

# Yealink

# Yealink IP DECT Phones Administrator Guide

Version 81.15  
Aug. 2016

## Copyright

### **Copyright © 2016 YEALINK(XIAMEN) NETWORK TECHNOLOGY**

Copyright © 2016 Yealink(Xiamen) 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(Xiamen) Network Technology CO., LTD. Under the law, reproducing includes translating into another language or format.

When this publication is made available on media, Yealink(Xiamen) 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(Xiamen) 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(XIAMEN) 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(Xiamen) 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(Xiamen) Network Technology CO., LTD. declares that this phone is in conformity with the essential requirements and other relevant provisions of the CE, FCC. Statements of compliance can be obtained by contacting [support@yealink.com](mailto:support@yealink.com).

## CE Mark Warning

This device is marked with the CE mark in compliance with R&TTE Directive 1999/5/EC.

## Part 15 FCC Rules

Any Changes or modifications not expressly approved by the party responsible for compliance could void

the user's authority to operate the equipment.

This device complies 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 experience 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](mailto:DocsFeedback@yealink.com).

## GNU GPL INFORMATION

Yealink IP DECT 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 from Yealink web site:

<http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage>.



## About This Guide

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

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

## Documentations

This guide covers W56P IP DECT phones. The following related documents are available:

- Quick Start Guide, which describes how to assemble IP DECT phones and configure the most basic features available on IP DECT phones.
- User Guide, which describes the basic and advanced features available on IP DECT phones.
- Auto Provisioning Guide, which describes how to provision IP DECT phones using the configuration files.
- Description of Configuration Parameters in CFG Files, which describes all configuration parameters in configuration files.
- y00000000025.cfg and <MAC>.cfg template configuration files.
- IP DECT phones Deployment Guide for BroadSoft UC-One Environments, which describes how to configure BroadSoft features on the BroadWorks web portal and IP DECT phones.

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

## Conventions Used in Yealink Documentations

Yealink documentations contain a few typographic conventions.

You need to know the following basic typographic conventions to distinguish types of in-text information:

Convention	Description
<b>Bold</b>	Highlights the web/handset user interface items such as menus, menu selections, soft keys, or directory names when they are involved in a procedure or user action (e.g., Click on <b>Settings-&gt;Upgrade</b> ).

Convention	Description
	Also used to emphasize text (e.g., <b>Important!</b> ).
<i>Italics</i>	Used to show the format of examples (e.g., <i>http(s)://[IPv6 address]</i> ), or to show the title of a section in the reference documentations available on the Yealink Technical Support Website (e.g., <i>Triggering the IP DECT phone to Perform the Auto Provisioning</i> ).
Blue Text	Used for cross references to other sections within this documentation (e.g., refer to <a href="#">Tones</a> on page 307), for hyperlinks to non-Yealink websites (e.g., <a href="#">RFC 3315</a> ) or for hyperlinks to Yealink Technical Support website.
<i>Blue Text in Italics</i>	Used for hyperlinks to Yealink resources outside of this documentation such as the Yealink documentations (e.g., <a href="#">Yealink IP DECT Phones Description of Configuration Parameters in CFG Files_V80.xlsx</a> ).

## In This Guide

The information detailed in this guide is applicable to W56P base firmware version 80 or higher and the base firmware format is like 25.x.x.x.rom. The second x from left must be greater than or equal to 80. This administrator guide includes the following chapters:

- Chapter 1, "[Product Overview](#)" describes the base station, handset and battery.
- Chapter 2, "[Getting Started](#)" describes how to install and connect IP DECT phones, configuration methods and resource files.
- Chapter 3, "[Configuring the Handset](#)" describes how to configure the handsets.
- Chapter 4, "[Configuring Basic Features](#)" describes how to configure the basic features on IP DECT phones.
- Chapter 5, "[Configuring Advanced Features](#)" describes how to configure the advanced features on IP DECT phones.
- Chapter 6, "[Configuring Audio Features](#)" describes how to configure the audio features on IP DECT phones.
- Chapter 7, "[Configuring Security Features](#)" describes how to configure the security features on IP DECT phones.
- Chapter 8, "[Troubleshooting](#)" describes how to troubleshoot IP DECT phones and provides some common troubleshooting solutions.
- Chapter 9, "[Appendix](#)" provides the glossary, reference information about IP DECT phones compliant with [RFC 3261](#), SIP call flows and the sample configuration files.

## Summary of Changes

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

### Changes for Release 80, Guide Version 80.15

The following sections are new:

- [IPv6 Support](#) on page 49
- [Voice Quality Monitoring \(VQM\)](#) on page 331

Major updates have occurred to the following sections:

- [Product Overview](#) on page 1
- [DHCP](#) on page 32
- [Configuring Network Parameters Manually](#) on page 42
- [PPPoE](#) on page 46
- [Language](#) on page 104
- [Display Method on Dialing](#) on page 122
- [Methods of Transmitting DTMF Digit](#) on page 326



# Table of Contents

<b>About This Guide .....</b>	<b>i</b>
Documentations .....	i
Conventions Used in Yealink Documentations .....	i
In This Guide .....	ii
Summary of Changes .....	iii
Changes for Release 80, Guide Version 80.15 .....	iii
<b>Table of Contents.....</b>	<b>v</b>
<b>Product Overview .....</b>	<b>1</b>
Base Station .....	2
Handset Models.....	3
Battery Information .....	3
<b>Getting Started.....</b>	<b>5</b>
Connecting the IP DECT Phones .....	5
Connecting the Base Station .....	5
Setting up the Handset .....	7
Setting up the Charger Cradle.....	7
Charging the Handset.....	8
Registering the Handset.....	9
Initialization Process Overview .....	10
Verifying Startup.....	11
Icon Instructions .....	11
Configuration Methods .....	12
Handset User Interface.....	13
Web User Interface.....	13
Configuration Files .....	14
Obtaining Configuration Files and Resource Files .....	15
Configuration File Parameters Description .....	17
Characters Supported.....	17
Keep User Personalized Settings.....	17

Configuration Parameters.....	18
Scenario A Protect Personalized settings.....	21
Scenario B Clear Personalized Settings.....	25
Scenario C Protecting Personalized Settings after Reset.....	26
Scenario D Importing or Exporting the Local Configuration File.....	28
Provisioning Server.....	29
Supported Provisioning Protocols.....	29
Setting up the Provisioning Server.....	30
Deploying Phones from the Provisioning Server.....	30
Setting Up DECT Phone Network.....	31
DHCP.....	32
DHCP Options.....	37
Configuring Network Parameters Manually.....	42
PPPoE.....	46
IPv6 Support.....	49
Web Server Type.....	58
VLAN.....	61
VPN.....	68
Quality of Service.....	71
802.1X Authentication.....	74
Upgrading Firmware.....	83
Upgrading Firmware via Web User Interface.....	83
Upgrading Firmware from the Provisioning Server.....	85
<b>Configuring the Handset.....</b>	<b>93</b>
Handset Power Indicator LED.....	93
Keypad Light.....	95
Advisory Tone.....	97
Backlight.....	99
Wallpaper.....	101
Screen Saver.....	102
Handset Name.....	103
Language.....	104
Loading Language Packs.....	105
Specifying the Language to Use.....	108
<b>Configuring Basic Features.....</b>	<b>111</b>

