00 00 00 00  00 00 00 00               ...j.... ....

File: "C:\DOCUME~1…  Packets: 510 Displayed: 111 Marked: 0 Dropped: 0  Profile: Default
```

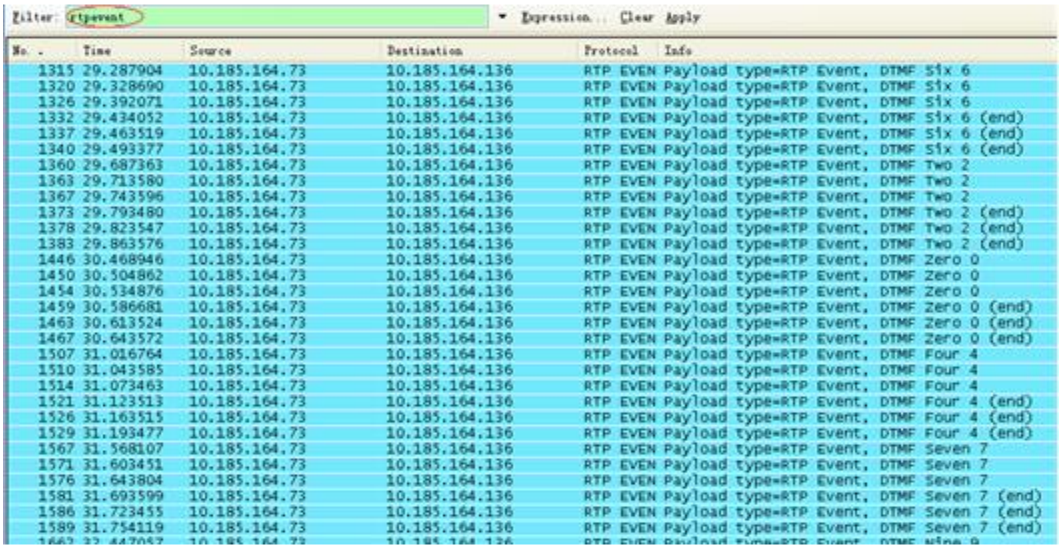
Using the RTP to Analyze 2833 Packets

To use the RTP to analyze 2833 packets, proceed as follows:

1. Use the Wireshark to open the bearer network port captured file in .pcap or .cap format.
2. Enter **(rtp) && (rtp.p_type** > **34)** or **rtpevent** in the **Filter** text box.
3. Press **Enter**.

   All files that are transferred using RFC 2833 in the captured information are filtered out, as shown in Figure 5-80.

Figure 5-80 RTP information

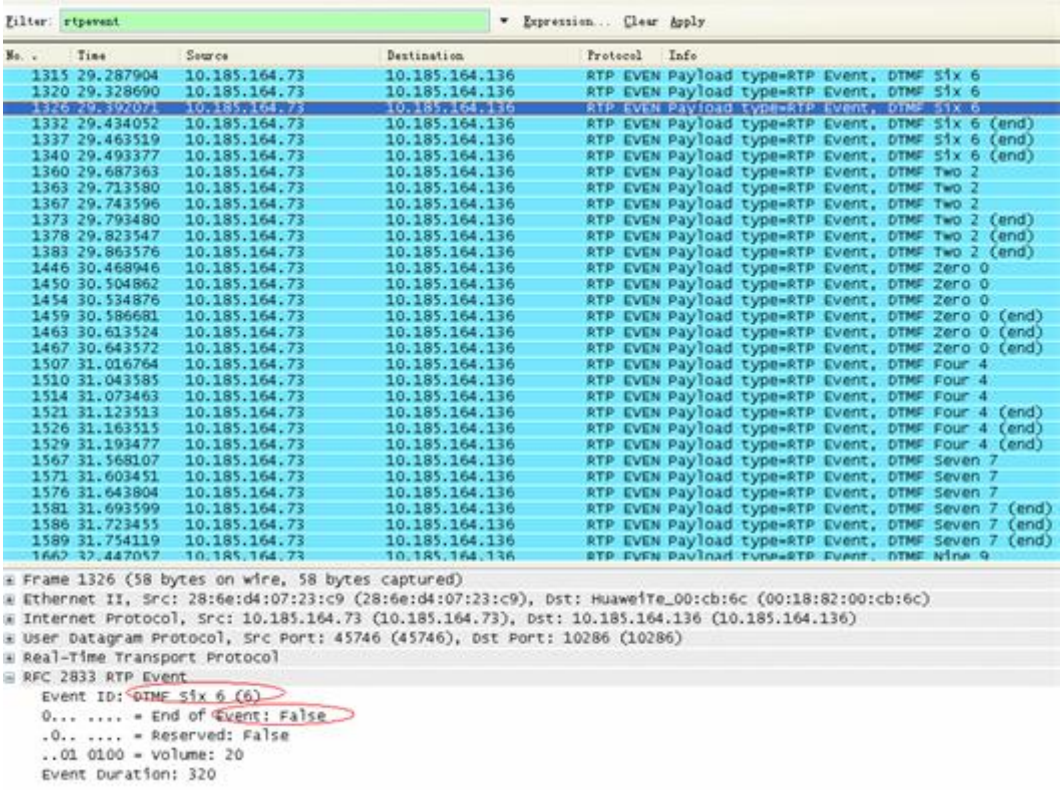


```
No. .  Time       Source          Destination      Protocol  Info
 1315 29.287904  10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Six 6
 1320 29.328690  10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Six 6
 1326 29.392071  10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Six 6
 1332 29.434052  10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Six 6 (end)
 1337 29.463519  10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Six 6 (end)
 1340 29.493377  10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Six 6 (end)
 1360 29.687363  10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Two 2
 1363 29.713580  10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Two 2
 1367 29.743596  10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Two 2
 1373 29.793480  10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Two 2 (end)
 1378 29.823547  10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Two 2 (end)
 1383 29.863576  10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Two 2 (end)
 1446 30.468946  10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Zero 0
 1450 30.504862  10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Zero 0
 1454 30.534876  10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Zero 0
 1459 30.586681  10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Zero 0 (end)
 1463 30.613524  10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Zero 0 (end)
 1467 30.643572  10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Zero 0 (end)
 1507 31.016764  10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Four 4
 1510 31.043585  10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Four 4
 1514 31.073463  10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Four 4
 1521 31.123513  10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Four 4 (end)
 1526 31.163515  10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Four 4 (end)
 1529 31.193477  10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Four 4 (end)
 1567 31.568107  10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Seven 7
 1571 31.603451  10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Seven 7
 1576 31.643804  10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Seven 7
 1581 31.693599  10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Seven 7 (end)
 1586 31.723455  10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Seven 7 (end)
 1589 31.754119  10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Seven 7 (end)
 1662 32.447057  10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Nine 9
```

2833 packets use the sampling mode to send a number for multiple times. Numbers are separated by RTP packets whose **Event** is **TRUE**, as shown in Figure 5-81. The procedure for sending the number 6 is used as an example.

