

Yealink



Ultra-elegant SIP-T4X IP Phones Administrator Guide

Version 72.1

Dec. 2013

Copyright

Copyright © 2013 YEALINK NETWORK TECHNOLOGY

Copyright © 2013 Yealink Network Technology CO., LTD. All rights reserved. No parts of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, photocopying, recording, or otherwise, for any purpose, without the express written permission of Yealink Network Technology CO., LTD. Under the law, reproducing includes translating into another language or format.

When this publication is made available on media, Yealink Network Technology CO., LTD. gives its consent to downloading and printing copies of the content provided in this file only for private use but not for redistribution. No parts of this publication may be subject to alteration, modification or commercial use. Yealink Network Technology CO., LTD. will not be liable for any damages arising from use of an illegally modified or altered publication.

Warranty

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS GUIDE ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS GUIDE ARE BELIEVED TO BE ACCURATE AND PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF PRODUCTS.

YEALINK NETWORK TECHNOLOGY CO., LTD. MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS GUIDE, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Yealink Network Technology CO., LTD. shall not be liable for errors contained herein nor for incidental or consequential damages in connection with the furnishing, performance, or use of this guide.

Declaration of Conformity



Hereby, Yealink Network Technology CO., LTD. declares that this phone is in conformity with the essential requirements and other relevant provisions of the CE, FCC.

CE Mark Warning

This device is marked with the CE mark in compliance with EC Directives 2006/95/EC and 2004/108/EC.

Part 15 FCC Rules

This device is compliant with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

Class B Digital Device or Peripheral

Note: This device is tested and complies with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

WEEE Warning



To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Customer Feedback

We are striving to improve our documentation quality and we appreciate your feedback. Email your opinions and comments to DocsFeedback@yealink.com.

GNU GPL INFORMATION

Yealink SIP-T4X IP phone firmware contains third-party software under the GNU General Public License (GPL). Yealink uses software under the specific terms of the GPL. Please refer to the GPL for the exact terms and conditions of the license.

The original GPL license, source code of components licensed under GPL and used in Yealink products can be downloaded online:

<http://www.yealink.com/GPLOpenSource.aspx?BaseInfoCatelId=293&NewsCatelId=293&CatelId=293>.

About This Guide

The guide is intended for administrators who need to properly configure, customize, manage, and troubleshoot the IP phone system rather than the end-users. It provides details on the functionality and configuration of SIP-T4X IP phones.

Many of the features described in this guide involve network settings, which could affect the IP phone's performance in the network. So an understanding of the IP networking and prior knowledge of IP telephony concepts are necessary.

Documentations

This guide covers SIP-T46G, T42G and T41P IP phones. The following related documents for SIP-T4X IP phones are available:

- Quick Installation Guides, which describe how to assemble IP phones.
- Quick Reference Guides, which describe the most basic features available on IP phones.
- User Guides, which describe basic and advanced features available on IP phones.
- Auto Provisioning Deployment Guide, which describes how to provision IP phones using the configuration files.
- Configuration Conversion Tool User Guide, which describes how to convert and encrypt the configuration files using the Configuration Conversion Tool.
- <y0000000000xx>.cfg and <MAC>.cfg template configuration files.
- IP Phones Deployment Guide for BroadSoft UC-One Environments, which describes how to configure the BroadSoft features on the BroadWorks web portal and IP phones.

For support or service, please contact your Yealink reseller or go to Yealink Technical Support online: <http://www.yealink.com/Support.aspx>.

In This Guide

The information detailed in this guide is applicable to the firmware version 72 or higher. The firmware format is like x.x.x.x.rom. The second x from left should be greater than or equal to 72 (e.g., the firmware version of SIP-T46G IP phone: 28.72.0.10.rom). This administrator guide includes the following chapters:

- Chapter 1, "[Product Overview](#)" describes SIP components and SIP IP phones.
- Chapter 2, "[Getting Started](#)" describes how to install and connect IP phones and configuration methods.

- Chapter 3, "[Configuring Basic Features](#)" describes how to configure basic features on IP phones.
- Chapter 4, "[Configuring Advanced Features](#)" describes how to configure advanced features on IP phones.
- Chapter 5, "[Configuring Audio Features](#)" describes how to configure audio features on IP phones.
- Chapter 6, "[Configuring Security Features](#)" describes how to configure security features on IP phones.
- Chapter 7, "[Upgrading Firmware](#)" describes how to upgrade the firmware of IP phones.
- Chapter 8, "[Resource Files](#)" describes the resource files that can be downloaded by IP phones.
- Chapter 9, "[Troubleshooting](#)" describes how to troubleshoot IP phones and provides some common troubleshooting solutions.
- Chapter 10, "[Appendix](#)" provides the glossary, reference information about IP phones compliant with RFC 3261, SIP call flows and sample configuration files.

Summary of Changes

This section describes the changes to this guide for each release and guide version.

Changes for Release 72, Guide Version 72.1

The following sections are new for this version:

- [Power Indicator LED](#) on page 36
- [Contrast](#) on page 38

Major updates have occurred to the following sections:

- [DHCP](#) on page 18
- [Backlight](#) on page 41
- [Time and Date](#) on page 47
- [Key as Send](#) on page 59
- [Anonymous Call](#) on page 75
- [Busy Lamp Field](#) on page 136
- [Action URL](#) on page 156
- [IPv6 Support](#) on page 187
- [Transport Layer Security](#) on page 203

Changes for Release 71.0, Guide Version 71.181

Major updates have occurred to the following section:

- [Language](#) on page 52

Changes for Release 71.0, Guide Version 71.180

Major updates have occurred to the following sections:

- [Language](#) on page 52
- [Anonymous Call](#) on page 75

Changes for Release 71.0, Guide Version 71.171

Major updates have occurred to the following sections:

- [Backlight](#) on page 41
- [Language](#) on page 52
- [Logo Customization](#) on page 55
- [Anonymous Call](#) on page 75
- [Action URL](#) on page 156
- [Action URI](#) on page 159
- [Audio Codecs](#) on page 193

Changes for Release 71.0, Guide Version 71.170

Major updates have occurred to the following sections:

- [Language](#) on page 52
- [Auto Answer](#) on page 72
- [Audio Codecs](#) on page 193
- [Encrypting Configuration Files](#) on page 211

Changes for Release 71.0, Guide Version 71.150

This version is updated to incorporate T41P as one of the T4X device models. The following section is new for this version:

- [Logo Customization](#) on page 55

Major updates have occurred to the following sections:

- [SIP IP Phone Models](#) on page 3
- [Configuring Transmission Methods of the Internet Port and PC Port](#) on page 25
- [Language](#) on page 52
- [Remote Phone Book](#) on page 131
- [Server Redundancy](#) on page 162
- [Audio Codecs](#) on page 193
- [Transport Layer Security](#) on page 203
- [Secure Real-Time Transport Protocol](#) on page 209

Changes for Release 71.0, Guide Version 71.80

This version is updated to incorporate T42G as one of the T4X device models. The following section is new for this version:

- [SIP IP Phone Models](#) on page 3

Major updates have occurred to the following sections:

- [Reading Icons](#) on page 16
- [PPPoE](#) on page 24
- [Backlight](#) on page 41
- [Language](#) on page 52
- [Call Completion](#) on page 74
- [TR-069 Device Management](#) on page 185
- [IPv6 Support](#) on page 187
- [Audio Codecs](#) on page 193
- [Upgrading Firmware](#) on page 215
- [Configuring DSS Key](#) on page 381

Table of Contents

About This Guide	v
Documentations.....	v
In This Guide	v
Summary of Changes	vi
Changes for Release 72, Guide Version 72.1.....	vi
Changes for Release 71.0, Guide Version 71.181.....	vii
Changes for Release 71.0, Guide Version 71.180.....	vii
Changes for Release 71.0, Guide Version 71.171.....	vii
Changes for Release 71.0, Guide Version 71.170.....	vii
Changes for Release 71.0, Guide Version 71.150.....	vii
Changes for Release 71.0, Guide Version 71.80.....	viii
Table of Contents	ix
Product Overview.....	1
VoIP Principle.....	1
SIP Components.....	2
SIP IP Phone Models.....	3
Physical Features of SIP-T4X IP Phones	4
Key Features of SIP-T4X IP Phones	6
Getting Started.....	9
Connecting the IP Phone.....	9
Initialization Process Overview	12
Verifying Startup	14
Configuration Methods.....	14
Phone User Interface.....	14
Web User Interface	14
Configuration Files.....	15
Reading Icons	16
Configuring Basic Network Parameters	18
DHCP	18
Configuring Network Parameters Manually	21
PPPoE	24
Configuring Transmission Methods of the Internet Port and PC Port	25
Creating Dial Plan	28

Replace Rule	29
Dial-now	30
Area Code.....	32
Block Out.....	33

Configuring Basic Features 35

Power Indicator LED	36
Contrast	38
Wallpaper.....	39
Backlight.....	41
User Password	42
Administrator Password	43
Phone Lock	44
Time and Date	47
Language	52
Loading Language Packs	53
Specifying the Language to Use.....	54
Logo Customization	55
Softkey Layout.....	56
Key as Send	59
Hotline	61
Call Log.....	63
Missed Call Log	64
Local Directory.....	65
Live Dialpad.....	68
Call Waiting.....	68
Auto Redial.....	70
Auto Answer.....	72
Call Completion.....	74
Anonymous Call.....	75
Anonymous Call Rejection	77
Do Not Disturb.....	79
Busy Tone Delay.....	83
Return Code When Refuse	84
Early Media.....	85
180 Ring Workaround.....	86
Use Outbound Proxy in Dialog.....	87
SIP Session Timer	88
Session Timer	89
Call Hold.....	90
Call Forward	92
Call Transfer	98
Network Conference	100
Transfer on Conference Hang Up	101

Directed Call Pickup.....	102
Group Call Pickup.....	105
Dialog-Info Call Pickup.....	108
Call Return.....	110
Call Park.....	111
Web Server Type.....	112
Calling Line Identification Presentation.....	114
Connected Line Identification Presentation.....	115
DTMF.....	116
Suppress DTMF Display.....	119
Transfer via DTMF.....	120
Intercom.....	121
Outgoing Intercom Calls.....	121
Incoming Intercom Calls.....	122
Configuring Advanced Features.....	125
Distinctive Ring Tones.....	125
Tones.....	129
Remote Phone Book.....	131
LDAP.....	133
Busy Lamp Field.....	136
Music on Hold.....	141
Automatic Call Distribution.....	142
Message Waiting Indicator.....	144
Multicast Paging.....	147
Sending RTP Stream.....	147
Receiving RTP Stream.....	149
Call Recording.....	151
Hot Desking.....	155
Action URL.....	156
Action URI.....	159
Server Redundancy.....	162
SIP Server Domain Name Resolution.....	164
LLDP.....	167
VLAN.....	170
VPN.....	174
Quality of Service.....	176
Network Address Translation.....	178
802.1X Authentication.....	180
TR-069 Device Management.....	185
IPv6 Support.....	187
Configuring Audio Features.....	191

Headset Prior	191
Dual Headset	192
Audio Codecs	193
Acoustic Clarity Technology.....	197
Acoustic Echo Cancellation	197
Voice Activity Detection	198
Comfort Noise Generation	199
Jitter Buffer	200
Configuring Security Features.....	203
Transport Layer Security.....	203
Secure Real-Time Transport Protocol.....	209
Encrypting Configuration Files	211
Upgrading Firmware.....	215
Resource Files	219
Replace Rule Template	219
Dial-now Template.....	220
Softkey Layout Template.....	221
Local Contact File	223
Remote XML Phone Book.....	224
Directory Template	226
Super Search Template.....	227
Specifying the Access URL of Resource Files	228
Troubleshooting	231
Troubleshooting Methods	231
Viewing Log Files.....	231
Capturing Packets	234
Enabling the Watch Dog Feature.....	234
Getting Information from Status Indicators.....	235
Analyzing Configuration Files	235
Troubleshooting Solutions	236
Why is the LCD screen blank?	236
Why doesn't the IP phone get an IP address?	236
How do I find the basic information of the IP phone?.....	237
Why doesn't the IP phone upgrade firmware successfully?.....	237
Why doesn't the IP phone display time and date correctly?	237
Why do I get poor sound quality during a call?	237
What is the difference between a remote phone book and a local phonebook?	238
What is the difference between user name, register name and display name?	238

How to reboot IP phone remotely?.....	238
How to increase or decrease the volume?.....	238
What will happen if I connect both PoE cable and power adapter? Which has the higher priority?.....	239
What is auto provisioning?	239
What is PnP?	239
Why doesn't the IP phone update the configuration?	239
What do "on code" and "off code" mean?	239
How to solve the IP conflict problem?	240
How to reset your phone to factory configurations?.....	240
How to restore the administrator password?	241
Appendix	243
Appendix A: Glossary.....	243
Appendix B: Time Zones.....	245
Appendix C: Configuration Parameters.....	248
Setting Parameters in Configuration Files.....	248
Basic and Advanced Feature Parameters.....	248
Audio Feature Parameters.....	359
Upgrading Firmware	371
Resource Files	374
Troubleshooting	379
Configuring DSS Key	381
Appendix D: SIP (Session Initiation Protocol).....	396
RFC and Internet Draft Support	396
SIP Request.....	399
SIP Header	400
SIP Responses	401
SIP Session Description Protocol (SDP) Usage	403
Appendix E: SIP Call Flows.....	404
Successful Call Setup and Disconnect	405
Unsuccessful Call Setup—Called User is Busy	407
Unsuccessful Call Setup—Called User Does Not Answer	410
Successful Call Setup and Call Hold	412
Successful Call Setup and Call Waiting	414
Call Transfer without Consultation	419
Call Transfer with Consultation.....	423
Always Call Forward.....	428
Busy Call Forward	432
No Answer Call Forward	435
Call Conference.....	438
Appendix F: Sample Configuration File	443
Index.....	449

Product Overview

This chapter contains the following information about SIP-T4X IP phones:

- [VoIP Principle](#)
- [SIP Components](#)
- [SIP IP Phone Models](#)

VoIP Principle

VoIP

VoIP (Voice over Internet Protocol) is a technology using the Internet Protocol instead of traditional Public Switch Telephone Network (PSTN) technology for voice communications.

It is a family of technologies, methodologies, communication protocols, and transmission techniques for the delivery of voice communications and multimedia sessions over IP networks. The H.323 and Session Initiation Protocol (SIP) are two popular VoIP protocols that are found in widespread implementation.

H.323

H.323 is a recommendation from the ITU Telecommunication Standardization Sector (ITU-T) that defines the protocols to provide audio-visual communication sessions on any packet network. The H.323 standard addresses call signaling and control, multimedia transport and control, and bandwidth control for point-to-point and multi-point conferences.

It is widely implemented by voice and video conference equipment manufacturers, is used within various Internet real-time applications such as GnuGK and NetMeeting and is widely deployed by service providers and enterprises for both voice and video services over IP networks.

SIP

SIP (Session Initiation Protocol) is the Internet Engineering Task Force's (IETF's) standard for multimedia conferencing over IP. It is an ASCII-based, application-layer control protocol (defined in RFC 3261) that can be used to establish, maintain, and terminate calls between two or more endpoints. Like other VoIP protocols, SIP is designed to address the functions of signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call.

SIP provides capabilities to:

- Determine the location of the target endpoint -- SIP supports address resolution, name mapping, and call redirection.
- Determine the media capabilities of the target endpoint -- Via Session Description Protocol (SDP), SIP determines the "lowest level" of common services between endpoints. Conferences are established using only the media capabilities that can be supported by all endpoints.
- Determine the availability of the target endpoint -- A call cannot be completed because the target endpoint is unavailable. SIP determines whether the called party is already on the IP phone or does not answer in the allotted number of rings. It then returns a message indicating why the target endpoint is unavailable.
- Establish a session between the origin and target endpoint -- The call can be completed, SIP establishes a session between endpoints. SIP also supports mid-call changes, such as the addition of another endpoint to the conference or the change of a media characteristic or codec.
- Handle the transfer and termination of calls -- SIP supports the transfer of calls from one endpoint to another. During a call transfer, SIP simply establishes a session between the transferee and a new endpoint (specified by the transferring party) and terminates the session between the transferee and the transferring party. At the end of a call, SIP terminates the sessions between all parties.

SIP Components

SIP is a peer-to-peer protocol. The peers in a session are called User Agents (UAs). A user agent can function as one of the following roles:

- User Agent Client (UAC) -- A client application that initiates the SIP request.
- User Agent Server (UAS) -- A server application that contacts the user when a SIP request is received and that returns a response on behalf of the user.

User Agent Client (UAC)

The UAC is an application that initiates up to six feasible SIP requests to the UAS. The six requests issued by the UAC are: INVITE, ACK, OPTIONS, BYE, CANCEL and REGISTER. When the SIP session is being initiated by the UAC SIP component, the UAC determines the information essential for the request, which is the protocol, the port and the IP address of the UAS to which the request is being sent. This information can be dynamic and will make it challenging to put through a firewall. For this reason, it may be recommended to open the specific application type on the firewall. The UAC is also capable of using the information in the request URI to establish the course of the SIP request to its destination, as the request URI always specifies the host which is essential. The port and protocol are not always specified by the request URI. Thus if the request does not specify a port or protocol, a default port or protocol is contacted. It may be

preferential to use this method when not using an application layer firewall. Application layer firewalls like to know what applications are flowing through which ports and it is possible to use content types of other applications other than the one you are trying to let through what has been denied.

User agent server (UAS)

UAS is a server that hosts the application responsible for receiving the SIP requests from a UAC, and on reception it returns a response to the request back to the UAC. The UAS may issue multiple responses to the UAC, not necessarily a single response.

Communication between UAC and UAS is client/server and peer-to-peer.

Typically, a SIP endpoint is capable of functioning as both a UAC and a UAS, but it functions only as one or the other per transaction. Whether the endpoint functions as a UAC or a UAS depends on the UA that initiates the request.

SIP IP Phone Models

This section introduces the SIP-T4X IP phone family. SIP-T4X IP phones are endpoints in the overall network topology, which are designed to interoperate with other compatible equipments including application servers, media servers, internet-working gateways, voice bridges, and other endpoints. SIP-T4X IP phones are characterized by a large number of functions, which simplify business communication with a high standard of security and can work seamlessly with a large number of SIP PBXs.

SIP-T4X IP phones provide a powerful and flexible IP communication solution for Ethernet TCP/IP networks, delivering excellent voice quality. The high-resolution graphic display supplies content in multiple languages for system status, call log and directory access. SIP-T4X IP phones also support advanced functionalities, including LDAP, Busy Lamp Field, Sever Redundancy and Network Conference.

The following IP phone models are described:

- SIP-T46G
- SIP-T42G
- SIP-T41P

SIP-T4X IP phones comply with the SIP standard (RFC 3261), and they can only be used within a network that supports this type of phone.

In order to operate as SIP endpoints in your network successfully, SIP-T4X IP phones must meet the following requirements:

- A working IP network is established.
- Routers are configured for VoIP.
- VoIP gateways are configured for SIP.
- The latest (or compatible) firmware of SIP-T4X IP phones is available.

- A call server is active and configured to receive and send SIP messages.

Physical Features of SIP-T4X IP Phones

This section lists the available physical features of SIPT4X IP phones.

SIPT46G



Physical Features:

- 4.3" TFT-LCD, 480 x 272 pixel, 16.7M colors
- 6 VoIP accounts, BroadSoft/Avaya/Asterisk validated
- HD Voice: HD Codec, HD Handset, HD Speaker
- 41 keys including 10 line keys
- 1xRJ9 (4P4C) handset port
- 1xRJ9 (4P4C) headset port
- 2xRJ45 10/100/1000Mbps Ethernet ports
- 1XRJ12 (6P6C) expansion module port
- 14 LEDs: 1xpower, 10xline, 1xmute, 1xheadset, 1xspeakerphone
- Power adapter: AC 100~240V input and DC 5V/2A output
- Power over Ethernet (IEEE 802.3af)
- Built-in USB port, support Bluetooth headset

SIPT42G



Physical Features:

- 192 x 64 graphic LCD
- 3 VoIP accounts, BroadSoft/Avaya/Asterisk validated
- HD Voice: HD Codec, HD Handset, HD Speaker
- 35 keys including 6 line keys
- 1xRJ9 (4P4C) handset port
- 1xRJ9 (4P4C) headset port
- 2xRJ45 10/100/1000Mbps Ethernet ports
- 1XRJ12 (6P6C) EHS36 headset adapter port
- 10 LEDs: 1xpower, 6xline, 1xmute, 1xheadset, 1xspeakerphone
- Power adapter: AC 100~240V input and DC 5V/1.2A output
- Power over Ethernet (IEEE 802.3af)

SIP-T41P



Physical Features:

- 192 x 64 graphic LCD
- 3 VoIP accounts, BroadSoft/Avaya/Asterisk validated
- HD Voice: HD Codec, HD Handset, HD Speaker
- 35 keys including 6 line keys
- 1xRJ9 (4P4C) handset port
- 1xRJ9 (4P4C) headset port
- 2xRJ45 10/100Mbps Ethernet ports
- 1XRJ12 (6P6C) EHS36 headset adapter port
- 10 LEDs: 1xpower, 6xline, 1xmute, 1xheadset, 1xspeakerphone
- Power adapter: AC 100~240V input and DC 5V/1.2A output
- Power over Ethernet (IEEE 802.3af)

Key Features of SIP-T4X IP Phones

In addition to physical features introduced above, SIP-T4X IP phones also support the following key features when running the latest firmware:

- **Phone Features**
 - **Call Options:** emergency call, call waiting, call hold, call mute, call forward, call transfer, call pickup, conference.
 - **Basic Features:** DND, phone lock, auto redial, live dialpad, dial plan, hotline,

caller identity, auto answer.

- **Advanced Features:** BLF, server redundancy, distinctive ring tones, remote phone book, LDAP, 802.1x authentication.

- **Codecs and Voice Features**

- Wideband codec: G.722
- Narrowband codec: G.711, G.723.1, G.726, G.729AB, GSM, iLBC .
- VAD, CNG, AEC, PLC, AJB, AGC
- Full-duplex speakerphone with AEC

- **Network Features**

- SIP v1 (RFC2543), v2 (RFC3261)
- IPv4/IPv6 support
- NAT Traversal: STUN mode
- DTMF: INBAND, RFC2833, SIP INFO
- Proxy mode and peer-to-peer SIP link mode
- IP assignment: Static/DHCP/PPPoE (for SIP-T46G only)
- TFTP/DHCP client
- HTTP/HTTPS server
- DNS client
- NAT/DHCP server

- **Management**

- FTP/TFTP/HTTP/PnP auto-provision
- Configuration: browser/phone/auto-provision
- Direct IP call without SIP proxy
- Dial number via SIP server
- Dial URL via SIP server

- **Security**

- HTTPS (server/client)
- SRTP (RFC3711)
- Transport Layer Security (TLS)
- VLAN (802.1q), QoS
- Digest authentication using MD5/MD5-sess
- Secure configuration file via AES encryption
- Phone lock for personal privacy protection
- Admin/User configuration mode

Getting Started

This chapter provides basic information and installation instructions of SIP-T4X IP phones.

This chapter provides the following sections:

- [Connecting the IP Phone](#)
- [Initialization Process Overview](#)
- [Verifying Startup](#)
- [Configuration Methods](#)
- [Reading Icons](#)
- [Configuring Basic Network Parameters](#)
- [Creating Dial Plan](#)

Connecting the IP Phone

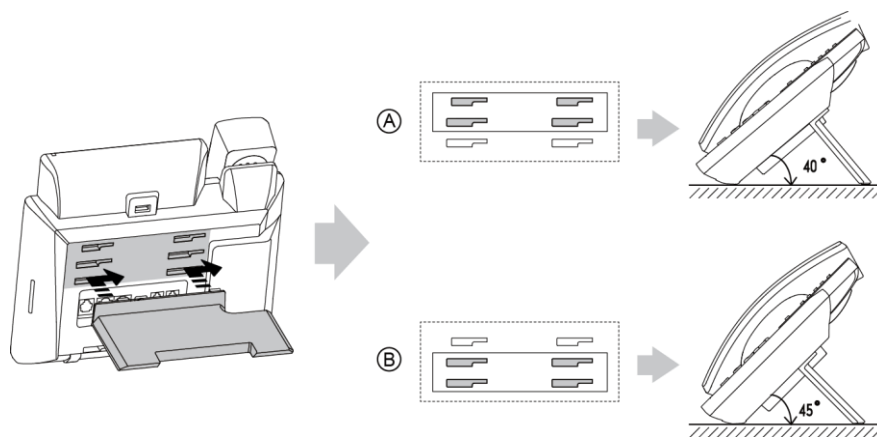
This section introduces how to install SIP-T4X IP phones with the components in packaging contents.

1. Attach the stand
2. Connect the handset and optional headset
3. Connect the network and power

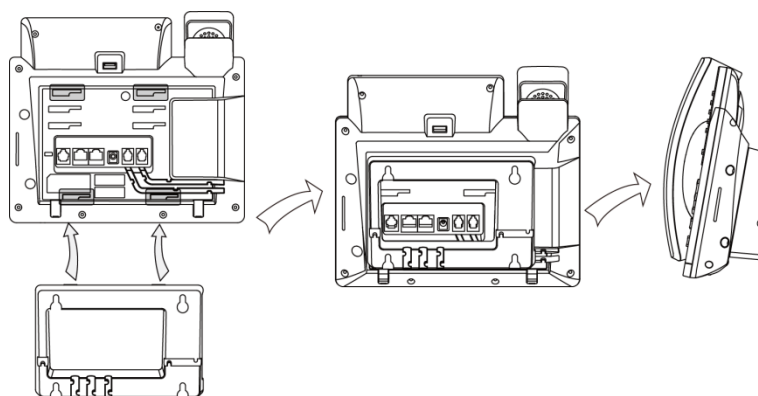
Note

A headset, wall mount bracket and power adapter are not included in packaging contents.

1) Attach the stand:



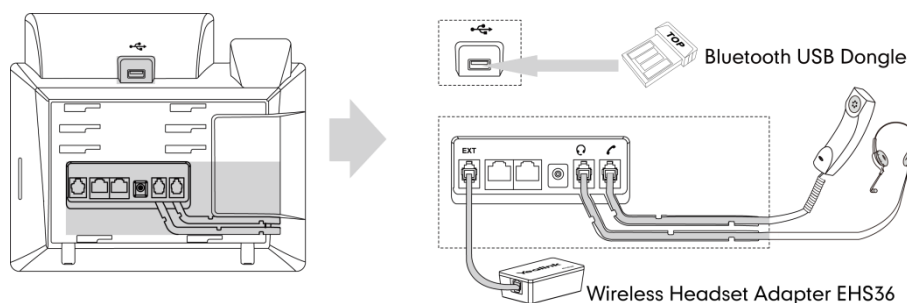
Desk Mount Method



Wall Mount Method (Optional)

Note For more information on how to mount the phone to a wall, refer to *Yealink Wall Mount Quick Installation Guide for SIP-T4X IP Phones*.

2) Connect the handset, optional headset and Bluetooth headset:



Note

Wireless headset adapter EHS36 and Bluetooth USB dongle should be purchased separately.

For more information on how to use the EHS36 on the IP phone, refer to *Yealink EHS36 User Guide*.

Bluetooth can only be used on SIP-T46G IP phones. For more information on how to use the Bluetooth on SIP-T46G IP phones, refer to *Yealink Bluetooth USB Dongle BT40 User Guide*.

EXT port can also be used to connect the expansion module EXP40. For more information on how to connect EXP40, refer to *Yealink EXP40 User Guide*.

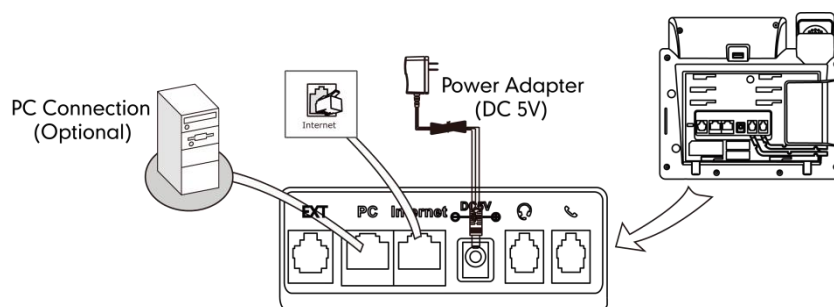
3) Connect the network and power:

- AC power
- Power over Ethernet (PoE)

AC Power

To connect the AC power and network:

1. Connect the DC plug of the power adapter to the DC5V port on IP phones and connect the other end of the power adapter into an electrical power outlet.
2. Connect the included or a standard Ethernet cable between the Internet port on IP phones and the one on the wall or switch/hub device port.

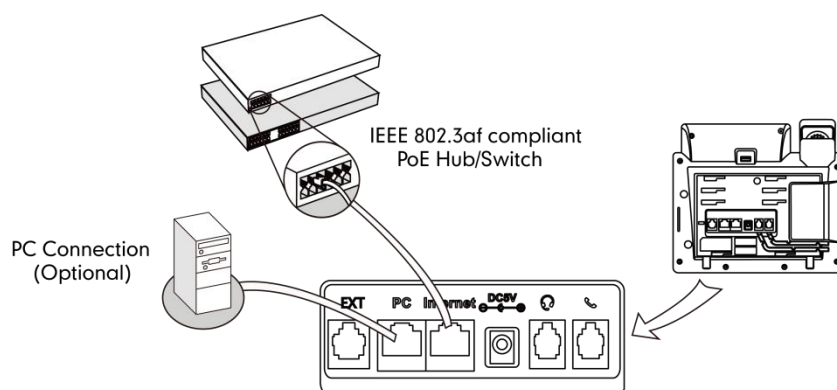


Power over Ethernet

With the included or a regular Ethernet cable, IP phones can be powered from a PoE-compliant switch or hub.

To connect the PoE:

1. Connect the Ethernet cable between the Internet port on IP phones and an available port on the in-line power switch/hub.



Note

If in-line power switch/hub is provided, you don't need to connect the phone to the power adapter. Make sure the switch/hub is PoE-compliant.

IP phones can also share the network with another network device such as a PC (personal computer). It is an optional connection.

Important! Do not unplug or remove the power while IP phones are updating firmware and configurations.

Initialization Process Overview

The initialization process of IP phones is responsible for network connectivity and operation of IP phones in your local network.

Once you connect your IP phone to the network and to an electrical supply, the IP phone begins its initialization process.

During the initialization process, the following events proceed:

Loading the ROM file

The ROM file resides in the flash memory of IP phones. IP phones come from the factory with a ROM file preloaded. During initialization, IP phones run a bootstrap loader that loads and executes the ROM file.

Configuring the VLAN

If IP phones are connected to a switch, the switch notifies IP phones of the VLAN information defined on the switch (if using LLDP). IP phones can then proceed with the

DHCP request for its network settings (if using DHCP).

Querying the DHCP (Dynamic Host Configuration Protocol) Server

IP phones are capable of querying a DHCP server. DHCP is enabled on IP phones by default. The following network parameters can be obtained from the DHCP server during initialization:

- IP Address
- Subnet Mask
- Gateway
- Primary DNS (Domain Name Server)
- Secondary DNS

You need to configure the network parameters of IP phones manually if any of them is not supplied by the DHCP server. For more information on configuring network parameters manually, refer to [Configuring Network Parameters Manually](#) on page 21.

Contacting the auto provisioning server

SIP-T4X IP phones support the FTP, TFTP, HTTP, and HTTPS protocols for auto provisioning and are configured by default to use TFTP protocol. If IP phones are configured to obtain configurations from the TFTP server, they will connect to the TFTP server and download the configuration file(s) during startup. IP phones will be able to resolve and apply the configurations written in the configuration file(s). If IP phones do not obtain the configurations from the TFTP server, IP phones will use the configurations stored in the flash memory.

Updating firmware

If the access URL of the firmware is defined in the configuration file, the IP phone will download the firmware from the provisioning server. If the MD5 value of the downloaded firmware file differs from that of the image stored in the flash memory, the IP phone will perform a firmware update.

Downloading the resource files

In addition to configuration file(s), IP phones may require resource files before it can deliver service. These resource files are optional, but if some particular features are being deployed, these files are required.

The followings show examples of resource files:

- Language packs
- Ring tones
- Contact files

Verifying Startup

After connected to the power and network, the IP phone begins the initializing process by cycling through the following steps:

1. The power indicator LED illuminates.
2. The message "Initializing...Please wait" appears on the LCD screen when the IP phone starts up.
3. The main LCD screen displays the following:
 - Time and date
 - Soft key labels
4. Press the OK key to check the IP phone status, the LCD screen displays the valid IP address, MAC address, firmware version, etc.

If the IP phone has successfully passed through these steps, it starts up properly and is ready for use.

Configuration Methods

You can use the following methods to set up and configure IP phones:

- [Phone User Interface](#)
- [Web User Interface](#)
- [Configuration Files](#)

The following sections describe how to configure IP phones using each method above.

Phone User Interface

An administrator or a user can configure and use IP phones via phone user interface. Specific features access is restricted to the administrator. These specific features are password protected by default. The default password is "admin" (case-sensitive). Not all features are available on phone user interface.

Web User Interface

An administrator or a user can configure IP phones via web user interface. The default user name and password for the administrator to log into the web user interface are both "admin" (case-sensitive). Almost all features are available for configuring via web user interface. IP phones support both HTTP and HTTPS protocols for accessing the web user interface. For more information, refer to [Web Server Type](#) on page 112.

Configuration Files

You can deploy IP phones using configuration files. There are two configuration files both of which are CFG formatted. We call them Common CFG file and MAC-Oriented CFG file. A Common CFG file will be effectual for all IP phones of the same model. However, a MAC-Oriented CFG file will only be effectual for a specific IP phone. The Common CFG file has a fixed name for each IP phone model, while the MAC-Oriented CFG file is named as the MAC address of IP phones. For example, if the MAC address of a SIP-T46G IP phone is 001565113af5, the names of these two configuration files must be: y000000000028.cfg and 001565113af5.cfg.

The name of the Common CFG file for each SIP-T4X IP phone model is:

- SIP-T46G: y000000000028.cfg
- SIP-T42G: y000000000029.cfg
- SIP-T41P: y000000000036.cfg

In order to deploy IP phones using configuration files (<y0000000000xx>.cfg and <MAC>.cfg), you need to use a text-based editing application to edit the configuration files, and store configuration files to a provisioning server. IP phones support downloading configuration files using any of the following protocols: FTP, TFTP, HTTP and HTTPS.

IP phones can obtain the address of the provisioning server during startup through one of the following processes: Zero Touch, PnP, DHCP Options and Phone Flash. Then IP phones download configuration files from the provisioning server, resolve and update the configurations written in the configuration files. This entire process is called auto provisioning. For more information on auto provisioning, refer to *Yealink_SIP-T2_Series_T19P_T4_Series_IP_Phones_Auto_Provisioning_Guide*.

When modifying parameters, learn the following:

- Parameters in configuration files override those stored in IP phones' flash memory.
- The .cfg extension of the configuration files must be in lowercase.
- Each line in a configuration file must use the following format and adhere to the following rules:

```
variable-name = value
```

- Associate only one value with one variable.
- Separate variable name and value with equal sign.
- Set only one variable per line.
- Put the variable and value on the same line, and do not break the line.
- Comment the variable on a separated line. Use the pound (#) delimiter to distinguish the comments.




























IP phones can accept two sources of configuration data:



































- Downloaded from configuration files
- Changed on the phone user interface or the web user interface

The latest value configured on the IP phone takes effect finally.

Reading Icons

Icons associated with different features may appear on the LCD screen. The following table provides a description for each icon on SIP-T4X IP phone models.

SIP-T46G	SIP-T42G/T41P	Description
		Network is unavailable
		Registered successfully
		Register failed
		Registering
		Hands-free speakerphone mode
		Handset mode
		Headset mode
		Voice Mail
	/	Text Message
	AA	Auto Answer
	DND	Do Not Disturb
		Call Forward
		Call Hold
		Call Mute
		Ringer volume is 0

SIP-T46G	SIP-T42G/T41P	Description
		Phone Lock
		Multi-lingual lowercase letters input mode
		Multi-lingual uppercase letters input mode
		Alphanumeric input mode
		Numeric input mode
		Multi-lingual uppercase and lowercase letters input mode
		Received Calls
		Placed Calls
		Missed Calls
		Recording box is full
		A call cannot be recorded
		Recording starts successfully
		Recording cannot be started
		Recording cannot be stopped
	VPN	VPN is enabled
	/	Bluetooth
	/	Bluetooth headset is both paired and connected
	/	Conference
	/	The default contact icon
	/	The default caller photo

Configuring Basic Network Parameters

This section describes how to configure basic network parameters for the IP phone.

Note

This section mainly introduces IPv4 network parameters. For more information on IPv6, refer to [IPv6 Support](#) on page 187.

DHCP

DHCP (Dynamic Host Configuration Protocol) is a network protocol used to dynamically allocate network parameters to network hosts. The automatic allocation of network parameters to hosts eases the administrative burden of maintaining an IP network. IP phones comply with the DHCP specifications documented in RFC 2131. If DHCP is used, IP phones connected to the network become operational without having to be manually assigned IP addresses and additional network parameters. Static DNS address(es) can be configured and used when DHCP is enabled.

DHCP Option

DHCP provides a framework for passing information to TCP/IP network devices. Network and other control information are carried in tagged data items that are stored in the options field of the DHCP message. The data items themselves are also called options. DHCP can be initiated by simply connecting the IP phone with the network. IP phones broadcast DISCOVER messages to request the network information carried in DHCP options, and the DHCP server responds with the specific values in the corresponding options.

The following table lists the common DHCP options supported by IP phones.

Parameter	DHCP Option	Description
Subnet Mask	1	Specify the client's subnet mask.
Time Offset	2	Specify the offset of the client's subnet in seconds from Coordinated Universal Time (UTC).
Router	3	Specify a list of IP addresses for routers on the client's subnet.
Time Server	4	Specify a list of time servers available to the client.
Domain Name Server	6	Specify a list of domain name servers available to the client.
Log Server	7	Specify a list of MIT-LCS UDP servers

Parameter	DHCP Option	Description
		available to the client.
Host Name	12	Specify the name of the client.
Domain Server	15	Specify the domain name that client should use when resolving hostnames via DNS.
Broadcast Address	28	Specify the broadcast address in use on the client's subnet.
Network Time Protocol Servers	42	Specify a list of the NTP servers available to the client by IP address.
Vendor-Specific Information	43	Identify the vendor-specific information.
Vendor Class Identifier	60	Identify the vendor type.
TFTP Server Name	66	Identify a TFTP server when the 'sname' field in the DHCP header has been used for DHCP options.
Bootfile Name	67	Identify a bootfile when the 'file' field in the DHCP header has been used for DHCP options.

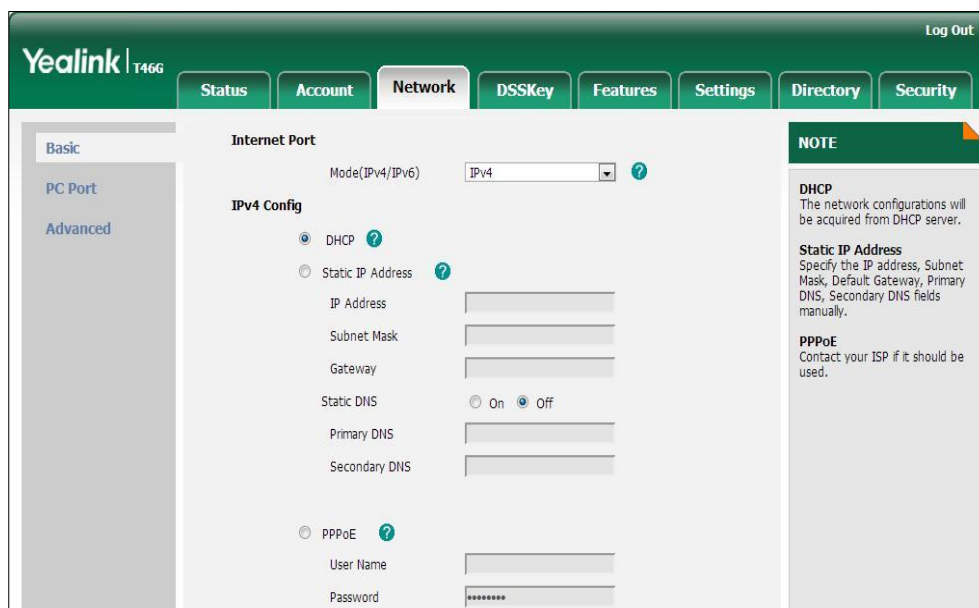
Procedure

DHCP can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure DHCP on the IP phone. Configure static DNS address when DHCP is used. For more information, refer to DHCP on page 248.
Local	Web User Interface	Configure DHCP on the IP phone. Configure static DNS address when DHCP is used. Navigate to: http://<phoneIPAddress>/servlet?p=network&q=load
	Phone User Interface	Configure DHCP on the IP phone.

To configure DHCP via web user interface:

1. Click on **Network->Basic**.
2. In the **IPv4 Config** block, mark the **DHCP** radio box.

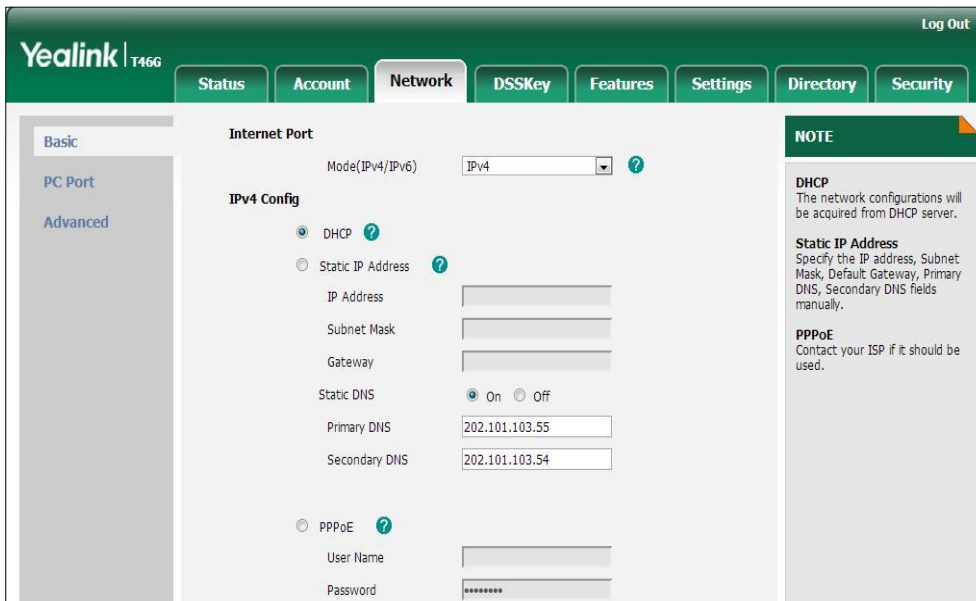


3. Click **Confirm** to accept the change.
A dialog box pops up to prompt that settings will take effect after reboot.
4. Click **OK** to reboot the IP phone.

To configure static DNS address when DHCP is used via web user interface:

1. Click on **Network->Basic**.
2. In the **IPv4 Config** block, mark the **DHCP** radio box.
3. Mark the **Static DNS** radio box.

4. Enter the desired values in the **Primary DNS** and **Secondary DNS** fields.



The screenshot shows the Yealink T46G web interface. The 'Network' tab is selected. Under 'Internet Port', the 'Mode(IPv4/IPv6)' is set to 'IPv4'. In the 'IPv4 Config' section, 'DHCP' is selected. Under 'Static DNS', 'On' is selected. The 'Primary DNS' field contains '202.101.103.55' and the 'Secondary DNS' field contains '202.101.103.54'. A 'NOTE' box on the right provides instructions for DHCP, Static IP Address, and PPPoE configurations.

5. Click **Confirm** to accept the change.

A dialog box pops up to prompt that settings will take effect after a reboot.

6. Click **OK** to reboot the IP phone.

To configure DHCP via phone user interface:

1. Press **Menu->Advanced** (password: admin) ->**Network->WAN Port->IPv4**.
2. Press **◀** or **▶** , or the **Switch** soft key to select the **DHCP** from the **Type** field.
3. Press the **Save** soft key to accept the change.

The IP phone reboots automatically to make settings effective after a period of time.

Configuring Network Parameters Manually

If DHCP is disabled or IP phones cannot obtain network parameters from the DHCP server, you need to configure the network parameters manually. The following parameters should be configured for IP phones to establish network connectivity:

- IP Address
- Subnet Mask
- Default Gateway
- Primary DNS
- Secondary DNS

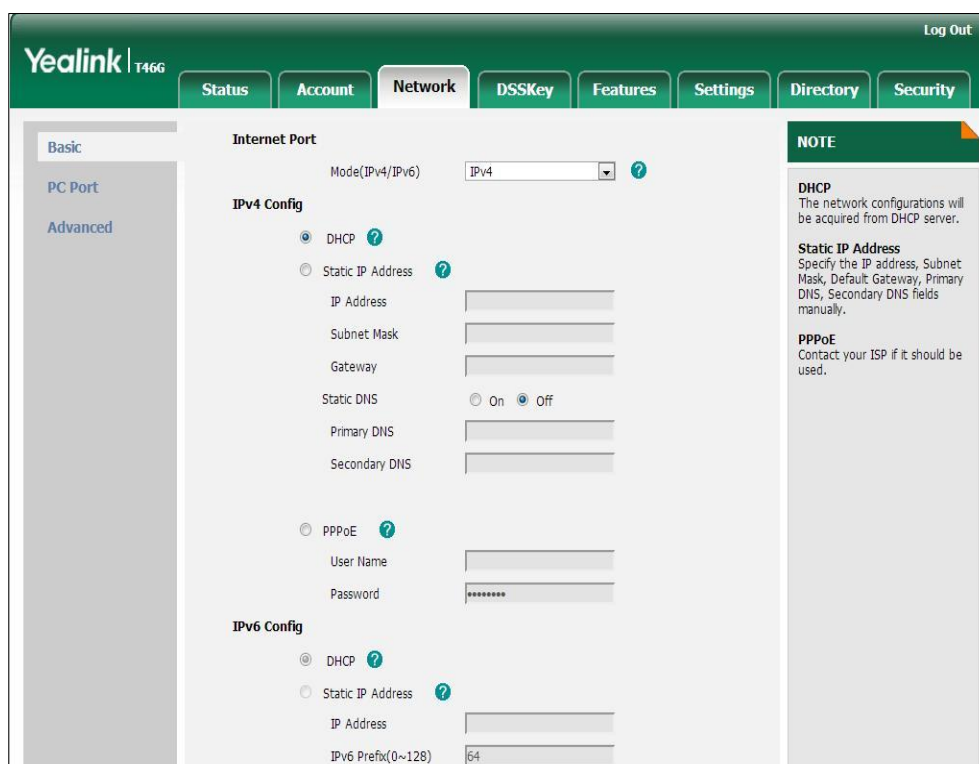
Procedure

Network parameters can be configured manually using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure network parameters of the IP phone manually. For more information, refer to Static Network Settings on page 249.
Local	Web User Interface	Configure network parameters of the IP phone manually. Navigate to: http://<phoneIPAddress>/servlet?p=network&q=load
	Phone User Interface	Configure network parameters of the IP phone manually.

To configure the IP address mode via web user interface:

1. Click on **Network->Basic**.
2. Select the desired value from the pull-down list of **Mode (IPv4/IPv6)**.



3. Click **Confirm** to accept the change.
A dialog box pops up to prompt that settings will take effect after reboot.
4. Click **OK** to reboot the IP phone.

To configure a static IPv4 address via web user interface:

1. Click on **Network->Basic**.
2. In the **IPv4 Config** block, mark the **Static IP Address** radio box.
3. Enter the IP address, subnet mask, default gateway, primary DNS and secondary DNS in the corresponding fields.

The screenshot shows the Yealink T466 web interface. The 'Network' tab is active, and the 'Basic' sub-tab is selected. Under 'Internet Port', the 'Mode(IPv4/IPv6)' is set to 'IPv4'. In the 'IPv4 Config' section, the 'Static IP Address' radio button is selected. The fields are filled with: IP Address: 192.168.1.10, Subnet Mask: 255.255.255.0, Gateway: 192.168.1.254, Static DNS: On, Primary DNS: 202.101.103.55, and Secondary DNS: 202.101.103.54. A 'NOTE' box on the right contains information about DHCP and PPPoE.

4. Click **Confirm** to accept the change.
A dialog box pops up to prompt that settings will take effect after reboot.
5. Click **OK** to reboot the IP phone.

To configure the IP address mode via phone user interface:

1. Press **Menu->Advanced** (password: admin) ->**Network->WAN Port**.
2. Press **▲** or **▼** to highlight the **IP Address Mode** field.
3. Press **◀** or **▶** to select **IPv4** or **IPv4&IPv6** from the **IP Address Mode** field.
4. Press the **Save** soft key to accept the change.

The IP phone reboots automatically to make settings effective after a period of time.

To configure a static IPv4 address via phone user interface:

1. Press **Menu->Advanced** (password: admin) ->**Network->WAN Port->IPv4**.
2. Press **◀** or **▶**, or the **Switch** soft key to select the **Static IP** from the **Type** field.
3. Enter the desired values in the **IP Address**, **Subnet Mask**, **Gateway**, **Primary DNS** and **Secondary DNS** fields respectively.
4. Press the **Save** soft key to accept the change.

The IP phone reboots automatically to make settings effective after a period of time.

Note

Using the wrong network settings may result in inaccessibility of your phone and may also have an impact on your network performance. For more information on these parameters, contact your network administrator.

PPPoE

PPPoE (Point-to-Point Protocol over Ethernet) is a network protocol used by Internet Service Providers (ISPs) to provide Digital Subscriber Line (DSL) high speed Internet services. PPPoE allows an office or building-full of users to share a common DSL connection to the Internet. PPPoE connection is supported by the Internet port of the IP phone. Contact your ISP for the PPPoE user name and password. PPPoE is not applicable to SIP-T42G and SIP-T41P IP phones.

Procedure

PPPoE can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure PPPoE on the IP phone. For more information, refer to PPPoE on page 252.
Local	Web User Interface	Configure PPPoE on the IP phone. Navigate to: http://<phoneIPAddress>/servlet ?p=network&q=load
	Phone User Interface	Configure PPPoE on the IP phone.

To configure PPPoE via web user interface:

1. Click on **Network->Basic**.
2. In the **IPv4 Config** block, mark the **PPPoE** radio box.

- Enter the user name and password in the corresponding fields.

The screenshot shows the Yealink T466 web interface. The top navigation bar includes 'Status', 'Account', 'Network', 'DSSKey', 'Features', 'Settings', 'Directory', and 'Security'. The 'Network' tab is selected. On the left, there is a sidebar with 'Basic', 'PC Port', and 'Advanced' options. The main content area is titled 'Internet Port' and contains the following configuration options:

- Mode(IPv4/IPv6):** A dropdown menu set to 'IPv4'.
- IPv4 Config:**
 - DHCP
 - Static IP Address
 - IP Address: [text input]
 - Subnet Mask: [text input]
 - Gateway: [text input]
 - Static DNS: On Off
 - Primary DNS: [text input]
 - Secondary DNS: [text input]
- PPPoE
 - User Name: [text input with value 'xmy/52000']
 - Password: [password input with masked characters]
- IPv6 Config:**
 - DHCP
 - Static IP Address
 - IP Address: [text input]
 - IPv6 Prefix(0~128): [text input with value '64']

On the right side, there is a 'NOTE' box with the following text:

DHCP
The network configurations will be acquired from DHCP server.

Static IP Address
Specify the IP address, Subnet Mask, Default Gateway, Primary DNS, Secondary DNS fields manually.

PPPoE
Contact your ISP if it should be used.

- Click **Confirm** to accept the change.
A dialog box pops up to prompt that settings will take effect after reboot.
- Click **OK** to reboot the IP phone.

To configure PPPoE via phone user interface:

- Press **Menu**->**Advanced** (password: admin) ->**Network**->**WAN Port**->**IPv4**.
- Press **←** or **→**, or the **Switch** soft key to select the **PPPoE** from the **Type** field.
- Enter the user name and password in the corresponding fields.
- Press the **Save** soft key to accept the change.

The IP phone reboots automatically to make settings effective after a period of time.

Configuring Transmission Methods of the Internet Port and PC Port

There are two Ethernet ports on the back of IP phones: Internet port and PC port. Three optional methods of transmission configuration for SIP-T4X IP phone Internet or PC Ethernet ports:

- Auto-negotiation
- Half-duplex
- Full-duplex

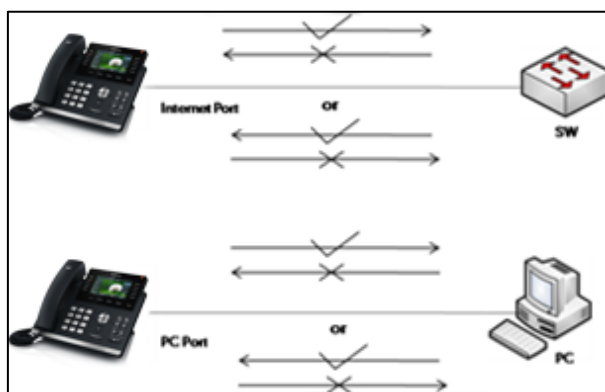
Auto-negotiation is configured for both Internet and PC ports on the IP phone by default.

Auto-negotiation

Auto-negotiation means that all connected devices choose common transmission parameters (e.g., speed and duplex mode) to transmit voice or data over Ethernet. This process entails devices first sharing transmission capabilities and then selecting the highest performance transmission mode supported by both. You can configure the Internet port and PC port on IP phones to auto-negotiate during the transmission.

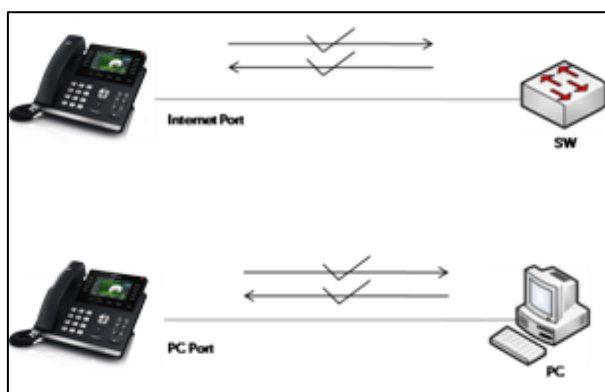
Half-duplex

Half-duplex transmission refers to transmitting voice or data in both directions, but in one direction at a time; this means one device can send data on the line, but not receive data simultaneously. You can configure the half-duplex transmission on both Internet port and PC port for IP phones to transmit in 10Mbps, 100Mbps or 1000Mbps (not applicable to SIP-T41P).



Full-duplex

Full-duplex transmission refers to transmitting voice or data in both directions at the same time; this means one device can send data on the line while receiving data. You can configure the full-duplex transmission on both Internet port and PC port for IP phones to transmit in 10Mbps, 100Mbps or 1000Mbps (not applicable to SIP-T41P).



Procedure

The transmission method of Ethernet port can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure the transmission method of Ethernet port. For more information, refer to Internet and PC Ports Transmission Methods on page 253.
Local	Web User Interface	Configure the transmission method of Ethernet port. Navigate to: http://<phoneIPAddress>/servlet?p=network-adv&q=load

To configure the transmission method of Ethernet port via web user interface:

1. Click on **Network->Advanced**.
2. Select the desired value from the pull-down list of **WAN Port Link**.
3. Select the desired value from the pull-down list of **PC Port Link**.

The screenshot shows the Yealink T466 web user interface. The 'Network' tab is selected, and the 'Advanced' sub-tab is active. The 'Port Link' section is expanded, showing the following settings:

- WAN Port Link:** Auto Negotiate
- PC Port Link:** Auto Negotiate

Other visible settings include:

- LLDP:** Active, Enabled
- VLAN:** Active, Packet Interval (1-3600s): 60, WAN Port: Disabled, VID (1-4094): 1, Priority: 0
- PC Port:** Active, VID (1-4094): 1, Priority: 0
- DHCP VLAN:** Active, Option: 132
- Voice QoS:** Voice QoS (0~63): 46, SIP QoS (0~63): 26

A 'NOTE' box on the right side of the page provides information about VLAN and QoS.

4. Click **Confirm** to accept the change.

Creating Dial Plan

Regular expression, often called a pattern, is an expression that specifies a set of strings. A regular expression provides a concise and flexible means to "match" (specify and recognize) strings of text, such as particular characters, words, or patterns of characters. Regular expression is used by many text editors, utilities, and programming languages to search and manipulate text based on patterns.

Regular expression can be used to define IP phone dial plan. Dial plan is a string of characters that governs the way for IP phones to process the inputs received from the IP phone's keypads. IP phones support the following dial plan features:

- [Replace Rule](#)
- [Dial-now](#)
- [Area Code](#)
- [Block Out](#)

You need to know the following basic regular expression syntax when creating dial plan:

.	The dot "." can be used as a placeholder or multiple placeholders for any string. Example: "12." would match "123", "1234", "12345", "12abc", etc.
x	The "x" can be used as a placeholder for any character. Example: "12x" would match "121", "122", "123", "12a", etc.
-	The dash "-" can be used to match a range of characters within the brackets. Example: "[5-7]" would match the number "5", "6" or "7".
,	The comma "," can be used as a separator within the bracket. Example: "[2,5,8]" would match the number "2", "5" or "8".
[]	The square bracket "[]" can be used as a placeholder for a single character which matches any of a set of characters. Example: "91[5-7]1234" would match "9151234", "9161234", "9171234".
()	The parenthesis "()" can be used to group together patterns, for instance, to logically combine two or more patterns. Example: "([1-9])([2-7])3" would match "923", "153", "673", etc.
\$	The "\$" followed by the sequence number of a parenthesis means the characters placed in the parenthesis. The sequence number stands for the corresponding parenthesis. Example: A replace rule configuration, Prefix: "001(xxx)45(xx)", Replace:

	"9001\$145\$2". When you dial out "0012354599" on your phone, the IP phone will replace the number with "90012354599". "\$1" means three digits in the first parenthesis, that is, "235". "\$2" means two digits in the second parenthesis, that is, "99".
--	--

Replace Rule

Replace rule is an alternative string that replaces the numbers entered by the user. IP phones support up to 100 replace rules, which can be created either one by one or in batch using a replace rule template. For more information on the replace rule template, refer to [Replace Rule Template](#) on page 219.

Procedure

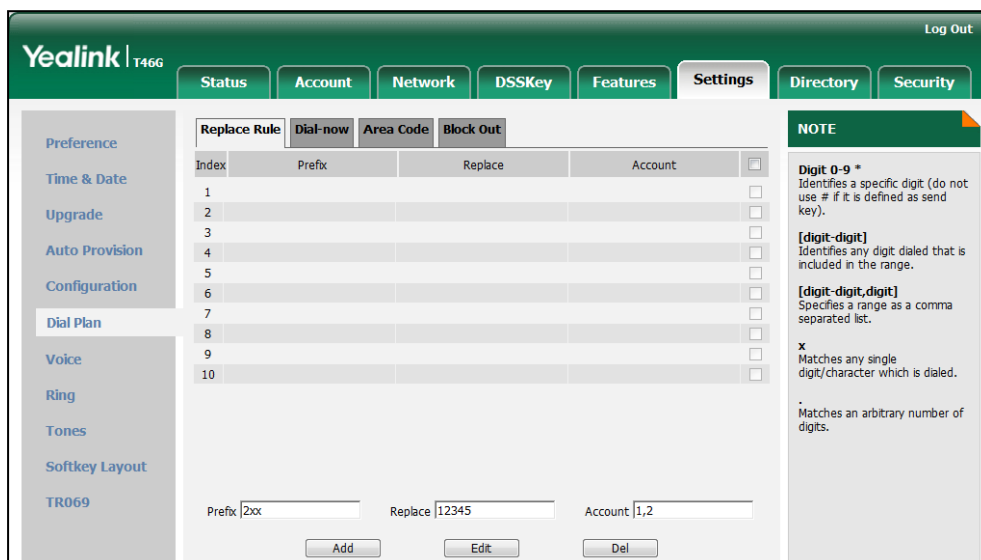
Replace rule can be created using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Create the replace rule for the IP phone. For more information, refer to Dial Plan on page 254.
Local	Web User Interface	Create the replace rule for the IP phone. Navigate to: http://<phoneIPAddress>/servlet?p=settings-dialplan&q=load

To create a replace rule via web user interface:

1. Click on **Settings->Dial Plan->Replace Rule**.
2. Enter the string in the **Prefix** field.
3. Enter the string in the **Replace** field.

- Enter the desired line ID in the **Account** field or leave it blank.
If you leave the field blank or enter 0, the replace rule will apply to all accounts on the IP phone.



- Click **Add** to add the replace rule.

Dial-now

Dial-now is a string used to match the numbers entered by the user. When entered numbers match the predefined dial-now rule, IP phones will automatically dial out the numbers without pressing the send key. IP phones support up to 100 dial-now rules, which can be created either one by one or in batch using a dial-now rule template. For more information on the dial-now template, refer to [Dial-now Template](#) on page 220.

Delay Time for Dial-now Rule

IP phones will automatically dial out the entered number, which matches the dial-now rule, after a specified period of time.

Procedure

Dial-now rule can be created using the configuration files or locally.

<p>Configuration File</p>	<p><y0000000000xx>.cfg</p>	<p>Create the dial-now rule for the IP phone.</p> <p>For more information, refer to Dial Plan on page 254.</p> <p>Configure the delay time for the dial-now rule.</p> <p>For more information, refer to Dial</p>
----------------------------------	----------------------------------	--

		Plan on page 254.
Local	Web User Interface	<p>Create the dial-now rule for the IP phone.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet?p=settings-dialnow&q=load</p> <p>Configure the delay time for the dial-now rule.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet?p=features-general&q=load</p>

To create a dial-now rule via web user interface:

1. Click on **Settings->Dial Plan->Dial-now.**
2. Enter the desired value in the **Rule** field.
3. Enter the desired line ID in the **Account** field or leave it blank.

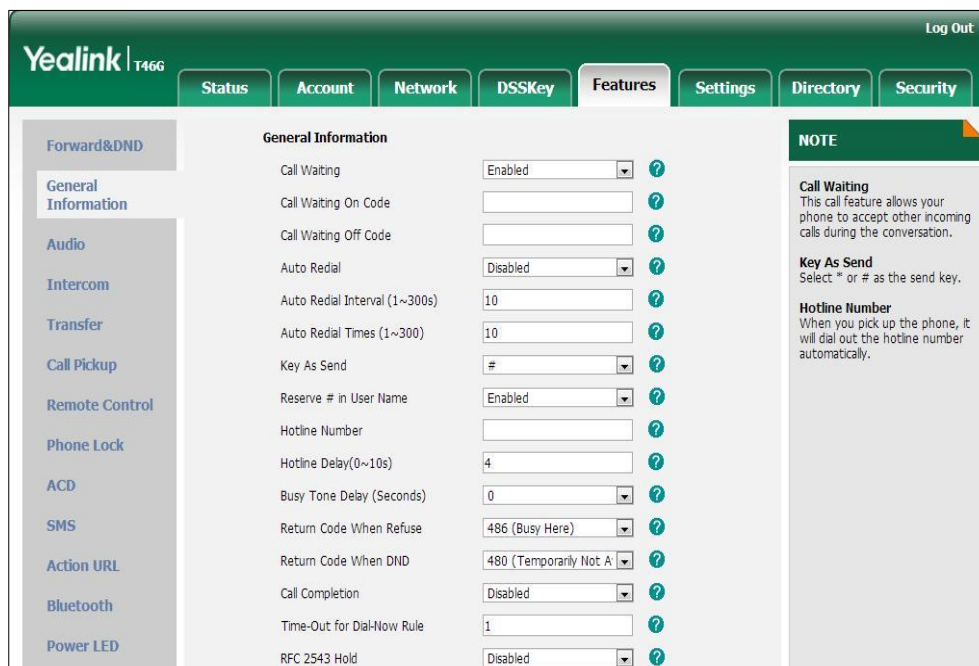
If you leave the field blank or enter 0, the dial-now rule will apply to all accounts on the IP phone.

4. Click **Add** to add the dial-now rule.

To configure the delay time for the dial-now rule via web user interface:

1. Click on **Features->General Information.**

- Enter the desired time within 1-14 (in seconds) in the **Time-Out for Dial-Now Rule** field.



- Click **Confirm** to accept the change.

Area Code

Area codes are also known as Numbering Plan Areas (NPAs). They usually indicate geographical areas in one country. When the entered numbers match the predefined area code rule, the IP phone will automatically add the area code before the numbers when dialing out them. IP phones only support one area code rule.

Procedure

Area code rule can be configured using the configuration files or locally.

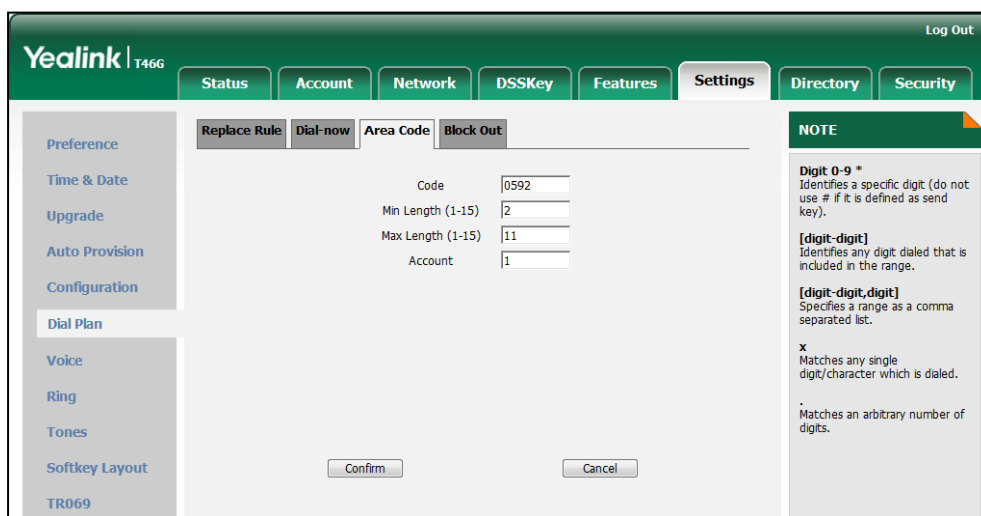
Configuration File	<y0000000000xx>.cfg	Create the area code rule and specify the maximum and minimum lengths of the entered numbers. For more information, refer to Dial Plan on page 254.
Local	Web User Interface	Create the area code rule and specify the maximum and minimum lengths of entered numbers. Navigate to:

		http://<phoneIPAddress>/servlet ?p=settings-areacode&q=load
--	--	--

To configure an area code rule via web user interface:

1. Click on **Settings->Dial Plan->Area Code**.
2. Enter desired values in the **Code**, **Min Length (1-15)** and **Max Length (1-15)** fields.
3. Enter the desired line ID in the **Account** field or leave it blank.

If you leave the field blank or enter 0, the area code rule will apply to all accounts on the IP phone.



4. Click **Confirm** to accept the change.

Block Out

Block out rule prevents users from dialing out specific numbers. When the entered numbers match the predefined block out rule, the LCD screen prompts "Forbidden Number". IP phones support up to 10 block out rules.

Procedure

Block out rule can be created using the configuration files or locally.

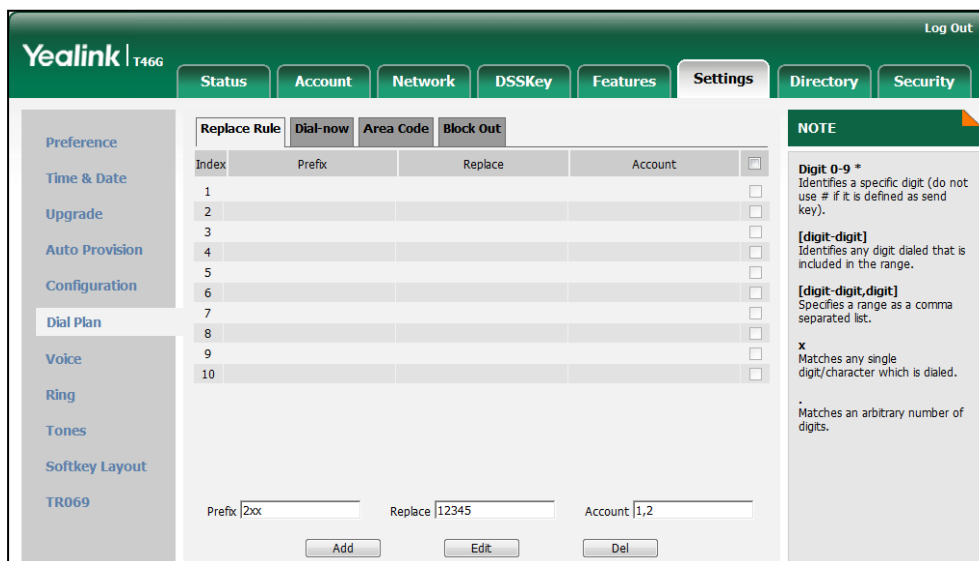
Configuration File	<y0000000000xx>.cfg	Create the block out rule for the IP phone. For more information, refer to Dial Plan on page 254.
Local	Web User Interface	Create the block out rule for the desired line. Navigate to: http://<phoneIPAddress>/servlet

		?p=settings-blackout&q=load
--	--	-----------------------------

To create a block out rule via web user interface:

1. Click on **Settings->Dial Plan->Block Out**.
2. Enter the desired value in the **BlockOut Number** field.
3. Enter the desired line ID in the **Account** field or leave it blank.

If you leave the field blank or enter 0, the block out rule will apply to all accounts on the IP phone.



4. Click **Confirm** to add the block out rule.

Configuring Basic Features

This chapter provides information for making configuration changes for the following basic features:

- [Power Indicator LED](#)
- [Contrast](#)
- [Backlight](#)
- [User Password](#)
- [Administrator Password](#)
- [Phone Lock](#)
- [Time and Date](#)
- [Language](#)
- [Logo Customization](#)
- [Softkey Layout](#)
- [Key as Send](#)
- [Hotline](#)
- [Call Log](#)
- [Missed Call Log](#)
- [Local Directory](#)
- [Live Dialpad](#)
- [Call Waiting](#)
- [Auto Redial](#)
- [Auto Answer](#)
- [Call Completion](#)
- [Anonymous Call](#)
- [Anonymous Call Rejection](#)
- [Do Not Disturb](#)
- [Busy Tone Delay](#)
- [Return Code When Refuse](#)
- [Early Media](#)
- [180 Ring Workaround](#)
- [Use Outbound Proxy in Dialog](#)
- [SIP Session Timer](#)

- [Session Timer](#)
- [Call Hold](#)
- [Call Forward](#)
- [Call Transfer](#)
- [Network Conference](#)
- [Transfer on Conference Hang Up](#)
- [Directed Call Pickup](#)
- [Group Call Pickup](#)
- [Dialog-Info Call Pickup](#)
- [Call Return](#)
- [Call Park](#)
- [Web Server Type](#)
- [Calling Line Identification Presentation](#)
- [Connected Line Identification Presentation](#)
- [DTMF](#)
- [Suppress DTMF Display](#)
- [Transfer via DTMF](#)
- [Intercom](#)

Power Indicator LED

Power indicator LED indicates power status and phone status. There are six configuration options for power indicator LED:

Common Power Light On

Common Power Light On allows the power indicator LED to be turned on.

Ring Power Light Flash

Ring Power Light Flash allows the power indicator LED to flash when the IP phone receives an incoming call. If this option is disabled, the status of the power indicator LED is determined by the option "Common Power Light On".

Voice/Text Mail Power Light Flash

Voice/Text Mail Power Light Flash allows the power indicator LED to flash when the IP phone receives a voice mail or a text message. If this option is disabled, the status of the power indicator LED is determined by the option "Common Power Light On".

Mute Power Light Flash

Mute Power Light Flash allows the power indicator LED to flash when a call is mute. If

this option is disabled, the status of the power indicator LED is determined by the option “Common Power Light On”.

Hold/Held Power Light Flash

Hold/Held Power Light Flash allows the power indicator LED to flash when a call is placed on hold or is held. If this option is disabled, the status of the power indicator LED is determined by the option “Common Power Light On”.

Talk/Dial Power Light On

Talk/Dial Power Light On allows the power indicator LED to be turned on when the IP phone is busy. If this option is disabled, the status of the power indicator LED is determined by the option “Common Power Light On”.

Procedure

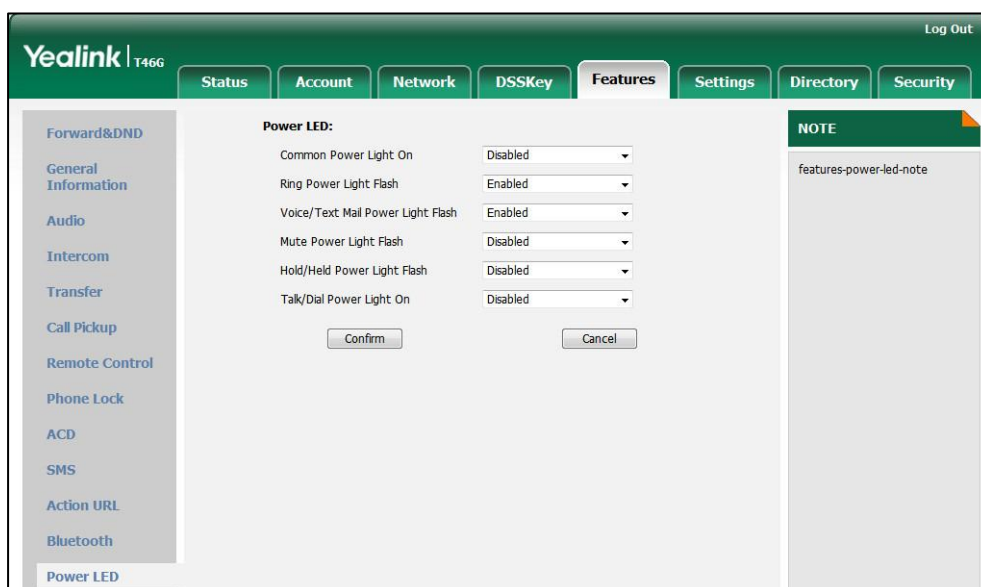
Power indicator LED can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure the power indicator LED. For more information, refer to Power Indicator LED on page 258.
Local	Web User Interface	Configure the power indicator LED. Navigate to: http://<phoneIPAddress>/servlet ?p=features-poweredled&q=load

To configure the power Indicator LED via web user interface:

1. Click on **Features->Power LED**.
2. Select the desired value from the pull-down list of **Common Power Light On**.
3. Select the desired value from the pull-down list of **Ring Power Light Flash**
4. Select the desired value from the pull-down list of **Voice/Text Mail Power Light Flash**.
5. Select the desired value from the pull-down list of **Mute Power Light Flash**.
6. Select the desired value from the pull-down list of **Hold/Held Power Light Flash**.

7. Select the desired value from the pull-down list of **Talk/Dial Power Light On**.



8. Click **Confirm** to accept the change.

Contrast

Contrast determines the readability of the texts displayed on the LCD screen. Adjusting the contrast to a comfortable level can optimize the screen viewing experience. When configured properly, contrast allows users to read the LCD’s display with minimal eyestrain. For SIP-T46G IP phones, you can only configure the LCD’s contrast of the connected EXP40. Make sure the expansion module has been connected to the IP phone before adjustment.

Procedure

Contrast can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure the contrast of the LCD screen. For more information, refer to Contrast on page 261.
Local	Phone User Interface	Configure the contrast of the LCD screen.

To configure contrast via phone user interface (only applicable to EXP40 connected to SIP-T46G IP phones):

1. Press **Menu**-> **Basic**->**Display**->**Contrast**.
2. Press  or  , or the **Switch** soft key to increase or decrease the intensity of contrast.

The default contrast level is 6.

3. Press the **Save** soft key to accept the change.

Wallpaper

Wallpaper is an image used as the background of the phone idle screen. Users can select an image from IP phone's built-in background or customize wallpaper from personal pictures. To set the custom wallpaper as the phone background, you need to upload the custom wallpaper to the IP phone in advance. The wallpaper is not applicable to SIP-T42G and SIP-T41P IP phones.

The following table lists the supported wallpaper image format and resolution for SIP-T46G IP phones:

Wallpaper Image Format	Resolution	Size
.jpg/.png/.bmp	<=480*272	<=5MB

Procedure

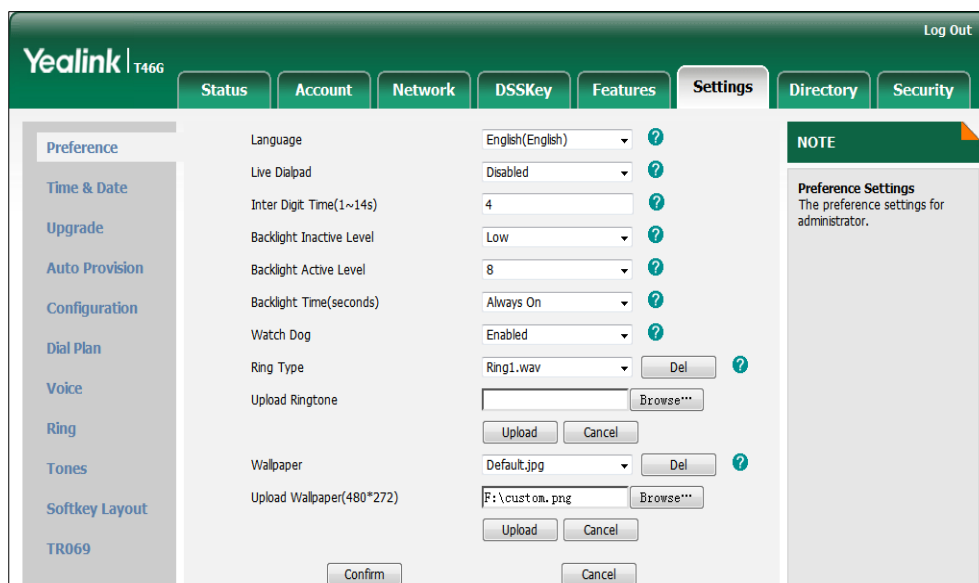
Wallpaper can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Specify the access URL of the custom wallpaper. For more information, refer to Access URL of Wallpaper Image on page 379.
Local	Web User Interface	Upload the custom wallpaper. Change the wallpaper via web user interface. Navigate to: http://<phoneIPAddress>/servlet?p=settings-preference&q=load
	Phone User Interface	Change the wallpaper via phone user interface.

To upload custom wallpaper via web user interface:

1. Click on **Settings**->**Preference**.

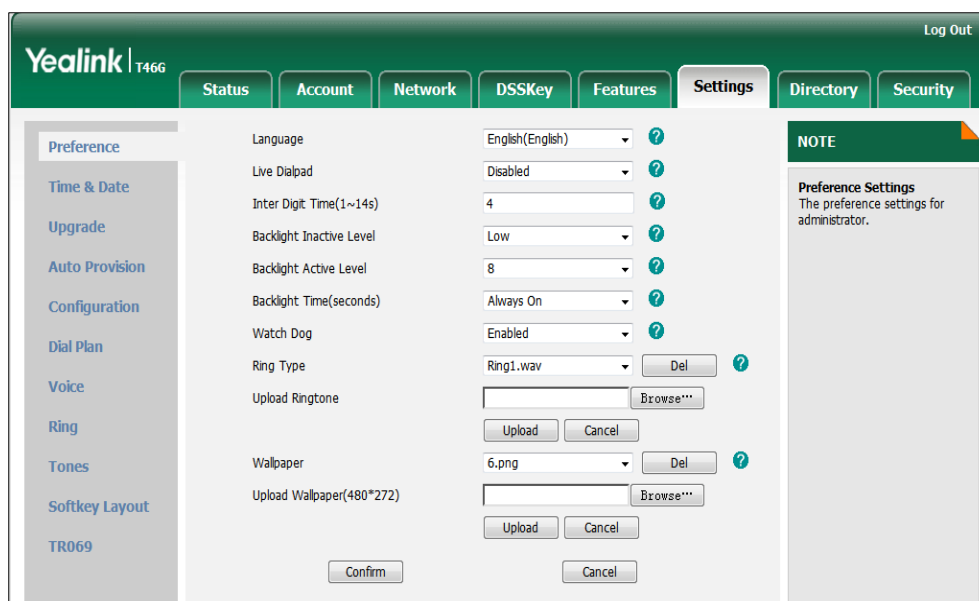
2. In the **Upload Wallpaper (480*272)** field, click **Browse** to locate the wallpaper image from your local system.
3. Click **Upload** to upload the file.



4. Click **Confirm** to accept the change.
The custom wallpaper appears in the pull-down list of **Wallpaper**.



To change the wallpaper via web user interface:

1. Click on **Settings->Preference**.
2. Select the desired wallpaper from the pull-down list of **Wallpaper**.



3. Click **Confirm** to accept the change.

To change the wallpaper via phone user interface:

1. Press **Menu->Basic->Display->Wallpaper**.
2. Press  or , or the **Switch** soft key to select the desired wallpaper.
3. Press the **Save** soft key to accept the change.

Backlight

Backlight determines the brightness of the LCD screen display, allowing users to read easily in dark environments. Backlight time specifies the delay time to turn off or dusky the backlight when the IP phone is inactive. Backlight time is applicable to SIP-T4X IP phones and EXP40 connected to SIP-T46G IP phones.

You can configure the backlight time as one of the following types:

- **Always On:** Backlight is turned on permanently.
- **15, 30, 60, 120, 300, 600 or 1800:** Backlight is turned off or turned dusky when the IP phone is inactive after a preset period of time. It is automatically turned on if the status of the IP phone changes or any key is pressed.

Backlight Active Level is used to adjust the backlight intensity of the LCD screen, and Backlight Inactive Level is used to turn off or dusky the backlight after a period of inactivity. Backlight Active Level is only applicable to SIP-T46G IP phones and the connected EXP40. Backlight Inactive Level is only applicable to SIP-T46G IP phones.

Procedure

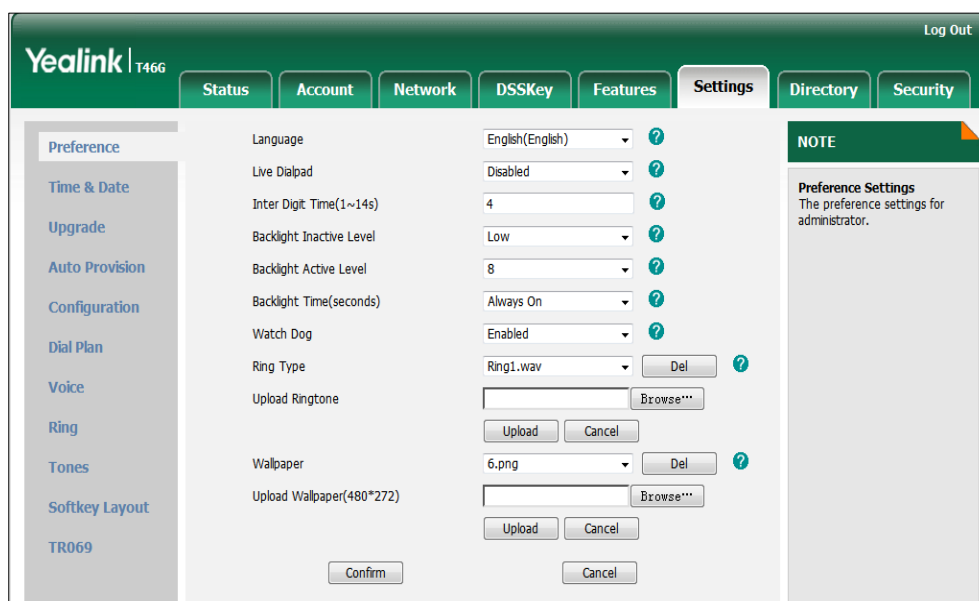
Backlight can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure the backlight of the LCD screen. For more information, refer to Backlight on page 262.
Local	Web User Interface	Configure the backlight of the LCD screen. Navigate to: http://<phoneIPAddress>/servlet?p=settings-preference&q=load
	Phone User Interface	Configure the backlight of the LCD screen.

To configure the backlight via web user interface:

1. Click on **Settings->Preference**.
2. Select the desired value from the pull-down list of **Backlight Inactive Level**.
3. Select the desired value from the pull-down list of **Backlight Active Level**.

4. Select the desired value from the pull-down list of **Backlight Time (seconds)**.



5. Click **Confirm** to accept the change.

To configure the backlight via phone user interface:

1. Press **Menu->Basic->Display-> Backlight**.
2. Press **◀** or **▶**, or the **Switch** soft key to select the desired level from the **Backlight Active Level** field.
3. Press **◀** or **▶**, or the **Switch** soft key to select the desired value from the **Backlight Inactive Level** field.
4. Press **◀** or **▶**, or the **Switch** soft key to select the desired time from the **Backlight Time** field.
5. Press the **Save** soft key to accept the change.

User Password

Some menu options are protected by two privilege levels, user and administrator, each with its own password. When logging into the web user interface, you need to enter the user name and password to access various menu options.

A user or an administrator can change the user password. The default user password is "user". For security reasons, the user or the administrator should change the default user password as soon as possible.

Procedure

User password can be changed using the configuration files or locally.

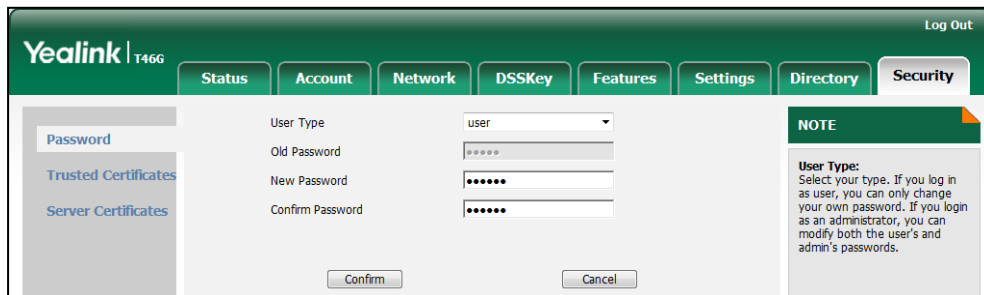
Configuration File	<y0000000000xx>.cfg	Change the user password of the IP phone.
---------------------------	---------------------	---

		For more information, refer to User Password on page 263.
Local	Web User Interface	Change the user password of the IP phone. Navigate to: http://<phoneIPAddress>/servlet?p=security&q=load

To change the user password via web user interface:

1. Click on **Security->Password**.
2. Select **user** from the pull-down list of **User Type**.
3. Enter a new password in the **New Password** and **Confirm Password** fields.

A new password should contain at least 6 characters, where at least one numeric and one alphabetic characters. Valid characters are A-Z, a-z, 0-9,#,!,@,-,.,*,+ and \$.



4. Click **Confirm** to accept the change.

Note If logging into the web user interface of the phone with the user credential, user needs to enter the current user password in the **Old Password** field.

Administrator Password

Advanced menu options are strictly used by administrators. Users can configure them only if they have administrator privileges.

The administrator password can only be changed by an administrator. The default administrator password is “admin”. For security reasons, the administrator should change the default administrator password as soon as possible.

Procedure

Administrator password can be changed using the configuration files or locally.

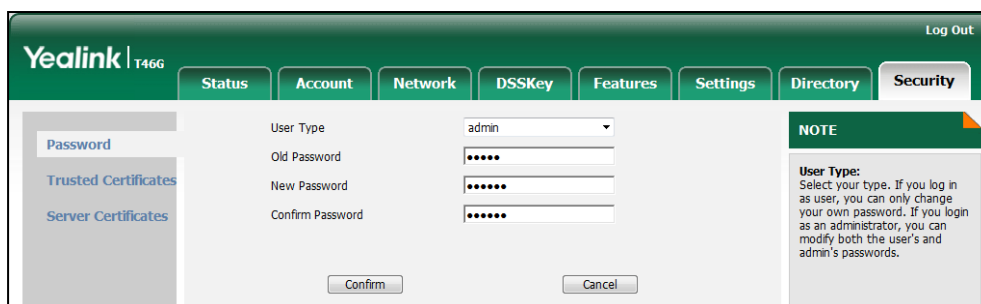
Configuration File	<y0000000000xx>.cfg	Change the administrator password. For more information, refer to
---------------------------	---------------------	--

		Administrator Password on page 263.
Local	Web User Interface	Change the administrator password. Navigate to: http://<phoneIPAddress>/servlet?p=security&q=load
	Phone User Interface	Change the administrator password.

To change the administrator password via web user interface:

1. Click on **Security->Password**.
2. Select **admin** from the pull-down list of **User Type**.
3. Enter the current administrator password in the **Old Password** field.
4. Enter a new administrator password in the **New Password** and **Confirm Password** fields.

A new password should contain at least 6 characters, where at least one numeric and one alphabetic characters. Valid characters contain A-Z, a-z, 0-9,#,!,@,-,.,*,+ and \$.



5. Click **Confirm** to accept the change.

To change the administrator password via phone user interface:

1. Press **Menu->Advanced** (password: admin) -> **Set Password**.
2. Enter the current administrator password in the **Current Password** field.
3. Enter a new administrator password in the **New Password** field and **Confirm Password** field.
4. Press the **Save** soft key to accept the change.

Phone Lock

Phone lock is used to lock the IP phone to prevent it from unauthorized use. Once the IP phone is locked, a user must enter the password to unlock it. IP phones offer three types

of phone lock: Menu Key, Function Keys and All Keys. The IP phone will not be locked immediately after the phone lock type is configured. One of the following steps is also needed:

- Long press the pound key when the IP phone is idle.
- Press the keypad lock key (if configured) when the IP phone is idle.

In addition to the above steps, you can configure IP phones to automatically lock the keypad after a period of time.

Procedure

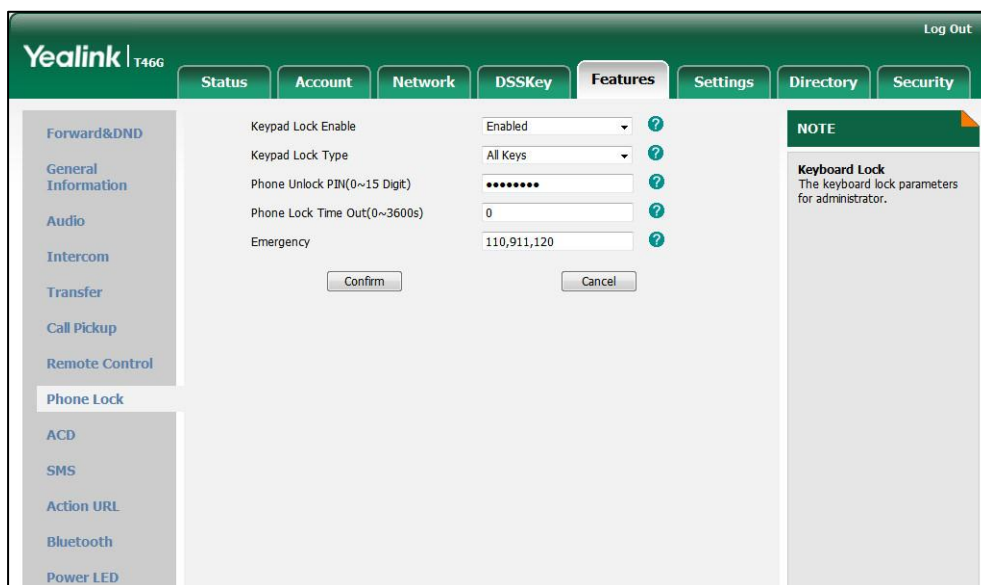
Phone lock can be configured using the configuration files or locally.