---

Register Power Light Flash.....	112
Account Registration .....	113
Call Display.....	120
Display Method on Dialing .....	122
Number Assignment .....	124
Time and Date .....	129
NTP Time Server .....	130
Time and Date Settings.....	135
Daylight Saving Time .....	138
Input Method .....	145
Specifying the Default Input Method .....	145
Key As Send.....	147
Dial Plan .....	148
Replace Rule.....	149
Dial-now .....	153
Area Code .....	158
Block Out.....	160
Auto Dial.....	162
Local Directory.....	164
Customizing a Directory Template File.....	166
Search Source in Dialing .....	167
Customizing a Super Search Template File .....	167
Save Call Log .....	170
Call Waiting.....	172
Auto Answer .....	175
Allow IP Call.....	176
Accept SIP Trust Server Only.....	177
Anonymous Call .....	179
Anonymous Call Rejection .....	183
Do Not Disturb (DND) .....	186
Busy Tone Delay .....	190
Return Code When Refuse .....	192
Early Media .....	193
180 Ring Workaround.....	193
Use Outbound Proxy in Dialog .....	195
SIP Session Timer.....	197
Session Timer .....	199

Call Hold .....	201
Call Forward .....	203
Call Transfer .....	213
Network Conference.....	215
Feature Key Synchronization .....	217
Recent Call in Dialing.....	219
Call Number Filter .....	220
Calling Line Identification Presentation .....	222
Connected Line Identification Presentation .....	226
Intercom .....	228
Call Timeout .....	230
Ringing Timeout.....	231
Send user=phone .....	232
SIP Send MAC .....	234
SIP Send Line .....	235
Reserve # in User Name .....	237
Unregister When Reboot .....	239
100 Reliable Retransmission.....	240
Reboot in Talking .....	242
End Call on Hook .....	244
<b>Configuring Advanced Features.....</b>	<b>247</b>
Remote Phone Book .....	247
Lightweight Directory Access Protocol (LDAP) .....	251
Shared Call Appearance (SCA) .....	260
Message Waiting Indicator.....	262
Server Redundancy .....	266
Server Domain Name Resolution.....	277
Static DNS Cache.....	281
Network Address Translation.....	289
NAT Types.....	289
NAT Traversal.....	290
Keep Alive.....	296
Rport .....	297
Real-Time Transport Protocol .....	299
TR-069 Device Management .....	301



<b>Configuring Audio Features .....</b>	<b>307</b>
Tones .....	307
Voice Mail Tone .....	311
Audio Codecs .....	312
Acoustic Clarity Technology .....	319
Background Noise Suppression .....	319
Automatic Gain Control .....	319
Voice Activity Detection.....	319
Comfort Noise Generation.....	321
Jitter Buffer .....	323
DTMF .....	325
Methods of Transmitting DTMF Digit .....	326
Suppress DTMF Display .....	329
Voice Quality Monitoring (VQM) .....	331
RTCP-XR .....	331
VQ-RTCPXR .....	333
<b>Configuring Security Features .....</b>	<b>343</b>
User Password .....	343
Administrator Password.....	345
Auto-Logout Time .....	346
Base PIN .....	348
Emergency Number .....	349
Transport Layer Security .....	350
Secure Real-Time Transport Protocol.....	360
Encrypting Configuration Files.....	363
<b>Troubleshooting .....</b>	<b>369</b>
Troubleshooting Methods.....	369
Viewing Log Files .....	369
Capturing Packets .....	383
Enabling Watch Dog Feature .....	384
Analyzing Configuration File .....	385
Troubleshooting Solutions .....	389
Base Issue .....	389
Register Issue.....	390

Display Issue.....	391
Upgrade Issue.....	392
Time and Date Issue.....	392
Audio Issue .....	392
Phone Book Issues .....	393
Provisioning Issues .....	394
Resetting Issues.....	394
Password Issues .....	398
System Log Issue.....	399
Hardware Issue.....	399
Other Issues.....	400

**Appendix .....403**

Appendix A: Glossary .....	403
Appendix B: Time Zones .....	405
Appendix C: Trusted Certificates.....	406
Appendix D: Auto Provisioning Flowchart (Keep user personalized configuration settings).....	408
Appendix E: Configurations Defined Never be Saved to <MAC>-local.cfg file.....	409
Appendix F: SIP (Session Initiation Protocol) .....	414
RFC and Internet Draft Support .....	414
SIP Request .....	417
SIP Header.....	418
SIP Responses.....	419
SIP Session Description Protocol (SDP) Usage .....	422
Appendix G: SIP Call Flows .....	422
Successful Call Setup and Disconnect .....	423
Unsuccessful Call Setup—Called User is Busy .....	425
Unsuccessful Call Setup—Called User Does Not Answer.....	427
Successful Call Setup and Call Hold .....	429
Successful Call Setup and Call Waiting .....	432
Call Transfer without Consultation .....	437
Call Transfer with Consultation.....	441
Always Call Forward .....	446
Busy Call Forward.....	449
No Answer Call Forward.....	452
Call Conference .....	456

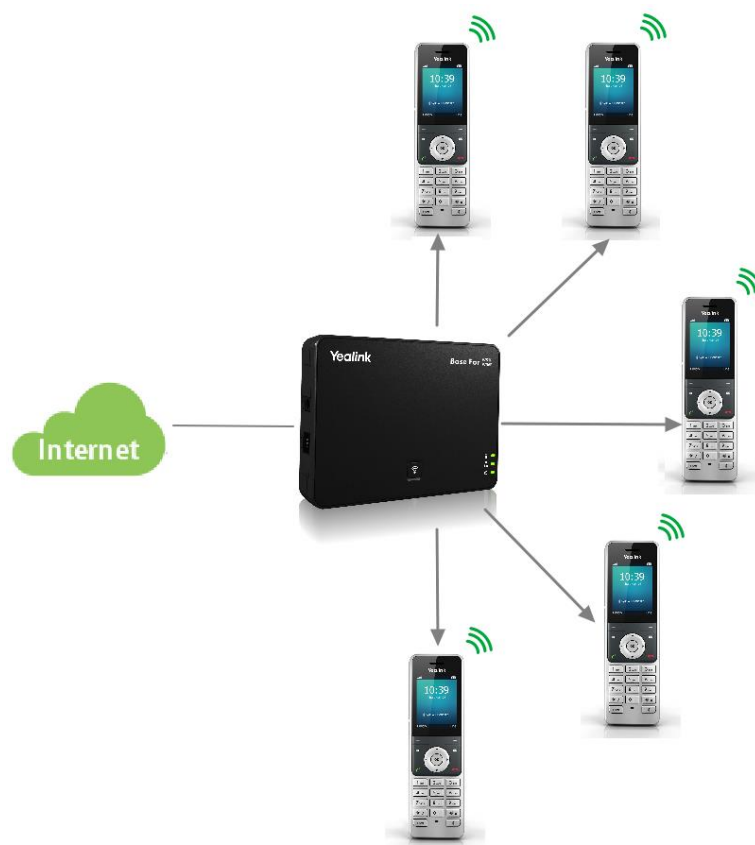
**Index.....461**



## Product Overview

Yealink IP DECT phone is a SIP Cordless Phone System designed for small business, which consists of base station and cordless handset. The Yealink W56P IP DECT phone consists of Base for W52P/W56P and W56H handsets. Yealink IP DECT phone supports the following features:

- Up to 5 Handsets for one base depending on your needs.
- Up to 4 different bases to register per handset.
- Up to 4 simultaneous external calls.
- Up to 2 simultaneous calls per handset
- Increase range with up to 6 repeaters.
- Energy-saving ECO features.



This chapter contains the following information about IP DECT phones:

- [Base Station](#)
- [Handset Models](#)

- [Battery Information](#)

## Base Station



### Physical Features:

3 LEDs on Base: 1\*power, 1\*network, 1\*handset

1\*RJ45 10/100Mbps Ethernet port

1 dedicated hard key (Paging key)

5 VoIP accounts

Indoor range: 20m~50m (The ideal distance is 50m)

Outdoor range: 300m (In ideal conditions)

Power adapter: DC 5V/600mA output

Power over Ethernet (IEEE 802.3af)

## Handset Models



2.4" 240x320 pixels color display

10 numerical keys, 6 function keys, 5 navigation keys, 2 softkeys, # key, \* key

1 earphone jack (3.5 mm)

14 key backlight

Energy-saving ECO mode/ECO Mode+

Power adapter: DC 5V/600mA output

## Battery Information

**Applicable Standards:** GB/T 18287—2013/GB 31241-2014

**Voltage:** 3.7V

**Capacity:** 1460mAh

**Maximum charging voltage:** 4.2V

**Charge Temperature:** 0~45°C

**Charging time:** approximately 3.5~4 hours (fully discharged to full capacity).

**Standby time:** up to 400 hours when the backlight is disabled.

**Talk time:** up to 30 hours active talk time (with full charged batteries).

### Note

Due to their construction, undergo some wear and tear. The lifetime of battery also depends on correct maintenance. Charging and discharging are the most important factors.





# Getting Started

---

This chapter provides basic information and installation instructions of IP DECT phones.

This chapter provides the following sections:

- [Connecting the IP DECT Phones](#)
- [Initialization Process Overview](#)
- [Verifying Startup](#)
- [Icon Instructions](#)
- [Configuration Methods](#)
- [Obtaining Configuration Files and Resource Files](#)
- [Keep User Personalized Settings](#)
- [Provisioning Server](#)
- [Setting Up DECT Phone Network](#)
- [Upgrading Firmware](#)

## Connecting the IP DECT Phones

### Connecting the Base Station

You have two options for power and network connection of the base station. Your system administrator will advise you which one to use.

- AC power (Optional)
- Power over Ethernet (PoE)

**Note**

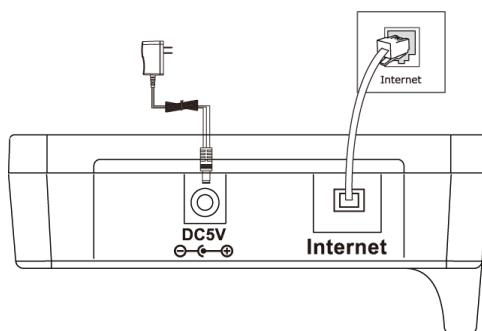
Please pay attention to the radio coverage of the base station. It is up to 300m in unobstructed outdoor areas and up to 50m inside buildings.

Set up the base station and the charger cradle at a central location on a flat, non-slip surface in your house or apartment.

## AC Power (Optional)

### To connect the AC power:

1. Connect the DC plug on the power adapter to the DC5V port on the base station and connect the other end of the power adapter into an electrical power outlet.
2. Connect the supplied Ethernet cable between the Internet port on the base station and the Internet port in your network or the switch/hub device port.



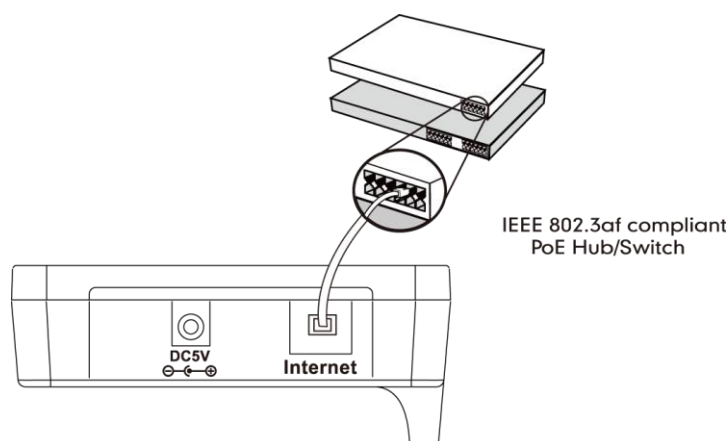
**Note** The base station should be used with original power adapter (5V/600mA) only. The use of the third-party power adapter may cause the damage to the phone.

## Power over Ethernet

Using a regular Ethernet cable, the base station can be powered from a PoE-compliant (IEEE 802.3af) switch or hub.

### To connect the PoE:

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



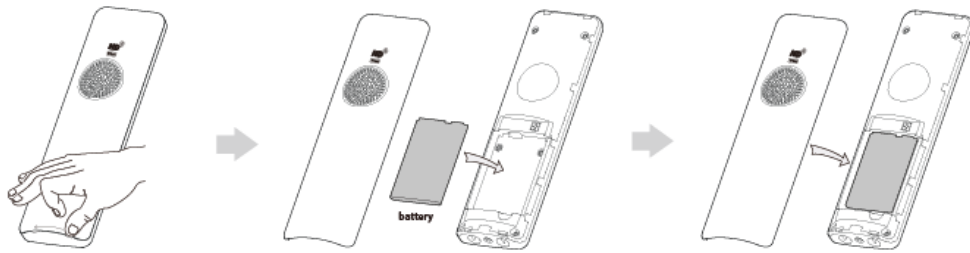
**Note** If in-line power is provided, you don't need to connect the AC adapter. Make sure the switch/hub is PoE compliant.