- The message "End of Event: False" in the packet parsing area indicates that the number 6 has not been sent completely.

Figure 5-81 Message "End of Event: False"

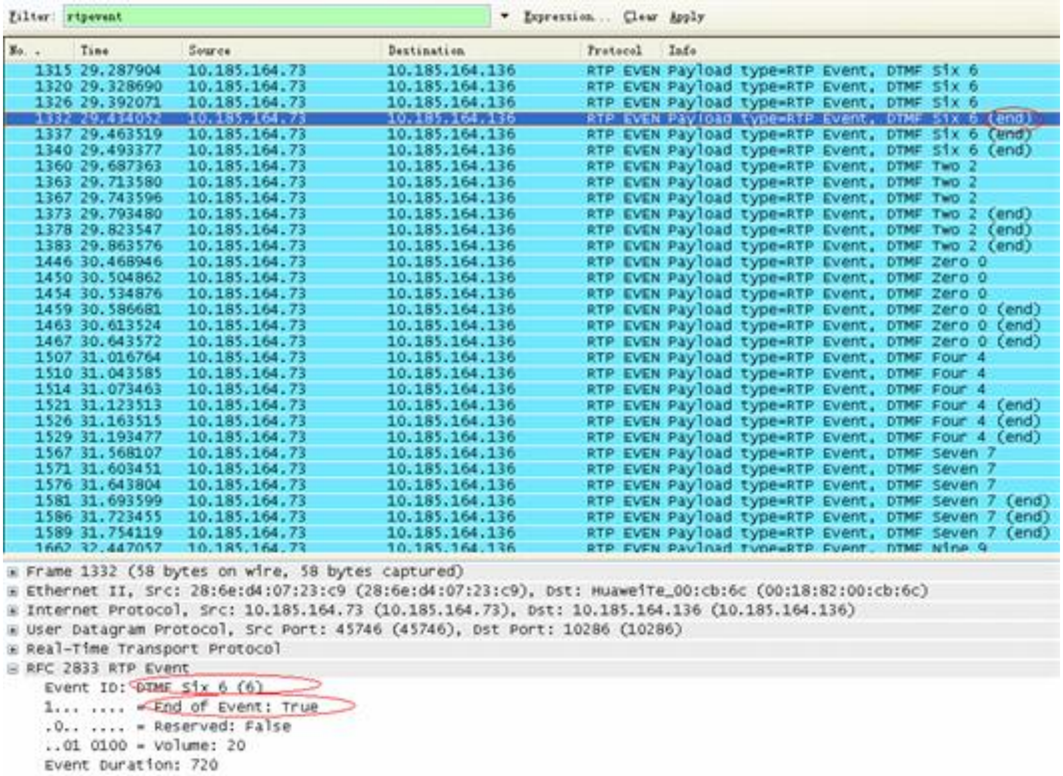


```
No. .   Time        Source          Destination      Protocol Info
  1315 29.287904   10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Six 6
  1320 29.328690   10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Six 6
  1326 29.392071   10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Six 6
  1332 29.434052   10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Six 6 (end)
  1337 29.463519   10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Six 6 (end)
  1340 29.493377   10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Six 6 (end)
  1360 29.687363   10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Two 2
  1363 29.713580   10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Two 2
  1367 29.743596   10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Two 2
  1373 29.793480   10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Two 2 (end)
  1378 29.823547   10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Two 2 (end)
  1383 29.863576   10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Two 2 (end)
  1446 30.468946   10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Zero 0
  1450 30.504862   10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Zero 0
  1454 30.534876   10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Zero 0
  1459 30.586681   10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Zero 0 (end)
  1463 30.613524   10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Zero 0 (end)
  1467 30.643572   10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Zero 0 (end)
  1507 31.016764   10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Four 4
  1510 31.043585   10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Four 4
  1514 31.073463   10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Four 4
  1521 31.123513   10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Four 4 (end)
  1526 31.163515   10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Four 4 (end)
  1529 31.193477   10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Four 4 (end)
  1567 31.568107   10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Seven 7
  1571 31.603451   10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Seven 7
  1576 31.643804   10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Seven 7
  1581 31.693599   10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Seven 7 (end)
  1586 31.723455   10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Seven 7 (end)
  1589 31.754119   10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Seven 7 (end)
  1662 32.447057   10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Nine 9
```

```
⊞ Frame 1326 (58 bytes on wire, 58 bytes captured)
⊞ Ethernet II, Src: 28:6e:d4:07:23:c9 (28:6e:d4:07:23:c9), Dst: HuaweiTe_00:cb:6c (00:18:82:00:cb:6c)
⊞ Internet Protocol, Src: 10.185.164.73 (10.185.164.73), Dst: 10.185.164.136 (10.185.164.136)
⊞ User Datagram Protocol, Src Port: 45746 (45746), Dst Port: 10286 (10286)
⊞ Real-Time Transport Protocol
⊟ RFC 2833 RTP Event
    Event ID: DTMF Six 6 (6)
    0... .... = End of Event: False
    .0.. .... = Reserved: False
    ..01 0100 = Volume: 20
    Event Duration: 320
```

- The message "End of Event: True" in the packet parsing area indicates that the number 6 has been sent to the media stream. Then the number collection process is complete.