<p>Configuration File</p>	<p><y0000000000xx>.cfg</p>	<p>Configure the phone lock type. Change the unlock password. Configure the IP phone to automatically lock the keypad after a time interval. For more information, refer to Phone Lock on page 264. Assign a keypad lock key. For more information, refer to Keypad Lock Key on page 386.</p>
<p>Local</p>	<p>Web User Interface</p>	<p>Configure the phone lock type. Change the unlock password. Configure the IP phone to automatically lock the keypad after a time interval. Navigate to: http://<phoneIPAddress>/servlet?p=features-phonelock&q=load Assign a keypad lock key. Navigate to: http://<phoneIPAddress>/servlet?p=dsskey&model=1&q=load&linepage=1</p>
	<p>Phone User Interface</p>	<p>Configure the phone lock type. Assign a keypad lock key.</p>

To configure phone lock via web user interface:

1. Click on **Features->Phone Lock**.

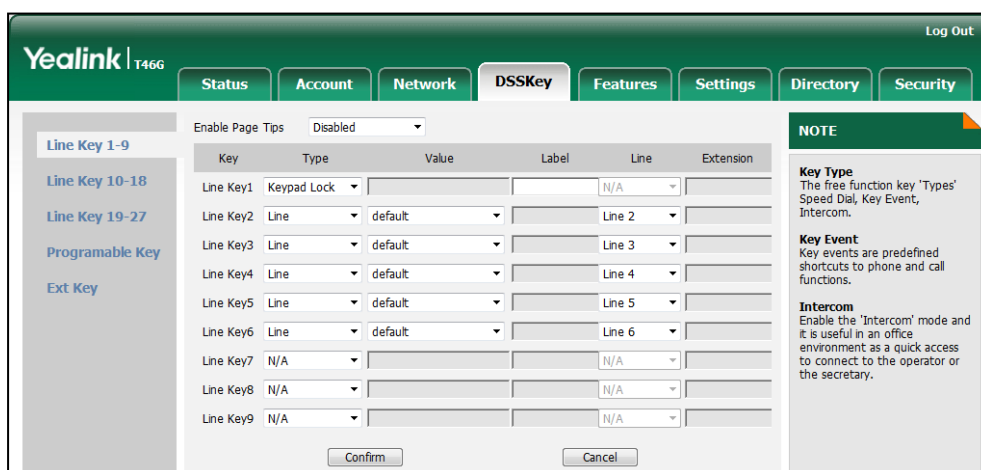
2. Select the desired type from the pull-down list of **Keypad Lock Enable**.
3. Select the desired type from the pull-down list of **Keypad Lock Type**.
4. Enter unlock password (numeric characters) in the **Phone Unlock PIN (0~15 Digit)** field.
5. Enter the desired time in the **Phone Lock Time Out (0~3600s)** field.



6. Click **Confirm** to accept the change.

To configure a keypad lock key via web user interface:

1. Click on **DSSKey->Line Key**.
2. In the desired DSS key field, select **Keypad Lock** from the pull-down list of **Type**.



3. Click **Confirm** to accept the change.

To configure phone lock type via phone user interface:

1. Press **Menu->Advanced** (password: admin) ->**Phone Settings->Keypad Lock**.

2. Press ◀ or ▶ , or the **Switch** soft key to select the desired value from the **Keypad Lock Enable** field.
3. Press ◀ or ▶ , or the **Switch** soft key to select the desired type from the **Keypad Lock Type** field.
4. Press the **Save** soft key to accept the change.

To configure a keypad lock key via phone user interface:

1. Press **Menu->Call Features->DSS Keys**.
2. Select the desired DSS key.
3. Press ◀ or ▶ , or the **Switch** soft key to select **Key Event** from the **Type** field.
4. Press ◀ or ▶ , or the **Switch** soft key to select **Keypad Lock** from the **Key Event** field.
5. (Optional.) Enter the string that will appear on the LCD screen in the **Label** field.
6. Press the **Save** soft key to accept the change.

Time and Date

IP phones maintain a local clock and calendar. Time and date are displayed on the idle screen of the IP phone. Time and date are synced automatically from the NTP server by default. The NTP server can be obtained by DHCP or configured manually. If IP phones cannot obtain the time and date from the NTP server, you need to manually configure them. The time and date display can use one of several different formats.

Time Zone

A time zone is a region on Earth that has a uniform standard time. It is convenient for areas in close commercial or other communication to keep the same time. When configuring IP phones to obtain the time and date from the NTP server, you must set the time zone.

Daylight Saving Time

Daylight Saving Time (DST) is the practice of temporary advancing clocks during the summertime so that evenings have more daylight and mornings have less. Typically, clocks are adjusted forward one hour at the start of spring and backward in autumn. Many countries have used the DST at various times, details vary by location. The DST can be adjusted automatically from the time zone configuration. Typically, there is no need to change this setting.

The following table lists available methods for configuring time and date:

Option	Methods of Configuration
Time Zone	Configuration Files Web User Interface Phone User Interface
Time	Web User Interface Phone User Interface
Time Format	Configuration Files Web User Interface Phone User Interface
Date	Web User Interface Phone User Interface
Date Format	Configuration Files Web User Interface Phone User Interface
Daylight Saving Time	Configuration Files Web User Interface

Procedure

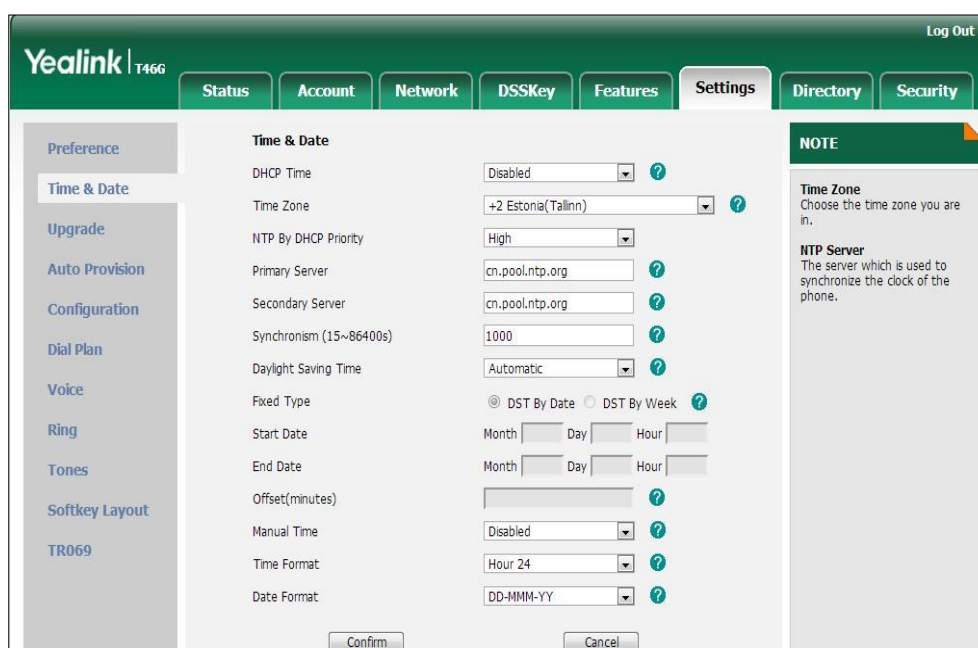
Configuration changes can be performed using the configuration files or locally.

Configuration File	<MAC>.cfg	<p>Configure NTP by DHCP priority feature.</p> <p>Configure the NTP server, time zone and DST.</p> <p>Configure the time and date formats.</p> <p>For more information, refer to Time and Date on page 266.</p>
Local	Web User Interface	<p>Configure NTP by DHCP priority feature.</p> <p>Configure the NTP server, time zone and DST.</p> <p>Configure the time and date manually.</p> <p>Configure the time and date formats.</p>

		<p>Navigate to: <a href="http://<phoneIPAddress>/servlet?p=settings-datettime&q=load">http://<phoneIPAddress>/servlet?p=settings-datettime&q=load</p>
	Phone User Interface	<p>Configure the NTP server and time zone.</p> <p>Configure the time and date manually.</p> <p>Configure the time and date formats.</p>

To configure NTP by DHCP priority feature via web user interface:

1. Click on **Settings->Time & Date**.
2. Select the desired value from the pull-down list of **NTP By DHCP Priority**.



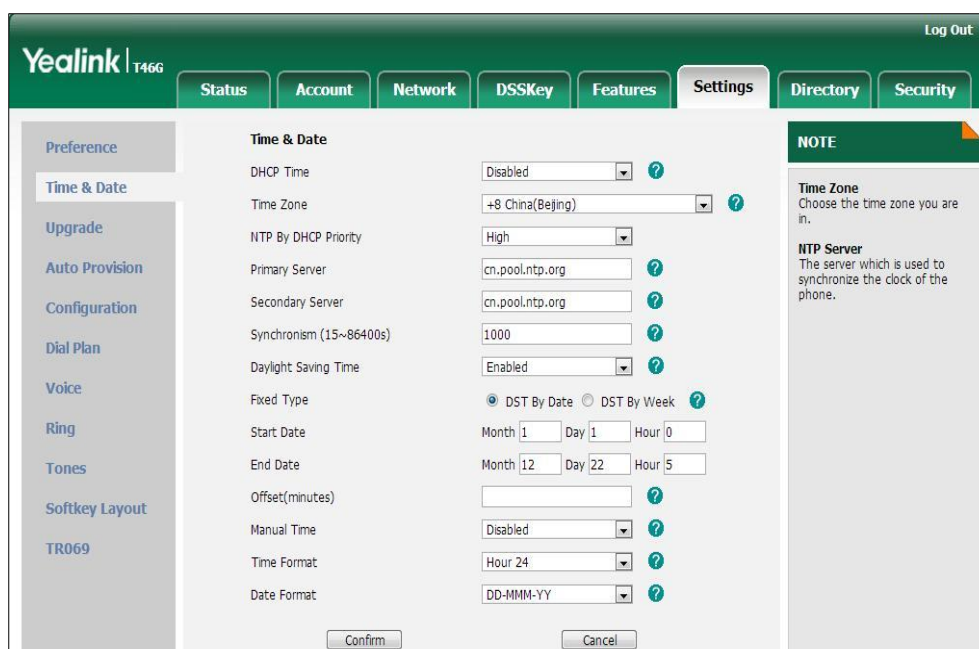
3. Click **Confirm** to accept the change.

To configure the NTP server, time zone and DST via web user interface:

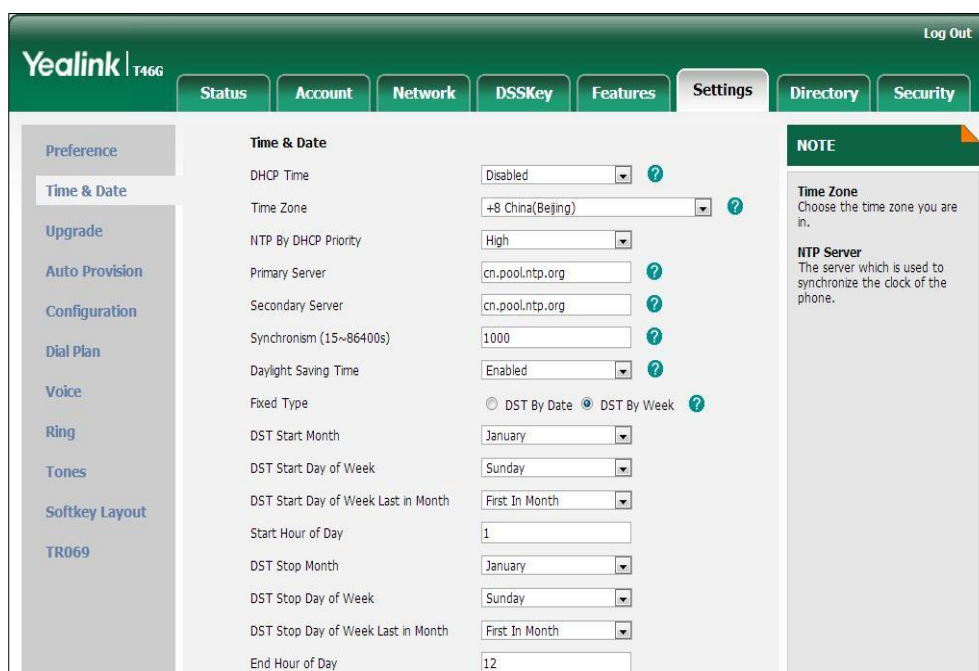
1. Click on **Settings->Time & Date**.
2. Select **Disabled** from the pull-down list of **Manual Time**.
3. Select the desired time zone from the pull-down list of **Time Zone**.
4. Enter the domain names or IP addresses in the **Primary Server** and **Secondary Server** fields respectively.
5. Enter the desired time interval in the **Synchronism (15~86400s)** field.
6. Select the desired value from the pull-down list of **Daylight Saving Time**.

If you select **Enabled**, do one of the following:

- Mark the **DST By Date** radio box in the **Fixed Type** field.
Enter the start time in the **Start Date** field.
Enter the end time in the **End Date** field.



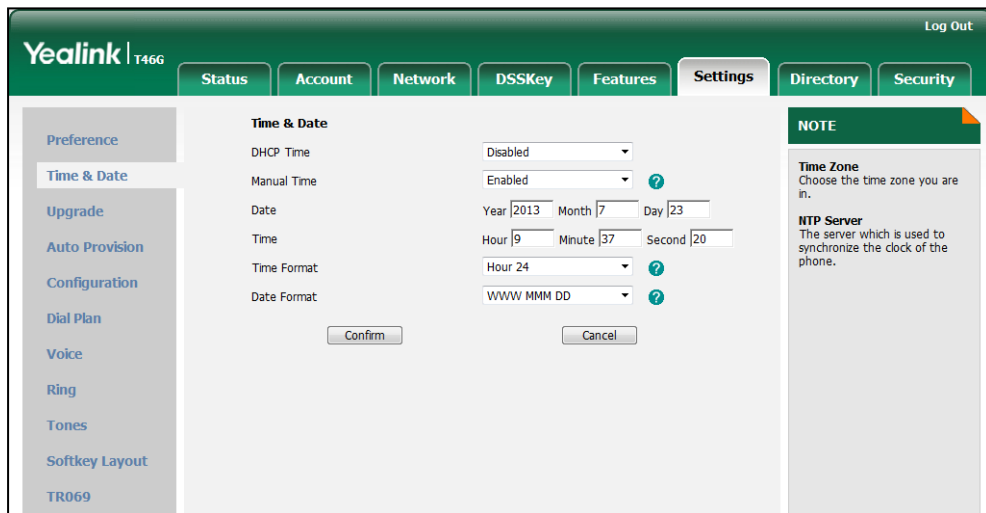
- Mark the **DST By Week** radio box in the **Fixed Type** field.
Select the desired values from the pull-down lists of **DST Start Month**, **DST Start Day of Week**, **DST Start Day of Week Last in Month**, **DST Stop Month**, **DST Stop Day of Week** and **DST Stop Day of Week Last in Month**.
Enter the desired time in the **Start Hour of Day** field.
Enter the desired time in the **End Hour of Day** field.



7. Enter the desired offset time in the **Offset (minutes)** field.
8. Click **Confirm** to accept the change.

To configure the time and date manually via web user interface:

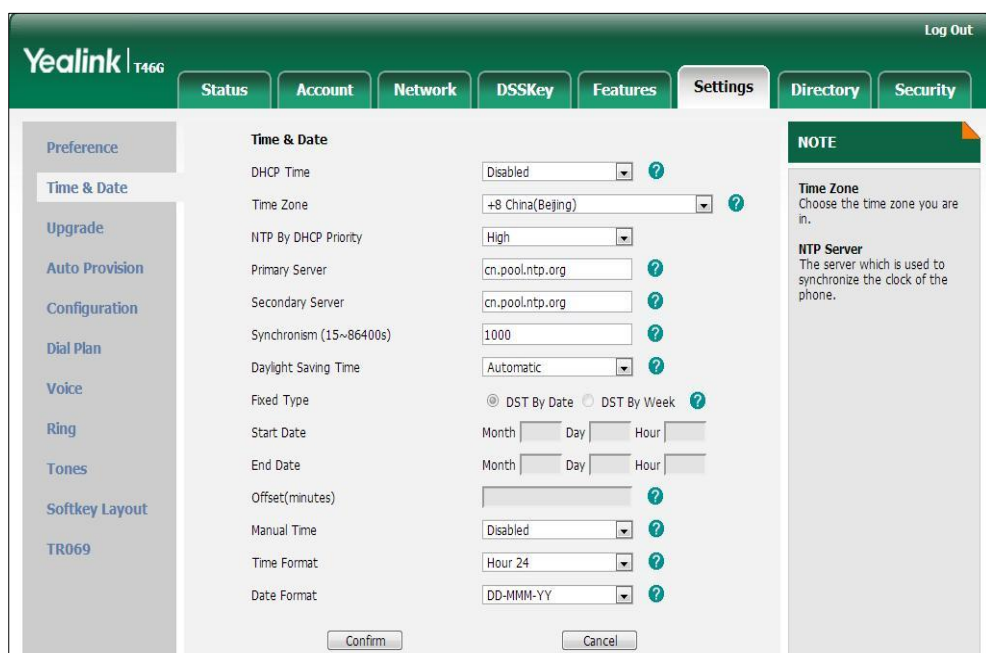
1. Click on **Settings->Time & Date**.
2. Select **Enabled** from the pull-down list of **Manual Time**.
3. Enter the time and date in the corresponding fields.



4. Click **Confirm** to accept the change.





To configure the time and date format via web user interface:

1. Click on **Settings->Time & Date**.
2. Select the desired value from the pull-down list of **Time Format**.
3. Select the desired value from the pull-down list of **Date Format**.



4. Click **Confirm** to accept the change.





To configure the NTP server and time zone via phone user interface:

1. Press **Menu->Basic->Time & Date->General->SNTP Settings**.
2. Press  or , or the **Switch** soft key to select the time zone that applies to your area from the **Time Zone** field.
The default time zone is "+8 China(Beijing)".
3. Enter the domain names or IP addresses in the **NTP Server 1** and **NTP Server 2** fields respectively.
4. Press  or , or the **Switch** soft key to select **Automatic** from the **Daylight Saving** field.
5. Press the **Save** soft key to accept the change.

To configure the time and date manually via phone user interface:

1. Press **Menu->Basic->Time & Date->General->Manual Settings**.
2. Enter the specific time and date.
3. Press the **Save** soft key to accept the change.

To configure the time and date formats via phone user interface:

1. Press **Menu->Basic->Time & Date->Format**.
2. Press  or , or the **Switch** soft key to select the desired date format from the **Date Format** field.
3. Press  or , or the **Switch** soft key to select the desired time format (12 Hour or 24 Hour) from the **Time Format** field.
4. Press the **Save** soft key to accept the change.

Language

IP phones support multiple languages. Languages used on the phone user interface and web user interface can be specified respectively as required.

The following table lists the languages supported by the phone user interface and the web user interface respectively.

Phone User Interface	Web User Interface
English	English
Simplified Chinese (not applicable to SIP-T42G/T41P)	Simplified Chinese (not applicable to SIP-T42G/T41P)
Traditional Chinese (not applicable to SIP-T42G/T41P)	Traditional Chinese (not applicable to SIP-T42G/T41P)
French	French

Phone User Interface	Web User Interface
German	German
Italian	Italian
Polish	Turkish
Portuguese	Portuguese
Spanish	Spanish
Turkish	

Loading Language Packs

Not all of the supported languages are available for selection. Languages available for selection depend on language packs currently loaded to IP phones. You can make languages available for use on the phone user interface by loading language packs to the IP phone. Language packs can only be loaded using the configuration files.

The following table lists available languages and the associated language packs:

Available Language	Associated Language Pack for SIP-T42G/T41P	Associated Language Pack for SIP-T46G
English	lang+English.txt	lang+English.txt
Simplified Chinese	/	lang-Chinese_S.txt
Traditional Chinese	/	lang-Chinese_T.txt
German	lang-German.txt	lang-German.txt
French	lang-French.txt	lang-French.txt
Italian	lang-Italian.txt	lang-Italian.txt
Polish	lang-Polish.txt	lang-Portuguese.txt
Portuguese	lang-Portuguese.txt	lang-Polish.txt
Spanish	lang-Spanish.txt	lang-Spanish.txt
Turkish	lang-Turkish.txt	lang-Turkish.txt

To update translation of a built-in language, the file name of the language file cannot be changed. For more information, refer to *Yealink SIP-T2 Series_T19P_T4_Series_IP_Phones_Auto_Provisioning_Guide*.

Procedure

Loading language pack can only be performed using the configuration files.

Configuration File	<y0000000000xx>.cfg	Specify the access URL of the language pack.
---------------------------	---------------------	--

		For more information, refer to Language on page 272.
--	--	--

Specifying the Language to Use

The default language used on the phone user interface is English. The default language used on the web user interface depends on the language preferences in the browser (if the language is not supported by the IP phone, the web user interface uses English). You can specify the languages for the phone user interface and web user interface.

Procedure

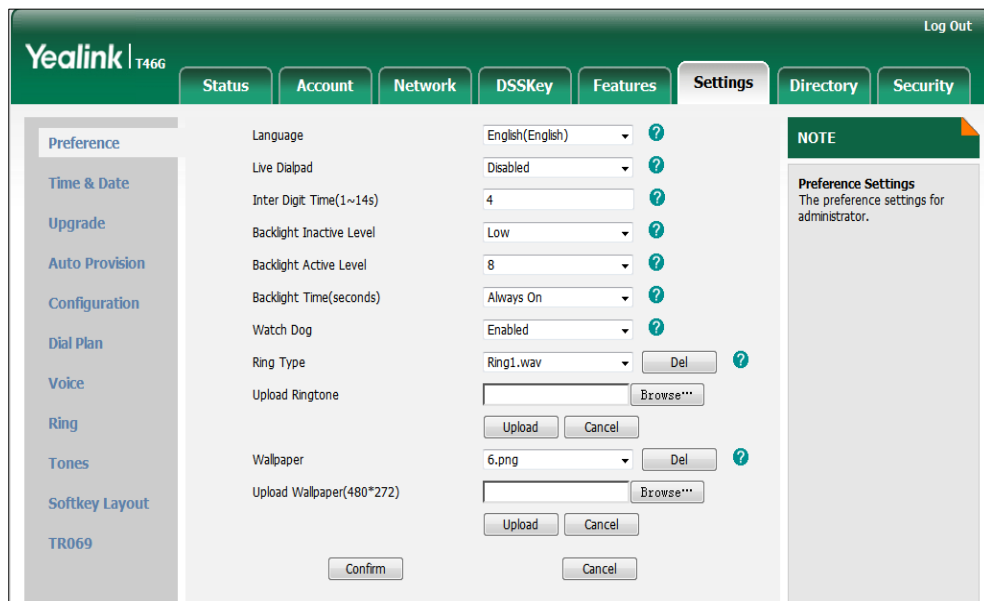
Specify the language for the web user interface or the phone user interface using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Specify the languages for the phone user interface and the web user interface. For more information, refer to Language on page 272.
Local	Web User Interface	Specify the language for the web user interface. Navigate to: http://<phoneIPAddress>/servlet?p=settings-preference&q=load
	Phone User Interface	Specify the language for the phone user interface.

To specify the language for the web user interface via web user interface:

1. Click on **Settings->Preference**.

2. Select the desired language from the pull-down list of **Language**.



3. Click **Confirm** to accept the change.

To specify the language for the phone user interface via phone user interface:

1. Press **Menu->Basic->Language**.
2. Press **▲** or **▼** to select the desired language.
3. Press the **Save** soft key to accept the change.

Logo Customization

Logo customization allows unifying the IP phone appearance or displaying a custom image on the idle screen such as a company logo, instead of the default system logo. Logo is not applicable to SIP-T46G IP phones. The logo file format must be *.dib, and the resolution of SIP-T42G/T41P IP phones is 192*64 graphic.

Note

Before uploading your custom logo to IP phones, ensure the logo file is correctly formatted. For more information on customizing a logo file, refer to *Yealink_SIP-T2 Series_T19P_T4_Series_IP_Phones_Auto_Provisioning_Guide*.

Procedure

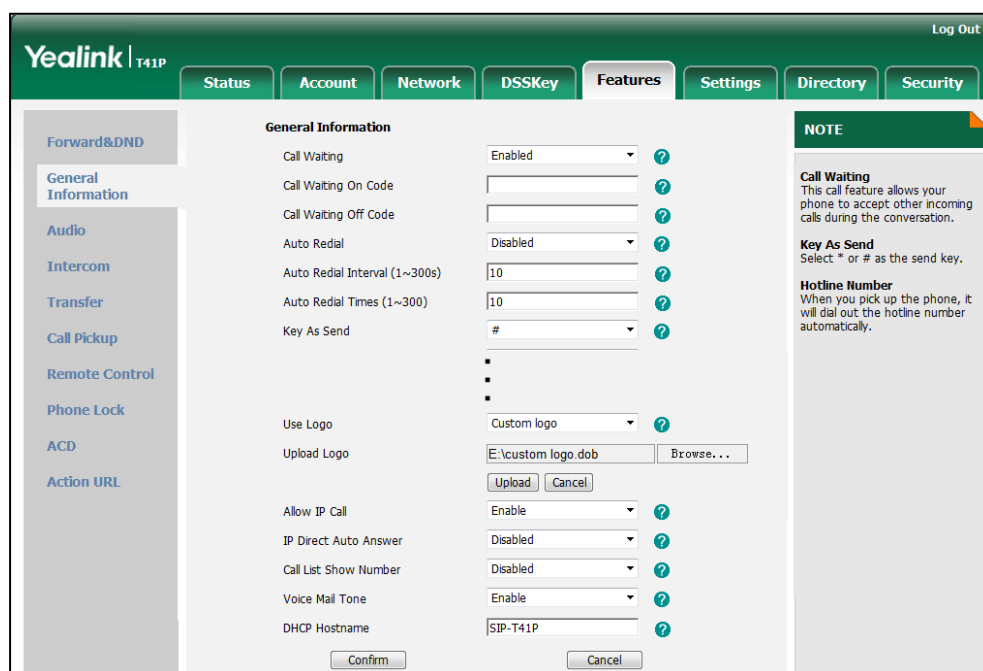
The logo shown on the idle screen can be configured using the configuration files or locally.

<p>Configuration File</p>	<p><y0000000000xx>.cfg</p>	<p>Configure the logo shown on the idle screen. For more information, refer to Logo Customization on page 273.</p>
----------------------------------	----------------------------------	--

<p>Local</p>	<p>Web User Interface</p>	<p>Configure the logo shown on the idle screen.</p> <p>Navigate to: <a href="http://<phoneIPAddress>/servlet?p=features-general&q=load">http://<phoneIPAddress>/servlet?p=features-general&q=load</p>
---------------------	---------------------------	---

To configure a custom logo via web user interface:

1. Click on **Features->General Information**.
2. Select **Custom logo** from the pull-down list of **Use Logo**.



3. Click **Browse** to select the logo file from your local system.
4. Click **Upload** to upload the file.
5. Click **Confirm** to accept the change.

The custom logo screen and the idle screen are displayed alternately.

Softkey Layout

Softkey layout is used to customize the soft keys at the bottom of the LCD screen to best meet users' requirements. It can be configured based on call states. In addition to specifying which soft keys to display, you can determine their display order. You can create a template about the softkey layout for the different call states. For more information on the softkey layout template, refer to [Softkey Layout Template](#) on page 221.

The following table lists the soft keys available for IP phones in different states:

Call State		Default Soft Key	Optional Soft Key
CallFailed		NewCall Empty Empty Empty	Empty Switch Cancel
CallIn		Answer Forward Silence Reject	Empty Switch
Connecting	Connecting	Empty Empty Empty Cancel	Empty Switch
	SemiAttendTrans	Transfer Empty Empty Cancel	Empty Switch
Dialing		Send IME Delete Cancel	Empty History Switch Line Favorite GPickup DPickup
RingBack	RingBack	Empty Empty Empty Cancel	Empty Switch CC
	SemiAttendTransBack	Transfer Empty Empty Cancel	Empty Switch CC
Talking	Talk	Transfer HOLD	Empty MUTE

Call State		Default Soft Key	Optional Soft Key
		Conference Cancel	SWAP NewCall Switch Answer Reject
	Hold	Transfer Resume NewCall Cancel	Empty Switch Answer Reject
	Held	Empty Empty Empty Cancel	Empty Switch Answer Reject NewCall
	PreTrans	Transfer IME Delete Cancel	Empty Directory Switch Send
	Conferenced	Empty Hold Split Cancel	Empty Switch Answer Reject Mute Manager





Procedure

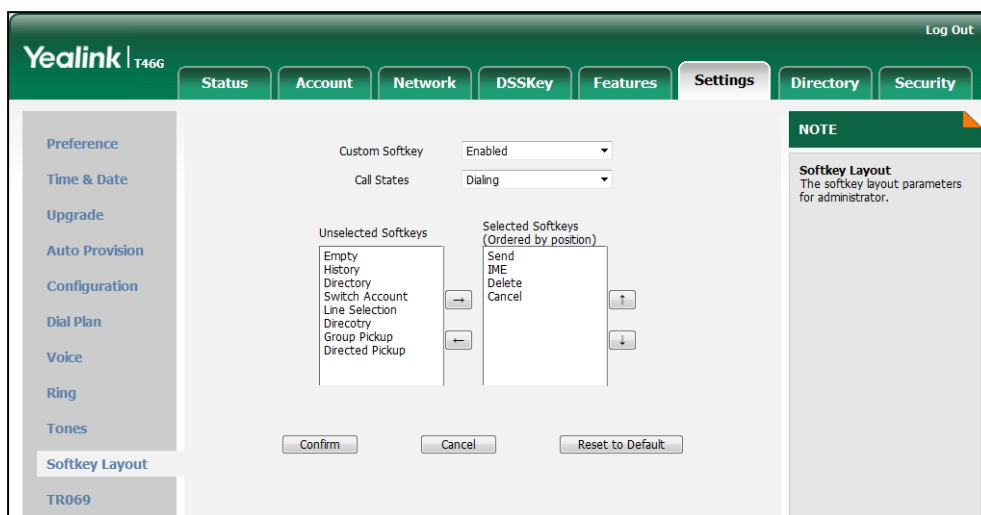
Softkey layout can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Specify the access URL of the softkey layout template. For more information, refer to Access URL of Softkey Layout Template on page 375.
Local	Web User Interface	Configure the softkey layout. Navigate to: http://<phoneIPAddress>/servlet

		?p=settings-softkey&q=load
--	--	----------------------------

To configure softkey layout via web user interface:

1. Click on **Settings->Softkey Layout**.
2. Select the desired value from the pull-down list of **Custom Softkey**.
3. Select the desired state from the pull-down list of **Call States**.
4. Select the desired soft key from the **Unselected Softkeys** column and click  .
The selected soft key appears in the **Selected Softkeys** column. If more than four soft keys are selected, a More soft key appears on the LCD screen, and the selected soft keys are displayed in two pages.
5. Repeat the step 4 to add more soft keys to the **Selected Softkeys** column.
6. Click  to remove the soft key from the **Selected Softkeys** column.
7. Click  or  to adjust the display order of the soft key.



8. Click **Confirm** to accept the change.

Key as Send

Key as send allows assigning the pound key or star key as a send key. Send sound allows the IP phone to play a key tone when a user presses the send key. Key tone allows the IP phone to play a key tone when a user presses any key. Send sound works only if Key tone is enabled.

Procedure

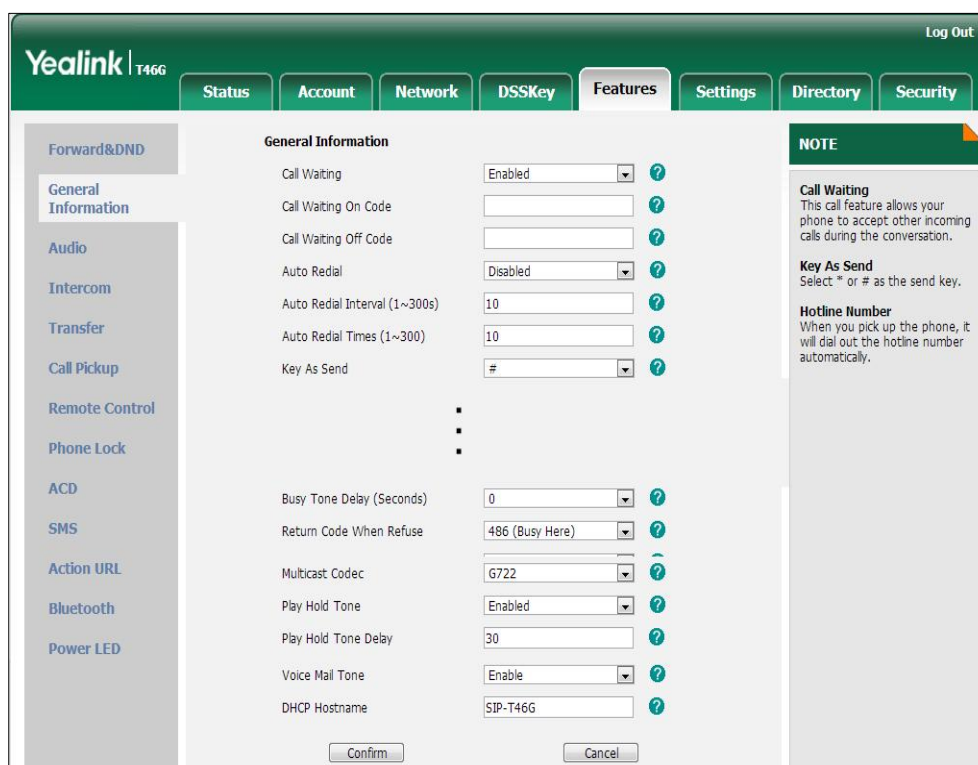
Key as send can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure a send key. Configure a key tone and send tone.
---------------------------	---------------------	--

		For more information, refer to Key as Send on page 274.
Local	Web User Interface	<p>Configure a send key.</p> <p>Navigate to: <a href="http://<phoneIPAddress>/servlet?p=features-general&q=load">http://<phoneIPAddress>/servlet?p=features-general&q=load</p> <p>Configure a key tone and send tone.</p> <p>Navigate to: <a href="http://<phoneIPAddress>/servlet?p=features-audio&q=load">http://<phoneIPAddress>/servlet?p=features-audio&q=load</p>
	Phone User Interface	Configure the send key.

To configure a send key via web user interface:

1. Click on **Features->General Information**.
2. Select the desired value from the pull-down list of **Key As Send**.

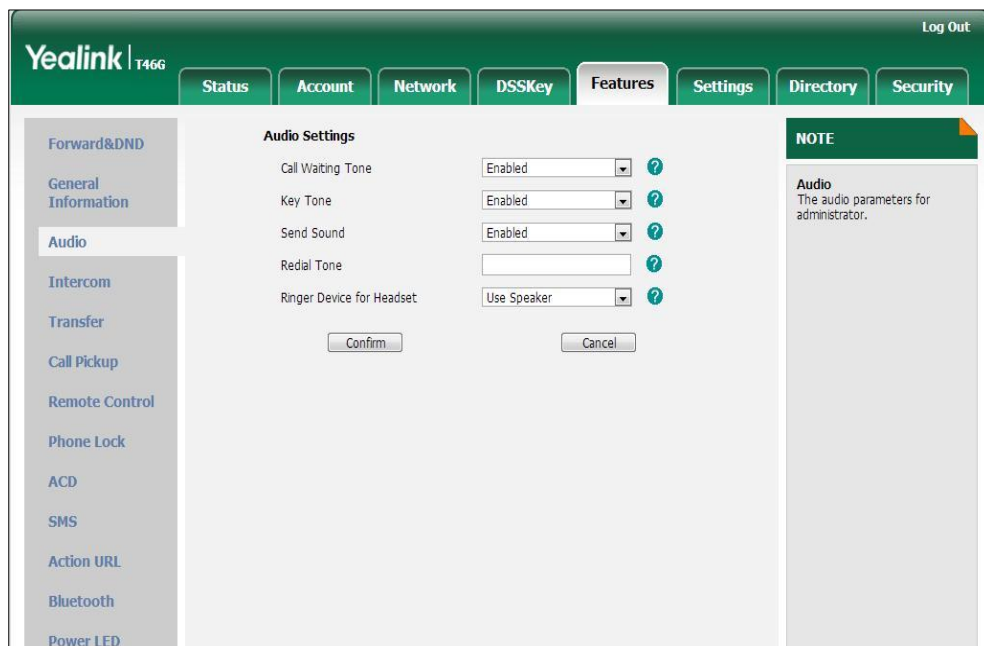


3. Click **Confirm** to accept the change.

To configure a key tone and send tone via web user interface:

1. Click on **Features->Audio**.
2. Select the desired value from the pull-down list of **Key Tone**.

3. Select the desired value from the pull-down list of **Send Sound**.



4. Click **Confirm** to accept the change.

To configure a send key via phone user interface:

1. Press **Menu->Call Features->Others->General**.
2. Press **←** or **→**, or the **Switch** soft key to select **#** or ***** from the **Key as Send** field, or select **Disabled** to disable this feature.
3. Press the **Save** soft key to accept the change.

Note

Send tone works only if key tone is enabled. Key tone is enabled by default.

Hotline

A hotline is a point-to-point communication link in which a call is automatically directed to the preset hotline number. The IP phone automatically dials out the hotline number using the first available line after a time interval when off-hook. IP phones only support one hotline number.

Procedure

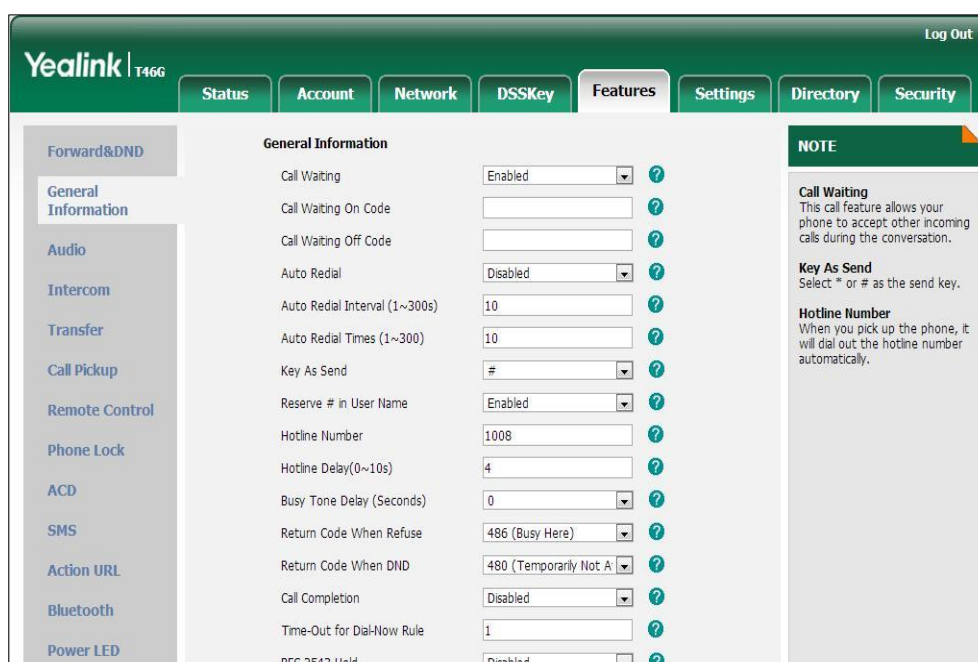
Hotline can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure the hotline number. Specify the time (in seconds) the IP phone waits to automatically dial out the hotline number. For more information, refer to
---------------------------	---------------------	---

		Hotline on page 276.
Local	Web User Interface	<p>Configure the hotline number.</p> <p>Specify the time (in seconds) the IP phone waits to automatically dial out the hotline number.</p> <p>Navigate to: <a href="http://<phoneIPAddress>/servlet?p=features-general&q=load">http://<phoneIPAddress>/servlet?p=features-general&q=load</p>
	Phone User Interface	<p>Configure the hotline number.</p> <p>Specify the time (in seconds) the IP phone waits to automatically dial out the hotline number.</p>

To configure hotline via web user interface:

1. Click on **Features->General Information**.
2. Enter the hotline number in the **Hotline Number** field.
3. Enter the delay time in the **Hotline Delay (0~10s)** field.



4. Click **Confirm** to accept the change.

To configure hotline via phone user interface:

1. Press **Menu->Call Features->Others->Hotline**.
2. Enter the hotline number in the **Number** field.
3. Enter the delay time in the **Hotline Delay 0-10(s)** field.
4. Press the **Save** soft key to accept the change.

Call Log

Call log contains call information such as remote party identification, time and date, and call duration. IP phones maintain a local call log. Call log consists of four lists: Missed calls, Placed calls, Received calls and Forwarded calls. Each call log list supports up to 100 entries. To store call information, you must enable the save call log feature in advance.

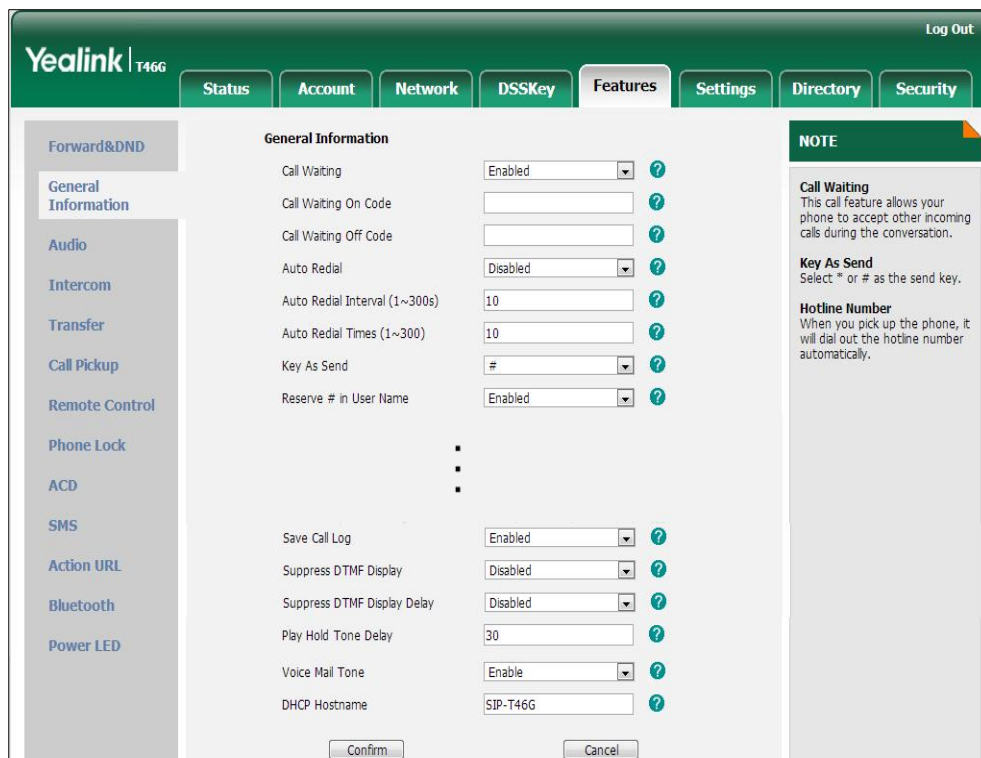
Procedure

Call log can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure the call log. For more information, refer to Call Log on page 277.
Local	Web User Interface	Configure the call log. Navigate to: http://<phoneIPAddress>/servlet? p=features-general&q=load
	Phone User Interface	Configure the call log.



To configure the call log via web user interface:

1. Click on **Features->General Information**.
2. Select the desired value from the pull-down list of **Save Call log**.



3. Click **Confirm** to accept the change.

To configure the call log via phone user interface:

1. Press **Menu->Call Features->Others->General**.
2. Press  or , or the **Switch** soft key to select the desired value from the **History Record** field.
3. Press the **Save** soft key to accept the change.

Missed Call Log

Missed call log allows IP phones to display the number of the missed calls with an indicator icon on the idle screen, and to log the missed calls in the missed calls list when IP phones miss calls. It is configurable on a per-line basis. Once the user accesses the Missed calls list, the prompt message and an indicator icon on the idle screen are cleared.

Procedure

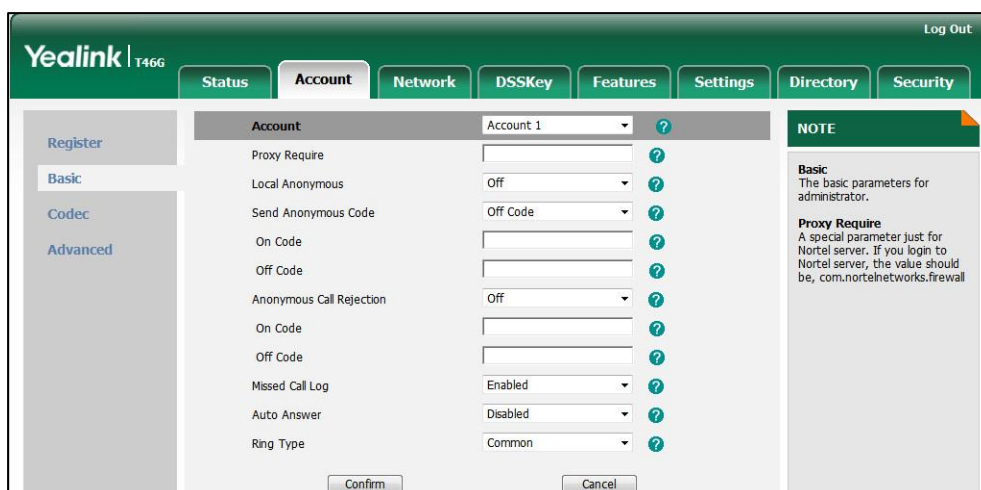
Missed call log can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure the missed call log feature. For more information, refer to Missed Call Log on page 277.
Local	Web User Interface	Configure the missed call log feature. Navigate to: http://<phoneIPAddress>/servlet ?p=account-basic&q=load&acc=0

To configure missed call log via web user interface:

1. Click on **Account**.
2. Select the desired account from the pull-down list of **Account**.
3. Click on **Basic**.

- Select the desired value from the pull-down list of **Missed Call Log**.



- Click **Confirm** to accept the change.

Local Directory

The IP phone maintains a local directory. The local directory can store up to 1000 contacts and 48 groups (including the default groups: Company, Family and Friend). When adding a contact to the local directory, in addition to name and phone numbers, you can also specify the account, ring tone and group for the contact. Contacts and groups can be added either one by one or in batch using a contact file. For more information on the contact file, refer to [Local Contact File](#) on page 223.

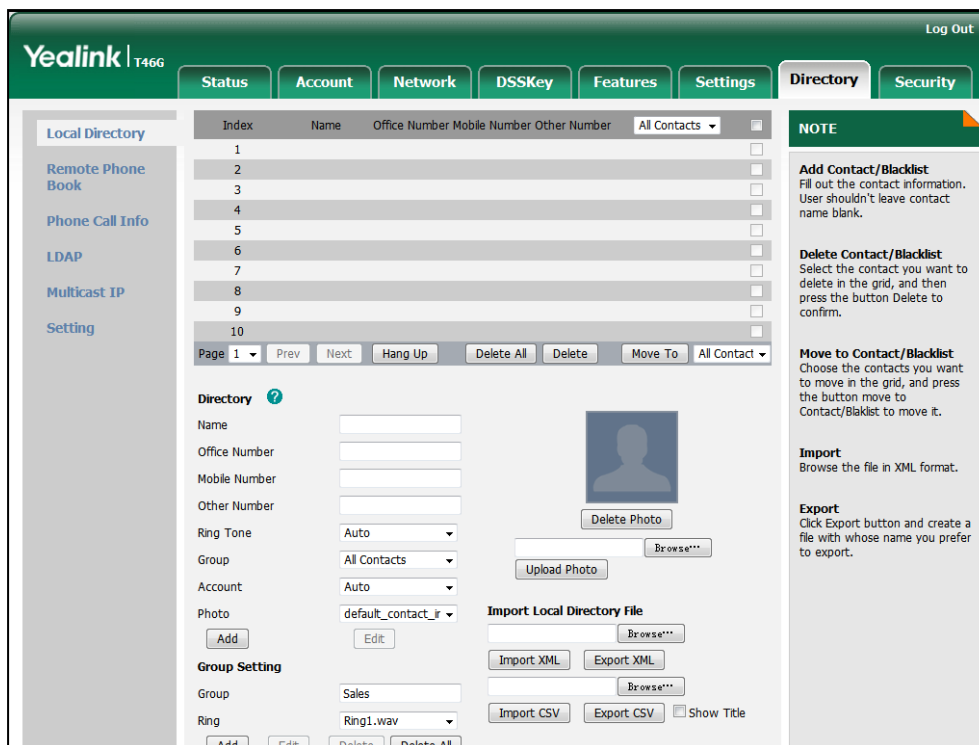
Procedure

Configuration changes can be performed using the configuration files or locally.

<p>Configuration File</p>	<p><y0000000000xx>.cfg</p>	<p>Specify the access URL of the local contact file.</p> <p>For more information, refer to Access URL of Local Contact File on page 377.</p>
<p>Local</p>	<p>Web User Interface</p>	<p>Add a new group and a contact to the local directory.</p> <p>Navigate to: http://<phoneIPAddress>/servlet?p=contactsbasic&q=load&num=1&group=</p>
	<p>Phone User Interface</p>	<p>Add a new group and a contact to the local directory.</p>

To add a new group to the local directory via web user interface:

1. Click on **Directory**->**Local Directory**.
2. In the **Group Setting** block, enter the new group name in the **Group** field.
3. Select the desired group ring tone from the pull-down list of **Ring**.

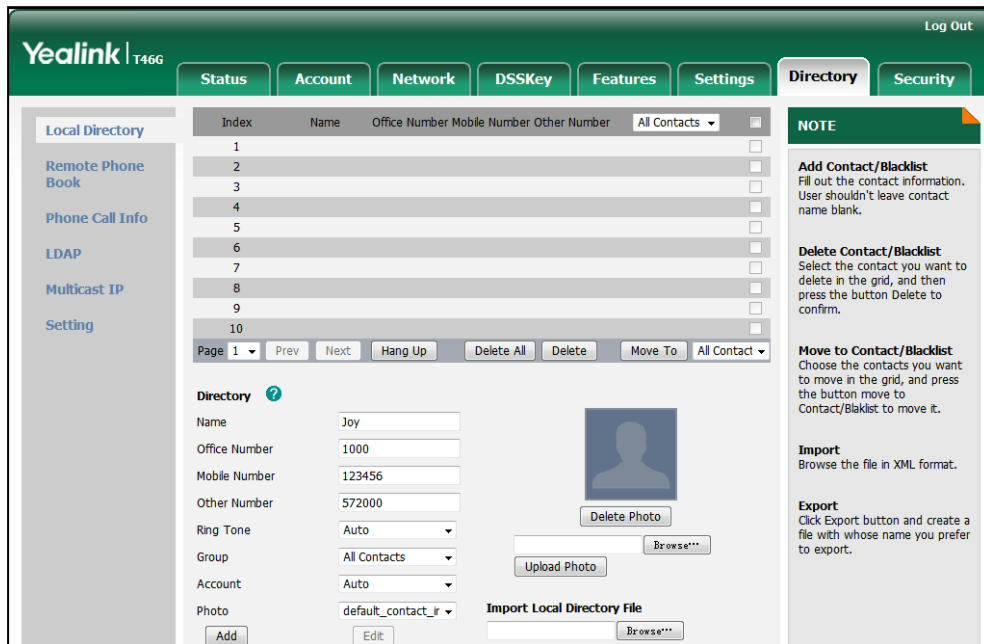


4. Click **Add** to add the new group.

To add a contact to the local directory via web user interface:

1. Click on **Directory**->**Local Directory**.
2. Enter the name and the office, mobile or other numbers in the corresponding fields.
3. Select the desired ring tone from the pull-down list of **Ring Tone**.
4. Select the desired group from the pull-down list of **Group**.
5. Select the desired account from the pull-down list of **Account**.

- Select the desired photo from the pull-down list of **Photo**.
It is not applicable to SIP-T42G and SIP-T41P IP phones.



- Click **Add** to add the contact.

To add a group to the local directory via phone user interface:

- Press **Menu->Directory->Local Group**.
- Press the **Add Group** soft key.
- Enter the desired group name in the **Group Name** field.
- Press **◀** or **▶** to select the desired group ring tone from the **Ring Tones** field.
- Press the **Save** soft key to accept the change or the **Back** soft key to cancel.

To add a contact to the local directory via phone user interface:

- Press **Menu->Directory->Local Group**.
- Select the desired contact group and press the **Enter** soft key.
- Press the **Add** soft key.
- Enter the name and the office, mobile or other numbers in the corresponding fields.
- Press **◀** or **▶**, or the **Switch** soft key to select the desired account from the **Account** field.

If **Auto** is selected, the IP phone will use the first available account when placing calls to the contact from the local directory.

- Press **◀** or **▶**, or the **Switch** soft key to select the desired ring tone from the **Ring** field.
- Press **◀** or **▶**, or the **Switch** soft key to select the desired photo from the **Photo** field.
- Press the **Save** soft key to accept the change.

Live Dialpad

Live dialpad allows IP phones to automatically dial out the entered phone number after a specified period of time.

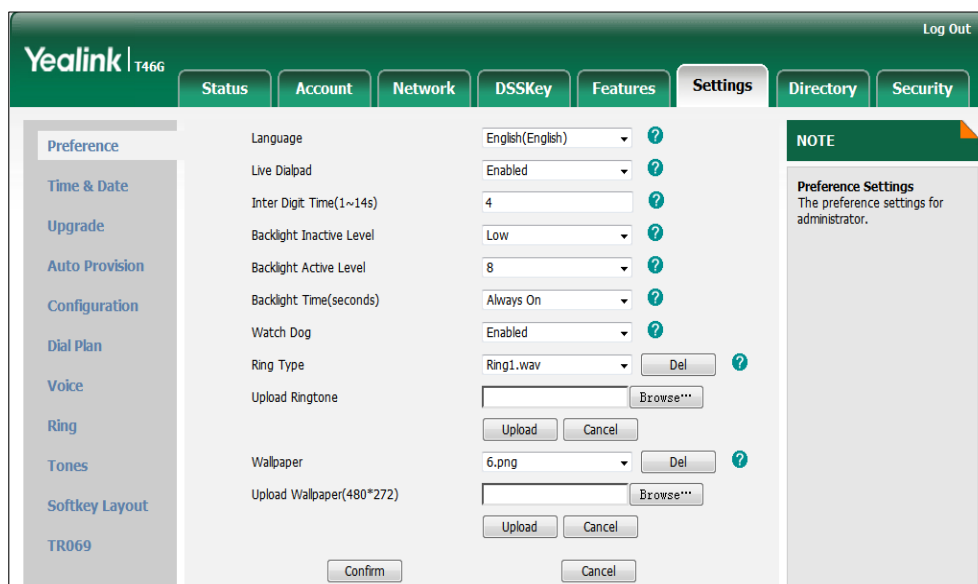
Procedure

Live dialpad can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure live dialpad. For more information, refer to Live Dialpad on page 278.
Local	Web User Interface	Configure live dialpad. Navigate to: http://<phoneIPAddress>/servlet ?p=settings-preference&q=load

To configure live dialpad via web user interface:

1. Click on **Settings->Preference**.
2. Select the desired value from the pull-down list of **Live Dialpad**.
3. Enter the desired delay time in the **Inter Digit Time (1~14s)** field.



4. Click **Confirm** to accept the change.

Call Waiting

Call waiting allows IP phones to receive a new call when there is already an active call. The new call is presented to the user visually on the LCD screen. Call waiting tone

allows the phone to play a short tone, to remind the user audibly of a new incoming call during conversation. Call waiting tone works only if call waiting is enabled.

The call waiting on code and call waiting off code configured on IP phones are used to activate/deactivate the server-side call waiting feature. They may vary on different servers.

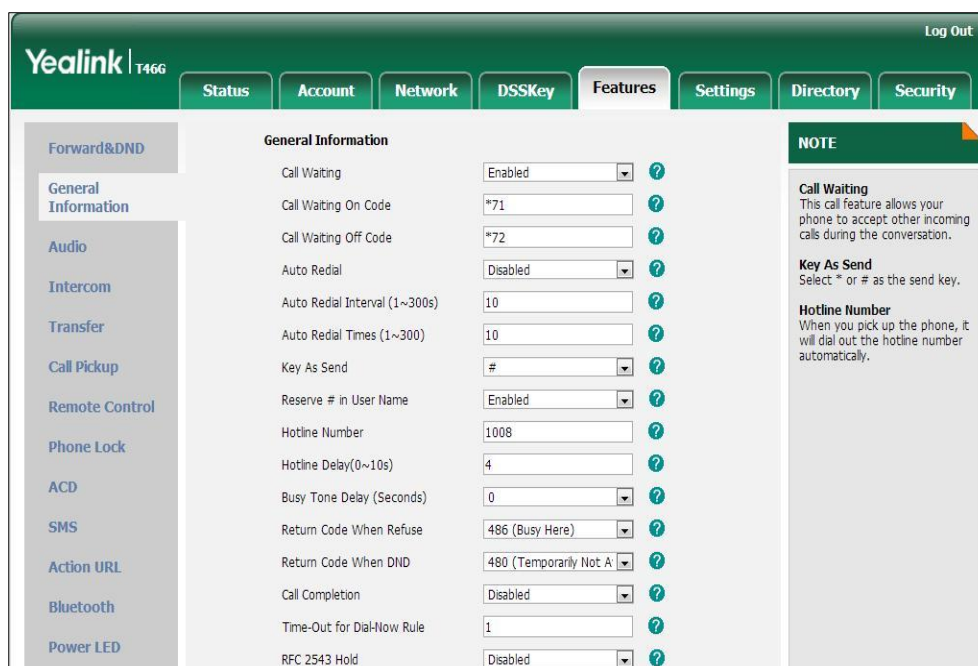
Procedure

Call waiting and call waiting tone can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure call waiting. For more information, refer to Call Waiting on page 278.
Local	Web User Interface	Configure call waiting. Navigate to: http://<phoneIPAddress>/servlet?p=features-general&q=load
	Phone User Interface	Configure call waiting.

To configure call waiting via web user interface:

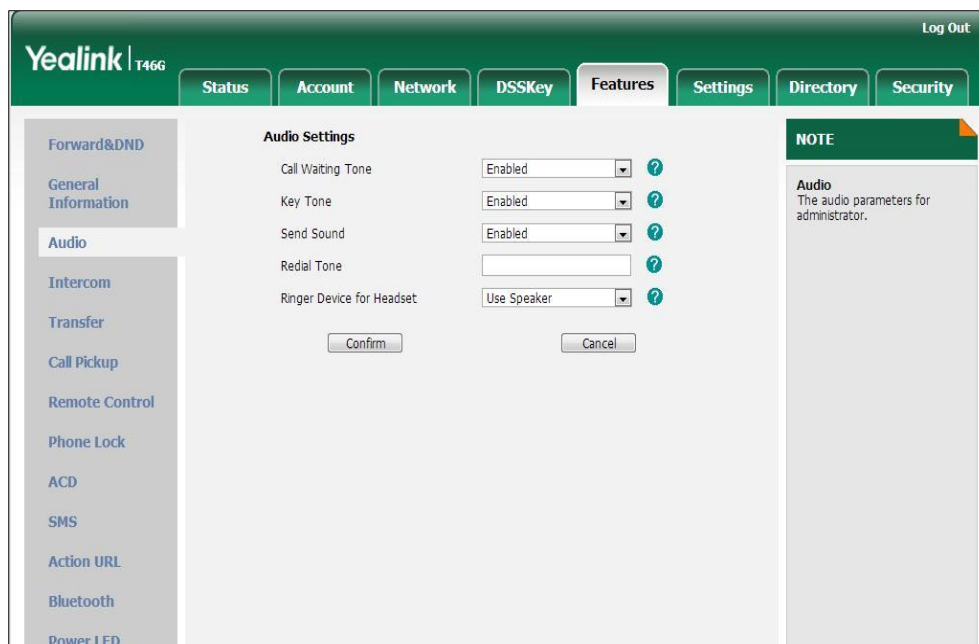
1. Click on **Features->General Information**.
2. Select the desired value from the pull-down list of **Call Waiting**.
3. (Optional.) Enter the call waiting on code in the **Call Waiting On Code** field.
4. (Optional.) Enter the call waiting off code in the **Call Waiting Off Code** field.



5. Click **Confirm** to accept the change.

To configure the call waiting tone via web user interface:

1. Click on **Features->Audio**.
2. Select the desired value from the pull-down list of **Call Waiting Tone**.



3. Click **Confirm** to accept the change.

To configure call waiting and call waiting tone via phone user interface:

1. Press **Menu->Call Features->Call Waiting**.
2. Press **◀** or **▶**, or the **Switch** soft key to select the desired value from the **Call Waiting** field.
3. Press **◀** or **▶**, or the **Switch** soft key to select the desired value from the **Play Tone** field.
4. (Optional.) Enter the call waiting on code in the **On Code** field.
5. (Optional.) Enter the call waiting off code in the **Off Code** field.
6. Press the **Save** soft key to accept the change.

Auto Redial

Auto redial allows IP phones to redial a busy number after the first attempt. Both the number of attempts and waiting time between redials are configurable.

Procedure

Auto redial can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure auto redial. For more information, refer to Auto Redial on page 280.
Local	Web User Interface	Configure auto redial. Navigate to: http://<phoneIPAddress>/servlet ?p=features-general&q=load
	Phone User Interface	Configure auto redial.

To configure auto redial via web user interface:

1. Click on **Features->General Information**.
2. Select the desired value from the pull-down list of **Auto Redial**.
3. Enter the desired time interval (in seconds) in the **Auto Redial Interval (1~300s)** field.

The default time interval is 10s.

4. Enter the desired times in the **Auto Redial Times (1~300)** field.

The default times are 10.

The screenshot shows the Yealink T466 web interface. The 'Features' tab is selected, and the 'General Information' sub-tab is active. The 'Auto Redial' section is expanded, showing the following settings:



- Call Waiting: Enabled
- Call Waiting On Code: [Empty]
- Call Waiting Off Code: [Empty]
- Auto Redial: Enabled
- Auto Redial Interval (1~300s): 10
- Auto Redial Times (1~300): 10
- Key As Send: #
- Reserve # in User Name: Enabled
- Hotline Number: 1008
- Hotline Delay(0~10s): 4
- Busy Tone Delay (Seconds): 0
- Return Code When Refuse: 486 (Busy Here)
- Return Code When DND: 480 (Temporarily Not A
- Call Completion: Disabled
- Time-Out for Dial-Now Rule: 1
- RFC 2543 Hold: Disabled

A 'NOTE' box on the right side of the page provides information about 'Call Waiting', 'Key As Send', and 'Hotline Number'.

5. Click **Confirm** to accept the change.

To configure auto redial via phone user interface:

1. Press **Menu->Call Features->Others->Auto Redial**.

2. Press  or , or the **Switch** soft key to select the desired value from the **Auto Redial** field.
3. Enter the desired time in the **Redial Interval** field.
4. Enter the desired times in the **Redial Times** field.
5. Press the **Save** soft key to accept the change.

Auto Answer

Auto answer allows IP phones to automatically answer an incoming call. IP phones will not automatically answer the incoming call during a call even if auto answer is enabled. You can specify a period of delay time before the IP phone automatically answers incoming calls. Auto answer is configurable on a per-line basis.

Procedure

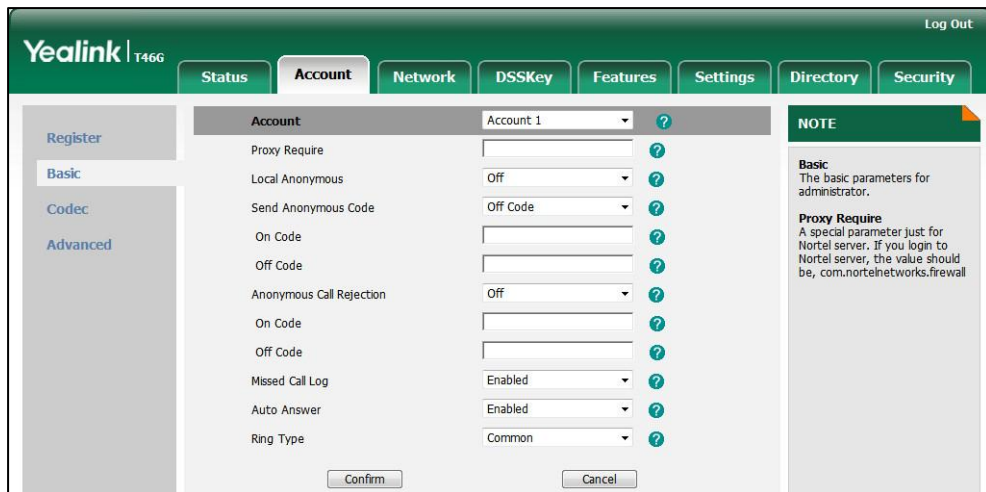
Auto answer can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure auto answer. For more information, refer to Auto Answer on page 281.
	<y0000000000xx>.cfg	Specify a period of delay time for auto answer. For more information, refer to Auto Answer on page 281.
Local	Web User Interface	Configure auto answer. Navigate to: http://<phoneIPAddress>/servlet ?p=account-basic&q=load&acc=0 Specify a period of delay time for auto answer. http://<phoneIPAddress>/servlet ?p=features-general&q=load
	Phone User Interface	Configure auto answer.

To configure auto answer via web user interface:

1. Click on **Account**.
2. Select the desired account from the pull-down list of **Account**.
3. Click on **Basic**.

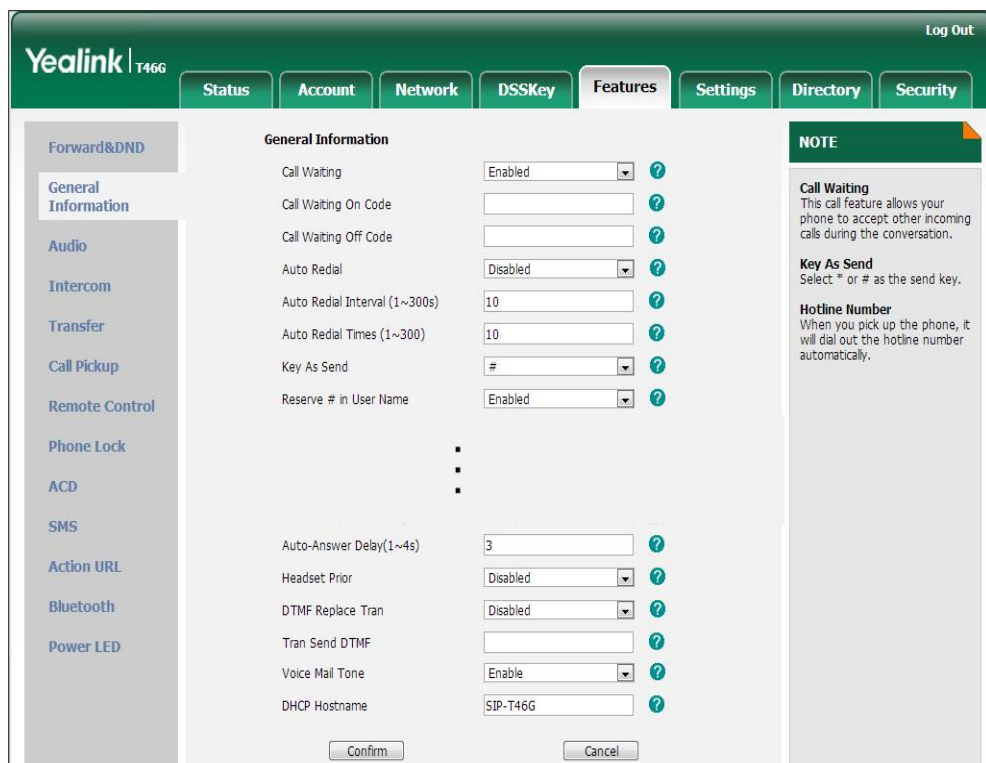
- Select the desired value from the pull-down list of **Auto Answer**.



- Click **Confirm** to accept the change.

To configure a period of delay time for auto answer via web user interface:



- Click on **Features->General Information**.
- Enter the desired time (in seconds) in the **Auto-Answer Delay (1~4s)** field.



- Click **Confirm** to accept the change.

To configure auto answer via phone user interface:

- Press **Menu->Call Features->Auto Answer**.
- Select the desired line and then press the **Enter** soft key.

3. Press  or  , or the **Switch** soft key to select the desired value from the **Auto Answer** field.
4. Press the **Save** soft key to accept the change.

Call Completion

Call completion allows users to monitor the busy party and establish a call when the busy party becomes available to receive a call. Two factors commonly prevent a call from connecting successfully:

- Callee does not answer
- Callee actively rejects the incoming call before answering

IP phones support call completion using the SUBSCRIBE/NOTIFY method, which is specified in draft-poetzl-sipping-call-completion-00, to subscribe to the busy party and receive notifications of their status changes. Call completion is not applicable to SIP-T42G and SIP-T41P IP phones.

Procedure

Call completion can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure call completion. For more information, refer to Call Completion on page 282.
Local	Web User Interface	Configure call completion. Navigate to: http://<phoneIPAddress>/servlet ?p=features-general&q=load
	Phone User Interface	Configure call completion.

To configure call completion via web user interface:

1. Click on **Features->General Information**.

- Select the desired value from the pull-down list of **Call Completion**.

The screenshot shows the Yealink T466 web interface with the 'Features' tab selected. The 'General Information' section contains the following configuration items:

Field	Value
Call Waiting	Enabled
Call Waiting On Code	
Call Waiting Off Code	
Auto Redial	Disabled
Auto Redial Interval (1~300s)	10
Auto Redial Times (1~300)	10
Key As Send	#
Reserve # in User Name	Enabled
Hotline Number	1008
Hotline Delay(0~10s)	4
Busy Tone Delay (Seconds)	0
Return Code When Refuse	486 (Busy Here)
Return Code When DND	480 (Temporarily Not A
Call Completion	Enabled
Time-Out for Dial-Now Rule	1
RFC 2543 Hold	Disabled

NOTE

Call Waiting
This call feature allows your phone to accept other incoming calls during the conversation.

Key As Send
Select * or # as the send key.

Hotline Number
When you pick up the phone, it will dial out the hotline number automatically.

- Click **Confirm** to accept the change.

To configure call completion via phone user interface:

- Press **Menu->Call Features->Others->Call Completion**.
- Press **◀** or **▶**, or the **Switch** soft key to select the desired value from the **Call Completion** field.
- Press the **Save** soft key to accept the change.

Anonymous Call

Anonymous call allows the caller to conceal the identity information displayed on the callee's screen. The callee's phone LCD screen prompts an incoming call from anonymity.

Example of anonymous SIP header:

```
Via: SIP/2.0/UDP 10.2.8.183:5063;branch=z9hG4bK1535948896
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=128043702
To: <sip:1011@10.2.1.199>
Call-ID: 1773251036@10.2.8.183
CSeq: 1 INVITE
Contact: <sip:1012@10.2.8.183:5063>
Content-Type: application/sdp
Allow: INVITE, INFO, PRACK, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REGISTER, SUBSCRIBE, REFER, PUBLISH, UPDATE, MESSAGE
```

```

Max-Forwards: 70
User-Agent: Yealink SIP-T46G 28.72.0.1
Privacy: id
Supported: replaces
Allow-Events: talk,hold,conference,refer,check-sync
P-Preferred-Identity: <sip:1012@10.2.1.199>
Content-Length: 302
    
```

The anonymous call on code and anonymous call off code configured on IP phones are used to activate/deactivate the server-side anonymous call feature. They may vary on different servers. Send Anonymous Code allows IP phones to send anonymous call on/off code to the server.

Procedure

Anonymous call can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure anonymous call. For more information, refer to Anonymous Call on page 282.
Local	Web User Interface	Configure anonymous call. Navigate to: http://<phoneIPAddress>/servlet ?p=account-basic&q=load&acc=0
	Phone User Interface	Configure anonymous call.

To configure the anonymous call via web user interface:

1. Click on **Account**.
2. Select the desired account from the pull-down list of **Account**.
3. Click on **Basic**.
4. Select the desired value from the pull-down list of **Local Anonymous**.
5. Select the desired value from the pull-down list of **Send Anonymous Code**.
6. (Optional.) Enter the anonymous call on code in the **On Code** field.

- (Optional.) Enter the anonymous call off code in the **Off Code** field.

The screenshot shows the Yealink T466 web interface. The top navigation bar includes 'Status', 'Account', 'Network', 'DSSKey', 'Features', 'Settings', 'Directory', and 'Security'. The 'Account' tab is selected, and the 'Basic' sub-tab is active. The 'Off Code' field is highlighted, showing the value '*72'. Other fields include Proxy Require, Local Anonymous, Send Anonymous Code, On Code, Anonymous Call Rejection, Missed Call Log, Auto Answer, and Ring Type. A 'NOTE' section on the right provides information about Proxy Require.

- Click **Confirm** to accept the change.

To configure the anonymous call via phone user interface:

- Press **Menu->Call Features->Anonymous**.
- Select the desired line and then press **Enter** soft key.
- Press **◀** or **▶**, or the **Switch** soft key to select the desired value from the **Local Anonymous** field.
- (Optional.) Press **◀** or **▶**, or the **Switch** soft key to select the desired value from the **Send Anonymous Code** field.
- (Optional.) Enter the anonymous call on code in the **On Code** field.
- (Optional.) Enter the anonymous call off code in the **Off Code** field.
- Press the **Save** soft key to accept the change.

Anonymous Call Rejection

Anonymous call rejection allows IP phones to automatically reject incoming calls from callers whose identity has been deliberately concealed. The anonymous caller's LCD screen presents "Anonymity Disallowed".

The anonymous call rejection on code and anonymous call rejection off code configured on IP phones are used to activate/deactivate the server-side anonymous call rejection feature. They may vary on different servers.

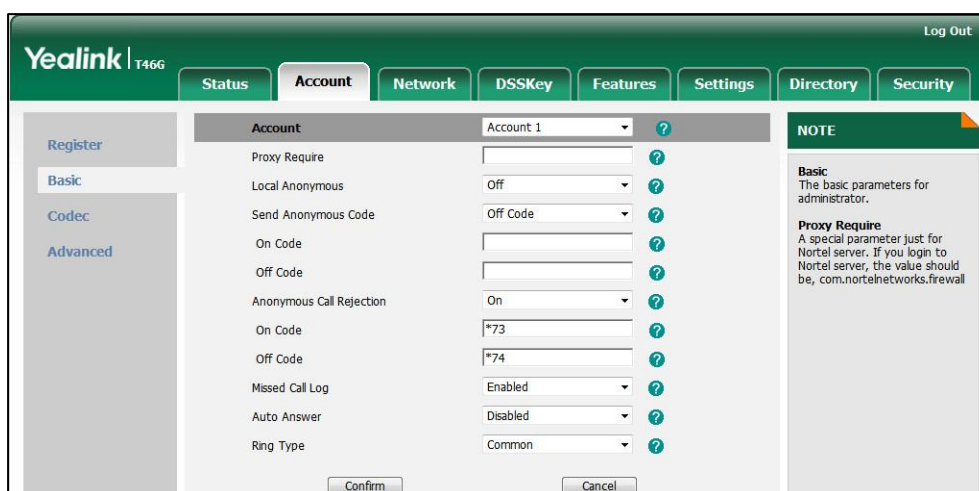
Procedure

Anonymous call rejection can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure anonymous call rejection. For more information, refer to Anonymous Call Rejection on page 284.
Local	Web User Interface	Configure anonymous call rejection. Navigate to: http://<phoneIPAddress>/servlet?p=account-basic&q=load&acc=0
	Phone User Interface	Configure anonymous call rejection.

To configure anonymous call rejection via web user interface:



1. Click on **Account**.
2. Select the desired account from the pull-down list of **Account**.
3. Click on **Basic**.
4. Select the desired value from the pull-down list of **Anonymous Call Rejection**.
5. (Optional.) Enter the anonymous call rejection on code in the **On Code** field.
6. (Optional.) Enter the anonymous call rejection off code in the **Off Code** field.



7. Click **Confirm** to accept the change.

To configure anonymous call rejection via phone user interface:

1. Press **Menu->Call Features->Anonymous**.

2. Select the desired line and then press **Enter** soft key.
3. Press  or  , or the **Switch** soft key to select the desired value from the **Anonymous Rejection** field.
4. (Optional.) Enter the anonymous call rejection on code in the **On Code** field.
5. (Optional.) Enter the anonymous call rejection off code in the **Off Code** field.
6. Press the **Save** soft key to accept the change.

Do Not Disturb

Do Not Disturb (DND) allows IP phones to ignore incoming calls. DND can be configured on a phone or per-line basis depending on the DND mode. Two DND modes:

- **Phone** (default): DND feature is effective for all accounts on the IP phone.
- **Custom**: DND feature can be configured for each or all accounts.

A user can activate or deactivate DND using the DND soft key or DND key. DND activated on IP phones disables the local call forward settings. The DND configurations on IP phones may be overridden by the server settings.

The DND on code and DND off code configured on IP phones are used to activate/deactivate the server-side DND feature. They may vary on different servers.

Return Message When DND

This feature defines the return code and the reason of the SIP response message for the rejected incoming call when DND is enabled on IP phones. The caller's LCD screen displays the received reason.

Procedure

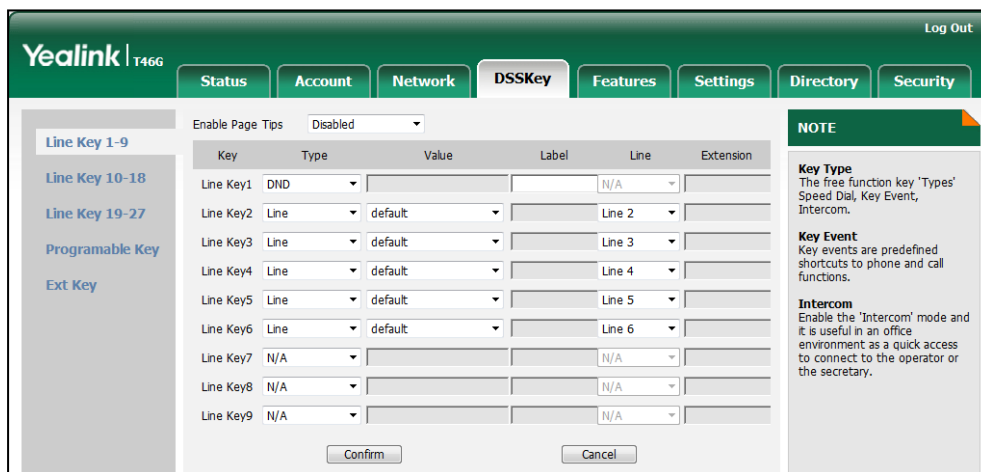
DND can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure DND in the custom mode. For more information, refer to Do Not Disturb on page 286.
	<y0000000000xx>.cfg	Assign a DND key. For more information, refer to DND Key on page 386. Configure the DND mode. Configure DND in the phone mode. Specify return code and reason of the SIP response message. For more information, refer to Do

		Not Disturb on page 286.
Local	Web User Interface	<p>Assign a DND key.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet? p=dsskey&model=1&q=load&line page=1</p> <p>Configure DND.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet? p=features-forward&q=load</p> <p>Specify return code and reason of the SIP response message.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet? p=features-general&q=load</p>
	Phone User Interface	<p>Assign a DND key.</p> <p>Configure DND.</p>

To configure a DND key via web user interface:

1. Click on **DSSKey->Line Key**.
2. In the desired DSS key field, select **DND** from the pull-down list of **Type**.



3. Click **Confirm** to accept the change.

To configure the DND feature via web user interface:

1. Click on **Features->Forward & DND**.
2. In the **DND** block, mark the desired radio box in the **Mode** field.
 - a) If you mark the **Phone** radio box:
 - 1) Mark the desired radio box in the **DND Status** field.

- 2) (Optional.) Enter the DND on code in the **DND On Code** field.
- 3) (Optional.) Enter the DND off code in the **DND Off Code** field.

The screenshot displays the Yealink T46G web interface for configuring Forward and DND features. The 'Forward' section is currently selected, showing the following configuration options:

- Mode:** Radio buttons for Phone and Custom.
- Account:** A dropdown menu showing '1005'.
- Always Forward:** Radio buttons for On and Off.
- Target:** An empty text input field.
- On Code:** An empty text input field.
- Off Code:** An empty text input field.

The 'DND' section is also visible below, with the following configuration options:

- DND Emergency:** A dropdown menu showing 'Disabled'.
- DND Authorized Numbers:** An empty text input field.
- Mode:** Radio buttons for Phone and Custom.
- Account:** A dropdown menu showing '1005'.
- DND Status:** Radio buttons for On and Off.
- DND On Code:** An empty text input field.
- DND Off Code:** An empty text input field.

A 'NOTE' box on the right side of the page provides the following information:

Forward
This feature allows you to forward an incoming call to another phone number.

Target
The number to which the incoming calls will be forwarded.

On Code
The code that will be sent to PBX when it is switched On.

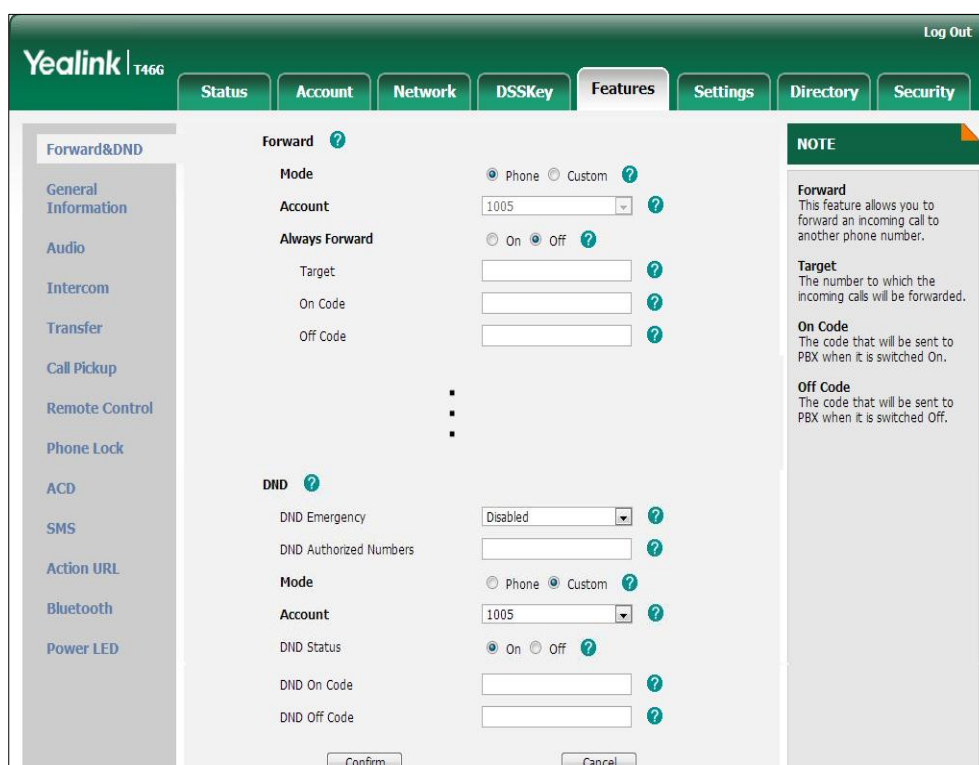
Off Code
The code that will be sent to PBX when it is switched Off.

At the bottom of the configuration area, there are 'Confirm' and 'Cancel' buttons.

b) If you mark the **Custom** radio box:

- 1) Select the desired account from the pull-down list of **Account**.
- 2) Mark the desired value in the **DND Status** field.
- 3) (Optional.) Enter the DND on code in the **DND On Code** field.

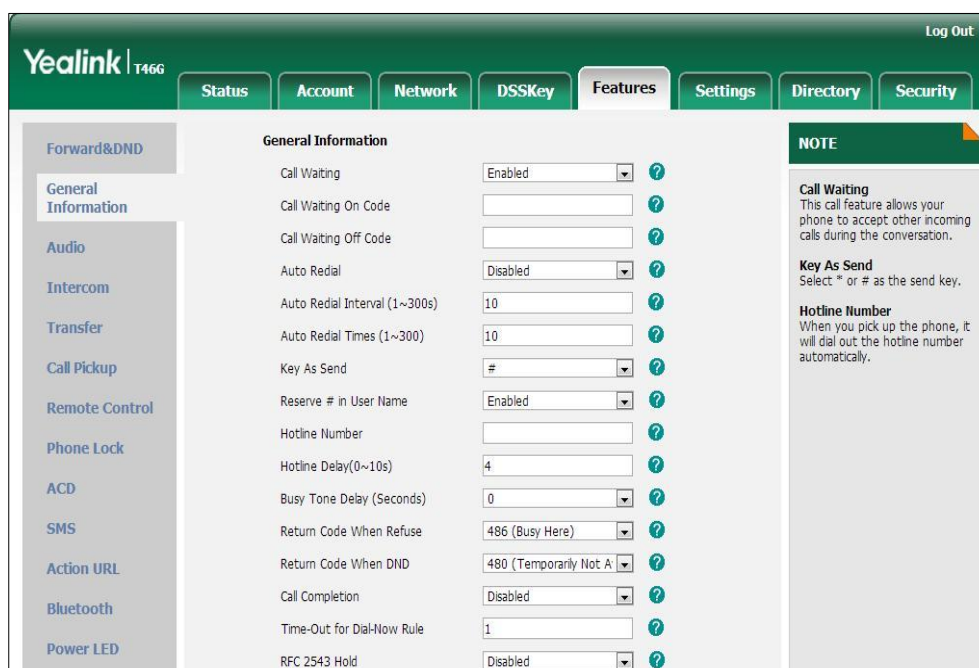
4) (Optional.) Enter the DND off code in the **DND Off Code** field.



3. Click **Confirm** to accept the change.





To specify the return code via web user interface:

1. Click on **Features->General Information**.
2. Select the desired type from the pull-down list of **Return Code When DND**.



- Click **Confirm** to accept the change.





To configure a DND key via phone user interface:

- Press **Menu->Call Features->DSS Keys**.
- Select the desired DSS key.
- Press  or  , or the **Switch** soft key to select **Key Event** from the **Type** field.
- Press  or  , or the **Switch** soft key to select **DND** from the **Key Event** field.
- (Optional.) Enter the string that will appear on the LCD screen in the **Label** field.
- Press the **Save** soft key to accept the change.

To configure DND in the phone mode via phone user interface:

- Press the **DND** soft key or the DND key when the IP phone is idle.

To configure DND in the custom mode for a specific account via phone user interface:

- Press the **DND** soft key or the DND key when the IP phone is idle.
The LCD screen displays a list of the accounts registered on the IP phone.
- Press  or  to select the desired account.
- Press  or  to select **On** to activate DND.
- Press the **Save** soft key to accept the change.

To configure DND in the custom mode for all accounts via phone user interface:

- Press the **DND** soft key or the DND key when the IP phone is idle.
The LCD screen displays a list of the accounts registered on the IP phone.
- Press the **All On** soft key to activate DND for all accounts.
- Press the **Save** soft key to accept the change.

Busy Tone Delay

Busy tone is audible to the other party, indicating that the call connection has been broken when one party releases a call. Busy tone delay can define a period of time during which the busy tone is audible.

Procedure

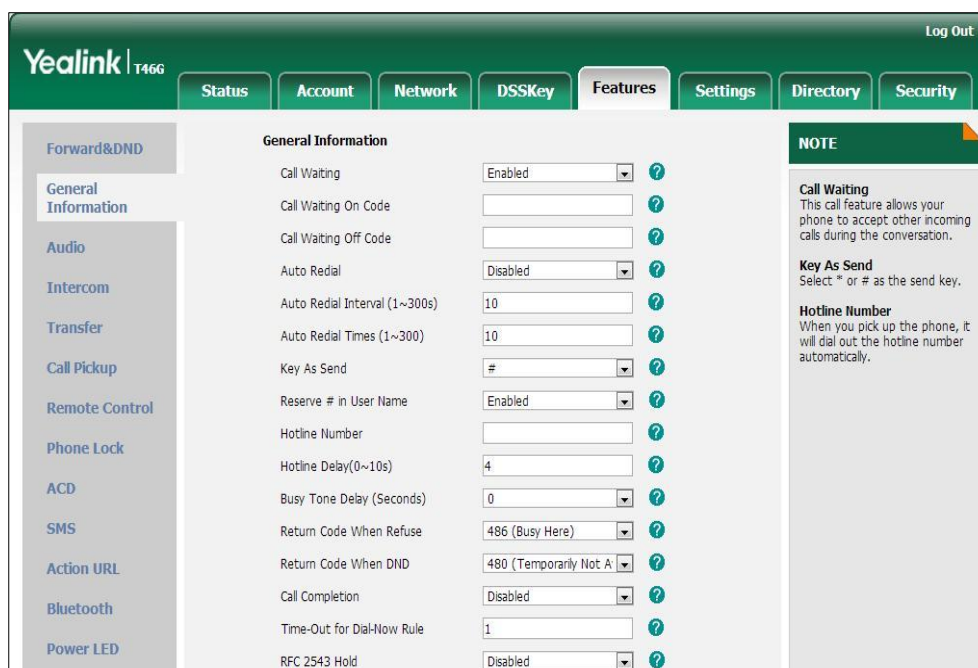
Busy tone delay can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure the busy tone delay feature. For more information, refer to Busy Tone Delay on page 279.
Local	Web User Interface	Configure the busy tone delay feature.

		<p>Navigate to: <a href="http://<phoneIPAddress>/servlet?p=features-general&q=load">http://<phoneIPAddress>/servlet?p=features-general&q=load</p>
--	--	---

To configure busy tone delay via web user interface:

1. Click on **Features->General Information**.
2. Select the desired value from the pull-down list of **Busy Tone Delay (Seconds)**.