**Important!** Do not remove the power and network to the base station while it is updating firmware and configurations.

## Setting up the Handset

To insert battery into the handset:

1. Open the battery cover.
2. Insert the battery and press it down.
3. Close the battery cover.



### Note

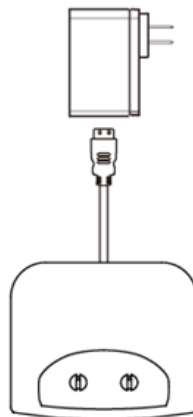
Do not short-circuit the battery, as short-circuiting the terminals may damage the battery or the handset.

Do not use a damaged battery, as this may cause an explosion.

Before replacing the battery, please turn off the handset to prevent memory loss.

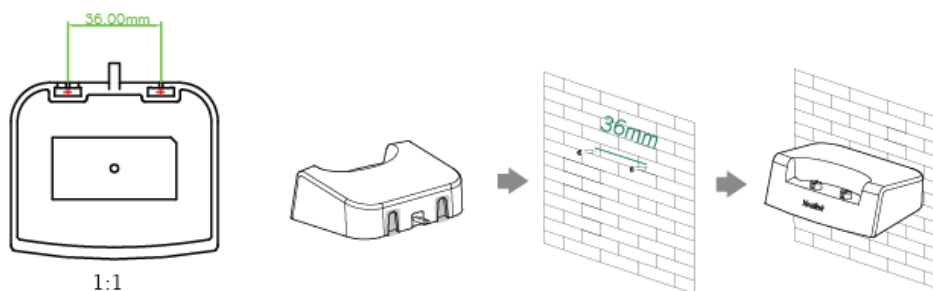
## Setting up the Charger Cradle

1. Connect the USB plug on the charger cradle to the DC5V port on the power adapter.
2. Connect the power adapter into an electrical power outlet.



You can also mount the charger cradle on the wall, as shown below:

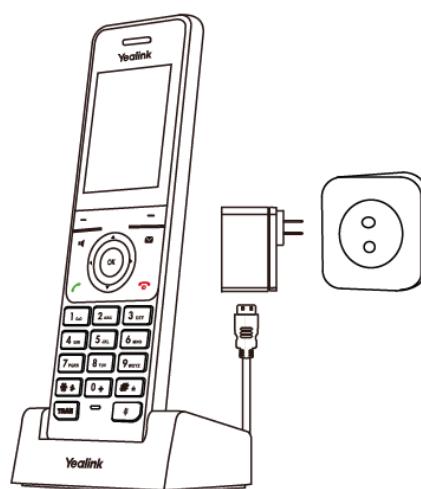
1. Drive the screws into the wall using the wall template as shown below.
2. Mount the charge cradle securely on the screws.



## Charging the Handset

**To charge the handset:**

1. After setting up the handset and charger cradle, place the handset in the charger cradle.








### Note

The handset should be used with original power adapter (5V/600mA) only. The use of third-party power adapter may cause the damage to the phone.

## Battery Charging Status



Charging status of battery is displayed on the top right-hand corner of the LCD screen:

For W56H	
	--Fully Charged
	--80% Charged
	--60% Charged
	--40% Charged
	--20% Charged

## Registering the Handset

You can register up to 5 handsets to one base station. Each handset can be registered to 4 different base stations.

**To register a handset manually:**

- Do one of the following:
  - Long press  on the base station till the Registration LED slow flashes.  
Press **OK->Settings->Registration->Register Handset**.
  - If the handset LCD screen prompts "Press base page 2s then press OK", long press  on the base station till the registration LED slow flashes.  
Press the **OK** soft key on the handset, select **Registration->Register Handset**.

The LCD screen displays the Base1 to Base4.
- Press **▲** or **▼** to select the desired base, and then press the **OK** soft key on the handset to enter the main menu.  
The handset begins to search for the base station.
- Press the **OK** soft key when the LCD screen displays the RFPI code of the base station.
- Enter the system PIN (default: 0000), and then press the **Done** soft key.  
The handset LCD screen prompts "Handset Subscribed", which indicates the handset is registered successfully.

You can also enable the registration mode of the base station via web user interface at the path **Status->Handset&VoIP->Register New Handsets**.

After initializing data successfully, an icon with internal handset number and handset name appears on the LCD screen.

## Initialization Process Overview

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

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

During the initialization process, the following events take place:

### **Loading the ROM file**

The ROM file resides in the flash memory of the IP DECT phone. The IP DECT phone comes from the factory with a ROM file preloaded. During initialization, the IP DECT phone runs a bootstrap loader that loads and executes the ROM file.

### **Configuring the VLAN**

If the IP DECT phone is connected to a switch, the switch notifies the IP DECT phone of the VLAN information defined on the switch (if using LLDP). The IP DECT phone can then proceed with the DHCP request for its network settings (if using DHCP).

### **Querying the DHCP (Dynamic Host Configuration Protocol) Server**

The IP DECT phone is capable of querying a DHCP server. DHCP is enabled on the IP DECT phone 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 network parameters of the IP DECT phone 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 42.

### **Contacting the provisioning server**

If the IP DECT phone is configured to obtain configurations from the provisioning server, it will connect to the provisioning server and download the configuration file(s) during startup. The IP DECT phone will be able to resolve and update configurations written in the configuration file(s). If the IP DECT phone does not obtain configurations from the provisioning server, the IP DECT phone will use configurations stored in the flash memory.

### **Updating firmware**

If the access URL of firmware is defined in the configuration file, the IP DECT phone will download 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 DECT phone will perform a firmware update.

### Downloading these source files

In addition to configuration file(s), the IP DECT phone 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
- Contact files

## Verifying Startup

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

1. After connected to the power, the power indicator LED illuminates solid green.
2. After connected to the available network, the network indicator LED illuminates solid green.
3. After at least one handset registered to the base station, the registration LED illuminates solid green.




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





















You can view the system status on your handset. Available information of the system status includes:

- **Base station status** (e.g., IP address, firmware version, MAC address and device certificate status of the base station and RFPI)
- **Handset status** (e.g., handset model, hardware version, firmware version of the handset, IPUI code and area)
- **Line status**

## Icon Instructions

Icons appearing on the LCD screen are described in the following table:

W56H	Description
	Registered handset icon (e.g., "1" is internal handset number, indicate the handset is register to NO.1)
	Earpiece Mode On
	Headset Mode On

W56H	Description
	Speakerphone Mode On
	Keypad Lock
	Voice Mail
	Silence Mode On
	Contact icon
	Received Calls
	Placed Calls
	Call Forward
	Missed Calls
	Call Hold
	Call Mute
	Conference Call
	Do Not Disturb
	Unassigned outgoing line
	Intercom Call
	Shared line is idle.
	Shared line is dialing, in conversation or placed on private hold.
 (flash)	Shared line receives an incoming call or is placed on public hold.
	Anonymous call enabled
	Anonymous rejection enabled

## Configuration Methods

Yealink IP DECT phones can be configured automatically through configuration files stored on a central provisioning server, manually via handset user interface or web user interface, or by a combination of the automatic and manual methods.