Figure 5-82 Message "End of Event: True"



```
No. .  Time      Source          Destination      Protocol Info
  1315 29.287904 10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Six 6
  1320 29.328690 10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Six 6
  1326 29.392071 10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Six 6
  1332 29.434052 10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Six 6 (end)
  1337 29.463519 10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Six 6 (end)
  1340 29.493377 10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Six 6 (end)
  1360 29.687363 10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Two 2
  1363 29.713580 10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Two 2
  1367 29.743596 10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Two 2
  1373 29.793480 10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Two 2 (end)
  1378 29.823547 10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Two 2 (end)
  1383 29.863576 10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Two 2 (end)
  1446 30.468946 10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Zero 0
  1450 30.504862 10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Zero 0
  1454 30.534876 10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Zero 0
  1459 30.586681 10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Zero 0 (end)
  1463 30.613524 10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Zero 0 (end)
  1467 30.643572 10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Zero 0 (end)
  1507 31.016764 10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Four 4
  1510 31.043585 10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Four 4
  1514 31.073463 10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Four 4
  1521 31.123513 10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Four 4 (end)
  1526 31.163515 10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Four 4 (end)
  1529 31.193477 10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Four 4 (end)
  1567 31.568107 10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Seven 7
  1571 31.603451 10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Seven 7
  1576 31.643804 10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Seven 7
  1581 31.693599 10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Seven 7 (end)
  1586 31.723455 10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Seven 7 (end)
  1589 31.754119 10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Seven 7 (end)
  1662 32.447057 10.185.164.73   10.185.164.136   RTP EVEN Payload type=RTP Event, DTMF Nine 9
```

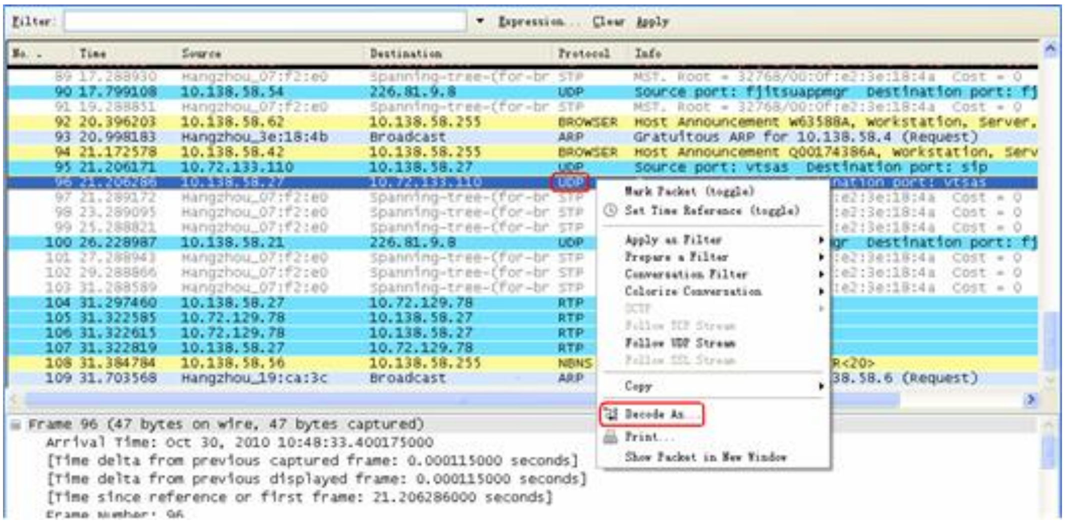
```
⊞ Frame 1332 (58 bytes on wire, 58 bytes captured)
⊞ Ethernet II, Src: 28:6e:d4:07:23:c9 (28:6e:d4:07:23:c9), Dst: HuaweiTe_00:cb:6c (00:18:82:00:cb:6c)
⊞ Internet Protocol, Src: 10.185.164.73 (10.185.164.73), Dst: 10.185.164.136 (10.185.164.136)
⊞ User Datagram Protocol, Src Port: 45746 (45746), Dst Port: 10286 (10286)
⊞ Real-Time Transport Protocol
⊟ RFC 2833 RTP Event
    Event ID: DTMF Six 6 (6)
    1... .... = End of Event: True
    .0.. .... = Reserved: False
    ..01 0100 = Volume: 20
    Event Duration: 720
```

To convert the captured UDP packets to RTP packets, go to 4.

4. Right-click a signaling record in the **UDP** column.

   A shortcut menu is displayed, as shown in Figure 5-83.