3. Click **Confirm** to accept the change.

Return Code When Refuse

Return code when refuse defines the return code and reason of the SIP response message for call rejection. The caller's LCD screen displays the reason according to the return code received. Available return codes and reasons are:

- 404 (Not found)
- 480 (Temporarily not available)
- 486 (Busy here)

Procedure

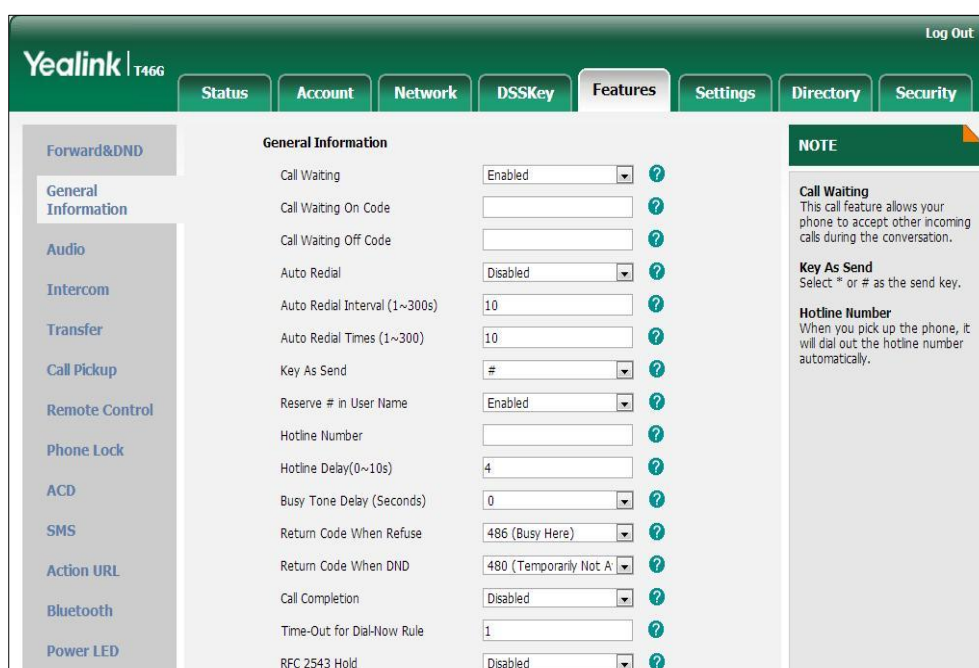
Return code for call rejection can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	<p>Configure the return code when refusing a call.</p> <p>For more information, refer to</p>
---------------------------	---------------------	--

		Return Code When Refuse on page 289.
Local	Web User Interface	Configure the return code when refusing a call. Navigate to: http://<phoneIPAddress>/servlet?p=features-general&q=load

To specify the return code when refusing a call via web user interface:

1. Click on **Features->General Information**.
2. Select the desired value from the pull-down list of **Return Code When Refuse**.



3. Click **Confirm** to accept the change.

Early Media

Early media refers to media (e.g., audio and video) played to the caller before a SIP call is actually established. Current implementation supports early media through the 183 message. When the caller receives a 183 message with SDP before the call is established, a media channel is established. This channel is used to provide the early media stream for the caller.

180 Ring Workaround

180 ring workaround defines whether to deal with the 180 message received after the 183 message. When the caller receives a 183 message, it suppresses any local ringback tone and begins to play the media received. 180 ring workaround allows IP phones to resume and play the local ringback tone upon a subsequent 180 message received.

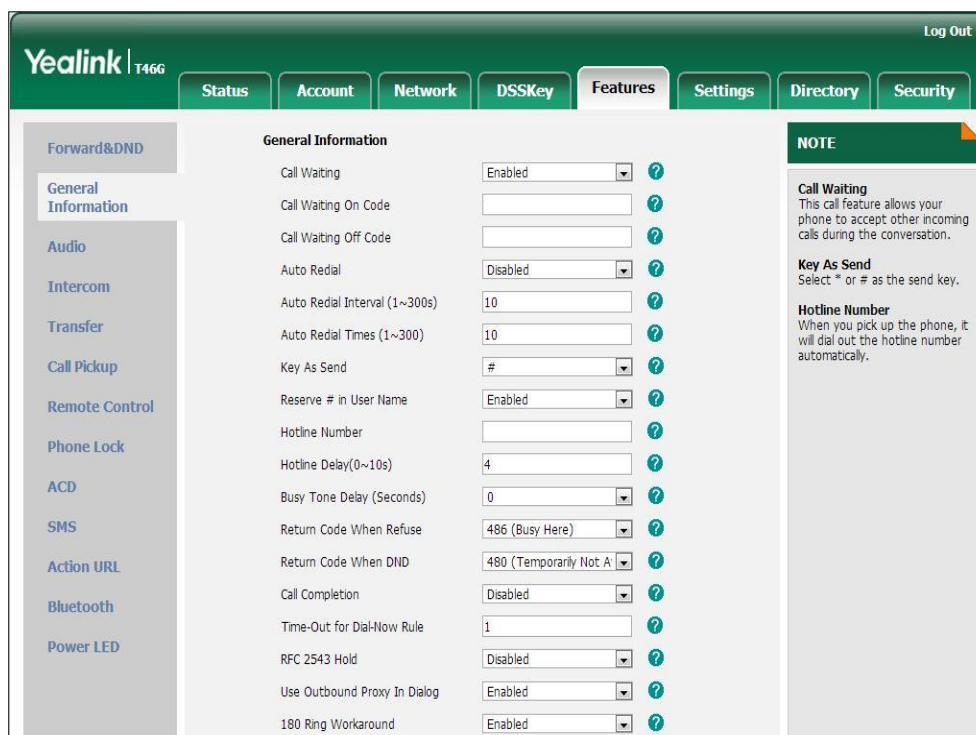
Procedure

180 ring workaround can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure 180 ring workaround. For more information, refer to 180 Ring Workaround on page 290.
Local	Web User Interface	Configure 180 ring workaround. Navigate to: http://<phoneIPAddress>/servlet ?p=features-general&q=load

To configure 180 ring workaround via web user interface:

1. Click on **Features->General Information**.
2. Select the desired value from the pull-down list of **180 Ring Workaround**.



3. Click **Confirm** to accept the change.

Use Outbound Proxy in Dialog

An outbound proxy server can receive all initiating request messages and route them to the designated destination. If the IP phone is configured to use an outbound proxy server within a dialog, all SIP request messages from the IP phone will be sent to the outbound proxy server forcefully.

Note

To use this feature, make sure the outbound server has been correctly configured on the IP phone.

Procedure

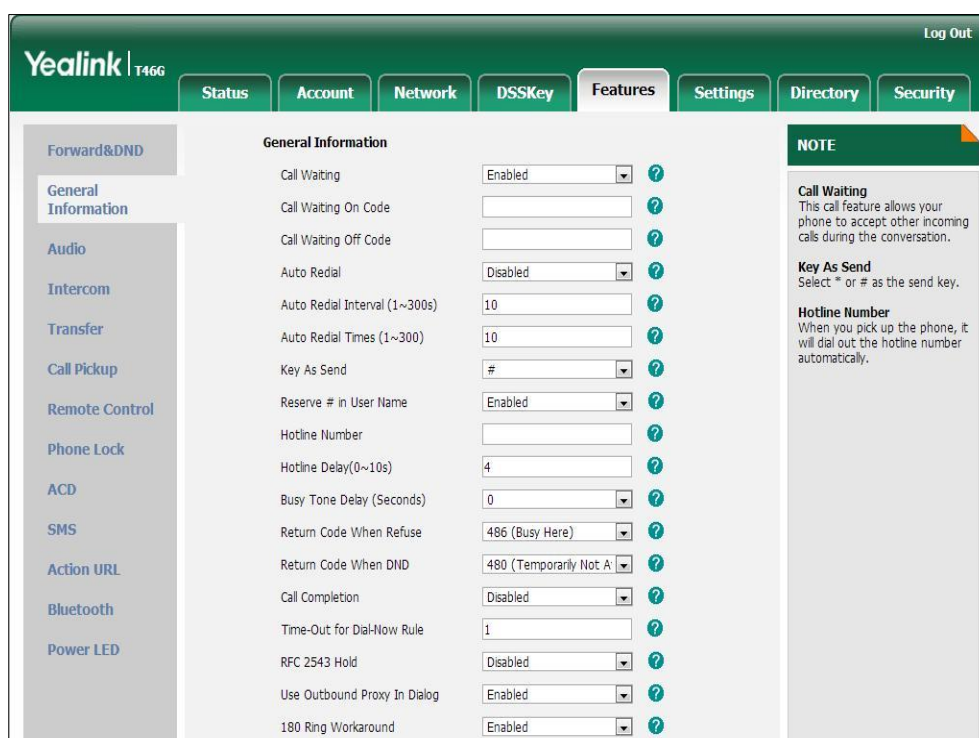
Use outbound proxy in dialog can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Specify whether to use outbound proxy in a dialog. For more information, refer to Use Outbound Proxy in Dialog on page 290.
Local	Web User Interface	Specify whether to use outbound proxy in a dialog. Navigate to: http://<phoneIPAddress>/servlet?p=features-general&q=load

To specify whether to use outbound proxy server in a dialog via web user interface:

1. Click on **Features->General Information**.

2. Select the desired value from the pull-down list of **Use Outbound Proxy In Dialog**.



3. Click **Confirm** to accept the change.

SIP Session Timer

SIP session timers T1, T2 and T4 are SIP transaction layer timers defined in RFC 3261. Timer T1 is an estimate of the Round Trip Time (RTT) of transactions between a SIP client and SIP server. Timer T2 represents the maximum retransmitting time of any SIP request message. The re-transmitting and doubling of T1 will continue until the retransmitting time reaches the T2 value. Timer T4 represents the time the network will take to clear messages between the SIP client and server. These session timers are configurable on IP phones.

Procedure

SIP session timer can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure SIP session timer. For more information, refer to SIP Session Timer on page 291.
Local	Web User Interface	Configure SIP session timer. Navigate to: http://<phoneIPAddress>/servlet ?p=account-adv&q=load&acc=0

To configure session timer via web user interface:

1. Click on **Account**.
2. Select the desired account from the pull-down list of **Account**.
3. Click on **Advanced**.
4. Enter the desired value in the **SIP Session Timer T1 (0.5~10s)** field.
The default value is 0.5s.
5. Enter the desired value in the **SIP Session Timer T2 (2~40s)** field.
The default value is 4s.
6. Enter the desired value in the **SIP Session Timer T4 (2.5~60s)** field.
The default value is 5s.

The screenshot shows the Yealink T466 web interface. The top navigation bar includes 'Status', 'Account', 'Network', 'DSSKey', 'Features', 'Settings', 'Directory', and 'Security'. The 'Account' tab is active, and the 'Advanced' sub-tab is selected. The configuration table is as follows:

Parameter	Value	Help
Account	Account 1	
Keep Alive Type	Default	?
Keep Alive Interval (Seconds)	30	
Local SIP Port	5062	?
RPort	Disabled	?
SIP Session Timer T1 (0.5~10s)	0.5	?
SIP Session Timer T2 (2~40s)	4	
SIP Session Timer T4 (2.5~60s)	5	
Subscribe Period (Seconds)	1800	?
DTMF Type	RFC2833	?
DTMF Info Type	DTMF-Relay	
DTMF Payload Type(96~255)	101	
Retransmission	Disabled	?
Subscribe for MWI	Disabled	?
MWI Subscription Period(Seconds)	3600	
Subscribe MWI To Voice Mail	Disabled	

A 'NOTE' box on the right states: 'Advanced: The Advanced parameters for administrator.'

7. Click **Confirm** to accept the change.

Session Timer

Session timer allows a periodic refresh of SIP sessions through a re-INVITE request, to determine whether a SIP session is still active. Session timer is specified in RFC 4028. IP phones support two refresher modes: UAC and UAS. The UAC mode means refreshing the session from the client, while the UAS mode means refreshing the session from the server. The session expiration and session refresher are negotiated via the Session-Expires header in the INVITE message. The negotiated refresher will send a re-INVITE request at or before the negotiated session expiration.

Procedure

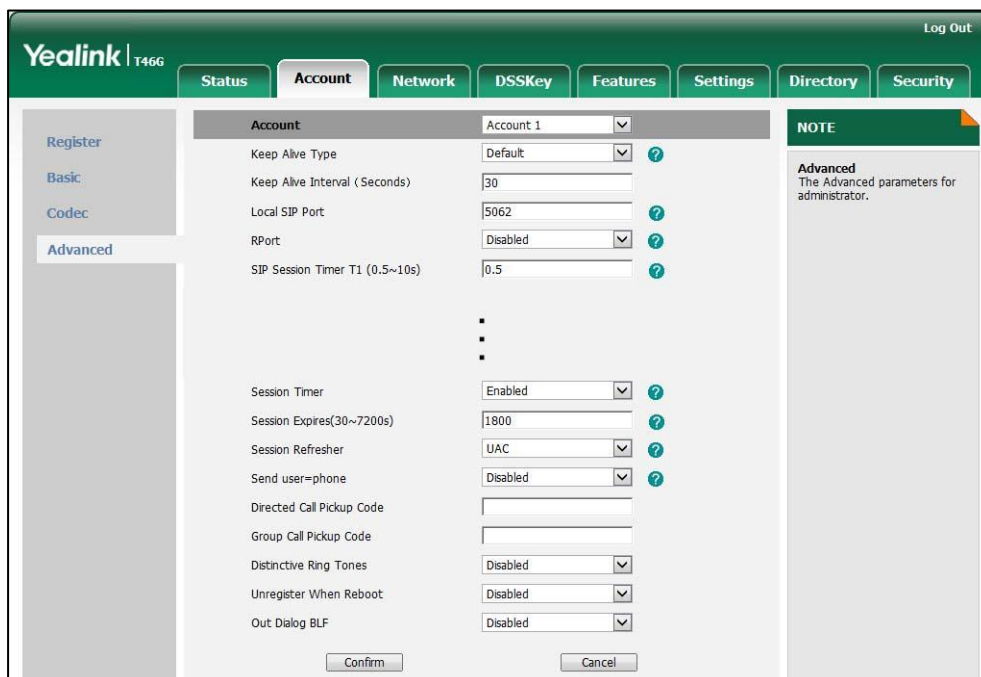
Session timer can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure session timer. For more information, refer to
---------------------------	-----------	--

		Session Timer on page 292.
Local	Web User Interface	Configure session timer. Navigate to: http://<phoneIPAddress>/servlet ?p=account-adv&q=load&acc= 0

To configure session timer via web user interface:

1. Click on **Account**.
2. Select the desired account from the pull-down list of **Account**.
3. Click on **Advanced**.
4. Select the desired value from the pull-down list of **Session Timer**.
5. Enter the desired time interval in the **Session Expires (30~7200s)** field.
6. Select the desired refresher from the pull-down list of **Session Refresher**.



7. Click **Confirm** to accept the change.

Call Hold

Call hold provides a service of putting an active call on hold. When a call is placed on hold, the IP phone sends an INVITE request with a HOLD SDP to the server. IP phones support two call hold methods, one is RFC 3264, which sets the "a" (media attribute) in the SDP to sendonly, recvonly or inactive (e.g., a=sendonly). The other is RFC 2543, which sets the "c" (connection addresses for the media streams) in the SDP to zero (e.g., c=0.0.0.0). The call hold tone feature allows IP phones to play a hold tone at regular

intervals when there is a call on hold.

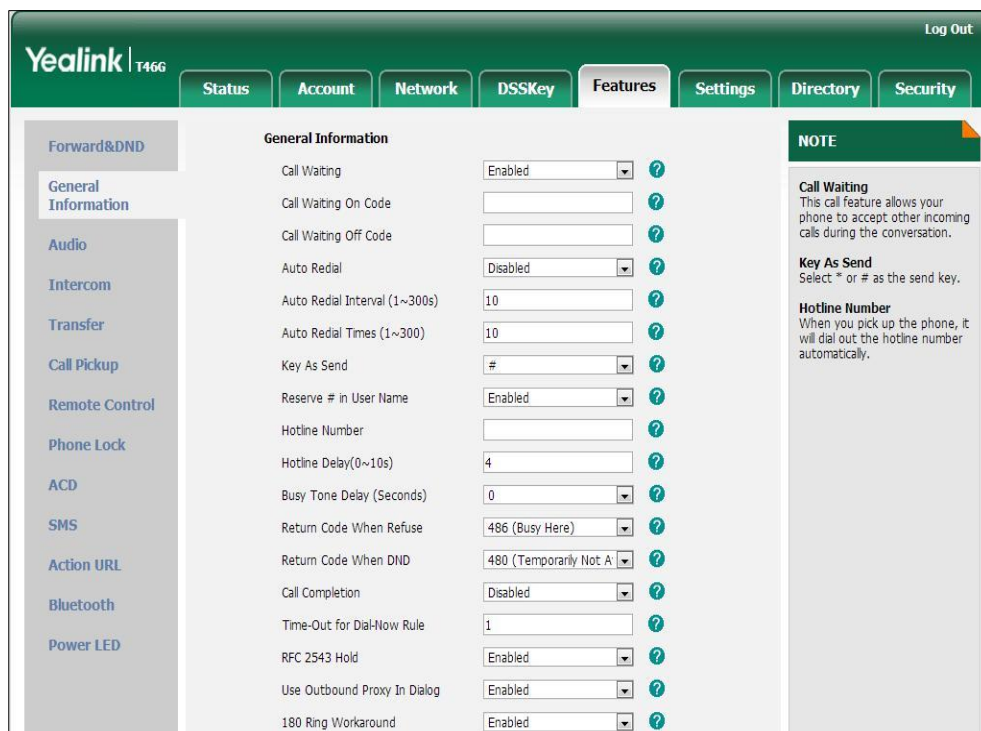
Procedure

Call hold can be configured using the configuration files or locally.

<p>Configuration File</p>	<p><y0000000000xx>.cfg</p>	<p>Configure the call hold tone and call hold tone delay.</p> <p>Specify whether RFC 2543 (c=0.0.0.0) outgoing hold signaling is used.</p> <p>For more information, refer to Call Hold on page 293.</p>
<p>Local</p>	<p>Web User Interface</p>	<p>Configure the call hold tone and call hold tone delay.</p> <p>Specify whether RFC 2543 (c=0.0.0.0) outgoing hold signaling is used.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet?p=features-general&q=load</p>

To configure call hold method via web user interface:

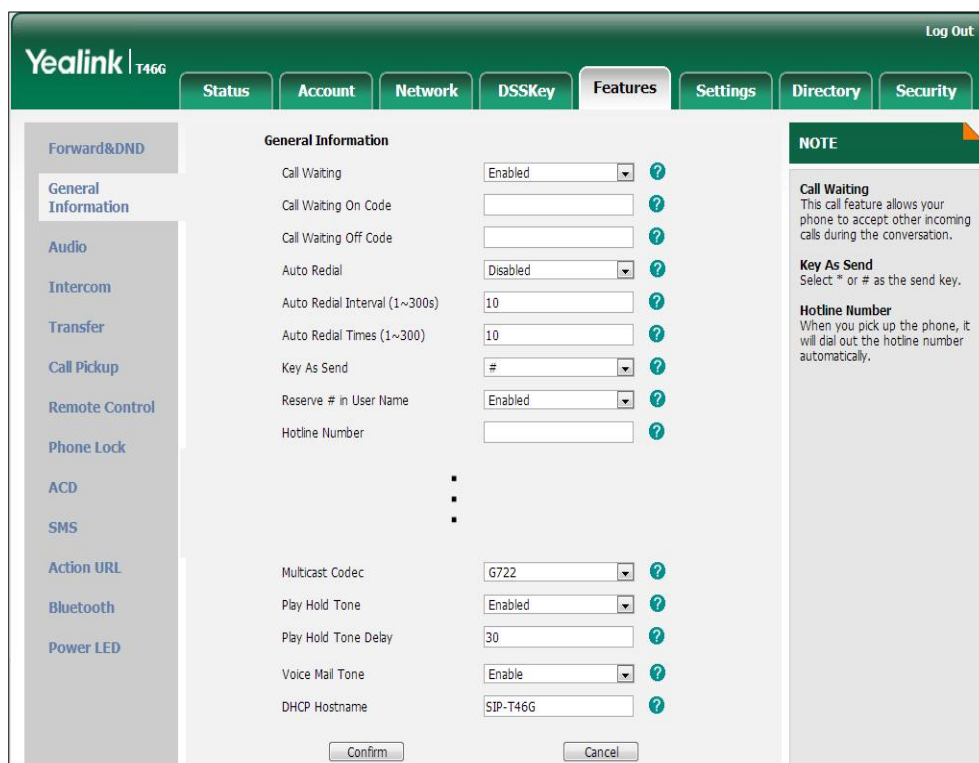
1. Click on **Features->General Information**.
2. Select the desired value from the pull-down list of **RFC 2543 Hold**.



3. Click **Confirm** to accept the change.

To configure call hold tone and call hold tone delay via web user interface:

1. Click on **Features->General Information**.
2. Select the desired value from the pull-down list of **Play Hold Tone**.
3. Enter the desired time in the **Play Hold Tone Delay** field.



4. Click **Confirm** to accept the change.

Call Forward

Call forward allows users to redirect an incoming call to a third party. IP phones redirect an incoming INVITE message by responding with a 302 Moved Temporarily message, which contains a Contact header with a new URI that should be tried. Three types of call forward:

- **Always Forward** -- Forward the incoming calls immediately.
- **Busy Forward** -- Forward the incoming call when the callee is busy.
- **No Answer Forward** -- Forward the incoming call after a period of ring time.

Call forward can be configured on a phone or per-line depending on the call forward mode. The following describes the call forward modes:

- **Phone** (default): Call forward feature is effective for all accounts on the IP phone.
- **Custom**: Call forward feature can be configured for each or all accounts.

The call forward on code and call forward off code configured on IP phones are used to activate/deactivate the server-side call forward feature. They may vary on different servers.

Forward International

Forward international allows users to forward an incoming call to an international telephone number. This feature is enabled by default.

Procedure

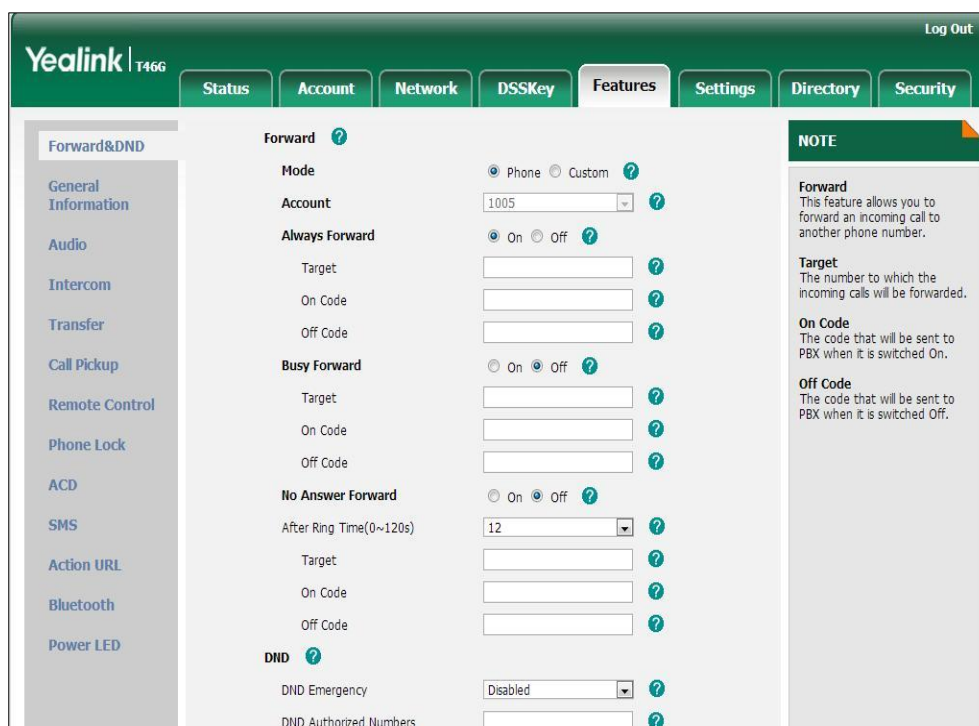
Call forward can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure call forward in custom mode. For more information, refer to Call Forward on page 294.
	<y0000000000xx>.cfg	Configure the call forward mode. Configure call forward in phone mode. Configure forward international. For more information, refer to Call Forward on page 294.
Local	Web User Interface	Configure call forward. Navigate to: http://<phoneIPAddress>/servlet?p=features-forward&q=load Configure forward international. Navigate to: http://<phoneIPAddress>/servlet?p=features-general&q=load
	Phone User Interface	Configure call forward.

To configure call forward via web user interface:

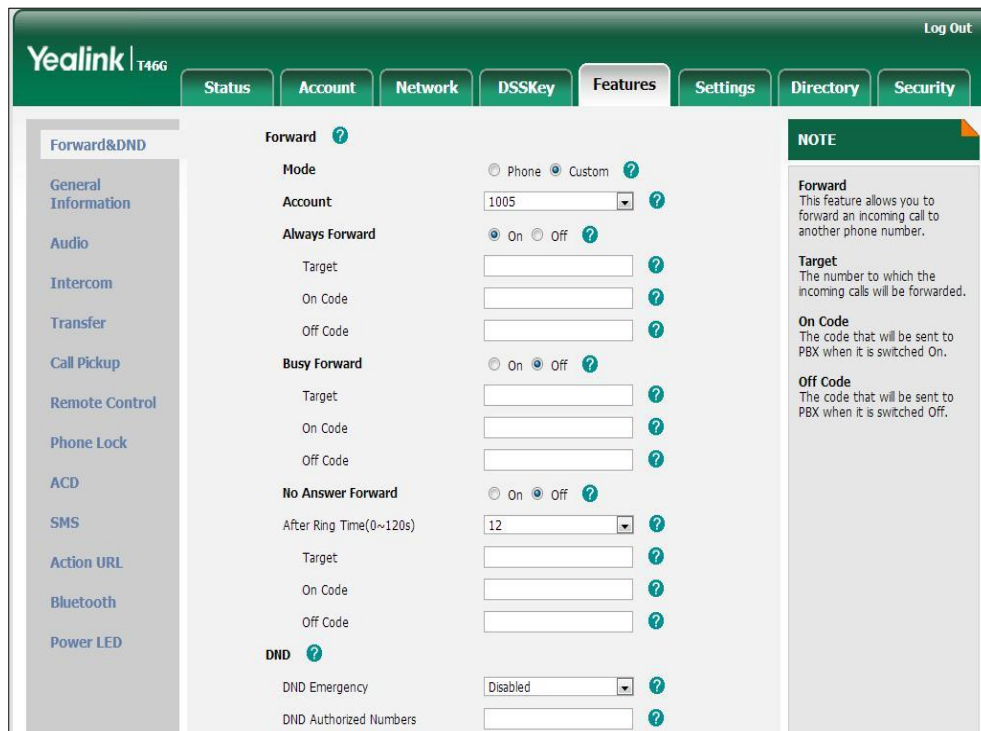
1. Click on **Features->Forward & DND**.

2. In the **Forward** block, mark the desired radio box in the **Mode** field.
 - a) If you mark the **Phone** radio box:
 - 1) Mark the desired radio box in the **Always Forward/Busy Forward/No Answer Forward** field.
 - 2) Enter the destination number you want to forward in the **Target** field.
 - 3) (Optional.) Enter the on code and off code in the **On Code** and **Off Code** fields.
 - 4) Select the ring time to wait before forwarding from the pull-down list of **After Ring Time (0~120s)** (only for the no answer forward).



- b) If you mark the **Custom** radio box:
 - 1) Select the desired account from the pull-down list of **Account**.
 - 2) Mark the desired radio box in the **Always Forward/Busy Forward/No Answer Forward** field.
 - 2) Enter the destination number you want to forward in the **Target** field.
 - 3) (Optional.) Enter the on code and off code in the **On Code** and **Off Code** fields.

- 4) Select the ring time to wait before forwarding from the pull-down list of **After Ring Time (0~120s)** (only for no answer forward).

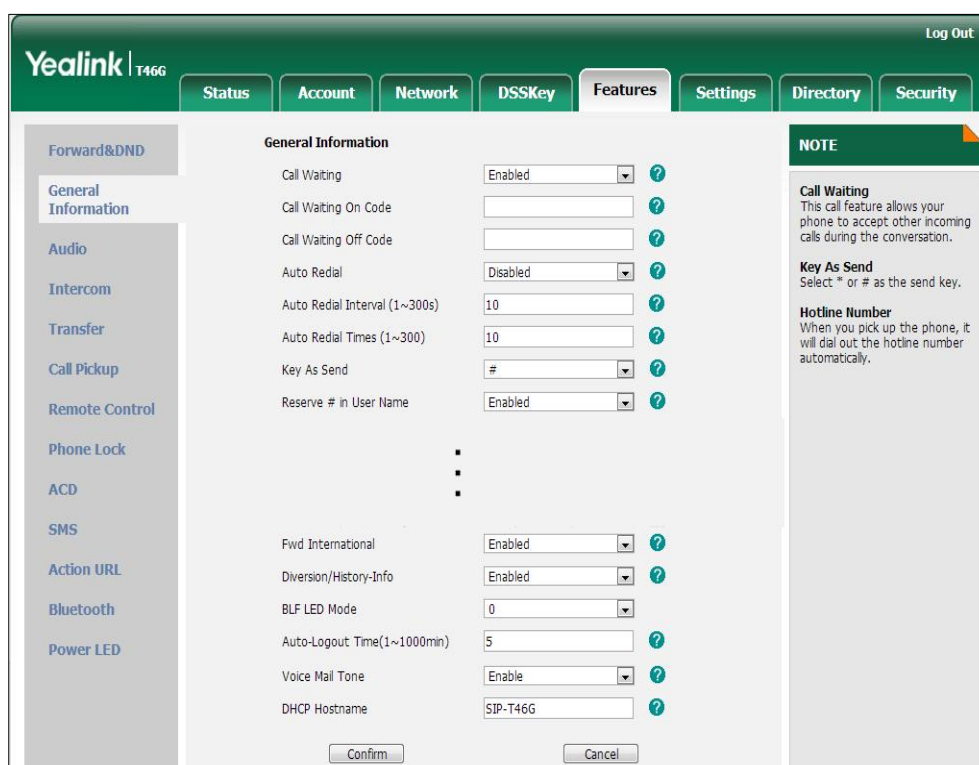


3. Click **Confirm** to accept the change.

To configure the forward international feature via web user interface:

1. Click on **Features->General Information**.

2. Select the desired value from the pull-down list of **Fwd International**.







3. Click **Confirm** to accept the change.

To configure call forward in phone mode via phone user interface:







1. Press **Menu->Call Features->Call Forward**.
2. Press **▲** or **▼** to select the desired forwarding type, and then press the **Enter** soft key.
3. Depending on your selection:
 - a) If you select **Always Forward**:
 - 1) Press **◀** or **▶**, or the **Switch** soft key to select the desired value from the **Always Forward** field.
 - 2) Enter the destination number you want to forward all incoming calls to in the **Forward To** field.
 - 3) (Optional.) Enter the always forward on code and off code respectively in the **On Code** and **Off Code** fields.
 - b) If you select **Busy Forward**:
 - 1) Press **◀** or **▶**, or the **Switch** soft key to select the desired value from the **Busy Forward** field.
 - 2) Enter the destination number you want to forward all incoming calls to when the IP phone is busy in the **Forward To** field.
 - 3) (Optional.) Enter the busy forward on code and off code respectively in the **On Code** and **Off Code** fields.

c) If you select **No Answer Forward**:



- 1) Press  or  , or the **Switch** soft key to select the desired value from the **No Answer Forward** field.
- 2) Enter the destination number you want to forward all unanswered incoming calls to in the **Forward To** field.
- 3) Press  or  , or the **Switch** soft key to select the ring time to wait before forwarding from the **After Ring Time** field.
The default ring time is 12 seconds.
- 4) (Optional.) Enter the no answer forward on code and off code respectively in the **On Code** and **Off Code** fields.

4. Press the **Save** soft key to accept the change.



To configure call forward in custom mode via phone user interface:

1. Press **Menu->Call Features->Call Forward**.
2. Press  or  to select the desired account, and then press the **Enter** soft key.
3. Press  or  to select the desired forwarding type, and then press the **Enter** soft key.
4. Depending on your selection:
 - a) If you select **Always Forward**, you can configure it for a specific account.
 - 1) Press  or  , or the **Switch** soft key to select the desired value from the **Always Forward** field.
 - 2) Enter the destination number you want to forward all incoming calls to in the **Forward To** field.
 - 3) (Optional.) Enter the always forward on code and off code respectively in the **On Code** and **Off Code** fields.







You can also configure the always forward for all accounts. After the always forward was configured for a specific account, do the following:

- 1) Press  or  to highlight the **Always Forward** field.
- 2) Press the **All Lines** soft key.
The LCD screen prompts "Copy to all lines?".
- 3) Press the **OK** soft key to accept the change.



b) If you select **Busy Forward**, you can configure it for a specific account.

- 1) Press  or  , or the **Switch** soft key to select the desired value from the **Busy Forward** field.
- 2) Enter the destination number you want to forward all incoming calls to when the IP phone is busy in the **Forward To** field.
- 3) (Optional.) Enter the busy forward on code and off code respectively in the **On Code** and **Off Code** fields.

You can also configure the busy forward for all accounts. After the busy forward was configured for a specific account, do the following:

- 1) Press  or  to highlight the **Busy Forward** field.
 - 2) Press the **All Lines** soft key.
The LCD screen prompts "Copy to all lines?".
 - 3) Press the **OK** soft key to accept the change.
- c) If you select **No Answer Forward**, you can configure it for a specific account.
- 1) Press  or , or the **Switch** soft key to select the desired value from the **No Answer Forward** field.
 - 2) Enter the destination number you want to forward all unanswered incoming calls to in the **Forward To** field.
 - 3) Press  or , or the **Switch** soft key to select the ring time to wait before forwarding from the **After Ring Time** field
The default ring time is 12 seconds.
 - 4) (Optional.) Enter the no answer forward on code and off code respectively in the **On Code** and **Off Code** fields.

You can also configure the no answer forward for all accounts. After the no answer forward was configured for a specific account, do the following:

- 1) Press  or  to highlight the **No Answer Forward** field.
 - 2) Press the **All Lines** soft key.
The LCD screen prompts "Copy to all lines?".
 - 3) Press the **OK** soft key to accept the change.
5. Press the **Save** soft key to accept the change.

Call Transfer

Call transfer enables IP phones to transfer an existing call to another party. IP phones support call transfer using the REFER method specified in RFC 3515 and offer three types of transfer:

- **Blind Transfer** -- Transfer a call directly to another party without consulting. Blind transfer is implemented by a simple REFER method without Replaces in the Refer-To header.
- **Semi-attended Transfer** -- Transfer a call after hearing the ringback tone. Semi-attended transfer is implemented by a REFER method with Replaces in the Refer-To header.
- **Attended Transfer** -- Transfer a call with prior consulting. Attended transfer is implemented by a REFER method with Replaces in the Refer-To header.

Normally, call transfer is completed by pressing the transfer key. The blind transfer on hook and attended transfer on hook features allow the IP phone to complete the

transfer through on-hook.

When a user performs a semi-attended transfer, semi-attended transfer determines whether to display the prompt “1 New Missed Call(s)” on the destination party’s LCD screen.

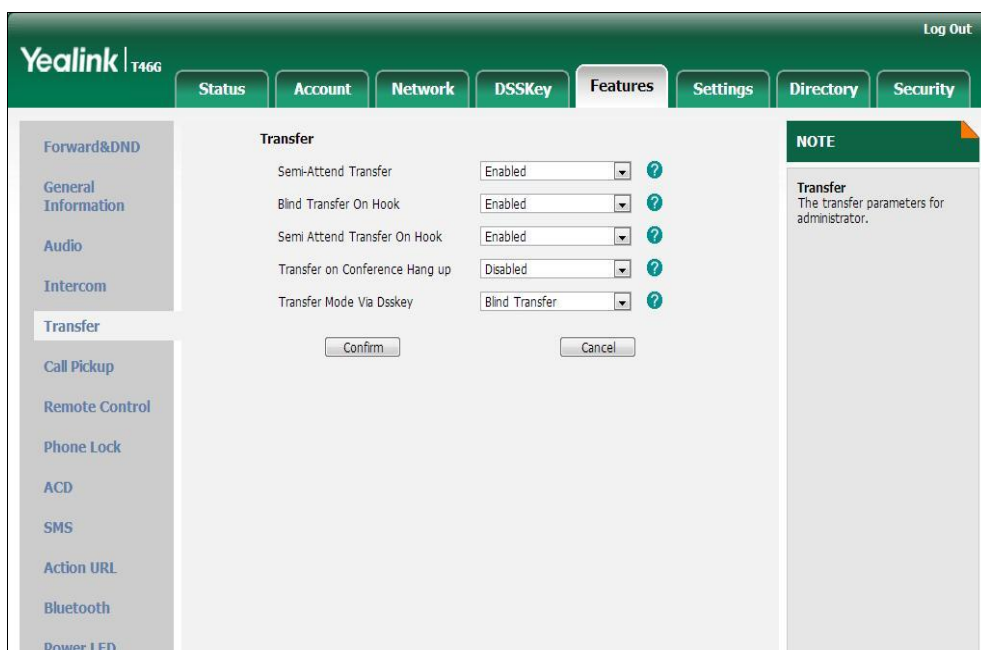
Procedure

Call transfer can be configured using the configuration files or locally.

Configuration File	<y000000000xx>.cfg	Specify whether to complete the transfer through on-hook. Configure the semi-attended transfer feature. For more information, refer to Call Transfer on page 304.
Local	Web User Interface	Specify whether to complete the transfer through on-hook. Configure the semi-attended transfer feature. Navigate to: http://<phoneIPAddress>/servlet?p=features-transfer&q=load

To configure call transfer via web user interface:

1. Click on **Features->Transfer**.
2. Select the desired values from the pull-down lists of **Semi-Attend Transfer**, **Blind Transfer On Hook** and **Semi Attend Transfer On Hook**.



3. Click **Confirm** to accept the change.

Network Conference

Network conference, also known as centralized conference, provides users with flexibility of call with multiple participants (more than three). IP phones implement network conference using the REFER method specified in RFC 4579. This feature depends on support from a SIP server.

Procedure

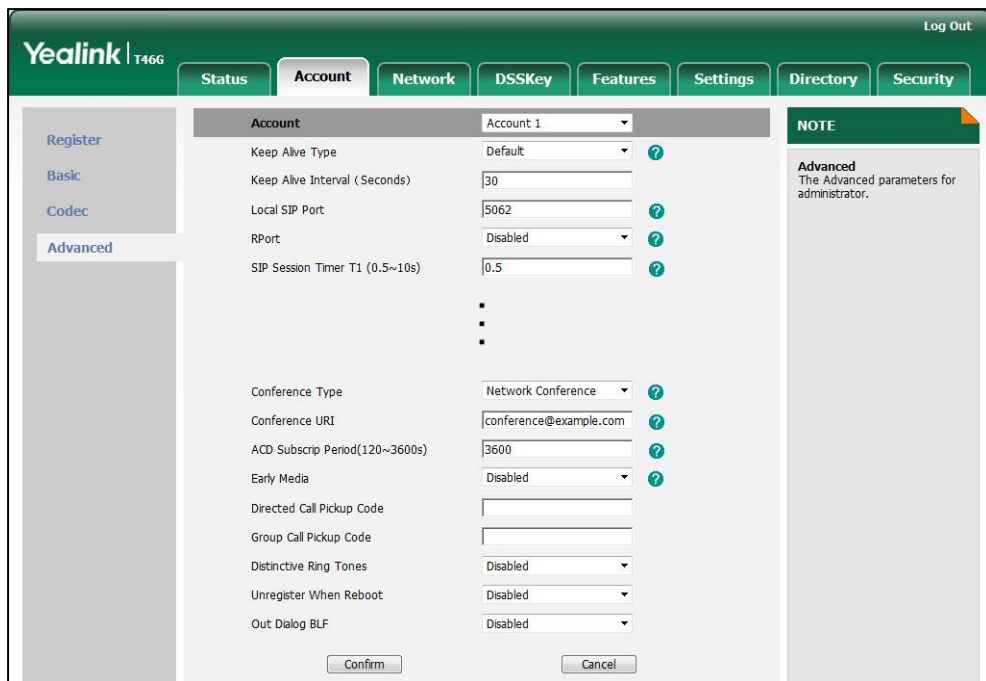
Network conference can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure network conference. For more information, refer to Network Conference on page 305.
Local	Web User Interface	Configure network conference. Navigate to: http://<phoneIPAddress>/servlet ?p=account-adv&q=load&acc=0

To configure the network conference via web user interface:

1. Click on **Account**.
2. Select the desired account from the pull-down list of **Account**.
3. Click on **Advanced**.
4. Select **Network** from the pull-down list of **Conference Type**.

- Enter the conference URI in the **Conference URI** field.



- Click **Confirm** to accept the change.

Transfer on Conference Hang Up

For local conference, all parties drop the call when the conference initiator drops the conference call. Transfer on conference hang up allows the other two parties to remain connected when the conference initiator drops the conference call.

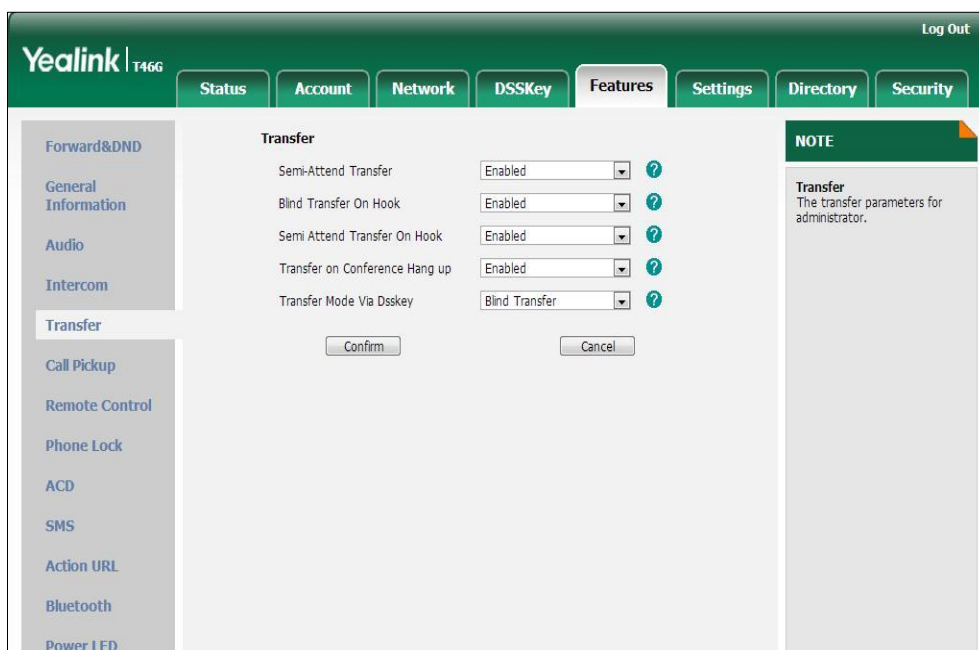
Procedure

Transfer on conference hang up feature can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure transfer on conference hang up. For more information, refer to Transfer on Conference Hang Up on page 306.
Local	Web User Interface	Configure transfer on conference hang up. Navigate to: http://<phoneIPAddress>/servlet?p=features-transfer&q=load

To configure Transfer on Conference Hang up via web user interface:

1. Click on **Features->Transfer**.
2. Select the desired value from the pull-down list of **Transfer on Conference Hang up**.



3. Click **Confirm** to accept the change.

Directed Call Pickup

Directed call pickup is used for picking up an incoming call on a specific extension. A user can pick up the incoming call using a directed pickup key or the DPickup soft key. This feature depends on support from a SIP server. For many SIP servers, directed call pickup requires a directed pickup code, which can be configured on a phone or per-line basis.

Note It is recommended not to configure the directed call pickup key and the DPickup soft key simultaneously. If you do, the directed call pickup key will not be used correctly.

Procedure

Directed call pickup can be configured using the configuration files or locally.

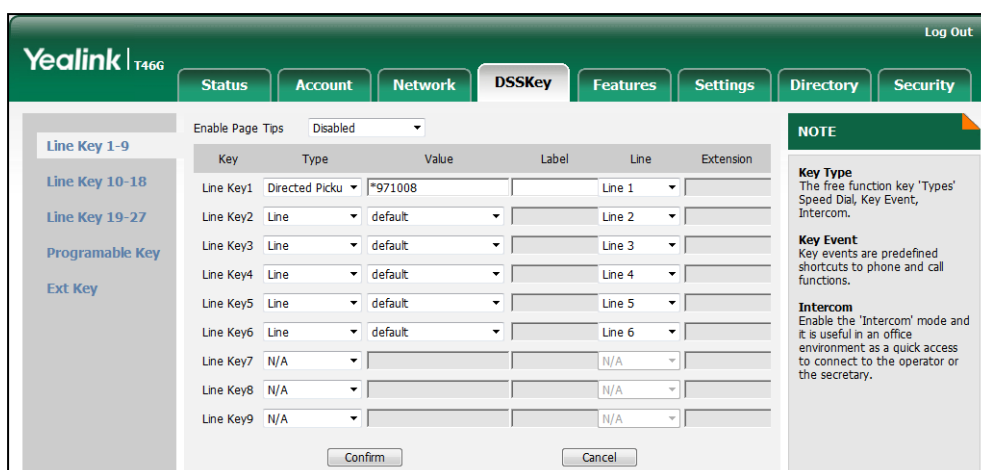
<p>Configuration File</p>	<p><MAC>.cfg</p>	<p>Configure the directed call pickup code on a per-line basis.</p> <p>Configure directed call pickup feature on a phone basis.</p> <p>For more information, refer to Directed Call Pickup on page</p>
----------------------------------	------------------------	--

		307.
	<y0000000000xx>.cfg	Assign a directed call pickup key. For more information, refer to Directed Call Pickup Key on page 387.
Local	Web User Interface	Assign a directed call pickup key. Navigate to: http://<phoneIPAddress>/servlet?p=dsskey&model=1&q=load&linepage=1 Configure the directed call pickup feature on a phone basis. Navigate to: http://<phoneIPAddress>/servlet?p=features-callpickup&q=load Configure the directed call pickup code on a per-line basis. Navigate to: http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0
	Phone User Interface	Assign a directed call pickup key.

To configure a directed call pickup key via web user interface:

1. Click on **DSSKey->Line Key**.
2. In the desired DSS key field, select **Directed Pickup** from the pull-down list of **Type**.
3. Enter the directed call pickup code followed by the specific extension in the **Value** field.

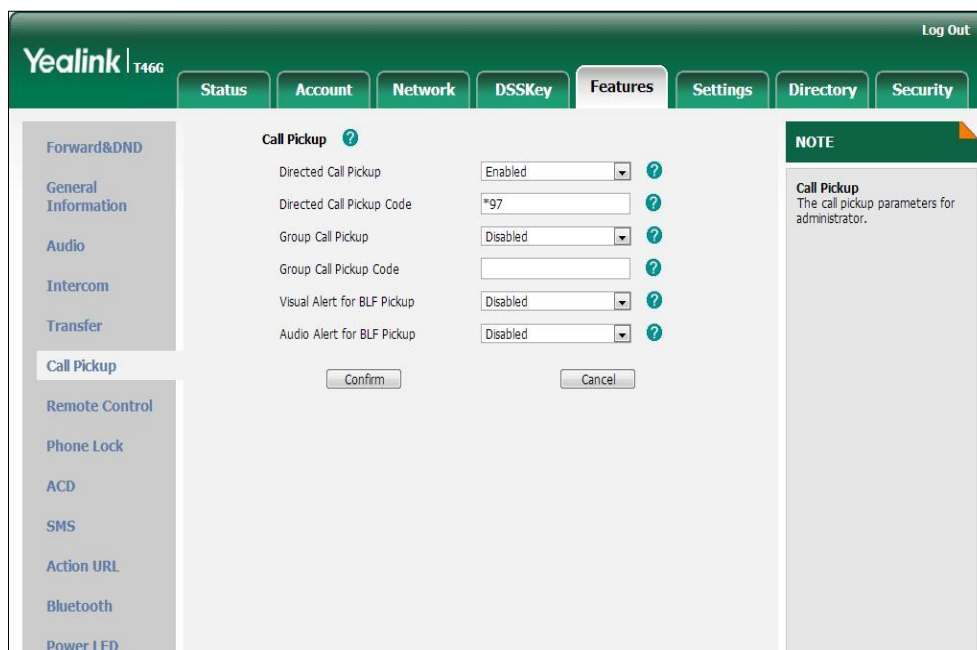
4. Select the desired line from the pull-down list of **Line**.



5. Click **Confirm** to accept the change.

To configure the directed call pickup feature on a phone basis via web user interface:

1. Click on **Features->Call Pickup**.
2. Select the desired value from the pull-down list of **Directed Call Pickup**.
3. Enter the directed call pickup code in the **Directed Call Pickup Code** field.



4. Click **Confirm** to accept the change.

To configure the directed call pickup code on a per-line basis via web user interface:

1. Click on **Account**.
2. Select the desired account from the pull-down list of **Account**.
3. Click on **Advanced**.

- Enter the directed call pickup code in the **Directed Call Pickup Code** field.

The screenshot shows the Yealink T466 web interface with the 'Account' tab selected. The 'Advanced' sub-tab is active, displaying various configuration parameters for 'Account 1'. The 'Directed Call Pickup Code' field is highlighted with a red box and contains the value '*97'. Other visible fields include 'Keep Alive Type' (Default), 'Keep Alive Interval (Seconds)' (30), 'Local SIP Port' (5062), 'RPort' (Disabled), 'SIP Session Timer T1 (0.5~10s)' (0.5), 'SIP Session Timer T2 (2~40s)' (4), 'SIP Session Timer T4 (2.5~60s)' (5), 'Subscribe Period (Seconds)' (1800), and 'DTMF Type' (RFC2833). There are also fields for 'Music Server URI', 'Group Call Pickup Code', 'Distinctive Ring Tones', 'Unregister When Reboot', and 'Out Dialog BLF', all currently set to 'Disabled'. A 'NOTE' box on the right states: 'Advanced: The Advanced parameters for administrator.' At the bottom, there are 'Confirm' and 'Cancel' buttons.

- Click **Confirm** to accept the change.

To configure a directed pickup key via phone user interface:

- Press **Menu->Call Features->DSS Keys**.
- Select the desired DSS key.
- Press **◀** or **▶**, or the **Switch** soft key to select **Key Event** from the **Type** field.
- Press **◀** or **▶**, or the **Switch** soft key to select **Directed Pickup** from the **Key Event** field.
- Press **◀** or **▶**, or the **Switch** soft key to select the desired line from the **Account ID** field.
- (Optional.) Enter the string that will appear on the LCD screen in the **Label** field.
- Enter the directed call pickup code followed by the specific extension in the **Value** field.
- Press the **Save** soft key to accept the change.

Group Call Pickup

Group call pickup is used for picking up incoming calls within a pre-defined group. If the group receives many incoming calls at once, the user will pick up the first incoming call, using a group pickup key or the GPickup soft key. This feature depends on support from a SIP server. For many SIP servers, group call pickup requires a group pickup code, which can be configured on a phone or per-line basis.

Procedure

Group call pickup can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	<p>Configure the group call pickup code on a per-line basis.</p> <p>Configure group call pickup feature on a phone basis.</p> <p>For more information, refer to Group Call Pickup on page 308.</p>
	<y000000000xx>.cfg	<p>Assign a group call pickup key.</p> <p>For more information, refer to Group Call Pickup Key on page 388.</p>
Local	Web User Interface	<p>Assign a group call pickup key.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet?p=dsskey&model=1&q=load&linepage=1</p> <p>Configure the group call pickup feature on a phone basis.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet?p=features-callpickup&q=load</p> <p>Configure the group call pickup code on a per-line basis.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0</p>
	Phone User Interface	<p>Assign a group call pickup key.</p>

To configure a group call pickup key via web user interface:

1. Click on **DSSKey->Line Key**.
2. In the desired DSS key field, select **Group Pickup** from the pull-down list of **Type**.
3. Enter the group call pickup code in the **Value** field.

- Select the desired line from the pull-down list of **Line**.

Key	Type	Value	Label	Line	Extension
Line Key1	Group Pickup	*98		Line 1	
Line Key2	Line	default		Line 2	
Line Key3	Line	default		Line 3	
Line Key4	Line	default		Line 4	
Line Key5	Line	default		Line 5	
Line Key6	Line	default		Line 6	
Line Key7	N/A			N/A	
Line Key8	N/A			N/A	
Line Key9	N/A			N/A	

- Click **Confirm** to accept the change.

To configure the group call pickup feature on a phone basis via web user interface:

- Click on **Features->Call Pickup**.
- Select the desired value from the pull-down list of **Group Call Pickup**.
- Enter the group call pickup code in the **Group Call Pickup Code** field.

- Click **Confirm** to accept the change.

To configure the group call pickup code on a per-line basis via web user interface:

- Click on **Account**.
- Select the desired account from the pull-down list of **Account**.
- Click on **Advanced**.

- Enter the group call pickup code in the **Group Call Pickup Code** field.

The screenshot shows the Yealink T466 web interface with the 'Account' tab selected. The 'Group Call Pickup Code' field is highlighted with a red box and contains the value '*98'. Other fields include 'Keep Alive Type' (Default), 'Keep Alive Interval (Seconds)' (30), 'Local SIP Port' (5062), 'RPort' (Disabled), 'SIP Session Timer T1 (0.5~10s)' (0.5), 'SIP Session Timer T2 (2~40s)' (4), 'SIP Session Timer T4 (2.5~60s)' (5), 'Subscribe Period (Seconds)' (1800), and 'DTMF Type' (RFC2833). There are also fields for 'Directed Call Pickup Code', 'Distinctive Ring Tones', 'Unregister When Reboot', and 'Out Dialog BLF'. A 'NOTE' section on the right states: 'Advanced: The Advanced parameters for administrator.'

- Click **Confirm** to accept the change.

To configure a group pickup key via phone user interface:

- Press **Menu->Call Features->DSS Keys**.
- Select the desired DSS key.
- Press **◀** or **▶**, or the **Switch** soft key to select **Key Event** from the **Type** field.
- Press **◀** or **▶**, or the **Switch** soft key to select **Group Pickup** from the **Key Event** field.
- Press **◀** or **▶**, or the **Switch** soft key to select the desired line from the **Account ID** field.
- (Optional.) Enter the string that will appear on the LCD screen in the **Label** field.
- Enter the group call pickup code in the **Value** field.
- Press the **Save** soft key to accept the change.

Dialog-Info Call Pickup

Call pickup is implemented through SIP signals on some specific servers. IP phones can pick up incoming calls via a NOTIFY message with dialog-info event. A user can pick up an incoming call by pressing a DSS key used to monitor a specific extension (such as a BLF key).

Example of the dialog-info message carried in NOTIFY message:

```
<?xml version="1.0"?>
<dialog-info xmlns="urn:ietf:params:xml:ns:dialog-info" version="6" state="full"
entity="sip:1013@10.2.1.199">
<dialog id="706655206@10.2.8.213" call-id="706655206@10.2.8.213" local-tag="827932784"
remote-tag="1887460740" direction="recipient">
<state>early</state>
<local>
<identity>sip:1013@10.2.1.199</identity>
<target uri="sip:1013@10.2.1.199">
</target>
</local>
<remote>
<identity>sip:1011@10.2.1.199</identity>
<target uri="sip:1011@10.2.8.213:5063">
</target>
</remote>
</dialog>
</dialog-info>
```

Procedure

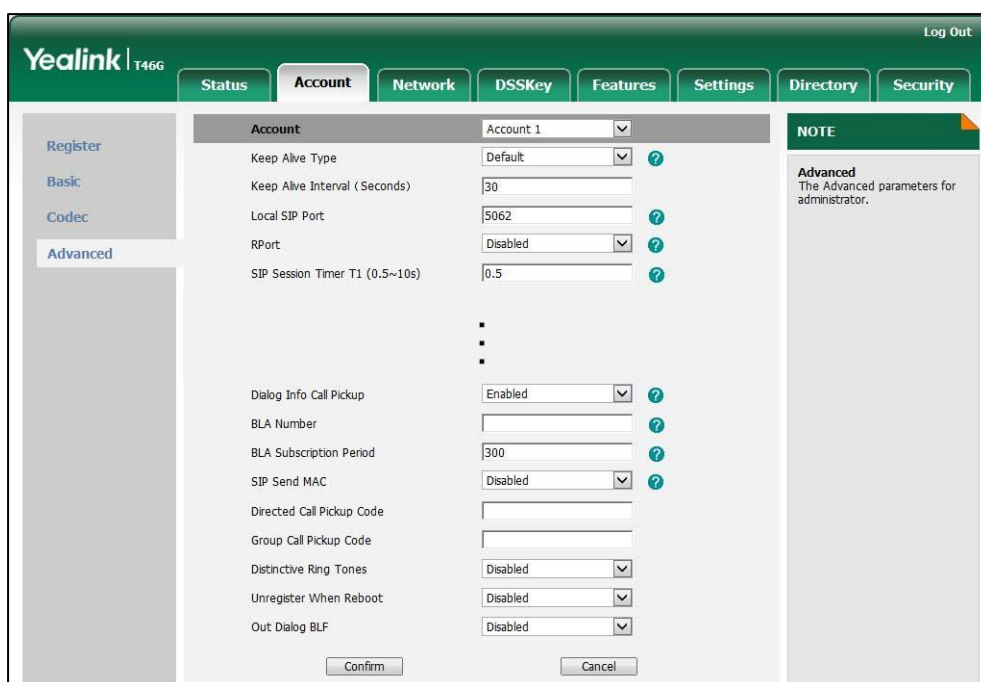
Dialog-info call pickup can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure dialog-info call pickup on the IP phone. For more information, refer to Dialog-Info Call Pickup on page 309.
Local	Web User Interface	Configure dialog-info call pickup on the IP phone. Navigate to: http://<phoneIPAddress>/servl et?p=account-adv&q=load&ac c=0

To configure dialog-info call pickup via web user interface:

1. Click on **Account**.
2. Select the desired account from the pull-down list of **Account**.
3. Click on **Advanced**.

- Select the desired value from the pull-down list of **Dialog Info Call Pickup**.



- Click **Confirm** to accept the change.

Call Return

Call return, also known as last call return, allows users to place a call back to the last caller. Call return is implemented on IP phones using a call return key.

Procedure

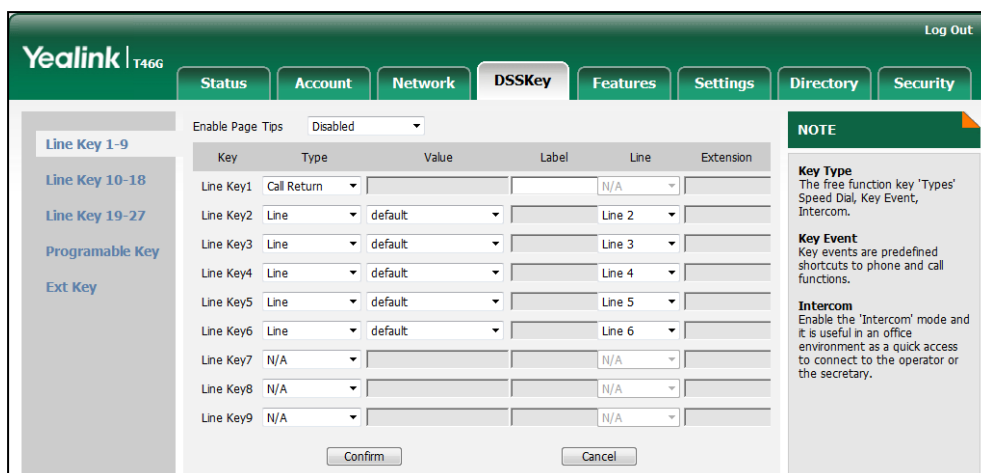
Call return key can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Assign a call return key. For more information, refer to Call Return Key on page 389.
Local	Web User Interface	Assign a call return key. Navigate to: http://<phoneIPAddress>/servlet ?p=dsskey&model=1&q=load&li nepage=1
	Phone User Interface	Assign a call return key.

To configure a call return key via web user interface:

- Click on **DSSKey->Line Key**.

- In the desired DSS key field, select **Call Return** from the pull-down list of **Type**.



- Click **Confirm** to accept the change.

To configure a call return key via phone user interface:

- Press **Menu->Call Features->DSS Keys**.
- Select the desired DSS key.
- Press **◀** or **▶**, or the **Switch** soft key to select **Key Event** from the **Type** field.
- Press **◀** or **▶**, or the **Switch** soft key to select **Call Return** from the **Key Event** field.
- (Optional.) Enter the string that will appear on the LCD screen in the **Label** field.
- Press the **Save** soft key to accept the change.

Call Park

Call park allows users to park a call on a special extension and then retrieve it on any other phone in the system. Users can park calls on the extension, known as call park orbit, by pressing a call park key. The current call is put on hold and can be retrieved on another IP phone. This feature depends on support from a SIP server.

Procedure

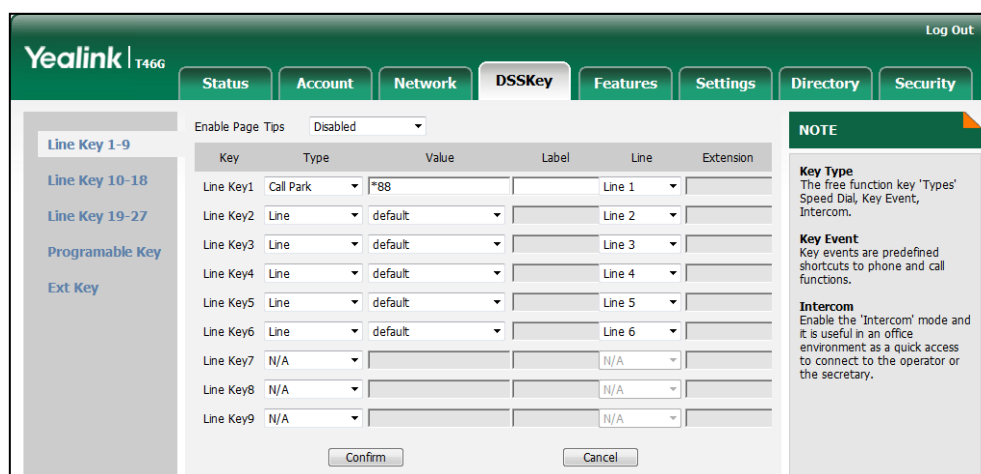
Call park key can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Assign a call park key. For more information, refer to Call Park Key on page 389.
Local	Web User Interface	Assign a call park key. Navigate to: http://<phoneIPAddress>/servlet?p=dsskey&model=1&q=loa

		d&linepage=1
	Phone User Interface	Assign a call park key.

To configure a call park key via web user interface:

1. Click on **DSSKey->Line Key**.
2. In the desired DSS key field, select **Call Park** from the pull-down list of **Type**.
3. Enter the desired value (e.g., call park feature code) in the **Value** field.
4. Select the desired line from the pull-down list of **Line**.



5. Click **Confirm** to accept the change.

To configure a call park key via phone user interface:

1. Press **Menu->Call Features->DSS Keys**.
2. Select the desired DSS key.
3. Press **←** or **→**, or the **Switch** soft key to select **Key Event** from the **Type** field.
4. Press **←** or **→**, or the **Switch** soft key to select **Call Park** from the **Key Event** field.
5. Press **←** or **→**, or the **Switch** soft key to select the desired line from the **Account ID** field.
6. (Optional.) Enter the string that will appear on the LCD screen in the **Label** field.
7. Enter the desired value (e.g., call park feature code) in the **Value** field.
8. Press the **Save** soft key to accept the change.

Web Server Type

Web server type determines access permission of the IP phone's web user interface. IP phones support both HTTP and HTTPS protocols for accessing the web user interface. HTTP is an application protocol that runs on top of the TCP/IP suite of protocols. HTTPS is a web protocol that encrypts and decrypts user page requests as well as the pages returned by the web server. Both the HTTP and HTTPS port numbers are configurable.

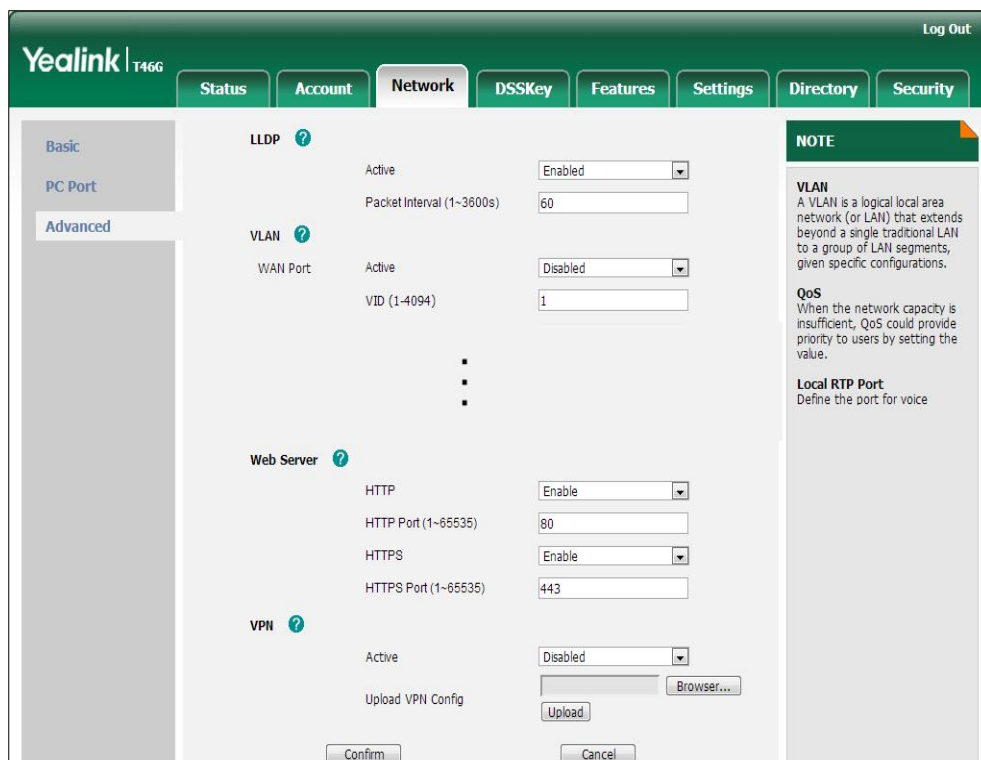
Procedure

Web server type can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Specify the web access type, HTTP port and HTTPS port. For more information, refer to Web Server Type on page 310.
Local	Web User Interface	Specify the web access type, HTTP port and HTTPS port. Navigate to: http://<phoneIPAddress>/servlet?p=network-adv&q=load
	Phone User Interface	Specify the web access type.





To configure the web server type via web user interface:

1. Click on **Network->Advanced**.
2. In the **Web Server** block, select the desired value from the pull-down list of **HTTP**.
3. Enter the HTTP port in the **HTTP Port (1~65535)** field.
The default HTTP port is 80.
4. Select the desired value from the pull-down list of **HTTPS**.
5. Enter the HTTPS port in the **HTTPS Port (1~65535)** field.
The default HTTPS port is 443.



6. Click **Confirm** to accept the change.
A dialog box pops up to prompt that the settings will take effect after reboot.
7. Click **OK** to reboot the IP phone.

To configure the web server type via phone user interface:

1. Press **Menu->Advanced** (password: admin) ->**Network->Webserver Type**.
2. Press  or  , or the **Switch** soft key to select the desired value in the **HTTP Status** field.
3. Enter the HTTP port in the **HTTP Port** field.
4. Press  or  , or the **Switch** soft key to select the desired icon in the **HTTPS Status** field.
5. Enter the HTTPS port in the **HTTPS Port** field.
6. Press the **Save** soft key to accept the change.

The IP phone reboots automatically to make the settings effective after a period of time.

Calling Line Identification Presentation

Calling line identification presentation (CLIP) allows IP phones to display the caller identity, derived from a SIP header contained in the INVITE message when receiving an incoming call. IP phones support deriving caller identity from three types of SIP header: From, P-Asserted-Identity and Remote-Party-ID. Identity presentation is based on the identity in the relevant SIP header.

If the caller has existed in the local directory, the local name assigned to the caller should be preferentially displayed.

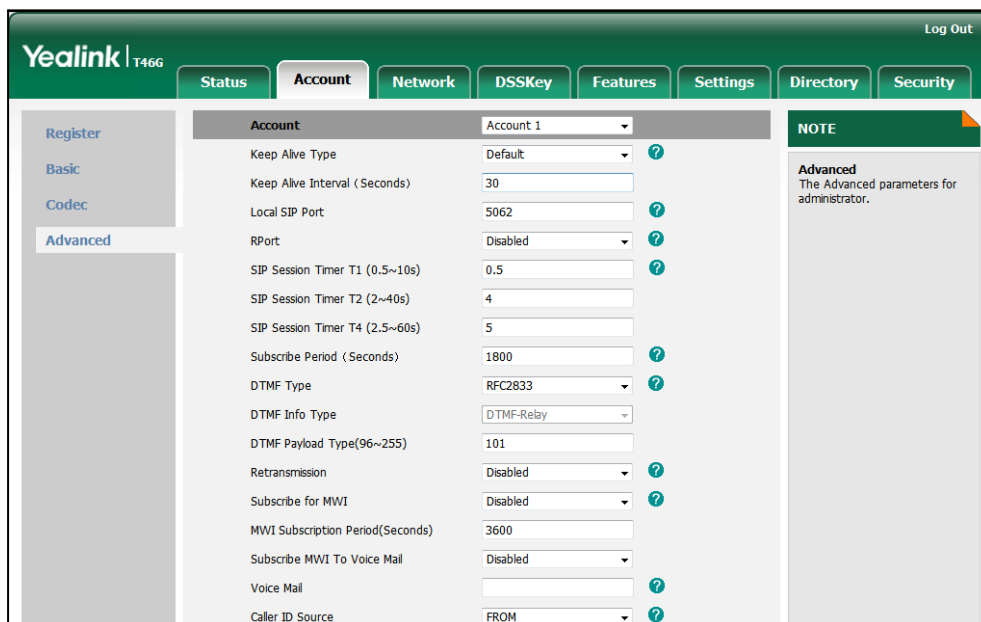
Procedure

CLIP can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure the presentation of the caller identity. For more information, refer to Calling Line Identification Presentation on page 311.
Local	Web User Interface	Configure the presentation of the caller identity. Navigate to: http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

To configure the presentation of the caller identity via web user interface:

1. Click on **Account**.
2. Select the desired account from the pull-down list of **Account**.
3. Click on **Advanced**.
4. Select the desired value from the pull-down list of the **Caller ID Source**.



5. Click **Confirm** to accept the change.

Connected Line Identification Presentation

Connected line identification presentation (COLP) allows IP phones to display the identity of the callee specified for outgoing calls. The IP phone can display the Dialed Digits, or the identity in a SIP header (Remote-Party-ID or P-Asserted-Identity) received, or the identity in the From header carried in the UPDATE message sent by the callee as described in RFC 4916.

If the callee has existed in the directory, the local name assigned to the callee should be preferentially displayed.

Procedure

COLP can be configured only using the configuration files.

Configuration File	<MAC>.cfg	<p>Configure the presentation of the callee identity.</p> <p>For more information, refer to Connected Line Identification Presentation on page 312.</p>
---------------------------	-----------	---

DTMF

DTMF (Dual Tone Multi-frequency), better known as touch-tone, is used for telecommunication signaling over analog telephone lines in the voice-frequency band. DTMF is the signal sent from the IP phone to the network, which is generated when pressing the IP phone's keypad during a call. Each key pressed on the IP phone generates one sinusoidal tone of two frequencies. One is generated from a high frequency group and the other from a low frequency group.

The DTMF keypad is laid out in a 4x4 matrix, with each row representing a low frequency, and each column representing a high frequency. Pressing a digit key (such as '1') will generate a sinusoidal tone for each of two frequencies (697 and 1209 hertz (Hz)).

DTMF Keypad Frequencies:

	1209 Hz	1336 Hz	1447 Hz	1633 Hz
697 Hz	1	2	3	A
770 Hz	4	5	6	B
852 Hz	7	8	9	C
941 Hz	*	0	#	D

Three methods of transmitting DTMF digits on SIP calls:

- **RFC 2833** --DTMF digits are transmitted by RTP Events compliant to RFC 2833.
- **INBAND** -- DTMF digits are transmitted in the voice band.
- **SIP INFO** -- DTMF digits are transmitted by the SIP INFO messages.

The method of transmitting DTMF digits is configurable on a per-line basis.

RFC 2833

DTMF digits are transmitted using the RTP Event packets that are sent along with the voice path. These packets use RFC 2833 format and must have a payload type that matches what the other end is listening for. The payload type for the RTP Event packets is configurable. IP phones default to 101 for the payload type, which use the definition to negotiate with the other end during call establishment.

The RTP Event packet contains 4 bytes. The 4 bytes are distributed over several fields denoted as Event, End bit, R-bit, Volume and Duration. If the End bit is set to 1, the packet contains the end of the DTMF event. You can configure the sending times of the end RTP Event packet.

INBAND

DTMF digits are transmitted within the audio of the IP phone conversation. It uses the

same VoIP codec as your voice and is audible to the conversation partners.

SIP INFO

DTMF digits are transmitted by the SIP INFO messages when the voice stream is established after a successful SIP 200 OK-ACK message sequence. The SIP INFO message is sent along the signaling path of the call. The SIP INFO message can transmit DTMF digits in three ways: DTMF, DTMF-Relay and Telephone-Event.

Procedure

Configuration changes can be performed using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure the method of transmitting DTMF digit and the payload type. For more information, refer to DTMF on page 313 .
	<y0000000000xx>.cfg	Configure the number of times for the IP phone to send the end RTP Event packet. For more information, refer to DTMF on page 313 .
Local	Web User Interface	Configure the method of transmitting DTMF digits and the payload type. Navigate to: <code>http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0</code> Configure the number of times for the IP phone to send the end RTP Event packet. Navigate to: <code>http://<phoneIPAddress>/servlet?p=features-general&q=load</code>

To configure the method of transmitting DTMF digits via web user interface:

1. Click on **Account**.
2. Select the desired account from the pull-down list of **Account**.
3. Click on **Advanced**.
4. Select the desired value from the pull-down list of **DTMF Type**.

If **SIP INFO** or **AUTO** or **SIP INFO** is selected, select the desired value from the pull-down list of **DTMF Info Type**.

5. Enter the desired value in the **DTMF Payload Type (96~127)** field.

The screenshot shows the 'Account' configuration page for a Yealink T46G phone. The 'DTMF Payload Type(96~127)' field is set to 101. Other fields include 'DTMF Type' (RFC2833), 'DTMF Info Type' (DTMF-Relay), and various session timers.

Field	Value
Account	Account 1
Keep Alive Type	Default
Keep Alive Interval (Seconds)	30
Local SIP Port	5062
RPort	Disabled
SIP Session Timer T1 (0.5~10s)	0.5
SIP Session Timer T2 (2~40s)	4
SIP Session Timer T4 (2.5~60s)	5
Subscribe Period (Seconds)	1800
DTMF Type	RFC2833
DTMF Info Type	DTMF-Relay
DTMF Payload Type(96~127)	101

6. Click **Confirm** to accept the change.

To configure the number of times to send the end RTP Event packet via web user interface:

1. Click on **Features->General Information**.
2. Select the desired value (1-3) from the pull-down list of **DTMF Repetition**.

The screenshot shows the 'Features -> General Information' configuration page. The 'DTMF Repetition' field is set to 3. Other fields include 'Call Waiting' (Enabled), 'Auto Redial' (Disabled), and 'Key As Send' (#).

Field	Value
Call Waiting	Enabled
Call Waiting On Code	
Call Waiting Off Code	
Auto Redial	Disabled
Auto Redial Interval (1~300s)	10
Auto Redial Times (1~300)	10
Key As Send	#
DTMF Repetition	3
Multicast Codec	G722
Play Hold Tone	Enabled
Play Hold Tone Delay	30
Allow Mute	Enabled
Voice Mail Tone	Enable
DHCP Hostname	SIP-T46G

3. Click **Confirm** to accept the change.

Suppress DTMF Display

Suppress DTMF display allows IP phones to suppress the display of DTMF digits. The DTMF digits are displayed as “*” on the LCD screen. Suppress DTMF display delay defines whether to display the DTMF digits for a short period of time before displaying as “*”.

Procedure

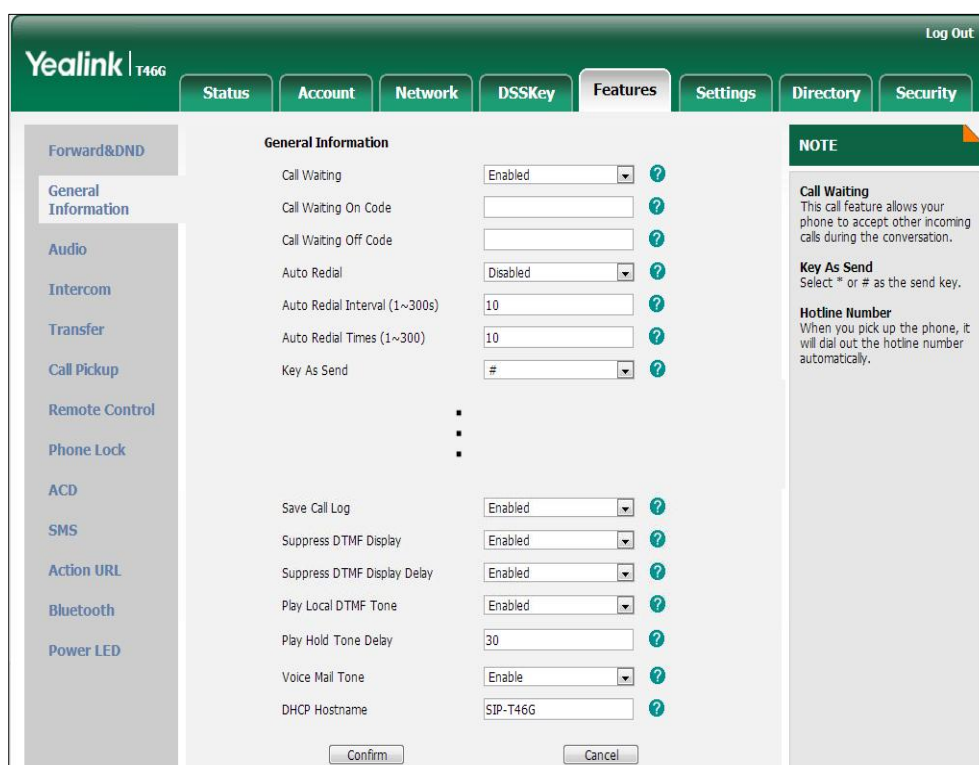
Configuration changes can be performed using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure suppress DTMF display and suppress DTMF display delay. For more information, refer to Suppress DTMF Display on page 315.
Local	Web User Interface	Configure suppress DTMF display and suppress DTMF display delay. Navigate to: http://<phoneIPAddress>/servlet?p=features-general&q=load

To configure suppress DTMF display and suppress DTMF display delay via web user interface:

1. Click on **Features->General Information**.
2. Select the desired value from the pull-down list of **Suppress DTMF Display**.

3. Select the desired value from the pull-down list of **Suppress DTMF Display Delay**.



4. Click **Confirm** to accept the change.

Transfer via DTMF

Call transfer is implemented via DTMF on some traditional servers. The IP phone sends specified DTMF digits to the server for transferring calls to a third party.

Procedure

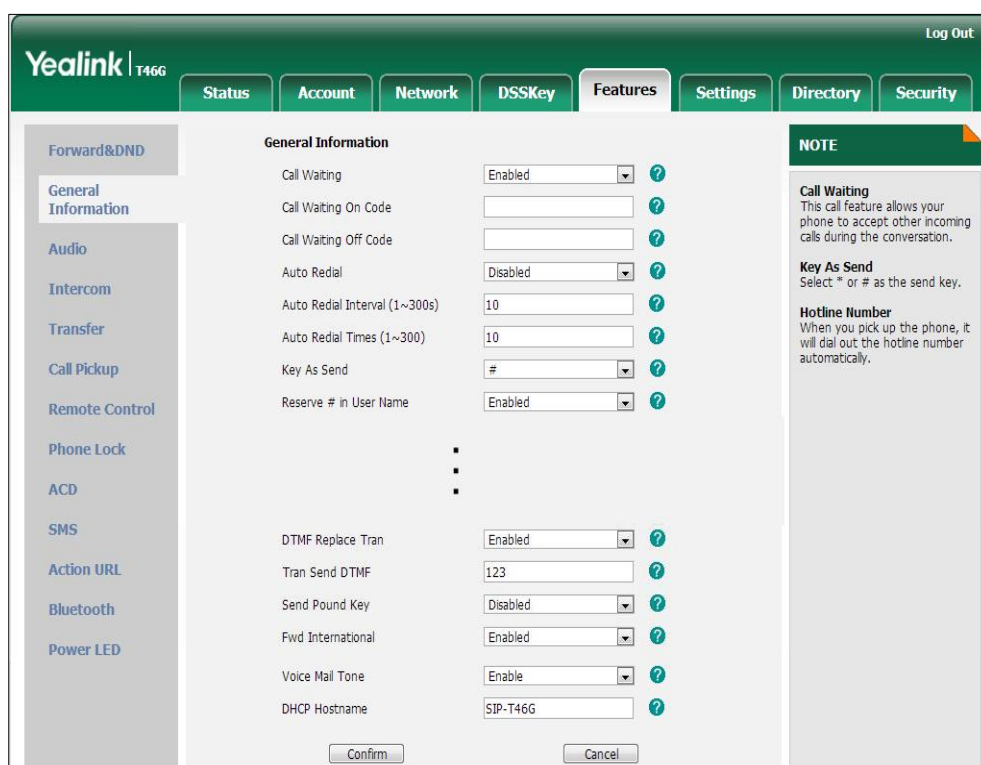
Configuration changes can be performed using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure transfer via DTMF. For more information, refer to Transfer via DTMF on page 315.
Local	Web User Interface	Configure transfer via DTMF. Navigate to: http://<phoneIPAddress>/servlet?&p=features-general&q=load

To configure the transfer via DTMF feature via web user interface:

1. Click on **Features->General Information**.
2. Select the desired value from the pull-down list of **DTMF Replace Tran**.

- Enter the specified DTMF digits in the **Tran Send DTMF** field.



- Click **Confirm** to accept the change.

Intercom

Intercom allows establishing an audio conversation directly. The IP phone can answer intercom calls automatically. This feature depends on support from a SIP server.

Outgoing Intercom Calls

Intercom is a useful feature in office environments to quickly connect with an operator or secretary. Users can press an intercom key to automatically initiate an outgoing intercom call with a remote extension.

Procedure

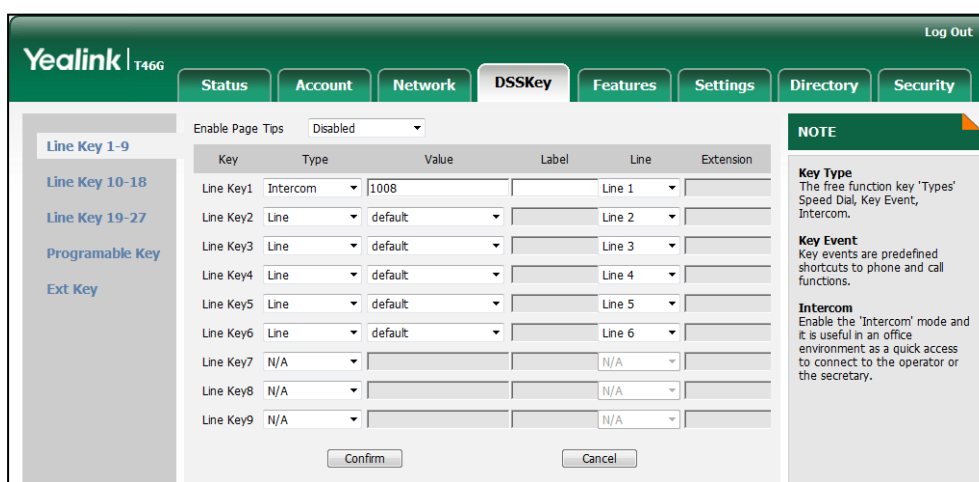
Intercom key can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Assign an intercom key. For more information, refer to Intercom Key on page 390.
Local	Web User Interface	Assign an intercom key. Navigate to: http://<phoneIPAddress>/servlet

		?p=dsskey&model=1&q=load&linepage=1
	Phone User Interface	Assign an intercom key.

To configure an intercom key via web user interface:

1. Click on **DSSKey->Line Key**.
2. In the desired DSS key field, select **Intercom** from the pull-down list of **Type**.
3. Enter the remote extension number in the **Value** field.
4. Select the desired line from the pull-down list of **Line**.



5. Click **Confirm** to accept the change.

To configure an intercom key via phone user interface:

1. Press **Menu->Call Features->DSS Keys**.
2. Select the desired DSS key.
3. Press **◀** or **▶**, or the **Switch** soft key to select **Intercom** from the **Type** field.
4. Select the desired line from the **Account ID** field.
5. (Optional.) Enter the string that will appear on the LCD screen in the **Label** field.
6. Enter the remote extension number in the **Value** field.
7. Press the **Save** soft key to accept the change.

Incoming Intercom Calls

The IP phone can process incoming calls differently depending on settings. There are four configuration options for incoming intercom calls.

Accept Intercom

Accept Intercom allows the IP phone to automatically answer an incoming intercom call.

Intercom Mute

Intercom Mute allows the IP phone to mute the microphone for incoming intercom calls.

Intercom Tone

Intercom Tone allows the IP phone to play a warning tone before answering an intercom call.

Intercom Barge

Intercom Barge allows the IP phone to automatically answer an incoming intercom call while an active call is in progress. The active call will be placed on hold.

Procedure

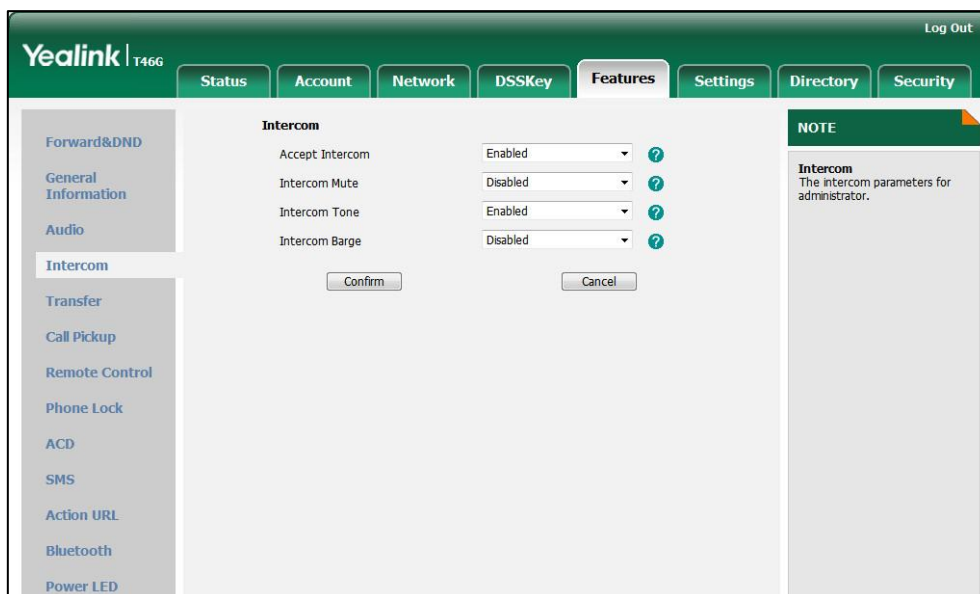
Incoming intercom calls can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure the incoming intercom call feature. For more information, refer to Incoming Intercom calls on page 316.
Local	Web User Interface	Configure the incoming intercom call feature. Navigate to: http://<phoneIPAddress>/servlet?p=features-intercom&q=load
	Phone User Interface	Configure the incoming intercom call feature.

To configure intercom via web user interface:

1. Click on **Features->Intercom**.

2. Select the desired values from the pull-down lists of **Accept Intercom**, **Intercom Mute**, **Intercom Tone** and **Intercom Barge**.



3. Click **Confirm** to accept the change.

To configure intercom via phone user interface:

1. Press **Menu->Call Features->Intercom**.
2. Press **◀** or **▶** , or the **Switch** soft key to select the desired values from the **Accept Intercom**, **Intercom Mute**, **Intercom Tone** and **Intercom Barge** fields.
3. Press the **Save** soft key to accept the change.

Configuring Advanced Features

This chapter provides information for making configuration changes for the following advanced features:

- [Distinctive Ring Tones](#)
- [Tones](#)
- [Remote Phone Book](#)
- [LDAP](#)
- [Busy Lamp Field](#)
- [Music on Hold](#)
- [Automatic Call Distribution](#)
- [Message Waiting Indicator](#)
- [Multicast Paging](#)
- [Call Recording](#)
- [Hot Desking](#)
- [Action URL](#)
- [Action URI](#)
- [Server Redundancy](#)
- [LLDP](#)
- [VLAN](#)
- [VPN](#)
- [Quality of Service](#)
- [Network Address Translation](#)
- [802.1X Authentication](#)
- [TR-069 Device Management](#)
- [IPv6 Support](#)

Distinctive Ring Tones

Distinctive ring tones allows particular incoming calls to trigger IP phones to play distinctive ring tones. The IP phone inspects the INVITE request for an "Alert-Info" header when receiving an incoming call. If the INVITE request contains an "Alert-Info" header, the IP phone strips out the URL and keyword parameter and maps it to the appropriate ring tone.

Alert-Info headers in the following two formats:

Alert-Info: localIP/Bellcore-drN

Alert-Info: <URL>;info=info text;x-line-id=0

- If the Alter-Info header contains the keyword "Bellcore-drN", the IP phone will play the Bellcore-drN ring tone (N=1, 2, 3, 4 or 5) (if the parameter "features.alert_info_tone" is set to 1).

Example:

Alert-Info: http://127.0.0.1/Bellcore-dr1

The following table identifies the different Bellcore ring tone patterns and cadences (These ring tones are designed for the BroadWorks server).

Bellcore Tone	Pattern ID	Pattern	Cadence	Minimum Duration (ms)	Nominal Duration (ms)	Maximum Duration (ms)
Bellcore-dr1 (standard)	1	Ringing	2s On	1800	2000	2200
		Silent	4s Off	3600	4000	4400
Bellcore-dr2	2	Ringing	Long	630	800	1025
		Silent		315	400	525
		Ringing	Long	630	800	1025
		Silent		3475	4000	4400
Bellcore-dr3	3	Ringing	Short	315	400	525
		Silent		145	200	525
		Ringing	Short	315	400	525
		Silent		145	200	525
		Ringing	Long	630	800	1025
		Silent		2975	4000	4400
Bellcore-dr4	4	Ringing	Short	200	300	525
		Silent		145	200	525
		Ringing	Long	800	1000	1100
		Silent		145	200	525
		Ringing	Short	200	300	525
		Silent		2975	4000	4400
Bellcore-dr5	5	Ringing		450	500	550

Note

"Bellcore-dr5" is a ring splash tone that reminds the user that DND or Always Call Forward feature is enabled on the server-side.