The recommended method for configuring IP DECT phones is automatically through a central provisioning server. If a central provisioning server is not available, the manual method will allow changes to most features.

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

- [Handset User Interface](#)
- [Web User Interface](#)



- Configuration Files

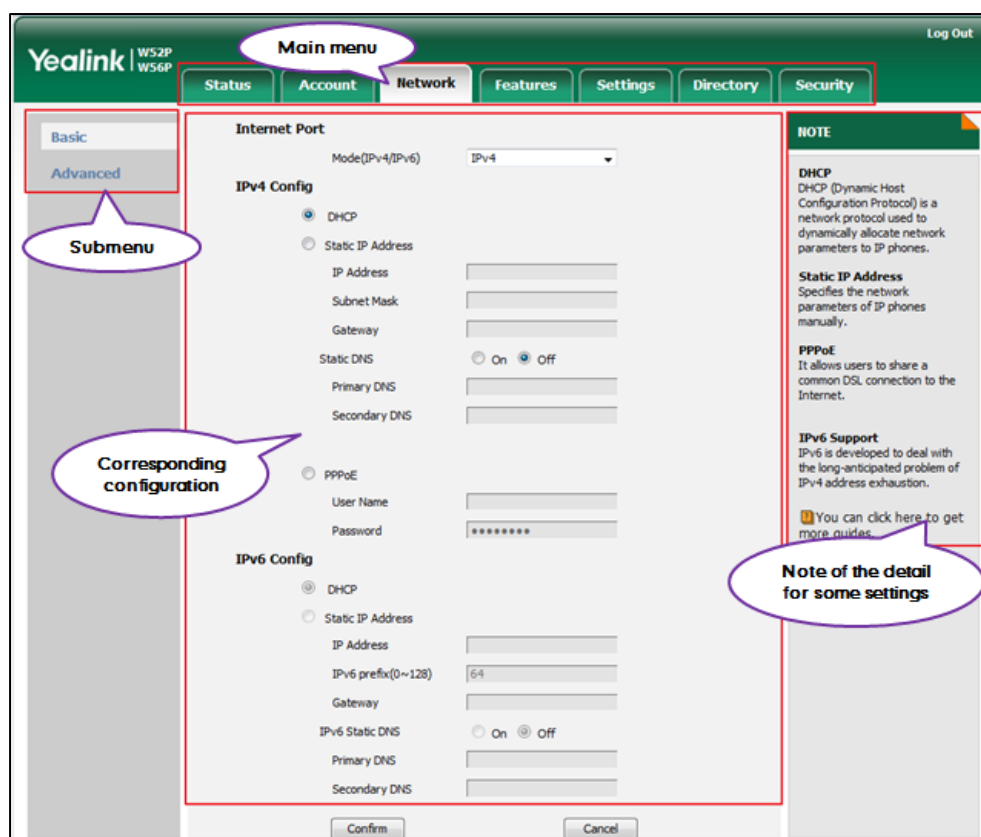
## Handset User Interface

An administrator or a user can configure and use IP DECT phones via handset user interface. Not all features are available on handset user interface. You can only access some features when the handset disconnecting with the base station.

## Web User Interface

An administrator or a user can configure IP DECT phones via web user interface from a PC connected to the same network. The default user name and password for the administrator to log into the web user interface are both “admin” (case-sensitive). Most features are available for configuring via web user interface. Yealink IP DECT phones support both HTTP and HTTPS protocols for accessing the web user interface. For more information, refer to [Web Server Type](#) on page 58.

The following web user interface takes **Network->Basic** as an example:



## Configuration Files

An administrator can deploy and maintain a mass of IP DECT phones using configuration files. The configuration files consist of:

- Common CFG file
- MAC-Oriented CFG file
- MAC-local CFG file

### Common CFG file

A Common CFG file contains parameters that affect the basic operation of the IP DECT phone, such as language and contacts. It will be effectual for all IP DECT phones. The common CFG file has a fixed name for IP DECT phone. The name is "y000000000025.cfg".

### MAC-Oriented CFG file

A MAC-Oriented CFG file contains parameters unique to a particular phone. It will only be effectual for a specific IP DECT phone. The MAC-Oriented CFG file is named after the MAC address of the base station. For example, if the MAC address of a base station is 0015655f9d7e, the name of the MAC-Oriented CFG file must be 0015655f9d7e.cfg (case-sensitive).

### MAC-local CFG file

A MAC-local CFG file contains changes that users make via web user interface and handset user interface. It will only be effectual for a specific IP DECT phone. The MAC-local CFG file is named after the MAC address of the base station. This file is stored locally on the base station and can also be uploaded to the provisioning server.

Most configurations made by users via web user interface and handset user interface can be saved to the <MAC>-local.cfg file, but some configurations listed as below are defined never to be saved to the <MAC>-local.cfg file.

- The following specified configurations.

```
#Configure always forward feature for account X. (X stands for the serial number  
of account)
```

```
account.X.always_fwd.enable =
```

```
account.X.always_fwd.target =
```

```
account.X.always_fwd.off_code =
```

```
account.X.always_fwd.on_code =
```

```
#Configure busy forward feature.
```

```
account.X.busy_fwd.enable =
```

```
account.X.busy_fwd.target =
```

```
account.X.busy_fwd.off_code =
```

```

account.X.busy_fwd.on_code =
#Configure no answer forward feature.
account.X.timeout_fwd.enable =
account.X.timeout_fwd.target =
account.X.timeout_fwd.timeout =
account.X.timeout_fwd.off_code =
account.X.timeout_fwd.on_code =
#Configure DND feature for account X. (X stands for the serial number of account).
account.X.dnd.enable
account.X.dnd.on_code
account.X.dnd.off_code

```

The MAC-local CFG file enables the DECT phone to keep user personalized settings. For more information on how to keep user personalized settings, refer to [Keep User Personalized Settings](#) on page 17.

#### Note

The <MAC>-local.cfg file only saves configurations of the base station configured via the handset or web user interface. Configurations of the handset cannot be saved to the <MAC>-local.cfg file.

## Central Provisioning

IP DECT phones can be centrally provisioned from a provisioning server using the configuration files (y00000000025.cfg and <MAC>.cfg). You can use a text-based editing application to edit configuration files, and then store configuration files to a provisioning server. For more information on the provisioning server, refer to [Provisioning Server](#) on page 29.

IP DECT phones can obtain the provisioning server address during startup. Then IP DECT phones download configuration files from the provisioning server, resolve and update the configurations written in configuration files. This entire process is called auto provisioning. For more information on auto provisioning, refer to [Yealink\\_SIP-T2 Series\\_T19\(P\) E2\\_T4 Series\\_CP860\\_W56P\\_IP\\_Phones\\_Auto\\_Provisioning\\_Guide](#).

## Obtaining Configuration Files and Resource Files

When configuring particular features, you may need to upload resource files (e.g., local contact directory, remote phonebook) to IP DECT phones. If the resource file is to be used for all IP DECT phones, the resource file access URL is best specified in the y00000000025.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.