Figure 5-83 Displayed shortcut menu



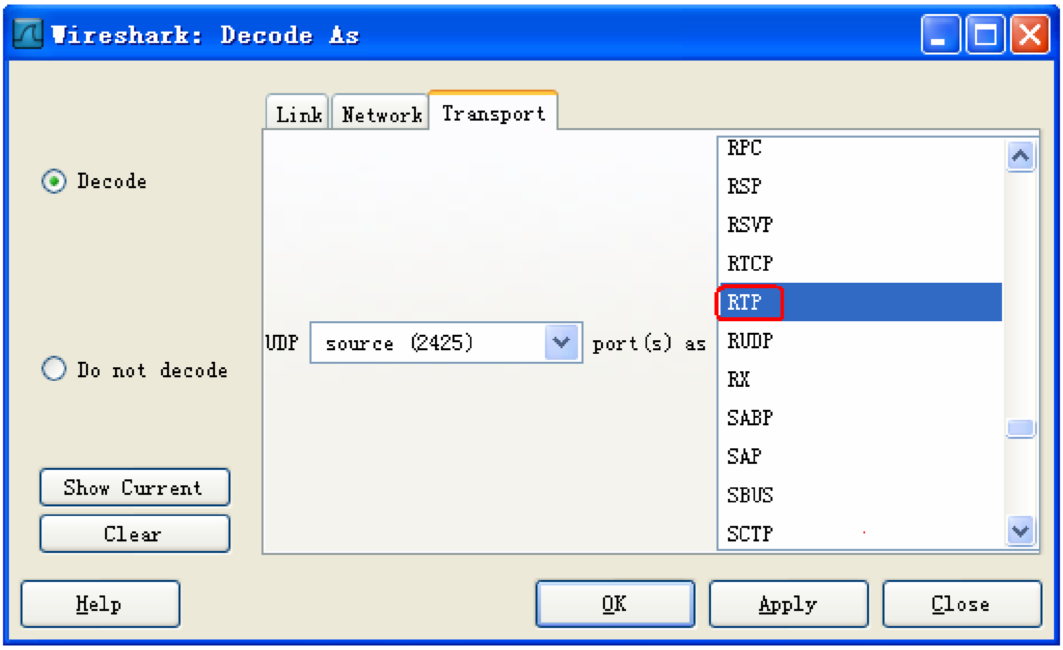
```
No. .  Time      Source              Destination          Protocol Info
    89 17.288930 Hangzhou_07:f2:e0   Spanning-tree-(for-br STP     MST. Root = 32768/00:0f:e2:3e:18:4a  Cost = 0
    90 17.799108 10.138.58.54        226.81.9.8           UDP      Source port: fjitsuappmgr  Destination port: fj
    91 19.288851 Hangzhou_07:f2:e0   Spanning-tree-(for-br STP     MST. Root = 32768/00:0f:e2:3e:18:4a  Cost = 0
    92 20.396203 10.138.58.62        10.138.58.255        BROWSER  Host Announcement W63588A, Workstation, Server,
    93 20.998183 Hangzhou_3e:18:4b   Broadcast            ARP      Gratuitous ARP for 10.138.58.4 (Request)
    94 21.172578 10.138.58.42        10.138.58.255        BROWSER  Host Announcement Q00174386A, Workstation, Serv
    95 21.206171 10.72.133.110       10.138.58.27         UDP      Source port: vtsas  Destination port: sip
    96 21.206286 10.138.58.27        10.72.133.110        UDP                                  nation port: vtsas
    97 21.289172 Hangzhou_07:f2:e0   Spanning-tree-(for-br STP                                 :e2:3e:18:4a  Cost = 0
    98 23.289095 Hangzhou_07:f2:e0   Spanning-tree-(for-br STP                                 :e2:3e:18:4a  Cost = 0
    99 25.288821 Hangzhou_07:f2:e0   Spanning-tree-(for-br STP                                 :e2:3e:18:4a  Cost = 0
   100 26.228987 10.138.58.21        226.81.9.8           UDP                                  gr  Destination port: fj
   101 27.288943 Hangzhou_07:f2:e0   Spanning-tree-(for-br STP                                 :e2:3e:18:4a  Cost = 0
   102 29.288866 Hangzhou_07:f2:e0   Spanning-tree-(for-br STP                                 :e2:3e:18:4a  Cost = 0
   103 31.288589 Hangzhou_07:f2:e0   Spanning-tree-(for-br STP                                 :e2:3e:18:4a  Cost = 0
   104 31.297460 10.138.58.27        10.72.129.78         RTP
   105 31.322585 10.72.129.78        10.138.58.27         RTP
   106 31.322615 10.72.129.78        10.138.58.27         RTP
   107 31.322819 10.138.58.27        10.72.129.78         RTP
   108 31.384784 10.138.58.56        10.138.58.255        NBNS                                 R<20>
   109 31.703568 Hangzhou_19:ca:3c   Broadcast            ARP                                  38.58.6 (Request)
```

```
⊟ Frame 96 (47 bytes on wire, 47 bytes captured)
    Arrival Time: Oct 30, 2010 10:48:33.400175000
    [Time delta from previous captured frame: 0.000115000 seconds]
    [Time delta from previous displayed frame: 0.000115000 seconds]
    [Time since reference or first frame: 21.206286000 seconds]
    Frame Number: 96
```

5. Choose **Decode As...**.

   The **Decode As** dialog box is displayed, as shown in Figure 5-84.