- If the Alert-Info header contains a remote URL, the IP phone will try to download the WAV ring tone file from the URL and then play the remote ring tone (if the parameter "account.X.alert_info_url_enable" is set to 1). If it fails to download the file, the IP phone will play the local ring tone associated with **info text**. If there is no text matched, the IP phone will play the preconfigured local ring tone in about ten seconds.

Example:

Alert-Info: http://192.168.0.12:8080/ring.wav/info=family;x-line-id=0

Procedure

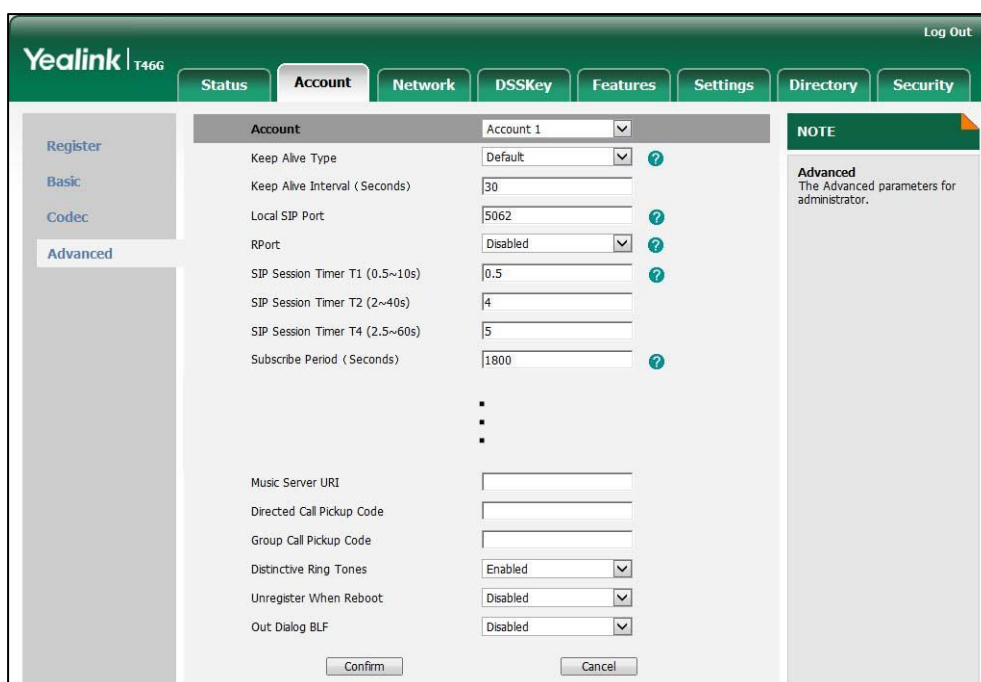
Distinctive ring tones can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure distinctive ring tones feature. For more information, refer to Distinctive Ring Tones on page 318.
	<y000000000xx>.cfg	Configure the internal ringer text and internal ringer file. For more information, refer to Distinctive Ring Tones on page 318.
Local	Web User Interface	Configure distinctive ring tones feature. Navigate to: http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0 Configure the internal ringer text and internal ringer file. Navigate to: http://<phoneIPAddress>/servlet?p=settings-ring&q=load

To configure distinctive ring tones via web user interface:

1. Click on **Account**.
2. Select the desired account from the pull-down list of **Account**.
3. Click on **Advanced**.

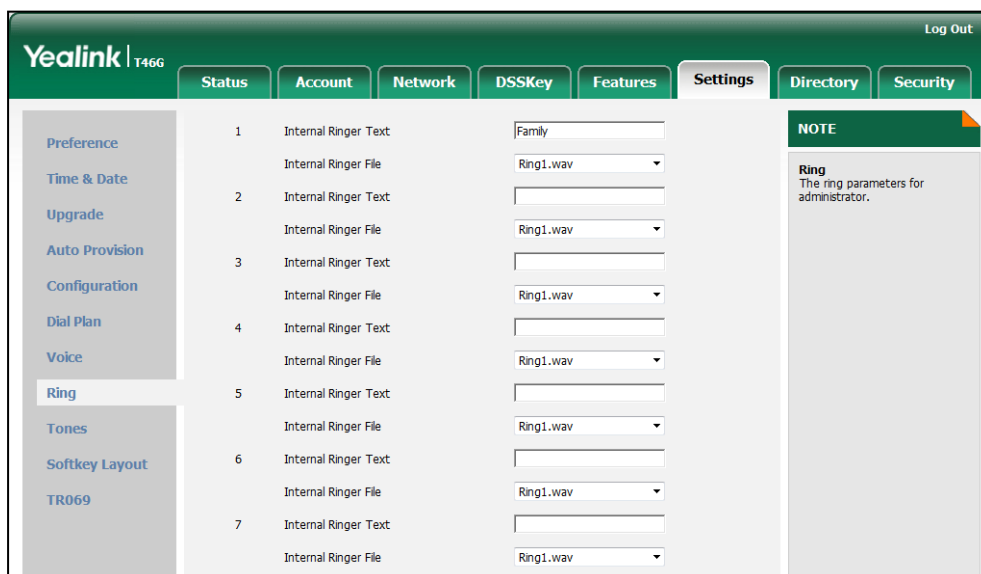
4. Select the desired value from the pull-down list of **Distinctive Ring Tones**.



5. Click **Confirm** to accept the change.

To configure the internal ringer text and internal ringer file via web user interface:

1. Click on **Settings->Ring**.
2. Enter the keywords in the **Internal Ringer Text** fields.
3. Select the desired ring tones for each text from the pull-down lists of **Internal Ringer File**.



4. Click **Confirm** to accept the change.

Tones

When receiving a message or recording a call, the IP phone will play a warning tone. You can customize tones or select specialized tone sets (vary from country to country) to indicate different conditions of the IP phone. The default tones used on IP phones are the US tone sets. Available tone sets for IP phones:

- Australia
- Austria
- Brazil
- Belgium
- China
- Czech
- Denmark
- Finland
- France
- Germany
- Great Britain
- Greece
- Hungary
- Lithuania
- India
- Italy
- Japan
- Mexico
- New Zealand
- Netherlands
- Norway
- Portugal
- Spain
- Switzerland
- Sweden
- Russia
- United States
- Chile
- Czech ETSI

Configured tones can be heard on the IP phone for the following conditions:

Condition	Description
Dial	When in the pre-dialing interface
Ring Back	Ring-back tone
Busy	When the callee is busy
Congestion	When the network is congested
Call Waiting	Call waiting tone
Dial Recall	When receiving a call back
Record	When recording a call
Info	When receiving a special message
Stutter	When receiving a voice mail
Message	When receiving a text message
Auto Answer	When automatically answering a call

Procedure

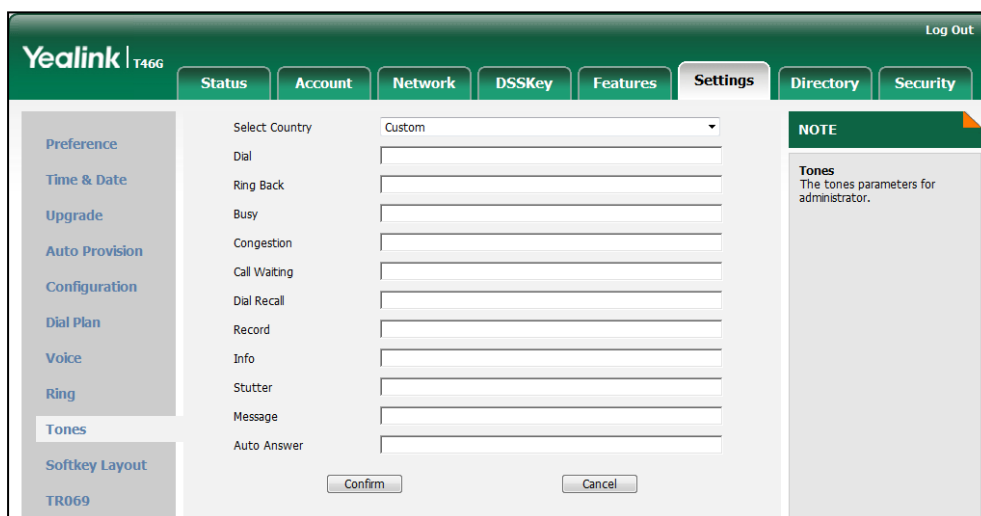
Tones can be configured using the configuration files or locally.

Configuration File	<y000000000xx>.cfg	Configure the tones for the IP phone. For more information, refer to Tones on page 320.
Local	Web User Interface	Configure the tones for the IP phone. Navigate to: http://<phoneIPAddress>/servlet?p=settings-tones&q=load

To configure tones via web user interface:

1. Click on **Settings->Tones**.

2. Select the desired type from the pull-down list of **Select Country**.
If you select **Custom**, you can customize the tone for indicating each condition of the IP phone.



3. Click **Confirm** to accept the change.

Remote Phone Book

Remote phone book is a centrally maintained phone book, stored on the remote server. Users only need the access URL of the remote phone book. The IP phone can establish a connection with the remote server and download the entries, and then display the remote phone book entries on the phone user interface. IP phones support up to 5 remote phone books. For SIP-T46G IP phones, all remote phone books must be less than 0.5MB in size. SIP-T42G and T41P IP phones support up to 5000 entries. Remote phone book is customizable. For more information, refer to [Remote XML Phone Book](#) on page 224.

Sremote Name allows IP phones to query the entry names from the remote phone book when receiving incoming calls. Sremote Name Flash Time defines how often IP phones refresh the local cache of the remote phone book.

Procedure

Remote phone book can be configured using the configuration files or locally.

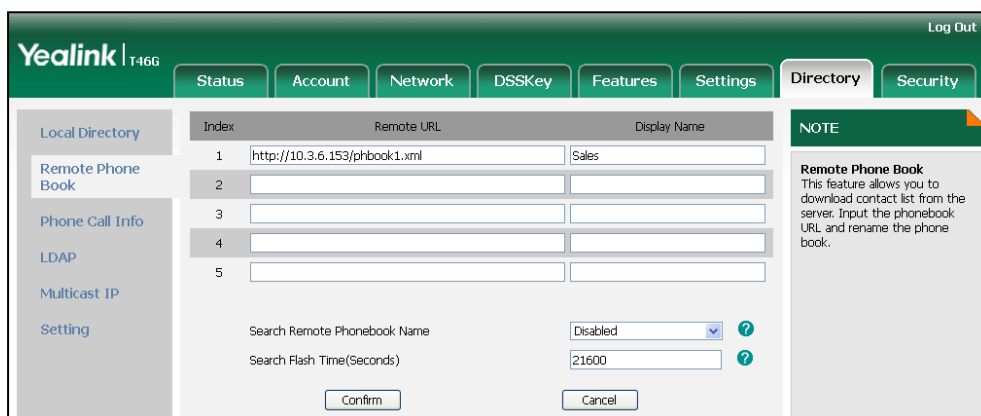
<p>Configuration File</p>	<p><y0000000000xx>.cfg</p>	<p>Specify the access URL of the remote phone book.</p> <p>For more information, refer to Remote Phone Book on page 322.</p> <p>Specify whether to query the entry names from the remote</p>
----------------------------------	----------------------------------	--

		<p>phone book when the IP phone receives incoming calls.</p> <p>Specify how often the IP phone refreshes the local cache of the remote phone book.</p> <p>For more information, refer to Remote Phone Book on page 322.</p>
Local	Web User Interface	<p>Specify the access URL of the remote phone book.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet?p=contacts-remote&q=load</p> <p>Specify whether to query the contact names from the remote phone book when the IP phone receives incoming calls.</p> <p>Specify how often the IP phone refreshes the local cache of the remote phone book.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet?p=contacts-remote&q=load</p>

To specify the access URL of the remote phone book via web user interface:

1. Click on **Directory->Remote Phone Book**.
2. Enter the access URL in the **Remote URL** field.

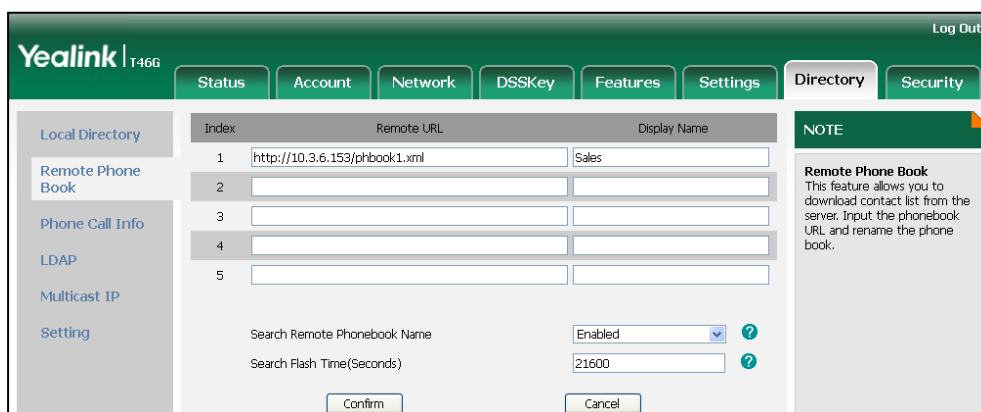
3. Enter the name in the **Display Name** field.



4. Click **Confirm** to accept the change.

To configure the remote phone book via web user interface:

1. Click on **Directory->Remote Phone Book**.
2. Select the desired value from the pull-down list of **Search Remote Phonebook Name**.
3. Enter the desired time in the **Search Flash Time (Seconds)** field.



4. Click **Confirm** to accept the change.

LDAP

LDAP (Lightweight Directory Access Protocol) is an application protocol for accessing and maintaining information services for the distributed directory over an IP network. IP phones can be configured to interface with a corporate directory server that supports LDAP version 2 or 3 (Microsoft’s Active Directory is included).

The biggest plus for LDAP is that users can access the central LDAP directory of the corporation using IP phones, so they do not have to maintain the local directory. Users can search and dial out from the LDAP directory and save LDAP entries to the local directory. LDAP entries displayed on the IP phone are read only, which cannot be added,

edited or deleted by users. When an LDAP server is properly configured, the IP phone can look up entries from the LDAP server in a wide variety of ways. The LDAP server indexes all the data in its entries, and "filters" may be used to select the desired contact or group, and return the desired information.

The configurations on the IP phone limit the amount of displayed entries when querying from the LDAP server, and decide how the attributes are displayed and sorted.

You can assign a DSS key to be an LDAP key, and press the LDAP key to enter the LDAP search screen when the IP phone is idle.

LDAP Attributes

The following table lists the most common attributes used to configure the LDAP lookup on IP phones:

Abbreviation	Name	Description
gn	givenName	First name
cn	commonName	LDAP attribute being made up from given name joined to surname.
sn	surname	Last name or family name
dn	distinguishedName	Unique identifier for each entry
dc	dc	Domain component
-	company	Company or organization name
-	telephoneNumber	Office phone number
mobile	mobilephoneNumber	Mobile or cellular phone number
ipPhone	IPphoneNumber	Home phone number

Procedure

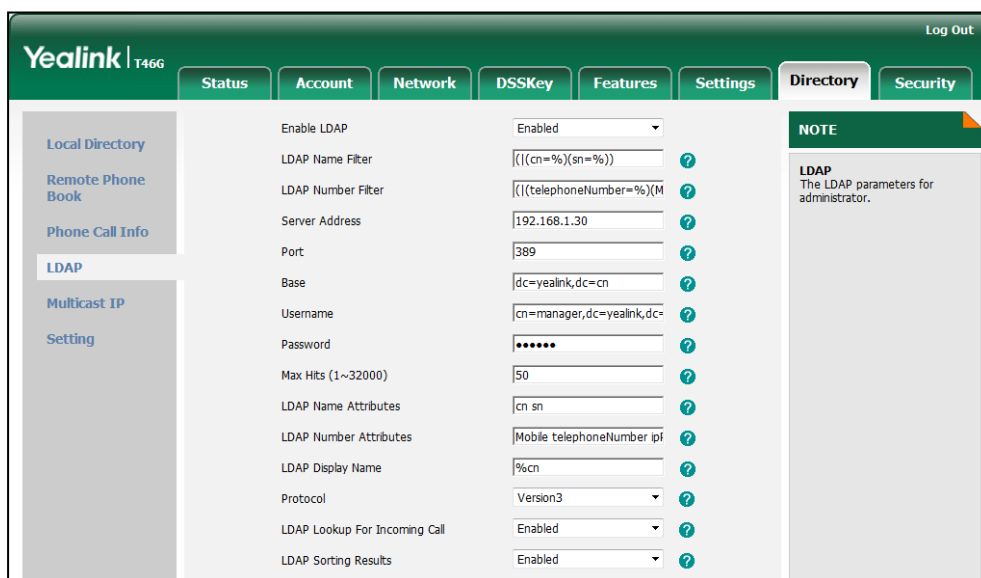
LDAP can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure the LDAP feature. For more information, refer to LDAP on page 324. Assign an LDAP key. For more information, refer to LDAP Key on page 391.
Local	Web User Interface	Configure the LDAP feature. Navigate to: http://<phoneIPAddress>/servl

		<p>et?p=contacts-LDAP&q=load</p> <p>Assign an LDAP key.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servl et?p=dsskey&model=1&q=loa d&linepage=1</p>
	Phone User Interface	Assign an LDAP key.

To configure LDAP via web user interface:

1. Click on **Directory->LDAP**.
2. Select **Enabled** from the pull-down list of **Enable LDAP**.
3. Enter the values in the corresponding fields.
4. Select the desired values from the corresponding pull-down lists.

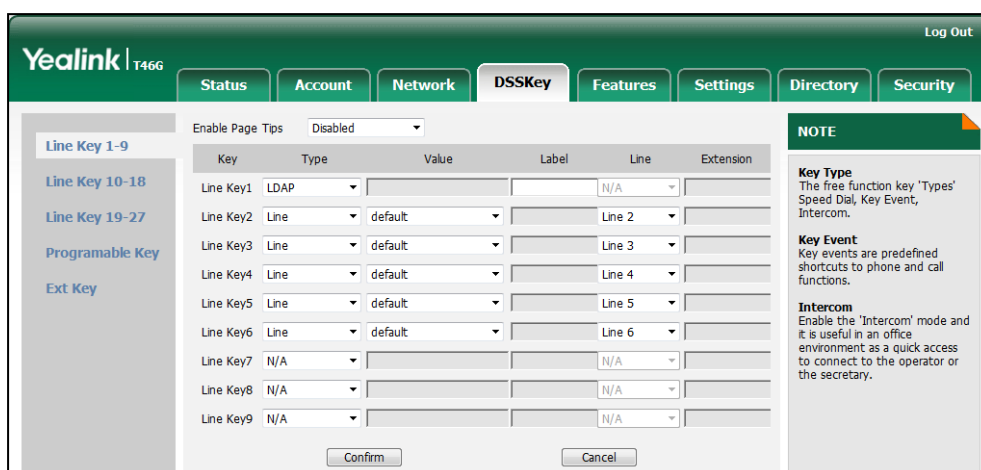


5. Click **Confirm** to accept the change.

To configure an LDAP key via web user interface:

1. Click on **DSSKey->Line Key**.

- In the desired DSS key field, select **LDAP** from the pull-down list of **Type**.



- Click **Confirm** to accept the change.

To configure an LDAP key via phone user interface:

- Press **Menu->Call Features->DSS Keys**.
- Select the desired DSS key.
- Press **◀** or **▶**, or the **Switch** soft key to select **Key Event** from the **Type** field.
- Press **◀** or **▶**, or the **Switch** soft key to select **LDAP** from the **Key Event** field.
- (Optional.) Enter the string that will appear on the LCD screen in the **Label** field.
- Press the **Save** soft key to accept the change.

Busy Lamp Field

Busy Lamp Field (BLF) is used to monitor a specific user for status changes on IP phones. For example, you can configure a BLF key on a supervisor's phone to monitor the phone user status (busy or idle). Then when the user places a call, a busy indicator on the supervisor's phone indicates that the user's phone is in use.

When the monitored user is idle, the supervisor can press the BLF key to dial out the phone number. When the monitored user receives an incoming call, the supervisor can press the BLF key to pick up the call directly. When the monitored user is on a call, the supervisor can press the BLF key to interrupt and set up a conference call.

Visual Alert and Audio Alert for BLF Pickup

Visual alert and audio alert for BLF pickup allow the supervisor's phone to play an alert tone and display a visual prompt (e.g., "6001 <- 6002", 6001 is the monitored extension and receives an incoming call from 6002) when the monitored user receives an incoming call. In addition to the BLF key, visual alert for BLF pickup enables the supervisors to pick up the monitored user's incoming call by pressing the Pickup soft key. The directed call pickup code must be configured in advance. For more information on

how to configure the directed call pickup code for the Pickup soft key, refer to [Directed Call Pickup](#) on page 102.

BLF LED Mode

BLF LED Mode provides four kinds of definition for the BLF key LED status. The following table lists the LED statuses of the BLF key when BLF LED Mode is set to 0, 1, 2 or 3 respectively. The default value of BLF LED mode is 0.

Line key LED (configured as a BLF key and BLF LED Mode is set to 0)

LED Status	Description
Solid green	The monitored user is idle.
Fast flashing red (200ms)	The monitored user receives an incoming call.
Solid red	The monitored user is busy.
Slow flashing red (1s)	The call is parked against the monitored user's phone number. The monitored user's conversation is placed on hold.
Off	The monitored user does not exist.

Line key LED (configured as a BLF key and BLF LED Mode is set to 1)

LED Status	Description
Fast flashing red (200ms)	The monitored user receives an incoming call.
Solid red	The monitored user is busy.
Slow flashing red (1s)	The call is parked against the monitored user's phone number. The monitored user's conversation is placed on hold.
Off	The monitored user is idle. The monitored user does not exist.

Line key LED (configured as a BLF key and BLF LED Mode is set to 2)

LED Status	Description
Fast flashing red (200ms)	The monitored user receives an incoming call.
Solid red	The monitored user is busy.
Slow flashing red (1s)	The call is parked against the monitored user's phone number. The monitored user's conversation is placed on hold.
Off	The monitored user is idle. The monitored user does not exist.

Line key LED (configured as a BLF key and BLF LED Mode is set to 3)

LED Status	Description
Fast flashing red (200ms)	The monitored user receives an incoming call.
Solid red	The monitored user is busy. The monitored user's conversation is placed on hold.
Slow flashing red (1s)	The call is parked against the monitored user's phone number.
Off	The monitored user is idle. The monitored user does not exist.

Procedure

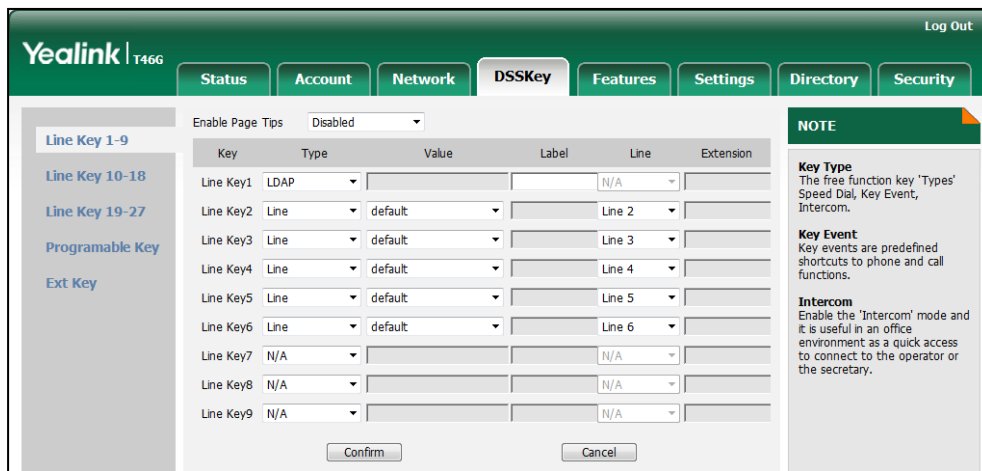
BLF can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Specify whether to use visual alert and audio alert for BLF pickup. For more information, refer to BLF on page 329 .
	y000000000xx.cfg	Assign a BLF key. For more information, refer to BLF Key on page 392 . Configure BLF LED mode. For more information, refer to BLF on page 329 .
Local	Web User Interface	Assign a BLF key. Navigate to: http://<phoneIPAddress>/servlet?p=dsskey&model=1&q=load&linepage=1 Specify whether to use visual alert and audio alert for BLF pickup. Navigate to: http://<phoneIPAddress>/servlet?p=features-callpickup&q=load Configure BLF LED mode. Navigate to: http://<phoneIPAddress>/servlet?p=features-general&q=load

		d
	Phone User Interface	Assign a BLF key.

To configure a BLF key via web user interface:

1. Click on **DSSKey->Line Key**.
2. In the desired DSS key field, select **BLF** from the pull-down list of **Type**.
3. Enter the phone number or extension you want to monitor in the **Value** field.
4. Select the desired line from the pull-down list of **Line**.
5. (Optional.) Enter the directed call pickup code in the **Extension** field.

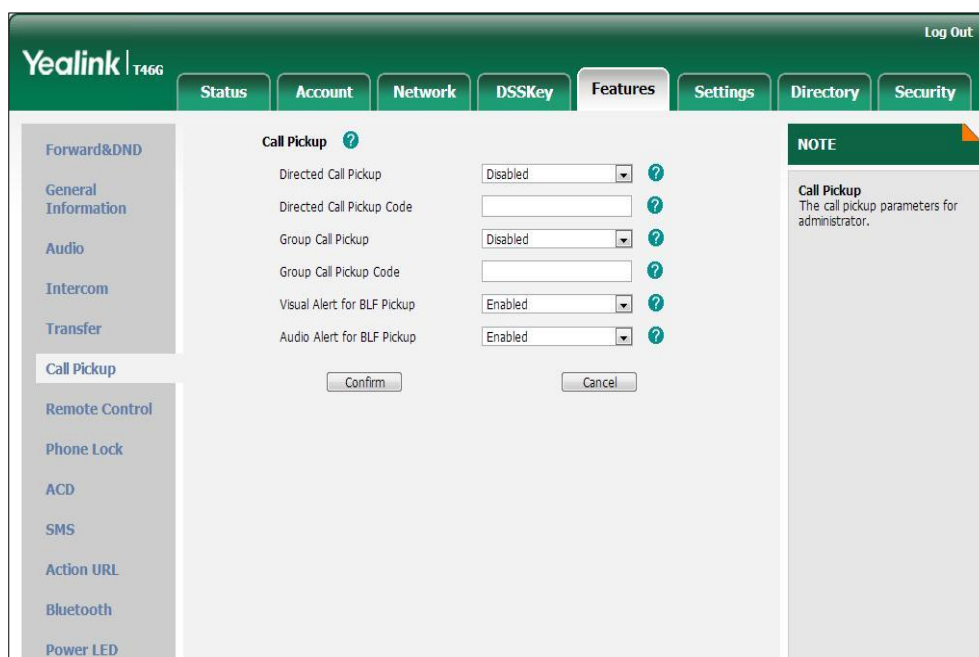


6. Click **Confirm** to accept the change.

To configure visual alert and audio alert features via web user interface:

1. Click on **Features->Call Pickup**.
2. Select the desired value from the pull-down list of **Visual Alert for BLF Pickup**.

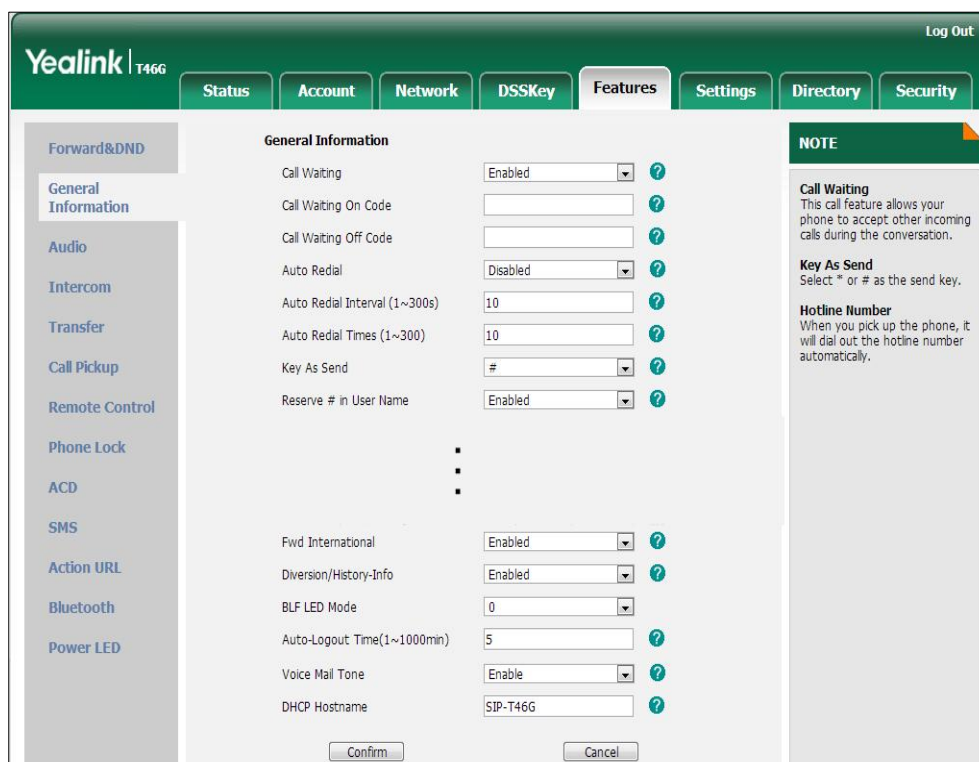
3. Select the desired value from the pull-down list of **Audio Alert for BLF Pickup**.



4. Click **Confirm** to accept the change.





To configure BLF LED mode via web user interface:

1. Click on **Features->General Information**.
2. Select the desired value from the pull-down list of **BLF LED mode**.



3. Click **Confirm** to accept the change.

To configure a BLF key via phone user interface:

1. Press **Menu->Call Features->DSS Keys**.
2. Select the desired DSS key.
3. Press  or  , or the **Switch** soft key to select **BLF** from the **Type** field.
4. Press  or  , or the **Switch** soft key to select the desired line from the **Account ID** field.
5. (Optional.) Enter the string that will appear on the LCD screen in the **Label** field.
6. Enter the phone number or extension you want to monitor in the **Value** field.
7. (Optional.) Enter the directed call pickup code in the **Extension** field.
8. Press the **Save** soft key to accept the change.

Music on Hold

Music on Hold (MoH) is the business practice of playing recorded music to fill the silence that would be heard by the party who has been placed on hold. To use this feature, specify a SIP URI pointing to an MoH server account. When a call is placed on hold, the IP phone will send an INVITE message to the specified MoH server account according to the SIP URI. The MoH server account automatically responds to the INVITE message and immediately plays audio from some source located anywhere (LAN, Internet) to the held party.

Procedure

Music on Hold can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure the MoH feature on a per-line basis. For more information, refer to Music on Hold on page 330.
Local	Web User Interface	Configure the MoH feature on a per-line basis. Navigate to: http://<phoneIPAddress>/servlet ?p=account-adv&q=load&acc=0

To configure MoH via web user interface:

1. Click on **Account**.
2. Select the desired account from the pull-down list of **Account**.
3. Click on **Advanced**.

- Enter the SIP URI (e.g., sip:moh@sip.com) in the **Music Server URI** field.

The screenshot shows the Yealink T466 web interface with the 'Account' tab selected. The 'Account' section is expanded, showing various configuration fields. The 'Music Server URI' field is highlighted in blue and contains the text 'sip:moh@sip.com'. Other fields include 'Keep Alive Type' (Default), 'Keep Alive Interval (Seconds)' (30), 'Local SIP Port' (5062), 'RPort' (Disabled), 'SIP Session Timer T1 (0.5~10s)' (0.5), 'SIP Session Timer T2 (2~40s)' (4), 'SIP Session Timer T4 (2.5~60s)' (5), 'Subscribe Period (Seconds)' (1800), and 'DTMF Type' (RFC2833). There are also fields for 'Directed Call Pickup Code', 'Group Call Pickup Code', 'Distinctive Ring Tones' (Disabled), 'Unregister When Reboot' (Disabled), and 'Out Dialog BLF' (Disabled). A 'NOTE' box on the right indicates that these are advanced parameters for administrators. 'Confirm' and 'Cancel' buttons are at the bottom.

- Click **Confirm** to accept the change.

Automatic Call Distribution

Automatic Call Distribution (ACD) enables organizations to manage a large number of phone calls on an individual basis. ACD enables the use of IP phones in a call-center role by automatically distributing incoming calls to available users, or agents. ACD depends on support from a SIP server. ACD is disabled on the phone by default. You need to enable it on a per-line basis before logging into the ACD system.

After the IP phone user logs into the queue, the server monitors the phone status and then decides whether to assign an incoming call to the user's IP phone. When the phone status is changed to unavailable, the server stops distributing calls to the IP phone. The IP phone will remain in the unavailable status until the IP phone user manually changes the phone status or the ACD auto available timer (if configured) expires. How long the IP phone remains unavailable is configurable by the auto available timer. When the timer expires, the phone status is automatically changed to available. The ACD auto available timer feature depends on support from a SIP server.

You need to configure an ACD key for the user to log into the ACD system. The ACD key LED on the IP phone can indicate the ACD status.

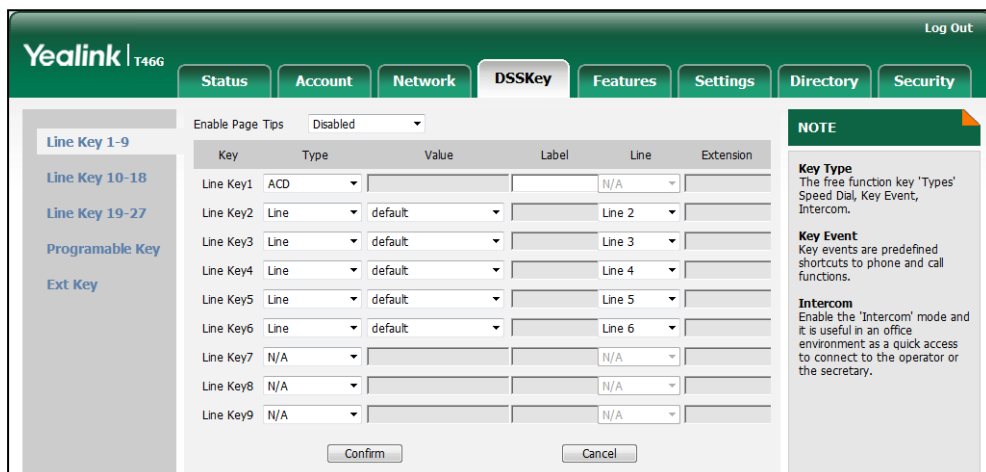
Procedure

ACD can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure ACD. For more information, refer to ACD on page 331.
	<y0000000000xx>.cfg	Assign an ACD key. For more information, refer to ACD Key on page 393. Configure ACD auto available timer. For more information, refer to ACD on page 331.
Local	Web User Interface	Assign an ACD key. Navigate to: http://<phoneIPAddress>/servlet? p=dsskey&model=1&q=load&linepage=1 Configure ACD auto available timer. Navigate to: http://<phoneIPAddress>/servlet? p=features-acd&q=load
	Phone User Interface	Assign an ACD key.

To configure an ACD key via web user interface:

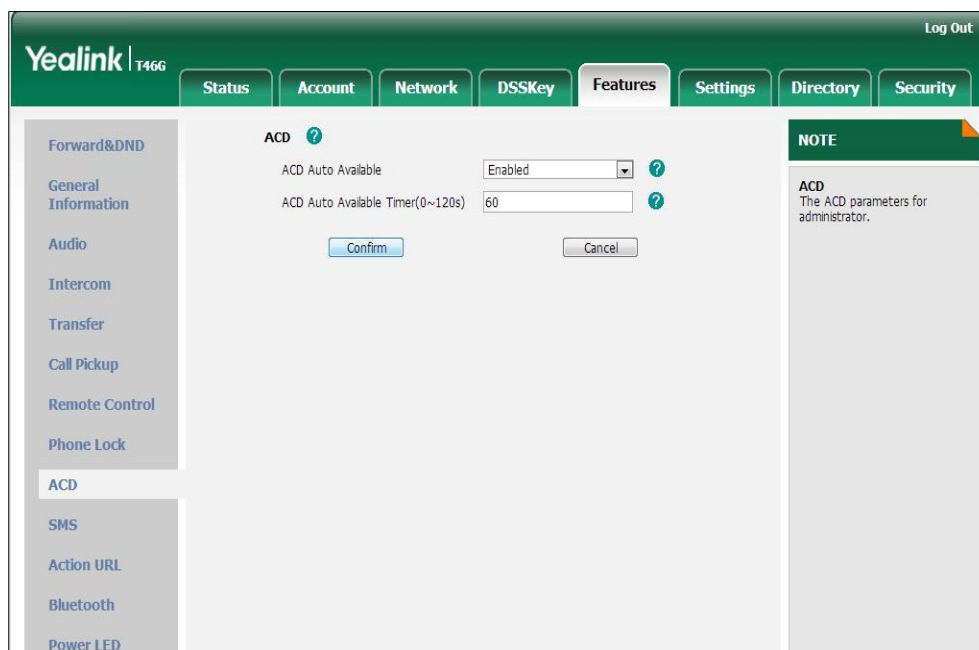
1. Click on **DSSKey->Line Key**.
2. In the desired DSS key field, select **ACD** from the pull-down list of **Type**.



3. Click **Confirm** to accept the change.

To configure the ACD auto available timer feature via web user interface:

1. Click on **Features->ACD**.
2. Select the desired value from the pull-down list of **ACD Auto Available**.
3. Enter the desired timer in the **ACD Auto Available Timer (0~120s)** field.



4. Click **Confirm** to accept the change.

To configure an ACD key via phone user interface:

1. Press **Menu->Call Features->DSS Keys**.
2. Select the desired DSS key.
3. Press **◀** or **▶**, or the **Switch** soft key to select **ACD** from the **Type** field.
4. (Optional.) Enter the string that will appear on the LCD screen in the **Label** field.
5. Press the **Save** soft key to accept the change.

Message Waiting Indicator

Message Waiting Indicator (MWI) informs users of the number of messages waiting in their mailbox without calling the mailbox. IP phones support both audio and visual MWI when receiving new voice messages.

IP phones support both solicited and unsolicited MWI. Unsolicited MWI is a server related feature.

IP phone sends a SUBSCRIBE message to the server for message-summary updates. The server sends a message-summary NOTIFY within the subscription dialog each time the MWI status changes. For solicited MWI, you must enable the MWI subscription

feature on IP phones. IP phones can subscribe the MWI messages to the account or the voice mail number.

IP phones do not need to subscribe to message-summary updates. The server automatically sends a message-summary NOTIFY in a new dialog each time the MWI status changes.

Procedure

Configuration changes can be performed using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure subscribe for MWI. Configure subscribe MWI to voice mail. For more information, refer to Message Waiting Indicator on page 332.
Local	Web User Interface	Configure subscribe for MWI. Configure subscribe MWI to voice mail. Navigate to: http://<phoneIPAddress>/servlet ?p=account-adv&q=load&acc= 0

To configure subscribe for MWI via web user interface:

1. Click on **Account**.
2. Select the desired account from the pull-down list of **Account**.
3. Click on **Advanced**.
4. Select the desired value from the pull-down list of **Subscribe for MWI**.

- Enter the period time in the **MWI Subscription Period (Seconds)** field.

Account	Account 1
Keep Alive Type	Default
Keep Alive Interval (Seconds)	30
Local SIP Port	5062
RPort	Disabled
SIP Session Timer T1 (0.5~10s)	0.5
SIP Session Timer T2 (2~40s)	4
SIP Session Timer T4 (2.5~60s)	5
Subscribe Period (Seconds)	1800
DTMF Type	RFC2833
DTMF Info Type	DTMF-Relay
DTMF Payload Type(96~255)	101
Retransmission	Disabled
Subscribe for MWI	Enabled
MWI Subscription Period(Seconds)	3600
Subscribe MWI To Voice Mail	Disabled
Voice Mail	

- Click **Confirm** to accept the change.

The IP phone will subscribe to the account number for MWI service by default.

To configure subscribe MWI to voice mail via web user interface:

- Click on **Account**.
- Select the desired account from the pull-down list of **Account**.
- Click on **Advanced**.
- Select the desired value from the pull-down list of **Subscribe MWI to Voice Mail**.
- Enter the desired voice number in the **Voice Mail** field.

Account	Account 1
Keep Alive Type	Default
Keep Alive Interval (Seconds)	30
Local SIP Port	5062
RPort	Disabled
SIP Session Timer T1 (0.5~10s)	0.5
SIP Session Timer T2 (2~40s)	4
SIP Session Timer T4 (2.5~60s)	5
Subscribe Period (Seconds)	1800
DTMF Type	RFC2833
DTMF Info Type	DTMF-Relay
DTMF Payload Type(96~255)	101
Retransmission	Disabled
Subscribe for MWI	Enabled
MWI Subscription Period(Seconds)	3600
Subscribe MWI To Voice Mail	Enabled
Voice Mail	1234

- Click **Confirm** to accept the change.

Multicast Paging

Multicast paging allows IP phones to send/receive Real-time Transport Protocol (RTP) streams to/from the pre-configured multicast address(es) without involving SIP signaling. Up to 10 listening multicast addresses can be specified on the IP phone.

Sending RTP Stream

Users can send an RTP stream without involving SIP signaling by pressing a configured multicast paging key. A multicast address (IP: Port) should be assigned to the multicast paging key, which is defined to transmit RTP stream to a group of designated IP phones. When the IP phone sends the RTP stream to a pre-configured multicast address, each IP phone that preconfigured to listen to the multicast address can receive the RTP stream. When the originator stops sending the RTP stream, the subscribers stop receiving it.

Procedure

Configuration changes can be performed using the configuration files or locally.

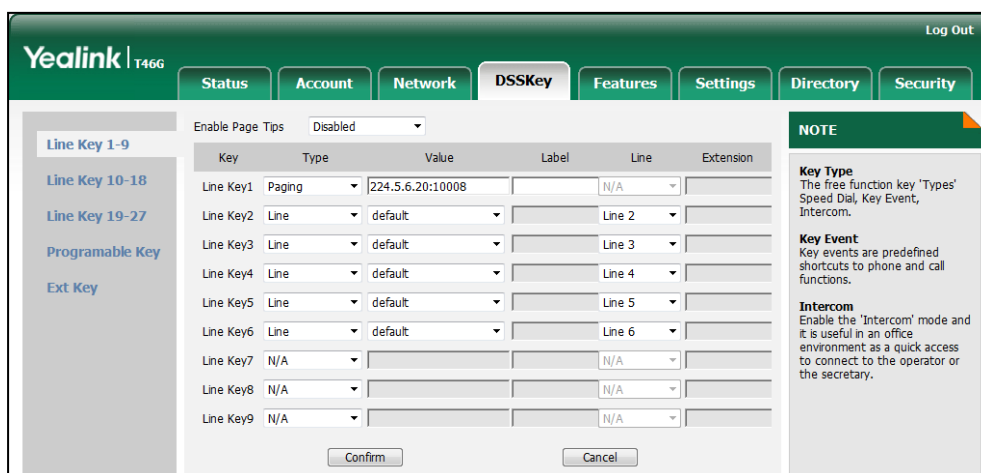
Configuration File	<y0000000000xx>.cfg	<p>Assign a multicast paging key.</p> <p>For more information, refer to Multicast Paging Key on page 394.</p> <p>Specify a multicast codec for the IP phone to use for multicast RTP.</p> <p>For more information, refer to Sending RTP Stream on page 334.</p>
Local	Web User Interface	<p>Assign a multicast paging key.</p> <p>Navigate to: http://<phoneIPAddress>/servlet?p=dsskey&model=1&q=load&linepage=1</p> <p>Specify a multicast codec for the IP phone to use to send the RTP stream.</p> <p>Navigate to: http://<phoneIPAddress>/servlet?p=features-general&q=load</p>
	Phone User Interface	Assign a multicast paging key.

To configure a multicast paging key via web user interface:

1. Click on **DSSKey->Line Key**.

- In the desired DSS key field, select **Paging** from the pull-down list of **Type**.
- Enter the multicast IP address and port number in the **Value** field.

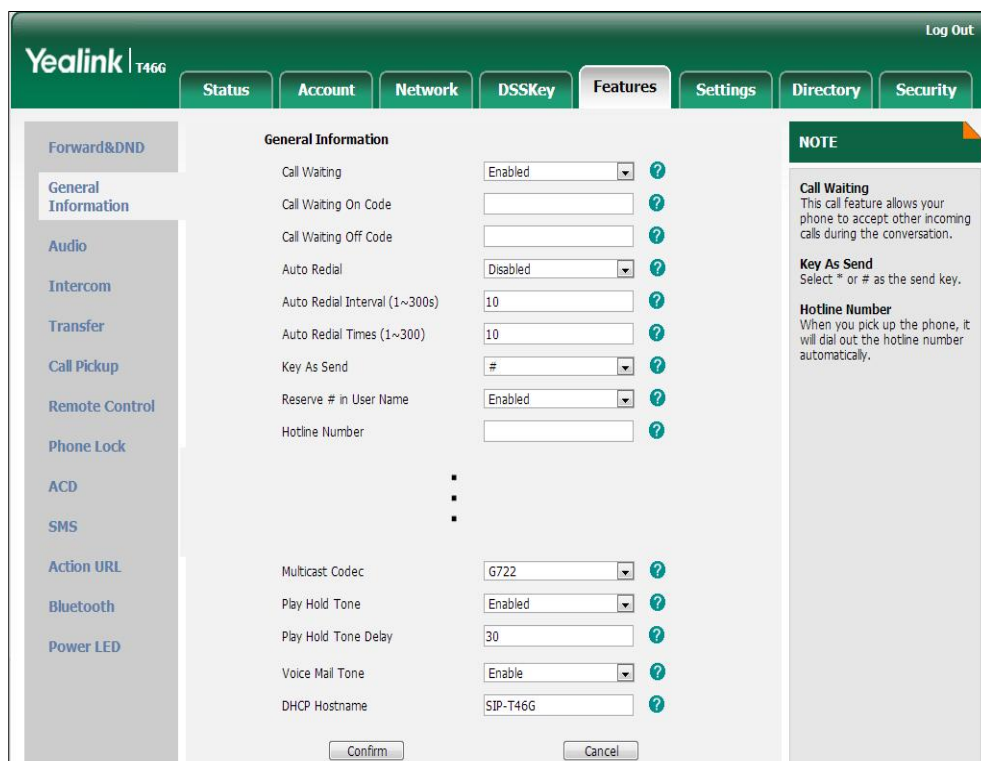
The valid multicast IP addresses range from 224.0.0.0 to 239.255.255.255.



- Click **Confirm** to accept the change.

To configure a codec for multicast paging via web user interface:

- Click on **Features** ->**General Information**.
- Select the desired codec from the pull-down list of **Multicast Codec**.



- Click **Confirm** to accept the change.

To configure a multicast paging key via phone user interface:

1. Press **Menu->Call Features->DSS Keys**.
2. Select the desired DSS key.
3. Press **◀** or **▶** , or the **Switch** soft key to select **Key Event** from the **Type** field.
4. Press **◀** or **▶** , or the **Switch** soft key to select **Multicast Paging** from the **Key Event** field.
5. (Optional.) Enter the string that will appear on the LCD screen in the **Label** field.
6. Enter the multicast IP address and port number in the **Value** field.
7. Press the **Save** soft key to accept the change.

Receiving RTP Stream

IP phones can receive an RTP stream from the pre-configured multicast address(es) without involving SIP signaling, and can handle the incoming multicast paging calls differently depending on the configurations of Paging Barge and Paging Priority Active.

Paging Barge

This parameter defines the priority of the voice call in progress, and decides how the IP phone handles the incoming multicast paging calls when there is already a voice call in progress. If the parameter is configured as disabled, all incoming multicast paging calls will be automatically ignored. If the parameter is the priority value, the incoming multicast paging calls with higher priority are automatically answered and the ones with lower priority are ignored.

Paging Priority Active

This parameter decides how the IP phone handles the incoming multicast paging calls when there is already a multicast paging call in progress. If the parameter is configured as disabled, the IP phone will automatically ignore all incoming multicast paging calls. If the parameter is configured as enabled, an incoming multicast paging call with higher priority is automatically answered, and the one with lower priority is ignored.

Procedure

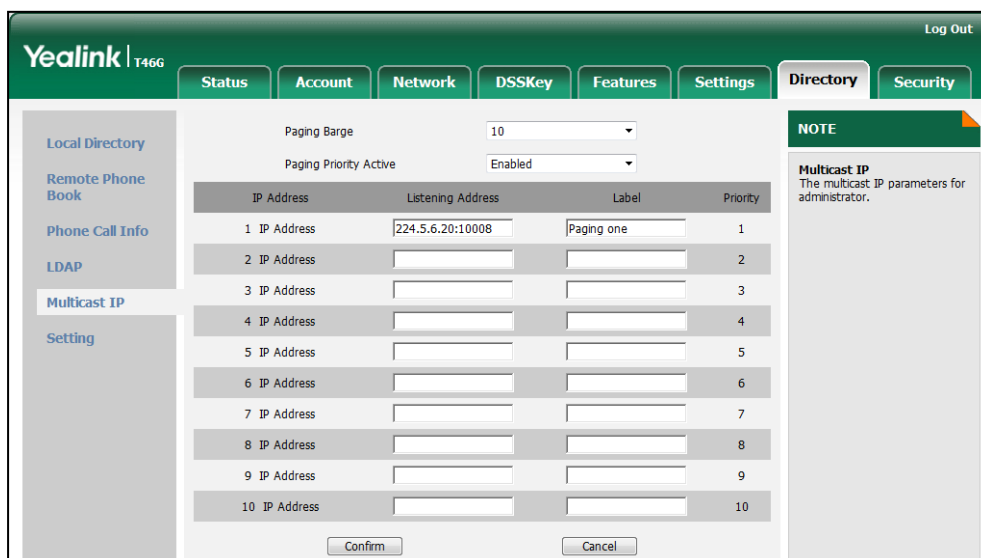
Configuration changes can be performed using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	<p>Configure the listening multicast address.</p> <p>Configure the Paging Barge and Paging Priority Active features.</p> <p>For more information, refer to Receiving RTP Stream on page 334.</p>
---------------------------	---------------------	--

<p>Local</p>	<p>Web User Interface</p>	<p>Configure the listening multicast address.</p> <p>Configure the Paging Barge and Paging Priority Active features.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet?p=contacts-multicastIP&q=load</p>
---------------------	---------------------------	--

To configure a listening multicast address via web user interface:

1. Click on **Directory->Multicast IP**.
2. Enter the listening multicast address and port number in the **Listening Address** field.
1 is the highest priority and 10 is the lowest priority.
3. Enter the label in the **Label** field.
The label will appear on the LCD screen when receiving the RTP multicast.



4. Click **Confirm** to accept the change.

To configure the paging barge and paging priority active features via web user interface:

1. Click on **Directory->Multicast IP**.
2. Select the desired value from the pull-down list of **Paging Barge**.

- Select the desired value from the pull-down list of **Paging Priority Active**.

IP Address	Listening Address	Label	Priority
1 IP Address	224.5.6.20:10008	Paging one	1
2 IP Address			2
3 IP Address			3
4 IP Address			4
5 IP Address			5
6 IP Address			6
7 IP Address			7
8 IP Address			8
9 IP Address			9
10 IP Address			10

- Click **Confirm** to accept the change.

Call Recording

Call recording enables users to record calls. It depends on support from a SIP server. When the user presses the call record key, the IP phone sends a record request to the server. IP phones themselves do not have memory to store the recording, what they can do is to trigger the recording and indicate the recording status.

Normally, there are 2 main methods to trigger a recording on a certain server. We call them record and URL record. Record is for the IP phone to send the server a SIP INFO message containing a specific header. URL record is for the IP phone to send the server an HTTP GET message containing a specific URL. The server processes these messages and decides to start or stop a recording.

Record

When a user presses a record key for the first time during a call, the IP phone sends a SIP INFO message to the server with the specific header "Record: on", and then the recording starts.

Example of a SIP INFO message:

```
Via: SIP/2.0/UDP 10.1.4.148:5063;branch=z9hG4bK1139980711
From: "827" <sip:827@192.168.1.199>;tag=2066430997
To: <sip:614@192.168.1.199>;tag=371745247
Call-ID: 1895019940@10.1.4.148
CSeq: 2 INFO
Contact: <sip:827@10.1.4.148:5063>
Max-Forwards: 70
```

```
User-Agent: Yealink SIP-T46G 28.72.0.1
Record: on
Content-Length: 0
```

When the user presses the record key for the second time, the IP phone sends a SIP INFO message to the server with the specific header "Record: off", and then the recording stops.

Example of a SIP INFO message:

```
Via: SIP/2.0/UDP 10.1.4.148:5063;branch=z9hG4bK1619489730
From: "827" <sip:827@192.168.1.199>;tag=1831694891
To: <sip:614@192.168.1.199>;tag=2228378244
Call-ID: 1051886688@10.1.4.148
CSeq: 3 INFO
Contact: <sip:827@10.1.4.148:5063>
Max-Forwards: 70
User-Agent: Yealink SIP-T46G 28.72.0.1
Record: off
Content-Length: 0
```

URL Record

When a user presses a URL record key for the first time during a call, the IP phone sends an HTTP GET message to the server.

Example of an HTTP GET message:

```
Get /phonerecording.cgi?model=yealink HTTP/1.0\r\n
Request Method: GET
Request URI: /phonerecording.cgi?model=yealink
Request version: HTTP/1.0
Host: 10.1.2.224\r\n
User-agent: yealink SIP-T46G 28.72.0.1 00:16:65:11:30:68\r\n
```

If the recording is successfully started, the server will respond with a 200 OK message.

Example of a 200 OK message:

```
<YealinkIPPhoneText>
<Title>
  </Title>
<Text>
  The recording session is successfully started.
</Text>
</YealinkIPPhoneText>
```

If the recording fails for some reasons, for example, the recording box is full, the server will respond with a 200 OK message.

Example of a 200 OK message:

```
<YealinkIPPhoneText>
<Title>
  </Title>
<Text>
  Probably the recording box is full.
</Text>
</YealinkIPPhoneText>
```

When the user presses the URL record key for the second time, the IP phone sends an HTTP GET message to the server, and then the server will respond with a 200 OK message.

Example of a 200 OK message:

```
<YealinkIPPhoneText>
<Title>
  </Title>
<Text>
  The recording session is successfully stopped.
</Text>
</YealinkIPPhoneText>
```

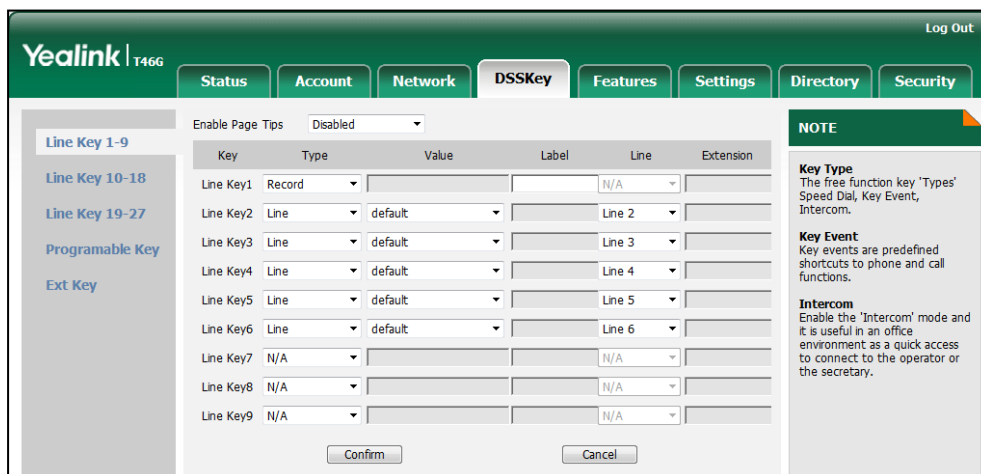
Procedure

Call recording key can be configured using the configuration files or locally.

<p>Configuration File</p>	<p><y0000000000xx>.cfg</p>	<p>Assign a record key. For more information, refer to Record Key on page 394. Assign a URL record key. For more information, refer to URL Record Key on page 395.</p>
<p>Local</p>	<p>Web User Interface</p>	<p>Assign a record key. Assign a URL record key. Navigate to: http://<phoneIPAddress>/servlet?p=dsskey&model=1&q=load&linepage=1</p>
	<p>Phone User Interface</p>	<p>Assign a record key. Assign a URL record key.</p>

To configure a record key via web user interface:

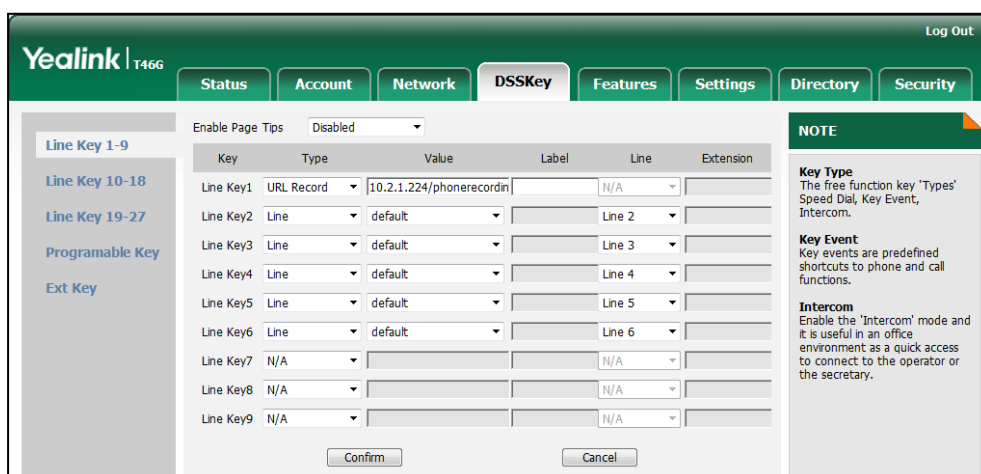
1. Click on **DSSKey->Line Key**.
2. In the desired DSS key field, select **Record** from the pull-down list of **Type**.



3. Click **Confirm** to accept the change.

To configure a URL record key via web user interface:

1. Click on **DSSKey->Line Key**.
2. In the desired DSS key field, select **URL Record** from the pull-down list of **Type**.
3. Enter the URL in the **Value** field.



4. Click **Confirm** to accept the change.

To configure a record key via phone user interface:

1. Press **Menu->Call Features->DSS Keys**.
2. Select the desired DSS key.
3. Press **◀** or **▶**, or the **Switch** soft key to select **Key Event** from the **Type** field.
4. Press **◀** or **▶**, or the **Switch** soft key to select **Record** from the **Key Event** field.

5. (Optional.) Enter the string that will appear on the LCD screen in the **Label** field.
6. Press the **Save** soft key to accept the change.

To configure a URL record key via phone user interface:

1. Press **Menu->Call Features->DSS Keys**.
2. Select the desired DSS key.
3. Press **◀** or **▶** , or the **Switch** soft key to select **URL Record** from the **Type** field.
4. Enter the URL in the **URL Record** field.
5. (Optional.) Enter the string that will appear on the LCD screen in the **Label** field.
6. Press the **Save** soft key to accept the change.

Hot Desking

Hot desking originates from the definition of being the temporary physical occupant of a work station or surface by a particular employee. A primary motivation for hot desking is cost reduction. Hot desking is regularly used in places where not all the employees are in the office at the same time, or not in the office for a long time, which means actual personal offices would often be vacant, consuming valuable space and resources.

The hot desking feature allows a user to clear registration configurations of all accounts on the IP phone, and then register his account on line 1. To use this feature, you need to assign a hot desking key.

Procedure

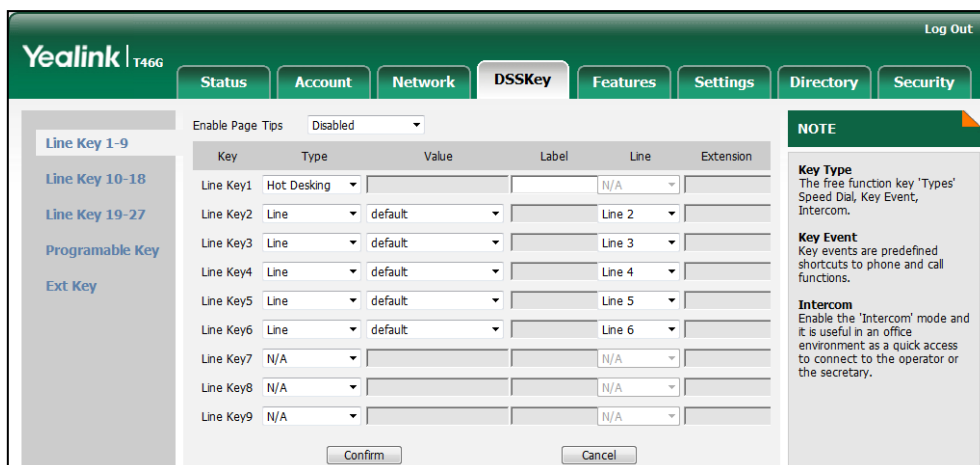
Hot desking key can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Assign a hot desking key. For more information, refer to Hot Desking Key on page 395.
Local	Web User Interface	Assign a hot desking key. Navigate to: http://<phoneIPAddress>/servlet ?p=dsskey&q=load&model=1
	Phone User Interface	Assign a hot desking key.

To configure a hot desking key via web user interface:

1. Click on **DSSKey->Line Keys**.

- In the desired DSS key field, select **Hot Desking** from the pull-down list of **Type**.



- Click **Confirm** to accept the change.

To configure a hot desking key via phone user interface:

- Press **Menu->Call Features->DSS Keys**.
- Select the desired DSS key.
- Press **◀** or **▶**, or the **Switch** soft key to select **Key Event** from the **Type** field.
- Press **◀** or **▶**, or the **Switch** soft key to select **Hot Desking** from the **Key Event** field.
- (Optional.) Enter the string that will appear on the LCD screen in the **Label** field.
- Press the **Save** soft key to accept the change.

Action URL

Action URL allows IP phones to interact with web server applications by sending an HTTP or HTTPS GET request. You can specify a URL that triggers a GET request when a specified event occurs. Action URL can only be triggered by the pre-defined events (e.g., log on). The valid URL format is: http(s)://IP address of the server/help.xml?.

The following table lists the pre-defined events for action URL.

Event	Description
Setup Completed	When the IP phone completes startup.
Registered	When the IP phone successfully registers an account.
Unregistered	When the IP phone logs off the registered account.
Register Failed	When the IP phone fails to register an account.
Off Hook	When the IP phone is off hook.
On Hook	When the IP phone is on hook.

Event	Description
Incoming Call	When the IP phone receives an incoming call.
Outgoing Call	When the IP phone places a call.
Established	When the IP phone establishes a call.
Terminated	When the IP phone terminates a call.
Open DND	When the IP phone enables the DND mode.
Close DND	When the IP phone disables the DND mode.
Open Always Forward	When the IP phone enables the always forward.
Close Always Forward	When the IP phone disables the always forward.
Open Busy Forward	When the IP phone enables the busy forward.
Close Busy Forward	When the IP phone disables the busy forward.
Open No Answer Forward	When the IP phone enables the no answer forward.
Close No Answer Forward	When the IP phone disables the no answer forward
Transfer Call	When the IP phone transfers a call.
Blind Transfer	When the IP phone blind transfers a call.
Attended Transfer	When the IP phone performs the attended transfer.
Hold	When the IP phone places a call on hold.
UnHold	When the IP phone retrieves a hold call.
Mute	When the IP phone mutes a call.
UnMute	When the IP phone unmutes a call.
Missed Call	When the IP phone misses a call.
IP Changed	When the IP address of the IP phone changes.
Forward Incoming Call	When the IP phone forwards an incoming call.
Reject Incoming Call	When the IP phone rejects an incoming call.
Answer New-In Call	When the IP phone answers a new call.
Transfer Finished	When the IP phone completes to transfer a call.
Transfer Failed	When the IP phone fails to transfer a call.
Idle to Busy	When the state of the IP phone changes from idle to busy.
Busy to Idle	When the state of phone changes from busy to idle.

An HTTP or HTTPS GET request may contain variable name and variable value, separated by “=”. Each variable value starts with \$ in the query part of the URL. The valid URL format is: `http(s)://IP address of server/help.xml?variable name=$variable`

value. Variable name can be customized by users, while the variable value is pre-defined. For example, a URL "*http://192.168.1.10/help.xml?mac=\$mac*" is specified for the event Mute, \$mac will be dynamically replaced with the MAC address of the IP phone when the IP phone mutes a call.

The following table lists the pre-defined variable values.

Variable Value	Description
\$mac	MAC address of the IP phone
\$ip	The current IP address of the IP phone
\$model	Phone model
\$firmware	Phone firmware version
\$active_url	The SIP URI of the current account when the IP phone places a call, receives an incoming call or establishes a call.
\$active_user	The user part of the SIP URI for the current account when the IP phone places a call, receives an incoming call or establishes a call.
\$active_host	The host part of the SIP URI for the current account when the IP phone places a call, receives an incoming call or establishes a call.
\$local	The SIP URI of the caller when the IP phone places a call. The SIP URI of the callee when the IP phone receives an incoming call.
\$remote	The SIP URI of the callee when the IP phone places a call. The SIP URI of the caller when the IP phone receives an incoming call.
\$display_local	The display name of the caller when the IP phone places a call. The display name of the callee when the IP phone receives an incoming call.
\$display_remote	The display name of the callee when the IP phone places a call. The display name of the caller when the IP phone receives an incoming call.
\$call_id	The call-id of the active call.

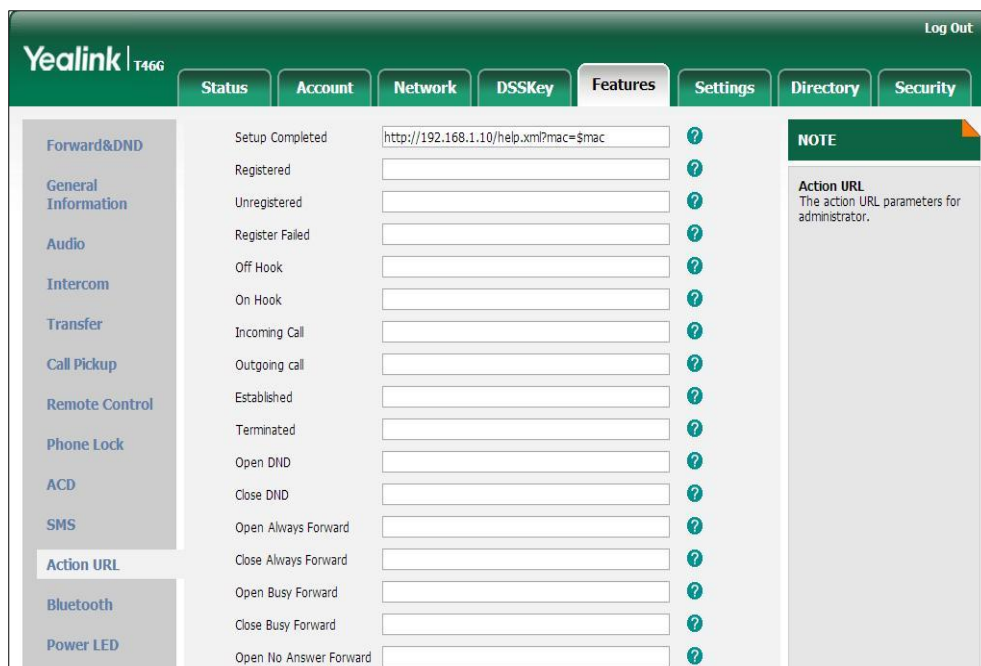
Procedure

Action URL can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure the action URL on the IP phone. For more information, refer to Action URL on page 336.
Local	Web User Interface	Configure the action URL on the IP phone. Navigate to: http://<phoneIPAddress>/servlet?p=features-actionurl&q=load

To configure action URL via web user interface:

1. Click on **Features->Action URL**.
2. Enter the action URLs in the corresponding fields.



3. Click **Confirm** to accept the change.

Action URI

Opposite to action URL, action URI allows IP phones to interact with web server application by receiving and handling an HTTP or HTTPS GET request. When receiving a GET request, the IP phone will perform the specified action and respond with a 200 OK

message. A GET request may contain variable named as "key" and variable value, which are separated by "=". The valid URI format is:

http(s)://phone IP address/servlet?key=variable value.

The following table lists the pre-defined variable values.

Variable Value	Phone Action
OK	Press the OK key.
ENTER	Press the Enter soft key
SPEAKER	Press the Speaker key.
F_TRANSFER	Press the TRANSFER key (only for SIP-T46G) or the Transfer soft key.
VOLUME_UP	Increase the volume.
VOLUME_DOWN	Decrease the volume.
MUTE	Press the MUTE key.
F_HOLD	Press the HOLD key (only for SIP-T46G) or the Hold soft key.
X	Press the X key.
CANCEL	Return to a previous screen or cancel a call.
0-9/*/POUND	Send the DTMF digit (0-9, * or #).
L1-LX	Press the line key (for SIP-T46G, X=27, for SIP-T42G/T41P, X=15).
F_CONFERENCE	Press the Conference soft key.
F1-F4	Press the soft key.
MSG	Press the MESSAGE key.
HEADSET	Press the HEADSET key.
RD	Press the REDIAL key.
UP/DOWN/LEFT/RIGHT	Press the Navigation keys.
Reboot	Reboot the IP phone.
AutoP	Let the IP phone perform auto provisioning.
DNDOon	Activate the DND mode.
DNDOff	Deactivate the DND mode.
number=xxx&outgoing_uri=y	Place a call to xxx from SIP URI y.
OFFHOOK	Pick up the handset.
ONHOOK	Hang up the handset.

Variable Value	Phone Action
ANSWER	Answer a call.
Reset	Reset a phone.
ATrans=xxx	Perform a semi-attended/attended transfer to xxx.
BTrans=xxx	Perform a blind transfer to xxx.
CALLEND	End a call.

Note

The variable value is not applicable to all events. For example, the variable value "MUTE" is only applicable when the IP phone is during a call.

When authentication is required, you must enter "p=login&q=login&username=xxx&pwd=yyy&jumpto=URI&" before the variable "key". xxx refers to the login user name and yyy refers to the login password.

For security reasons, IP phones do not receive and handle the HTTP/HTTPS GET requests by default. You need to specify the trusted IP address for action URI. When the IP phone receives a GET request from the specified IP address for the first time, the LCD screen prompts the message "Allow Remote Control?". You can specify one or more trusted IP addresses on the IP phone, or configure the IP phone to receive and handle the URI from any IP address.

Procedure

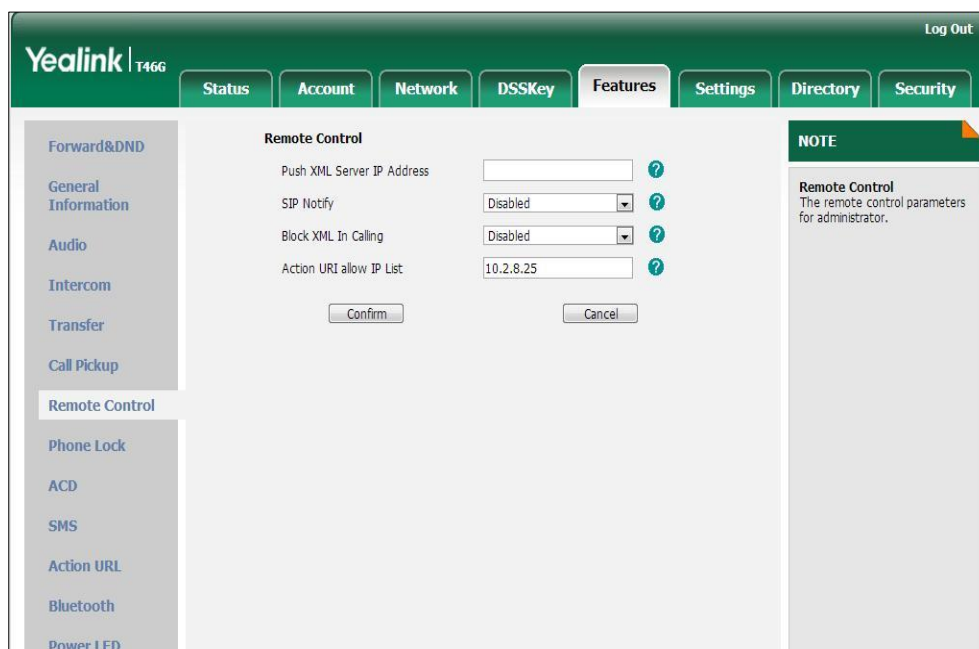
Specify the trusted IP address for Action URI using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Specify the trusted IP address(es) for sending the Action URI to the IP phone. For more information, refer to Action URI on page 337 .
Local	Web User Interface	Specify the trusted IP address(es) for sending the Action URI to the IP phone. Navigate to: http://<phoneIPAddress>/servlet?p=features-remotecontrl&q=load

To configure the trusted IP address(es) for Action URI via web user interface:

1. Click on **Features->Remote Control**.

- Enter the IP address or any in the **Action URI allow IP List** field.
Multiple IP addresses are separated by commas. If you enter "any" in this field, the IP phone can receive and handle GET requests from any IP address. If you leave the field blank, the IP phone cannot receive or handle any HTTP GET request.



- Click **Confirm** to accept the change.

Server Redundancy

Server redundancy is often required in VoIP deployments to ensure continuity of phone service, for events where the server needs to be taken offline for maintenance, the server fails, or the connection between the IP phone and the server fails.

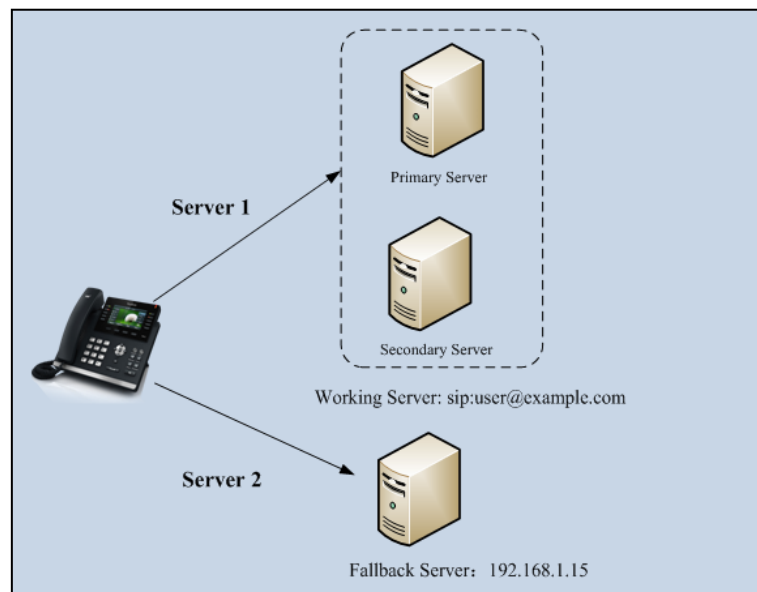
Two types of redundancy are possible. In some cases, a combination of the two may be deployed:

- Failover:** In this mode, the full phone system functionality is preserved by having a second equivalent capability call server take over from the one that has gone down/off-line. This mode of operation should be done using the DNS mechanisms from the primary to the secondary server.
- Fallback:** In this mode, a second less featured call server (fallback server) with SIP capability takes over call control to provide basic calling capability, but without some of the advanced features offered by the working server (for example, shared lines, call recording and MWI). IP phones support configuration of two SIP servers per SIP registration for fallback purpose.

Phone Configuration for Redundancy Implementation

To assist in explaining the redundancy behavior, an illustrative example of how an IP

phone may be configured is shown as below. In the example, server redundancy for fallback and failover purposes is deployed. Two separate SIP servers (a working server and a fallback server) are configured for per line registration.



Working Server: Server 1 is configured with the domain name of the working server. For example, sip:user@example.com. DNS mechanism is used such that the working server is capable of resolving to multiple physical SIP servers for failover purpose. The working server is deployed in redundant pairs, designated as primary and secondary servers. The primary server is the highest priority server in a cluster of servers resolved by the DNS server. The secondary server backs up a primary server when the primary server fails and offers the same functionality as the primary server.

Fallback Server: Server 2 is configured with the address of the fallback server. For example, 192.168.1.15. A fallback server offers less functionality than the working server.

Phone Registration

Two registration methods for fallback mode:

- **Concurrent registration:** The IP phone registers to two SIP servers (working server and fallback server) at the same time. In a failure situation, a fallback server can take over the basic calling capability, but without some advanced features offered by the working server (default registration method).
- **Successive registration:** The IP phone only registers to one server at a time. The IP phone first registers to the working server. In a failure situation, the IP phone registers to the fallback server.

When registering to the working server, the IP phone must always register to the primary server first except in failover conditions. When the primary server registration is unavailable, the secondary server will serve as the working server.

Procedure

Server redundancy can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure the server redundancy on the IP phone. For more information, refer to Server Redundancy on page 338.
Local	Web User Interface	Configure the server redundancy on the IP phone. Navigate to: http://<phoneIPAddress>/servlet?p=account-register&q=load&acc=0

SIP Server Domain Name Resolution

If a domain name is configured for a SIP server, the IP address(es) associated with that domain name will be discovered through DNS as specified by RFC 3263. The DNS query involves NAPTR, SRV and A queries, which allows the IP phone to adapt to various deployment environments. The IP phone performs the NAPTR query for the SRV pointer and service type (UDP, TCP and TLS), the SRV query on the record returned from the NAPTR for the host name and the port number, and the A query for the IP addresses.

If a port is set to 0 and the transport type is set to DNS-NAPTR, NAPTR and SRV queries will be tried before falling back to A query. If no port is found through the DNS query, 5060 will be used. If an explicit port (except 0) is specified and the transport type is set to DNS-NAPTR, the only lookup will be an A query.

The following details the procedures of DNS query for the IP phone to resolve the domain name of working server into the IP address, port and transport protocol.

NAPTR (Naming Authority Pointer)

First, the IP phone sends the NAPTR query to get the SRV pointer and service type. The IP phone performs a NAPTR query for the domain name. Example of NAPTR records:

	order	pref	flags	service	regexp	replacement
IN NAPTR	90	50	"s"	"SIP+D2T"	""	_sip._tcp.example.com
IN NAPTR	100	50	"s"	"SIP+D2U"	""	_sip._udp.example.com

Parameters are explained in the following table:

Parameter	Description
order	Specify preferential treatment for the specific record. The order is from lowest to highest, lower order is MORE preferred.
pref	Specify the preference for processing multiple NAPTR records with the same order value. Lower value is MORE preferred.
flags	The flag "s" means to perform an SRV lookup.
service	Specify the transport protocols supported by the domain server: SIP+D2U: SIP over UDP SIP+D2T: SIP over TCP SIP+D2S: SIP over SCTP SIPS+D2T: SIPS over TCP
regexp	Always empty for SIP services.
replacement	Specify a domain name for the next query.

The IP phone picks the first record, because its order of 90 is lower than 100. The pref parameter is unimportant as there is no other record with order 90. The flag "s" indicates performing the SRV query next. TCP will be used, targeted to a host determined by an SRV query of "_sip._tcp.example.com". If the flag of the NAPTR record returned is empty, the IP phone will perform the NAPTR query again according to the previous NAPTR query result.

SRV (Service Location Record)

The IP phone performs a SRV query on the record returned from the NAPTR for the host name and the port number. Example of SRV records:

	Priority	Weight	Port	Target
IN SRV	0	1	5060	server1.example.com
IN SRV	0	2	5060	server2.example.com

Parameters are explained in the following table:

Parameter	Description
Priority	Specify preferential treatment for the specific host entry. Lower priority is MORE preferred.
Weight	When priorities are equal, weight is used to differentiate the preference. The preference is from highest to lowest. Keep the same to load balance.
Port	Identify the port number to be used.
Target	Identify the actual host for an A query.

SRV query returns two records. The two SRV records point to different hosts and have the same priority 0. The weight of the second record is higher than the first one, so the second record will be picked first. The two records also contain a port “5060”, the IP phone uses this port. If the Target is not a numeric IP address, the IP phone performs the A query. So in this case, the IP phone uses “server1.example.com” and “server2.example.com” for the A query.

A (Host IP Address)

The IP phone performs A query for the IP address of the target host name. Example of A records:

IN A 62.10.1.10

INA 62.10.1.20

The IP phone picks the IP address “62.10.1.20” first.

Outgoing Call When the Working Server Connection Fails

When a user initiates a call, the phone will go through the following steps to connect the call:

1. Sends the INVITE request to the primary server.
2. If the primary server does not respond correctly to the INVITE, then tries to make the call using the secondary server.
3. If the secondary server is also unavailable, the IP phone will try the fallback server until it either succeeds in making a call or exhausts all servers at which point the call will fail.

At the start of a call, server availability is determined by SIP signaling failure. SIP signaling failure depends on the SIP protocol being used as described below:

- If TCP is used, then the signaling fails if the connection or the send fails.
- If UDP is used, then the signaling fails if ICMP is detected or if the signal times out. If the signaling has been attempted through all servers in the list and this is the last server, then the signaling fails after the complete UDP timeout defined in RFC 3261. If it is not the last server in the list, the maximum number of retries depends on the configured retry count.

Procedure

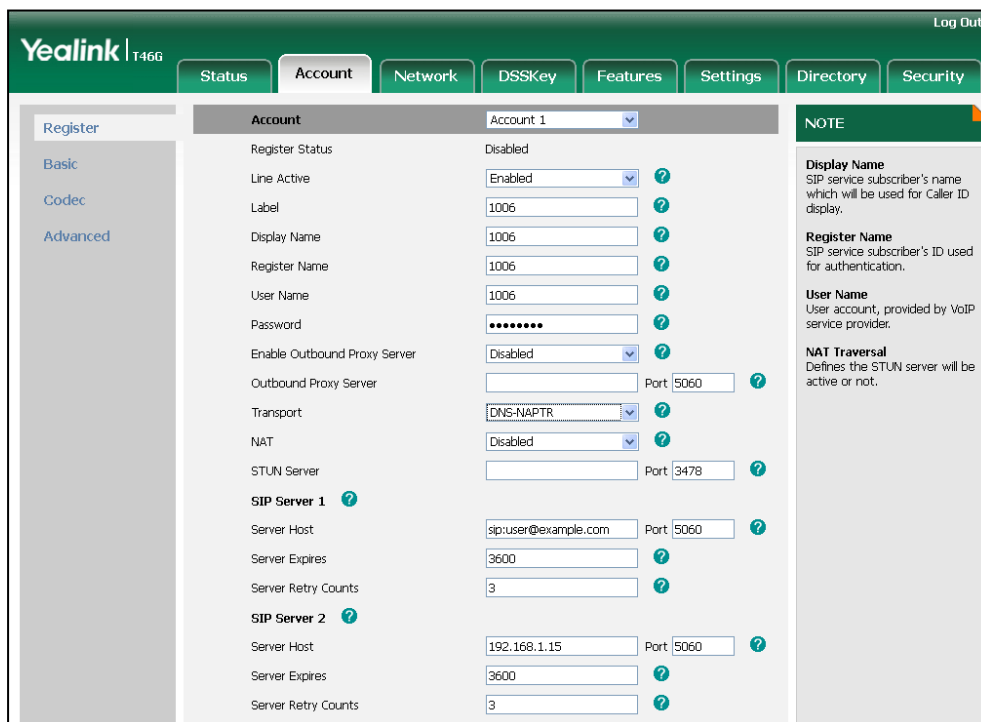
SIP server domain name resolution can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure the transport type. For more information, refer to SIP Server Domain Name Resolution on page 343.
---------------------------	-----------	--

Local	Web User Interface	Configure the transport type. Navigate to: http://<phoneIPAddress>/servlet?p=account-register&q=load&acc=0
-------	--------------------	---

To configure the server redundancy and transport type via web user interface:

1. Click on **Account**.
2. Select the desired account from the pull-down list of **Account**.
3. Select the desired value from the pull-down list of **Transport**.
4. Configure parameters of the SIP server 1 in the corresponding fields.
5. Configure parameters of the SIP server 2 in the corresponding fields.



6. Click **Confirm** to accept the change.

LLDP

LLDP (Linker Layer Discovery Protocol) is a vendor-neutral Link Layer protocol, which allows IP phones to receive and/or transmit device-related information from/to directly connected devices on the network that are also using the protocol, and store the information about other devices. LLDP transmits information as packets called LLDP Data Units (LLDPDUs). An LLDPDU consists of a set of Type-Length-Value (TLV) elements, each of which contains a particular type of information about the device or port transmitting it.

LLDP-MED (Media Endpoint Discovery)

LLDP-MED is published by the Telecommunications Industry Association (TIA). It is an extension to LLDP that operates between endpoint devices and network connectivity devices. LLDP-MED provides the following capabilities for IP phones:

- Capabilities Discovery -- allows LLDP-MED IP phones to determine the capabilities that the connected switch supports and has enabled.
- Network Policy -- provides voice VLAN configuration to notify IP phones which VLAN to use and QoS-related configuration for voice data. It provides a "plug and play" network environment.
- Power Management -- provides information related to how IP phones are powered, power priority, and how much power IP phones need.
- Inventory Management -- provides a means to effectively manage IP phones and their attributes such as model number, serial number and software revision.

TLVs supported by IP phones are summarized in the following table:

TLV Type	TLV Name	Description
Mandatory TLVs	Chassis ID	The network address of the IP phone.
	Port ID	The MAC address of the IP phone.
	Time To Live	Seconds until data unit expires. The default value is 60s.
	End of LLDPDU	Marks end of LLDPDU.
Optional TLVs	System Name	Name assigned to the IP phone. The default value is "yealink".
	System Description	Description of the IP phone. The default value is "yealink".
	System Capabilities	The supported and enabled phone capabilities. The supported capabilities are Bridge, Telephone and Router. The enabled capabilities are Bridge and Telephone by default.
	Port Description	Description of port that sends data unit. The default value is "WAN PORT".
IEEE Std 802.3 Organizational Specific TLV	MAC/PHY Configuration/Status	Duplex and bit rate settings of the IP phone. The Auto Negotiation is supported and enabled by default.

TLV Type	TLV Name	Description
		The advertised capabilities of PMD. Auto-Negotiation is: 100BASE-TX (full duplex mode), 100BASE-TX (half duplex mode), 10BASE-T (full duplex mode), 10BASE-T (half duplex mode).
TIA Organizationally Specific TLVs	Media Capabilities	The MED device type of the IP phone and the supported LLDP-MED TLV type can be encapsulated in LLDPDU. The supported LLDP-MED TLV types are: LLDP-MED Capabilities, Network Policy, Extended Power via MDI-PD, Inventory.
	Network Policy	Port VLAN ID, application type, L2 priority and DSCP value.
	Extended Power-via-MDI	Power type, source, priority and value.
	Inventory – Hardware Revision	Hardware revision of phone.
	Inventory – Firmware Revision	Firmware revision of phone.
	Inventory – Software Revision	Software revision of phone.
	Inventory – Serial Number	Serial number of phone.
	Inventory – Manufacturer Name	Manufacturer name of phone. The default value is “yealink”.
	Inventory – Model Name	Model name of phone.
	Asset ID	Assertion identifier of phone. The default value is “asset”.

Procedure

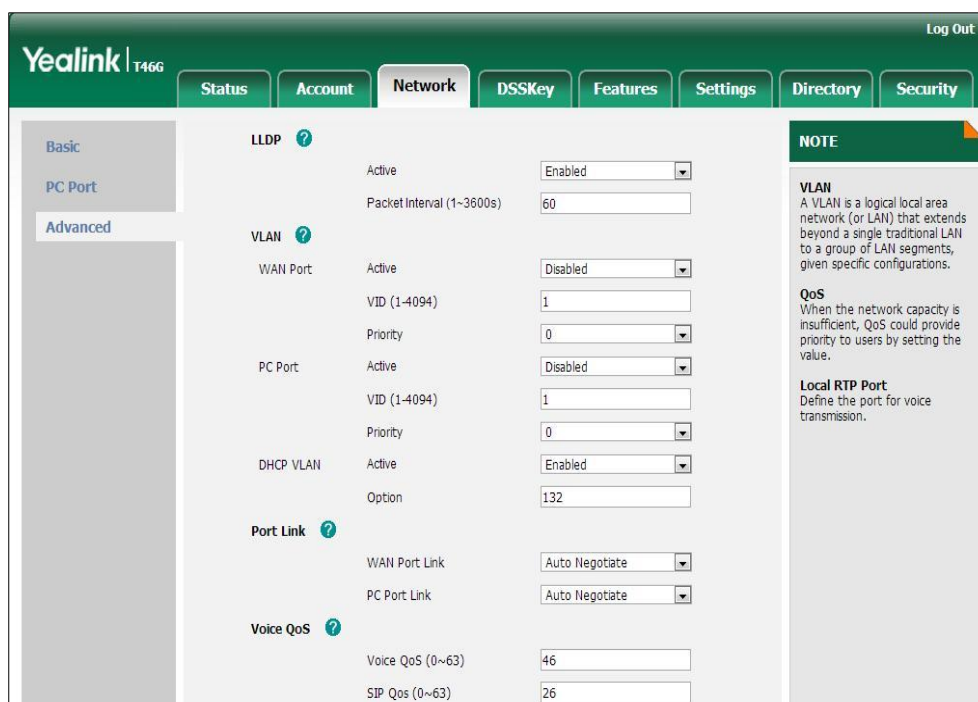
LLDP can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure LLDP feature. For more information, refer to LLDP on page 344.
Local	Web User Interface	Configure LLDP feature.

		<p>Navigate to: <a href="http://<phoneIPAddress>/servlet?p=network-adv&q=load">http://<phoneIPAddress>/servlet?p=network-adv&q=load</p>
--	--	---

To configure LLDP via web user interface:

1. Click on **Network->Advanced**.
2. In the **LLDP** block, select the desired value from the pull-down list of **Active**.
3. Enter the desired time interval in the **Packet Interval (1~3600s)** field.



4. Click **Confirm** to accept the change.
 A dialog box pops up to prompt that the settings will take effect after reboot.
5. Click **OK** to reboot the IP phone.

VLAN

VLAN (Virtual Local Area Network) is used to logically divide a physical network into several broadcast domains. VLAN membership can be configured through software instead of physically relocating devices or connections. Grouping devices with a common set of requirements regardless of their physical location can greatly simplify network design. VLANs can address issues such as scalability, security, and network management.

The purpose of VLAN configurations on the IP phone is to insert tag with VLAN information to the packets generated by the IP phone. When VLAN is properly configured for the ports (internet port and PC port) on the IP phone, the IP phone will tag all packets from these ports with the VLAN ID. The switch receives and forwards the

tagged packets to the corresponding VLAN according to the VLAN ID in the tag as described in IEEE Std 802.3.