The names of the Yealink-supplied template files are:

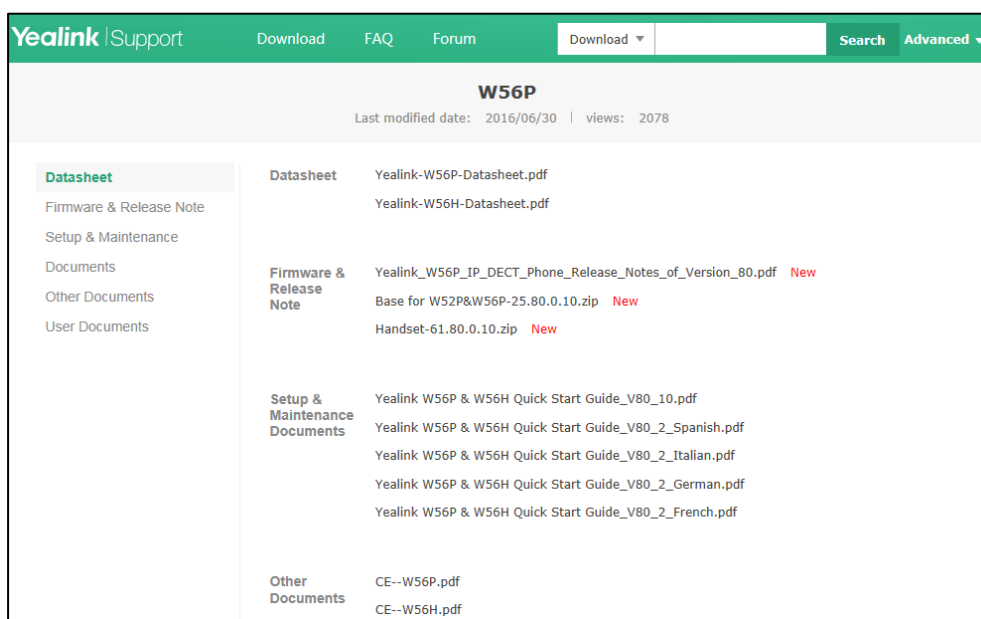
Template File		File Name
Configuration Files	Common CFG file	Common.cfg
	MAC-Oriented CFG file	MAC.cfg
Resource Files	Auto DST Template	AutoDST.xml
	Language Packs	For example: 1.English.js
	Replace Rule Template	dialplan.xml
	Dial-now Template	Dialnow.xml
	Local Contact File	ContactData.xml
	Super Search Template	super_search.xml
	Remote Phone Book Template	remote_phonebook_list.xml
	Blacklist Template	blacklist.xml

You can ask the distributor or Yealink FAE for template files. You can also obtain the template files online:

<http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage>.

**To download template files:**

1. Go to Yealink [Document Download](#) Page and select the desired phone model.



2. Download and extract the combined configuration files to your local system.
3. Open the folder you extracted and identify the template file you will edit according

to the table introduced above.

## Configuration File Parameters Description

You need to know the following basic information of parameter description that shown below. The information includes parameter name, permitted value, default value, description, handset user interface and web user interface.

**Parameters:** system predefined parameter in the configuration file and that cannot be changed.

**Permitted Value:** indicates the permitted value and value format for the corresponding parameter.

**Default:** indicates the factory default value of the parameter.

**Handset user interface:** specify the reference path for the corresponding parameter in the handset user interface.

**Web User Interface:** specify the reference path for the corresponding parameter in the web user interface.

## Characters Supported

For some features, you can customize the filename as required. The following table lists the special characters supported by Yealink IP DECT phones:

Platform \ Server	HTTP/HTTPS	TFTP/FTP
Windows	<p><b>Support:</b> ~`!@\$^()_.,;[]{} (including space)</p> <p><b>Not Support:</b>  &lt;&gt;:"^*?#%&amp;=+</p>	<p><b>Support:</b> ~`!@\$^()_.,;[]{}%&amp;=+ (including space)</p> <p><b>Not Support:</b>  &lt;&gt;:"^*?#</p>
Linux	<p><b>Support:</b> ~`!@\$^()_.,;[]{} &lt;&gt;:" (including space)</p> <p><b>Not Support:</b> ^*?#%&amp;=+</p>	<p><b>Support:</b> ~`!@\$^()_.,;[]{} &lt;&gt;:"%&amp;=+ (including space)</p> <p><b>Not Support:</b> ^*?#</p>

## Keep User Personalized Settings

Generally, the administrator deploys IP DECT phones in batch via auto provisioning, yet

some users would like to keep the personalized settings (e.g., ring tone, dial plan and handset name) after auto provisioning. The IP DECT phones running firmware version 73 or later can be configured to protect personalized settings after auto provisioning.

The MAC-local CFG file enables the DECT phone to keep user personalized settings. For more information, refer to [MAC-local CFG file](#) on page 14.

Several specific scenarios are illustrated in the following sections to assist in explaining the personalized settings protecting process.

**Note**

Yealink IP DECT phones support FTP, TFTP, HTTP and HTTPS protocols for uploading the MAC-local CFG file. This section takes the TFTP protocol as an example. Before performing the following, make sure that the provisioning server supports uploading.

If you are using the HTTP(S) server, you can specify the way the IP DECT phone uploads the MAC-local CFG file to the provisioning server. It is determined by the value of the parameter "auto\_provision.custom.upload\_method". For more information, refer to [Configuration Parameters](#) on page 18.

## Configuration Parameters

The following table lists the configuration parameters used to determine the DECT phone behavior for protecting personalized settings:

Parameters	Permitted Values	Default
<b>auto_provision.custom.protect</b>	<b>0 or 1</b>	<b>0</b>
<p><b>Description:</b>                      Enables or disables the IP DECT phone to protect personalized settings after auto provisioning.</p> <p><b>0-Disabled</b>  <b>1-Enabled</b></p> <p>If it is set to 1 (Enabled), personalized settings of the base station configured via the handset or web user interface and the handset settings configured via the handset will be remained after auto provisioning.</p> <p><b>Web User Interface:</b>                      None</p> <p><b>Handset User Interface:</b>                      None</p>		
<b>auto_provision.custom.sync</b>	<b>0 or 1</b>	<b>0</b>
<p><b>Description:</b>                      Enables or disables the IP DECT phone to periodically (every 5 minutes) upload the</p>		