Figure 5-84 Decode As



Wireshark: Decode As

● Decode

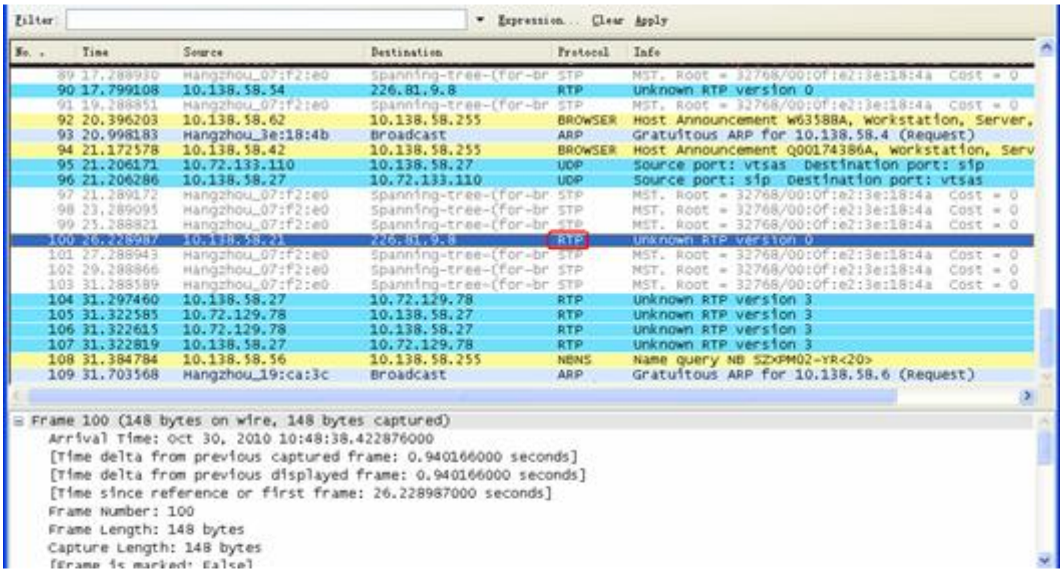
○ Do not decode

UDP source (2425) port(s) as RTP

6. Select **RTP** on the right pane.
7. Click **OK**.

   A page shown in Figure 5-85 is displayed. The captured UDP packets have been converted to RTP packets. Then perform 1 through 3 to verify that the packet information has been transmitted to the media stream.

Figure 5-85 Converting UDP packets to RTP packets



```
No. .  Time       Source               Destination           Protocol  Info
 89 17.288930  Hangzhou_07:f2:e0    Spanning-tree-(for-br STP       MST. Root = 32768/00:0f:e2:3e:18:4a  Cost = 0
 90 17.799108  10.138.58.54         226.81.9.8            RTP       Unknown RTP version 0
 91 19.288851  Hangzhou_07:f2:e0    Spanning-tree-(for-br STP       MST. Root = 32768/00:0f:e2:3e:18:4a  Cost = 0
 92 20.396203  10.138.58.62         10.138.58.255         BROWSER   Host Announcement W63588A, Workstation, Server,
 93 20.998183  Hangzhou_3e:18:4b    Broadcast             ARP       Gratuitous ARP for 10.138.58.4 (Request)
 94 21.172578  10.138.58.42         10.138.58.255         BROWSER   Host Announcement Q00174386A, Workstation, Serv
 95 21.206171  10.72.133.110        10.138.58.27          UDP       Source port: vtsas  Destination port: sip
 96 21.206286  10.138.58.27         10.72.133.110         UDP       Source port: sip  Destination port: vtsas
 97 21.289172  Hangzhou_07:f2:e0    Spanning-tree-(for-br STP       MST. Root = 32768/00:0f:e2:3e:18:4a  Cost = 0
 98 23.289095  Hangzhou_07:f2:e0    Spanning-tree-(for-br STP       MST. Root = 32768/00:0f:e2:3e:18:4a  Cost = 0
 99 25.288821  Hangzhou_07:f2:e0    Spanning-tree-(for-br STP       MST. Root = 32768/00:0f:e2:3e:18:4a  Cost = 0
100 26.228987  10.138.58.21         226.81.9.8            RTP       Unknown RTP version 0
101 27.288943  Hangzhou_07:f2:e0    Spanning-tree-(for-br STP       MST. Root = 32768/00:0f:e2:3e:18:4a  Cost = 0
102 29.288866  Hangzhou_07:f2:e0    Spanning-tree-(for-br STP       MST. Root = 32768/00:0f:e2:3e:18:4a  Cost = 0
103 31.288589  Hangzhou_07:f2:e0    Spanning-tree-(for-br STP       MST. Root = 32768/00:0f:e2:3e:18:4a  Cost = 0
104 31.297460  10.138.58.27         10.72.129.78          RTP       Unknown RTP version 3
105 31.322585  10.72.129.78         10.138.58.27          RTP       Unknown RTP version 3
106 31.322615  10.72.129.78         10.138.58.27          RTP       Unknown RTP version 3
107 31.322819  10.138.58.27         10.72.129.78          RTP       Unknown RTP version 3