The VLAN feature on IP phones allows simultaneous access for a regular PC. This feature allows a PC to be daisy chained to an IP phone and the connection for both PC and IP phone to be trunked through the same physical Ethernet cable.

In addition to manual configuration, the IP phone also supports automatic discovery of VLAN via LLDP or DHCP. The assignment takes place in this order: assignment via LLDP, manual configuration, then assignment via DHCP.

VLAN Discovery via DHCP

IP phones support VLAN discovery via DHCP. When the VLAN Discovery method is set to DHCP, the IP phone will examine DHCP option for a valid VLAN ID. The predefined option 132 is used to supply the VLAN ID by default. You can customize the DHCP option used to request the VLAN ID.

Procedure

VLAN can be configured using the configuration files or locally.

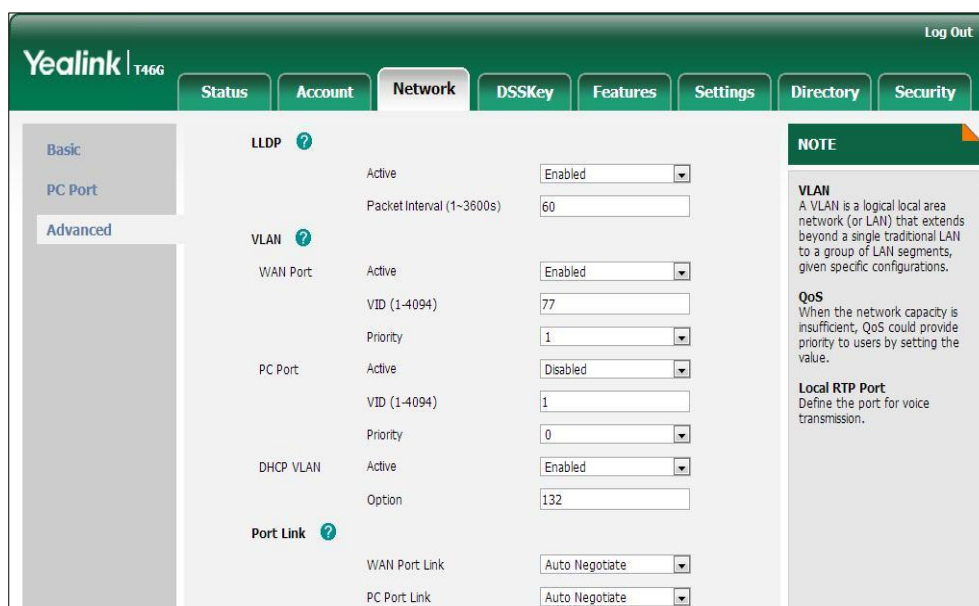
<p>Configuration File</p>	<p><y0000000000xx>.cfg</p>	<p>Configure VLAN for the Internet port. For more information, refer to VLAN on page 344. Configure VLAN for the PC port. For more information, refer to VLAN on page 344. Configure the DHCP VLAN discovery feature. For more information, refer to VLAN on page 344.</p>
<p>Local</p>	<p>Web User Interface</p>	<p>Configure VLAN for the Internet port and PC port and the DHCP VLAN discovery feature. Navigate to: http://<phoneIPAddress>/servlet?p=network-adv&q=load</p>
	<p>Phone User Interface</p>	<p>Configure VLAN for the Internet port and PC port.</p>

To configure VLAN for Internet port via web user interface:

1. Click on **Network->Advanced**.
2. In the **VLAN** block, select the desired value from the pull-down list of **WAN Port**

Active.

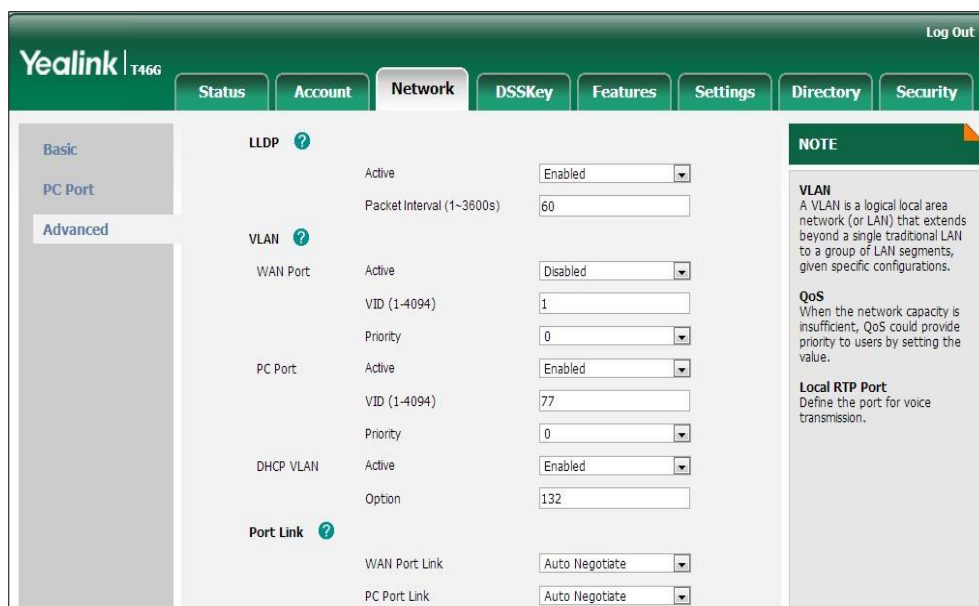
3. Enter the VLAN ID in the **VID (1-4094)** field.
4. Select the desired value (0-7) from the pull-down list of **Priority**.



5. Click **Confirm** to accept the change.
A dialog box pops up to prompt reboot to make the settings effective.
6. Click **OK** to reboot the IP phone.

To configure VLAN for PC port via web user interface:

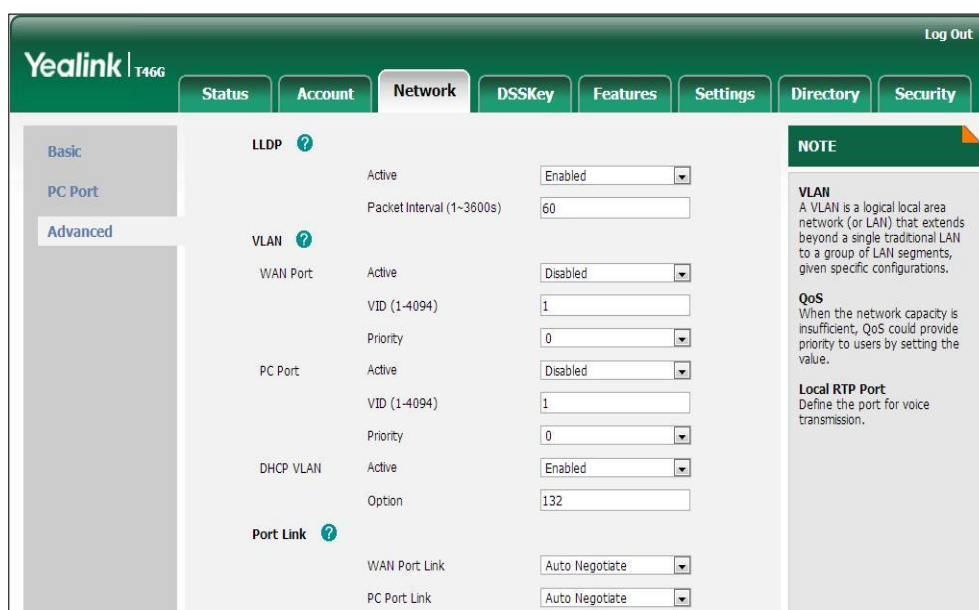
1. Click on **Network->Advanced**.
2. In the **VLAN** block, select the desired value from the pull-down list of **PC Port Active**.
3. Enter the VLAN ID in the **VID (1-4094)** field.
4. Select the desired value (0-7) from the pull-down list of **Priority**.



5. Click **Confirm** to accept the change.
A dialog box pops up to prompt that settings will take effect after reboot.
6. Click **OK** to reboot the IP phone.

To configure the DHCP VLAN discovery via web user interface:

1. Click on **Network->Advanced**.
2. In the **VLAN** block, select the desired value from the pull-down list of **DHCP VLAN Active**.
3. Enter the desired option in the **Option** field.
The default option is 132.



4. Click **Confirm** to accept the change.
A dialog box pops up to prompt that settings will take effect after reboot.
5. Click **OK** to reboot the IP phone.

To configure VLAN for Internet port (or PC port) via phone user interface:

1. Press **Menu->Advanced** (password: admin) ->**Network->VLAN->WAN Port** (or **PC Port**).
2. Press **◀** or **▶** , or the **Switch** soft key to select the desired value from the **VLAN Status** field.
3. Enter the VLAN ID (1-4094) in the **VID Number** field.
4. Enter the priority value (0-7) in the **Priority** field.
5. Press the **Save** soft key to accept the change.

The IP phone reboots automatically to make settings effective after a period of time.

VPN

VPN (Virtual Private Network) is a secured private network connection built on top of public telecommunication infrastructure, such as the Internet. It provides remote offices or individual users with secure access to their organization's network. VPN has become more prevalent due to the benefits of scalability, reliability, convenience and security. There are two types of VPN access: remote-access VPN (connecting an individual device to a network) and site-to-site VPN (connecting two networks together). Remote-access VPN allows employees to access their company's intranet from home or outside the office, and site-to-site VPN allows employees in geographically separated offices to share one cohesive virtual network. VPN can be also classified by the protocols used to tunnel the traffic. It provides security through tunneling protocols: IPSec, SSL, L2TP and PPTP.

IP phones support SSL VPN, which provides remote-access VPN capabilities through SSL. OpenVPN is a full featured SSL VPN software solution that creates secure connections in remote access facilities, designed to work with the TUN/TAP virtual networking interface. TUN and TAP are virtual network kernel devices. TAP simulates a link layer device and provides a virtual point-to-point connection, while TUN simulates a network layer device and provides a virtual network segment. IP phones use OpenVPN to achieve the VPN feature. To prevent disclosure of private information, tunnel endpoints must authenticate each other before secure VPN tunnel is established. After the VPN feature is configured properly on the IP phone, the IP phone acts as a VPN client and uses the certificates to authenticate the VPN server.

To use the VPN feature, the compressed package of VPN-related files should be uploaded to the IP phone in advance. The file format of the compressed package must be .tar. The VPN-related files are: certificates (ca.crt and client.crt), key (client.key) and the configuration file (vpn.cnf) of the VPN client. For more information on how to package a .tar file, refer to *OpenVPN Feature on Yealink IP Phones*.

Procedure

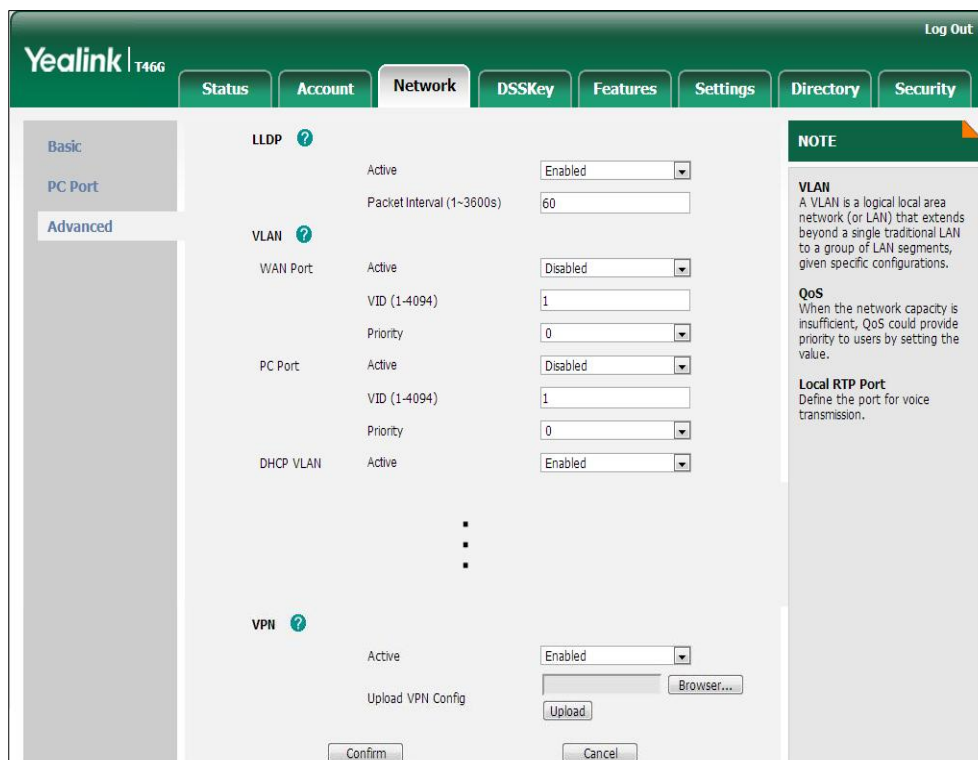
VPN can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure the OpenVPN feature and upload a tar file to the IP phone. For more information, refer to VPN on page 347.
Local	Web User Interface	Configure the OpenVPN feature and upload a tar package to the IP phone. Navigate to: http://<phoneIPAddress>/servl

		et?p=network-adv&q=load
	Phone User Interface	Configure the OpenVPN feature.

To upload the tar file to the IP phone and configure VPN via web user interface:

1. Click on **Network->Advanced**.
2. Click **Browse** to locate the tar package from the local system.
3. Click **Upload** to upload the tar file.



The web user interface prompts the message “Import config...”.

4. In the **VPN** block, select the desired value from the pull-down list of **Active**.
5. Click **Confirm** to accept the change.

A dialog box pops up to prompt that settings will take effect after reboot.

6. Click **OK** to reboot the IP phone.

To configure VPN via phone user interface after uploading the tar file:

1. Press **Menu->Advanced** (password: admin) ->**Network->VPN**.
2. Press **◀** or **▶** , or the **Switch** soft key to select the desired value from the **VPN Active** field.
3. Press the **Save** soft key to accept the change.

The IP phone reboots automatically to make settings effective after a period of time.

Quality of Service

Quality of Service (QoS) is the ability to provide different priorities to different packets in the network, allowing the transport of traffic with special requirements. QoS guarantees are important for applications that require fixed bit rate and are delay sensitive when the network capacity is insufficient. There are four major QoS factors to be considered when configuring a modern QoS implementation: bandwidth, delay, jitter and loss.

QoS provides better network service through the following features:

- Supporting dedicated bandwidth
- Improving loss characteristics
- Avoiding and managing network congestion
- Shaping network traffic
- Setting traffic priorities across the network

The Best-Effort service is the default QoS model in the IP networks. It provides no guarantees for data delivering, which means delay, jitter, packet loss and bandwidth allocation are unpredictable. Differentiated Services (DiffServ or DS) is the most widely used QoS model. It provides a simple and scalable mechanism for classifying and managing network traffic and providing QoS on modern IP networks. Differentiated Services Code Point (DSCP) is used to define DiffServ classes and stored in the first six bits of the ToS (Type of Service) field. Each router on the network can provide QoS simply based on the DiffServ class. The DSCP value ranges from 0 to 63 with each DSCP specifying a particular per-hop behavior (PHB) applicable to a packet. A PHB refers to the packet scheduling, queuing, policing, or shaping behavior of a node on any given packet.

There are four standard PHBs available to construct a DiffServ-enabled network and achieve QoS:

- **Class Selector PHB** – backwards compatible with IP precedence. Class Selector code points are of the form “xxx000”. The first three bits are the IP precedence bits. These class selector PHBs retain almost the same forwarding behavior as nodes that implement IP precedence-based classification and forwarding.
- **Expedited Forwarding PHB** – the key ingredient in DiffServ model for providing a low-loss, low-latency, low-jitter and assured bandwidth service.
- **Assured Forwarding PHB** – defines a method by which BAs can be given different forwarding assurances.
- **Default PHB** – specifies that a packet marked with a DSCP value of “000000” gets the traditional best effort service from a DS-compliant node.

VoIP is extremely bandwidth- and delay-sensitive. QoS is a major issue in VoIP implementations, regarding how to guarantee that packet traffic not to be delayed or dropped due to interference from other lower priority traffic. VoIP can guarantee

high-quality QoS only if the voice and the SIP packets are given priority over other kinds of network traffic. IP phones support the DiffServ model of QoS.

Voice QoS

In order to make VoIP transmissions intelligible to receivers, voice packets should not be dropped, excessively delayed, made to suffer varying delay. DiffServ model can guarantee high-quality voice transmission when the voice packets are configured to a higher DSCP value.

SIP QoS

SIP protocol is used for creating, modifying and terminating two-party or multi-party sessions. To ensure good voice quality, SIP packets emanated from IP phones should be configured with a high transmission priority.

DSCPs for voice and SIP packets can be specified respectively.

Note

The DSCP value of voice traffic in the received LLDP packet will override the manual configuration.

Procedure

DSCPs for voice packets and SIP packets can be configured using the configuration files or locally.

Configuration File	<y000000000xx>.cfg	Configure the DSCPs for voice packets and SIP packets. For more information, refer to QoS on page 348 .
Local	Web User Interface	Configure the DSCPs for voice packets and SIP packets. Navigate to: http://<phoneIPAddress>/servlet?p=network-adv&q=load

To configure DSCPs for voice packets and SIP packets via web user interface:

1. Click on **Network->Advanced**.
2. Enter the desired value in the **Voice QoS (0~63)** field.

3. Enter the desired value in the **SIP Qos (0~63)** field.

The screenshot shows the Yealink T466 web interface with the 'Network' tab selected. The 'Voice QoS' section is expanded, showing the following settings:

Setting	Value
LLDP	Active: Enabled
Packet Interval (1~3600s)	60
VLAN	Active: Disabled
WAN Port	Active: Disabled
VID (1-4094)	1
Priority	0
PC Port	Active: Disabled
VID (1-4094)	1
Priority	0
DHCP VLAN	Active: Enabled
Option	132
Port Link	WAN Port Link: Auto Negotiate
PC Port Link	Auto Negotiate
Voice QoS	Voice QoS (0~63): 46
SIP QoS	SIP QoS (0~63): 26

A 'NOTE' box on the right side of the interface provides information about VLAN and QoS settings.

4. Click **Confirm** to accept the change.
A dialog box pops up to prompt that the settings will take effect after reboot.
5. Click **OK** to reboot the IP phone.

Network Address Translation

Network Address Translation (NAT) is essentially a translation table that maps public IP address and port combinations to private ones. This reduces the need for a large number of public IP addresses. The NAT feature ensures security since each outgoing or incoming request must first go through a translation process. But in the VoIP environment, NAT breaks end-to-end connectivity.

NAT Traversal

NAT traversal is a general term for techniques that establish and maintain IP connections traversing NAT gateways, typically required for client-to-client networking applications, especially for VoIP deployments. STUN is one of the NAT traversal techniques supported by IP phones.

STUN (Simple Traversal of UDP over NATs)

STUN is a network protocol, used in NAT traversal for applications of real-time voice, video, messaging, and other interactive IP communications. The STUN protocol allows applications to operate behind a NAT to discover the presence of the network address translator, and to obtain the mapped (public) IP address and port number that the NAT

has allocated for the UDP connections to remote parties. The protocol requires assistance from a third-party network server (STUN server) usually located on public Internet. The IP phone can be configured to act as a STUN client, sending exploratory STUN messages to the STUN server. The STUN server uses those messages to determine the public IP address and port used, and then informs the client.

The NAT traversal and STUN server are configurable on a per-line basis.

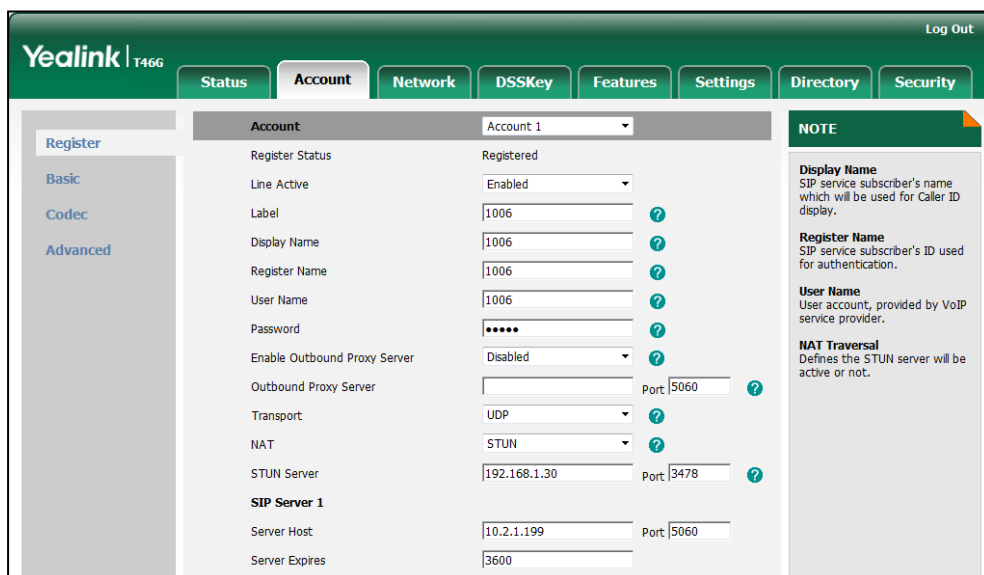
Procedure

NAT traversal and STUN server can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure NAT traversal and STUN server on the IP phone. For more information, refer to Network Address Translation on page 349.
Local	Web User Interface	Configure the NAT traversal and STUN server on the IP phone. Navigate to: http://<phoneIPAddress>/servlet?p=account-register&q=load&acc=0

To configure the NAT traversal and STUN server via web user interface:

1. Click on **Account**.
2. Select the desired account from the pull-down list of **Account**.
3. Select **STUN** from the pull-down list of **NAT**.
4. Enter the IP address or the domain name in the **STUN Server** field.



- Click **Confirm** to accept the change.

802.1X Authentication

IEEE 802.1X authentication is an IEEE standard for Port-based Network Access Control (PNAC), part of the IEEE 802.1 group of networking protocols. It offers an authentication mechanism for devices to connect to a LAN or WLAN. The 802.1X authentication involves three parties: a supplicant, an authenticator and an authentication server. The supplicant is the IP phone that wishes to attach to the LAN or WLAN. With 802.1X port-based authentication, the IP phone provides credentials, such as user name and password, for the authenticator, and then the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the IP phone is allowed to access resources located on the protected side of the network.

IP phones support protocols EAP-MD5, EAP-TLS, PEAP-MSCHAPv2 and EAP-TTLS/EAP-MSCHAPv2 for 802.1X authentication.

Procedure

802.1X authentication can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure the 802.1X authentication on the IP phone. For more information, refer to 802.1X on page 350.
Local	Web User Interface	Configure the 802.1X authentication on the IP phone. Navigate to: http://<phoneIPAddress>/servlet?p=network-adv&q=load
	Phone User Interface	Configure the 802.1X authentication on the IP phone.

To configure the 802.1X via web user interface:

- Click on **Network->Advanced**.
- In the **802.1x** block, select the desired protocol from the pull-down list of **Mode 802.1x**.
 - If you select **EAP-MD5**:
 - Enter the user name for authentication in the **Identity** field.

2) Enter the password for authentication in the **MD5 Password** field.

The screenshot shows the Yealink T46G web interface with the 'Network' tab selected. The '802.1x' section is expanded, showing the following configuration options:

- LLDP**: Active (Enabled), Packet Interval (1-3600s) (60)
- VLAN**: WAN Port (Active, Disabled)
- 802.1x**:
 - 802.1x Mode: EAP-MD5
 - Identity: yealink
 - MD5 Password: [Masked]
 - CA Certificates: [Browse...]
 - Device Certificates: [Upload]
- VPN**: Active (Disabled), Upload VPN Config: [Upload]

A **NOTE** section on the right provides information about VLAN and QoS:

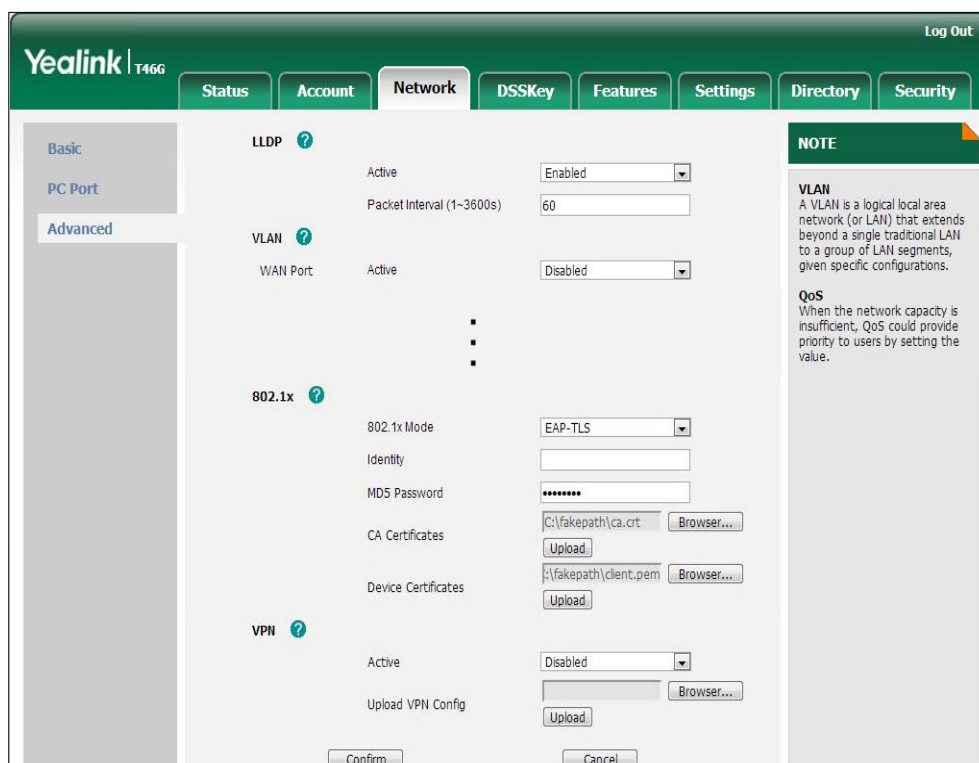
VLAN
A VLAN is a logical local area network (or LAN) that extends beyond a single traditional LAN to a group of LAN segments, given specific configurations.

QoS
When the network capacity is insufficient, QoS could provide priority to users by setting the value.

b) If you select **EAP-TLS**:

- 1) Enter the user name for authentication in the **Identity** field.
- 2) Leave the **MD5 Password** field blank.
- 3) In the **CA Certificates** field, click **Browse** to locate the desired CA certificate (*.pem, *.crt, *.cer or *.der) from your local system.
- 4) In the **Device Certificates** field, click **Browse** to locate the desired client certificate (*.pem or *.cer) from your local system.

5) Click **Upload** to upload the certificates.



c) If you select **PEAP-MSCHAPv2**:

- 1) Enter the user name for authentication in the **Identity** field.
- 2) Enter the password for authentication in the **MD5 Password** field.
- 3) In the **CA Certificates** field, click **Browse** to locate the desired certificate (*.pem, *.crt, *.cer or *.der) from your local system.

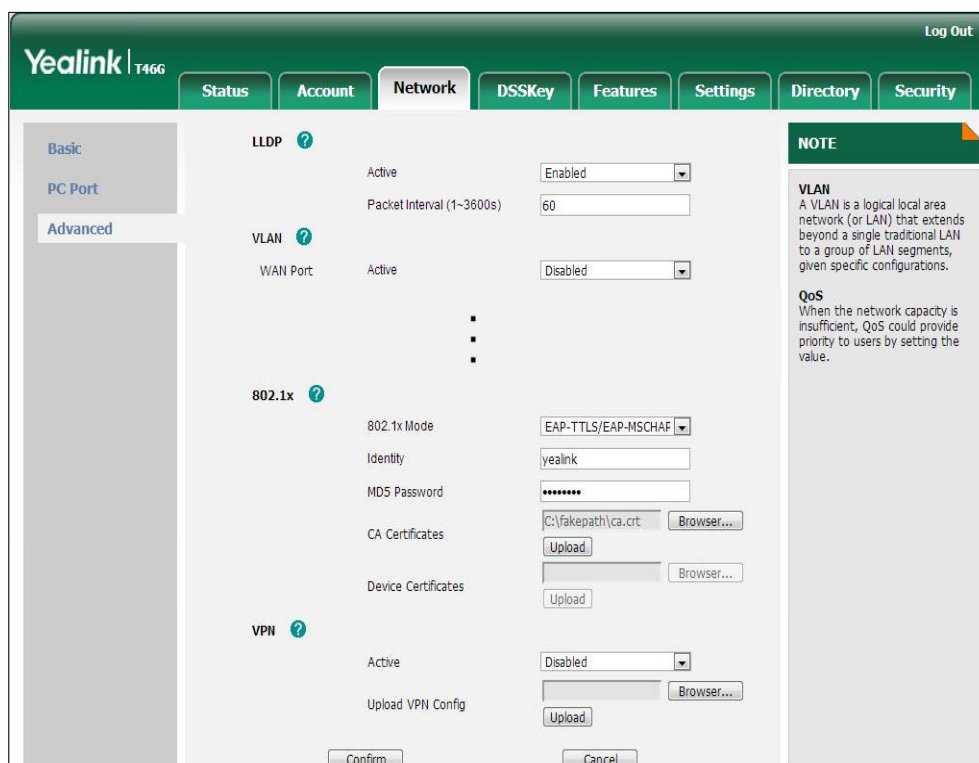
4) Click **Upload** to upload the certificate.

The screenshot shows the Yealink T46G web interface. The 'Network' tab is active, and the 'Advanced' sub-tab is selected. The configuration is for 802.1x authentication. The '802.1x Mode' is set to 'PEAP-MSCHAPv2'. The 'Identity' field is filled with 'yealink'. The 'MD5 Password' field is masked with asterisks. The 'CA Certificates' field shows a file path 'C:\fakepath\ca.crt' and an 'Upload' button. The 'Device Certificates' field has an 'Upload' button. The 'VPN' section is also visible, with 'Active' set to 'Disabled' and an 'Upload VPN Config' button. A 'NOTE' box on the right explains VLAN and QoS.

d) If you select **EAP-TTLS/EAP-MSCHAPv2**:

- 1) Enter the user name for authentication in the **Identity** field.
- 2) Enter the password for authentication in the **MD5 Password** field.
- 3) In the **CA Certificates** field, click **Browse** to locate the desired certificate (*.pem, *.crt, *.cer or *.der) from your local system.

- 4) Click **Upload** to upload the certificate.



3. Click **Confirm** to accept the change.
A dialog box pops up to prompt that the settings will take effect after reboot.
4. Click **OK** to reboot the IP phone.

To configure the 802.1X via phone user interface after:

1. Press **Menu->Advanced** (password: admin) ->**Network->802.1x Settings**.
2. Press **◀** or **▶** , or the **Switch** soft key to select the desired value from the **802.1x Mode** field.
 - a) If you select **EAP-MD5**:
 - 1) Enter the user name for authentication in the **Identity** field.
 - 2) Enter the password for authentication in the **Password** field.
 - b) If you select **EAP-TLS**:
 - 1) Enter the user name for authentication in the **Identity** field.
 - 2) Leave the **Password** field blank.
 - c) If you select **PEAP-MSCHAPV2**:
 - 1) Enter the user name for authentication in the **Identity** field.
 - 2) Enter the password for authentication in the **Password** field.
 - d) If you select **EAP-TTLS/EAP-MSCHAPV2**:
 - 1) Enter the user name for authentication in the **Identity** field.
 - 2) Enter the password for authentication in the **Password** field.

3. Click **Save** to accept the change.

The IP phone reboots automatically to make the settings effective after a period of time.

TR-069 Device Management

TR-069 is a technical specification defined by the Broadband Forum, which defines a mechanism that encompasses secure auto-configuration of a CPE (Customer-Premises Equipment), and incorporates other CPE management functions into a common framework. TR-069 uses common transport mechanisms (HTTP and HTTPS) for communication between CPE and ACS (Auto Configuration Servers). The HTTP(S) messages contain XML-RPC methods defined in the standard for configuration and management of the CPE.

TR-069 is intended to support a variety of functionalities to manage a collection of CPEs, including the following primary capabilities:

- Auto-configuration and dynamic service provisioning
- Software or firmware image management
- Status and performance monitoring
- Diagnostics

TR-069 is not applicable to SIP-T42G and SIP-T41P IP phones.

The following table provides a description of RPC methods supported by IP phones.

RPC Method	Description
GetRPCMethods	This method is used to discover the set of methods supported by the CPE.
SetParameterValues	This method is used to modify the value of one or more CPE parameters.
GetParameterValues	This method is used to obtain the value of one or more CPE parameters.
GetParameterNames	This method is used to discover the parameters accessible on a particular CPE.
GetParameterAttributes	This method is used to read the attributes associated with one or more CPE parameters.
SetParameterAttributes	This method is used to modify attributes associated with one or more CPE parameters.
Reboot	This method causes the CPE to reboot.
Download	This method is used to cause the CPE to download a specified file from the designated location.

RPC Method	Description
	File types supported by IP phones are: <ul style="list-style-type: none"> • Firmware Image • Configuration File
Upload	This method is used to cause the CPE to upload a specified file to the designated location. File types supported by IP phones are: <ul style="list-style-type: none"> • Configuration File • Log File
ScheduleInform	This method is used to request the CPE to schedule a one-time Inform method call (separate from its periodic Inform method calls) sometime in the future.
FactoryReset	This method resets the CPE to its factory default state.
TransferComplete	This method informs the ACS of the completion (either successful or unsuccessful) of a file transfer initiated by an earlier Download or Upload method call.
AddObject	This method is used to add a new instance of an object defined on the CPE.
DeleteObject	This method is used to remove a particular instance of an object.

Procedure

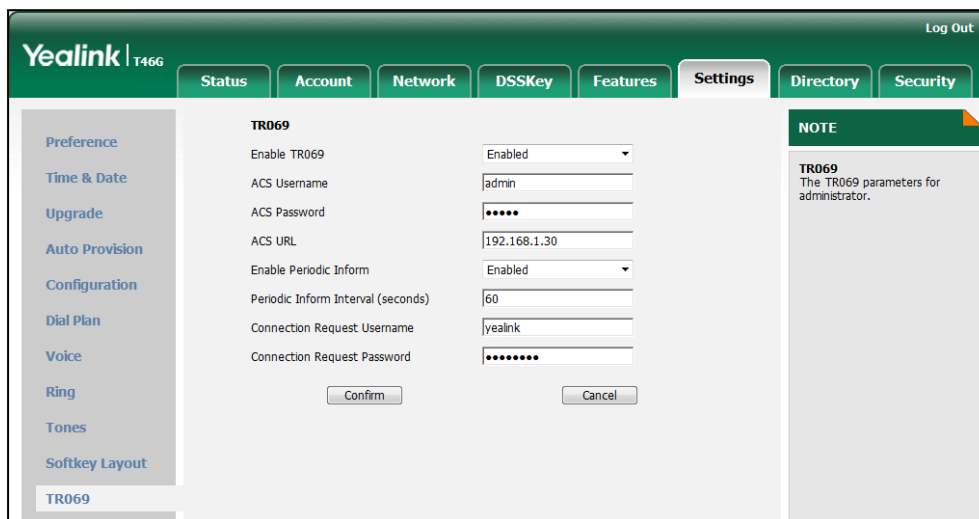
TR-069 can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure the TR-069 feature. For more information, refer to TR-069 on page 351.
Local	Web User Interface	Configure the TR-069 feature. Navigate to: http://<phoneIPAddress>/servlet?p=settings-preference&q=load

To configure TR-069 via web user interface:

1. Click on **Settings->TR069**.
2. Select **Enabled** from the pull-down list of **Enable TR069**.
3. Enter the user name and password authenticated by the ACS in the **ACS Username** and **ACS Password** fields.

4. Enter the URL of the ACS in the **ACS URL** field.
5. Select the desired value from the pull-down list of **Enable Periodic Inform**.
6. Enter the desired time in the **Periodic Inform Interval (seconds)** field.
7. Enter the user name and password authenticated by the IP phone in the **Connection Request Username** and **Connection Request Password** fields.



8. Click **Confirm** to accept the change.

IPv6 Support

IPv6 is the next generation network layer protocol, designed as a replacement for the current IPv4 protocol. IPv6 is developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. IPv6 uses a 128-bit address, consisting of eight groups of four hexadecimal digits separated by colons. VoIP network based on IPv6 can ensure QoS, a set of service requirements to deliver performance guarantee while transporting traffic over the network.

IP phones support IPv4 only addressing mode, IPv6 only addressing mode, as well as an IPv4/IPv6 dual stack addressing mode.

IPv6 Address Assignment Method

Supported IPv6 address assignment methods:

- **Manual Assignment:** An IPv6 address and other configuration parameters (e.g., DNS server) for the IP phone can be statically configured by an administrator.
- **Stateless Address Autoconfiguration (SLAAC):** SLAAC is one of the most convenient methods to assign IP addresses to IPv6 nodes. SLAAC requires no manual configuration of the IP phone, minimal (if any) configuration of routers, and no additional servers. To use IPv6 SLAAC, the IP phone must be connected to a network with at least one IPv6 router connected. This router is configured by the network administrator and sends out Router Advertisement announcements onto

the link. These announcements can allow the on-link connected IP phone to configure itself with IPv6 address, as specified in RFC 4862.

- Stateful DHCPv6:** The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) has been standardized by the IETF through RFC3315. DHCPv6 enables DHCP servers to pass configuration parameters such as IPv6 network addresses to IPv6 nodes. It offers the capability of automatic allocation of reusable network addresses and additional configuration flexibility. This protocol is a stateful counterpart to "IPv6 Stateless Address Autoconfiguration", and can be used separately or in addition to the stateless autoconfiguration to obtain configuration parameters.

Note

SIPT42G and SIPT41P IP phones do not support the stateful DHCPv6 address assignment method.

If the IP phone enables the SLAAC and DHCPv6 features simultaneously, the phone will obtain the IP address via SLAAC and obtain other network parameters via DHCPv6.

Procedure

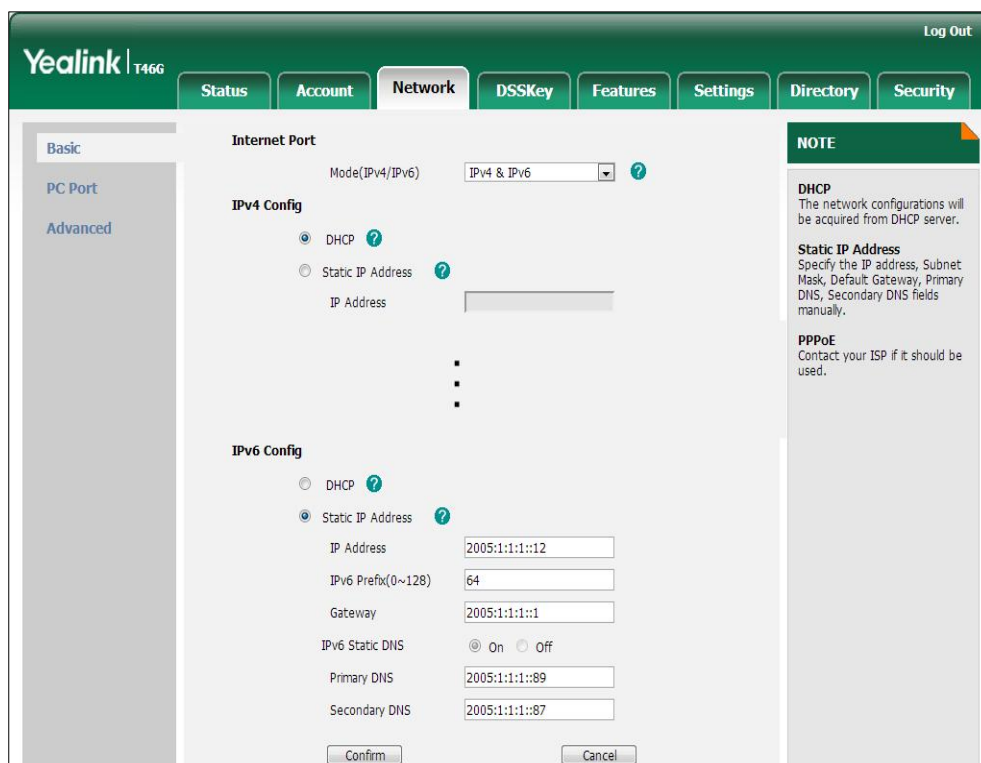
IPv6 can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure the IPv6 address assignment method. For more information, refer to IPv6 on page 355.
Local	Web User Interface	Configure the IPv6 address assignment method. Navigate to: http://<phoneIPAddress>/servlet?p=network&q=load

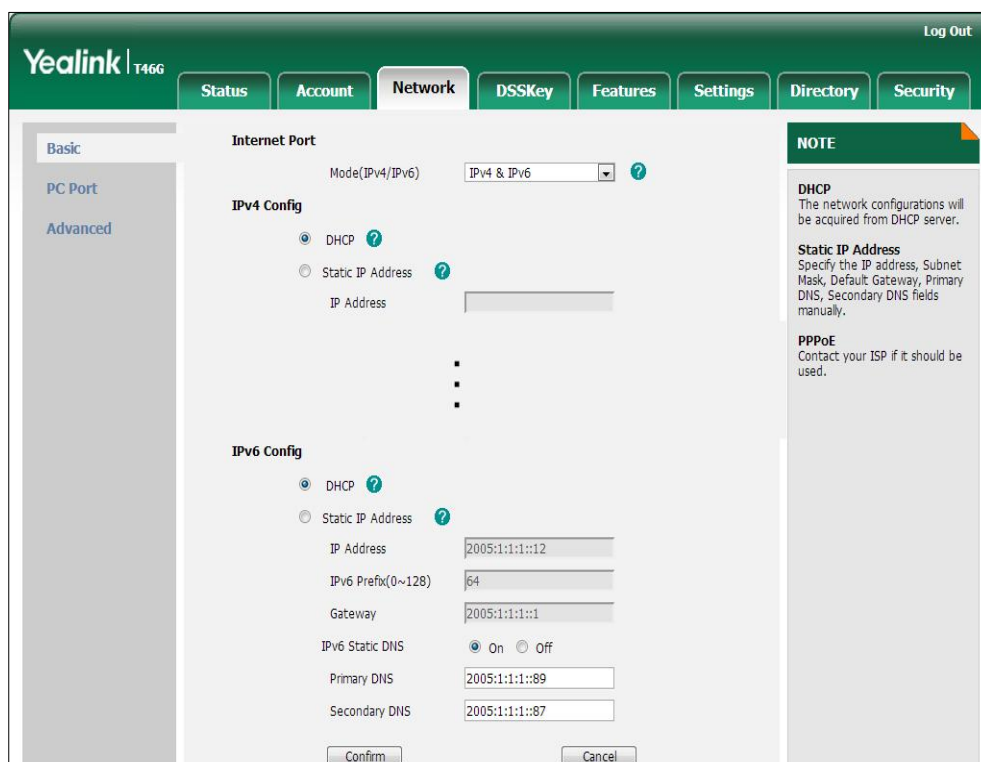
To configure IPv6 address assignment method via web user interface:

1. Click on **Network->Basic**.
2. Select the desired address mode (IPv6 or IPv4&IPv6) from the pull-down list of **Mode (IPv4/IPv6)**.

3. In the **IPv6 Config** block, mark the **DHCP** or the **Static IP Address** radio box.
 - If you mark the **Static IP Address** radio box, configure the IPv6 address and other configuration parameters in the corresponding fields.



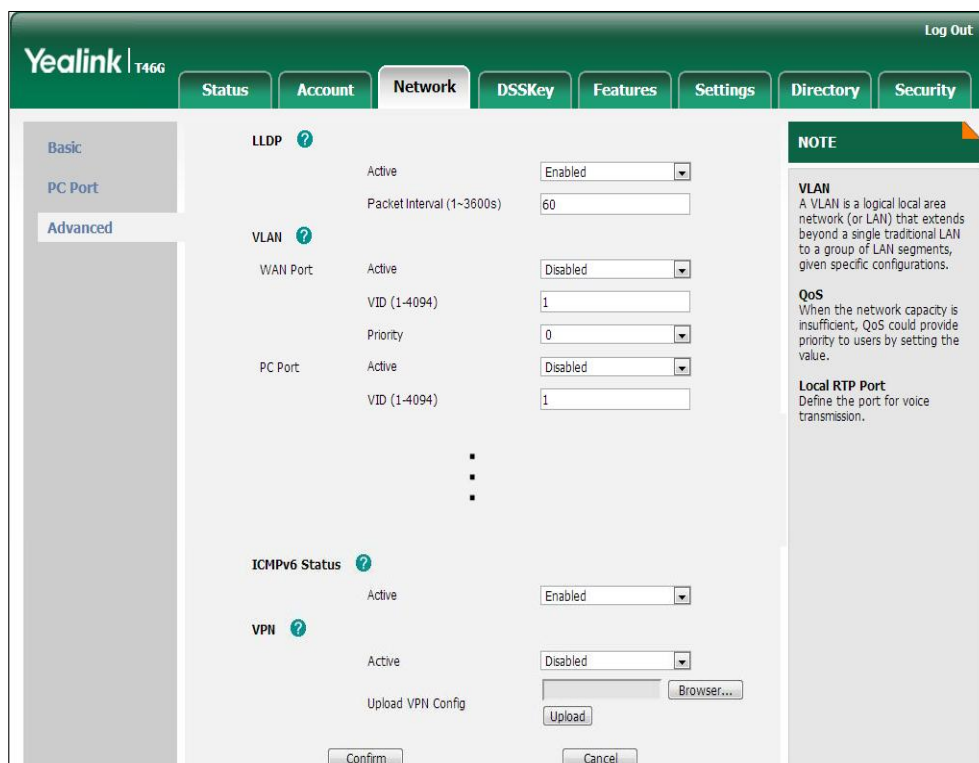
- (Optional.) If you mark the **DHCP** radio box, you can configure the static DNS address in the corresponding fields.



4. Click **Confirm** to accept the change.
A dialog box pops up to prompt that the settings will take effect after reboot.
5. Click **OK** to reboot the IP phone.

To configure SLAAC feature via web user interface (not applicable to SIP-T42G/T41P):

1. Click on **Network->Advanced**.
2. In the **ICMPv6 Status** block, select the desired value from the pull-down list of **Active**.



3. Click **Confirm** to accept the change.

To configure IPv6 address via phone user interface:

1. Press **Menu->Advanced** (password: admin) ->**Network->WAN Port**.
2. Press **◀** or **▶** to select the desired address mode from the **IP Address Mode** field.
3. Press **▲** or **▼** to highlight **IPv6** and press the **Enter** soft key.
4. Press **▲** or **▼** to select the desired IPv6 address assignment method.

If you select the **Static IP**, configure the IPv6 address and other configuration parameters in the corresponding fields.

5. Press the **Save** soft key to accept the change

The IP phone reboots automatically to make the settings effective after a period of time.

Configuring Audio Features

This chapter provides information for making configuration changes for the following audio features:

- [Headset Prior](#)
- [Dual Headset](#)
- [Audio Codecs](#)
- [Acoustic Clarity Technology](#)

Headset Prior

Headset prior allows users to use headset preferentially if a headset is physically connected to the IP phone. This feature is especially useful for permanent or full-time headset users.

Procedure

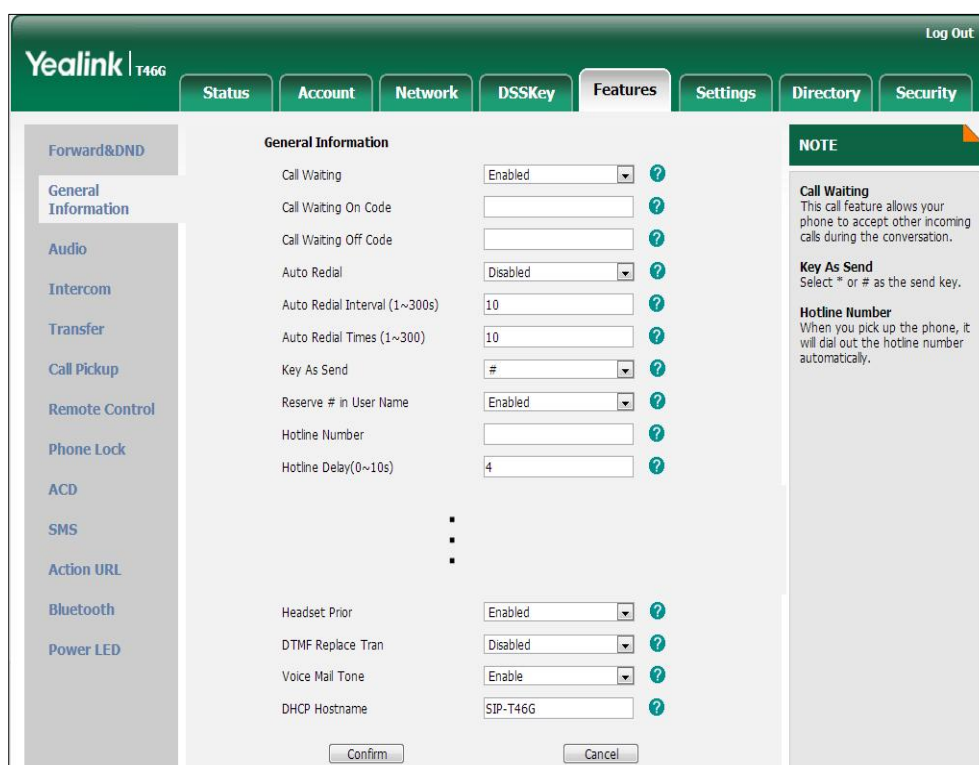
Headset prior can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure headset prior. For more information, refer to Headset Prior on page 359.
Local	Web User Interface	Configure headset prior. Navigate to: http://<phoneIPAddress>/servlet ?p=features-general&q=load

To configure headset prior via web user interface:

1. Click on **Features->General Information**.

2. Select the desired value from the pull-down list of **Headset Prior**.



3. Click **Confirm** to accept the change.

Dual Headset

Dual headset allows users to use two headsets on one IP phone. To use this feature, users need to physically connect two headsets to the headset and handset jacks respectively. Once the phone connects to a call, the user with the headset connected to the headset jack has full-duplex capabilities, while the user with the headset connected to the handset jack is only able to listen.

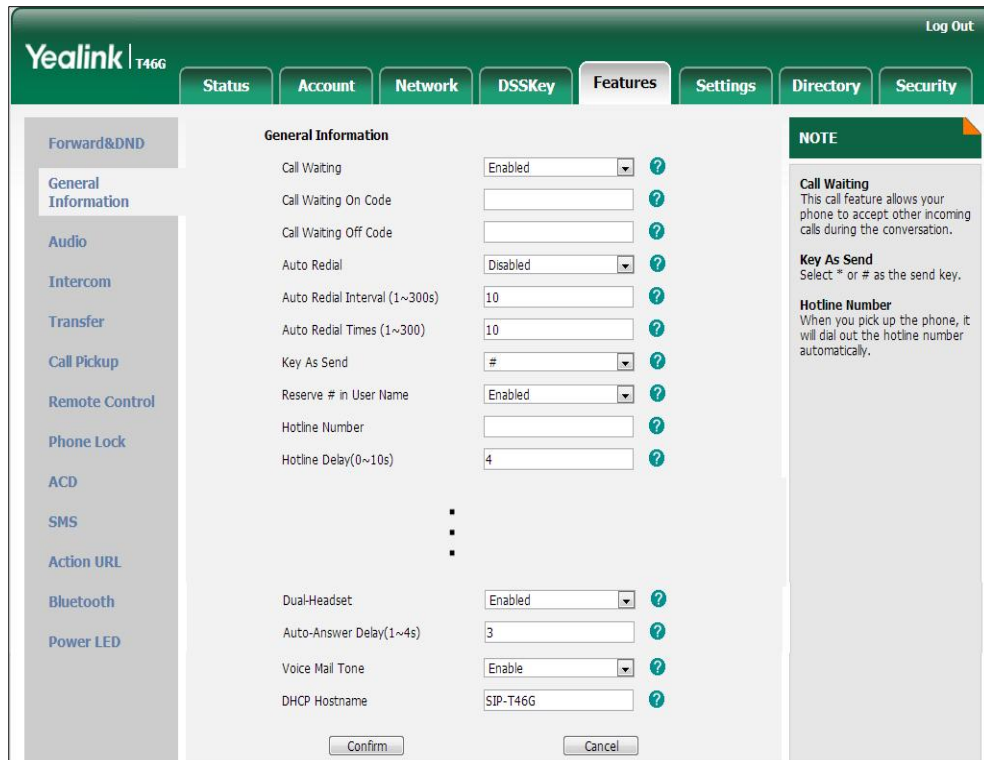
Procedure

Dual headset can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure dual headset. For more information, refer to Dual Headset on page 360.
Local	Web User Interface	Configure dual headset. Navigate to: http://<phoneIPAddress>/servlet ?p=features-general&q=load

To configure dual headset via web user interface:

1. Click on **Features->General Information**.
2. Select the desired value from the pull-down list of **Dual-Headset**.



3. Click **Confirm** to accept the change.

Audio Codecs

CODEC is an abbreviation of COmpress-DECompress, capable of coding or decoding a digital data stream or signal by implementing an algorithm. The object of the algorithm is to represent the high-fidelity audio signal with minimum number of bits while retaining the quality. This can effectively reduce the frame size and the bandwidth required for audio transmission.

The default codecs used on IP phones are summarized in the following table:

Codec	Algorithm	Bit Rate	Sample Rate	Packetization Time
PCMA	G.711 a-law	64 Kbps	8 Ksps	20ms
PCMU	G.711 u-law	64 Kbps	8 Ksps	20ms
G729	G.729	8 Kbps	8 Ksps	20ms
G722	G.722	64 Kbps	16 Ksps	20ms

In addition to the codecs introduced above, IP phones also support codecs: G723_53, G723_63, G726-16, G726-24, G726-32, G726-40, GSM and iLBC. Codecs and priorities of

these codecs are configurable on a per-line basis. The attribute "rtptime" is used to define a mapping from RTP payload codes to a codec, clock rate and other encoding parameters.

The corresponding attributes of the codec are listed as follows:

Codec	Configuration Methods	Priority	RTPmap
PCMU	Configuration Files Web User Interface	1	0
PCMA	Configuration Files Web User Interface	2	8
G729	Configuration Files Web User Interface	3	18
G722	Configuration Files Web User Interface	4	9
G723_53	Configuration Files Web User Interface	0	4
G723_63	Configuration Files Web User Interface	0	4
G726-16	Configuration Files Web User Interface	0	103
G726-24	Configuration Files Web User Interface	0	104
G726-32	Configuration Files Web User Interface	0	102
G726-40	Configuration Files Web User Interface	0	105
GSM	Configuration Files Web User Interface	0	97
iLBC	Configuration Files Web User Interface	0	106

Packetization Time

Ptime (Packetization Time) is a measurement of the duration (in milliseconds) of the audio data in each RTP packet sent to the destination, and defines how much network bandwidth is used for the RTP stream transfer. Before establishing a conversation, codec and ptime are negotiated through SIP signaling. The valid values of ptime range from



10 to 60, in increments of 10 milliseconds. The default ptime is 20ms. You can also disable the ptime negotiation.



Procedure

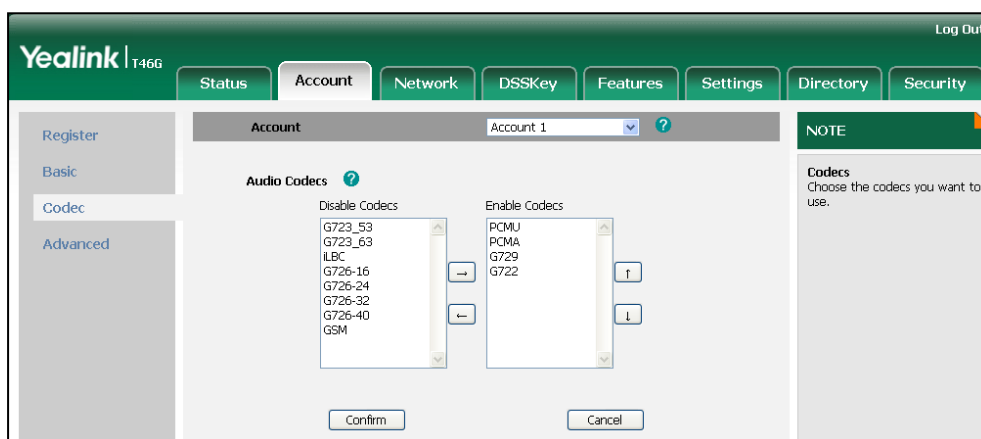
Configuration changes can be performed using the configuration files or locally.

Configuration File	<MAC>.cfg	<p>Configure the codecs to use on a per-line basis.</p> <p>Configure the priority and rtpmap for the enabled codec.</p> <p>For more information, refer to Audio Codecs on page 360.</p> <p>Configure the ptime.</p> <p>For more information, refer to Audio Codecs on page 360.</p>
Local	Web User Interface	<p>Configure the codecs and adjust the priority of the enabled codecs on a per-line basis.</p> <p>Configure the ptime.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet?p=account-codec&q=load&acc=0</p>

To configure the codecs and adjust the priority of the enabled codecs on a per-line basis via web user interface:

1. Click on **Account**.
2. Select the desired account from the pull-down list of **Account**.
3. Click on **Codec**.
4. Select the desired codec from the **Disable Codecs** column and click  .
The selected codec appears in the **Enable Codecs** column.
5. Repeat the step 4 to add more codecs to the **Enable Codecs** column.
6. Click  to remove the codec from the **Enable Codecs** column.

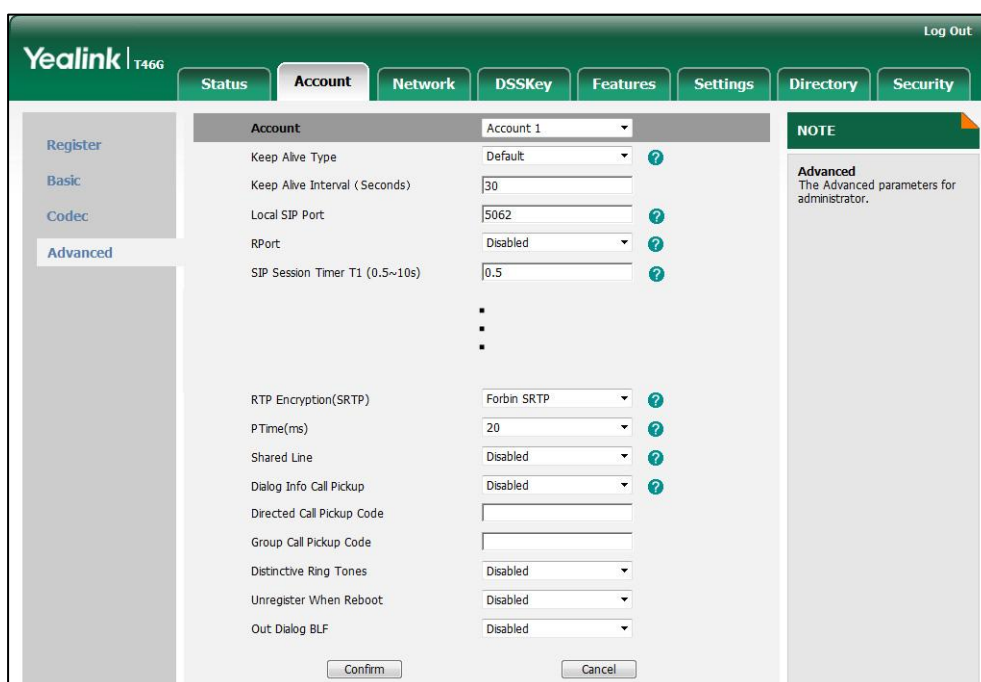
- Click  or  to adjust the priority of the enabled codecs.



- Click **Confirm** to accept the change.

To configure the PTime on a per-line basis via web user interface:

- Click on **Account**.
- Select the desired account from the pull-down list of **Account**.
- Click on **Advanced**.
- Select the desired value from the pull-down list of **PTime (ms)**.



- Click **Confirm** to accept the change.

Acoustic Clarity Technology

Acoustic Echo Cancellation

Acoustic Echo Cancellation (AEC) is used to remove acoustic echo from a voice communication in order to improve the voice quality. It also increases the capacity achieved through silence suppression by preventing echo from traveling across a network. IP phones employ advanced AEC for hands-free operation. Echo cancellation is achieved using the echo canceller.

Procedure

AEC can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure AEC. For more information, refer to Acoustic Echo Cancellation on page 363.
Local	Web User Interface	Configure AEC. Navigate to: http://<phoneIPAddress>/servlet?p=settings-voice&q=load

To configure AEC via web user interface:

1. Click on **Settings->Voice**.
2. Select the desired value from the pull-down list of **ECHO**.

The screenshot shows the Yealink T466 web user interface. The 'Settings' tab is active, and the 'Voice' sub-tab is selected. The 'Echo Cancellation' section is visible, with the following settings:

- ECHO:** Enabled
- VAD:** Disabled
- CNG:** Enabled
- JITTER BUFFER:**
 - Type: Adaptive Fixed
 - Min Delay: 60
 - Max Delay: 240
 - Normal: 120

Buttons for 'Confirm' and 'Cancel' are located at the bottom of the configuration area. A 'NOTE' section on the right provides additional information:

- VAD:** Voice Activity Detection.
- CNG:** Comfort Noise Generation.
- JITTER BUFFER:** It is a shared data area where voice packets can be collected, stored, and sent to the voice processor in evenly.

3. Click **Confirm** to accept the change.

Voice Activity Detection

Voice Activity Detection (VAD) is used in speech processing to detect the presence or absence of human speech. When detecting period of "silence", VAD replaces that silence efficiently with special packets that indicate silence is occurring. It can facilitate speech processing, and deactivate some processes during non-speech section of an audio session. VAD can avoid unnecessary coding or transmission of silence packets in VoIP applications, saving on computation and network bandwidth.

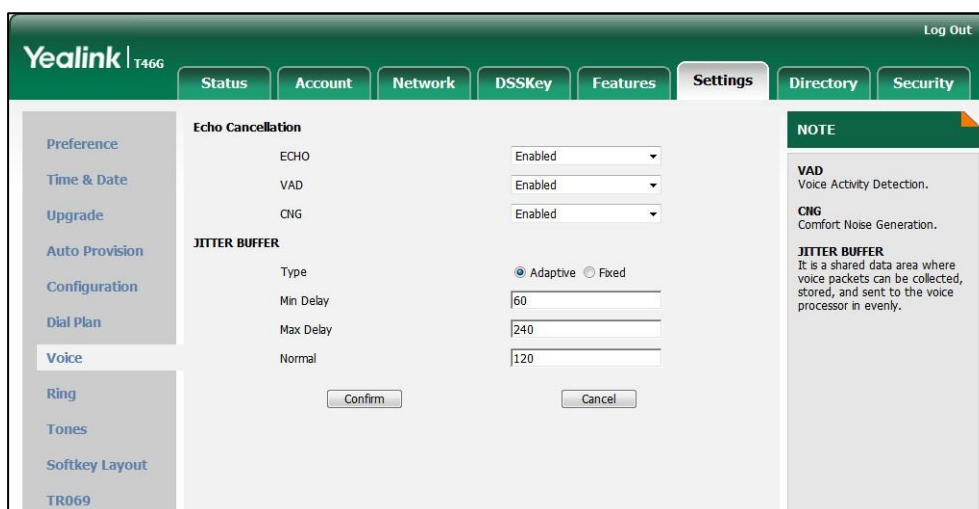
Procedure

VAD can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure VAD. For more information, refer to Voice Activity Detection on page 364.
Local	Web User Interface	Configure VAD. Navigate to: http://<phoneIPAddress>/servlet?p=settings-voice&q=load

To configure VAD via web user interface:

1. Click on **Settings->Voice**.
2. Select the desired value from the pull-down list of **VAD**.



3. Click **Confirm** to accept the change.

Comfort Noise Generation

Comfort Noise Generation (CNG) is used to generate background noise for voice communications during periods of silence in a conversation. It is a part of the silence suppression or VAD handling for VoIP technology. CNG, in conjunction with VAD algorithms, quickly responds when periods of silence occur and inserts artificial noise until voice activity resumes. The insertion of artificial noise gives the illusion of a constant transmission stream, so that background sound is consistent throughout the call and the listener does not think the line has released. The purpose of VAD and CNG is to maintain an acceptable perceived QoS while simultaneously keeping transmission costs and bandwidth usage as low as possible.

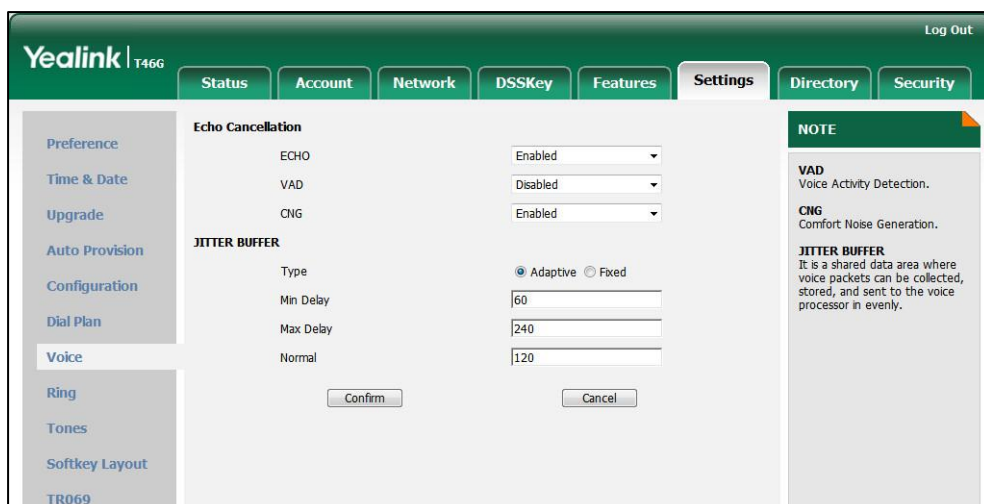
Procedure

CNG can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure CNG. For more information, refer to Comfort Noise Generation on page 364 .
Local	Web User Interface	Configure CNG. Navigate to: http://<phoneIPAddress>/servlet?p=settings-voice&q=load

To configure CNG via web user interface:

1. Click on **Settings->Voice**.
2. Select the desired value from the pull-down list of **CNG**.



3. Click **Confirm** to accept the change.

Jitter Buffer

Jitter buffer is a shared data area where voice packets can be collected, stored, and sent to the voice processor in even intervals. Jitter is a term indicating variations in packet arrival time, which can occur because of network congestion, timing drift or route changes. The jitter buffer, located at the receiving end of the voice connection, intentionally delays the arriving packets so that the end user experiences a clear connection with very little sound distortion. IP phones support two types of jitter buffers: static and dynamic. A static jitter buffer adds the fixed delay to voice packets. You can configure the delay time for the static jitter buffer on IP phones. A dynamic jitter buffer is capable of adapting the changes in the network's delay. The range of the delay time for the dynamic jitter buffer added to packets can be also configured on IP phones.

Procedure

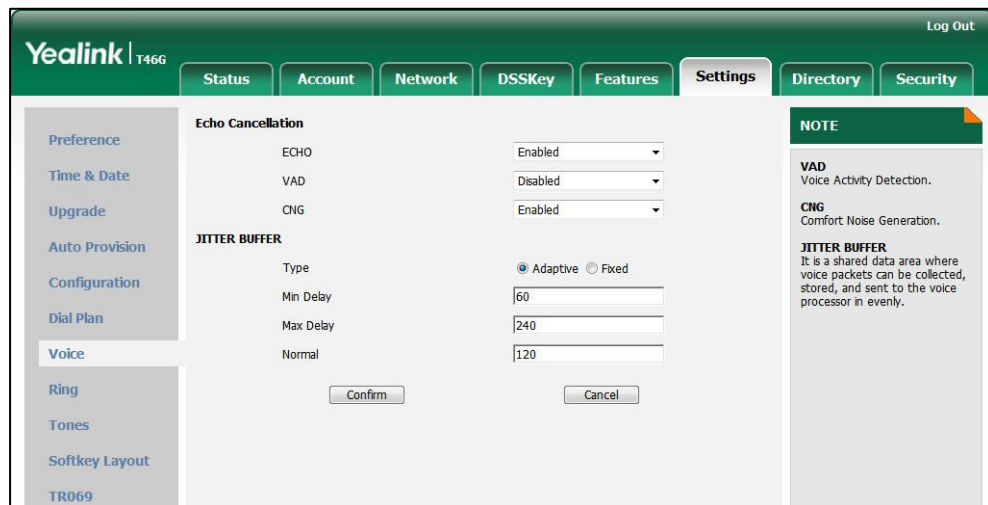
Jitter buffer can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure the mode of jitter buffer and the delay time for jitter buffer. For more information, refer to Jitter Buffer on page 364.
Local	Web User Interface	Configure the mode of jitter buffer and the delay time for jitter buffer. Navigate to: http://<phoneIPAddress>/servlet?p=settings-voice&q=load

To configure Jitter Buffer via web user interface:

1. Click on **Settings->Voice**.
2. Mark the desired radio box in the **Type** field.
3. Enter the minimum delay time for adaptive jitter buffer in the **Min Delay** field.
Valid values range from 0 to 300.
4. Enter the maximum delay time for adaptive jitter buffer in the **Max Delay** field.
Valid values range from 0 to 300.

- Enter the fixed delay time for fixed jitter buffer in the **Normal** field.
Valid values range from 0 to 300.



- Click **Confirm** to accept the change.

Configuring Security Features

This chapter provides information for making configuration changes for the following security-related features:

- [Transport Layer Security](#)
- [Secure Real-Time Transport Protocol](#)
- [Encrypting Configuration Files](#)

Transport Layer Security

TLS is a commonly-used protocol for providing communications privacy and managing the security of message transmission, allowing IP phones to communicate with other remote parties and connect to the HTTPS URL for provisioning in a way that is designed to prevent eavesdropping and tampering.

TLS protocol is composed of two layers: TLS Record Protocol and TLS Handshake Protocol. The TLS Record Protocol completes the actual data transmission and ensures the integrity and privacy of the data. The TLS Handshake Protocol allows the server and client to authenticate each other and negotiate an encryption algorithm and cryptographic keys before data is exchanged.

The TLS protocol uses asymmetric encryption for authentication of key exchange, symmetric encryption for confidentiality, and message authentication codes for integrity.

- **Symmetric encryption:** For symmetric encryption, the encryption key and the corresponding decryption key can be told by each other. In most cases, the encryption key is the same as the decryption key.
- **Asymmetric encryption:** For asymmetric encryption, each user has a pair of cryptographic keys – a public encryption key and a private decryption key. The information encrypted by the public key can only be decrypted by the corresponding private key and vice versa. Usually, the receiver keeps its private key. The public key is known by the sender, so the sender sends the information encrypted by the known public key, and then the receiver uses the private key to decrypt it.

SIP-T4X IP phones support TLS 1.0. A cipher suite is a named combination of authentication, encryption, and message authentication code (MAC) algorithms used to negotiate the security settings for a network connection using the TLS/SSL network protocol. SIP-T4X IP phones support the following cipher suites:

- DHE-RSA-AES256-SHA
- DHE-DSS-AES256-SHA

- AES256-SHA
- EDH-RSA-DES-CBC3-SHA
- EDH-DSS-DES-CBC3-SHA
- DES-CBC3-SHA
- DHE-RSA-AES128-SHA
- DHE-DSS-AES128-SHA
- AES128-SHA
- IDEA-CBC-SHA
- DHE-DSS-RC4-SHA
- RC4-SHA
- RC4-MD5
- EXP1024-DHE-DSS-DES-CBC-SHA
- EXP1024-DES-CBC-SHA
- EDH-RSA-DES-CBC-SHA
- EDH-DSS-DES-CBC-SHA
- DES-CBC-SHA
- EXP1024-DHE-DSS-RC4-SHA
- EXP1024-RC4-SHA
- EXP1024-RC4-MD5
- EXP-EDH-RSA-DES-CBC-SHA
- EXP-EDH-DSS-DES-CBC-SHA
- EXP-DES-CBC-SHA
- EXP-RC4-MD5

The following figure illustrates the TLS messages exchanged between the IP phone and TLS server to establish an encrypted communication channel:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.3.86	192.168.0.230	SSLV3	Client Hello
2	0.021345	192.168.0.230	192.168.3.86	SSLV3	Server Hello, Certificate, Server Key Exchange, Server Hello Done
3	0.954947	192.168.3.86	192.168.0.230	SSLV3	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
4	0.970099	192.168.0.230	192.168.3.86	SSLV3	Change Cipher Spec, Encrypted Handshake Message
5	1.012295	192.168.3.86	192.168.0.230	SSLV3	Application Data, Application Data
6	1.013562	192.168.0.230	192.168.3.86	SSLV3	Application Data
7	1.013667	192.168.0.230	192.168.3.86	SSLV3	Application Data

Frame 13: 652 bytes on wire (5216 bits), 652 bytes captured (5216 bits)
 Ethernet II, Src: Vmware_72:c9:2e (00:0c:29:72:c9:2e), Dst: Xiamenye_11:12:b7 (00:15:65:11:12:b7)
 Internet Protocol, Src: 192.168.0.230 (192.168.0.230), Dst: 192.168.3.86 (192.168.3.86)
 Transmission Control Protocol, Src Port: https (443), Dst Port: nmserver (2244), Seq: 1482, Ack: 437, Len: 586
 Secure Socket Layer

Step1: IP phone sends “Client Hello” message proposing SSL options.

Step2: Server responds with “Server Hello” message selecting the SSL options, sends its public key information in “Server Key Exchange” message and concludes its part of the

negotiation with “Server Hello Done” message.

Step3: The IP phone sends session key information (encrypted by server’s public key) in the “Client Key Exchange” message.

Step4: Server sends “Change Cipher Spec” message to activate the negotiated options for all future messages it will send.

IP phones can encrypt SIP with TLS, which is called SIPS. When TLS is enabled for an account, the SIP message of this account will be encrypted, and a lock icon will appear on the LCD screen after the successful TLS negotiation.

Certificates

The IP phone can serve as a TLS client or a TLS server. The TLS requires the following security certificates to perform the TLS handshake:

- **Trusted Certificate:** When the IP phone requests a TLS connection with a server, the IP phone should verify the certificate sent by the server to decide whether it is trusted based on the trusted certificates list. The IP phone has 30 built-in trusted certificates. You can upload up to 10 custom certificates to the IP phone. The format of the certificates must be *.pem, *.cer, *.crt and *.der.
- **Server Certificate:** When clients request a TLS connection with the IP phone, the IP phone sends the server certificate to the clients for authentication. The IP phone has two types of built-in server certificates: a unique server certificate and a generic server certificate. You can only upload one server certificate to the IP phone. The old server certificate will be overridden by the new one. The format of the server certificate files must be *.pem and *.cer.
 - **A unique server certificate:** It is installed by default and is unique to an IP phone (based on the MAC address) and issued by the Yealink Certificate Authority (CA).
 - **A generic server certificate:** It is installed by default and is issued by the Yealink Certificate Authority (CA). Only if no unique certificate exists, the IP phone may send a generic certificate for authentication.

The IP phone can authenticate the server certificate based on the trusted certificates list. The trusted certificates list and the server certificates list contain the default and custom certificates. You can specify the type of certificates the IP phone accepts: default certificates, custom certificates, or all certificates.

Common Name Validation feature enables the IP phone to mandatorily validate the common name of the certificate sent by the connecting server.

Note

In TLS feature, we use the terms trusted and server certificates. These are also known as CA and device certificates.

Firmware upgrade from version 71 to 72 will result in update of the default server certificates.

Procedure

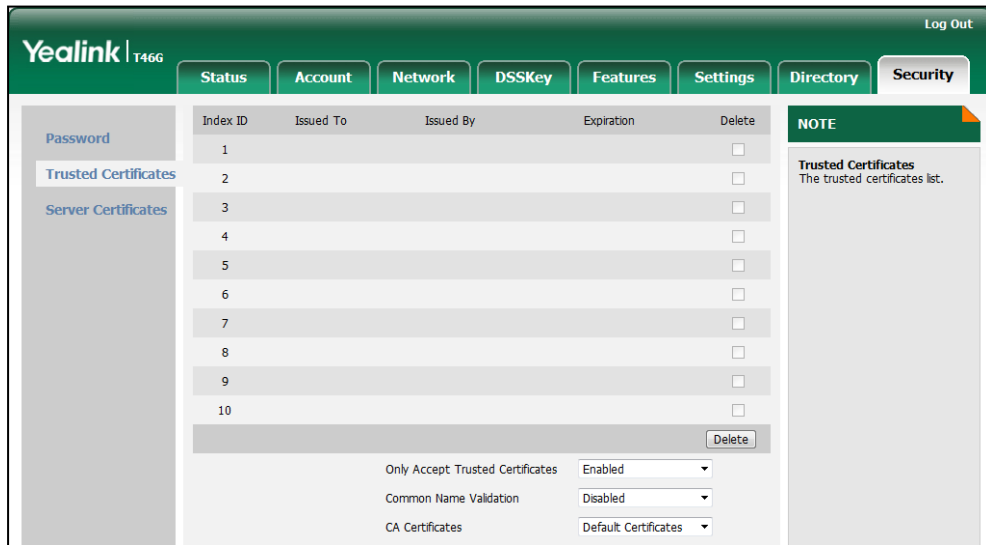
Configuration changes can be performed using the configuration files or locally.

Configuration File	<MAC>.cfg	<p>Configure TLS on a per-line basis.</p> <p>For more information, refer to TLS on page 366.</p>
	<y0000000000xx>.cfg	<p>Configure the trusted certificates feature.</p> <p>Configure the server certificates feature.</p> <p>For more information, refer to TLS on page 366.</p> <p>Upload the trusted certificates.</p> <p>Upload the server certificates.</p> <p>For more information, refer to Uploading Certificates on page 366.</p>
Local	Web User Interface	<p>Configure TLS on a per-line basis.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet?p=account-register&q=load&acc=0</p> <p>Configure the trusted certificates feature.</p> <p>Upload the trusted certificates.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet?p=trusted-cert&q=load</p> <p>Configure the server certificates feature.</p> <p>Upload the server certificates.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet?p=server-cert&q=load</p>

To configure the trusted certificates feature via web user interface:

1. Click on **Security->Trusted Certificates**.
2. Select the desired value from the pull-down list of **Only Accept Trusted Certificates**.

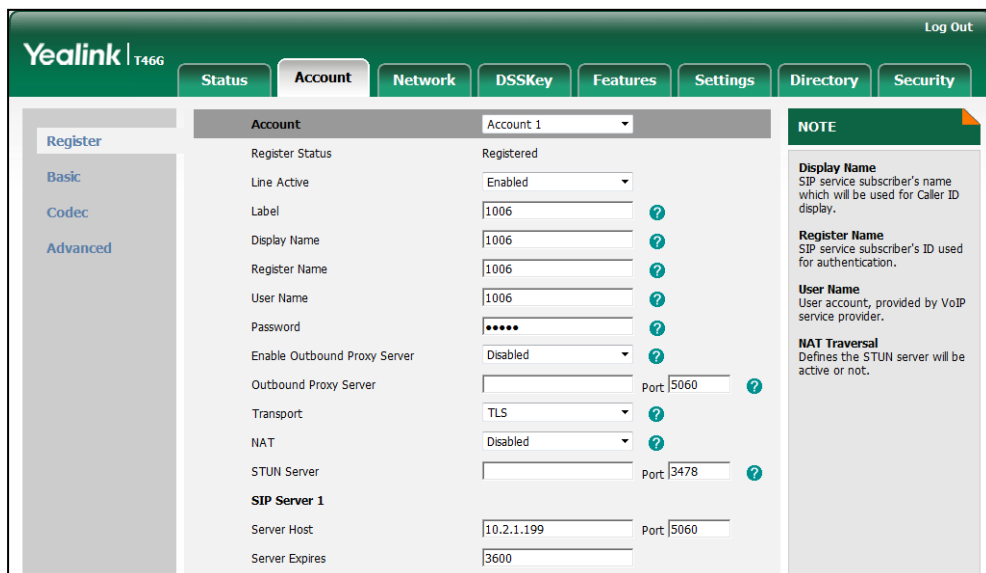
3. Select the desired value from the pull-down list of **Common Name Validation**.
4. Select the desired value from the pull-down list of **CA Certificates**.



5. Click **Confirm** to accept the change.
A dialog box pops up to prompt that the settings will take effect after reboot.
6. Click **OK** to reboot the IP phone.

To configure TLS on a per-line basis via web user interface:

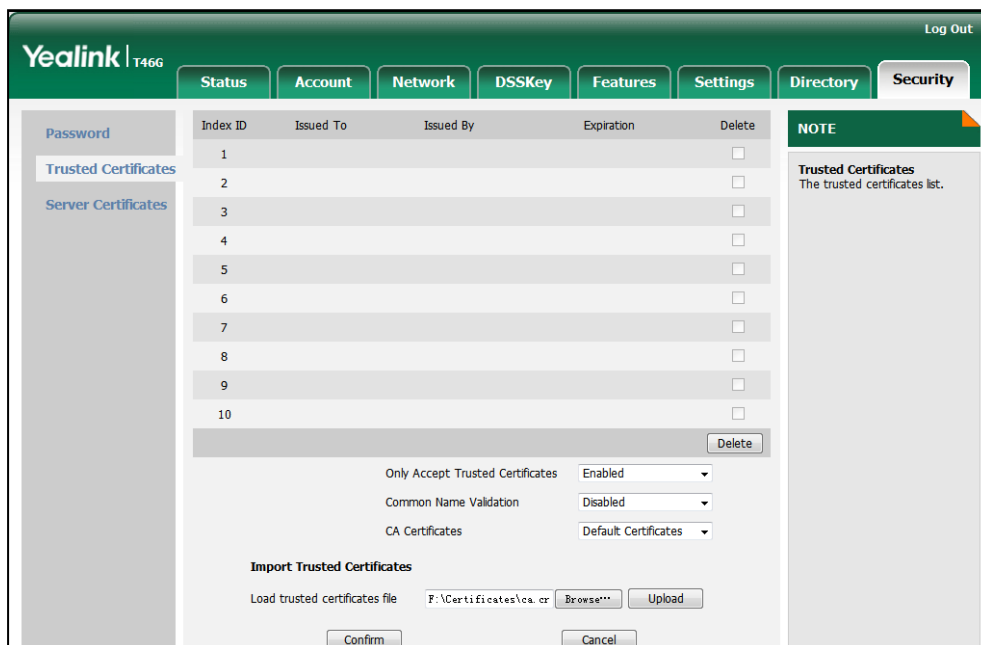
1. Click on **Account**.
2. Select the desired account from the pull-down list of **Account**.
3. Select **TLS** from the pull-down list of the **Transport**.



4. Click **Confirm** to accept the change.

To upload a trusted certificate via web user interface:

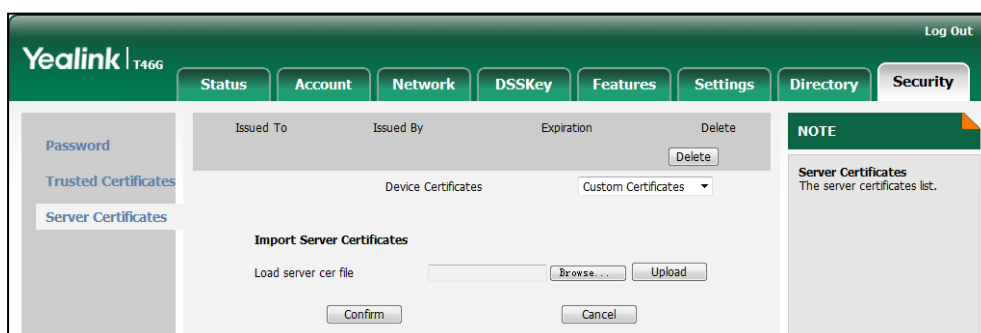
1. Click on **Security->Trusted Certificates**.
2. Click **Browse** to locate the certificate (*.pem,*.crt, *.cer or *.der) from your local system.



3. Click **Upload** to upload the certificate.

To configure the server certificates feature via web user interface:

1. Click on **Security->Server Certificates**.
2. Select the desired value from the pull-down list of **Device Certificates**.

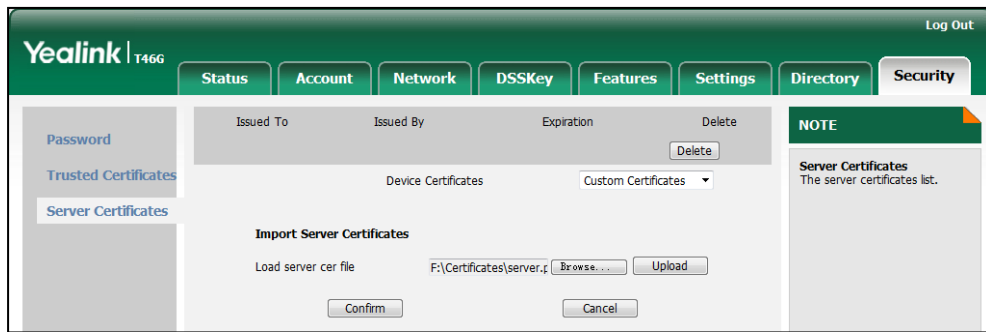


3. Click **Confirm** to accept the change.
A dialog box pops up to prompt that the settings will take effect after reboot.
4. Click **OK** to reboot the IP phone.

To upload a server certificate via web user interface:

1. Click on **Security->Server Certificates**.

- Click **Browse** to locate the certificate (*.pem or *.cer) from your local system.



- Click **Upload** to upload the certificate.

The dialog box pops up to prompt "Success: The Server Certificate has been loaded! Rebooting, please wait...".

Secure Real-Time Transport Protocol

Secure Real-Time Transport Protocol (SRTP) encrypts RTP streams during VoIP phone calls to avoid interception and eavesdropping. The parties participating in the call must enable SRTP simultaneously. When this feature is enabled on both phones, the encryption algorithm utilized for the session is negotiated between IP phones. This negotiation process is compliant with RFC 4568.

When a user places a call on the enabled SRTP phone, the IP phone sends an INVITE message with the RTP encryption algorithm to the destination phone.

Example of the RTP encryption algorithm carried in the SDP of the INVITE message:

```
m=audio 11780 RTP/SAVP 0 8 18 9 101
a=crypto:1 AES_CM_128_HMAC_SHA1_80
inline:NzFINTUwZDk2OGVIOTc3YzNkYTkwZWVkMTM1YWFj
a=crypto:2 AES_CM_128_HMAC_SHA1_32
inline:NzkyM2FjNzQ2ZDgxYjg0MzQwMGVmMGUxMzdmNWFm
a=crypto:3 F8_128_HMAC_SHA1_80 inline:NDIiMWIwZGE1ZTAwZjA5ZGFhNjQ5YmEANTMzYzA0
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:9 G722/8000
a=fmtp:101 0-15
a=rtpmap:101 telephone-event/8000
a=ptime:20
a=sendrecv
```

The callee receives the INVITE message with the RTP encryption algorithm, and then answers the call by responding with a 200 OK message which carries the negotiated RTP encryption algorithm.

Example of the RTP encryption algorithm carried in the SDP of the 200 OK message:

```
m=audio 11780 RTP/SAVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=crypto:1 AES_CM_128_HMAC_SHA1_80
inline:NGY4OGViMDYzZjQzYTNiOTNkOWRiYzRiMjM0Yzcy
a=sendrecv
a=ptime:20
a=fmtp:101 0-15
```

SRTP feature is configurable on a per-line basis. When SRTP is enabled on both IP phones, RTP streams will be encrypted, and a lock icon appears on the LCD screen of each IP phone after successful negotiation.

Note

If you enable SRTP, then you should also enable TLS. This ensures the security of SRTP encryption. For more information on TLS, refer to [Transport Layer Security](#) on page 203.

Procedure

SRTP can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure SRTP feature on a per-line basis. For more information, refer to SRTP on page 369.
Local	Web User Interface	Configure SRTP feature on a per-line basis. Navigate to: http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

To configure SRTP via web user interface:

1. Click on **Account**.
2. Select the desired account from the pull-down list of **Account**.
3. Click on **Advanced**.

- Select the desired value from the pull-down list of **RTP Encryption (SRTP)**.

The screenshot shows the Yealink T466 web interface with the 'Advanced' settings page selected. The 'RTP Encryption(SRTP)' setting is set to 'Compulsory'. Other settings include 'Keep Alive Type' (Default), 'Keep Alive Interval(Seconds)' (30), 'Local SIP Port' (5062), 'RPort' (Disabled), 'SIP Session Timer T1 (0.5~10s)' (0.5), 'SIP Session Timer T2 (2~40s)' (4), 'SIP Session Timer T4 (2.5~60s)' (5), 'Subscribe Period(Seconds)' (1800), 'DTMF Type' (RFC2833), 'DTMF Info Type' (DTMF-Relay), 'DTMF Payload Type(96~127)' (101), 'Retransmission' (Disabled), 'Subscribe for MWI' (Disabled), 'MWI Subscription Period(Seconds)' (3600), 'Subscribe MWI To Voice Mail' (Disabled), 'Voice Mail' (6008), 'Caller ID Source' (FROM), 'Session Timer' (Disabled), 'Session Expires(30~7200s)' (1800), 'Session Refresher' (UAC), 'Send user=phone' (Disabled), and 'PTime(ms)' (20). A 'NOTE' box on the right states: 'Advanced The Advanced parameters for administrator.'

- Click **Confirm** to accept the change.

Encrypting Configuration Files

Encrypted configuration files can be downloaded from the provisioning server to protect against unauthorized access and tampering of sensitive information (e.g., login passwords, registration information). Yealink provides a configuration encryption tool for encrypting configuration files. The encryption tool encrypts plaintext <y0000000000xx>.cfg and <MAC>.cfg files (one by one or in batch) using 16-character symmetric keys (the same or different keys for configuration files) and generates encrypted configuration files with the same file name as before. This tool also encrypts the plaintext 16-character symmetric keys using a fixed key, which is the same as the one built in the IP phone, and generates new files named as <xx_Security>.enc (xx indicates the name of the configuration file, for example, y000000000028_Security.enc for y000000000028.cfg file). This tool generates another new file named as Aeskey.txt to store the plaintext 16-character symmetric keys for each configuration file.

For a Microsoft Windows platform, you can use a Yealink-supplied encryption tool "Config_Encrypt_Tool.exe" to encrypt the <y0000000000xx>.cfg and <MAC>.cfg files respectively.

Note

Yealink also provides a configuration encryption tool (yealinkencrypt) for Linux platform if required. For more information, refer to *Yealink Configuration Encryption Tool User Guide*.