Parameters	Permitted Values	Default
<p>&lt;MAC&gt;-local.cfg file to the provisioning server, and download the &lt;MAC&gt;-local.cfg file from the provisioning server during auto provisioning.</p> <p><b>0</b>-Disabled</p> <p><b>1</b>-Enabled</p> <p>If it is set to 1 (Enabled), the IP DECT phone will periodically upload the &lt;MAC&gt;-local.cfg file to the provisioning server to back up this file. During auto provisioning, the IP DECT phone will download the &lt;MAC&gt;-local.cfg file from the provisioning server to override the one stored on the phone.</p> <p>If it is set to 0 (Disabled), the IP DECT phone will not upload the &lt;MAC&gt;-local.cfg file to the provisioning server. During auto provisioning, the IP DECT phone will not download the &lt;MAC&gt;-local.cfg file from the provisioning server.</p> <p><b>Web User Interface:</b></p> <p>None</p> <p><b>Handset User Interface:</b></p> <p>None</p>		
<b>auto_provision.custom.upload_method</b>	<b>0 or 1</b>	<b>0</b>
<p><b>Description:</b></p> <p>Configures the way the IP DECT phone uploads the &lt;MAC&gt;-local.cfg file to the provisioning server (for HTTP/HTTPS server only).</p> <p><b>0</b>-PUT</p> <p><b>1</b>-POST</p> <p><b>Note:</b> It works only if the value of the parameter "auto_provision.custom.sync" is set to 1 (Enabled).</p> <p><b>Web User Interface:</b></p> <p>None</p> <p><b>Handset User Interface:</b></p> <p>None</p>		
<b>auto_provision.handset_configured.enable</b>	<b>0 or 1</b>	<b>1</b>
<p><b>Description:</b></p> <p>Enables or disables the base station to deliver handset settings via auto provisioning to the registered handset or after the handset registering to the base station successfully.</p> <p><b>0</b>-Disabled</p> <p><b>1</b>-Enabled</p>		

Parameters	Permitted Values	Default
<p>If it is set to 0 (Disabled), the base station will not deliver handset configurations via auto provisioning to the handset. The handset settings can be only changed via the handset.</p> <p>If it is set to 1 (Enabled), the base station will deliver the handset configurations via auto provisioning to the handset. Handset reboot or registration will also trigger the base station to deliver the stored handset settings to the handset. If the parameter "auto_provision.custom.protect" is also set to 0 (Disabled), the personalized handset settings will be overridden, and other handset settings will be changed. If the parameter "auto_provision.custom.protect" is set to 1 (Enabled), the personalized handset settings will not be overridden, but other handset settings will be changed.</p> <p><b>Web User Interface:</b> None</p> <p><b>Handset User Interface:</b> None</p>		

For more information on how to configure these parameters in different scenarios, refer to the following introduced scenarios.

The following lists the configuration parameters for handset settings:

<p>#Configures the language of the handset.</p>
<p>custom.handset.language</p>
<p>#Configures the time format of the handset.</p>
<p>custom.handset.time_format</p>
<p>#Configures the date format of the handset.</p>
<p>custom.handset.date_format</p>
<p>#Configures whether the W56P IP DECT phone automatically answers an incoming #internal intercom call and plays a warning tone.</p>
<p>custom.handset.auto_intercom</p>
<p>#Enables or disables screen saver feature of the handset.</p>
<p>custom.handset.screen_saver.enable</p>
<p>#Enables or disables the handset to always turn on the backlight when it is in the #charging state.</p>
<p>custom.handset.backlight_in_charger.enable</p>
<p>#Enables or disables the handset to always turn on the backlight when it is not in #the charging state.</p>
<p>custom.handset.backlight_out_of_charger.enable</p>
<p>#Enables or disables the handset to turn on the keypad light when any key is #pressed.</p>
<p>custom.handset.keypad_light.enable</p>



```

custom.handset.keypad_light.enable
#Enables or disables the handset to play a tone when any key is pressed.
custom.handset.keypad_tone.enable
#Enables or disables the handset to play a tone when a user saves settings or
#places the handset in the charger cradle.
custom.handset.confirmation_tone.enable
#Enables or disables the handset to play a tone when the capacity of the batteries
#is low.
custom.handset.low_battery_tone.enable
#Enables or disables a user to answer incoming calls by lifting the handset from
#the charger cradle without having to press the off-hook key.
custom.handset.auto_answer.enable
#Enables or disables the eco mode to greatly reduce the transmission power and
#signal output when the handset is in the talk mode.
custom.handset.eco_mode.enable
#Configures the wallpaper to display on the handset.
custom.handset.wallpaper

```

**Note** The input method of the handset can be only configured via the handset.

## Scenario A Protect Personalized settings

### Protecting Personalized Settings of the Base Station

The administrator wishes to upgrade firmware to the latest version. Meanwhile, protect personalized settings after auto provisioning and upgrade.

#### Scenario Conditions:

- The current firmware version of the base station is 25.80.0.1.
- The target firmware version: 25.80.0.10.
- The current and target firmware versions both support protecting personalized settings and generating a <MAC>-local.cfg file.
- The MAC address of the IP DECT phone is 0015655f9d7e.
- Provisioning server URL: tftp://192.168.1.211
- Place the target firmware to the root directory of the provisioning server.

To protect personalized settings after auto provisioning and upgrade, you need to configure the value of the parameter "auto\_provision.custom.protect" to 1 in the

configuration file.

**Do one of the following operations:**

### Scenario Operation I

1. Add/Edit the following parameters in the y000000000025.cfg file or the 0015655f9d7e.cfg file you want the IP DECT phone to download:

```
auto_provision.custom.protect=1  
  
auto_provision.custom.sync=1  
  
firmware.url = tftp://192.168.1.211/25.80.0.10.rom
```

2. Trigger the IP DECT phone to perform the auto provisioning process. For more information on how to trigger auto provisioning process, refer to *Triggering the IP DECT Phone to Perform the Auto Provisioning* section in [Yealink\\_SIP-T2 Series\\_T19\(P\) E2\\_T4 Series\\_CP860\\_W56P\\_IP\\_Phones\\_Auto\\_Provisioning\\_Guide](#).

During auto provisioning, the IP DECT phone first downloads the y000000000025.cfg file, and then downloads firmware from the root directory of the provisioning server.

The base station reboots to complete firmware upgrade, and then starts auto provisioning process again which is triggered by base station reboot (the power on mode is enabled by default). It downloads the y000000000025.cfg, 0015655f9d7e.cfg and the 0015655f9d7e-local.cfg file in sequence from the provisioning server, and then updates configurations in these downloaded configuration files orderly to the IP DECT phone system. The IP DECT phone starts up successfully, and the personalized settings are remained after auto provisioning.

When a user modifies configurations of the base station via the handset or web user interface, the IP DECT phone will save the personalized settings to the 0015655f9d7e-local.cfg file on the phone, and then periodically (every 5 minutes) upload this file to the provisioning server.

#### Note

If a configuration item is both in the downloaded MAC-local.cfg file and Common CFG file/MAC-Oriented CFG file, setting of the configuration item in the MAC-local CFG file will be written and saved to the IP DECT phone system.