108 31.384784  10.138.58.56         10.138.58.255         NBNS      Name query NB SZXPM02-YR<20>
109 31.703568  Hangzhou_19:ca:3c    Broadcast             ARP       Gratuitous ARP for 10.138.58.6 (Request)
```

```
⊟ Frame 100 (148 bytes on wire, 148 bytes captured)
    Arrival Time: Oct 30, 2010 10:48:38.422876000
    [Time delta from previous captured frame: 0.940166000 seconds]
    [Time delta from previous displayed frame: 0.940166000 seconds]
    [Time since reference or first frame: 26.228987000 seconds]
    Frame Number: 100
    Frame Length: 148 bytes
    Capture Length: 148 bytes
    [Frame is marked: False]
```

Viewing Call Processes

The Wireshark allows you to view call processes and play voice recordings. The procedure is as follows:

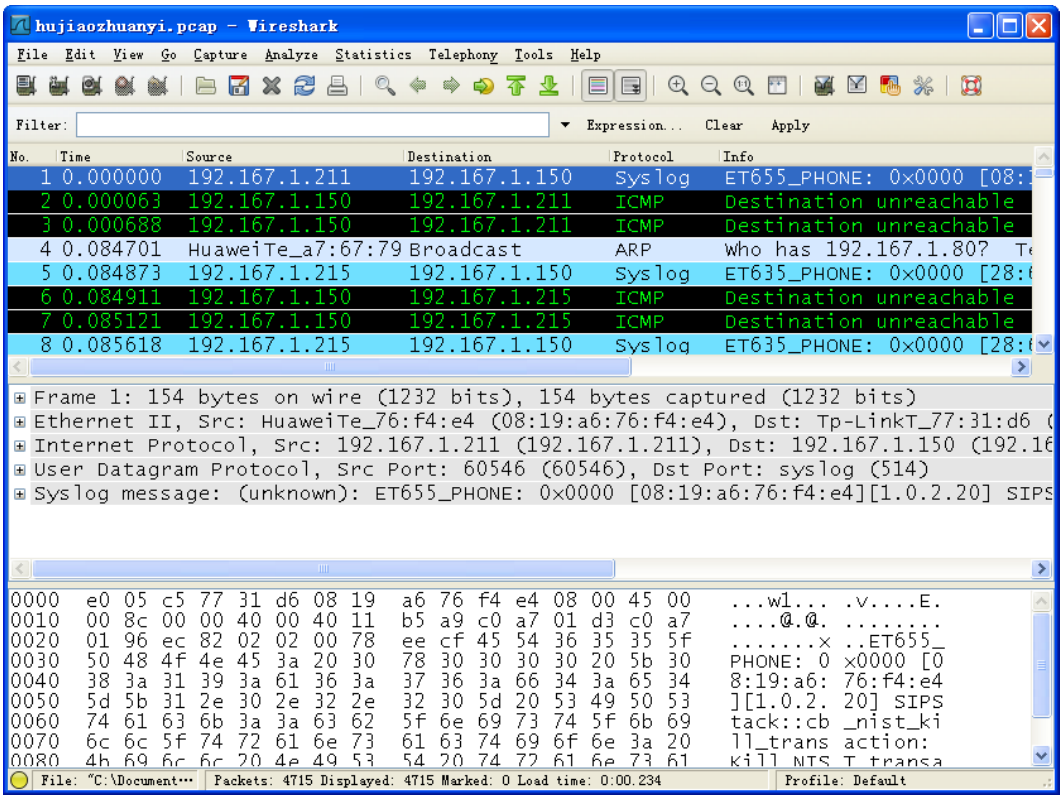
NOTE

This topic describes how to view the call forwarding process. First you need to capture the data packets related to call forwarding and save the captured packets as a .pcap file, such as **hujiaozhuanyi.pcap**.

1. Double-click **hujiaozhuanyi.pcap** on the PC.

   The system shows the call forwarding data, as shown in Figure 5-86.

Figure 5-86 Call forwarding



```
No. Time       Source              Destination    Protocol Info
  1 0.000000   192.167.1.211       192.167.1.150  Syslog   ET655_PHONE: 0x0000 [08:1
  2 0.000063   192.167.1.150       192.167.1.211  ICMP     Destination unreachable
  3 0.000688   192.167.1.150       192.167.1.211  ICMP     Destination unreachable
  4 0.084701   HuaweiTe_a7:67:79   Broadcast      ARP      Who has 192.167.1.80?  Te
  5 0.084873   192.167.1.215       192.167.1.150  Syslog   ET635_PHONE: 0x0000 [28:6
  6 0.084911   192.167.1.150       192.167.1.215  ICMP     Destination unreachable
  7 0.085121   192.167.1.150       192.167.1.215  ICMP     Destination unreachable
  8 0.085618   192.167.1.215       192.167.1.150  Syslog   ET635_PHONE: 0x0000 [28:6
```

```
⊞ Frame 1: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits)
⊞ Ethernet II, Src: HuaweiTe_76:f4:e4 (08:19:a6:76:f4:e4), Dst: Tp-LinkT_77:31:d6 (
⊞ Internet Protocol, Src: 192.167.1.211 (192.167.1.211), Dst: 192.167.1.150 (192.16
⊞ User Datagram Protocol, Src Port: 60546 (60546), Dst Port: syslog (514)
⊞ Syslog message: (unknown): ET655_PHONE: 0x0000 [08:19:a6:76:f4:e4][1.0.2.20] SIPS
```

```
0000  e0 05 c5 77 31 d6 08 19  a6 76 f4 e4 08 00 45 00   ...w1... .v....E.
0010  00 8c 00 00 40 00 40 11  b5 a9 c0 a7 01 d3 c0 a7   ....@.@. ........