For the security reasons, administrator should upload encrypted configuration files, <y0000000000xx_Security>.enc and/or <MAC_Security>.enc files to the root directory of the provisioning server. During auto provisioning, the IP phone requests to download <y0000000000xx>.cfg file first. If the downloaded configuration file is encrypted, the phone will request to download <y0000000000xx_Security>.enc file (if enabled) and decrypt it into the plaintext key (e.g., key2) using the built-in key (e.g., key1). Then the IP phone decrypts <y0000000000xx>.cfg file using key2. After decryption, the IP phone resolves configuration files and updates configuration settings onto the IP phone system.

The way the IP phone processes the <MAC>.cfg file is the same to that of the <y0000000000xx>.cfg file.

Procedure to Encrypt Configuration Files

To encrypt the <y0000000000xx>.cfg file:

1. Double click "Config_Encrypt_Tool.exe" to start the application tool.

The screenshot of the main page is shown as below:



When you start the application tool, a file folder named "Encrypted" is created automatically in the directory where the application tool is located.

2. Click **Browse** to locate configuration file(s) (e.g., y000000000028.cfg) from your local system in the **Select File(s)** field.

To select multiple configuration files, you can select the first file and then press and hold the **Ctrl** key and select the next files.

3. (Optional.) Click **Browse** to locate the target directory from your local system in the **Target Directory** field.

The tool uses the file folder "Encrypted" as the target directory by default.

4. (Optional.) Mark the desired radio box in the **AES Model** field.

If you mark the **Manual** radio box, you can enter an AES key in the **AES KEY** field or click **Re-Generate** to generate an AES key in the **AES KEY** field. The configuration file(s) will be encrypted using the AES key in the **AES KEY** field.

If you mark the **Auto Generate** radio box, the configuration file(s) will be encrypted

using random AES key. The AES keys of configuration files are different.

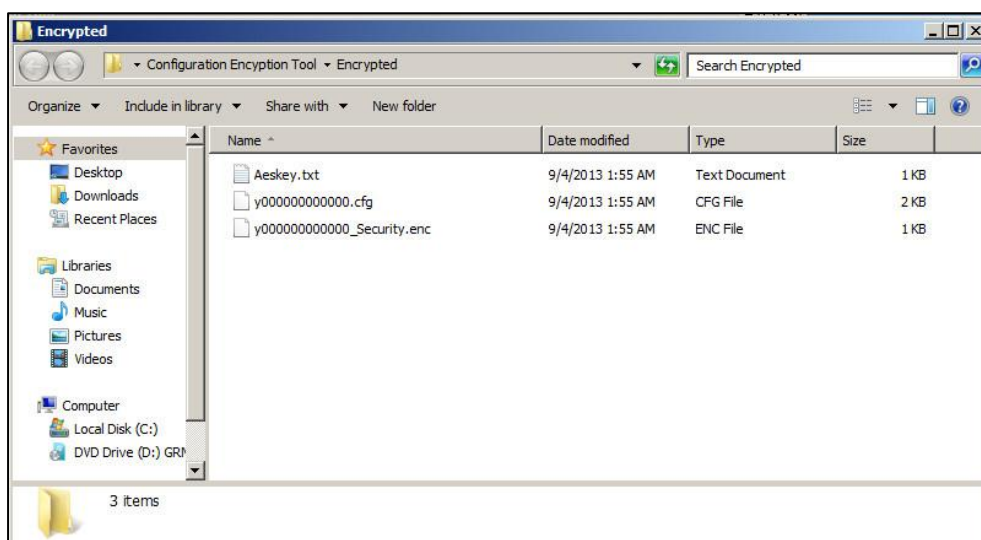
Note AES keys must be 16 characters and the supported characters contain: 0 ~ 9, A ~ Z, a ~ z.

5. Click **Encrypt** to encrypt the configuration file(s).



6. Click **OK**.

The target directory will be automatically opened. You can find the encrypted configuration file(s), encrypted key file(s) and an Aeskey.txt file storing plaintext AES key(s).



Procedure

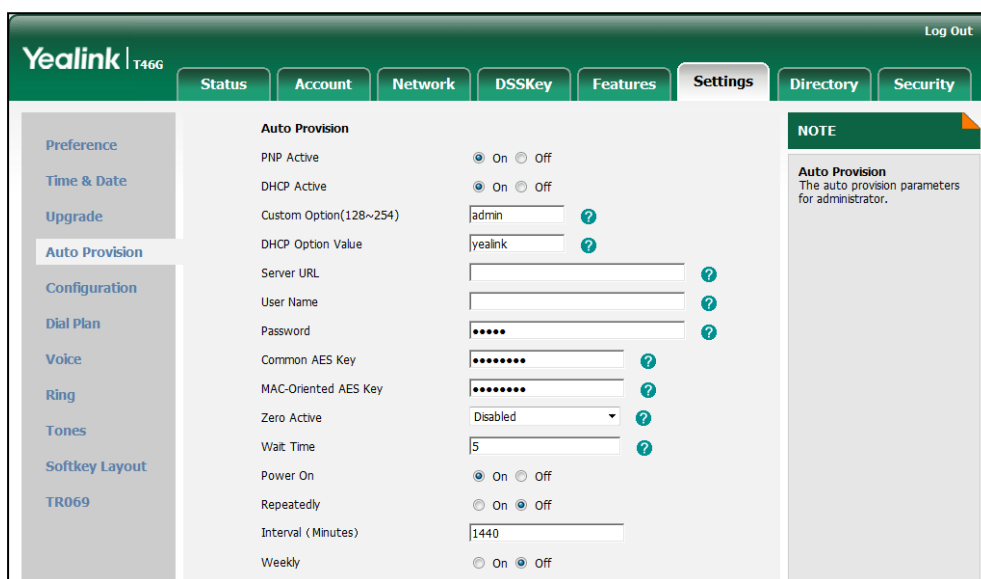
Encryption method and AES keys can be configured using the configuration files or locally.

<p>Configuration File</p>	<p><y0000000000xx>.cfg</p>	<p>Configure the decryption method and AES keys. For more information, refer to Configuring Decryption Method</p>
----------------------------------	----------------------------------	---

		on page 369 .
Local	Web User Interface	Configure the AES keys. Navigate to: http://<phoneIPAddress>/servlet?p=settings-autop&q=load

To configure the AES keys via web user interface:

1. Click on **Settings->Auto Provision**.
2. Enter the values in the **Common AES Key** and **MAC-Oriented AES Key** fields.



3. Click **Confirm** to accept the change.

Upgrading Firmware

This chapter provides information about upgrading the IP phone firmware. Two methods of firmware upgrade:

- Manually, from the local system.
- Automatically, from the provisioning server.

The following table lists the associated firmware name for each IP phone model (X is replaced by the actual firmware version).

IP Phone Model	Associated Firmware Name
SIP-T46G	28.x.x.x.rom
SIP-T42G	29.x.x.x.rom
SIP-T41P	36.x.x.x.rom

Note

You can download the latest firmware online:

<http://www.yealink.com/DocumentDownload.aspx?CatId=142&flag=142>.

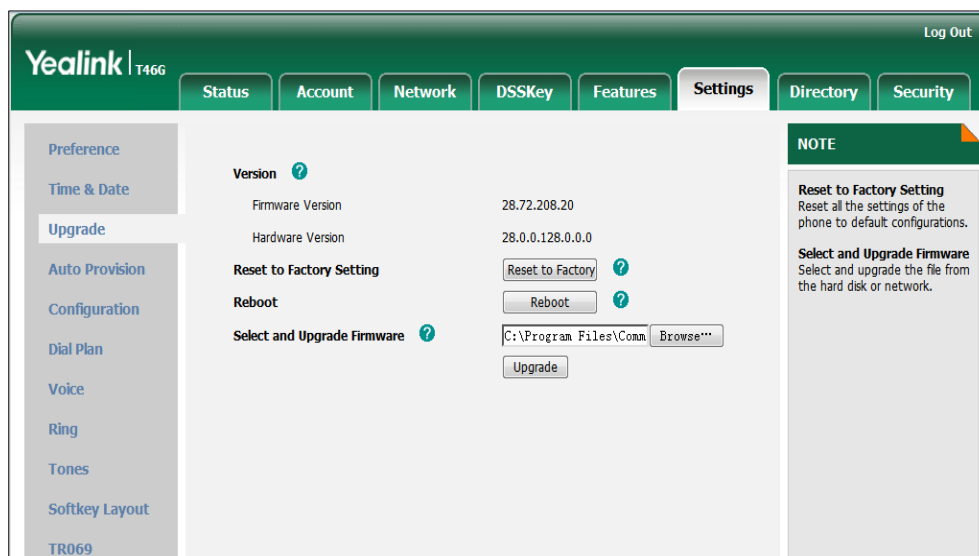
Upgrade via Web User Interface

To manually upgrade firmware via web user interface, you need to store the firmware to the local system in advance.

To upgrade firmware manually via web user interface:

1. Click on **Settings->Upgrade**.
2. Click **Browse**.
3. Select the firmware from the local system.
4. Click **Upgrade**.

A dialog box pops up to prompt "Firmware of the SIP Phone will be updated. It will take 5 minutes to complete. Please don't power off!".



5. Click **OK** to confirm the upgrade.

Note Do not unplug the network and power cables when the IP phone is upgrading firmware. Do not close and refresh the browser when the IP phone is upgrading firmware via web user interface.

Upgrade Firmware from the Provisioning Server

IP phones support to use the FTP, TFTP, HTTP, and HTTPS protocols to download the configuration files and firmware from the provisioning server, and then upgrade firmware automatically.

IP phones can download firmware stored on the provisioning server in one of two ways:

- Check for both configuration files and firmware stored on the provisioning server during booting up.
- Automatically check for configuration files and firmware at a fixed interval or specific time.

Method of checking for configuration files and firmware is configurable.

Procedure

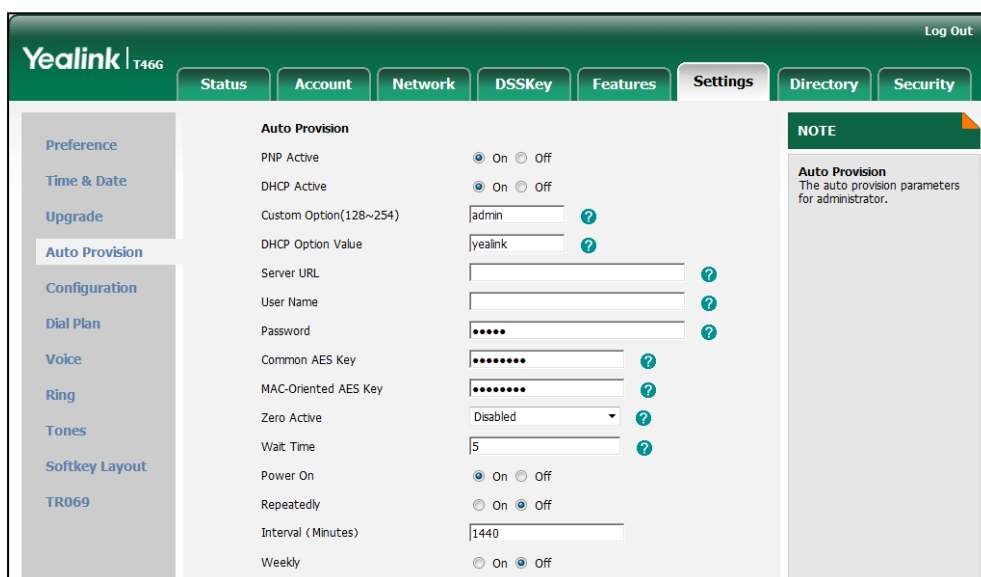
Configuration changes can be performed using the configuration files or locally.

<p>Configuration File</p>	<p><y0000000000xx>.cfg</p>	<p>Configure the way for the IP phone to check for configuration files.</p> <p>Specify the access URL of the firmware.</p>
----------------------------------	----------------------------------	--

		For more information, refer to Upgrading Firmware on page 371.
Local	Web User Interface	Configure the way for the IP phone to check for configuration files. Navigate to: <code>http://<phoneIPAddress>/servlet?<phoneIPAddress>/servlet?p=settings-autop&q=load</code>

To configure the way for the IP phone to check for new configuration files via web user interface:

1. Click on **Settings->Auto Provision**.
2. Make the desired change.



3. Click **Confirm** to accept the change.

When the “Power On” is set to **On**, the IP phone will check configuration files stored on the provisioning server during startup and then will download firmware from the server.

Resource Files

When configuring particular features, you may need to upload resource files (e.g., local contact directory, remote phone book) to the IP phone. The resources files can be local contact directory, remote phone book and so on. Ask Yealink field application engineer for resource file templates. If the resource file is to be used for all IP phones of the same model, the resource file access URL is best specified in the <y0000000000xx>.cfg file. However, if you want to specify the desired phone to use the resource file, the resource file access URL should be specified in the <MAC>.cfg file.

This chapter provides the detailed information on how to customize the following resource files and specify the access URL:

- [Replace Rule Template](#)
- [Dial-now Template](#)
- [Softkey Layout Template](#)
- [Local Contact File](#)
- [Remote XML Phone Book](#)
- [Directory Template](#)
- [Super Search Template](#)
- [Specifying the Access URL of Resource Files](#)

Replace Rule Template

The replace rule template helps with the creation of multiple replace rules. The existing replace rules on the phones will be overwritten by the downloaded replace rules. After setup, you need to place the replace rule template to the provisioning server and specify the access URL in the configuration files.

When editing a replace rule template file, learn the following:

- <DialRule> indicates the start of the template file and </DialRule> indicates the end of the template file.
- Create replace rules between <DialRule> and </DialRule>.
- When specifying the desired line(s) to apply the replace rule, the valid values are 0 and line ID. The digit 0 stands for all lines. Multiple line IDs are separated by commas.
- At most 100 replace rules can be added to the IP phone.
- The expression syntax in the replace rule template is the same as that introduced in the section [Creating Dial Plan](#) on page 28.

Procedure

Use the following procedures to customize a replace rule template.

To customize a replace rule template:

1. Open the template file using an ASCII editor.
2. Add the following string to the template, each starting on a separate line:

```
<Data Prefix="" Replace="" LineID=""/>
```

Where:

Prefix="" specifies the numbers to be replaced.

Replace="" specifies the alternate string instead of what the user enters.

LineID="" specifies the desired line(s) for this rule. When leaving it blank, this replace rule will apply to all lines.

3. Specify the values within double quotes.
4. Save the change and place this file to the provisioning server.

The following is an example of a replace rule file:

```
<DialRule>
  <Data Prefix="1" Replace="05928665234" LineID=""/>
  <Data Prefix="2(xx)" Replace="002$1" LineID="0"/>
  <Data Prefix="5([6-9]) (.)" Replace="3$2" LineID="1,2,3"/>
  <Data Prefix="0(.)" Replace="9$1" LineID="2"/>
  <Data Prefix="1009" Replace="05921009" LineID="1"/>
</DialRule>
```

Dial-now Template

The dial-now template helps with the creation of multiple dial-now rules. After setup, you need to place the dial-now template to the provisioning server and specify the access URL in the configuration files.

When editing a dial-now template, learn the following:

- <DialNow> indicates the start of a template and </DialNow> indicates the end of a template.
- Create dial-now rules between <DialNow> and </DialNow>.
- When specifying the desired line(s) for the dial-now rule, the valid values are 0 and line ID. 0 stands for all lines. Multiple line IDs are separated by commas.
- At most 100 dial-now rules can be added to the IP phone.
- The expression syntax in the dial-now rule template is the same as that introduced in the section [Creating Dial Plan](#) on page 28.

Procedure

Use the following procedures to customize a dial-now template.

To customize a dial-now template:

1. Open the template file using an ASCII editor.
2. Add the following string to the template, each starting on a separate line:

```
<Data DialNowRule="" LineID=""/>
```

Where:

DialNowRule="" specifies the dial-now rule.

LineID="" specifies the desired line(s) for this rule. When leaving it blank, this rule will apply to all lines.

3. Specify the values within double quotes.
4. Save the change and place this file to the provisioning server.

The following is an example of a dial-now template:

```
<DialNow>
  <Data DialNowRule="1234" LineID="1"/>
  <Data DialNowRule="52[0-6]" LineID="1"/>
  <Data DialNowRule="xxxxxx" LineID=""/>
</DialNow>
```

Softkey Layout Template

The softkey layout template allows assigning different soft key layouts to different call states. The call states include CallFailed, CallIn, Connecting, Dialing, RingBack and Talking. After setup, place the templates to the provisioning server and specify the access URL in the configuration files.

When editing a softkey layout template, learn the following:

- <Call States> indicates the start of a template and </Call States> indicates the end of a template. For example, <CallFailed> </CallFailed>.
- <Disable> indicates the start of the disabled soft key list and </Disable> indicates the end of the soft key list, the disabled soft keys are not displayed on the LCD screen.
- Create disabled soft keys between <Disable> and </Disable>.
- <Enable> indicates the start of the enabled soft key list and </Enable> indicates the end of the soft key list, the enabled soft keys are displayed on the LCD screen.
- Create enabled soft keys between <Enable> and </Enable>.
- <Default> indicates the start of the default soft key list and </Default> indicates

the end of the default soft key list, the default soft keys are displayed on the LCD screen by default.

Procedure

Use the following procedures to customize a softkey layout template.

To customize a softkey layout template:

1. Open the template file using an ASCII editor.
2. For each soft key that you want to enable, add the following string to the file. Each starts on a separate line:

```
<Key Type=""/>
```

Where:

Key Type="" specifies the enabled soft key (This value cannot be blank).

For each disabled soft key and each default soft key that you want to add, add the same string introduced above.

3. Specify the values within double quotes.
4. Save the change and place this file to the provisioning server.

The following is an example of the CallFailed template file:

```
<CallFailed>
  <Disable>
    <Key Type="Empty"/>
    <Key Type="Switch"/>
    <Key Type="Cancel"/>
  </Disable>
  <Enable>
    <Key Type="NewCall"/>
    <Key Type="Empty"/>
    <Key Type="Empty"/>
    <Key Type="Empty"/>
  </Enable>
  <Default>
    <Key Type="NewCall"/>
    <Key Type="Empty"/>
    <Key Type="Empty"/>
    <Key Type="Empty"/>
  </Default>
</CallFailed>
```

Local Contact File

You can add contacts one by one on the IP phone directly. You can also add multiple contacts at a time and/or share contacts between IP phones using the local contact template file. After setup, place the template file to the provisioning server, and specify the access URL of the template file in the configuration files.

When editing a local contact file, learn the following:

- `<root_contact>` indicates the start of a contact list and `</root_contact>` indicates the end of a contact list.
- `<root_group>` indicates the start of a group list and `</root_group>` indicates the end of a group list.
- When specifying a ring tone for a contact or a group, the format of the value must be Auto (the first registered line), Resource:RingN.wav (the default system ring tone, integer N ranges from 1 to 8 for SIP-T46G IP phones; integer N ranges from 1 to 5 for SIP-T42G/T41P IP phones) or Custom:Name.wav (the custom ring tone).
- When specifying a desired line for a contact, the valid values are -1 and integer 0~5 (for SIP-T42G/T41P: 0~2). -1 stands for Auto, and integer 0~5 stand for line1~line6. Multiple line IDs are separated by commas.
- When specifying an avatar for a contact, valid values are Default: avatar name (the built-in avatar) and Config: avatar name (the custom avatar). It is not applicable to SIP-T42G and SIP-T41P IP phones.

Procedure

Use the following procedures to customize a local contact template file.

To customize a local contact file:

1. Open the template file using an ASCII editor.
2. For each group that you want to add, add the following string to the file. Each starts on a separate line:

```
<group display_name="" ring="" />
```

Where:

`display_name=""` specifies the name of the group.

`ring=""` specifies the desired ring tone for this group.

3. For each contact that you want to add, add the following string to the file. Each starts on a separate line:

```
<contact display_name="" office_number="" mobile_number="" other_number=""
line="" ring="" group_id_name="" default_photo="" />
```

Where:

`display_name=""` specifies the name of the contact (This value cannot be blank or duplicated).

`office_number=""` specifies the office number of the contact.

`mobile_number=""` specifies the mobile number of the contact.

`other_number=""` specifies the other number of the contact.

`line=""` specifies the line you want to add this contact to.

`ring=""` specifies the ring tone for this contact.

`group_id_name=""` specifies the existing group you want to add the contact to.

`default_photo=""` specifies the photo for this contact.

4. Specify the values within double quotes.
5. Save the change and place this file to the provisioning server.

The following is an example of a local contact file:

```
<root_group>
  <group display_name="Friend" ring=""/>
  <group display_name="Family" ring="Resource:Ring1.wav"/>
</root_group>
<root_contact>
  <contact display_name="John" office_number="1001"
mobile_number="12345678910" other_number="" line="0" ring="Auto"
group_id_name="All Contacts"
default_photo="Default:default_contact_image.png"/>
  <contact display_name="Alice" office_number="1002" mobile_number=""
other_number="" line="2" ring="Resource:Ring2.wav"
group_id_name="Friend" default_photo="Config:custom.png"/>
</root_contact>
```

Remote XML Phone Book

The IP phone can access 5 remote phone books. You can customize the remote XML phone book for the IP phone as required. Before specifying the access URL of the remote phone book in the configuration files, you need to create a remote XML phone book and then place it to the provisioning server.

When creating an XML phone book, learn the following:

- `<YealinkIPPhoneDirectory>` indicates the start of a phone book and `</YealinkIPPhoneDirectory>` indicates the end of a phone book.
- `<DirectoryEntry>` indicates the start of a contact and `</DirectoryEntry>` indicates the end of a contact.

Procedure

Use the following procedures to customize an XML phone book.

To customize an XML phone book:

1. Open the template file using an ASCII editor.
2. For each contact that you want to add, add the following strings to the IP phone book. Each starts on a separate line:

```
<Name>Mary</Name>
<Telephone>1001</Telephone>
```

Where:

Specify the contact name between <Name> and </Name>.

Specify the contact number between <Telephone> and </Telephone>.

3. Specify the values within double quotes.
4. Save the file and place this file to the provisioning server.

The following is an example of an XML phone book:

```
<YealinkIPPhoneDirectory>
  <DirectoryEntry>
    <Name>Jack</Name>
    <Telephone>1003</Telephone>
  </DirectoryEntry>
  <DirectoryEntry>
    <Name>John</Name>
    <Telephone>1004</Telephone>
  </DirectoryEntry>
  <DirectoryEntry>
    <Name>Marry</Name>
    <Telephone>1005</Telephone>
  </DirectoryEntry>
</YealinkIPPhoneDirectory>
```

Note

Yealink supplies a phone book generation tool to quickly generate a remote XML phone book. For more information, refer to *Yealink Phonebook Generation Tool User Guide*.

Directory Template

Directory provides easy access to frequently used lists. The lists may contain Local Directory, History, Remote Phone Book and LDAP. Users can access the lists by pressing the Directory soft key when the IP phone is idle. After setup, place the directory template to the provisioning server and specify the access URL in the configuration files.

When editing a directory template, learn the following:

- `<root_favorite_set>` indicates the start of a template and `</root_favorite_set>` indicates the end of a template.
- Create directory between `<root_favorite_set>` and `</root_favorite_set>`.
- When specifying the display name of the directory list, the valid values are Local Contacts, History, Remote Phone Book and LDAP.
- When specifying the display priority of the directory list, the valid values are 1, 2, 3 and 4. 1 is the highest priority, 4 is the lowest.
- When enabling or disabling the desired directory list, the valid values are 0 and 1. 0 stands for Disabled, 1 stands for Enabled.

Procedure

Use the following procedures to customize a directory template.

Customizing a directory template:

1. Open the template file using an ASCII editor.
2. For each directory list that you want to configure, add the following string to the file. Each starts on a separate line:

```
<item id_name="" display_name="" priority="" enable="" />
```

Where:

`id_name=""` specifies the existing directory list you want to configure. We do not recommend editing this field.

`display_name=""` specifies the display name of the directory list. We do not recommend editing this field.

`priority=""` specifies the display priority of the directory list.

`enable=""` enables or disables the directory list.

3. Specify the values within double quotes.
4. Place this file to the provisioning server.

The following is an example of a directory template:

```
<root_favorite_set>
  <item id_name="localdirectory" display_name="Local Directory" priority="1"
  enable="1" />
  <item id_name="history" display_name="History" priority="2" enable="0" />
  <item id_name="remotedirectory" display_name="Remote Phone Book"
  priority="3" enable="0" />
  <item id_name="ldap" display_name="LDAP" priority="4" enable="0" />
</root_favorite_set>
```

Super Search Template

The super search template allows you to search for a contact in your desired lists when the phone is in the dialing screen. The lists may contain Local Directory, History, Remote Phone Book and LDAP. After setup, place the super search template to the provisioning server and specify the access URL in the configuration files.

When editing a super search template, learn the following:

- `<root_super_search>` indicates the start of a template and `</root_super_search>` indicates the end of a template.
- Create super search between `<root_super_search>` and `</root_super_search>`.
- When specifying the display name of the directory list, the valid values are Local Contacts, History, Remote Phone Book and LDAP.
- When specifying the priority of search results, the valid values are 1, 2, 3 and 4. 1 is the highest priority, 4 is the lowest.
- When enabling or disabling the desired directory list, the valid values are 0 and 1. 0 stands for Disabled, 1 stands for Enabled.

Procedure

Use the following procedures to customize a super search template.

Customizing a super search template:

1. Open the template file using an ASCII editor.
2. For each directory list that you want to configure, add the following string to the file. Each starts on a separate line:

```
<item id_name="" display_name="" priority="" enable="" />
```

Where:

`id_name=""` specifies the existing directory list you want to configure. We do not recommend editing this field.

`display_name=""` specifies the display name of the directory list. We do not

recommend editing this field.

priority="" specifies the priority of search results.

enable="" enables or disables the directory list.

3. Specify the values within double quotes.
4. Place this file to the provisioning server.

The following is an example of a super search template:

```
<root_super_search>
  <item id_name="local_directory_search" display_name="Local Contacts"
    priority="1" enable="1" />
  <item id_name="calllog_search" display_name="History" priority="2"
    enable="1" />
  <item id_name="remote_directory_search" display_name="Remote Phone
    Book" priority="3" enable="0" />
  <item id_name="ldap_search" display_name="LDAP" priority="4" enable="0" />
</root_super_search>
```

Specifying the Access URL of Resource Files

Access URL of the resource file can be configured in the configuration files:

Configuration File	<y0000000000xx>.cfg	Configure the access URL of the replace rule template. For more information, refer to Access URL of Replace Rule Template on page 374.
Configuration File	<y0000000000xx>.cfg	Configure the access URL of the dial-now rule template. For more information, refer to Access URL of Dial-now Template on page 374.
Configuration File	<y0000000000xx>.cfg	Configure the access URL of the softkey layout template. For more information, refer to Access URL of Softkey Layout Template on page 375.
Configuration File	<y0000000000xx>.cfg	Configure the access URL of the local contact file. For more information, refer to Access URL of Local Contact

		File on page 377.
Configuration File	<y0000000000xx>.cfg	Configure the access URL of the remote XML phonebook. For more information, refer to Access URL of Remote XML Phone Book on page 378.
Configuration File	<y0000000000xx>.cfg	Configure the access URL of the directory template. For more information, refer to Access URL of Directory Template on page 378.
Configuration File	<y0000000000xx>.cfg	Configure the access URL of the super search template. For more information, refer to Access URL of Super Search Template on page 378.

Troubleshooting

This chapter provides an administrator with general information for troubleshooting some common problems that he (or she) may encounter while using SIP-T4X IP phones.

Troubleshooting Methods

IP phones can provide feedback in a variety of forms such as log files, packets, status indicators and so on, which can help an administrator more easily find the system problem and fix it.

The following are helpful for better understanding and resolving the working status of the IP phone.

- [Viewing Log Files](#)
- [Capturing Packets](#)
- [Enabling the Watch Dog Feature](#)
- [Getting Information from Status Indicators](#)
- [Analyzing Configuration Files](#)

Viewing Log Files

The IP phone can log various events to log files. So if your IP phone encounters some problems, commonly the log files are used. You can export the log files to a syslog server or the local system. You can also specify the severity level of the log to be reported to a log file. The default system log level is 3.

In the configuration files, you can use the following parameters to configure system log settings:

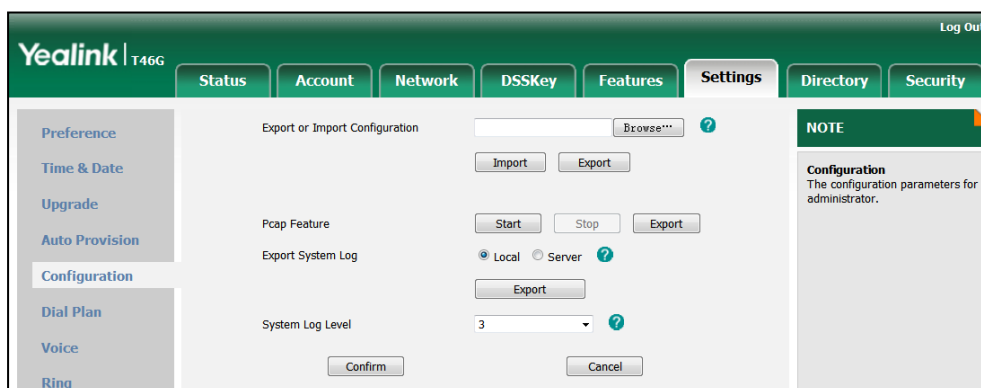
- **syslog.server** -- Specify the IP address of the syslog server to which the log will be exported.
- **syslog.log_level** -- Specify the system log level (Changes to this parameter via web user interface require a reboot).

For more information on the system log setting configuration parameters, refer to [Log Settings](#) on page 379.

To configure the system log level via web user interface:

1. Click on **Settings->Configuration**.

2. Select the desired level from the pull-down list of **System Log Level**.

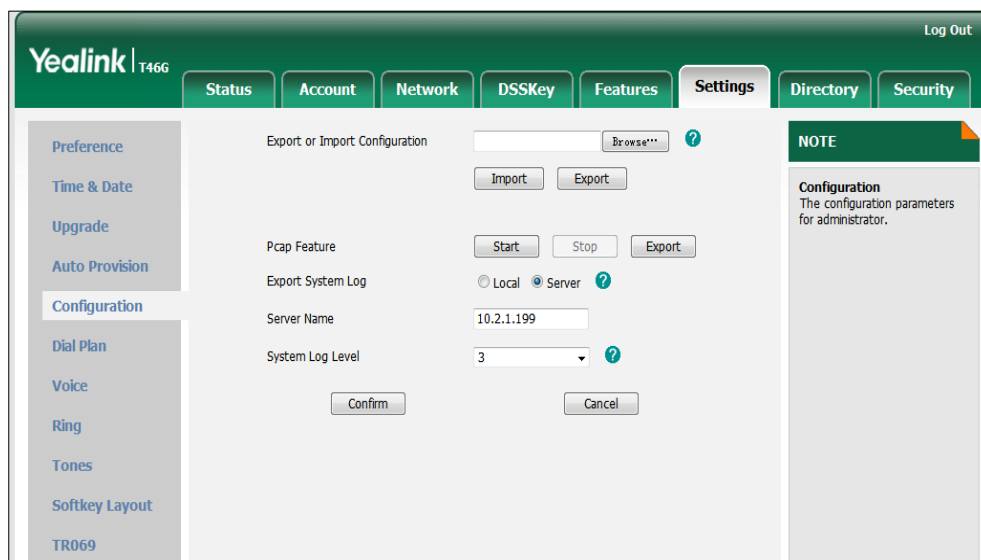


3. Click **Confirm** to accept the change.
A dialog box pops up to prompt "Do you want to restart your machine?".
4. Click **OK** to reboot the IP phone.
The configuration will take effect after reboot.

Note Administrator level debugging may make some sensitive information accessible (e.g., password-dial number). We recommend that you reset the system log level to 3 after having provided the system log file.

To configure the phone to export the system log to a syslog server via web user interface:

1. Click on **Settings->Configuration**.
2. Mark the **Server** radio box in the **Export System Log** field.
3. Enter the IP address or domain name of the syslog server in the **Server Name** field.

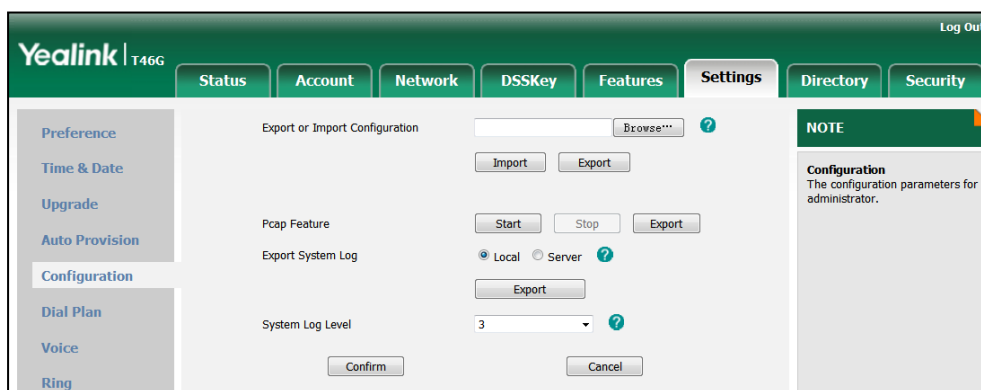


4. Click **Confirm** to accept the change.
A dialog box pops up to prompt "Do you want to restart your machine?".

- Click **OK** to reboot the IP phone.
The system log will be exported to the desired syslog server after reboot.

To export a log file to the local system via web user interface:

- Click on **Settings->Configuration**.
- Mark the **Local** radio box in the **Export System Log** field.
- Click **Export** to open file download window, and then save the file to your local system.
- Reproduce the issue.



The following figure shows a portion of a log file:

```

190 root      2856 S      /bin/sh /boot/script/netapp.sh
197 root      22484 S     /boot/bin/rtServer.exx
210 root      2856 S      /usr/sbin/telnetd
211 root      17448 S     /boot/bin/autoServer.exx
249 root      3440 S      ./sbin/lighttpd -f /phone/bin/lighttpd/config/lighttpd
252 root      18924 S     /phone/www/WEB-INFO/bin/fcgiServer.exx
263 root      2856 S      /sbin/syslogd -S -O /tmp/log/000000000000.log -s 200
275 root      2856 S      /bin/sh /phone/scripts/phoneapp.sh
276 root      6092 S      ./pcap.exx
291 root      140m S     /phone/bin/dskPhone.exx -qws
300 root          0 SW<    [ethTx/0]
301 root          0 SW<    [ethStatus/0]
309 root      5060 S      /boot/bin/lldpd
310 root      5572 S      /boot/bin/lldpd
357 root          0 DW     [hwthread]
358 root          0 DW     [hausioctl]
359 root          0 SW<    [frameProfiler]
360 root          0 DW<    [Cadence]
369 root      14016 S     /phone/bin/vaServer -q -w -m ANY=5
388 root      2920 S      /phone/bin/snmpd -c /etc/snmpd.conf
389 root      2856 S      /bin/sh /phone/scripts/sipapp.sh
396 root      41396 S N    /phone/bin/sipServer.exx
415 root      1628 S      /phone/bin/busybox udhcpc -b -i eth0 -a -s /boot/bin/
487 root      2856 S      sh -c cd /tmp;ifconfig >> log/000000000000.log;ps >>
489 root      3180 R      ps
Mar 12 03:32:58 fcgiServer.exx: HttpResponseImpl::write() Begin. size= 1;count=1024
Mar 12 03:32:58 fcgiServer.exx: HttpResponseImpl::commitHeader() Begin
Mar 12 03:32:58 fcgiServer.exx: HttpResponseImpl::commitHeader() End2
Mar 12 03:32:58 fcgiServer.exx: HttpResponseImpl::write() End.write 1024 bytes
Mar 12 03:32:58 fcgiServer.exx: HttpResponseImpl::write() Begin. size= 1;count=1024
Mar 12 03:32:58 fcgiServer.exx: HttpResponseImpl::commitHeader() Begin
Mar 12 03:32:58 fcgiServer.exx: HttpResponseImpl::commitHeader() End

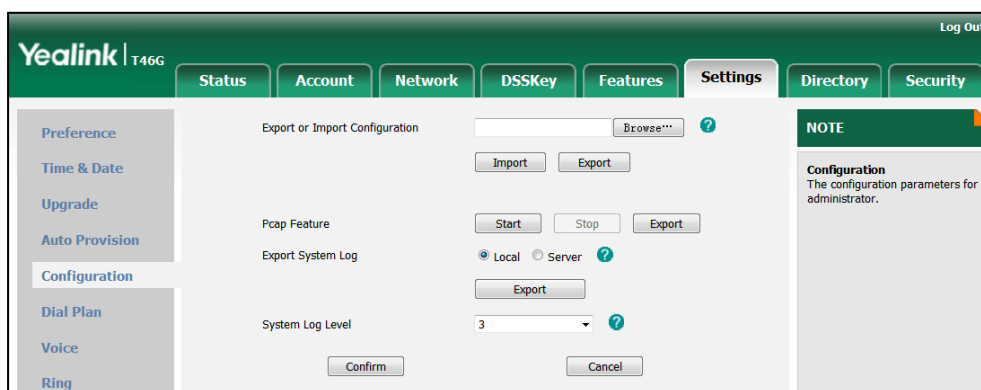
```

Capturing Packets

You can capture packets in two ways: capturing the packets via web user interface or using the Ethernet software. You can analyze the packets captured for troubleshooting purpose.

To capture packets via web user interface:

1. Click on **Settings->Configuration**.
2. Click **Start** to start capturing signal traffic.
3. Reproduce the issue to get stack traces.
4. Click **Stop** to stop capturing.
5. Click **Export** to open the file download window, and then save the file to your local system.



To capture packets using the Ethernet software:

Connect the Internet port of the IP phone and the PC to the same HUB, and then use Sniffer, Ethereal or Wireshark software to capture the signal traffic.

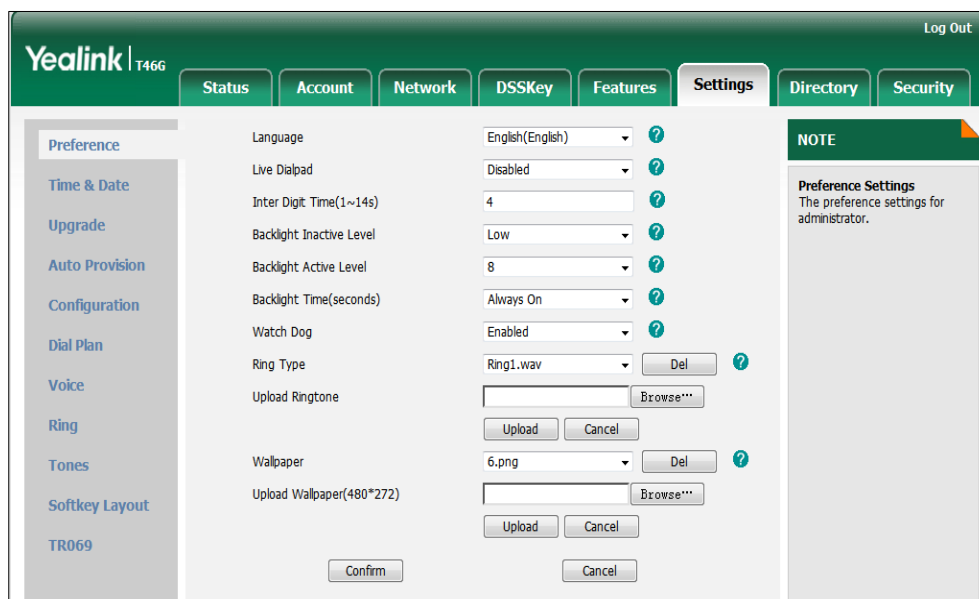
Enabling the Watch Dog Feature

IP phones support a troubleshooting feature called Watch Dog, which helps you monitor IP phones status and provides the ability to get stack traces from the last time the IP phone failed. If watch dog is enabled, IP phones will automatically reboot when it detects a fatal failure. This feature can be configured using the configuration files or via web user interface.

You can use the "watch_dog.enable" parameter to configure watch dog in the configuration files. For more information, refer to [Watch Dog](#) on page 380.

To configure watch dog via web user interface:

1. Click on **Settings->Preference**.
2. Select the desired value from the pull-down list of **Watch Dog**.



3. Click **Confirm** to accept the change.

Getting Information from Status Indicators

Status indicators may consist of the power LED, line key indicator, headset key indicator mute key indicator and the on-screen icon.

The following shows two examples of obtaining the phone information from status indicators on SIP-T46G IP phones:

- If a LINK failure of the IP phone is detected, a prompting message “Network Unavailable” and the icon will appear on the LCD screen.
- If an active call on the IP phone is on mute, the Mute key LED illuminates.

For more information on the icons, refer to [Reading Icons](#) on page 16.

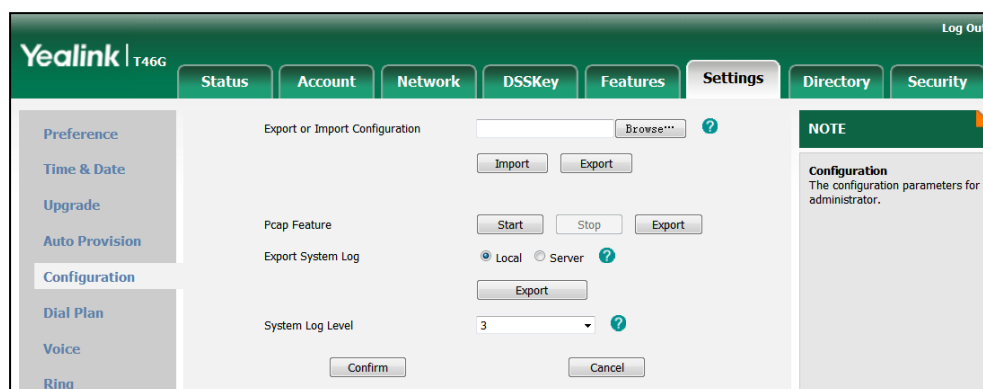
Analyzing Configuration Files

Wrong configurations may have an impact on your phone use. You can export configuration file to check the current configuration of the IP phone and troubleshoot if necessary.

To export configuration file via web user interface:

1. Click on **Settings->Configuration**.

2. In the **Export or Import Configuration** block, click **Export** to open the file download window, and then save the file to your local system.



Troubleshooting Solutions

This section describes solutions to common issues that may occur while using the IP phone. Upon encountering a scenario not listed in this section, contact your Yealink reseller for further support.

Why is the LCD screen blank?

Do one of the following:

- Ensure that the IP phone is properly plugged into a functional AC outlet.
- Ensure that the IP phone is plugged into a socket controlled by a switch that is on.
- If the IP phone is plugged into a power strip, try plugging it directly into a wall outlet.
- If your phone is PoE powered, ensure you are using a PoE-compliant switch or hub.

Why doesn't the IP phone get an IP address?

Do one of the following:

- Ensure that the Ethernet cable is plugged into the Internet port on the IP phone and the Ethernet cable is not loose.
- Ensure that the Ethernet cable is not damaged.
- Ensure that the IP address and related network parameters are set correctly.
- Ensure that your network switch or hub is operational.

How do I find the basic information of the IP phone?

Press the OK key when the IP phone is idle to check the basic information (e.g., IP address, MAC address and firmware version).

Why doesn't the IP phone upgrade firmware successfully?

Do one of the following:

- Ensure that the target firmware is not the same as the current firmware.
- Ensure that the target firmware is applicable to the IP phone model.
- Ensure that the current or the target firmware is not protected.
- Ensure that the power is on and the network is available in the process of upgrading.
- Ensure that the web browser is not closed and refreshed when upgrading firmware via web user interface.

Why doesn't the IP phone display time and date correctly?

Check if the IP phone is configured to obtain the time and date from the NTP server automatically. If your phone is unable to access the NTP server, configure the time and date manually.

Why do I get poor sound quality during a call?

If you have poor sound quality/acoustics like intermittent voice, low volume, echo or other noise, the possible reasons could be:

- Users are seated too far out of recommended microphone range and sound faint, or are seated too close to sensitive microphones and cause echo.
- Intermittent voice is mainly caused by packet loss, due to network congestion, and jitter, due to message recombination of transmission or receiving equipment (i.e. timeout handling, retransmission mechanism, buffer under run).
- Noisy equipment, such as a computer or a fan, may cause voice interference. Turn off any noisy equipment.
- Line issues can also cause this problem; disconnect the old line and redial the call to ensure another line may provide better connection.

What is the difference between a remote phone book and a local phonebook?

A remote phone book is placed on a server, while a local phonebook is placed on the IP phone flash. A remote phone book can be used by everyone that can access the server, while a local phonebook can only be used by a specific phone. A remote phone book is always used as a central phonebook for a company; each employee can load it to obtain the real-time data from the same server.

What is the difference between user name, register name and display name?

Both user name and register name are defined by the server. User name identifies the account, while register name matched with a password is for authentication purposes. Display name is the caller ID that will be displayed on the callee's phone LCD screen. Server configurations may override the local ones.

How to reboot IP phone remotely?

IP phones support remote reboot by a SIP NOTIFY message with "Event: check-sync" header. The parameter "reboot=true" makes the IP phone reboot immediately after receiving the NOTIFY message. The message is formed as below:

```
NOTIFY sip:<user>@<dsthost> SIP/2.0
To: sip:<user>@<dsthost>
From: sip:sipsak@<srchost>
CSeq: 10 NOTIFY
Call-ID: 1234@<srchost>
Event: check-sync;reboot=true
```

How to increase or decrease the volume?

You can press the volume key to increase or decrease the ringer volume and receiver volume. Press the volume key to adjust the ringer volume when the phone is idle, or to adjust the volume of the engaged audio device (handset, speakerphone or headset) when there is an active call in progress.

What will happen if I connect both PoE cable and power adapter?

Which has the higher priority?

IP phones use the PoE preferentially.

What is auto provisioning?

Auto provisioning refers to the update of IP phones, including update on the configuration parameters, local phonebook, firmware and so on. You can use auto provisioning on a single phone, but it makes more sense in mass deployment.

What is PnP?

Plug and Play (PnP) is a method for IP phones to acquire the provisioning server address. With PnP enabled, the IP phone broadcasts the PNP SUBSCRIBE message to obtain a provisioning server address during startup. Any SIP server recognizing the message will respond with the preconfigured provisioning server address, so the IP phone will be able to download the configuration files from the provisioning server. PnP depends on support from a SIP server.

Why doesn't the IP phone update the configuration?

Do one of the following:

- Ensure that the configuration is set correctly.
- Reboot the IP phone. Some configurations require a reboot to take effect.
- Ensure that the configuration is applicable to the IP phone model.
- The configuration may depend on support from a server.

What do "on code" and "off code" mean?

They are codes that the IP phone sends to the server when a certain action takes place. On code is used to activate a feature on the server side, while off code is used to deactivate a feature on the server side.

For example, if you set the Always Forward on code to be *78 (may vary on different servers), and the target number to be 201. When you enable Always Forward on the IP phone, the IP phone sends *78201 to the server, and then the server will enable the Always Forward feature on the server side, hence being able to get the right status of the extension.

How to solve the IP conflict problem?

Do one of the following:

- Reset another available IP address for the IP phone.
- Check network configuration via phone user interface at the path **Menu->Advanced->Network->WAN Port->IPv4 (or IPv6)**. If the Static IP is selected, select DHCP instead.

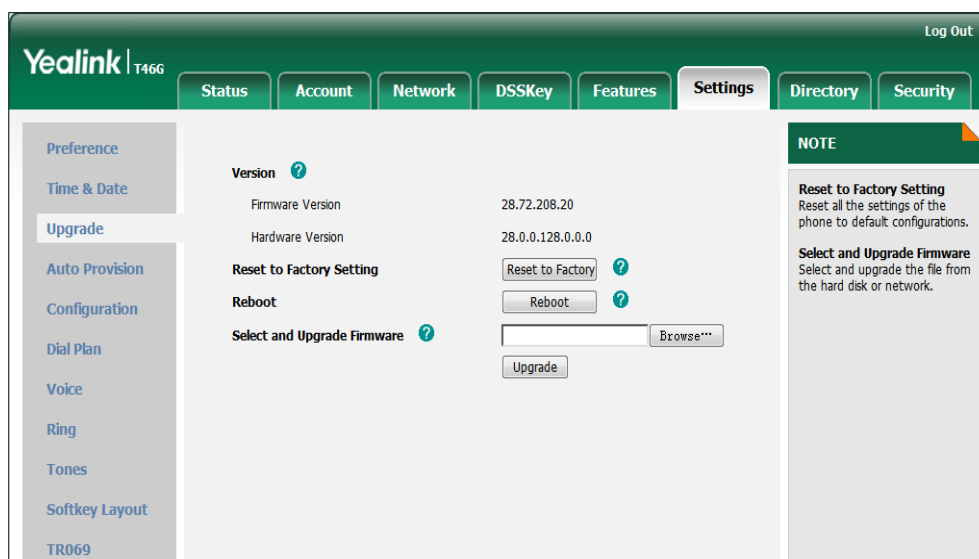
How to reset your phone to factory configurations?

Reset your phone to factory configurations after you have tried all troubleshooting suggestions but do not resolve the problem. Note that all custom settings will be overwritten after resetting.

To reset your phone via web user interface:

1. Click on **Settings->Upgrade**.
2. Click **Reset** in the **Reset to Factory Setting** field.

The web user interface prompts the message "Do you want to reset to factory?".



3. Click **OK** to confirm the resetting.
The phone will be reset to factory successfully after startup.

Note

Reset of the phone may take a few minutes. Do not power off until the phone starts up successfully.

How to restore the administrator password?

Factory reset can restore the original password. All custom settings will be overwritten after reset.

Appendix

Appendix A: Glossary

802.1x — an IEEE Standard for port-based Network Access Control (PNAC). It is a part of the IEEE 802.1 group of networking protocols. It offers an authentication mechanism for devices to connect to a LAN or WLAN.

ACD (Automatic Call Distribution) — used to distribute calls from large volumes of incoming calls to the registered IP phone users.

ACS (Auto Configuration server) — responsible for auto-configuration of the Central Processing Element (CPE).

Cryptographic Key — a piece of variable data that is fed as input into a cryptographic algorithm to perform operations such as encryption and decryption, or signing and verification.

DHCP (Dynamic Host Configuration Protocol) — built on a client-server model, where designated DHCP server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts.

DHCP Option — can be configured for specific values and enabled for assignment and distribution to DHCP clients based on server, scope, class or client-specific levels.

DNS (Domain Name System) — a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network.

EAP-MD5 (Extensible Authentication Protocol-Message Digest Algorithm 5) — only provides authentication of the EAP peer to the EAP server but not mutual authentication.

EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) — Provides for mutual authentication, integrity-protected cipher suite negotiation between two endpoints.

PEAP-MSCHAPV2 (Protected Extensible Authentication Protocol-Microsoft Challenge Handshake Authentication Protocol Version 2) — Provides for mutual authentication, but does not require a client certificate on the IP phone.

FAC (Feature Access Code) — special patterns of characters that are dialed from a phone keypad to invoke particular features.

HTTP (Hypertext Transfer Protocol) — used to request and transmit data on the World Wide Web.

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) — a widely-used communications protocol for secure communication over a network.

IEEE (Institute of Electrical and Electronics Engineers) — a non-profit professional association headquartered in New York City that is dedicated to advancing technological innovation and excellence.

LAN (Local Area Network) — used to interconnects network devices in a limited area such as a home, school, computer laboratory, or office building.

MIB (Management Information Base) — a virtual database used for managing the entities in a communications network.

OID (Object Identifier) — assigned to an individual object within a MIB.

PNP (Plug and Play) — a term used to describe the characteristic of a computer bus, or device specification, which facilitates the discovery of a hardware component in a system, without the need for physical device configuration, or user intervention in resolving resource conflicts.

ROM (Read-only Memory) — a class of storage medium used in computers and other electronic devices.

RTP (Real-time Transport Protocol) — provides end-to-end service for real-time data.

TCP (Transmission Control Protocol) — a transport layer protocol used by applications that require guaranteed delivery.

UDP (User Datagram Protocol) — a protocol offers non-guaranteed datagram delivery.

URI (Uniform Resource Identifier) — a compact sequence of characters that identifies an abstract or physical resource.

URL (Uniform Resource Locator) — specifies the address of an Internet resource.

VLAN (Virtual LAN) — a group of hosts with a common set of requirements, which communicate as if they were attached to the same broadcast domain, regardless of their physical location.

VoIP (Voice over Internet Protocol) — a family of technologies used for the delivery of voice communications and multimedia sessions over IP networks.

WLAN (Wireless Local Area Network) — a type of local area network that uses high-frequency radio waves rather than wires to communicate between nodes.

XML-RPC (Remote Procedure Call Protocol) — which uses XML to encode its calls and HTTP as a transport mechanism.

Appendix B: Time Zones

Time Zone	Time Zone Name
- 11:00	Samoa
- 10:00	United States-Hawaii-Aleutian
- 10:00	United States-Alaska-Aleutian
- 09:00	United States-Alaska Time
- 08:00	Canada(Vancouver, Whitehorse)
- 08:00	Mexico(Tijuana, Mexicali)
- 08:00	United States-Pacific Time
- 07:00	Canada(Edmonton, Calgary)
- 07:00	Mexico(Mazatlan, Chihuahua)
- 07:00	United States-Mountain Time
- 07:00	United States-MST no DST
- 06:00	Canada-Manitoba(Winnipeg)
- 06:00	Chile(Easter Islands)
- 06:00	Mexico(Mexico City, Acapulco)
- 06:00	United States-Central Time
- 05:00	Bahamas(Nassau)
- 05:00	Canada(Montreal, Ottawa, Quebec)
- 05:00	Cuba(Havana)
- 05:00	United States-Eastern Time
- 04:30	Venezuela(Caracas)
- 04:00	Canada(Halifax, Saint John)
- 04:00	Chile(Santiago)
- 04:00	Paraguay(Asuncion)
- 04:00	United Kingdom-Bermuda(Bermuda)
- 04:00	United Kingdom(Falkland Islands)
- 04:00	Trinidad&Tobago
- 03:30	Canada-New Foundland(St.Johns)
- 03:00	Denmark-Greenland(Nuuk)
- 03:00	Argentina(Buenos Aires)
- 03:00	Brazil(no DST)
- 03:00	Brazil(DST)
- 02:00	Brazil(no DST)
- 01:00	Portugal(Azores)
0	GMT
0	Greenland
0	Denmark-Faroe Islands(Torshavn)
0	Ireland(Dublin)
0	Portugal(Lisboa, Porto, Funchal)
0	Spain-Canary Islands(Las Palmas)

Time Zone	Time Zone Name
0	United Kingdom(London)
0	Morocco
+01:00	Albania(Tirane)
+01:00	Austria(Vienna)
+01:00	Belgium(Brussels)
+01:00	Caicos
+01:00	Chad
+01:00	Spain(Madrid)
+01:00	Croatia(Zagreb)
+01:00	Czech Republic(Prague)
+01:00	Denmark(Kopenhagen)
+01:00	France(Paris)
+01:00	Germany(Berlin)
+01:00	Hungary(Budapest)
+01:00	Italy(Rome)
+01:00	Luxembourg(Luxembourg)
+01:00	Macedonia(Skopje)
+01:00	Netherlands(Amsterdam)
+01:00	Namibia(Windhoek)
+02:00	Estonia(Tallinn)
+02:00	Finland(Helsinki)
+02:00	Gaza Strip(Gaza)
+02:00	Greece(Athens)
+02:00	Israel(Tel Aviv)
+02:00	Jordan(Amman)
+02:00	Latvia(Riga)
+02:00	Lebanon(Beirut)
+02:00	Moldova(Kishinev)
+02:00	Russia(Kaliningrad)
+02:00	Romania(Bucharest)
+02:00	Syria(Damascus)
+02:00	Turkey(Ankara)
+02:00	Ukraine(Kyiv, Odessa)
+03:00	East Africa Time
+03:00	Iraq(Baghdad)
+03:00	Russia(Moscow)
+03:30	Iran(Teheran)
+04:00	Armenia(Yerevan)
+04:00	Azerbaijan(Baku)
+04:00	Georgia(Tbilisi)
+04:00	Kazakhstan(Aktau)
+04:00	Russia(Samara)

Time Zone	Time Zone Name
+04:30	Afghanistan
+05:00	Kazakhstan(Aqtobe)
+05:00	Kyrgyzstan(Bishkek)
+05:00	Pakistan(Islamabad)
+05:00	Russia(Chelyabinsk)
+05:30	India(Calcutta)
+06:00	Kazakhstan(Astana, Almaty)
+06:00	Russia(Novosibirsk, Omsk)
+07:00	Russia(Krasnoyarsk)
+07:00	Thailand(Bangkok)
+08:00	China(Beijing)
+08:00	Singapore(Singapore)
+08:00	Australia(Perth)
+09:00	Korea(Seoul)
+09:00	Japan(Tokyo)
+09:30	Australia(Adelaide)
+09:30	Australia(Darwin)
+10:00	Australia(Sydney, Melbourne, Canberra)
+10:00	Australia(Brisbane)
+10:00	Australia(Hobart)
+10:00	Russia(Vladivostok)
+10:30	Australia(Lord Howe Islands)
+11:00	New Caledonia(Noumea)
+12:00	New Zealand(Wellington, Auckland)
+12:45	New Zealand(Chatham Islands)
+13:00	Tonga(Nukualofa)

Appendix C: Configuration Parameters

This appendix describes configuration parameters in the configuration files for each feature. The configuration files are <y0000000000xx>.cfg and <MAC>.cfg.

Setting Parameters in Configuration Files

You can set parameters in the configuration files to configure IP phones. The <y0000000000xx>.cfg and <MAC>.cfg files are stored on the provisioning server. The IP phone checks for configuration files and looks for resource files when restarting the IP phone. The <y0000000000xx>.cfg file stores configurations for all phones of the same model. The <MAC>.cfg file stores configurations for a specific IP phone with that MAC address.

Configuration changes made in the <MAC>.cfg file override the configuration settings in the <y0000000000xx>.cfg file.

Basic and Advanced Feature Parameters

DHCP

Parameter-	Configuration File
network.internet_port.type	<MAC>.cfg
Description	Configures the Internet port type. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer
Default Value	0
Range	Valid values are: 0-DHCP 1-PPPoE (not applicable to SIP-T42G/T41P) 2-Static IP Address
Example	network.internet_port.type= 0

Parameter-	Configuration File
network.static_dns_enable	<y0000000000xx>.cfg
Description	Enables or disables the phone to use manually configured static IPv4 DNS when the

	parameter "network.internet_port.type" is set to 0 (DHCP). Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	network.static_dns_enable= 0

Static Network Settings

Parameter- network.internet_port.type	Configuration File <MAC>.cfg
Description	Configures the Internet port type. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer
Default Value	0
Range	Valid values are: 0-DHCP 1-PPPoE (not applicable to SIP-T42G/T41P) 2-Static IP Address
Example	network.internet_port.type = 2

Parameter- network.ip_address_mode	Configuration File <MAC>.cfg
Description	Configures the IP addressing mode. IP phones support to use the IPv4 address only, the IPv6 address only or both IPv4 and IPv6 addresses. Note: If you change this parameter, the IP phone will reboot to make the change take effect.

Format	Integer
Default Value	0
Range	Valid values are: 0-IPv4 1-IPv6 2-IPv4&IPv6
Example	network.ip_address_mode = 0

Parameter- network.internet_port.ip	Configuration File <MAC>.cfg
Description	Configures the IP address when the Internet port type is configured as Static IP Address. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	IPv4 Address
Default Value	Blank
Range	Not Applicable
Example	network.internet_port.ip = 192.168.1.20

Parameter- network.internet_port.mask	Configuration File <MAC>.cfg
Description	Configures the subnet mask when the Internet port type is configured as Static IP Address. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Subnet Mask
Default Value	Blank
Range	Not Applicable
Example	network.internet_port.mask = 255.255.255.0

Parameter- network.internet_port.gateway	Configuration File <MAC>.cfg
Description	Configures the default gateway when the Internet port type is configured as Static IP

	Address. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	IPv4 Address
Default Value	Blank
Range	Not Applicable
Example	network.internet_port.gateway = 192.168.1.254

Parameter- network.primary_dns	Configuration File <MAC>.cfg
Description	Configures the primary DNS server when the Internet port type is configured as Static IP Address. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	IPv4 Address
Default Value	Blank
Range	Not Applicable
Example	network.primary_dns = 202.101.103.5

Parameter- network.secondary_dns	Configuration File <MAC>.cfg
Description	Configures the secondary DNS server when the Internet port type is configured as Static IP Address. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	IPv4 Address
Default Value	Blank
Range	Not Applicable
Example	network.secondary_dns = 202.101.103.6

PPPoE

Parameter-	Configuration File
network.internet_port.type	<MAC>.cfg
Description	Configures the Internet port type. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer
Default Value	0
Range	Valid values are: 0-DHCP 1-PPPoE (not applicable to SIP-T42G/T41P) 2-Static IP Address
Example	network.internet_port.type = 1

Parameter-	Configuration File
network.pppoe.user	<y0000000000xx>.cfg
Description	Configures the PPPoE user name when the Internet port type is configured as PPPoE. Note: If you change this parameter, the IP phone will reboot to make the change take effect. It is only applicable to SIP-T46G IP phones.
Format	String
Default Value	Blank
Range	String within 32 characters
Example	network.pppoe.user = xmyealink

Parameter-	Configuration File
network.pppoe.password	<y0000000000xx>.cfg
Description	Configures the PPPoE password when the Internet port type is configured as PPPoE. Note: If you change this parameter, the IP phone will reboot to make the change take effect. It is only applicable to SIP-T46G IP

	phones.
Format	String
Default Value	Blank
Range	String within 99 characters
Example	network.pppoe.password = yealink123

Internet and PC Ports Transmission Methods

Internet Port Negotiation

Parameter- network.internet_port.speed_duplex	Configuration File <y0000000000xx>.cfg
Description	Configures the transmission method of Internet port. Note: We recommend that you do not change this parameter. If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer
Default Value	0
Range	Valid values are: 0-Auto negotiate 1-Full duplex, 10Mbps 2-Full duplex, 100Mbps 3-Half duplex, 10Mbps 4-Half duplex, 100Mbps 5-Full duplex, 1000Mbps (not applicable to SIP-T41P)
Example	network.internet_port.speed_duplex = 0

PC Port Transmission Method

Parameter- network.pc_port.speed_duplex	Configuration File <y0000000000xx>.cfg
Description	Configures the transmission method of PC port. Note: We recommend that you do not change this parameter. If you change this parameter, the IP phone will reboot to make the change

	take effect.
Format	Integer
Default Value	0
Range	<p>Valid values are:</p> <ul style="list-style-type: none"> 0-Auto negotiate 1-Full duplex, 10Mbps 2-Full duplex, 100Mbps 3-Half duplex, 10Mbps 4-Half duplex, 100Mbps 5-Full duplex, 1000Mbps (not applicable to SIP-T41P)
Example	network.pc_port.speed_duplex = 0

Dial Plan

Replace Rule

Parameter-	Configuration File
dialplan.replace.prefix.X	<y0000000000xx>.cfg
Description	Configures the string you want to replace. X ranges from 1 to 100.
Format	String
Default Value	Blank
Range	String within 32 characters
Example	dialplan.replace.prefix.1 = 91([5-7])12

Parameter-	Configuration File
dialplan.replace.replace.X	<y0000000000xx>.cfg
Description	Configures the alternate string instead of what the user enters. X ranges from 1 to 100.
Format	String
Default Value	Blank
Range	String within 32 characters
Example	dialplan.replace.replace.1 = 91\$12

Parameter-	Configuration File
dialplan.replace.line_id.X	<y0000000000xx>.cfg
Description	Configures the desired line to apply this replace rule. X ranges from 1 to 100. Note: Multiple line IDs are separated by commas.
Format	String
Default Value	Blank
Range	Valid values are: 0 to 6 (for SIP-T46G) 0 to 3 (for SIP-T42G/T41P)
Example	dialplan.replace.line_id.1 = 1,2

Dial-now

Parameter-	Configuration File
dialplan.dialnow.rule.X	<y0000000000xx>.cfg
Description	Configures the string used to match the numbers entered by the user. When entered numbers match the predefined dial-now rule, the IP phone will automatically dial out the numbers without pressing the send key. X ranges from 1 to 100.
Format	String
Default Value	Blank
Range	String within 511 characters
Example	dialplan.dialnow.rule.1 = 2216

Parameter-	Configuration File
dialplan.dialnow.line_id.X	<y0000000000xx>.cfg
Description	Configures the desired line to apply this dial-now rule. X ranges from 1 to 100. Note: Multiple line IDs are separated by commas.
Format	String

Default Value	Blank
Range	Valid values are: 0 to 6 (for SIP-T46G) 0 to 3 (for SIP-T42G/T41P)
Example	dialplan.dialnow.line_id.1 = 1,2,3

Parameter-	Configuration File
phone_setting.dialnow_delay	<y0000000000xx>.cfg
Description	Configures the delay time (in seconds) for the dial-now rule. When the entered numbers match the predefined dial-now rule, the IP phone will automatically dial out the entered number after the specified delay time.
Format	Integer
Default Value	1
Range	1 to 14
Example	phone_setting.dialnow_delay = 1

Area Code

Parameter-	Configuration File
dialplan.area_code.code	<y0000000000xx>.cfg
Description	Configures the area code to add before the entered numbers.
Format	String
Default Value	Blank
Range	String within 16 characters
Example	dialplan.area_code.code = 010

Parameter-	Configuration File
dialplan.area_code.min_len	<y0000000000xx>.cfg
Description	Configures the minimum length of the entered numbers.
Format	Integer
Default Value	1

Range	1 to 15
Example	dialplan.area_code.min_len = 1

Parameter- dialplan.area_code.max_len	Configuration File <y0000000000xx>.cfg
Description	Configures the maximum length of the entered numbers. Note: The value must be larger than the minimum length.
Format	Integer
Default Value	15
Range	1 to 15
Example	dialplan.area_code.max_len = 15

Parameter- dialplan.area_code.line_id	Configuration File <y0000000000xx>.cfg
Description	Configures the desired line to apply this area code rule. Note: Multiple line IDs are separated by commas.
Format	Integer
Default Value	Blank (for all lines)
Range	Valid values are: 0 to 6 (for SIP-T46G) 0 to 3 (for SIP-T42G/T41P)
Example	dialplan.area_code.line_id = 1,2

Block Out

Parameter- dialplan.block_out.number.X	Configuration File <y0000000000xx>.cfg
Description	Configures the block out numbers. X ranges from 1 to 10.
Format	String
Default Value	Blank
Range	String within 32 characters

Example	dialplan.block_out.number.1 = 1000
----------------	------------------------------------

Parameter- dialplan.block_out.line_id.X	Configuration File <y0000000000xx>.cfg
Description	Configures the desired line to apply this block out rule. X ranges from 1 to 10. Note: Multiple line IDs are separated by commas.
Format	Integer
Default Value	Blank (for all lines)
Range	Valid values are: 0 to 6 (for SIP-T46G) 0 to 3 (for SIP-T42G/T41P)
Example	dialplan.block_out.line_id.1 = 1,2,3

Power Indicator LED

Parameter- phone_setting.common_power_led_enable	Configuration File <y0000000000xx>.cfg
Description	Enables or disables the power indicator LED to be turned on.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled (power indicator LED is off) 1-Enabled (power indicator LED is solid red)
Example	phone_setting.common_power_led_enable = 0

Parameter- phone_setting.ring_power_led_flash_enable	Configuration File <y0000000000xx>.cfg
Description	Enables or disables the power indicator LED to flash when the phone receives an incoming

	call. If it is set to 0, the status of the power indicator LED is determined by the value of the parameter "phone_setting.common_power_led_enable".
Format	Boolean
Default Value	1
Range	Valid values are: 0 -Disabled (power indicator LED does not flash) 1 -Enabled (power indicator LED fast flashes (300ms) red)
Example	phone_setting.ring_power_led_flash_enable = 1

Parameter- phone_setting.mail_power_led_flash_enable	Configuration File <y0000000000xx>.cfg
Description	Enables or disables the power indicator LED to flash when the phone receives a voice mail or a text message. If it is set to 0, the status of the power indicator LED is determined by the value of the parameter "phone_setting.common_power_led_enable".
Format	Boolean
Default Value	1
Range	Valid values are: 0 -Disabled (power indicator LED does not flash) 1 -Enabled (power indicator LED slow flashes (1000ms) red)
Example	phone_setting.mail_power_led_flash_enable = 1

Parameter- phone_setting.mute_power_led_flash_enable	Configuration File <y0000000000xx>.cfg
Description	Enables or disables the power indicator LED to flash when a call is mute. If it is set to 0, the status of the power indicator LED is determined by the value of the parameter "phone_setting.common_power_led_enable".
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled (power indicator LED does not flash) 1-Enabled (power indicator LED fast flashes (300ms) red)
Example	phone_setting.mute_power_led_flash_enable = 0

Parameter- phone_setting.hold_and_held_power_led_flash_enable	Configuration File <y0000000000xx>.cfg
Description	Enables or disables the power indicator LED to flash when a call is placed on hold or is held. If it is set to 0, the status of the power indicator LED is determined by the value of the parameter "phone_setting.common_power_led_enable".
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled (power indicator LED does not flash) 1-Enabled (power indicator LED fast flashes (500ms) red)
Example	phone_setting.hold_and_held_power_led_flash_enable = 0

Parameter-	Configuration File
phone_setting.talk_and_dial_power_led_enable	<y0000000000xx>.cfg
Description	Enables or disables the power indicator LED to be turned on when the phone is busy. If it is set to 0, the status of the power indicator LED is determined by the value of the parameter "phone_setting.common_power_led_enable".
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled (power indicator LED is off) 1-Enabled (power indicator LED is solid red)
Example	phone_setting.talk_and_dial_power_led_enable = 0

Contrast

Parameter-	Configuration File
phone_setting.contrast	<y0000000000xx>.cfg
Description	Configures the LCD's contrast of the connected EXP40 for SIP-T46G IP phones only. Note: We recommend that you set the contrast of the LCD screen to 6 as a more comfortable level.
Format	Integer
Default Value	6
Range	1 to 10
Example	phone_setting.contrast = 6

Backlight

Parameter- phone_setting.active_backlight_level	Configuration File <y0000000000xx>.cfg
Description	Configures the backlight level used to adjust the backlight intensity of the LCD screen. 10 is the brightest backlight level. Note: It is only applicable to SIP-T46G IP phones and the connected EXP40.
Format	Integer
Default Value	8
Range	1 to 10
Example	phone_setting.active_backlight_level = 8

Parameter- phone_setting.inactive_backlight_level	Configuration File <y0000000000xx>.cfg
Description	Configures whether the IP phone to turn off or turn dusky the backlight of the LCD screen after a period of inactivity. Note: It is only applicable to SIP-T46G IP phones.
Format	Boolean
Default Value	1
Range	Valid values are: 0-Off 1-Low
Example	phone_setting.inactive_backlight_level = 1

Parameter- phone_setting.backlight_time	Configuration File <y0000000000xx>.cfg
Description	Configures the delay time to turn off the backlight when the IP phone is inactive. If it is set to 60, the LCD backlight is turned off

	when the IP phone is inactive for 60 seconds.
Format	Integer
Default Value	0
Range	Valid values are: 0 -Always on 15 -15s 30 -30s 60 -60s 120 -120s 300 -300s 600 -600s 1800 -1800s
Example	phone_setting.backlight_time = 0

User Password

Parameter-	Configuration File
security.user_password	<y0000000000xx>.cfg
Description	<p>Configures a new user password for the IP phone.</p> <p>The IP phone uses "user" as the default user password.</p> <p>A valid password should contain at least 6 characters, where at least one numeric and one alphabetic characters.</p> <p>Note: IP phones support ASCII characters 32-126(0x20-0x7E) only in passwords.</p>
Format	user name:new password
Default Value	user
Range	ASCII characters 32-126(0x20-0x7E)
Example	security.user_password = user:password123

Administrator Password

Parameter-	Configuration File
security.user_password	<y0000000000xx>.cfg
Description	Configures a new administrator password for

	<p>the IP phone.</p> <p>The IP phone uses "admin" as the default administrator password.</p> <p>A valid password should contain at least 6 characters, where at least one numeric and one alphabetic characters.</p> <p>Note: IP phones support ASCII characters 32-126(0x20-0x7E) only in passwords.</p>
Format	administrator name:new password
Default Value	admin
Range	ASCII characters 32-126(0x20-0x7E)
Example	security.user_password = admin:password000

Phone Lock

Parameter- phone_setting.phone_lock.enable	Configuration File <y0000000000xx>.cfg
Description	Enables or disables phone lock feature.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	phone_setting.phone_lock.enable= 1

Parameter- phone_setting.phone_lock.lock_key_type	Configuration File <y0000000000xx>.cfg
Description	<p>Configures the type of phone lock.</p> <p>Menu Key: The Menu soft key is locked.</p> <p>Function Keys: MESSAGE, Redial, HOLD, MUTE, TRAN, OK, X, navigation keys, soft keys and line keys are locked.</p> <p>All Keys: All keys are locked, except the Volume, Headset, Speakerphone and digit keys.</p>

Format	Integer
Default Value	0
Range	Valid values are: 0-All Keys 1-Function Keys 2-Menu Key
Example	phone_setting.phone_lock.lock_key_type = 0

Parameter- phone_setting.phone_lock.unlock_pin	Configuration File <y0000000000xx>.cfg
Description	Configures a new unlock password. Once the IP phone is locked, you can use the default password "123" to unlock it.
Format	numeric characters
Default Value	123
Range	characters within 15 digits
Example	phone_setting.phone_lock.unlock_pin = 123

Parameter- phone_setting.phone_lock.lock_time_out	Configuration File <y0000000000xx>.cfg
Description	Configures the IP phone to automatically lock the keypad after a delay time (in seconds). If it is set to 0, the keypad will not be locked automatically. In this case, you can long press the pound key to lock the keypad. Note: This parameter works only if the IP phone lock type is preset.
Format	Integer
Default Value	0
Range	0 to 3600
Example	phone_setting.phone_lock.lock_time_out = 0

Time and Date

Parameter- local_time.manual_time_enable	Configuration File <MAC>.cfg
Description	Configures the phone to obtain time from NTP server or manual settings.
Format	Integer
Default Value	1
Range	Valid values are: 0-Manual 1-NTP
Example	local_time.manual_time_enable = 1

NTP Server

Parameter- local_time.manual_ntp_srv_prior	Configuration File <MAC>.cfg
Description	Enables or disables the phone to use manually configured NTP server preferentially.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled (use the NTP server obtained by DHCP preferentially) 1-Enabled
Example	local_time.manual_ntp_srv_prior = 0

Parameter- local_time.ntp_server1	Configuration File <MAC>.cfg
Description	Configures the IP address or the domain name of the primary NTP server.
Format	IP Address or Domain Name
Default Value	cn.pool.ntp.org
Range	String within 99 characters

Example	local_time.ntp_server1 = 192.168.0.5
----------------	--------------------------------------

Parameter-	Configuration File
local_time.ntp_server2	<MAC>.cfg
Description	Configures the IP address or the domain name of the secondary NTP server. If the primary NTP server is not configured or cannot be accessed, the IP phone will request the time and date from the secondary NTP server.
Format	IP Address or Domain Name
Default Value	cn.pool.ntp.org
Range	String within 99 characters
Example	local_time.ntp_server2 = 192.168.0.6

Parameter-	Configuration File
local_time.interval	<MAC>.cfg
Description	Configures the IP phone to update time and date from the NTP server at regular intervals (in seconds).
Format	Integer
Default Value	1000
Range	15 to 86400
Example	local_time.interval = 1000

Time Zone

Parameter-	Configuration File
local_time.time_zone	<MAC>.cfg
Description	Configures the time zone. For more available time zones, refer to Appendix B: Time Zones on page 245.
Format	String
Default Value	+8
Range	-11 to +13
Example	local_time.time_zone = +8

Parameter-	Configuration File
local_time.time_zone_name	<MAC>.cfg
Description	Configures the desired time zone name. For more available time zone names, refer to Appendix B: Time Zones on page 245.
Format	String
Default Value	China(Beijing)
Range	String within 32 characters
Example	local_time.time_zone_name = China(Beijing)

DST

Parameter-	Configuration File
local_time.summer_time	<MAC>.cfg
Description	Enables or disables Daylight Saving Time (DST) feature.
Format	Integer
Default Value	2
Range	Valid values are: 0-Disabled 1-Enabled 2-Automatic
Example	local_time.summer_time = 2

Parameter-	Configuration File
local_time.dst_time_type	<MAC>.cfg
Description	Configures the offset time (in minutes). Note: It works only if the parameter "local_time.summer_time" is set to 1 (Enabled).
Format	Integer
Default Value	0
Range	Valid values are: 0-By Date 1-By Week
Example	local_time.dst_time_type = 0

Parameter-	Configuration File
local_time.start_time	<MAC>.cfg
Description	<p>Configures the time to start DST.</p> <p>If "local_time.dst_time_type" is set to 0 (By Date), use the mapping:</p> <p>MM: 1=Jan, 2=Feb,..., 12=Dec</p> <p>DD:1=the first day in a month,..., 31= the last day in a month</p> <p>HH:0=1am, 1=2am,..., 23=12pm</p> <p>If "local_time.dst_time_type" is set to 1 (By Week), use the mapping:</p> <p>Month: 1=Jan, 2=Feb,..., 12=Dec</p> <p>Week of Month: 1=the first week in a month,..., 5=the last week in a month</p> <p>Day of Week: 1=Mon, 2=Tues,..., 7=Sun</p> <p>Hour of Day: 0=1am, 1=2am,..., 23=12pm</p> <p>Note: It works only if the parameter "local_time.summer_time" is set to 1 (Enabled).</p>
Format	<p>The value formats are:</p> <ul style="list-style-type: none"> • MM/DD/HH (For By Date) • Month/Week of Month/Day of Week/Hour of Day (For By Week)
Default Value	1/1/0
Range	1 to 12/1 to 31/0 to 23 (for By Date) 1 to 12/1 to 5/1 to 7/0 to 23 (for By Week)
Example	local_time.start_time = 1/1/0

Parameter-	Configuration File
local_time.end_time	<MAC>.cfg
Description	<p>Configures the time to end DST.</p> <p>If "local_time.dst_time_type" is set to 0 (By Date), use the mapping:</p> <p>MM: 1=Jan, 2=Feb,..., 12=Dec</p> <p>DD:1=the first day in a month,..., 31= the last day in a month</p> <p>HH:0=1am, 1=2am,..., 23=12pm</p>

	<p>If "local_time.dst_time_type" is set to 1 (By Week), use the mapping:</p> <p>Month: 1=Jan, 2=Feb,..., 12=Dec</p> <p>Week of Month: 1=the first week in a month,..., 5=the last week in a month</p> <p>Day of Week: 1=Mon, 2=Tues,..., 7=Sun</p> <p>Hour of Day: 0=1am, 1=2am,..., 23=12pm</p> <p>Note: It works only if the parameter "local_time.summer_time" is set to 1 (Enabled).</p>
Format	<p>The value formats are:</p> <ul style="list-style-type: none"> • MM/DD/HH (For By Date) • Month/Week of Month/Day of Week/Hour of Day (For By Week)
Default Value	12/31/23
Range	1to 12/1 to 31/0 to 23 (for By Date) 1 to 12/1 to 5/1 to 7/0 to 23 (for By Week)
Example	local_time.end_time = 12/31/23

Parameter-	Configuration File
local_time.dhcp_time	<MAC>.cfg
Description	<p>It enables or disables the phone to update time with the offset time obtained from the DHCP server.</p> <p>Note: It is only available to offset from GMT 0.</p>
Format	Boolean
Default Value	0
Range	<p>Valid values are:</p> <p>0-Disabled</p> <p>1-Enabled</p>
Example	local_time.dhcp_time = 1

Parameter-	Configuration File
local_time.offset_time	<MAC>.cfg
Description	<p>Configures the offset time (in minutes) of DST.</p> <p>Note: It works only if the parameter "local_time.summer_time" is set to 1</p>

	(Enabled).
Format	Integer
Default Value	Blank
Range	-300 to +300
Example	local_time.offset_time = 120

Time Format

Parameter-	Configuration File
local_time.time_format	<MAC>.cfg
Description	Configures the time format. If it is set to 0 (12 Hour), the time display will use 12 hour format. If it is set to 1 (24 Hour), the time display will use 24 hour format.
Format	Integer
Default Value	1
Range	Valid values are: 0-12 Hour 1-24 Hour
Example	local_time.time_format = 1

Date Format

Parameter-	Configuration File
local_time.date_format	<MAC>.cfg
Description	Configures the date format.
Format	Integer
Default Value	0
Range	Valid values are: 0-WWW MMM DD 1-DD-MMM-YY 2-YYYY-MM-DD 3-DD/MM/YYYY 4-MM/DD/YY 5-DD MMM YYYY 6-WWW DD MMM
Example	local_time.date_format = 0

Language

Parameter- gui_lang.url	Configuration File <y0000000000xx>.cfg
Description	Configures the access URL of the language pack. Note: The language packs you load are dependent on available language packs from the provisioning server. You can download the language pack to the phone user interface only.
Format	URL
Default Value	Blank
Range	String within 511 characters
Example	The following example uses HTTP to download a new Russian language pack "lang-Russian.txt" from the provisioning server 192.168.10.25. gui_lang.url = http://192.168.10.25/lang-Russian.txt

Parameter- lang.gui	Configuration File <y0000000000xx>.cfg
Description	Configures the language used on the phone user interface.
Format	String
Default Value	English
Range	Valid values are: English Chinese_S (not applicable to SIP-T42G/T41P) Chinese_T (not applicable to SIP-T42G/T41P) French German Italian Polish Portuguese Spanish Turkish

Example	lang.gui = English
Parameter- lang.wui	Configuration File <y0000000000xx>.cfg
Description	Configures the language used on the web user interface. Note: The default language used on the web user interface depends on the language preferences of your browser. If the language of your browser is not supported by the IP phone, the web user interface will use English by default.
Format	String
Default Value	Blank
Range	Valid values are: English Chinese_S (not applicable to SIP-T42G/T41P) Chinese_T (not applicable to SIP-T42G/T41P) French German Italian Portuguese Spanish Turkish
Example	lang.wui = French

Logo Customization

Parameter- phone_setting.lcd_logo.mode	Configuration File <y0000000000xx>.cfg
Description	Configures the logo mode of the LCD screen. If it is set to 0 (Disabled), the IP phone is not allowed to display a logo. If it is set to 1 (System logo), the LCD screen will display the system logo. If it is set to 2 (Custom logo), the LCD screen will display the custom logo (you need to upload a custom logo file to the phone).

	Note: It is not applicable to SIP-T46G IP phones.
Format	Integer
Default Value	0
Range	Valid values are: 0-Disabled 1-System logo 2-Custom logo
Example	phone_setting.lcd_logo.mode = 2

Parameter-	Configuration File
lcd_logo.url	<y0000000000xx>.cfg
Description	Configures the access URL of custom logo file. Note: It is not applicable to SIP-T46G IP phones.
Format	URL
Default Value	Blank
Range	String within 511 characters
Example	The following example uses HTTP to download the custom logo file (logo.dob) from the provisioning server 192.168.10.25. lcd_logo.url = http://192.168.10.25/logo.dob

Key as Send

Parameter-	Configuration File
features.key_as_send	<y0000000000xx>.cfg
Description	Configures the "#" or "*" key as the send key. If it is set to 0 (Disabled), neither "#" nor "*" can be used as a send key. If it is set to 1 (# key), the pound key is used as the send key. If it is set to 2 (* key), the asterisk key is used as the send key.
Format	Integer
Default Value	1
Range	Valid values are:

	0 -Disabled 1 -# key 2 -* key
Example	features.key_as_send = 1

Parameter- features.key_tone	Configuration File <y0000000000xx>.cfg
Description	Enables or disables the IP phone to play a tone when a user presses a key. If it is set to 1 (Enabled), the IP phone will play a tone when a user presses a key.
Format	Boolean
Default Value	1
Range	Valid values are: 0 -Disabled 1 -Enabled
Example	features.key_tone = 1

Parameter- features.send_key_tone	Configuration File <y0000000000xx>.cfg
Description	Enables or disables the IP phone to play a tone when a user presses a send key. If it is set to 1 (Enabled), the IP phone will play a tone when a user presses a send key. Note: It works only if the parameter "features.key_tone" is set to 1 (Enabled).
Format	Boolean
Default Value	1
Range	Valid values are: 0 -Disabled 1 -Enabled
Example	features.send_key_tone = 1

Hotline

Parameter-	Configuration File
features.hotline_number	<y0000000000xx>.cfg
Description	Configures the hotline number. It specifies a number that the IP phone automatically dials out when lifting the handset, pressing the speakerphone key or the line key. Leaving it blank disables hotline feature.
Format	String
Default Value	Blank
Range	String within 32 characters
Example	features.hotline_number = 3601

Parameter-	Configuration File
features.hotline_delay	<y0000000000xx>.cfg
Description	Configures the waiting time (in seconds) the IP phone automatically dials out the hotline number. If it is set to 0, the IP phone immediately will dial out the preconfigured hotline number when you lift the handset, press the speakerphone key or press the line key. If it is set to a value greater than 0, the IP phone will wait the specified seconds before dialing out the predefined hotline number when you lift the handset, press the speakerphone key or the line key.
Format	Integer
Default Value	4
Range	0 to 10
Example	features.hotline_delay = 4

Call Log

Parameter-	Configuration File
features.save_call_history	<y0000000000xx>.cfg
Description	Enables or disables the IP phone to save call log. If it is set to 0 (Disabled), the IP phone cannot log the placed calls, received calls, missed calls and the forwarded calls in the call log lists.
Format	Boolean
Default Value	1
Range	Valid values are: 0-Disabled 1-Enabled
Example	features.save_call_history = 1

Missed Call Log

Parameter-	Configuration File
account.x.missed_calllog	<MAC>.cfg
Description	Enables or disables missed call log feature for account X. If it is set to 0 (Disabled), there is no indicator displaying on the LCD screen, the IP phone does not log the missed call in the Missed Calls list. If it is set to 1 (Enabled), a prompt message "<number> New Missed Call(s)" along with an indicator icon is displayed on the IP phone idle screen when the IP phone misses calls. X ranges from 1 to 6.
Format	Boolean
Default Value	1
Range	Valid values are: 0-Disabled 1-Enabled

Example	account.1.missed_calllog = 1
----------------	------------------------------

Live Dialpad

Parameter- phone_setting.predial_autodial	Configuration File <y0000000000xx>.cfg
Description	Enables or disables live dialpad feature. If it is set to 1 (Enabled), the IP phone will automatically dial out the entered phone number without having to press any key.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	phone_setting.predial_autodial = 1

Parameter- phone_setting.inter_digit_time	Configuration File <y0000000000xx>.cfg
Description	Configures the time (in seconds) for the phone to automatically dial out the entered digits without pressing any other key. Note: It works only if the parameter "phone_setting.predial_autodial" is set to 1 (Enabled).
Format	Integer
Default Value	4
Range	1 to 14
Example	phone_setting.inter_digit_time = 4

Call Waiting

Parameter- call_waiting.enable	Configuration File <y0000000000xx>.cfg
Description	Enables or disables call waiting feature. If it is set to 0 (Disabled), a new incoming call

	is automatically rejected by the IP phone with a busy message while during a call. If it is set to 1 (Enabled), the LCD screen will present a new incoming call while during a call.
Format	Boolean
Default Value	1
Range	Valid values are: 0-Disabled 1-Enabled
Example	call_waiting.enable = 1

Parameter- call_waiting.on_code	Configuration File <y0000000000xx>.cfg
Description	Configures the call waiting on code to activate the server-side call waiting feature.
Format	String
Default Value	Blank
Range	String within 32 characters
Example	call_waiting.on_code = *55

Parameter- call_waiting.off_code	Configuration File <y0000000000xx>.cfg
Description	Configures the call waiting off code to deactivate the server-side call waiting feature.
Format	String
Default Value	Blank
Range	String within 32 characters
Example	call_waiting.off_code = *56

Parameter- call_waiting.tone	Configuration File <y0000000000xx>.cfg
Description	Enables or disables the playing of a call waiting tone when the IP phone receives an incoming call during a call.

	<p>If it is set to 1 (Enabled), the IP phone will perform an audible indicator when receiving a new incoming call during a call.</p> <p>Note: It works only if the parameter "call_waiting.enable" is set to 1 (Enabled).</p>
Format	Boolean
Default Value	1
Range	<p>Valid values are:</p> <p>0-Disabled</p> <p>1-Enabled</p>
Example	call_waiting.tone = 1

Auto Redial

Parameter-	Configuration File
auto_redial.enable	<y0000000000xx>.cfg
Description	<p>Enables or disables the IP phone to automatically redial the called number when it is busy.</p> <p>If it is set to 1 (Enabled), the IP phone will dial the previous dialed out number automatically when the dialed number is busy.</p>
Format	Boolean
Default Value	0
Range	<p>Valid values are:</p> <p>0-Disabled</p> <p>1-Enabled</p>
Example	auto_redial.enable = 1

Parameter-	Configuration File
auto_redial.interval	<y0000000000xx>.cfg
Description	<p>Configures the interval (in seconds) for the IP phone to wait between redials.</p> <p>The IP phone redials the dialed number at regular intervals till the callee answers the call.</p>

Format	Integer
Default Value	10
Range	1 to 300
Example	auto_redial.interval = 10

Parameter- auto_redial.times	Configuration File <y0000000000xx>.cfg
Description	Configures the redial times for the IP phone. The IP phone tries to redial the dialed number as many times as configured till the callee answers the call.
Format	Integer
Default Value	10
Range	1 to 300
Example	auto_redial.times = 10

Auto Answer

Parameter- account.X.auto_answer	Configuration File <MAC>.cfg
Description	Enables or disables auto answer feature for account X. If it is set to 1 (Enabled), the IP phone can automatically answer an incoming call. X ranges from 1 to 6. Note: The IP phone cannot automatically answer the incoming call during a call even if auto answer is enabled.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	account.1.auto_answer = 1

Parameter-	Configuration File
features.auto_answer_delay	<y0000000000xx>.cfg
Description	Configures the delay time (in seconds) before the IP phone automatically answers an incoming call.
Format	Integer
Default Value	1
Range	1 to 4
Example	features.auto_answer_delay = 1

Call Completion

Parameter-	Configuration File
features.call_completion_enable	<y0000000000xx>.cfg
Description	Enables or disables call completion feature. If a user places a call and the callee is temporarily not available to answer the call, call completion feature allows notifying the user when the callee becomes available to receive a call. If it is set to 1 (Enabled), the caller is notified when the callee becomes available to receive a call.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	features.call_completion_enable = 1

Anonymous Call

Parameter-	Configuration File
account.X.anonymous_call	<MAC>.cfg
Description	Enables or disables anonymous call feature for account X.

	<p>If it is set to 1 (Enabled), the IP phone will block its identity from showing up to the callee when placing a call. The callee's phone LCD screen presents anonymous instead of the caller's identity.</p> <p>X ranges from 1 to 6.</p>
Format	Boolean
Default Value	0
Range	<p>Valid values are:</p> <p>0-Disabled</p> <p>1-Enabled</p>
Example	account.1.anonymous_call = 1

Parameter-	Configuration File
account.X.send_anonymous_code	<MAC>.cfg
Description	<p>Configures the phone to send anonymous on/off code to activate/deactivate the server-side anonymous call feature for account X.</p> <p>If it is set to 0 (Off Code), the IP phone will send anonymous off code to deactivate the server-side anonymous call feature.</p> <p>If it is set to 1 (On Code), the IP phone will send anonymous on code to activate the server-side anonymous call feature.</p> <p>X ranges from 1 to 6.</p>
Format	Boolean
Default Value	0
Range	<p>Valid values are:</p> <p>0-Off Code</p> <p>1-On Code</p>
Example	account.1.send_anonymous_code = 1

Parameter- account.X.anonymous_call_oncode	Configuration File <MAC>.cfg
Description	Configures the anonymous call on code to activate the server-side anonymous call feature for account X (optional). X ranges from 1 to 6.
Format	String
Default Value	Blank
Range	String within 32 characters
Example	account.1.anonymous_call_oncode = *72

Parameter- account.X.anonymous_call_offcode	Configuration File <MAC>.cfg
Description	Configures the anonymous call off code to deactivate the server-side anonymous call feature for account X (optional). X ranges from 1 to 6.
Format	String
Default Value	Blank
Range	String within 32 characters
Example	account.1.anonymous_call_offcode = *73

Anonymous Call Rejection

Parameter- account.X.reject_anonymous_call	Configuration File <MAC>.cfg
Description	Enables or disables anonymous call rejection feature for account X. If it is set to 1 (Enabled), the IP phone will automatically reject incoming calls from anonymity. The anonymous user's LCD screen presents "Anonymity Disallowed". X ranges from 1 to 6.

Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	account.1.reject_anonymous_call = 1

Parameter- account.X.anonymous_reject_oncode	Configuration File <MAC>.cfg
Description	Configures the anonymous call rejection on code to activate the server-side anonymous call rejection feature for account X (optional). X ranges from 1 to 6.
Format	String
Default Value	Blank
Range	String within 32 characters
Example	account.1.anonymous_reject_oncode = *74

Parameter- account.X.anonymous_reject_offcode	Configuration File <MAC>.cfg
Description	Configures the anonymous call rejection off code to deactivate the server-side anonymous call rejection feature for account X (optional). X ranges from 1 to 6.
Format	String
Default Value	Blank
Range	String within 32 characters
Example	account.1.anonymous_reject_offcode = *75

Do Not Disturb

Return Message When DND

Parameter-	Configuration File
features.dnd_refuse_code	<y0000000000xx>.cfg
Description	Configures a return code and reason of SIP response messages when rejecting an incoming call by DND. A specific reason is displayed on the caller's phone LCD screen. If it is set to 486 (Busy here), the caller's LCD screen will display the reason "Busy here" when the callee enables DND.
Format	Integer
Default Value	480
Range	Valid values are: 404 -No Found 480 -Temporarily Not Available 486 -Busy Here
Example	features.dnd_refuse_code = 480

DND Mode

Parameter-	Configuration File
features.dnd_mode	<y0000000000xx>.cfg
Description	Configures the DND mode for the IP phone. If it is set to 0 (Phone), the DND feature is effective for the IP phone. If it is set to 1 (Custom), you can configure DND feature for each account.
Format	Integer
Default Value	0
Range	0 -Phone 1 -Custom
Example	features.dnd_mode = 0

DND in Phone Mode

Parameter-	Configuration File
features.dnd.enable	<y0000000000xx>.cfg
Description	Enables or disables DND feature. If it is set to 1 (Enabled), the IP phone will reject incoming calls on all accounts.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	features.dnd.enable = 1

Parameter-	Configuration File
features.dnd.on_code	<y0000000000xx>.cfg
Description	Configures the DND on code to activate the server-side DND feature.
Format	String
Default Value	Blank
Range	String within 32 characters
Example	features.dnd.on_code = *71

Parameter-	Configuration File
features.dnd.off_code	<y0000000000xx>.cfg
Description	Configures the DND off code to deactivate the server-side DND feature.
Format	String
Default Value	Blank
Range	String within 32 characters
Example	features.dnd.off_code = *72

DND in Custom Mode

Parameter- account.X.dnd.enable	Configuration File <MAC>.cfg
Description	Enables or disables DND for account X. If it is set to 1 (Enabled), the IP phone will reject incoming calls on account X. X ranges from 1 to 6.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	account.1.dnd.enable = 1

Parameter- account.X.dnd.on_code	Configuration File <MAC>.cfg
Description	Configures the DND on code to activate the server-side DND feature for account X (optional). X ranges from 1 to 6.
Format	String
Default Value	Blank
Range	String within 32 characters
Example	account.1.dnd.on_code = *73

Parameter- account.X.dnd.off_code	Configuration File <MAC>.cfg
Description	Configures the DND off code to deactivate the server-side DND feature for account X (optional). X ranges from 1 to 6.
Format	String
Default Value	Blank
Range	String within 32 characters

Example	account.1.dnd.off_code = *74
----------------	------------------------------

Busy Tone Delay

Parameter-	Configuration File
features.busy_tone_delay	<y0000000000xx>.cfg
Description	Configures a period of time (in seconds) for which the busy tone is audible on the IP phone. When one party releases the call, a busy tone is audible to the other party, indicating that the call connection breaks. If it is set to 3, a busy tone is audible for 3 seconds on the IP phone.
Format	Integer
Default Value	0
Range	Valid values are: 0-0s 3-3s 5-5s
Example	features.busy_tone_delay = 0

Return Code When Refuse

Parameter-	Configuration File
features.normal_refuse_code	<y0000000000xx>.cfg
Description	Configures a return code and reason of SIP response messages when rejecting an incoming call. A specific reason is displayed on the caller's phone LCD screen. If it is set to 486 (Busy here), the caller's LCD screen will display the message "Busy here" when the callee rejects the incoming call.
Format	Integer
Default Value	486
Range	Valid values are: 404-No Found 480-Temporarily not available

	486 -Busy here
Example	features.normal_refuse_code = 486

180 Ring Workaround

Parameter-	Configuration File
phone_setting.is_deal180	<y0000000000xx>.cfg
Description	Enables or disables the IP phone to deal with the 180 SIP message received after the 183 SIP message. If it is set to 1 (Enabled), the IP phone will resume and play the local ringback tone upon a subsequent 180 message received.
Format	Boolean
Default Value	1
Range	0-Disabled 1-Enabled
Example	phone_setting.is_deal180 = 1

Use Outbound Proxy in Dialog

Parameter-	Configuration File
sip.use_out_bound_in_dialog	<y0000000000xx>.cfg
Description	Enables or disables the IP phone to send the SIP requests to the outbound proxy server. If it is set to 1 (Enabled), all the SIP requests from the IP phone will be forced to send to the outbound proxy server. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Boolean
Default Value	1
Range	Valid values are: 0-Disabled 1-Enabled
Example	sip.use_out_bound_in_dialog = 1

SIP Session Timer

Parameter-	Configuration File
account.X.advanced.timer_t1	<MAC>.cfg
Description	Configures the SIP session timer T1 (in seconds) for account X. T1 is an estimate of the Round Trip Time (RTT) of transactions between a SIP client and SIP server. X ranges from 1 to 6.
Format	Float
Default Value	0.5
Range	0.5 to 10
Example	account.1.advanced.timer_t1 = 0.5

Parameter-	Configuration File
account.X.advanced.timer_t2	<MAC>.cfg
Description	Configures the session timer T2 (in seconds) for account X. T2 represents the maximum retransmit interval for non-INVITE requests and INVITE responses. The re-transmitting and doubling of T1 continues until the retransmitting time reaches the T2 value. X ranges from 1 to 6.
Format	Float
Default Value	4
Range	2 to 40
Example	account.1.advanced.timer_t2 = 4

Parameter-	Configuration File
account.X.advanced.timer_t4	<MAC>.cfg
Description	Configures the session timer of T4 (in seconds) for account X. T4 represents the maximum duration a message will remain in the network.

	X ranges from 1 to 6.
Format	Float
Default Value	5
Range	2.5 to 60
Example	account.1.advanced.timer_t4 = 5

Session Timer

Parameter-	Configuration File
account.X.session_timer.enable	<MAC>.cfg
Description	<p>Enables or disables the session timer for account X.</p> <p>If it is set to 1 (Enabled), IP phone will send periodic re-INVITE requests to refresh the session during a call.</p> <p>X ranges from 1 to 6.</p>
Format	Boolean
Default Value	0
Range	<p>Valid values are:</p> <p>0-Disabled</p> <p>1-Enabled</p>
Example	account.1.session_timer.enable = 1

Parameter-	Configuration File
account.X.session_timer.expires	<MAC>.cfg
Description	<p>Configures the IP phone to refresh the session during a call at regular intervals (in seconds) for account X.</p> <p>If it is set to 1800, the IP phone will refresh the session during a call before 1800 seconds.</p> <p>X ranges from 1 to 6.</p>
Format	Integer
Default Value	1800
Range	30 to 7200

Example	account.1.session_timer.expires = 1800
----------------	--

Parameter-	Configuration File
account.X.session_timer.refresher	<MAC>.cfg
Description	Configures the session timer refresher for account X. If it is set to 0 (UAC), refreshing the session is performed by the IP phone. If it is set to 1 (UAS), refreshing the session is performed by a SIP server. X ranges from 1 to 6.
Format	Integer
Default Value	0
Range	Valid values are: 0-UAC 1-UAS
Example	account.1.session_timer.refresher = 0

Call Hold

Parameter-	Configuration File
features.play_hold_tone.enable	<y0000000000xx>.cfg
Description	Enables or disables the IP phone to play a tone when there is a hold call on the IP phone.
Format	Boolean
Default Value	1
Range	Valid values are: 0-Disabled 1-Enabled
Example	features.play_hold_tone.enable = 1

Parameter-	Configuration File
features.play_hold_tone.delay	<y0000000000xx>.cfg
Description	Configures the interval (in seconds) at which

	<p>the IP phone plays a hold tone.</p> <p>If it is set to 30, the IP phone will play a hold tone every 30 seconds when there is a hold call on the IP phone.</p> <p>Note: It works only if the parameter "features.play_hold_tone.enable" is set to 1 (Enabled).</p>
Format	Integer
Default Value	30
Range	3 to 3600
Example	features.play_hold_tone.delay = 30

Parameter- sip.rfc2543_hold	Configuration File <y0000000000xx>.cfg
Description	<p>Configures whether RFC 2543 (c=0.0.0.0) outgoing hold signaling is used.</p> <p>If it is set to 0 (Disabled), the phone will use SDP media direction attributes (such as a=sendonly) per RFC 3264 when putting a call on hold.</p> <p>If it is set to 1 (Enabled), the phone will use SDP media connection address c=0.0.0.0 per RFC 2543 when putting a call on hold.</p>
Format	Boolean
Default Value	0
Range	<p>Valid values are:</p> <p>0-Disabled</p> <p>1-Enabled</p>
Example	sip.rfc2543_hold = 1

Call Forward

Call Forward Mode

Parameter- features.fwd_mode	Configuration File <y0000000000xx>.cfg
Description	Configures the call forward mode for the IP

	<p>phone.</p> <p>If it is set to 0 (Phone), call forward feature is effective for the IP phone.</p> <p>If it is set to 1 (Custom), you can configure call forward feature for each account.</p>
Format	Integer
Default Value	0
Range	<p>Valid values are:</p> <p>0-Phone</p> <p>1-Custom</p>
Example	features.fwd_mode = 0

Call Forward in Phone Mode

Always Forward

Parameter-	Configuration File
forward.always.enable	< y0000000000xx >.cfg
Description	<p>Enables or disables always forward feature.</p> <p>If it is set to 1 (Enabled), incoming call are forwarded to the destination number immediately.</p>
Format	Boolean
Default Value	0
Range	<p>Valid values are:</p> <p>0-Disabled</p> <p>1-Enabled</p>
Example	forward.always.enable = 1

Parameter-	Configuration File
forward.always.target	< y0000000000xx >.cfg
Description	Configures the destination number of the always forward.
Format	String
Default Value	Blank
Range	String within 32 characters
Example	forward.always.target = 3601

Parameter- forward.always.on_code	Configuration File < y0000000000xx >.cfg
Description	Configures the always forward on code to activate the server-side always forward feature.
Format	String
Default Value	Blank
Range	String within 32 characters
Example	forward.always.on_code = *72

Parameter- forward.always.off_code	Configuration File < y0000000000xx >.cfg
Description	Configures the always forward off code to deactivate the server-side always forward feature.
Format	String
Default Value	Blank
Range	String within 32 characters
Example	forward.always.off_code = *73

Busy Forward

Parameter- forward.busy.enable	Configuration File < y0000000000xx >.cfg
Description	Enables or disables busy forward feature. If it is set to 1 (Enabled), incoming calls are forwarded to the destination number when the callee is busy.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	forward.busy.enable = 1

Parameter-	Configuration File
forward.busy.target	< y0000000000xx >.cfg
Description	Configures the destination number of the busy forward.
Format	String
Default Value	Blank
Range	String within 32 characters
Example	forward.busy.target = 3602

Parameter-	Configuration File
forward.busy.on_code	< y0000000000xx >.cfg
Description	Configures the busy forward on code to activate the server-side busy forward feature.
Format	String
Default Value	Blank
Range	String within 32 characters
Example	forward.busy.on_code = *74

Parameter-	Configuration File
forward.busy.off_code	< y0000000000xx >.cfg
Description	Configures the busy forward off code to deactivate the server-side busy forward feature.
Format	String
Default Value	Blank
Range	String within 32 characters
Example	forward.busy.off_code = *75

No Answer Forward

Parameter-	Configuration File
forward.no_answer.enable	< y0000000000xx >.cfg
Description	Enables or disables no answer forward feature. If it is set to 1 (Enabled), incoming calls are

	forward to the destination number after a period of ring time.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	forward.no_answer.enable = 1

Parameter- forward.no_answer.target	Configuration File < y0000000000xx >.cfg
Description	Configures the destination number of the no answer forward.
Format	String
Default Value	Blank
Range	String within 32 characters
Example	forward.no_answer.target = 3603

Parameter- forward.no_answer.timeout	Configuration File < y0000000000xx >.cfg
Description	Configures the ring times (N) to wait before forwarding incoming calls. Incoming calls will be automatically forwarded when not answered after N*6 seconds.
Format	Integer
Default Value	2
Range	0 to 20
Example	forward.no_answer.timeout = 2

Parameter- forward.no_answer.on_code	Configuration File < y0000000000xx >.cfg
Description	Configures the no answer forward on code to activate the server-side no answer forward feature.

Format	String
Default Value	Blank
Range	String within 32 characters
Example	forward.no_answer.on_code = *76

Parameter-	Configuration File
forward.no_answer.off_code	< y0000000000xx >.cfg
Description	Configures the no answer forward off code to deactivate the server-side no answer forward feature.
Format	String
Default Value	Blank
Range	String within 32 characters
Example	forward.no_answer.off_code = *77

Call Forward in Custom Mode

Always Forward

Parameter-	Configuration File
account.X.always_fwd.enable	<MAC>.cfg
Description	Enables or disables always forward feature for account X. If it is set to 1 (Enabled), incoming calls to the account X are forwarded to the destination number immediately. X ranges from 1 to 6.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	account.1.always_fwd.enable = 1

Parameter-	Configuration File
account.X.always_fwd.target	<MAC>.cfg
Description	Configures the destination number of the always forward for account X. X ranges from 1 to 6.
Format	String
Default Value	Blank
Range	String within 32 characters
Example	account.1.always_fwd.target = 3601

Parameter-	Configuration File
account.X.always_fwd.on_code	<MAC>.cfg
Description	Configures the always forward on code activate the server-side always forward feature for account X. X ranges from 1 to 6.
Format	String
Default Value	Blank
Range	String within 32 characters
Example	account.1.always_fwd.on_code = *71

Parameter-	Configuration File
account.X.always_fwd.off_code	<MAC>.cfg
Description	Configures the always forward off code to deactivate the server-side always forward feature for account X. X ranges from 1 to 6.
Format	String
Default Value	Blank
Range	String within 32 characters
Example	account.1.always_fwd.off_code = *72

Busy Forward

Parameter-	Configuration File
account.X.busy_fwd.enable	<MAC>.cfg
Description	Enables or disables busy forward feature for account X. If it is set to 1 (Enabled), incoming calls to the account X are forwarded to the destination number when the callee is busy. X ranges from 1 to 6.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	account.1.busy_fwd.enable = 1

Parameter-	Configuration File
account.X.busy_fwd.target	<MAC>.cfg
Description	Configures the destination number of the busy forward for account X. X ranges from 1 to 6.
Format	String
Default Value	Blank
Range	String within 32 characters
Example	account.1.busy_fwd.target = 3602

Parameter-	Configuration File
account.X.busy_fwd.on_code	<MAC>.cfg
Description	Configures the busy forward on code to activate the server-side busy forward feature for account X. X ranges from 1 to 6
Format	String
Default Value	Blank

Range	String within 32 characters
Example	account.1.busy_fwd.on_code = *73

Parameter- account.X.busy_fwd.off_code	Configuration File <MAC>.cfg
Description	Configures the busy forward off code to deactivate the server-side busy forward feature for account X (optional). X ranges from 1 to 6
Format	String
Default Value	Blank
Range	String within 32 characters
Example	account.1.busy_fwd.off_code = *74

No Answer Forward

Parameter- account.X.timeout_fwd.enable	Configuration File <MAC>.cfg
Description	Enables or disables no answer forward feature for account X. If it is set to 1 (Enabled), incoming calls to the account X are forward to the destination number after a period of ring time. X ranges from 1 to 6.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	account.1.timeout_fwd.enable = 1

Parameter- account.X.timeout_fwd.target	Configuration File <MAC>.cfg
Description	Configures the destination number of the no answer forward for account X. X ranges from 1 to 6.

Format	String
Default Value	Blank
Range	String within 32 characters
Example	account.1.timeout_fwd.target = 3603

Parameter- account.X.timeout_fwd.timeout	Configuration File <MAC>.cfg
Description	Configures the ring times (N) to wait before forwarding incoming calls for account X. Incoming calls will be automatically forwarded when not answered after N*6 seconds. X ranges from 1 to 6.
Format	Integer
Default Value	2
Range	0 to 20
Example	account.1.timeout_fwd.timeout = 2

Parameter- account.X.timeout_fwd.on_code	Configuration File <MAC>.cfg
Description	Configures the no answer forward on code to activate the server-side no answer forward feature for account X. X ranges from 1 to 6.
Format	String
Default Value	Blank
Range	String within 32 characters
Example	account.1.timeout_fwd.on_code = *76

Parameter- account.X.timeout_fwd.off_code	Configuration File <MAC>.cfg
Description	Configures the no answer forward off code to activate the server-side no answer forward feature for account X.

	X ranges from 1 to 6.
Format	String
Default Value	Blank
Range	String within 32 characters
Example	account.1.timeout_fwd.off_code = *77

Fwd International

Parameter- forward.international.enable	Configuration File <y0000000000xx>.cfg
Description	Enables or disables the IP phone to forward an incoming call to an international phone number (the prefix is 00).
Format	Boolean
Default Value	1
Range	Valid values are: 0-Disabled 1-Enabled
Example	forward.international.enable = 1

Call Transfer

Parameter- transfer.blind_tran_on_hook_enable	Configuration File <y0000000000xx>.cfg
Description	Enables or disables the IP phone to complete the blind transfer through on-hook.
Format	Boolean
Default Value	1
Range	Valid values are: 0-Disabled 1-Enabled
Example	transfer.blind_tran_on_hook_enable = 1

Parameter- transfer.on_hook_trans_enable	Configuration File <y0000000000xx>.cfg
Description	Enables or disables the IP phone to complete the semi-attended transfer or the attended transfer through on-hook.
Format	Boolean
Default Value	1
Range	Valid values are: 0-Disabled 1-Enabled
Example	transfer.on_hook_trans_enable = 1

Parameter- transfer.semi_attend_tran_enable	Configuration File <y0000000000xx>.cfg
Description	Configures whether to display the missed call prompt on the destination party's phone when performing a semi-attended transfer.
Format	Boolean
Default Value	1
Range	Valid values are: 0-Enabled 1-Disabled
Example	transfer.semi_attend_tran_enable = 1

Network Conference

Parameter- account.X.conf_type	Configuration File <MAC>.cfg
Description	Configures the conference type for account X. If it is set to 0 (Local Conference), conference is set up on the IP phone locally. If it is set to 2 (Network Conference), conferences are set up by the server. X ranges from 1 to 6.

Format	Integer
Default Value	0
Range	Valid values are: 0-Local Conference 2-Network Conference
Example	account.1.conf_type = 0

Parameter- account.X.conf_uri	Configuration File <MAC>.cfg
Description	Configures the conference URI for account X. X ranges from 1 to 6. Note: It works only if the parameter "account.x.conf_type" is set to 2 (Network Conference).
Format	SIP URI
Default Value	Blank
Range	SIP URI within 511 characters
Example	account.1.conf_uri = conference@domain.com

Transfer on Conference Hang Up

Parameter- transfer.tran_others_after_conf_enable	Configuration File <y0000000000xx>.cfg
Description	Enables or disables the phone to transfer call to the two parties after a local conference call hangup. If it is enabled, the other two parties remain connected when the conference initiator drops the conference call. Note: It is only applicable to the local conference.
Format	Boolean
Default Value	0
Range	Valid values are:

	0-Disabled 1-Enabled
Example	transfer.tran_others_after_conf_enable = 1

Directed Call Pickup

Phone Basis

Parameter- features.pickup.direct_pickup_enable	Configuration File <MAC>.cfg
Description	Enables or disables the IP phone to display the DPickup soft key when the IP phone is off-hook.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	features.pickup.direct_pickup_enable = 1

Parameter- features.pickup.direct_pickup_code	Configuration File <MAC>.cfg
Description	Configures the directed call pickup code on a phone basis. Note: The directed call pickup code configured on a per-line basis takes precedence over that configured on a phone basis.
Format	String
Default Value	Blank
Range	String within 32 characters
Example	features.pickup.direct_pickup_code = *97

Per-line Basis

Parameter-	Configuration File
account.X.direct_pickup_code	<MAC>.cfg
Description	Configures the directed call pickup code on a per-line basis. X ranges from 1 to 6. Note: The directed call pickup code configured on a per-line basis takes precedence over that configured on a phone basis.
Format	String
Default Value	Blank
Range	String within 32 characters
Example	account.1.direct_pickup_code = *68

Group Call Pickup

Phone Basis

Parameter-	Configuration File
features.pickup.group_pickup_enable	<MAC>.cfg
Description	Enables or disables the IP phone to display the GPickup soft key when the IP phone is off-hook.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	features.pickup.group_pickup_enable = 1

Parameter-	Configuration File
features.pickup.group_pickup_code	<MAC>.cfg
Description	Configures the group call pickup code on a phone basis. Note: The group call pickup code configured on a per-line basis takes precedence over that configured on a phone basis.
Format	String
Default Value	Blank
Range	String within 32 characters
Example	features.pickup.group_pickup_code = *98

Per-line Basis

Parameter-	Configuration File
account.X.group_pickup_code	<MAC>.cfg
Description	Configures the group call pickup code on a per-line basis. X ranges from 1 to 6. Note: The group call pickup code configured on a per-line basis takes precedence over that configured on a phone basis.
Format	String
Default Value	Blank
Range	String within 32 characters
Example	account.1.group_pickup_code = *69

Dialog-Info Call Pickup

Parameter-	Configuration File
account.X.dialoginfo_callpickup	<MAC>.cfg
Description	Enables or disables the phone to pick up a call according to the SIP header of dialog-info for account X. If it is set to 1 (Enabled), call pickup is implemented through SIP signals.

	X ranges from 1 to 6.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	account.1.dialoginfo_callpickup = 1

Web Server Type

Parameter-	Configuration File
wui.http_enable	<y0000000000xx>.cfg
Description	Enables or disables the IP phone to access its web user interface using HTTP protocol. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Boolean
Default Value	1
Range	Valid values are: 0-Disabled 1-Enabled
Example	wui.http_enable = 1

Parameter-	Configuration File
network.port.http	<y0000000000xx>.cfg
Description	Configures the HTTP port used to access the web user interface of the IP phone. The default HTTP port is 80. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer
Default Value	80
Range	1 to 65535

Example	network.port.http = 80
----------------	------------------------

Parameter- wui.https_enable	Configuration File <y0000000000xx>.cfg
Description	Enables or disables the IP phone to access its web user interface using HTTPS protocol. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Boolean
Default Value	1
Range	Valid values are: 0-Disabled 1-Enabled
Example	wui.https_enable = 1

Parameter- network.port.https	Configuration File <y0000000000xx>.cfg
Description	Configures the HTTPS port used to access the web user interface of the IP phone. The default HTTPS port is 443. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer
Default Value	443
Range	1 to 65535
Example	network.port.https = 443

Calling Line Identification Presentation

Parameter- account.X.cid_source	Configuration File <MAC>.cfg
Description	Configures the presentation of the caller identity for account X.

	<p>0-FROM (Derives the name and number of the caller from the "From" header).</p> <p>1-PAI (Derives the name and number of the caller from the "PAI" header. If the server does not send the "PAI" header, displays "anonymity" on the callee's phone).</p> <p>2-PAI-FROM (Derives the name and number of the caller from the "PAI" header preferentially. If the server does not send the "PAI" header, derives from the "From" header).</p> <p>3-RPID-PAI-FROM</p> <p>4-PAI-RPID-FROM</p> <p>5-RPID-FROM</p> <p>X ranges from 1 to 6.</p>
Format	Integer
Default Value	0
Range	0 to 5
Example	account.1.cid_source = 0

Connected Line Identification Presentation

Parameter-	Configuration File
account.X.cp_source	<MAC>.cfg
Description	<p>Configures the presentation of the callee identity for account X.</p> <p>0-RPID-FROM (Derives the name and number of the callee from the "RPID" header preferentially. If the server does not send the "RPID" header, derives from the "From" header).</p> <p>1-Dialed Digits (Preferentially displays the dialed digits on the caller's phone).</p> <p>2-RFC 4916 (Derives the name and number of the callee from "From" header in the Update message).</p> <p>When the RFC 4916 is enabled on the IP phone, the caller sends the SIP request message which contains the from-change tag in the Supported header. The caller then</p>

	receives an UPDATE message from the callee, and displays the identity in the From header. X ranges from 1 to 6.
Format	Integer
Default Value	0
Range	0 to 2
Example	account.1.cp_source = 0

DTMF

Parameter- account.X.dtmf.type	Configuration File <MAC>.cfg
Description	Configures the DTMF type for account X. If it is set to 0 (INBAND), DTMF digits are transmitted in the voice band. If it is set to 1 (RFC 2833), DTMF digits are transmitted by RTP Events compliant to RFC 2833. If it is set to 2 (SIP INFO), DTMF digits are transmitted by the SIP INFO messages. If it is set to 3 (AUTO or SIP INFO), the IP phone will negotiate with the other end to use INBAND or RFC 2833, if there is no negotiation, using SIP INFO by default. X ranges from 1 to 6.
Format	Integer
Default Value	1
Range	Valid values are: 0-INBAND 1-RFC 2833 2-SIP INFO 3-AUTO or SIP INFO
Example	account.1.dtmf.type = 1

Parameter-	Configuration File
account.X.dtmf.dtmf_payload	<MAC>.cfg
Description	Configures the RFC 2833 payload type. X ranges from 1 to 6.
Format	Integer
Default Value	101
Range	Integer from 96 to 127
Example	account.1.dtmf.dtmf_payload = 101

Parameter-	Configuration File
account.X.dtmf.info_type	<MAC>.cfg
Description	Configures the DTMF info type when the DTMF type is configured as "SIP INFO", "AUTO or SIP INFO". X ranges from 1 to 6.
Format	Integer
Default Value	0
Range	Valid values are: 0-Disabled 1-DTMF-Relay 2-DTMF 3-Telephone-Event
Example	account.1.dtmf.info_type = 0

Parameter-	Configuration File
features.dtmf.repetition	<y0000000000xx>.cfg
Description	Configures the number of times for the IP phone to send the end RTP EVENT packet.
Format	Integer
Default Value	3
Range	1 to 3
Example	features.dtmf.repetition = 3

Suppress DTMF Display

Parameter-	Configuration File
features.dtmf.hide	<y0000000000xx>.cfg
Description	Enables or disables the IP phone to suppress the display of DTMF digits. If it is set to 1 (Enabled), the DTMF digits are displayed as asterisks.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	features.dtmf.hide = 1

Parameter-	Configuration File
features.dtmf.hide_delay	<y0000000000xx>.cfg
Description	Enables or disables the IP phone to display the DTMF digits for a short period before displaying as asterisks. Note: It works only if the parameter "features.dtmf.hide" is set to 1 (Enabled).
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	features.dtmf.hide_delay = 1

Transfer via DTMF

Parameter-	Configuration File
features.dtmf.replace_tran	<y0000000000xx>.cfg
Description	Enables or disables the phone to send DTMF sequences for transfer function when pressing

	<p>the transfer soft key or the transfer key.</p> <p>If it is set to 0 (Disabled), the IP phone will perform the transfer as normal when pressing the transfer key during a call.</p> <p>If it is set to 1 (Enabled), the IP phone will transmit the specified DTMF digits to the server for completing call transfer when pressing the transfer key during a call.</p>
Format	Boolean
Default Value	0
Range	<p>Valid values are:</p> <p>0-Disabled</p> <p>1-Enabled</p>
Example	features.dtmf.replace_tran = 1

Parameter-	Configuration File
features.dtmf.transfer	<y0000000000xx>.cfg
Description	<p>Configures the DTMF digits to be transmitted to complete the transfer.</p> <p>Note: It works only if the parameter "features.dtmf.replace_tran" is set to 1 (Enabled).</p>
Format	String
Default Value	Blank
Range	<p>Valid values are: 0-9, *, # and A-D.</p> <p>String within 32 characters.</p>
Example	features.dtmf.transfer = 123

Incoming Intercom calls

Parameter-	Configuration File
features.intercom.allow	<y0000000000xx>.cfg
Description	<p>Enables or disables the IP phone to automatically answer an incoming intercom call.</p> <p>If it is set to 0 (Disabled), the IP phone will</p>

	reject incoming intercom calls and sends a busy signal to the caller. If it is set to 1 (Enabled), the IP phone will automatically answer an incoming intercom call.
Format	Boolean
Default Value	1
Range	Valid values are: 0-Disabled 1-Enabled
Example	features.intercom.allow = 1

Parameter- features.intercom.mute	Configuration File <y0000000000xx>.cfg
Description	Enables or disables the IP phone to mute the microphone when answering an intercom call. If it is set to 0 (Disabled), the microphone is un-muted for incoming calls. If it is set to 1 (Enabled), the microphone is muted for intercom calls.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	features.intercom.mute = 1

Parameter- features.intercom.tone	Configuration File <y0000000000xx>.cfg
Description	Enables or disables the IP phone to play a warning tone when receiving an intercom call. If it is set to 0 (Disabled), the IP phone will automatically answer the intercom call without a warning tone.

	If it is set to 1 (Enabled), the IP phone will play a warning tone to alert you before answering the intercom call.
Format	Boolean
Default Value	1
Range	Valid values are: 0-Disabled 1-Enabled
Example	features.intercom.tone = 1

Parameter-	Configuration File
features.intercom.barge	<y0000000000xx>.cfg
Description	Enables or disables the IP phone to automatically answer an incoming intercom call while there is already an active call on the IP phone. If it is set to 0 (Disabled), the IP phone will handle an incoming intercom call like a waiting call while there is already an active call on the IP phone. If it is set to 1 (Enabled), the IP phone will automatically answer the intercom call while there is already an active call on the IP phone and puts the active call on hold.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	features.intercom.barge = 1

Distinctive Ring Tones

Parameter-	Configuration File
features.alert_info_tone	<y0000000000xx>.cfg
Description	Enables and disables the IP phone to map

	the keywords in the Alert-info header to the specified Bellcore ring tones.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	features.alert_info_tone = 1

Parameter-	Configuration File
account.X.alert_info_url_enable	<MAC>.cfg
Description	Enables or disables the distinctive ring tones feature for account X. If it is set to 1 (Enabled), the IP phone will try to download the WAV ring tone file from the URL and then play the remote ring tone when the Alert-Info header contains a remote URL. X ranges from 1 to 6.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	account.1.alert_info_url_enable = 1

Parameter-	Configuration File
distinctive_ring_tones.alert_info.X .text	<y0000000000xx>.cfg
Description	Configures the texts to map the keywords contained in the SIP header. X ranges from 1 to 10.
Format	String
Default Value	Blank
Range	String within 32 characters

Example	distinctive_ring_tones.alert_info.1.text = family
----------------	---

Parameter- distinctive_ring_tones.alert_info.X .ringer	Configuration File <y0000000000xx>.cfg
Description	Configures the desired ring tones for each text. The value ranges from 1 to 8, the digit stands for the appropriate ring tone. X ranges from 1 to 10.
Format	Integer
Default Value	1
Range	Valid values are: 1-Ring1.wav 2-Ring2.wav 3-Ring3.wav 4-Ring4.wav 5-Ring5.wav 6-Ring6.wav 7-Ring7.wav 8-Ring8.wav Ring 6-8 are not applicable to SIP-T42G/T41P.
Example	distinctive_ring_tones.alert_info.1.ringer = 1

Tones

Parameter- voice.tone.country	Configuration File <y0000000000xx>.cfg
Description	Configures the country tone for the IP phone.
Format	String
Default Value	Custom
Range	Valid values are: <ul style="list-style-type: none"> • Custom • Australia • Austria • Brazil

	<ul style="list-style-type: none"> • Belgium • China • Czech • Denmark • Finland • France • Germany • Great Britain • Greece • Hungary • Lithuania • India • Italy • Japan • Mexico • New Zealand • Netherlands • Norway • Portugal • Spain • Switzerland • Sweden • Russia • United States • Chile • Czech ETSI
Example	voice.tone.country = Austria

Parameter- voice.tone.dial voice.tone.ring voice.tone.busy voice.tone.congestion voice.tone.callwaiting voice.tone.dialrecall voice.tone.record voice.tone.info voice.tone.stutter voice.tone.message voice.tone.autoanswer	Configuration File <y0000000000xx>.cfg
Description	Customizes the tone for each condition. The parameter "voice.tone.message" is not

	<p>applicable to SIP-T42G/T41P IP phones.</p> <p>tonelist = element[,element] [,element]...</p> <p>Where</p> <p>element = [!]freq1[+freq2][+freq3][+freq4] /duration</p> <p>Freq: the frequency of the tone (ranges from 200 to 7000 Hz). If the frequency is set to 0Hz, it means silence. A tone can be comprised of at most four different frequencies.</p> <p>Duration: the time duration (in milliseconds, ranges from 0 to 30000ms) of the dial tone.</p> <p>You can configure at most eight different tones for one condition, each tone are separated by a comma (e.g., 250/200, !0/1000, 200+300/500, 600+700+800+1000/2000). The exclamation point (!) can be added optionally, which means these tones are only played once.</p> <p>Note: It works only if the parameter "voice.tone.country" is set to Custom.</p>
Format	Refer to the introduction above
Default Value	Blank
Range	Not Applicable
Example	voice.tone.dial = 800+200/1000, 0/100, 500/1200, 500+600+950+1500/5000

Remote Phone Book

Parameter-	Configuration File
remote_phonebook.data.X.name	<y0000000000xx>.cfg
Description	Configures the name of the remote phone book.
Format	String
Default Value	Blank
Range	String within 99 characters
Example	remote_phonebook.data.1.name = yl01

Parameter- remote_phonebook.display_name	Configuration File <y0000000000xx>.cfg
Description	Configures the display name of the remote phone book. If you leave it blank, Remote Phone Book is displayed on the LCD screen at the path Menu->Directory. Note: It is only applicable to SIP-T46G IP phones.
Format	String
Default Value	Blank
Range	String within 99 characters
Example	remote_phonebook.display_name = Remote Phone Book

Parameter- features.remote_phonebook.enable	Configuration File <y0000000000xx>.cfg
Description	Enables or disables the IP phone to perform a remote phone book search when receiving an incoming call.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	features.remote_phonebook.enable = 1

Parameter- features.remote_phonebook.flash_time	Configuration File <y0000000000xx>.cfg
Description	Configures how often to refresh the local cache of the remote phone book. If it is set to 3600, the IP phone will refresh the

	local cache of the remote phone book every 3600 seconds.
Format	Integer
Default Value	21600
Range	3600 to 2592000
Example	features.remote_phonebook.flash_time = 21600

LDAP

Parameter-	Configuration File
ldap.enable	<y0000000000xx>.cfg
Description	Enables or disables LDAP feature on the IP phone.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	ldap.enable =1

Parameter-	Configuration File
ldap.name_filter	<y0000000000xx>.cfg
Description	Configures the name attribute for LDAP searching. The "*" symbol in the filter stands for any character. The "%" symbol in the filter stands for the entering string used as the prefix of the filter condition.
Format	String
Default Value	Blank
Range	String within 99 characters
Example	ldap.name_filter = ((cn=%)(sn=%)) When the name prefix of the cn or sn of the contact record matches the search criteria, the record will be displayed on the LCD

	screen.
--	---------

Parameter-	Configuration File
ldap.number_filter	<y0000000000xx>.cfg
Description	Configures the number attribute for LDAP searching. The "*" symbol in the filter stands for any character. The "%" symbol in the filter stands for the entering string used as the prefix of the filter condition.
Format	String
Default Value	Blank
Range	String within 99 characters
Example	ldap.number_filter = ((telephoneNumber=%)(Mobile=%)(ipPhone=%)) When the number prefix of the telephoneNumber, Mobile or ipPhone of the contact record matches the search criteria, the record will be displayed on the LCD screen.

Parameter-	Configuration File
ldap.host	<y0000000000xx>.cfg
Description	Configures the domain name or IP address of the LDAP server.
Format	IP Address or Domain Name
Default Value	Blank
Range	Not Applicable
Example	ldap.host = 192.168.1.20

Parameter-	Configuration File
ldap.port	<y0000000000xx>.cfg
Description	Configures the LDAP server port.
Format	Integer
Default Value	389

Range	1 to 65535
Example	ldap.port = 389

Parameter-	Configuration File
ldap.base	<y0000000000xx>.cfg
Description	Configures the LDAP search base which corresponds to the location in the LDAP phonebook from which the LDAP search request begins. The search base narrows the search scope and decreases directory search time.
Format	String
Default Value	Blank
Range	String within 99 characters
Example	ldap.base = dc=yealink,dc=cn

Parameter-	Configuration File
ldap.user	<y0000000000xx>.cfg
Description	Configures the user name uses to login the LDAP server. This parameter can be left blank in case the server allows anonymous to login. Otherwise you will need to provide the user name to access the LDAP server.
Format	String
Default Value	Blank
Range	String within 99 characters
Example	ldap.user = cn=manager,dc=yealink,dc=cn

Parameter-	Configuration File
ldap.password	<y0000000000xx>.cfg
Description	Configures the password to login the LDAP server. This parameter can be left blank in case the server allows anonymous to login. Otherwise you will need to provide the password to

	access the LDAP server.
Format	String
Default Value	Blank
Range	String within 99 characters
Example	ldap.password = secret

Parameter-	Configuration File
ldap.max_hits	<y0000000000xx>.cfg
Description	Configures the maximum number of search results to be returned by the LDAP server. If the value of the "Max.Hits" is blank, the LDAP server will return all searched results. Please note that a very large value of the "Max. Hits" will slow down the LDAP search speed, therefore it should be configured according to the available bandwidth.
Format	Integer
Default Value	50
Range	1 to 32000
Example	ldap.max_hits = 50

Parameter-	Configuration File
ldap.name_attr	<y0000000000xx>.cfg
Description	Configures the name attributes of each record to be returned by the LDAP server. It compresses the search results. You can configure multiple name attributes separated by space.
Format	String
Default Value	Blank
Range	String within 99 characters
Example	ldap.name_attr = cn sn

Parameter-	Configuration File
ldap.numb_attr	<y0000000000xx>.cfg
Description	Configures the number attributes of each record to be returned by the LDAP server. It compresses the search results. You can configure multiple number attributes separated by space.
Format	String
Default Value	Blank
Range	String within 99 characters
Example	ldap.numb_attr = telephoneNumber

Parameter-	Configuration File
ldap.display_name	<y0000000000xx>.cfg
Description	Configures the display name of the contact record displayed on the LCD screen. Note: It must start with "%" symbol.
Format	String
Default Value	Blank
Range	String within 99 characters
Example	ldap.display_name = %cn The cn of the contact record is displayed on the LCD screen.

Parameter-	Configuration File
ldap.version	<y0000000000xx>.cfg
Description	Configures the LDAP protocol version supported by the IP phone. Make sure the protocol value corresponds with the version assigned on the LDAP server.
Format	Integer
Default Value	3
Range	2 or 3
Example	ldap.version = 3

Parameter-	Configuration File
ldap.call_in_lookup	<y0000000000xx>.cfg
Description	Enables or disables the IP phone to perform an LDAP search when receiving an incoming call.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	ldap.call_in_lookup = 1

Parameter-	Configuration File
ldap.ldap_sort	<y0000000000xx>.cfg
Description	Enables or disables the IP phone to sort the search results in alphabetical order or numerical order.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	ldap.ldap_sort = 1

BLF

Visual and Audio Alert for BLF Pickup

Parameter-	Configuration File
features.pickup.blf_visual_enable	<MAC>.cfg
Description	Enables or disables the IP phone to display a visual prompt when the monitored user receives an incoming call.
Format	Boolean
Default Value	0

Range	Valid values are: 0-Disabled 1-Enabled
Example	features.pickup.blf_visual_enable = 1

Parameter- features.pickup.blf_audio_enable	Configuration File <MAC>.cfg
Description	Enables or disables the IP phone to play an alert tone when the monitored user receives an incoming call.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	features.pickup.blf_audio_enable = 1

BLF LED Mode

Parameter- features.blf_led_mode	Configuration File <y0000000000xx>.cfg
Description	It configures BLF LED mode and provides four kinds of definition for the BLF key LED status. For more information, refer to Busy Lamp Field on page 136.
Format	Integer
Default Value	0
Range	0 to 3
Example	features.blf_led_mode = 0

Music on Hold

Parameter- account.X.music_server_uri	Configuration File <MAC>.cfg
Description	Configures the Music on Hold server

	<p>address. Examples for valid values: <10.1.3.165>, 10.1.3.165, sip:moh@ucap.com, <sip:moh@ucap.com>, <yealink.com> or yealink.com.</p> <p>X ranges from 1 to 6.</p> <p>Note: The DNS query in this parameter only supports A query.</p>
Format	String
Default Value	Blank
Range	String within 256 characters
Example	account.1.music_server_uri = <10.1.3.165>

ACD

Parameter-	Configuration File
account.X.acd.enable	<MAC>.cfg
Description	<p>Enables or disables ACD feature for account X.</p> <p>X ranges from 1 to 6.</p>
Format	Boolean
Default Value	0
Value	<p>Valid values are:</p> <p>0- Disabled</p> <p>1- Enabled</p>
Example	account.1.acd.enable = 1

Parameter-	Configuration File
acd.auto_available	<y0000000000xx>.cfg
Description	<p>Enables or disables ACD auto available timer feature.</p> <p>If it is set to 1 (Enabled), the IP phone will automatically change the phone status to available.</p>
Format	Boolean
Default Value	0
Value	Valid values are:

	0 - Disabled 1 - Enabled
Example	acd.auto_available = 1

Parameter- acd.auto_available_timer	Configuration File <y0000000000xx>.cfg
Description	Configures the length of time (in seconds) before the IP phone state is automatically reset to "available".
Format	Integer
Default Value	60
Value	0 to 120
Example	acd.auto_available_timer = 60

Message Waiting Indicator

Parameter- account.X.subscribe_mwi	Configuration File <MAC>.cfg
Description	<p>Enables or disables the IP phone to subscribe the message waiting indicator for account X.</p> <p>If it is set to 1 (Enabled), the IP phone will send a SUBSCRIBE message to the server for message-summary updates.</p> <p>X ranges from 1 to 6.</p>
Format	Boolean
Default Value	0
Value	Valid values are: 0 -Disabled 1 -Enabled
Example	account.1.subscribe_mwi = 1

Parameter- account.X.subscribe_mwi_expires	Configuration File <MAC>.cfg
Description	Configures MWI subscribe expiry time (in seconds) for account X.

	The IP phone is able to successfully refresh the SUBSCRIBE for message-summary events before expiration of the SUBSCRIBE dialog. X ranges from 1 to 6. Note: It works only if the parameter "account.x.subscribe_mwi" is set to 1 (Enabled).
Format	Integer
Default Value	3600
Value	0 to 84600
Example	account.1.subscribe_mwi_expires = 3600

Parameter- account.X.subscribe_mwi_to_vm	Configuration File <MAC>.cfg
Description	Enables or disables a subscription to the voice mail number for MWI service for account X. X ranges from 1 to 6.
Format	Boolean
Default Value	0
Value	Valid values are: 0-Disabled 1-Enabled
Example	account.1.subscribe_mwi_to_vm = 1

Parameter- voice_mail.number.X	Configuration File <MAC>.cfg
Description	Configures the voice mail number for account X. X ranges from 1 to 6. Note: It works only if the parameter "account.x.subscribe_mwi_to_vm" is set to 1 (Enabled).
Format	String
Default Value	Blank
Value	String within 99 characters

Example	voice_mail.number.1 = 3606
----------------	----------------------------

Sending RTP Stream

Parameter-	Configuration File
multicast.codec	<y0000000000xx>.cfg
Description	Configures a multicast codec for the IP phone to use to send an RTP stream.
Format	String
Default Value	G722
Range	Valid values are: <ul style="list-style-type: none"> • PCMU • PCMA • G729 • G722 • G726-16 • G726-24 • G726-32 • G726-40 • G723_53
Example	multicast.codec = G722

Receiving RTP Stream

Parameter-	Configuration File
multicast.receive_priority.enable	<y0000000000xx>.cfg
Description	<p>Enables or disables the IP phone to handle the incoming multicast paging calls when there is an active multicast paging call on the IP phone.</p> <p>If it is set to 1 (Enabled), the IP phone will answer the incoming multicast paging call with a higher priority and ignore that with a lower priority.</p>
Format	Boolean
Default Value	1
Range	Valid values are:

	0-Disabled 1-Enabled
Example	multicast.receive_priority.enable = 1

Parameter- multicast.receive_priority.priority	Configuration File < y0000000000xx >.cfg
Description	Configures the priority of multicast paging calls. 1 is the highest priority, 10 is the lowest priority. If it is set to 0, all incoming multicast paging calls will be automatically ignored.
Format	Integer
Default Value	10
Range	0 to 10
Example	multicast.receive_priority.priority = 10

Parameter- multicast.listen_address.X.label	Configuration File < y0000000000xx >.cfg
Description	Configures the label to be displayed on the LCD screen when receiving the RTP multicast. X ranges from 1 to 10.
Format	String
Default Value	Blank
Range	String within 99 characters
Example	multicast.listen_address.1.label = Paging1

Parameter- multicast.listen_address.X.ip_address	Configuration File < y0000000000xx >.cfg
Description	Configures the multicast address and port number that the IP phone listens to. X ranges from 1 to 10. Note: The valid multicast IP addresses range from 224.0.0.0 to 239.255.255.255.

Format	String
Default Value	Blank
Range	Not Applicable
Example	multicast.listen_address.1.ip_address = 224.5.6.20:10008

Action URL

Parameter-	Configuration File
action_url.setup_completed =	<y0000000000xx>.cfg
action_url.registered =	
action_url.unregisterd =	
action_url.register_failed =	
action_url.off_hook =	
action_url.on_hook =	
action_url.incoming_call =	
action_url.outgoing_call =	
action_url.call_established =	
action_url.dnd_on =	
action_url.dnd_off =	
action_url.always_fwd_on =	
action_url.always_fwd_off =	
action_url.busy_fwd_on =	
action_url.busy_fwd_off =	
action_url.no_answer_fwd_on =	
action_url.no_answer_fwd_off =	
action_url.transfer_call =	
action_url.blind_transfer_call =	
action_url.attended_transfer_call =	
action_url.hold =	
action_url.unhold =	
action_url.mute =	
action_url.unmute =	
action_url.missed_call =	
action_url.call_terminated =	
action_url.busy_to_idle =	

<pre> action_url.idle_to_busy = action_url.ip_change = action_url.forward_incoming_call = action_url.reject_incoming_call = action_url.answer_new_incoming_ call = action_url.transfer_finished = action_url.transfer_failed = </pre>	
Description	<p>Configures the URL for the predefined event.</p> <p>The value format is: http(s)://IP address of server/help.xml? variable name=variable value</p> <p>Valid variable values are:</p> <ul style="list-style-type: none"> • \$mac • \$ip • \$model • \$firmware • \$active_url • \$active_user • \$active_host • \$local • \$remote • \$display_local • \$display_remote • \$call_id
Format	URL
Default Value	Blank
Range	String within 511 characters
Example	<pre> action_url.mute = http://192.168.0.20/help.xml?model=\$mode l </pre>

Action URI

Parameter- features.action_uri_limit_ip	Configuration File <y0000000000xx>.cfg
Description	Configures the address(es) from which

	<p>Action URI will be accepted.</p> <p>For discontinuous IP addresses, each IP address is separated by a comma.</p> <p>For continuous IP addresses, the format likes *.*.* and the "*" stands for the values 0~255.</p> <p>For example: 10.10.*.* stands for the IP addresses that range from 10.10.0.0 to 10.10.255.255.</p> <p>If it is left blank, the IP phone cannot receive or handle any HTTP GET request.</p> <p>If it is set to "any", the IP phone will accept and handle HTTP GET requests from any IP address.</p>
Format	IP Address or any
Default Value	Blank
Range	String within 511 characters
Example	features.action_uri_limit_ip = any

Server Redundancy

Parameter- account.X.sip_server.Y.address	Configuration File <MAC>.cfg
Description	<p>Configures the IP address or domain name of the SIP server.</p> <p>X ranges from 1 to 6.</p> <p>Y ranges from 1 to 2.</p>
Format	IP Address or Domain Name
Default Value	Blank
Range	String within 256 characters
Example	<p>account.1.sip_server.1.address = user.example.com</p> <p>account.1.sip_server.2.address = 192.168.1.15</p>

Parameter- account.X.sip_server.Y.port	Configuration File <MAC>.cfg
Description	Configures the SIP server port. X ranges from 1 to 6. Y ranges from 1 to 2.
Format	Integer
Default Value	5060
Range	0 to 65535
Example	account.1.sip_server.1.port = 5060

Parameter- account.X.sip_server.Y.expires	Configuration File <MAC>.cfg
Description	Configures the registration expiration time (in seconds). X ranges from 1 to 6. Y ranges from 1 to 2.
Format	Integer
Default Value	3600
Range	30 to 2147483647
Example	account.1.sip_server.1.expires = 3600

Parameter- account.X.sip_server.Y.retry_counts	Configuration File <MAC>.cfg
Description	It configures the times for the phone to retransmit the request when the SIP server is unavailable or there is no respond from the SIP server. X ranges from 1 to 6. Y ranges from 1 to 2.
Format	Integer
Default Value	3
Range	0 to 20
Example	account.1.sip_server.1.retry_counts = 3

Fallback Mode

Parameter-	Configuration File
account.X.fallback.redundancy_type	<MAC>.cfg
Description	Configures the registration mode for the IP phone in fallback mode. X ranges from 1 to 6.
Format	Integer
Default Value	0
Range	Valid values are: 0 -Concurrent registration: the phone registers to the working server and fallback server at the same time. 1 -Successive registration: the phone registers to the working server first. When the working server fails, the phone registers to the fallback server.
Example	account.1.fallback.redundancy_type = 0

Parameter-	Configuration File
account.X.fallback.timeout	<MAC>.cfg
Description	Configures the time interval (in seconds) for the IP phone to detect whether the working server is available by sending the registration request after the fallback server takes over the call control. It is only applicable to the successive registration mode. X ranges from 1 to 6.
Format	Integer
Default Value	120
Range	10 to 2147483647
Example	account.1.fallback.timeout = 120

Failover Mode

Parameter-	Configuration File
account.X.sip_server.Y.failback_mode	<MAC>.cfg
Description	Configures the way in which the phone fails back to the primary server for call control when in the failover mode. X ranges from 1 to 6. Y ranges from 1 to 2.
Format	Integer
Default Value	0
Range	Valid values are: 0 -newRequests: all requests are forwarded to the primary server first, regardless of the secondary server that was used. 1 -DNSTTL: the IP phone will retry to use the primary server after the timeout of the DNSTTL configured for the SIP server. 2 -registration: the IP phone will retry to use the primary server when the SIP server's registration requires renewal. 3 -duration: the IP phone will retry to use the primary server after the timeout defined by the parameter "account.x.failback_timeout".
Example	account.1.sip_server.1.failback_mode = 0

Parameter-	Configuration File
account.X.sip_server.Y.failback_timeout	<MAC>.cfg
Description	Configures the time interval (in seconds) for the IP phone to detect whether the primary server is available by sending the registration request after the secondary server takes over the call control. If the value is configured to 0, the IP phone does not detect the primary server until a failover occurs.

	<p>When the value is configured between 1 and 59, the phone automatically sets the time interval to be 60.</p> <p>Note: This parameter is only valid when the parameter "account.x.sip_server.y.failback_mode" is configured to 3.</p> <p>X ranges from 1 to 6.</p> <p>Y ranges from 1 to 2.</p>
Format	Integer
Default Value	3600
Range	0, 60 to 65535
Example	account.1.sip_server.1.failback_timeout = 3600

Parameter- account.X.sip_server.Y.register_on_enable	Configuration File <MAC>.cfg
Description	<p>Enables or disables the IP phone to register to the secondary server before sending requests to the secondary server in the failover mode.</p> <p>X ranges from 1 to 6.</p> <p>Y ranges from 1 to 2.</p>
Format	Boolean
Default Value	0
Range	<p>Valid values are:</p> <p>0-Disabled</p> <p>1-Enabled</p>
Example	account.1.sip_server.1.register_on_enable = 0

SIP Server Domain Name Resolution

Parameter-	Configuration File
account.X.transport	<MAC>.cfg
Description	Configures the transport type for account X. If it is set to 3 (DNS-NAPTR) and no server port is given, the IP phone will perform the DNS NAPTR and SRV queries for the transport protocol, port and IP address. X ranges from 1 to 6.
Format	Integer
Default Value	0
Range	Valid values are: 0-UDP 1-TCP 2-TLS 3-DNS-NAPTR
Example	account.1.transport = 0

Parameter-	Configuration File
account.X.naptr_build	<MAC>.cfg
Description	Configures the transport protocol the phone constructs the SRV query for when no NAPTR records are returned. X ranges from 1 to 6.
Format	Integer
Default Value	0
Range	Valid values are: 0-UDP 1-Multiple Types
Example	account.1.naptr_build = 0

LLDP

Parameter-	Configuration File
network.lldp.enable	<y0000000000xx>.cfg
Description	Enables or disables LLDP feature on the IP phone. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Boolean
Default Value	1
Range	Valid values are: 0-Disabled 1-Enabled
Example	network.lldp.enable = 1

Parameter-	Configuration File
network.lldp.packet_interval	<y0000000000xx>.cfg
Description	Configures the amount of time (in seconds) between the transmissions of LLDP packet. Note: If you change this parameter, the IP phone will reboot to make the change take effect. It works only if the parameter "network.lldp.enable" is set to 1 (Enabled).
Format	Integer
Default Value	60
Range	1 to 3600
Example	network.lldp.packet_interval = 60

VLAN

Internet Port

Parameter-	Configuration File
network.vlan.internet_port_enable	<y0000000000xx>.cfg
Description	Enables or disables the IP phone to insert

	VLAN tag on packet from the Internet port. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	network.vlan.internet_port_enable = 1

Parameter-	Configuration File
network.vlan.internet_port_vid	<y0000000000xx>.cfg
Description	Configures the VLAN ID that is associated with the particular VLAN. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer
Default Value	1
Range	1 to 4094
Example	network.vlan.internet_port_vid = 1

Parameter-	Configuration File
network.vlan.internet_port_priority	<y0000000000xx>.cfg
Description	Configures the priority value used for passing VLAN packets. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer
Default Value	0
Range	0 to 7
Example	network.vlan.internet_port_priority = 0

PC Port

Parameter-	Configuration File
network.vlan.pc_port_enable	<y0000000000xx>.cfg
Description	Enables or disables the IP phone to insert VLAN tag on packet from the PC port. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	network.vlan.pc_port_enable = 1

Parameter-	Configuration File
network.vlan.pc_port_vid	<y0000000000xx>.cfg
Description	Configures the VLAN ID that is associated with the particular VLAN. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer
Default Value	1
Range	1 to 4094
Example	network.vlan.pc_port_vid = 1

Parameter-	Configuration File
network.vlan.pc_port_priority	<y0000000000xx>.cfg
Description	Configures the priority value used for passing VLAN packets. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer

Default Value	0
Range	0 to 7
Example	network.vlan.pc_port_priority = 0

DHCP VLAN Discovery

Parameter- network.vlan.dhcp_enable	Configuration File <y0000000000xx>.cfg
Description	Enables or disables DHCP VLAN discovery feature on the IP phone. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Boolean
Default Value	1
Range	Valid values are: 0-Disabled 1-Enabled
Example	network.vlan.dhcp_enable = 1

Parameter- network.vlan.dhcp_option	Configuration File <y0000000000xx>.cfg
Description	Configures the DHCP option from which the phone will obtain the VLAN settings. You can configure at most five DHCP options, and separate options by commas. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer
Default Value	132
Range	128 to 254
Example	network.vlan.dhcp_option = 132

VPN

Parameter-	Configuration File
network.vpn_enable	<y0000000000xx>.cfg
Description	Enables or disables VPN feature on the IP phone. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	network.vpn_enable = 0

Parameter-	Configuration File
openvpn.url	<y0000000000xx>.cfg
Description	Configures the access URL of the OpenVPN tar package.
Format	URL
Default Value	Blank
Range	String within 511 characters
Example	openvpn.url = http://192.168.10.25/OpenVPN.tar

QoS

Parameter-	Configuration File
network.qos.rtptos	<y0000000000xx>.cfg
Description	Configures the DSCP for voice packets. The default DSCP value for RTP packets is 46 (Expedited Forwarding). Note: If you change this parameter, the IP phone will reboot to make the change take

	effect.
Format	Integer
Default Value	46
Range	0 to 63
Example	network.qos.rtpptos = 46

Parameter-	Configuration File
network.qos.signaltos	<y0000000000xx>.cfg
Description	Configures the DSCP for SIP packets. The default DSCP value for SIP packets is 26 (Assured Forwarding). Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer
Default Value	26
Range	0 to 63
Example	network.qos.signaltos = 26

Network Address Translation

Parameter-	Configuration File
account.X.nat.nat_traversal	<MAC>.cfg
Description	Enables or disables the NAT traversal for account X. X ranges from 1 to 6.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	account.1.nat.nat_traversal = 0

Parameter-	Configuration File
account.X.nat.stun_server	<MAC>.cfg
Description	Configures the IP address or the domain name of the STUN server for account X. X ranges from 1 to 6.
Format	IP Address or Domain Name
Default Value	Blank
Range	Not Applicable
Example	account.1.nat.stun_server = 218.107.220.20

Parameter-	Configuration File
account.X.nat.stun_port	<MAC>.cfg
Description	Configures the port of the STUN server. X ranges from 1 to 6.
Format	Integer
Default Value	3478
Range	1024 to 65000
Example	account.1.nat.stun_port = 3478

802.1X

Parameter-	Configuration File
network.802_1x.mode	<y0000000000xx>.cfg
Description	Configures the 802.1X authentication mode to be used on the IP phone. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer
Default Value	0
Range	Valid values are: 0 -Disabled 1 -EAP-MD5 2 -EAP-TLS 3 -PEAP-MSCHAPV2

	4-EAP-TTLS/EAP-MSCHAPv2
Example	network.802_1x.mode = 0

Parameter-	Configuration File
network.802_1x.identity	<y0000000000xx>.cfg
Description	Enters the identity used for authenticating the IP phone. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	String
Default Value	Blank
Range	String within 32 characters
Example	network.802_1x.identity = admin

Parameter-	Configuration File
network.802_1x.md5_password	<y0000000000xx>.cfg
Description	Enters the password used for authenticating the IP phone. Note: If you change this parameter, the IP phone will reboot to make the change take effect. It is only applicable to EAP-MD5, PEAP-MSCHAPV2 and EAP-TTLS/EAP-MSCHAPv2 protocols.
Format	String
Default Value	Blank
Range	String within 32 characters
Example	network.802_1x.md5_password = admin123

Parameter-	Configuration File
network.802_1x.root_cert_url	<y0000000000xx>.cfg
Description	Configures the access URL of the CA certificate used for authentication. Note: If you change this parameter, the IP phone will reboot to make the change take

	effect. It is only applicable to EAP-TLS, PEAP-MSCHAPV2 and EAP-TTLS/EAP-MSCHAPv2 protocols. The format of the certificate must be *.pem, *.crt, *.cer or *.der.
Format	URL
Default Value	Blank
Range	String within 511 characters
Example	network.802_1x.root_cert_url = http://192.168.1.10/ca.pem

Parameter-	Configuration File
network.802_1x.client_cert_url	<y0000000000xx>.cfg
Description	Configures the access URL of the device certificate used for authentication. Note: If you change this parameter, the IP phone will reboot to make the change take effect. It is only applicable to the EAP-TLS protocol. The format of the certificate must be *.pem or *.cer.
Format	URL
Default Value	Blank
Range	String within 511 characters
Example	network.802_1x.client_cert_url = http://192.168.1.10/client.pem

TR-069

Parameter-	Configuration File
managementserver.enable	<y0000000000xx>.cfg
Description	Enables or disables TR-069 feature on the IP phone. Note: It is only applicable to SIP-T46G IP phones.
Format	Integer
Default Value	0

Range	Valid values are: 0-Disabled 1-Enabled
Example	managementserver.enable = 0

Parameter- managementserver.username	Configuration File <y0000000000xx>.cfg
Description	Enters the user name to authenticate with the ACS. This string is set to the empty string if no authentication is required. Note: It is only applicable to SIP-T46G IP phones.
Format	String
Default Value	Blank
Range	String within 128 characters
Example	managementserver.username = user1

Parameter- managementserver.password	Configuration File <y0000000000xx>.cfg
Description	Enters the password to authenticate with the ACS. This string is set to the empty string if no authentication is required. Note: It is only applicable to SIP-T46G IP phones.
Format	String
Default Value	Blank
Range	String within 64 characters
Example	managementserver.password = pwd123

Parameter- managementserver.url	Configuration File <y0000000000xx>.cfg
Description	Configures the URL of the ACS. Note: It is only applicable to SIP-T46G IP phones.
Format	URL

Default Value	Blank
Range	String within 511 characters
Example	managementserver.url = http://192.168.1.20/acs/

Parameter- managementserver.connection _request_username	Configuration File <y0000000000xx>.cfg
Description	Configures the user name for the IP phone to authenticate the incoming connection requests. Note: It is only applicable to SIPT46G IP phones.
Format	String
Default Value	Blank
Range	String within 128 characters
Example	managementserver.connection_request_username = acsuser

Parameter- managementserver.connection _request_password	Configuration File <y0000000000xx>.cfg
Description	Configures the password for the IP phone to authenticate the incoming connection requests. Note: It is only applicable to SIPT46G IP phones.
Format	String
Default Value	Blank
Range	String within 64 characters
Example	managementserver.connection_request_password = acspwd

Parameter- managementserver.periodic_in form_enable	Configuration File <y0000000000xx>.cfg
Description	Enables or disables the IP phone to periodically report its configuration information to the ACS. Note: It is only applicable to SIP-T46G IP phones.
Format	Boolean
Default Value	1
Range	Valid values are: 0-Disabled 1-Enabled
Example	managementserver.periodic_inform_enable = 1

Parameter- managementserver.periodic_in form_interval	Configuration File <y0000000000xx>.cfg
Description	Configures the interval (in seconds) to report its configuration information to the ACS. Note: It is only applicable to SIP-T46G IP phones.
Format	Integer
Default Value	60
Range	5 to 42946967295
Example	managementserver.periodic_inform_interval = 60

IPv6

Parameter- network.ip_address_mode	Configuration File <MAC>.cfg
Description	Configures the IP addressing mode. Note: If you change this parameter, the IP phone will reboot to make the change take

	effect.
Format	Integer
Default Value	0
Range	Valid values are: 0-IPv4 1-IPv6 2-IPv4&IPv6
Example	network.ip_address_mode = 1

Parameter- network.ipv6_internet_port.type	Configuration File <MAC>.cfg
Description	Configures the IPv6 address assignment method. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer
Default Value	0
Range	Valid values are: 0-DHCP 1-Static
Example	network.ipv6_internet_port.type = 0

Parameter- network.ipv6_static_dns_enable	Configuration File <MAC>.cfg
Description	Enables or disables the phone to use manually configured static IPv6 DNS when the parameter "network.ipv6_internet_port.type" is set to 0 (DHCP). Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled

	1-Enabled
Example	network.ipv6_static_dns_enable= 0

Parameter- network.ipv6_internet_port.ip	Configuration File <MAC>.cfg
Description	Configures the IPv6 address. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	IPv6 Address
Default Value	Blank
Range	Not Applicable
Example	network.ipv6_internet_port.ip = 2026:1234:1:1:215:65ff:fe1f:caa

Parameter- network.ipv6_prefix	Configuration File <MAC>.cfg
Description	Configures the prefix of the IPv6 address. Note: If you change this parameter, the IP phone will reboot to make change take effect.
Format	Integer
Default Value	64
Range	0 to 128
Example	network.ipv6_prefix = 64

Parameter- network.ipv6_internet_port.gateway	Configuration File <MAC>.cfg
Description	Configures the gateway when the Internet port type is defined as Static IP Address. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	IPv6 Address
Default Value	Blank

Range	Not Applicable
Example	network.ipv6_internet_port.gateway = 3036:1:1:c3c7:c11c:5447:23a6:255

Parameter-	Configuration File
network.ipv6_primary_dns	<MAC>.cfg
Description	Configures the primary DNS server when the Internet port type is defined as Static IP Address. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	IPv6 Address
Default Value	Blank
Range	Not Applicable
Example	network.ipv6_primary_dns = 3036:1:1:c3c7:c11c:5447:23a6:256

Parameter-	Configuration File
network.ipv6_secondary_dns	<MAC>.cfg
Description	Configures the secondary DNS server when the Internet port type is defined as Static IP Address. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	IPv6 Address
Default Value	Blank
Range	Not Applicable
Example	network.ipv6_secondary_dns = 2026:1234:1:1:c3c7:c11c:5447:23a6

Parameter-	Configuration File
network.ipv6_icmp_v6.enable	<MAC>.cfg
Description	Enables or disables ICMPv6 feature. If it is set to 1 (enabled), the IP phone will

	obtain network settings of the IPv6 from the ICMPv6 protocol. Note: If you change this parameter, the IP phone will reboot to make the change take effect. It is only applicable to SIP-T46G IP phones.
Format	Boolean
Default Value	1
Range	Valid values are: 0-Disabled 1-Enabled
Example	network.ipv6_icmp_v6.enable = 1

Audio Feature Parameters

Headset Prior

Parameter-	Configuration File
features.headset_prior	<y0000000000xx>.cfg
Description	Enables or disables headset prior feature. If it is set to 1 (enabled), a user needs to press the Headset key to activate the headset mode. The headset mode will not be deactivated until the user presses the Headset key again.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	features.headset_prior = 1

Dual Headset

Parameter-	Configuration File
features.headset_training	<y0000000000xx>.cfg
Description	Enables or disables dual headset feature. If it is set to 1 (Enabled), users can use two headsets on one phone. When the IP phone joins in a call, the users with the headset connected to the headset jack have a full-duplex conversation, while the users with the headset connected to the handset jack are only allowed to listen to.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	features.headset_training = 1

Audio Codecs

Parameter-	Configuration File
account.X.codec.Y.enable	<MAC>.cfg
Description	Enables or disables the IP phone to use the specific codec for account X. X ranges from 1 to 6. Y ranges from 1 to 14.
Format	Boolean
Default Value	When Y=1, the default value is 1; When Y=2, the default value is 1; When Y=3, the default value is 0; When Y=4, the default value is 0; When Y=5, the default value is 1; When Y=6, the default value is 1; When Y=7, the default value is 0; When Y=8, the default value is 0;

	<p>When Y=9, the default value is 0;</p> <p>When Y=10, the default value is 0;</p> <p>When Y=11, the default value is 0;</p> <p>When Y=12, the default value is 0.</p>
Range	<p>Valid values are:</p> <p>0-Disabled</p> <p>1-Enabled</p>
Example	account.1.codec.1.enable = 1

Parameter- account.X.codec.Y.payload_type	Configuration File <MAC>.cfg
Description	<p>Configures the codec for account X to use.</p> <p>X ranges from 1 to 6.</p> <p>Y ranges from 1 to 14.</p>
Format	String
Default Value	<p>When Y=1, the default value is PCMU;</p> <p>When Y=2, the default value is PCMA;</p> <p>When Y=3, the default value is G723_53;</p> <p>When Y=4, the default value is G723_63;</p> <p>When Y=5, the default value is G729;</p> <p>When Y=6, the default value is G722;</p> <p>When Y=7, the default value is iLBC;</p> <p>When Y=8, the default value is G726-16;</p> <p>When Y=9, the default value is G726-24;</p> <p>When Y=10, the default value is G726-32;</p> <p>When Y=11, the default value is G726-40;</p> <p>When Y=12, the default value is GSM.</p>
Range	<p>Valid values are:</p> <ul style="list-style-type: none"> • PCMU • PCMA • G729 • G722 • G723_53 • G723_63 • G726-16 • G726-24 • G726-32

	<ul style="list-style-type: none"> • G726-40 • iLBC • GSM
Example	account.1.codec.1.payload_type = PCMU

Parameter- account.X.codec.Y.priority	Configuration File <MAC>.cfg
Description	Configures the priority for the codec. X ranges from 1 to 6. Y ranges from 1 to 14.
Format	Integer
Default Value	When Y=1, the default value is 1; When Y=2, the default value is 2; When Y=3, the default value is 0; When Y=4, the default value is 0; When Y=5, the default value is 3; When Y=6, the default value is 4; When Y=7, the default value is 0; When Y=8, the default value is 0; When Y=9, the default value is 0; When Y=10, the default value is 0; When Y=11, the default value is 0; When Y=12, the default value is 0.
Range	0 to 11
Example	account.1.codec.1.priority = 1

Parameter- account.X.codec.Y.rtpmap	Configuration File <MAC>.cfg
Description	Configures the rtpmap. X ranges from 1 to 6. Y ranges from 1 to 14.
Format	Integer
Default Value	When Y=1, the default value is 0; When Y=2, the default value is 8; When Y=3, the default value is 4;

	<p>When Y=4, the default value is 4;</p> <p>When Y=5, the default value is 18;</p> <p>When Y=6, the default value is 9;</p> <p>When Y=7, the default value is 106;</p> <p>When Y=8, the default value is 103;</p> <p>When Y=9, the default value is 104;</p> <p>When Y=10, the default value is 102;</p> <p>When Y=11, the default value is 105;</p> <p>When Y=12, the default value is 97.</p>
Range	0 to 127
Example	account.1.codec.1.rtpmap = 0

Ptime

Parameter-	Configuration File
account.X.ptime	<MAC>.cfg
Description	<p>Configures the ptime (in milliseconds) for the codec.</p> <p>X ranges from 1 to 6.</p>
Format	Integer
Default Value	20
Range	<p>Valid values are:</p> <p>0 (Disabled)</p> <p>10, 20, 30, 40, 50, 60</p>
Example	account.1.ptime = 20

Acoustic Echo Cancellation

Parameter-	Configuration File
voice.echo_cancellation	<y0000000000xx>.cfg
Description	Enables or disables AEC feature on the IP phone.
Format	Boolean
Default Value	1
Range	<p>Valid values are:</p> <p>0-Disabled</p>

	1-Enabled
Example	voice.echo_cancellation = 1

Voice Activity Detection

Parameter- voice.vad	Configuration File <y0000000000xx>.cfg
Description	Enables or disables VAD feature on the IP phone.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	voice.vad = 1

Comfort Noise Generation

Parameter- voice.cng	Configuration File <y0000000000xx>.cfg
Description	Enables or disables CNG feature on the IP phone.
Format	Boolean
Default Value	1
Range	Valid values are: 0-Disabled 1-Enabled
Example	voice.cng = 1

Jitter Buffer

Parameter- voice.jib.adaptive	Configuration File <y0000000000xx>.cfg
Description	Configures the type of jitter buffer.

Format	Integer
Default Value	1
Range	Valid values are: 0-Fixed 1-Adaptive
Example	voice.jib.adaptive = 1

Parameter- voice.jib.min	Configuration File <y0000000000xx>.cfg
Description	Configures the minimum delay time for jitter buffer. Note: It works only if the parameter "voice.jib.adaptive" is set to 1 (Adaptive).
Format	Integer
Default Value	60
Range	0 to 400
Example	voice.jib.min = 60

Parameter- voice.jib.max	Configuration File <y0000000000xx>.cfg
Description	Configures the maximum delay time for jitter buffer. Note: It works only if the parameter "voice.jib.adaptive" is set to 1 (Adaptive).
Format	Integer
Default Value	240
Range	0 to 400
Example	voice.jib.max = 240

Parameter- voice.jib.normal	Configuration File <y0000000000xx>.cfg
Description	Configures the fixed delay time for jitter buffer. Note: It works only if the parameter "voice.jib.adaptive" is set to 0 (Fixed).

Format	Integer
Default Value	120
Range	0 to 400
Example	voice.jib.mormal = 120

Security Feature Parameters

TLS

Parameter-	Configuration File
account.X.transport	<MAC>.cfg
Description	Configures the transport type for account X. If it is set to 2 (TLS), the SIP message of this account will be encrypted after the successful TLS negotiation. X ranges from 1 to 6.
Format	Integer
Default Value	0 (UDP)
Range	Valid values are: 0-UDP 1-TCP 2-TLS 3-DNS-NAPTR
Example	account.1.transport = 0

Parameter-	Configuration File
security.trust_certificates	<y0000000000xx>.cfg
Description	Enables or disables the IP phone to authenticate the connecting server. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Boolean
Default Value	1
Range	Valid values are:

	0-Disabled 1-Enabled
Example	security.trust_certificates = 1

Parameter- security.ca_cert	Configuration File <y0000000000xx>.cfg
Description	Configures the type of certificates the IP phone used to authenticate the connecting server. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer
Default Value	2
Range	Valid values are: 0-Default certificates 1-Custom certificates 2-All certificates
Example	security.ca_cert = 2

Parameter- security.cn_validation	Configuration File <y0000000000xx>.cfg
Description	Enables or disables the IP phone to mandatorily validate the CommonName or subjectAltName of the certificate sent by the connecting server. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	security.cn_validation = 1

Parameter-	Configuration File
security.dev_cert	<y0000000000xx>.cfg
Description	Configures the type of certificates the IP phone sends for authentication. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer
Default Value	0
Range	Valid values are: 0-Default certificates 1-Custom certificates
Example	security.dev_cert = 0

Uploading Certificates

Parameter-	Configuration File
trusted_certificates.url	<y0000000000xx>.cfg
Description	Configures the access URL of the certificate used to authenticate the connecting server. Note: The certificate you want to upload must be in .pem, .crt, .cer or .der format.
Format	URL
Default Value	Blank
Range	String within 511 characters
Example	trusted_certificates.url = http://192.168.1.20/tc.crt

Parameter-	Configuration File
server_certificates.url	<y0000000000xx>.cfg
Description	Configures the access URL of the certificate the IP phone sends for authentication. Note: The certificate you want to upload must be in .pem or .cer format.
Format	URL

Default Value	Blank
Range	String within 511 characters
Example	server_certificates.url = http://192.168.1.20/ca.pem

SRTP

Parameter-	Configuration File
account.X.srtp_encryption	<MAC>.cfg
Description	Configures whether to use voice encryption service. If it is set to 1 (Optional), the phone will negotiate with the other phone what type of encryption to utilize for the session. If it is set to 2 (Compulsory), the phone is forced to use SRTP during a call. X ranges from 1 to 6.
Format	Integer
Default Value	0
Value	Valid values are: 0-Disabled 1-Optional 2-Compulsory
Example	account.1.srtp_encryption = 1

Configuring Decryption Method

Parameter-	Configuration File
auto_provision.aes_key_in_file	<y0000000000xx>.cfg
Description	Enables or disables the IP phone to decrypt configuration files using the encrypted AES keys. If it is set to 1 (Enabled), the IP phone will download <y0000000000xx_Security>.enc and <MAC_Security>.enc files during auto provisioning, and then decrypts these files into the plaintext keys (e.g., key2, key3)

	<p>respectively using the phone built-in key (e.g., key1). The IP phone then decrypts the encrypted configuration files using corresponding key (e.g., key2, key3).</p> <p>If it is set to 0 (Disabled), the IP phone will decrypt the encrypted configuration files using AES keys configured on the IP phone.</p>
Format	Boolean
Default Value	0
Range	<p>Valid values are:</p> <p>0-Disabled</p> <p>1-Enabled</p>
Example	auto_provision.aes_key_in_file = 0

Parameter- auto_provision.aes_key_16.com	Configuration File <y0000000000xx>.cfg
Description	<p>Configures the plaintext AES key which is used to decrypt the <y0000000000xx>.cfg file.</p> <p>Note: It works only if the parameter "auto_provision.aes_key_in_file" is set to 0 (Disabled).</p>
Format	String
Default Value	Blank
Range	16 characters and the supported characters contain: 0 ~ 9, A ~ Z, a ~ z.
Example	auto_provision.aes_key_16.com = 0123456789abcdef

Parameter- auto_provision.aes_key_16.mac	Configuration File <y0000000000xx>.cfg
Description	<p>Configures the plaintext AES key which is used to decrypt the <MAC>.cfg file.</p> <p>Note: It works only if the parameter "auto_provision.aes_key_in_file" is set to 0 (Disabled).</p>

Format	String
Default Value	Blank
Range	16 characters and the supported characters contain: 0 ~ 9, A ~ Z, a ~ z.
Example	auto_provision.aes_key_16.mac = 0123456789abmins

Upgrading Firmware

Parameter- firmware.url	Configuration File <y0000000000xx>.cfg
Description	Configures the access URL of firmware. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	URL
Default Value	Blank
Range	String within 511 characters
Example	firmware.url = http://192.168.1.20/2.71.0.140.rom

Parameter- auto_provision.power_on =	Configuration File <y0000000000xx>.cfg
Description	Enables or disables the IP phone to perform an auto provisioning process when powered on.
Format	Boolean
Default Value	1
Range	Valid values are: 0-Disabled 1-Enabled
Example	auto_provision.mode = 1

Parameter-	Configuration File
auto_provision.repeat.enable	< y0000000000xx >.cfg
Description	Enables or disables the phone to check new configuration repeatedly.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	auto_provision.repeat.enable = 1

Parameter-	Configuration File
auto_provision.repeat.minutes	< y0000000000xx >.cfg
Description	Configures the interval (in minutes) for the IP phone to check new configuration. Note: It works only if the parameter "auto_provision.repeat.enable" is set to 1(Enabled).
Format	Integer
Default Value	1440
Range	1 to 43200
Example	auto_provision.repeat.minutes = 1000

Parameter-	Configuration File
auto_provision.weekly.enable	< y0000000000xx >.cfg
Description	Enables or disables the phone to check new configuration weekly.
Format	Boolean
Default Value	0
Range	Valid values are: 0-Disabled 1-Enabled
Example	auto_provision.weekly.enable = 1

Parameter-	Configuration File
auto_provision.weekly.begin_time	< y0000000000xx >.cfg
Description	Configures the begin time of the day for the IP phone to check new configuration weekly. Note: It works only if the parameter "auto_provision.weekly.enable" is set to 1(Enabled).
Format	Time
Default Value	00:00
Range	00:00 to 23:59
Example	auto_provision.weekly.begin_time = 01:30

Parameter-	Configuration File
auto_provision.weekly.end_time	< y0000000000xx >.cfg
Description	Configures the end time of the day for the IP phone to check new configuration weekly. Note: It works only if the parameter "auto_provision.weekly.enable" is set to 1(Enabled).
Format	Time
Default Value	00:00
Range	00:00 to 23:59
Example	auto_provision.weekly.end_time = 21:30

Parameter-	Configuration File
auto_provision.weekly.dayofweek	< y0000000000xx >.cfg
Description	Configures the days of the week for the IP phone to check new configuration weekly.
Format	Integer
Default Value	0123456
Range	Valid values are: 0-Sunday

	1 -Monday 2 -Tuesday 3 -Wednesday 4 -Thursday 5 -Friday 6 -Saturday
Example	auto_provision.weekly.dayofweek = 0123456

Resource Files

Access URL of Replace Rule Template

Parameter-	Configuration File
dialplan_replace_rule.url	<y0000000000xx>.cfg
Description	Configures the access URL of the replace rule template.
Format	URL
Default Value	Blank
Range	String within 511 characters
Example	dialplan_replace_rule.url = http://192.168.10.25/dialplan.xml

Access URL of Dial-now Template

Parameter-	Configuration File
dialplan_dialnow.url	<y0000000000xx>.cfg
Description	Configures the access URL of the dial-now template.
Format	URL
Default Value	Blank
Range	String within 511 characters
Example	dialplan_dialnow.url = http://192.168.10.25/dialnow.xml

Access URL of Softkey Layout Template

Parameter-	Configuration File
custom_softkey_call_failed.url	<y0000000000xx>.cfg
Description	Configures the access URL of the custom file for the soft key presented on the LCD screen when in the CallFailed state.
Format	URL
Default Value	Blank
Range	String within 511 characters
Example	The following example uses HTTP to download the CallFailed state file from the "XMLfiles" directory on provisioning server 10.2.8.16 using 8080 port. custom_softkey_call_failed.url = http://10.2.8.16:8080/XMLfiles/CallFailed.xml

Parameter-	Configuration File
custom_softkey_call_in.url	<y0000000000xx>.cfg
Description	Configures the access URL of the custom file for the soft key presented on the LCD screen when in the CallIn state.
Format	URL
Default Value	Blank
Range	String within 511 characters
Example	The following example uses HTTP to download the CallIn state file from the "XMLfiles" directory on provisioning server 10.2.8.16 using 8080 port. custom_softkey_call_in.url = http://10.2.8.16:8080/XMLfiles/CallIn.xml

Parameter-	Configuration File
custom_softkey_connecting.url	<y0000000000xx>.cfg
Description	Configures the access URL of the custom file for the soft key presented on the LCD screen when in the Connecting state.
Format	URL
Default Value	Blank
Range	String within 511 characters
Example	The following example uses HTTP to download the Connecting state file from the "XMLfiles" directory on provisioning server 10.2.8.16 using 8080 port. custom_softkey_connecting.url = http://10.2.8.16:8080/XMLfiles/Connecting.xml

Parameter-	Configuration File
custom_softkey_dialing.url	<y0000000000xx>.cfg
Description	Configures the access URL of the custom file for the soft key presented on the LCD screen when in the Dialing state.
Format	URL
Default Value	Blank
Range	String within 511 characters
Example	The following example uses HTTP to download the Dialing state file from the "XMLfiles" directory on provisioning server 10.2.8.16 using 8080 port. custom_softkey_dialing.url = http://10.2.8.16:8080/XMLfiles/Dialing.xml

Parameter-	Configuration File
custom_softkey_ring_back.url	<y0000000000xx>.cfg
Description	Configures the access URL of the custom file for the soft key presented on the LCD screen when in the RingBack state.

Format	URL
Default Value	Blank
Range	String within 511 characters
Example	The following example uses HTTP to download the RingBack state file from the "XMLfiles" directory on provisioning server 10.2.8.16 using 8080 port. custom_softkey_ring_back.url = http://10.2.8.16:8080/XMLfiles/RingBack.xml

Parameter-	Configuration File
custom_softkey_talking.url	<y0000000000xx>.cfg
Description	Configures the access URL of the custom file for the soft key presented on the LCD screen when in the Talking state.
Format	URL
Default Value	Blank
Range	String within 511 characters
Example	The following example uses HTTP to download the Talking state file from the "XMLfiles" directory on provisioning server 10.2.8.16 using port 8080. custom_softkey_talking.url = http://10.2.8.16:8080/XMLfiles/Talking.xml

Access URL of Local Contact File

Parameter-	Configuration File
local_contact.data.url	<y0000000000xx>.cfg
Description	Configures the access URL of the local contact file.
Format	URL
Default Value	Blank
Range	String within 511 characters
Example	local_contact.data.url = http://192.168.10.25/contact.xml

Access URL of Remote XML Phone Book

Parameter-	Configuration File
remote_phonebook.data.X.url	<y0000000000xx>.cfg
Description	Configures the access URL of the remote XML phone book. X ranges from 1 to 5.
Format	URL
Default Value	Blank
Range	String within 511 characters
Example	remote_phonebook.data.1.url = http://192.168.10.25/phonebook.xml

Access URL of Directory Template

Parameter-	Configuration File
directory_setting.url	<y0000000000xx>.cfg
Description	Configures the access URL of the directory template.
Format	URL
Default Value	Blank
Range	String within 511 characters
Example	directory_setting.url = http://192.168.10.25/favorite_setting.xml

Access URL of Super Search Template

Parameter-	Configuration File
super_search.url	<y0000000000xx>.cfg
Description	Configures the access URL of the super search template.
Format	URL
Default Value	Blank
Range	String within 511 characters

Example	super_search.url = http://192.168.10.25/super_search.xml
----------------	---

Access URL of Wallpaper Image

Parameter-	Configuration File
wallpaper_upload.url	<y0000000000xx>.cfg
Description	Configures the access URL of the wallpaper image. Note: It is only applicable to SIP-T46G IP phones.
Format	URL
Default Value	Blank
Range	String within 511 characters
Example	wallpaper_upload.url = http://192.168.10.25/wallpaper.jpg

Troubleshooting

Log Settings

Parameter-	Configuration File
syslog.mode	<y0000000000xx>.cfg
Description	Configures the syslog mode. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer
Default Value	0
Range	0-Local 1-Server
Example	syslog.mode = 1

Parameter-	Configuration File
syslog.server	<y0000000000xx>.cfg
Description	Configures the IP address or domain name of the syslog server where to export the log files. Note: It works only if the parameter "syslog.mode" is set to 1 (Server). If you change this parameter, the IP phone will reboot to make the change take effect.
Format	IP Address or Domain Name
Default Value	Blank
Range	String within 99 characters
Example	syslog.server = 192.168.1.50

Parameter-	Configuration File
syslog.log_level	<y0000000000xx>.cfg
Description	Configures the severity level used to specify the type of syslog information to be exported. Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer
Default Value	3
Range	0 to 6
Example	syslog.log_level = 3

Watch Dog

Parameter-	Configuration File
watch_dog.enable	<y0000000000xx>.cfg
Description	Enables or disables watch dog feature.
Format	Boolean
Default Value	1
Range	Valid values are:

	0 -Disabled 1 -Enabled
Example	watch_dog.enable = 1

Configuring DSS Key

This section provides DSS key parameters you can configure on the IP phone.

DSS key can be assigned with various key features. The parameters of the DSS key are detailed in the following:

Parameter-	Configuration File
linekey.X.type	<y0000000000xx>.cfg
Description	<p>Configures the key feature for the line key. X ranges from 1 to 27 (for SIP-T46G). X ranges from 1 to 15 (for SIP-T42G/T41P).</p> <p>Valid types are:</p> <ul style="list-style-type: none"> • N/A (default to line key 7-27 for SIP-T46G or line key 4-15 for SIP-T42G/T41P) • Conference • Forward • Transfer • Hold • DND • Call Return • SMS (not applicable to SIP-T42G/T41P) • Directed Pickup • Call Park • DTMF • Voice Mail • Speed Dial • Intercom • Line (default for line key 1-6 of SIP-T46G or line key 1-3 of SIP-T42G/T41P) • BLF • URL • Group Listening • Hot Desking • XML Group • Group Pickup • Multicast Paging

	<ul style="list-style-type: none"> • Record • XML Browser • URL Record • LDAP • Prefix • Zero Touch • ACD • Local Group • Keypad Lock • Directory
Format	Integer
Default Value	<p>SIP-T46G: 15 for line key 1-6, 0 for line key 7-27.</p> <p>SIP-T42G/T41P: 15 for line key 1-3, 0 for line key 4-15.</p>
Range	<p>Valid values are:</p> <p>0-N/A</p> <p>1-Conference</p> <p>2-Forward</p> <p>3-Transfer</p> <p>4-Hold</p> <p>5-DND</p> <p>7-Call Return</p> <p>8-SMS</p> <p>9-Directed Pickup</p> <p>10-Call Park</p> <p>11-DTMF</p> <p>12-Voice Mail</p> <p>13-SpeedDial</p> <p>14-Intercom</p> <p>15-Line</p> <p>16-BLF</p> <p>17-URL</p> <p>18-Group Listening</p> <p>22-XML Group</p> <p>23-Group Pickup</p> <p>24-Multicast Paging</p> <p>25-Record</p> <p>27-XML browser</p> <p>34-Hot Desking</p> <p>35-URL Record</p> <p>38-LDAP</p> <p>40-Prefix</p>

	41 -Zero Touch 42 -ACD 45 -Local Group 50 -Keypad Lock 61 -Directory
Example	linekey.1.type = 15

Parameter- linekey.X.line	Configuration File <y0000000000xx>.cfg
Description	<p>Configures the desired line to apply the key feature.</p> <p>X ranges from 1 to 27 (for SIP-T46G).</p> <p>X ranges from 1 to 15 (for SIP-T42G/T41P).</p> <p>When assigning the following features, you don't need to configure this parameter:</p> <ul style="list-style-type: none"> • DTMF • Prefix • XML Browser • LDAP • Conference • Forward • Hold • DND • Call Return • SMS • Record • URL Record • Multicast Paging • Group Listening • Zero Touch • URL • ACD • Hot Desking • Keypad Lock • Directory
Format	Integer
Default Value	0
Range	<p>When specifying the line, valid values are:</p> <p>1 to 6 (for SIP-T46G)</p> <p>1 to 3 (for SIP-T42G/T41P)</p>

	1-Line 1 2-Line 2 ... 6-Line 6
Example	linekey.1.line = 2

Parameter- linekey.X.value	Configuration File <y0000000000xx>.cfg
Description	Configures the value for some key features. X ranges from 1 to 27 (for SIP-T46G). X ranges from 1 to 15 (for SIP-T42G/T41P).
Format	String
Default Value	Blank
Range	String within 99 characters
Example	When Speed Dial is assigned to the line key, this parameter is used to specify the number you want to dial out. linekey.1.value = 1001

Parameter- linekey.X.label	Configuration File <y0000000000xx>.cfg
Description	Configures the label displaying on the LCD screen for each line key. This is an optional configuration. X ranges from 1 to 27 (for SIP-T46G). X ranges from 1 to 15 (for SIP-T42G/T41P).
Format	String
Default Value	Blank
Range	String within 99 characters
Example	linekey.1.label = Dir

Parameter-	Configuration File
linekey.X.pickup_value	<y0000000000xx>.cfg
Description	Configures the pickup code for BLF feature. This parameter is only applicable to BLF feature. X ranges from 1 to 27 (for SIP-T46G). X ranges from 1 to 15 (for SIP-T42G/T41P).
Format	String
Default Value	Blank
Range	String within 256 characters
Example	linekey.1.pickup_value = *88

Parameter-	Configuration File
linekey.X.xml_phonebook	<y0000000000xx>.cfg
Description	Configures the desired group or remote phone book when multiple groups or remote phone books are configured on the IP phone. This parameter is only applicable to Local Group/XML Group features. X ranges from 1 to 27 (for SIP-T46G). X ranges from 1 to 15 (for SIP-T42G/T41P). When the key feature is configured as Local Group, valid values are: 0 -All contacts 1 -First local group ... 48 -Forty-eighth local group When the key feature is configured as XML Group (remote phone book), valid values are: 0 -First XML group 1 -Second XML group ... 4 -Fifth XML group
Format	Integer

Default Value	0
Range	0 to 48
Example	Configures the second remote phone book. linekey.1.xml_phonebook = 1

Keypad Lock Key

Parameter- linekey.X.type	Configuration File <y0000000000xx>.cfg
Description	Configures a line key to be a keypad lock key on the IP phone. The digit 50 stands for the key type Keypad Lock . X ranges from 1 to 27 (for SIP-T46G). X ranges from 1 to 15 (for SIP-T42G/T41P).
Format	Integer
Value	50
Example	linekey.1.type = 50

DND Key

Parameter- linekey.X.type	Configuration File <y0000000000xx>.cfg
Description	Configures a line key to be a DND key on the IP phone. The digit 5 stands for the key type DND . X ranges from 1 to 27 (for SIP-T46G). X ranges from 1 to 15 (for SIP-T42G/T41P).
Format	Integer
Value	5
Example	linekey.1.type = 5

Directed Call Pickup Key

Parameter- linekey.X.type	Configuration File <y0000000000xx>.cfg
Description	Configures a line key to be a directed call pickup key on the IP phone. The digit 9 stands for the key type Directed Pickup . X ranges from 1 to 27 (for SIP-T46G). X ranges from 1 to 15 (for SIP-T42G/T41P).
Format	Integer
Value	9
Example	linekey.1.type = 9

Parameter- linekey.X.line	Configuration File <y0000000000xx>.cfg
Description	Configures the desired line to apply the directed call pickup key. X ranges from 1 to 27 (for SIP-T46G). X ranges from 1 to 15 (for SIP-T42G/T41P).
Format	Integer
Range	Valid values are: 1 to 6 (for SIP-T46G) 1 to 3 (for SIP-T42G/T41P) 1-Line 1 2-Line 2 ... 6-Line 6
Example	linekey.1.line = 1

Parameter- linekey.X.value	Configuration File <y0000000000xx>.cfg
Description	Configures the directed call pickup feature code followed by the number of monitored extension. X ranges from 1 to 27 (for SIP-T46G).