0020  01 96 ec 82 02 02 00 78  ee cf 45 54 36 35 35 5f   .......x ..ET655_
0030  50 48 4f 4e 45 3a 20 30  78 30 30 30 30 20 5b 30   PHONE: 0 x0000 [0
0040  38 3a 31 39 3a 61 36 3a  37 36 3a 66 34 3a 65 34   8:19:a6: 76:f4:e4
0050  5d 5b 31 2e 30 2e 32 2e  32 30 5d 20 53 49 50 53   ][1.0.2. 20] SIPS
0060  74 61 63 6b 3a 3a 63 62  5f 6e 69 73 74 5f 6b 69   tack::cb _nist_ki
0070  6c 6c 5f 74 72 61 6e 73  61 63 74 69 6f 6e 3a 20   ll_trans action:
0080  4b 69 6c 6c 20 4e 49 53  54 20 74 72 61 6e 73 61   Kill NIST T transa
```

```
File: "C:\Document…   Packets: 4715 Displayed: 4715 Marked: 0 Load time: 0:00.234   Profile: Default
```

2. Select a data packet record and choose **Telephony** > **VoIP Calls**.

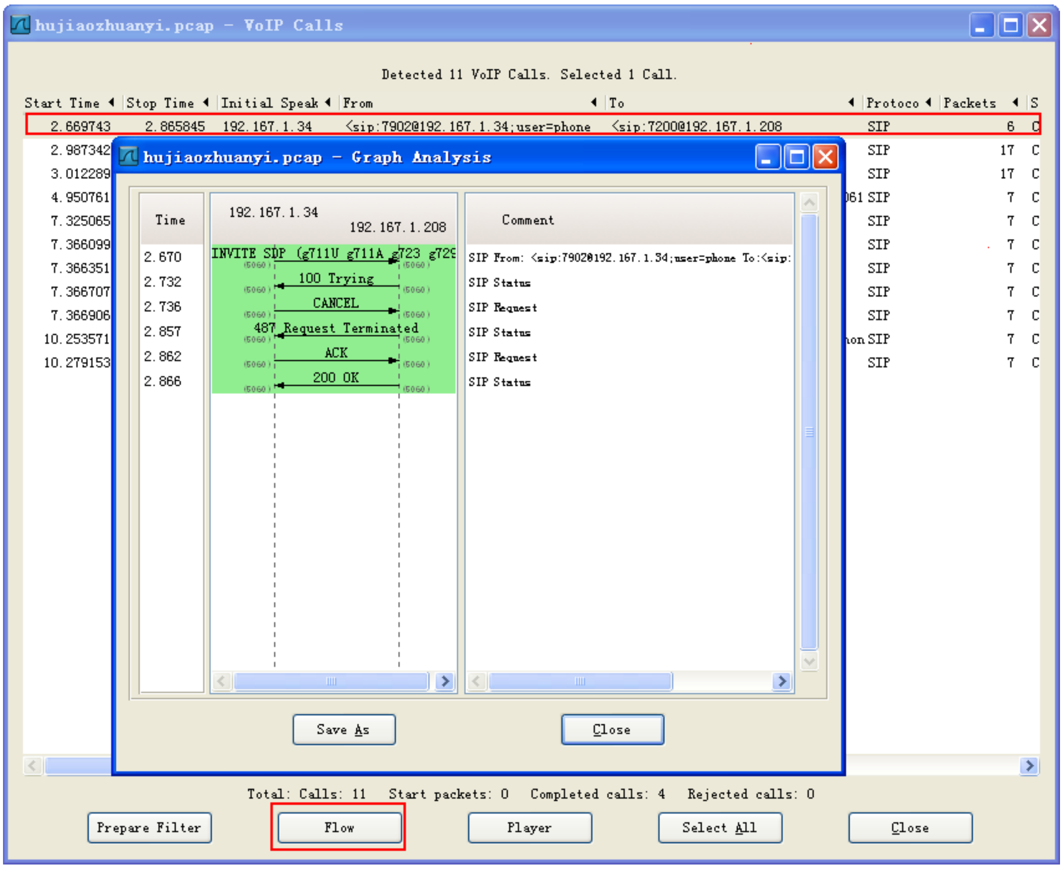
   The **VoIP Calls** page is displayed.

3. View the call process.

   a. Select a call record and click **Flow**.

      The **Graph Analysis** page is displayed, as shown in Figure 5-87.

Figure 5-87 Call process



hujiaozhuanyi.pcap - VoIP Calls
hujiaozhuanyi.pcap - Graph Analysis
Save As
Close
Prepare Filter
Flow
Player
Select All
Close

Detected 11 VoIP Calls. Selected 1 Call.

Start Time	Stop Time	Initial Speak	From	To	Protoco	Packets	S
2.669743	2.865845	192.167.1.34	<sip:7902@192.167.1.34;user=phone	<sip:7200@192.167.1.208	SIP	6	C
2.987342					SIP	17	C
3.012289					SIP	17	C
4.950761				061	SIP	7	C
7.325065					SIP	7	C
7.366099					SIP	7	C
7.366351					SIP	7	C
7.366707					SIP	7	C
7.366906					SIP	7	C
10.253571				hon	SIP	7	C
10.279153					SIP	7	C

Time	192.167.1.34 → 192.167.1.208	Comment
2.670	INVITE SDP (g711U g711A g723 g729	SIP From: <sip:7902@192.167.1.34;user=phone To:<sip:
2.732	100 Trying	SIP Status
2.736	CANCEL	SIP Request
2.857	487 Request Terminated	SIP Status
2.862	ACK	SIP Request
2.866	200 OK	SIP Status

Total: Calls: 11 Start packets: 0 Completed calls: 4 Rejected calls: 0

NOTE

To select all call records, click **Select All**.

b. (Optional) Click **Save as**.

Specify a path and file type, and enter the file name in the **Save file as** dialog box, and then click **Save**.