	X ranges from 1 to 15 (for SIP-T42G/T41P).
Format	String
Range	String within 99 characters
Example	linekey.1.value = *971001

Group Call Pickup Key

Parameter- linekey.X.type	Configuration File <y0000000000xx>.cfg
Description	Configures a line key to be a group call pickup key on the IP phone. The digit 23 stands for the key type Group Pickup . X ranges from 1 to 27 (for SIP-T46G). X ranges from 1 to 15 (for SIP-T42G/T41P).
Format	Integer
Value	23
Example	linekey.1.type = 23

Parameter- linekey.X.line	Configuration File <y0000000000xx>.cfg
Description	Configures the desired line to apply the group call pickup key. X ranges from 1 to 27 (for SIP-T46G). X ranges from 1 to 15 (for SIP-T42G/T41P).
Format	Integer
Range	Valid values are: 1 to 6 (for SIP-T46G) 1 to 3 (for SIP-T42G/T41P) 1-Line 1 2-Line 2 ... 6-Line 6
Example	linekey.1.line = 1

Parameter- linekey.X.value	Configuration File <y0000000000xx>.cfg
Description	Configures the group call pickup feature code. X ranges from 1 to 27 (for SIP-T46G). X ranges from 1 to 15 (for SIP-T42G/T41P).
Format	String
Range	String within 99 characters
Example	linekey.1.value = *98

Call Return Key

Parameter- linekey.X.type	Configuration File <y0000000000xx>.cfg
Description	Configures a line key to be a call return key on the IP phone. The digit 7 stands for the key type Call Return . X ranges from 1 to 27 (for SIP-T46G). X ranges from 1 to 15 (for SIP-T42G/T41P).
Format	Integer
Value	7
Example	linekey.2.type = 7

Call Park Key

Parameter- linekey.X.type	Configuration File <y0000000000xx>.cfg
Description	Configures a line key to be a call park key on the IP phone. The digit 10 stands for the key type Call Park . X ranges from 1 to 27 (for SIP-T46G). X ranges from 1 to 15 (for SIP-T42G/T41P).
Format	Integer
Value	10

Example	linekey.2.type = 10
----------------	---------------------

Parameter- linekey.X.line	Configuration File <y0000000000xx>.cfg
Description	Configures the desired line to apply the call park key. X ranges from 1 to 27 (for SIP-T46G). X ranges from 1 to 15 (for SIP-T42G/T41P).
Format	Integer
Range	Valid values are: 1 to 6 (for SIP-T46G) 1 to 3 (for SIP-T42G/T41P) 1-Line 1 2-Line 2 ... 6-Line 6
Example	linekey.2.line = 0

Parameter- linekey.X.value	Configuration File <y0000000000xx>.cfg
Description	Configures the call park feature code. X ranges from 1 to 27 (for SIP-T46G). X ranges from 1 to 15 (for SIP-T42G/T41P).
Format	String
Range	String within 99 characters
Example	linekey.2.value = *99

Intercom Key

Parameter- linekey.X.type	Configuration File <y0000000000xx>.cfg
Description	Configures a line key to be an intercom key. The digit 14 stands for the key type Intercom . X ranges from 1 to 27 (for SIP-T46G). X ranges from 1 to 15 (for SIP-T42G/T41P).

Format	Integer
Value	14
Example	linekey.2.type = 14

Parameter- linekey.X.line	Configuration File <y0000000000xx>.cfg
Description	Configures the desired line to apply the intercom key. X ranges from 1 to 27 (for SIP-T46G). X ranges from 1 to 15 (for SIP-T42G/T41P).
Format	Integer
Range	Valid values are: 1 to 6 (for SIP-T46G) 1 to 3 (for SIP-T42G/T41P) 1-Line 1 2-Line 2 ... 6-Line 6
Example	linekey.2.line = 1

Parameter- linekey.X.value	Configuration File <y0000000000xx>.cfg
Description	Configures the intercom number. X ranges from 1 to 27 (for SIP-T46G). X ranges from 1 to 15 (for SIP-T42G/T41P).
Format	String
Range	String within 99 characters
Example	linekey.2.value = 1008

LDAP Key

Parameter- linekey.X.type	Configuration File <y0000000000xx>.cfg
Description	Configures a line key to be an LDAP key on the IP phone.

	The digit 38 stands for the key type LDAP . X ranges from 1 to 27 (for SIP-T46G). X ranges from 1 to 15 (for SIP-T42G/T41P).
Format	Integer
Value	38
Example	linekey.2.type = 38

BLF Key

Parameter- linekey.X.type	Configuration File <y0000000000xx>.cfg
Description	Configures a line key to be a BLF key on the IP phone. The digit 16 stands for the key type BLF . X ranges from 1 to 27 (for SIP-T46G). X ranges from 1 to 15 (for SIP-T42G/T41P).
Format	Integer
Value	16
Example	linekey.3.type = 16

Parameter- linekey.X.line	Configuration File <y0000000000xx>.cfg
Description	Configures the desired line to apply the BLF key. X ranges from 1 to 27 (for SIP-T46G). X ranges from 1 to 15 (for SIP-T42G/T41P).
Format	Integer
Range	Valid values are: 1 to 6 (for SIP-T46G) 1 to 3 (for SIP-T42G/T41P) 1-Line 1 2-Line 2 ... 6-Line 6
Example	linekey.3.line = 2

Parameter- linekey.X.value	Configuration File <y0000000000xx>.cfg
Description	Configures the number of the monitored user. X ranges from 1 to 27 (for SIP-T46G). X ranges from 1 to 15 (for SIP-T42G/T41P).
Format	String
Range	String within 99 characters
Example	linekey.3.value = 1008

Parameter- linekey.X.pickup_value	Configuration File <y0000000000xx>.cfg
Description	Configures the pickup code for BLF feature. This parameter only applies to BLF feature. X ranges from 1 to 27 (for SIP-T46G). X ranges from 1 to 15 (for SIP-T42G/T41P).
Format	String
Default Value	Blank
Range	String within 256 characters
Example	linekey.3.pickup_value = *88

ACD Key

Parameter- linekey.X.type	Configuration File <y0000000000xx>.cfg
Description	Configures a line key to be an ACD key on the IP phone. The digit 42 stands for the key type ACD . X ranges from 1 to 27 (for SIP-T46G). X ranges from 1 to 15 (for SIP-T42G/T41P).
Format	Integer
Value	42
Example	linekey.2.type = 42

Multicast Paging Key

Parameter- linekey.X.type	Configuration File <y0000000000xx>.cfg
Description	Configures a line key to be a multicast paging key on the IP phone. The digit 24 stands for the key type Multicast Paging . X ranges from 1 to 27 (for SIP-T46G). X ranges from 1 to 15 (for SIP-T42G/T41P).
Format	Integer
Value	24
Example	linekey.3.type = 24

Parameter- linekey.X.value	Configuration File <y0000000000xx>.cfg
Description	Configures the multicast IP address and port number. X ranges from 1 to 27 (for SIP-T46G). X ranges from 1 to 15 (for SIP-T42G/T41P). Note: The valid multicast IP addresses range from 224.0.0.0 to 239.255.255.255.
Format	IP Address
Range	224.0.0.0 to 239.255.255.255.
Example	linekey.3.value = 224.5.5.6:10008

Record Key

Parameter- linekey.X.type	Configuration File <y0000000000xx>.cfg
Description	Configures a line key to be a record key on the IP phone. The digit 25 stands for the key type Record . X ranges from 1 to 27 (for SIP-T46G). X ranges from 1 to 15 (for SIP-T42G/T41P).
Format	Integer

Value	25
Example	linekey.2.type = 25

URL Record Key

Parameter- linekey.X.type	Configuration File <y0000000000xx>.cfg
Description	Configures a line key to be a URL record key on the IP phone. The digit 35 stands for the key type URL Record . X ranges from 1 to 27 (for SIP-T46G). X ranges from 1 to 15 (for SIP-T42G/T41P).
Format	Integer
Value	35
Example	linekey.2.type = 35

Parameter- linekey.X.value	Configuration File <y0000000000xx>.cfg
Description	Configures the URL to record a call. X ranges from 1 to 27 (for SIP-T46G). X ranges from 1 to 15 (for SIP-T42G/T41P).
Format	String
Default Value	Blank
Range	String within 99 characters
Example	linekey.2.value = http://10.1.2.224/phonerecording.cgi

Hot Desking Key

Parameter- linekey.X.type	Configuration File <y0000000000xx>.cfg
Description	Configures a line key to be a hot desking key on the IP phone. The digit 34 stands for the key type Hot

	Desking. X ranges from 1 to 27 (for SIP-T46G). X ranges from 1 to 15 (for SIP-T42G/T41P).
Format	Integer
Value	34
Example	linekey.2.type = 34

Appendix D: SIP (Session Initiation Protocol)

This section describes how Yealink SIPT4X IP phones comply with the IETF definition of SIP as described in RFC 3261.

This section contains compliance information in the following:

- [RFC and Internet Draft Support](#)
- [SIP Request](#)
- [SIP Header](#)
- [SIP Responses](#)
- [SIP Session Description Protocol \(SDP\) Usage](#)

RFC and Internet Draft Support

The following RFC's and Internet drafts are supported:

- RFC 1321—The MD5 Message-Digest Algorithm
- RFC 1889—RTP Media control
- RFC 2112—Multipart MIME
- RFC 2246—The TLS Protocol Version 1.0
- RFC 2327—SDP: Session Description Protocol
- RFC 2543—SIP: Session Initiation Protocol
- RFC 2616—Hypertext Transfer Protocol -- HTTP/1.1
- RFC 2617—Http Authentication: Basic and Digest access authentication
- RFC 2782—A DNS RR for specifying the location of services (DNS SRV)
- RFC 2806—URLs for Telephone Calls
- RFC 2833—RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
- RFC2915—The Naming Authority Pointer (NAPTR) DNS Resource Record
- RFC 3087—Control of Service Context using SIP Request-URI
- RFC 3261—SIP: Session Initiation Protocol (replacement for RFC 2543)

- RFC 3262—Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
- RFC 3263—Session Initiation Protocol (SIP): Locating SIP Servers
- RFC 3264—An Offer/Answer Model with the Session Description Protocol (SDP)
- RFC 3265—Session Initiation Protocol (SIP) - Specific Event Notification
- RFC 3266—Support for IPv6 in Session Description Protocol (SDP)
- RFC 3310—HTTP Digest Authentication Using Authentication and Key Agreement (AKA)
- RFC 3311—The Session Initiation Protocol (SIP) UPDATE Method
- RFC 3312—Integration of Resource Management and SIP
- RFC 3313—Private SIP Extensions for Media Authorization
- RFC 3323—A Privacy Mechanism for the Session Initiation Protocol (SIP)
- RFC 3324—Requirements for Network Asserted Identity
- RFC 3325—SIP Asserted Identity
- RFC 3326—The Reason Header Field for the Session Initiation Protocol (SIP)
- RFC 3361—DHCP-for-IPv4 Option for SIP Servers
- RFC 3372—SIP for Telephones (SIP-T): Context and Architectures
- RFC 3420—Internet Media Type message/sipfrag
- RFC 3428—Session Initiation Protocol (SIP) Extension for Instant Messaging
- RFC 3455—Private Header (P-Header) Extensions to the SIP for the 3GPP
- RFC 3486—Compressing the Session Initiation Protocol (SIP)
- RFC 3489—STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)
- RFC 3515—The Session Initiation Protocol (SIP) Refer Method
- RFC 3550—RTP , RTCP, IETF RFC 3550
- RFC 3556—Session Description Protocol (SDP) Bandwidth Modifiers for RTCP Bandwidth
- RFC 3581—An Extension to the SIP for Symmetric Response Routing
- RFC 3608—SIP Extension Header Field for Service Route Discovery During Registration
- RFC 3665—Session Initiation Protocol (SIP) Basic Call Flow Examples
- RFC 3666—SIP Public Switched Telephone Network (PSTN) Call Flows.
- RFC 3680—SIP Event Package for Registrations
- RFC 3702—Authentication, Authorization, and Accounting Requirements for the SIP
- RFC 3711—The Secure Real-time Transport Protocol (SRTP)
- RFC 3725—Best Current Practices for Third Party Call Control (3pcc) in the Session

Initiation Protocol (SIP)

- RFC 3842—A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)
- RFC 3856—A Presence Event Package for Session Initiation Protocol (SIP)
- RFC 3890—A Transport Independent Bandwidth Modifier for the SDP
- RFC 3891—The Session Initiation Protocol (SIP) “Replaces” Header
- RFC 3892—The Session Initiation Protocol (SIP) Referred-By Mechanism
- RFC 3959—The Early Session Disposition Type for SIP
- RFC 3960—Early Media and Ringing Tone Generation in SIP
- RFC3966—The tel URI for telephone number
- RFC 3968—The Internet Assigned Number Authority (IANA) Header Field Parameter Registry for the Session Initiation Protocol (SIP)
- RFC 3969—The Internet Assigned Number Authority (IANA) Uniform Resource Identifier (URI) Parameter Registry for the Session Initiation Protocol (SIP)
- RFC 4028—Session Timers in the Session Initiation Protocol (SIP)
- RFC 4235—An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP)
- RFC 4244—An Extension to the SIP for Request History Information
- RFC 4317—Session Description Protocol (SDP) Offer/Answer Examples
- RFC 4353—A Framework for Conferencing with the SIP
- RFC 4475—Session Initiation Protocol (SIP) Torture
- RFC 4485—Guidelines for Authors of Extensions to the SIP
- RFC 4504—SIP Telephony Device Requirements and Configuration
- RFC 4566—SDP: Session Description Protocol.
- RFC 4568—Session Description Protocol (SDP) Security Descriptions for Media Streams
- RFC 4575—A SIP Event Package for Conference State
- RFC 4579—SIP Call Control - Conferencing for User Agents
- RFC 4662—A SIP Event Notification Extension for Resource Lists
- RFC 5009—P-Early-Media Header
- RFC 5079—Rejecting Anonymous Requests in SIP
- RFC 5359—Session Initiation Protocol Service Examples
- RFC 5589—Session Initiation Protocol (SIP) Call Control - Transfer
- draft-levy-sip-diversion-04.txt—Diversion Indication in SIP
- draft-ietf-sip-cc-transfer-05.txt—SIP Call Control - Transfer

- draft-anil-sipping-bla-02.txt—Implementing Bridged Line Appearances (BLA) Using Session Initiation Protocol (SIP)
- draft-ietf-sip-privacy-04.txt—SIP Extensions for Network-Asserted Caller Identity and Privacy within Trusted Networks
- draft-ietf-sipping-cc-conferencing-03.txt—SIP Call Control - Conferencing for User Agents

To find the applicable Request for Comments (RFC) document, go to <http://www.ietf.org/rfc.html> and enter the RFC number.

SIP Request

The following SIP request messages are supported:

Method	Supported	Notes
REGISTER	Yes	
INVITE	Yes	Yealink SIP-T4X IP phones support mid-call changes such as putting a call on hold as signaled by a new INVITE that contains an existing Call-ID.
ACK	Yes	
CANCEL	Yes	
BYE	Yes	
OPTIONS	Yes	
SUBSCRIBE	Yes	
NOTIFY	Yes	
REFER	Yes	
PRACK	Yes	
INFO	Yes	
MESSAGE	Yes	
UPDATE	Yes	
PUBLISH	Yes	

SIP Header

The following SIP request headers are supported:

Method	Supported	Notes
Accept	Yes	
Alert-Info	Yes	
Allow	Yes	
Allow-Events	Yes	
Authorization	Yes	
Call-ID	Yes	
Call-Info	Yes	
Contact	Yes	
Content-Length	Yes	
Content-Type	Yes	
CSeq	Yes	
Diversion	Yes	
Event	Yes	
Expires	Yes	
From	Yes	
Max-Forwards	Yes	
Min-SE	Yes	
P-Asserted-Identity	Yes	
P-Preferred-Identity	Yes	
Proxy-Authenticate	Yes	
Proxy-Authorization	Yes	
RAck	Yes	
Record-Route	Yes	
Refer-To	Yes	
Referred-By	Yes	
Remote-Party-ID	Yes	
Replaces	Yes	

Method	Supported	Notes
Require	Yes	
Route	Yes	
RSeq	Yes	
Session-Expires	Yes	
Subscription-State	Yes	
Supported	Yes	
To	Yes	
User-Agent	Yes	
Via	Yes	

SIP Responses

The following SIP responses are supported:

1xx Response—Information Responses

1xx Response	Supported	Notes
100 Trying	Yes	
180 Ringing	Yes	
181 Call Is Being Forwarded	Yes	
183 Session Progress	Yes	

2xx Response—Successful Responses

2xx Response	Supported	Notes
200 OK	Yes	
202 Accepted	Yes	In REFER transfer.

3xx Response—Redirection Responses

3xx Response	Supported	Notes
300 Multiple Choices	Yes	
301 Moved Permanently	Yes	

3xx Response	Supported	Notes
302 Moved Temporarily	Yes	

4xx Response—Request Failure Responses

4xx Response	Supported	Notes
400 Bad Request	Yes	
401 Unauthorized	Yes	
402 Payment Required	Yes	
403 Forbidden	Yes	
404 Not Found	Yes	
405 Method Not Allowed	Yes	
406 Not Acceptable	No	
407 Proxy Authentication Required	Yes	
408 Request Timeout	Yes	
409 Conflict	No	
410 Gone	No	
411 Length Required	No	
413 Request Entity Too Large	No	
414 Request-URI Too Long	Yes	
415 Unsupported Media Type	Yes	
416 Unsupported URI Scheme	No	
420 Bad Extension	No	
421 Extension Required	No	
423 Interval Too Brief	Yes	
480 Temporarily Unavailable	Yes	
481 Call/Transaction Does Not Exist	Yes	
482 Loop Detected	Yes	
483 Too Many Hops	No	
484 Address Incomplete	Yes	
485 Ambiguous	No	

4xx Response	Supported	Notes
486 Busy Here	Yes	
487 Request Terminated	Yes	
488 Not Acceptable Here	Yes	
491 Request Pending	No	
493 Undecipherable	No	

5xx Response—Server Failure Responses

5xx Response	Supported	Notes
500 Internal Server Error	Yes	
501 Not Implemented	Yes	
502 Bad Gateway	No	
503 Service Unavailable	No	
504 Gateway Timeout	No	
505 Version Not Supported	No	

6xx Response—Global Responses

6xx Response	Supported	Notes
600 Busy Everywhere	Yes	
603 Decline	Yes	
604 Does Not Exist Anywhere	No	
606 Not Acceptable	No	

SIP Session Description Protocol (SDP) Usage

SDP Headers	Supported
v—Protocol version	Yes
o—Owner/creator and session identifier	Yes
a—Media attribute	Yes
c—Connection information	Yes

m—Media name and transport address	Yes
s—Session name	Yes
t—Active time	Yes

Appendix E: SIP Call Flows

SIP uses six request methods:

- INVITE—Indicates a user is being invited to participate in a call session.
- ACK—Confirms that the client has received a final response to an INVITE request.
- BYE—Terminates a call and can be sent by either the caller or the callee.
- CANCEL—Cancels any pending searches but does not terminate a call that has already been accepted.
- OPTIONS—Queries the capabilities of servers.
- REGISTER—Registers the address listed in the To header field with a SIP server.

The following types of responses are used by SIP and generated by the IP phone or the SIP server:

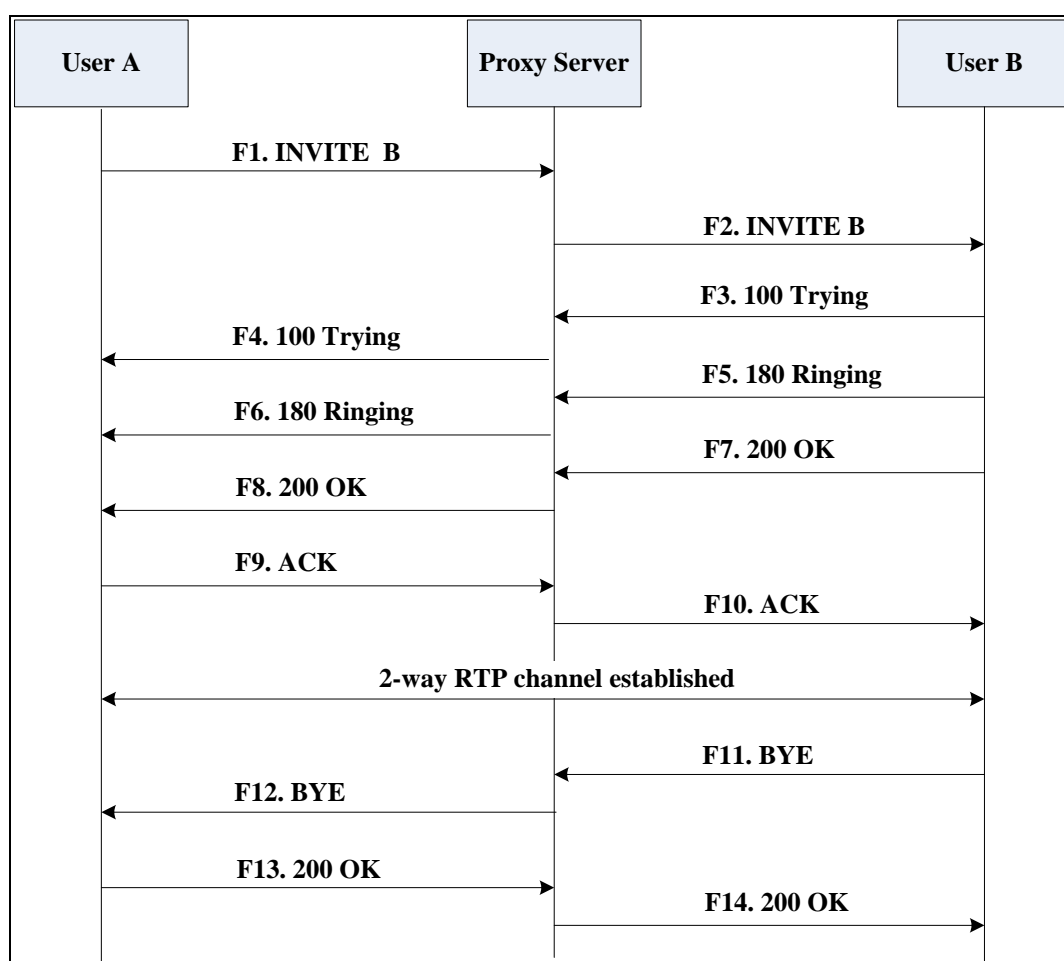
- SIP 1xx—Informational Responses
- SIP 2xx—Successful Responses
- SIP 3xx—Redirection Responses
- SIP 4xx—Client Failure Responses
- SIP 5xx—Server Failure Responses
- SIP 6xx—Global Failure Responses

Successful Call Setup and Disconnect

The following figure illustrates the scenario of a successful call. In this scenario, the two end users are User A and User B. User A and User B are located at Yealink SIP IP phones.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.
3. User B hangs up.



Step	Action	Description
F1	INVITE—User A to Proxy Server	<p>User A sends a SIP INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> • The IP address of User B is inserted in the Request-URI field. • User A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User A is ready to receive is specified. • The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	100 Trying—User B to Proxy Server	User B sends a SIP 100 Trying response to the proxy server. The 100 Trying response indicates that the INVITE request has been received by User B.
F4	100 Trying—Proxy Server to User A	The proxy server forwards the SIP 100 Trying to User A to indicate that the INVITE request has been received by User B.
F5	180 Ringing—User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the User B is being alerted.
F6	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.

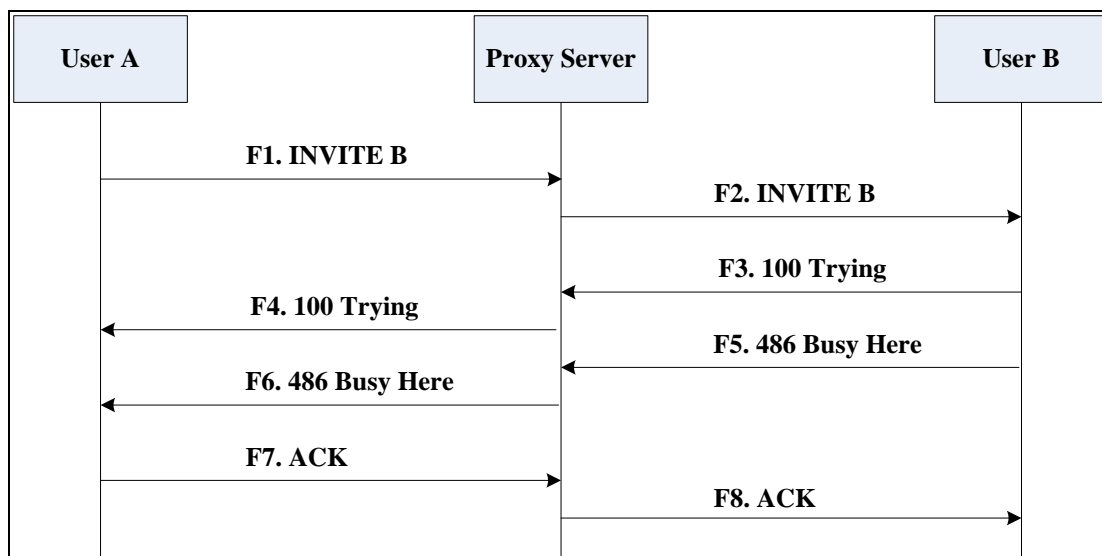
Step	Action	Description
F7	200 OK— User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F8	200OK—Proxy Server to User A	The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the connection has been made.
F9	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F10	ACK—Proxy Server to User B	The proxy server sends the SIP ACK to User B. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.
F11	BYE—User B to Proxy Server	User B terminates the call session by sending a SIP BYE request to the proxy server. The BYE request indicates that User B wants to release the call.
F12	BYE—Proxy Server to User A	The proxy server forwards the SIP BYE request to User A to notify that User B wants to release the call.
F13	200 OK—User A to Proxy Server	User A sends a SIP 200 OK response to the proxy server. The 200 OK response indicates that User A has received the BYE request. The call session is now terminated.
F14	200 OK—Proxy Server to User B	The proxy server forwards the SIP 200 OK response to User B to indicate that User A has received the BYE request. The call session is now terminated.

Unsuccessful Call Setup—Called User is Busy

The following figure illustrates the scenario of an unsuccessful call caused by the called user's being busy. In this scenario, the two end users are User A and User B. User A and User B are located at Yealink SIP IP phones.

The call flow scenario is as follows:

1. User A calls User B.
2. User B is busy on the IP phone and unable or unwilling to take another call.
The call cannot be set up successfully.



Step	Action	Description
F1	INVITE—User A to Proxy Server	<p>User A sends the INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> • The IP address of User B is inserted in the Request-URI field. • User A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User A is ready to receive is specified. • The port on which User B is prepared to receive the RTP data is

Step	Action	Description
		specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. Proxy server forwards the INVITE message to User B.
F3	100 Trying—User B to Proxy Server	User B sends a SIP 100 Trying response to the proxy server. The 100 Trying response indicates that the INVITE request has been received by User B.
F4	100 Trying—Proxy Server to User A	The proxy server forwards the SIP 100 Trying to User A to indicate that the INVITE request has already been received.
F5	486 Busy Here—User B to Proxy Server	User B sends a SIP 486 Busy Here response to the proxy server. The 486 Busy Here response is a client error response indicating that User B is successfully connected but User B is busy on the IP phone and unable or unwilling to take the call.
F6	486 Busy Here—Proxy Server to User A	The proxy server forwards the 486 Busy Here response to notify User A that User B is busy.
F7	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The SIP ACK message indicates that User A has received the 486 Busy Here message.
F8	ACK—Proxy Server to User B	The proxy server forwards the SIP ACK to User B to indicate that the 486 Busy Here message has already been received.

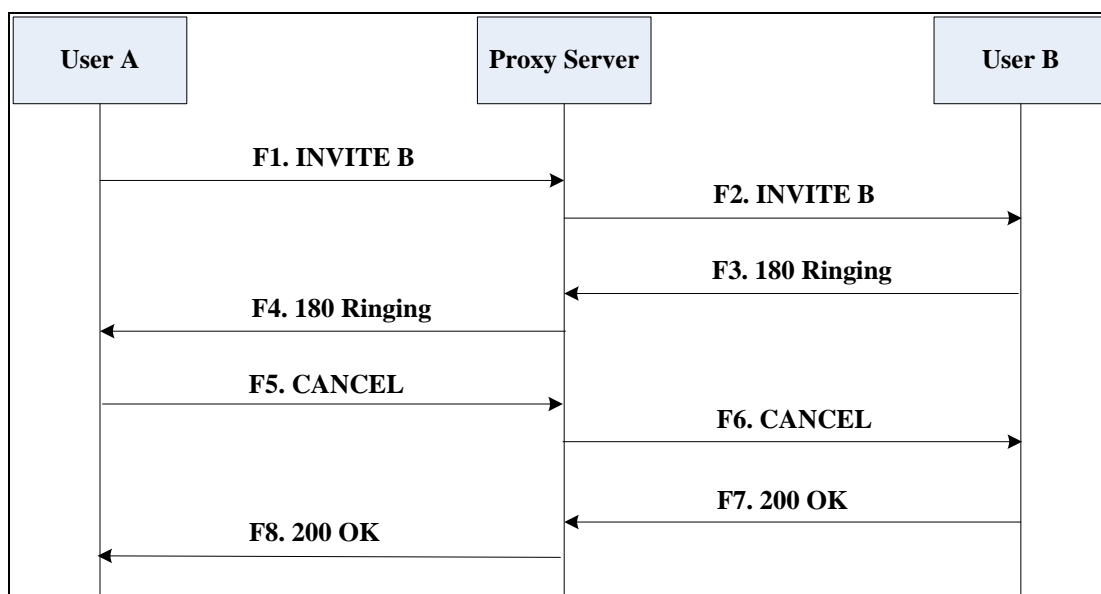
Unsuccessful Call Setup—Called User Does Not Answer

The following figure illustrates the scenario of an unsuccessful call caused by the called user’s no answering. In this scenario, the two end users are User A and User B. User A and User B are located at Yealink SIP IP phones.

The call flow scenario is as follows:

1. User A calls User B.
2. User B does not answer the call.
3. User A hangs up.

The call cannot be set up successfully.



Step	Action	Description
F1	INVITE—User A to Proxy Server	<p>User A sends an INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> • The IP address of User B is inserted in the Request-URI field. • User A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.

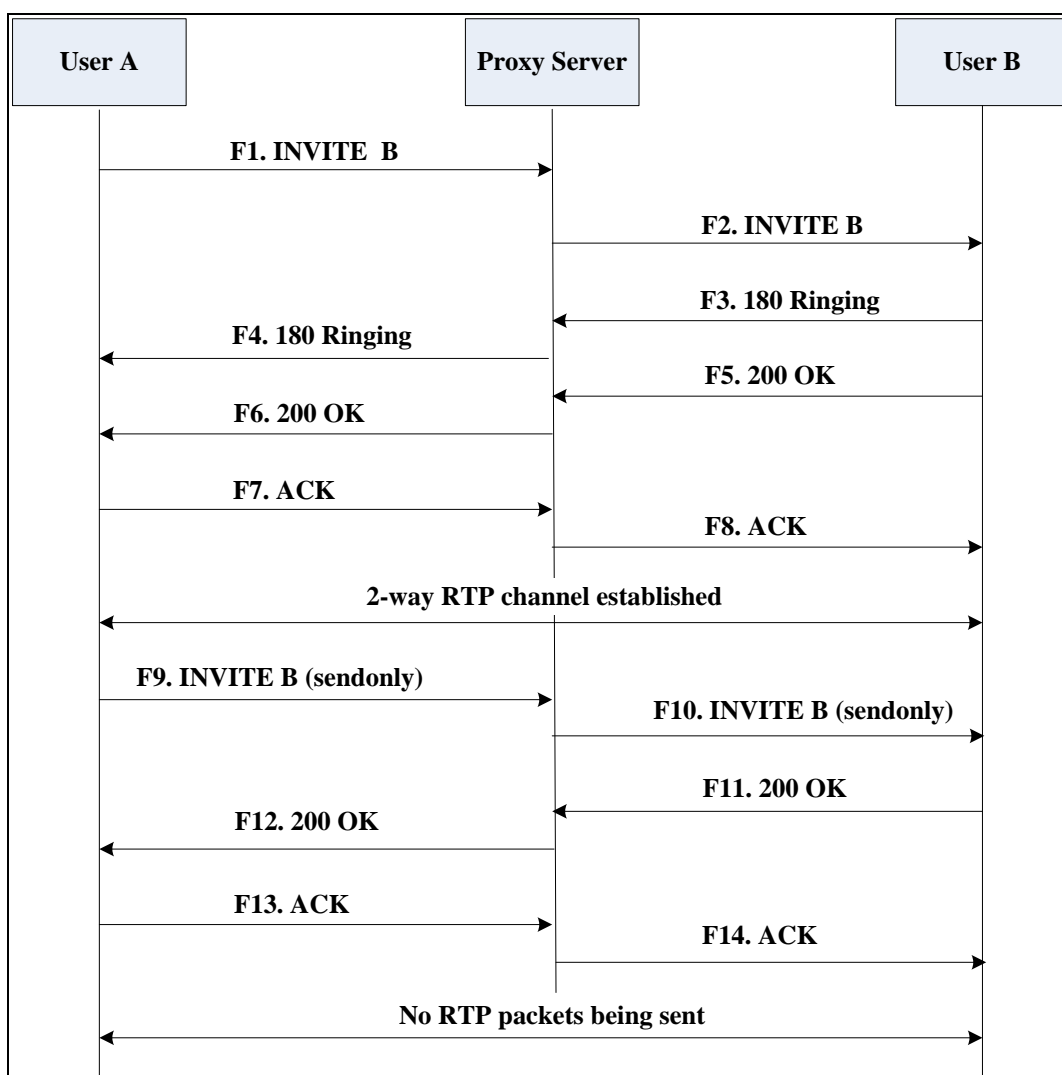
Step	Action	Description
		<ul style="list-style-type: none"> • The transaction number within a single call leg is identified in the CSeq field. • The media capability User A is ready to receive is specified. • The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. Proxy server forwards the INVITE message to User B.
F3	180 Ringing—User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	CANCEL—User A to Proxy Server	User A sends a SIP CANCEL request to the proxy server after not receiving an appropriate response within the time allocated in the INVITE request. The SIP CANCEL request indicates that User A wants to disconnect the call.
F6	CANCEL—Proxy Server to User B	The proxy server forwards the SIP CANCEL request to notify User B that User A wants to disconnect the call.
F7	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The SIP 200 OK response indicates that User B has received the CANCEL request.
F8	200 OK—Proxy Server to User A	The proxy server forwards the SIP 200 OK response to notify User A that the CANCEL request has been processed successfully.

Successful Call Setup and Call Hold

The following figure illustrates a successful call setup and call hold. In this scenario, the two end users are User A and User B. User A and User B are located at Yealink SIP IP phones.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.
3. User A puts User B on hold.



Step	Action	Description
F1	INVITE—User A to Proxy Server	<p>User A sends an INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> • The IP address of User B is inserted in the Request-URI field. • User A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User A is ready to receive is specified. • The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	180 Ringing—User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies the proxy server that the connection has been made.
F6	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the connection has been made.

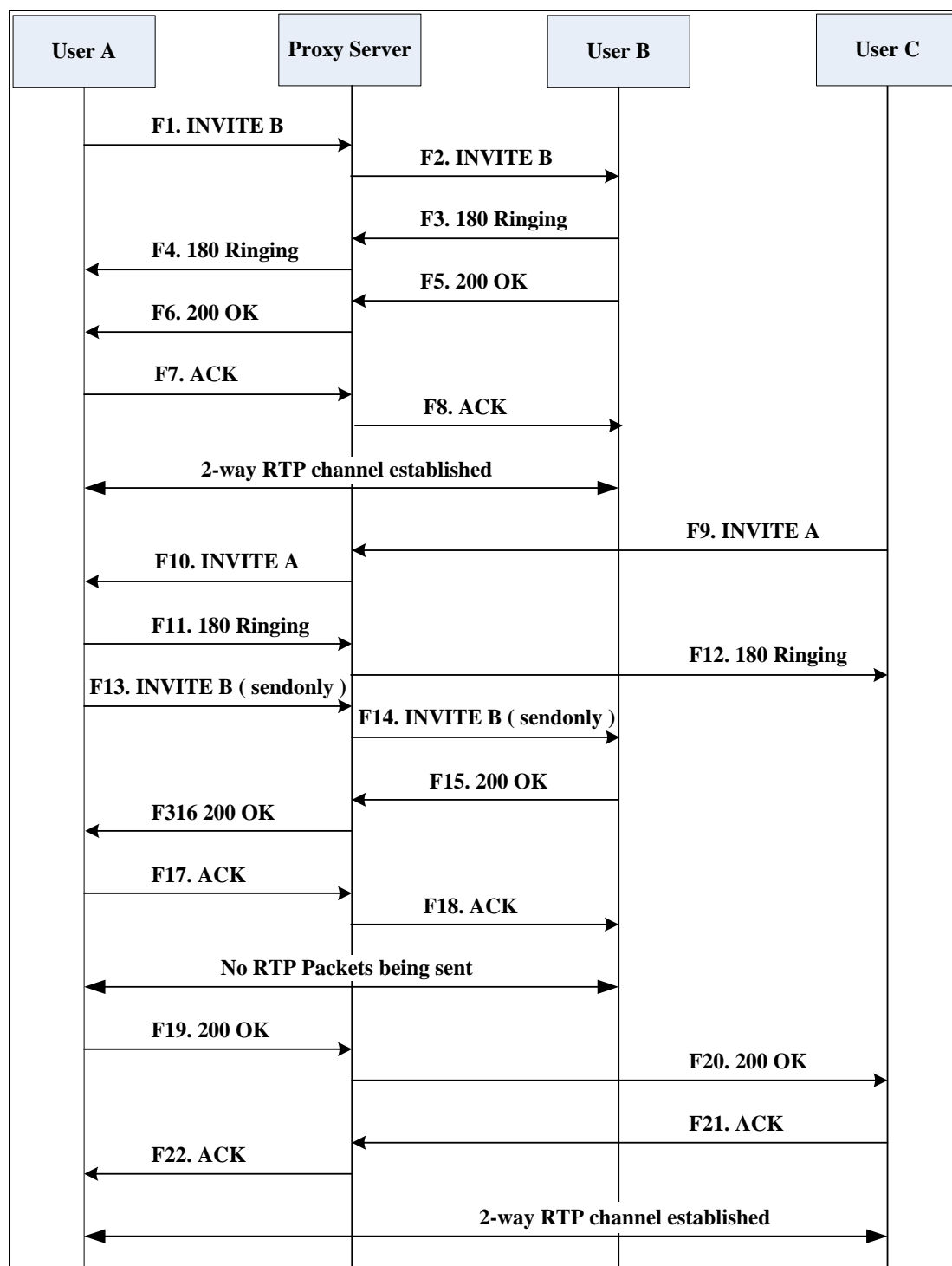
Step	Action	Description
F7	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F8	ACK—Proxy Server to User B	The proxy server sends the SIP ACK to User B. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.
F9	INVITE—User A to Proxy Server	User A sends a mid-call INVITE request to the proxy server with new SDP session parameters, which are used to place the call on hold.
F10	INVITE—Proxy Server to User B	The proxy server forwards the mid-call INVITE message to User B.
F11	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the INVITE is successfully processed.
F12	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK response to User A. The 200 OK response notifies User B is successfully put on hold.
F13	ACK—User A to Proxy Server	User A sends an ACK message to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now temporarily inactive. No RTP packets are being sent.
F14	ACK—Proxy Server to User B	The proxy server sends the ACK message to User B. The ACK confirms that the proxy server has received the 200 OK response.

Successful Call Setup and Call Waiting

The following figure illustrates a successful call between Yealink SIP IP phones in which two parties are in a call, one of the participants receives and answers an incoming call from a third party. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.
3. User C calls User B.
4. User B accepts the call from User C.



Step	Action	Description
F1	INVITE—User A to Proxy Server	<p>User A sends an INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> • The IP address of User B is inserted in the Request-URI field. • User A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User A is ready to receive is specified. • The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	180 Ringing—User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies proxy server that the connection has been made.
F6	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the connection has been made.

Step	Action	Description
F7	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server, The ACK confirms that User A has received the 200 OK response. The call session is now active.
F8	ACK—Proxy Server to User B	The proxy server sends the SIP ACK to User B. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.
F9	INVITE—User C to Proxy Server	<p>User C sends a SIP INVITE message to the proxy server. The INVITE request is an invitation to User A to participate in a call session.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> • The IP address of User A is inserted in the Request-URI field. • User C is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User C is ready to receive is specified. • The port on which User A is prepared to receive the RTP data is specified.
F10	INVITE—Proxy Server to User A	The proxy server maps the SIP URI in the To field to User A. The proxy server sends the INVITE message to User A.
F11	180 Ringing—User A to Proxy Server	User A sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F12	180 Ringing—Proxy Server to User C	The proxy server forwards the 180 Ringing response to User C. User C hears the ring-back tone indicating that User A is being alerted.

Step	Action	Description
F13	INVITE—User A to Proxy Server	User A sends a mid-call INVITE request to the proxy server with new SDP session parameters, which are used to place the call on hold.
F14	INVITE—Proxy Server to User B	The proxy server forwards the mid-call INVITE message to User B.
F15	200 OK—User B to Proxy Server	User B sends a 200 OK to the proxy server. The 200 OK response indicates that the INVITE was successfully processed.
F16	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK response to User A. The 200 OK response notifies User B is successfully put on hold.
F17	ACK—User A to Proxy Server	User A sends an ACK message to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now temporarily inactive. No RTP packets are being sent.
F18	ACK—Proxy Server to User B	The proxy server sends the ACK message to User B. The ACK confirms that the proxy server has received the 200 OK response.
F19	200 OK—User A to Proxy Server	User A sends a 200 OK response to the proxy server. The 200 OK response notifies that the connection has been made.
F20	200 OK—Proxy Server User C	The proxy server forwards the 200 OK message to User C.
F21	ACK—User C to Proxy Server	User C sends a SIP ACK to the proxy server. The ACK confirms that User C has received the 200 OK response. The call session is now active.
F22	ACK—Proxy Server to User A	The proxy server forwards the SIP ACK to User A to confirm that User C has received the 200 OK response.

Call Transfer without Consultation

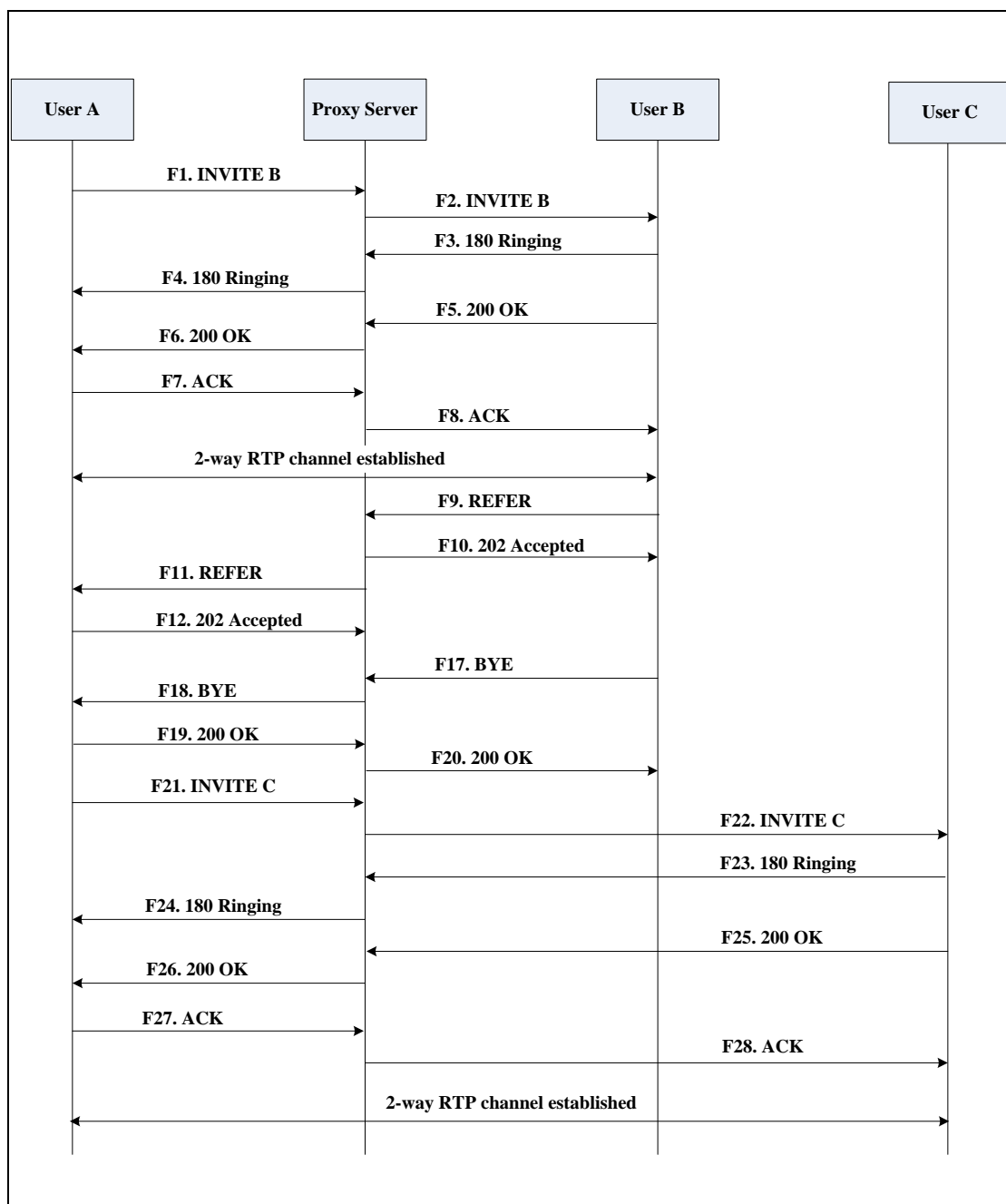
The following figure illustrates a successful call between Yealink SIP IP phones in which two parties are in a call and then one of the parties transfers the call to a third party without consultation. This is called a blind transfer. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.
3. User B transfers the call to User C.

4. User C answers the call.

Call is established between User A and User C.



Step	Action	Description
F1	INVITE—User A to Proxy Server	<p>User A sends an INVITE message to the proxy server. The INVITE request is an invitation to User B to participate in a call session.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> • The IP address of User B is inserted in the Request-URI field. • User A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User A is ready to receive is specified. • The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	180 Ringing—User B to Proxy server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F6	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the connection has been made.

Step	Action	Description
F7	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server, The ACK confirms that User A has received the 200 OK response. The call session is now active.
F8	ACK—Proxy Server to User B	The proxy server sends the SIP ACK to User B. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.
F9	REFER—User B to Proxy Server	User B sends a REFER message to the proxy server. User B performs a blind transfer of User A to User C.
F10	202 Accepted—Proxy Server to User B	The proxy server sends a SIP 202 Accept response to User B. The 202 Accepted response notifies User B that the proxy server has received the REFER message.
F11	REFER—Proxy Server to User A	The proxy server forwards the REFER message to User A.
F12	202 Accepted—User A to Proxy Server	User A sends a SIP 202 Accept response to the proxy server. The 202 Accepted response indicates that User A accepts the transfer.
F13	BYE—User B to Proxy Server	User B terminates the call session by sending a SIP BYE request to the proxy server. The BYE request indicates that User B wants to release the call.
F14	BYE—Proxy Server to User A	The proxy server forwards the BYE request to User A.
F15	200OK—User A to Proxy Server	User A sends a SIP 200 OK response to the proxy server. The 200 OK response confirms that User A has received the BYE request.
F16	200OK—Proxy Server to User B	The proxy server forwards the SIP 200 OK response to User B.
F17	INVITE—User A to Proxy Server	User A sends a SIP INVITE request to the proxy server. In the INVITE request, a unique Call-ID is generated and the Contact-URI field indicates that User A

Step	Action	Description
		requests the call.
F18	INVITE—Proxy Server to User C	The proxy server maps the SIP URI in the To field to User C.
F19	180 Ringing—User C to Proxy Server	User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F20	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User C is being alerted
F21	200OK—User C to Proxy Server	User C sends a SIP 200 OK response to the proxy server. The 200 OK response notifies the proxy server that the connection has been made.
F22	200OK—Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A.
F23	ACK— User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F24	ACK—Proxy Server to User C	The proxy server forwards the ACK message to User C. The ACK confirms that User A has received the 200 OK response. The call session is now active.

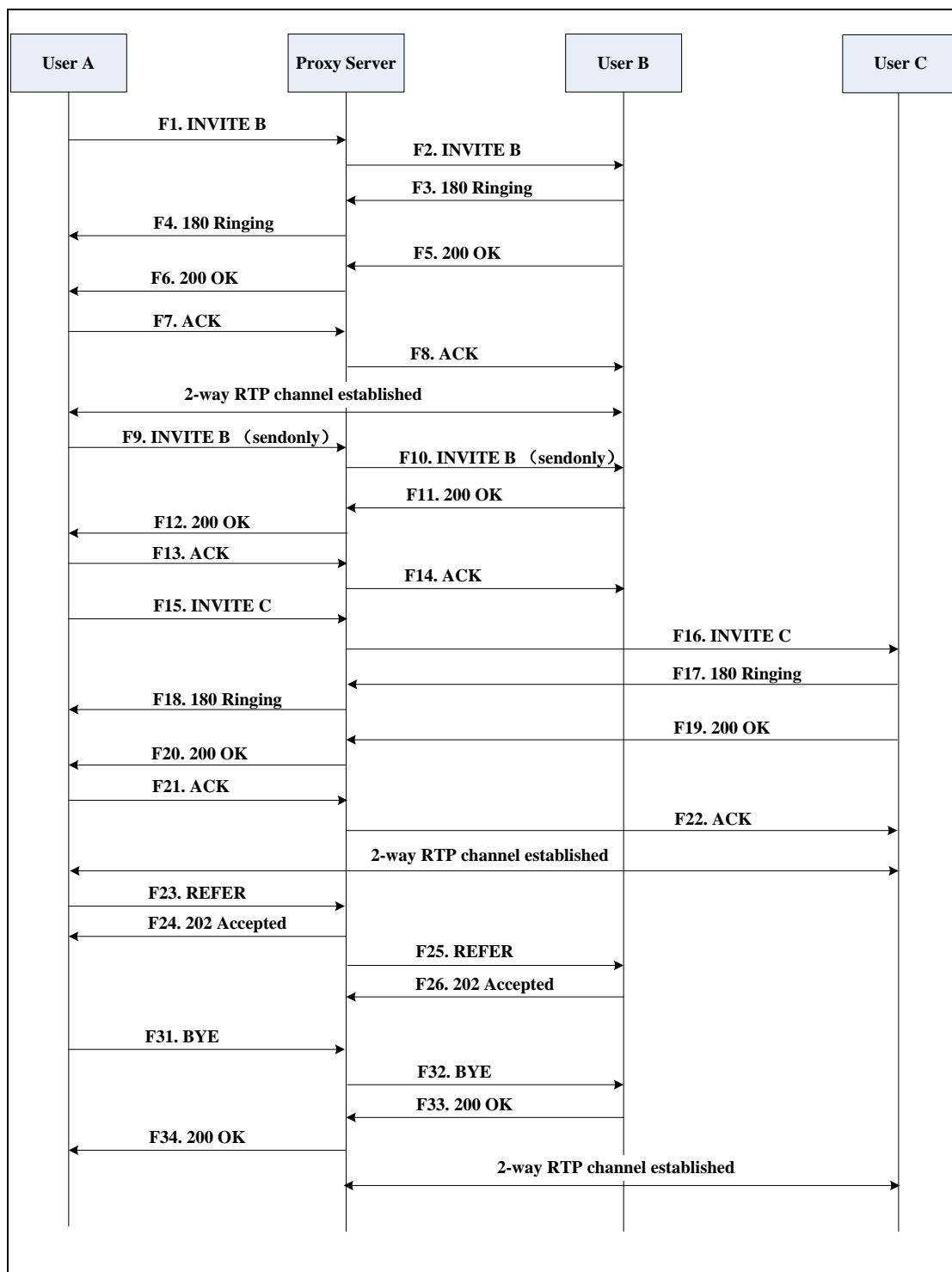
Call Transfer with Consultation

The following figure illustrates a successful call between Yealink SIP IP phones in which two parties are in a call and then one of the parties transfers the call to the third party with consultation. This is called attended transfer. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.
3. User A calls User C.
4. User C answers the call.

5. User A transfers the call to User C.
Call is established between User B and User C.



Step	Action	Description
F1	INVITE—User A to Proxy Server	<p>User A sends an INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> • The IP address of User B is inserted in the Request-URI field. • User A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User A is ready to receive is specified. • The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	180 Ringing—User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F6	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the connection has been made.

Step	Action	Description
F7	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server, The ACK confirms that User A has received the 200 OK response. The call session is now active.
F8	ACK—Proxy Server to User B	The proxy server sends the SIP ACK to User B. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.
F9	INVITE—User A to Proxy Server	User A sends a mid-call INVITE request to the proxy server with new SDP session parameters, which are used to place the call on hold.
F10	INVITE—Proxy Server to User B	The proxy server forwards the mid-call INVITE message to User B.
F11	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the INVITE was successfully processed.
F12	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK response to User A. The 200 OK response notifies User B is successfully put on hold.
F13	ACK—User A to Proxy Server	User A sends an ACK message to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now temporarily inactive. No RTP packets are being sent.
F14	ACK—Proxy Server to User B	The proxy server sends the ACK message to User B. The ACK confirms that the proxy server has received the 200 OK response.
F15	INVITE—User A to Proxy Server	User A sends a SIP INVITE request to the proxy server. In the INVITE request, a unique Call-ID is generated and the Contact-URI field indicates that User A requests the call.
F16	INVITE—Proxy Server to User	The proxy server maps the SIP URI in the To field to User C. The proxy server

Step	Action	Description
	C	sends the INVITE request to User C.
F17	180 Ringing—User C to Proxy Server	User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F18	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User C is being alerted.
F19	200OK—User C to Proxy Server	User C sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F20	200OK—Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A. The 200 OK response notifies User A that the connection has been made.
F21	ACK— User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F22	ACK—Proxy Server to User C	The proxy server forwards the ACK message to User C. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.
F23	REFER—User A to Proxy Server	User A sends a REFER message to the proxy server. User A performs a transfer of User B to User C.
F24	202 Accepted—Proxy Server to User A	The proxy server sends a SIP 202 Accepted response to User A. The 202 Accepted response notifies User A that the proxy server has received the REFER message.
F25	REFER—Proxy Server to User B	The proxy server forwards the REFER message to User B.
F26	202 Accepted—User B to Proxy Server	User B sends a SIP 202 Accept response to the proxy server. The 202 Accepted

Step	Action	Description
		response indicates that User B accepts the transfer.
F27	BYE—User A to Proxy Server	User A terminates the call session by sending a SIP BYE request to the proxy server. The BYE request indicates that User A wants to release the call.
F28	BYE—Proxy Server to User B	The proxy server forwards the BYE request to User B.
F29	200OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that User B has received the BYE request.
F30	200OK—Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A.

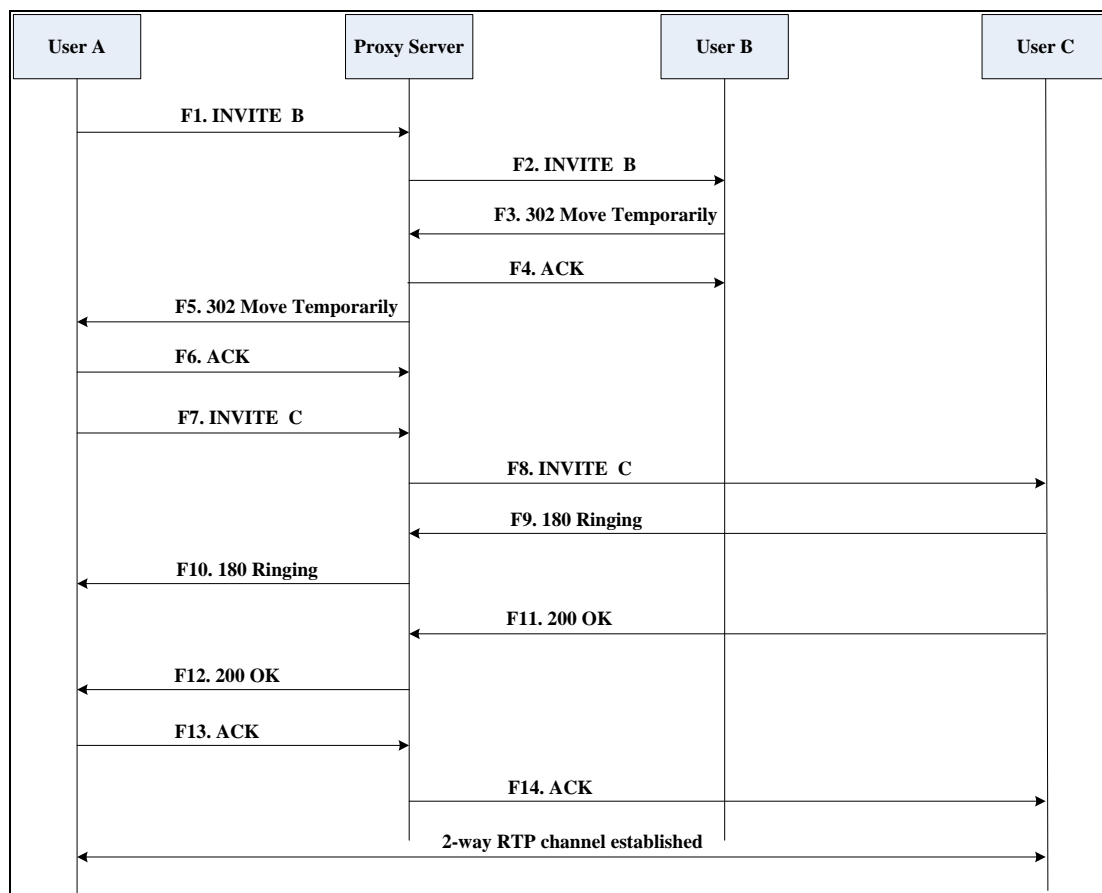
Always Call Forward

The following figure illustrates successful call forwarding between Yealink SIP IP phones in which User B has enabled always call forward. The incoming call is immediately forwarded to User C when User A calls User B. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User B enables always call forward, and the destination number is User C.
2. User A calls User B.
3. User B forwards the incoming call to User C.

- User C answers the call.
Call is established between User A and User C.



Step	Action	Description
F1	INVITE—User A to Proxy Server	<p>User A sends an INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> • The IP address of the User B is inserted in the Request-URI field. • User A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User A is ready to receive is specified. • The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	302 Move Temporarily—User B to Proxy Server	User B sends a SIP 302 Moved Temporarily message to the proxy server. The message indicates that User B is not available at SIP phone B. User B rewrites the contact-URI.
F4	ACK—Proxy Server to User B	The proxy server sends a SIP ACK to User B, the ACK message notifies User B that the proxy server has received the 302 Move Temporarily message.
F5	302 Move Temporarily—Proxy Server to User A	The proxy server forwards the 302 Moved Temporarily message to User A.
F6	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK message notifies the proxy server that User A has received the 302 Move Temporarily message.

Step	Action	Description
F7	INVITE—User A to Proxy Server	User A sends a SIP INVITE request to the proxy server. In the INVITE request, a unique Call-ID is generated and the Contact-URI field indicates that User A requested the call.
F8	INVITE—Proxy Server to User C	The proxy server maps the SIP URI in the To field to User C. The proxy server sends the SIP INVITE request to User C.
F9	180 Ringing—User C to Proxy Server	User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F10	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User C is being alerted.
F11	200OK—User C to Proxy Server	User C sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F12	200OK—Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A. The 200 OK response notifies User A that the connection has been made.
F13	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F14	ACK—Proxy Server to User C	The proxy server forwards the ACK message to User C. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.

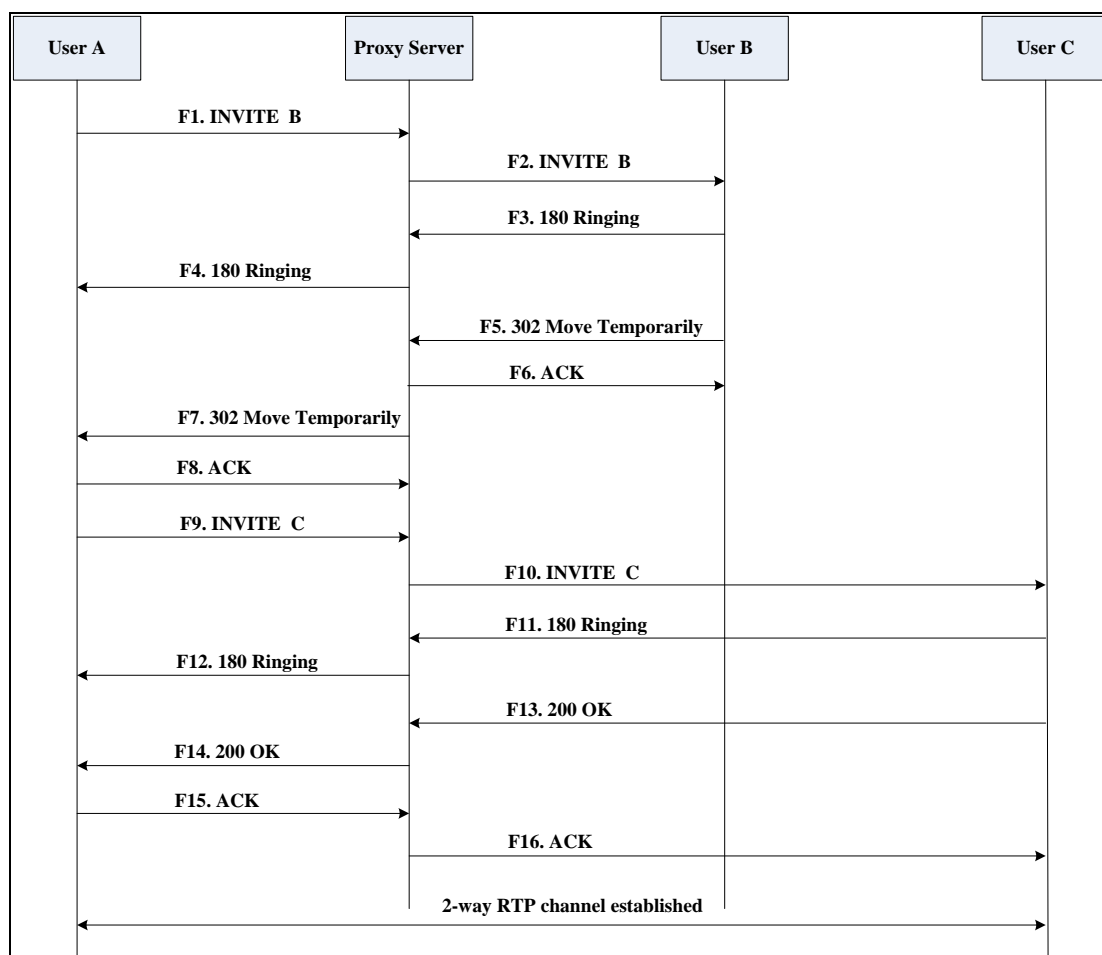
Busy Call Forward

The following figure illustrates successful call forwarding between Yealink SIP IP phones in which User B has enabled busy call forward. The incoming call is forwarded to User C when User B is busy. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User B enables busy call forward, and the destination number is User C.
2. User A calls User B.
3. User B is busy.
4. User B forwards the incoming call to User C.
5. User C answers the call.

Call is established between User A and User C.



Step	Action	Description
F1	INVITE—User A to Proxy Server	<p>User A sends the INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> • The IP address of User B is inserted in the Request-URI field. • User A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User A is ready to receive is specified. • The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	180 Ringing—User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	302 Move Temporarily—User B to Proxy Server	User B sends a SIP 302 Moved Temporarily message to the proxy server. The message indicates that User B is not available at SIP phone B. User B rewrites the contact-URI.
F6	ACK—Proxy Server to User B	The proxy server sends a SIP ACK to User B, the ACK message notifies User B that the proxy server has received the

Step	Action	Description
		ACK message.
F7	302 Move Temporarily—Proxy Server to User A	The proxy server forwards the 302 Moved Temporarily message to User A.
F8	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK message notifies the proxy server that User A has received the ACK message.
F9	INVITE—User A to Proxy Server	User A sends a SIP INVITE request to the proxy server. In the INVITE request, a unique Call-ID is generated and the Contact-URI field indicates that User A requests the call.
F10	INVITE—Proxy Server to User C	The proxy server forwards the SIP INVITE request to User C.
F11	180 Ringing—User C to Proxy Server	User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F12	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User C is being alerted.
F13	200OK—User C to Proxy Server	User C sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F14	200OK—Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A.
F15	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F16	ACK—Proxy Server to User C	The proxy server sends the ACK message to User C.

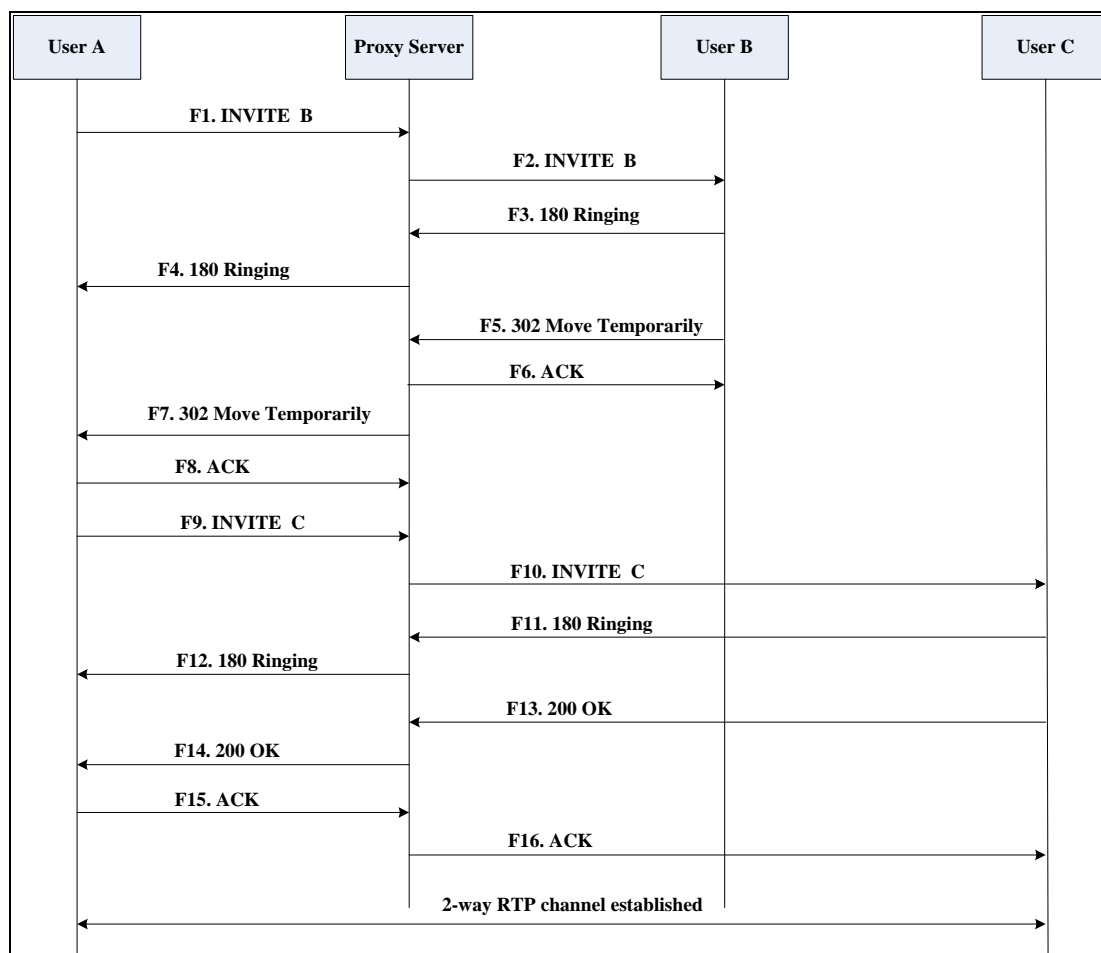
No Answer Call Forward

The following figure illustrates successful call forwarding between Yealink SIP IP phones in which User B has enabled no answer call forward. The incoming call is forwarded to User C when User B does not answer the incoming call after a period of time. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User B enables no answer call forward, and the destination number is User C.
2. User A calls User B.
3. User B does not answer the incoming call.
4. User B forwards the incoming call to User C.
5. User C answers the call.

Call is established between User A and User C.



Step	Action	Description
F1	INVITE—User A to Proxy Server	<p>User A sends the INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> • The IP address of User B is inserted in the Request-URI field. • User A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User A is ready to receive is specified. • The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	180 Ringing—User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	302 Move Temporarily—User B to Proxy Server	User B sends a SIP 302 Moved Temporarily message to the proxy server. The message indicates that User B is not available at SIP phone B. User B rewrites the contact-URI.
F6	ACK—Proxy Server to User B	The proxy server sends a SIP ACK to User B, the ACK message notifies User B that the proxy server has received the

Step	Action	Description
		ACK message.
F7	302 Move Temporarily—Proxy Server to User A	The proxy server forwards the 302 Moved Temporarily message to User A.
F8	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK message notifies the proxy server that User A has received the ACK message.
F9	INVITE—User A to Proxy Server	User A sends a SIP INVITE request to the proxy server. In the INVITE request, a unique Call-ID is generated and the Contact-URI field indicates that User A requests the call.
F10	INVITE—Proxy Server to User C	The proxy server forwards the SIP INVITE request to User C.
F11	180 Ringing—User C to Proxy Server	User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F12	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User C is being alerted.
F13	200OK—User C to Proxy Server	User C sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F14	200OK—Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A. The 200 OK response notifies User A that the connection has been made.
F15	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F16	ACK—Proxy Server to User C	The proxy server sends the ACK message to User C. The ACK confirms that the proxy server has received the 200 OK response.

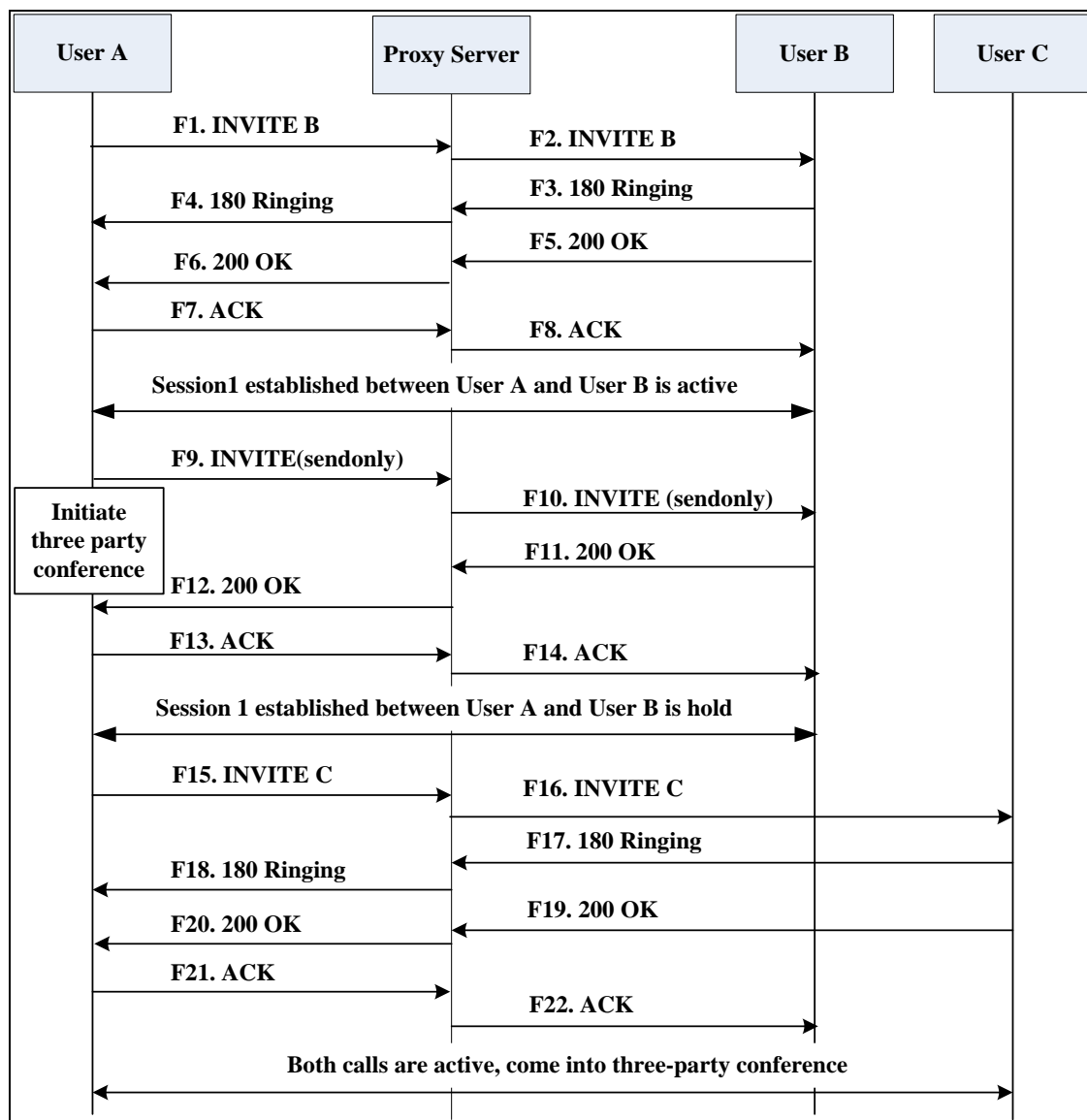
Call Conference

The following figure illustrates successful 3-way calling between Yealink SIP-T4X IP phones in which User A mixes two RTP channels and therefore establishes a conference between User B and User C. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.
3. User A puts User B on hold.
4. User A calls User C.
5. User C answers the call.

6. User A mixes the RTP channels and establishes a conference between User B and User C.



Step	Action	Description
F1	INVITE—User A to Proxy Server	<p>User A sends the INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> • The IP address of User B is inserted in the Request-URI field. • User A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User A is ready to receive is specified. • The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. Proxy server forwards the INVITE message to User B.
F3	180 Ringing—User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F6	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the connection has been made.

Step	Action	Description
F7	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F8	ACK—Proxy Server to User B	The proxy server sends the SIP ACK to User B. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.
F9	INVITE—User A to Proxy Server	User A sends a mid-call INVITE request to the proxy server with new SDP session parameters, which are used to place the call on hold.
F10	INVITE—Proxy Server to User B	The proxy server forwards the mid-call INVITE message to User B.
F11	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the INVITE is successfully processed.
F12	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK response to User A. The 200 OK response notifies User A that User B is successfully put on hold.
F13	ACK—User A to Proxy Server	User A sends the ACK message to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now temporarily inactive. No RTP packets are being sent.
F14	ACK—Proxy Server to User B	The proxy server sends the ACK message to User B. The ACK confirms that the proxy server has received the 200 OK response.
F15	INVITE—User A to Proxy Server	User A sends a SIP INVITE request to the proxy server. In the INVITE request, a unique Call-ID is generated and the Contact-URI field indicates that User A requests the call.
F16	INVITE—Proxy Server to User	The proxy server maps the SIP URI in the To field to User C. The proxy server

Step	Action	Description
	C	sends the SIP INVITE request to User C.
F17	180 Ringing—User C to Proxy Server	User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F18	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User C is being alerted.
F19	200OK—User C to Proxy Server	User C sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F20	200OK—Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A. The 200 OK response notifies User A that the connection has been made.
F21	ACK— User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F22	ACK—Proxy Server to User C	The proxy server sends the ACK message to User C. The ACK confirms that the proxy server has received the 200 OK response.

Appendix F: Sample Configuration File

This section provides the sample configuration file necessary to configure the IP phone. Any line beginning with a pound sign (#) is considered to be a comment, unless the # is contained within double quotes. For Boolean fields, 0 = disabled, 1 = enabled.

This file contains sample configurations for the <y0000000000xx>.cfg or <MAC>.cfg file. The parameters included here are examples only. Not all possible parameters are shown in the sample configuration file. You can configure or comment the values as required. The settings in the <y0000000000xx>.cfg file will be overridden by settings in the <MAC>.cfg file.

T4X Sample Configuration File

```
#!version:1.0.0.1
```

```
#!Note: This file header cannot be edited or deleted.
```

#Network Settings

```
network.internet_port.type =
```

```
#!Configure the WAN port type; 0-DHCP, 1-PPPoE, 2-Static IP Address.
```

```
#!If the WAN port type is configured as DHCP, you do not need to set the following network parameters.
```

```
#!If the WAN port type is configured as Static IP Address, configure the following parameters.
```

```
network.internet_port.ip =
```

```
network.internet_port.mask =
```

```
network.internet_port.gateway =
```

```
network.primary_dns=
```

```
network.secondary_dns =
```

```
#!If the WAN port type is configured as PPPoE, configure the following parameters. It is only applicable to SIP-T46G IP phone.
```

```
network.pppoe.user =
```

```
network.pppoe.password =
```

#Dial Plan Settings

```
dialplan.area_code.code =
```

```
dialplan.area_code.min_len =
```

```
dialplan.area_code.max_len =
```

```
dialplan.area_code.line_id =
```

```
dialplan.block_out.number.1 =
```

```
dialplan.block_out.line_id.1 =
```

```
dialplan.dialnow.rule.1 =
```

```
dialplan.dialnow.line_id.1 =
```

dialplan.replace.prefix.1 =
dialplan.replace.replace.1 =
dialplan.replace.line_id.1 =

#Time Settings

local_time.time_zone =
local_time.time_zone_name =
local_time.ntp_server1 =
local_time.ntp_server2 =
local_time.interval =
local_time.dhcp_time =

#Use the following parameters to set the time and date manually.

local_time.manual_time_enable =
local_time.date_format =
local_time.time_format =

#Auto DST Settings

local_time.summer_time =
local_time.dst_time_type =
local_time.start_time =
local_time.end_time =
local_time.offset_time =

#Phone Lock

phone_setting.lock =
phone_setting.phone_lock.lock_key_type =
phone_setting.phone_lock.unlock_pin =
phone_setting.phone_lock.lock_time_out =

#Language

lang.wui =
lang.gui =

#Call Waiting

call_waiting.enable =
call_waiting.tone =

#Auto Redial

auto_redial.enable =
auto_redial.interval =
auto_redial.times =

#Call Hold

features.play_hold_tone.enable =

```
features.play_hold_tone.delay =  
sip.rfc2543_hold =
```

#Hotline

```
features.hotline_number =  
features.hotline_delay =
```

#Web Server Type

```
wui.http_enable =  
network.port.http =  
wui.https_enable =  
network.port.https =
```

#DTMF Suppression

```
features.dtmf.hide =  
features.dtmf.hide_delay =
```

#Call Forward

In Phone Mode

```
features.fwd_mode = 0  
forward.always.enable =  
forward.always.target =  
forward.always.on_code =  
forward.always.off_code =  
forward.busy.enable =  
forward.busy.target =  
forward.busy.on_code =  
forward.busy.off_code =  
forward.no_answer.enable =  
forward.no_answer.target =  
forward.no_answer.timeout =  
forward.no_answer.on_code =  
forward.no_answer.off_code =
```

In Custom Mode

```
features.fwd_mode = 1  
account.1.always_fwd.enable =  
account.1.always_fwd.target =  
account.1.always_fwd.on_code =  
account.1.busy_fwd.off_code =  
account.1.busy_fwd.enable =  
account.1.busy_fwd.target =  
account.1.busy_fwd.on_code =  
account.1.busy_fwd.off_code =
```

account.1.timeout_fwd.enable =
account.1.timeout_fwd.target =
account.1.timeout_fwd.timeout =
account.1.timeout_fwd.on_code =
account.1.timeout_fwd.off_code =

#Call Transfer

transfer.semi_attend_tran_enable =
transfer.blind_tran_on_hook_enable =
transfer.on_hook_trans_enable =
transfer.tran_others_after_conf_enable =

#Call Conference

account.1.conf_type =
account.1.conf_uri =

#DTMF

account.1.dtmf.type =
account.1.dtmf.dtmf_payload =
account.1.dtmf.info_type =

#Distinctive Ring Tones

account.1.alert_info_url_enable =
distinctive_ring_tones.alert_info.1.text =
distinctive_ring_tones.alert_info.1.ringer =

#Tones

voice.tone.dial =
voice.tone.ring =
voice.tone.busy =
voice.tone.congestion =
voice.tone.callwaiting =
voice.tone.dialrecall =
voice.tone.record =
voice.tone.info =
voice.tone.stutter =
voice.tone.message =
voice.tone.autoanswer =

#Remote Phone Book

features.remote_phonebook.enable =
features.remote_phonebook.flash_time =

#LDAP

```
ldap.enable =  
ldap.name_filter =  
ldap.number_filter =  
ldap.host =  
ldap.port =  
ldap.base =  
ldap.user =  
ldap.password =  
ldap.max_hits =  
ldap.name_attr =  
ldap.numb_attr =  
ldap.display_name =  
ldap.version =  
ldap.call_in_lookup =  
ldap.ldap_sort =
```

#Action URL

```
action_url.setup_completed =  
action_url.registered =  
action_url.unregistered =  
action_url.register_failed =  
action_url.off_hook =  
action_url.on_hook =  
action_url.incoming_call =  
action_url.outgoing_call =  
action_url.call_established =  
action_url.dnd_on =  
action_url.dnd_off =  
action_url.always_fwd_on =  
action_url.always_fwd_off =  
action_url.busy_fwd_on =  
action_url.busy_fwd_off =  
action_url.no_answer_fwd_on =  
action_url.no_answer_fwd_off =  
action_url.transfer_call =  
action_url.blind_transfer_call =  
action_url.attended_transfer_call =  
action_url.hold =  
action_url.unhold =  
action_url.mute =  
action_url.unmute =  
action_url.missed_call =  
action_url.call_terminated =
```

action_url.busy_to_idle =
action_url.idle_to_busy =
action_url.ip_change =
action_url.forward_incoming_call =
action_url.reject_incoming_call =
action_url.answer_new_incoming_call =
action_url.transfer_finished =
action_url.transfer_failed =

#Access URL of Resource Files

dialplan_dialnow.url =
dialplan_replace_rule.url =
local_contact.data.url =
remote_phonebook.data.1.url =
directory_setting.url =
super_search.url =
wallpaper_upload.url =

Index

Numeric

- 180 Ring Workaround [86](#)
- 802.1x Authentication [180](#)

A

- About This Guide [v](#)
- Acoustic Echo Cancellation [197](#)
- Action URL [156](#)
- Action URI [159](#)
- Administrator Password [43](#)
- Always Forward [92](#)
- Analyzing the Configuration Files [235](#)
- Anonymous Call [75](#)
- Anonymous Call Rejection [77](#)
- Appendix [243](#)
- Appendix A: Glossary [243](#)
- Appendix B: Time Zones [245](#)
- Appendix C: Configuration Parameters [248](#)
- Appendix D: SIP [396](#)
- Appendix E: SIP Call Flows [404](#)
- Appendix F: Sample Configuration File [443](#)
- Area Code [32](#)
- Attach the Stand [10](#)
- Attended Transfer [98](#)
- Audio Codecs [193](#)
- Auto Answer [72](#)
- Auto Redial [70](#)
- Automatic Call Distribution [142](#)

B

- Backlight [41](#)
- Blind Transfer [98](#)
- Block Out [33](#)
- Busy Forward [92](#)
- Busy Lamp Field [136](#)
- Busy Tone Delay [83](#)

C

- Call Completion [74](#)
- Call Forward [92](#)
- Call Hold [90](#)
- Call Log [63](#)
- Call Park [111](#)
- Call Recording [151](#)
- Call Return [110](#)
- Call Transfer [98](#)
- Call Waiting [68](#)
- Call Waiting Tone [68](#)
- Calling Line Identification Presentation [114](#)
- Connected Line Identification Presentation [114](#)
- Capturing Packets [234](#)
- Comfort Noise Generation [199](#)
- Configuration Files [15](#)
- Configuration Methods [14](#)
- Configuring Advanced features [125](#)
- Configuring Basic Features [35](#)
- Configuring Basic Network Parameters [18](#)
- Connect the Network and Power [11](#)
- Connecting the IP phone [9](#)
- Creating Dial Plan [28](#)

D

- Dial-now [30](#)
- Dial-now Template [220](#)
- Directed Call Pickup [102](#)
- Distinctive Ring Tones [125](#)
- Do Not Disturb (DND) [79](#)
- Documentations [v](#)
- DTMF [116](#)
- Dual Headset [192](#)

E

- Early Media [85](#)
- Encrypting Configuration Files [211](#)
- Enabling the Watch Dog Feature [234](#)

G

- Getting Information from Status Indicators [235](#)
- Getting Started [9](#)
- Group Call Pickup [105](#)

H

- H.323 [1](#)
- Headset Prior [191](#)
- Hotline [61](#)
- Hot Desking [155](#)

I

- In This Guide [v](#)
- Index [449](#)
- Initialization Process Overview [12](#)
- Intercom [121](#)
- IPv6 Support [187](#)

J

- Jitter Buffer [200](#)

K

- Key as Send [59](#)
- Key Features of SIP-T4X IP Phones [4](#)

L

- Language [52](#)
- LDAP [133](#)
- Live Dialpad [68](#)
- LLDP [167](#)
- Loading Language Packs [53](#)
- Local Contact File [223](#)
- Local Directory [65](#)
- Logo Customization [55](#)

M

- Message Waiting Indicator [144](#)
- Missed Call Log [64](#)
- Multicast Paging [147](#)
- Music on Hold [141](#)

N

- NAT Traversal [178](#)
- Network Address Translation (NAT) [178](#)
- Network Conference [100](#)
- No Answer Forward [92](#)

P

- Phone Lock [44](#)
- Phone User Interface [14](#)
- Physical Features of SIP-T4X IP Phones [4](#)
- Product Overview [1](#)

Q

- Quality of Service [176](#)

R

- Reading Icons [16](#)
- Remote Phone Book [131](#)
- Remote XML Phonebook [224](#)
- Replace Rule [29](#)
- Replace Rule Template [219](#)
- Return Message When DND [79](#)
- Return Code When Refuse [84](#)
- RFC and Internet Draft Support [396](#)

S

- Security Features [203](#)
- Semi-attended Transfer [98](#)
- Server Redundancy [162](#)
- Session Timer [89](#)
- SIP [1](#)
- SIP Components [2](#)
- SIP Header [400](#)
- SIP Call Flows [404](#)
- SIP Request [399](#)
- SIP Responses [401](#)
- SIP IP Phone Models [3](#)
- SIP Session Description Protocol Usage [403](#)
- SIP Session Timer [88](#)
- Softkey Layout [55](#)
- Specifying the Language to Use [54](#)
- SRTP [209](#)

STUN Server [178](#)
Suppressing DTMF Display [119](#)

T

Table of Contents [ix](#)
Time and Date [47](#)
Transfer on Conference Hang Up [101](#)
Transfer via DTMF [120](#)
Transport Layer Security (TLS) [203](#)
Troubleshooting [231](#)
Troubleshooting Methods [231](#)
Troubleshooting Solutions [236](#)
TR-069 Device Management [185](#)

U

Upgrading Firmware [215](#)
Use Outbound Proxy in Dialog [87](#)
User Agent Client (UAC) [2](#)
User Agent Server (UAS) [3](#)
User Password [42](#)

V

Verifying Startup [14](#)
Viewing Log Files [231](#)
VLAN [170](#)
Voice Activity Detection [198](#)
VoIP Principle [1](#)
VPN [174](#)

W

Wallpaper [36](#)
Web Server Type [112](#)
Web User Interface [14](#)