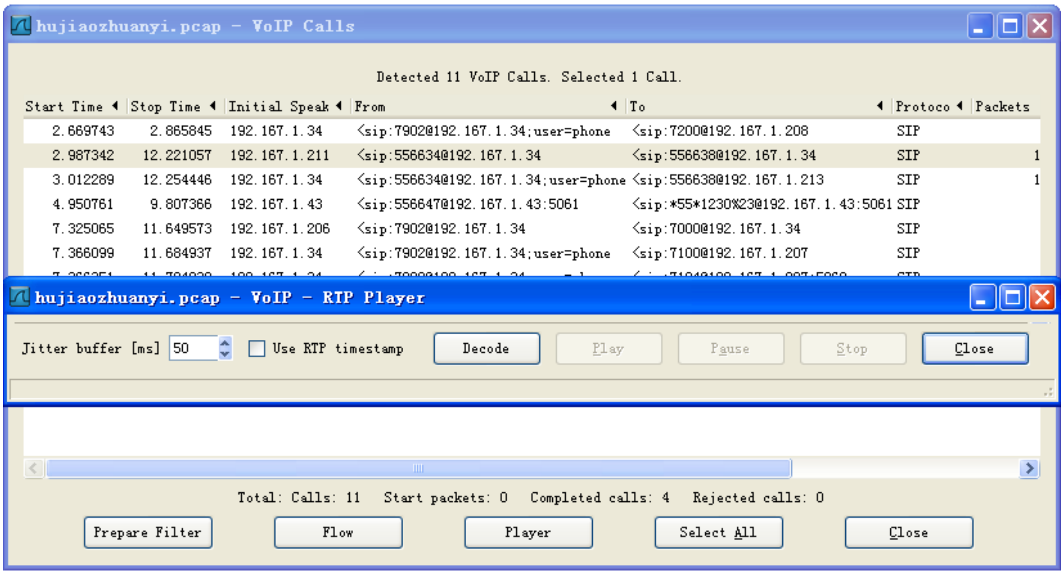
c. Click **Close**.

4. Play the voice recording.

a. Select a call record and click **Player**.

The **VoIP-RTP Player** page is displayed, as shown in Figure 5-88.

Figure 5-88 VoIP-RTP Player



Detected 11 VoIP Calls. Selected 1 Call.

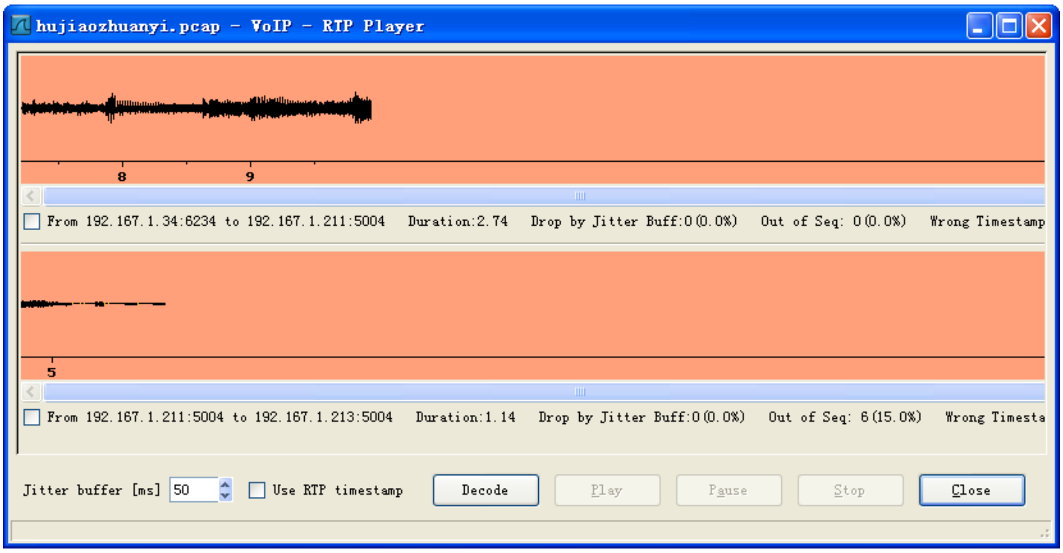
Start Time	Stop Time	Initial Speak	From	To	Protoco	Packets
2.669743	2.865845	192.167.1.34	<sip:7902@192.167.1.34;user=phone	<sip:7200@192.167.1.208	SIP	
2.987342	12.221057	192.167.1.211	<sip:556634@192.167.1.34	<sip:556638@192.167.1.34	SIP	1
3.012289	12.254446	192.167.1.34	<sip:556634@192.167.1.34;user=phone	<sip:556638@192.167.1.213	SIP	1
4.950761	9.807366	192.167.1.43	<sip:556647@192.167.1.43:5061	<sip:*55*1230%23@192.167.1.43:5061	SIP	
7.325065	11.649573	192.167.1.206	<sip:7902@192.167.1.34	<sip:7000@192.167.1.34	SIP	
7.366099	11.684937	192.167.1.34	<sip:7902@192.167.1.34;user=phone	<sip:7100@192.167.1.207	SIP	

Total: Calls: 11 Start packets: 0 Completed calls: 4 Rejected calls: 0

b. Click **Decode**.

The voice recording page is played is displayed, as shown in Figure 5-89.

Figure 5-89 Voice recordings



□ From 192.167.1.34:6234 to 192.167.1.211:5004 Duration:2.74 Drop by Jitter Buff:0(0.0%) Out of Seq: 0(0.0%) Wrong Timestamp

□ From 192.167.1.211:5004 to 192.167.1.213:5004 Duration:1.14 Drop by Jitter Buff:0(0.0%) Out of Seq: 6(15.0%) Wrong Timesta

c. Select one or more voice recordings, and click **Play**.

The system plays the recordings one by one.

NOTE

You can click **Pause** or **Stop** to stop the play.

d. Click **Close**.