### Scenario Operation II

1. Add/Edit the following parameters in the y000000000025.cfg file or the 0015655f9d7e.cfg file you want the IP DECT phone to download:

```
auto_provision.custom.protect=1  
  
auto_provision.custom.sync=0  
  
firmware.url = tftp://192.168.1.211/25.80.0.10.rom
```

2. Trigger the IP DECT phone to perform the auto provisioning process. For more

information on how to trigger auto provisioning process, refer to [Yealink\\_SIPT2 Series\\_T19\(P\) E2\\_T4 Series\\_CP860\\_W56P\\_IP\\_Phones\\_Auto\\_Provisioning\\_Guide](#).

During auto provisioning, the IP DECT phone first downloads the y00000000025.cfg file, and then downloads firmware from the root directory of the provisioning server.

The base station reboots to complete firmware upgrade, and then starts auto provisioning process again which is triggered by base station reboot (the power on mode is enabled by default). It downloads the y00000000025.cfg and 0015655f9d7e.cfg files in sequence from the provisioning server, and then updates configurations in the downloaded configuration files orderly to the IP DECT phone system. As the value of the parameter "auto\_provision.custom.protect" is set 1, the IP DECT phone will also update configurations in the 0015655f9d7e-local.cfg file saved on the IP DECT phone. As a result, the personalized settings are remained after auto provisioning.

When a user modifies configurations of the base station via the handset or web user interface, the IP DECT phone will save the personalized settings to the 0015655f9e7e-local.cfg file saved on the IP DECT phone only.

**Note**

In this scenario, the IP DECT phone will not upload the MAC-local.cfg file to provisioning server and request to download the MAC-local.cfg file from provisioning server during auto provisioning.

If a configuration item is both in the MAC-local.cfg file on the IP DECT phone and Common CFG file/ MAC-Oriented CFG file downloaded from auto provisioning server, setting of the configuration item in the MAC-local CFG file will be written and saved to the IP DECT phone system.

If value of the parameter "auto\_provision.custom.protect" is set to 0, the personalized settings will be overridden after auto provisioning, no matter what the value of the parameter "auto\_provision.custom.sync" is.

**Note**

If a configuration is modified via both web user interface and handset user interface, the later modification will prevail.

For more information on the flowchart of keep user personalized configuration settings, refer to [Appendix D: Auto Provisioning Flowchart \(Keep user personalized configuration settings\)](#) on page 408.

## Protecting personalized settings of the handset

The handset settings can be configured via the handset or auto provisioning. The personalized handset settings stand for the handset settings configured via the handset. The administrator wishes to change some handset settings via auto provisioning, but protect personalized handset settings after auto provisioning.

**Scenario Conditions:**

- The current firmware version of the base station and handset are 25.80.0.10 and 61.80.0.10 respectively. This firmware version supports protecting personalized handset settings after auto provisioning.
- Provisioning server URL: tftp://192.168.1.211.

To configure the handset settings via auto provisioning, you need to configure the value of the parameter "auto\_provision.handset\_configured.enable" to 1. To protect personalized handset settings after auto provisioning, you need to configure the value of the parameter "auto\_provision.custom.protect" to 1.

**Do the following operations:**

1. Add/Edit the following parameters in the y000000000025.cfg file or 0015655f9d7e.cfg file you want the IP DECT phone to download:

```
auto_provision.custom.protect = 1
```

```
auto_provision.handset_configured.enable = 1
```

2. Trigger the IP DECT phone to perform the auto provisioning process. For more information on how to trigger auto provisioning process, refer to [Yealink\\_SIPT2 Series\\_T19\(P\) E2\\_T4 Series\\_CP860\\_W56P\\_IP\\_Phones\\_Auto\\_Provisioning\\_Guide](#).

During auto provisioning, the IP DECT phone will download the configuration files and update configurations in the configuration files. As the value of the parameter "auto\_provision.handset\_configured.enable" is set to 1, handset settings will be changed via auto provisioning. As the value of the parameter "auto\_provision.custom.protect" is set to 1, the personalized handset settings will be remained after auto provisioning.

If value of the parameter "auto\_provision.custom.protect" is set to be 0, and the value of the parameter "auto\_provision.handset\_configured.enable" is set to 1, the personalized handset settings will be overridden after auto provisioning. If the value of the parameter "auto\_provision.handset\_configured.enable" is set to 0, the handset settings cannot be changed via auto provisioning no matter what the value of the parameter "auto\_provision.custom.protect" is.

For more information on the configuration parameters of handset settings, refer to [Configuration Parameters](#) on page 18.

## Scenario B Clear Personalized Settings

### Clearing Personalized Settings of the Base Station

The administrator or user wishes to clear personalized settings of the base station.

#### Scenario Conditions:

- The MAC address of the IP DECT phone is 0015655f9d7e.
- The current firmware of the base station is 25.80.0.1 or later.
- Provisioning server URL: tftp://192.168.1.211
- The value of the parameter "auto\_provision.custom.protect" is 1.

#### Note

The **Reset Local Config** option on the web user interface and the handset is available only if the value of the parameter "auto\_provision.custom.protect" was set to 1. If the value of the parameter "auto\_provision.custom.sync" was set to 1, the configurations in the 001565221229-local.cfg file on the provisioning server will be also cleared after resetting personalized settings of the base station.

#### Scenario Operations:

To reset the base station via handset user interface:

1. Press **OK** to enter the main menu.
2. Select **Settings->System Settings**.
3. Select **Base Reset**, and then press the **OK** soft key.
4. Enter the base PIN (default: 0000), and then press the **OK** soft key.

### Clearing personalized settings of the handset

The administrator or user wishes to clear personalized settings of the specified handset.

#### Scenario Conditions:

- The handset 1 was registered to the base station.

#### Note

You can only clear the personalized settings of the handset via the handset itself.

#### Scenario Operations:

To clear personalized settings of the handset:

1. Press **OK** to enter the main menu.

2. Select **Settings->System Settings**.
3. Select **Handset Reset**, and then press the **OK** soft key.  
The LCD screen prompts "Reset handset to default?".
4. Press the **Yes** soft key.

**Note**

If the value of the parameter "auto\_provision.handset\_configured.enable" is set to 1 (Enabled), the handset settings (configured via auto provisioning) stored on the base station will be delivered to the handset after handset reset. If the value of this parameter is set to 0 (Disabled), the handset settings will not be delivered to the handset after handset reset.

## Scenario C Protecting Personalized Settings after Reset

The base station requires factory reset when it has a breakdown, but the user wishes to remain personalized settings of the base station after factory reset. You can reset the base station via factory reset or base reset.

**Scenario Conditions:**

- The MAC address of the IP DECT phone is 0015655f9d7e.
- Provisioning server URL: tftp://192.168.1.211.
- The value of the parameter "auto\_provision.custom.sync" is 1.
- The value of the parameter "auto\_provision.custom.protect" is 1.

**Note**

As the parameter "auto\_provision.custom.sync" was set to 1, the 0015655f9d7e-local.cfg file on the IP DECT phone will be uploaded to the provisioning server at tftp://192.168.1.211.

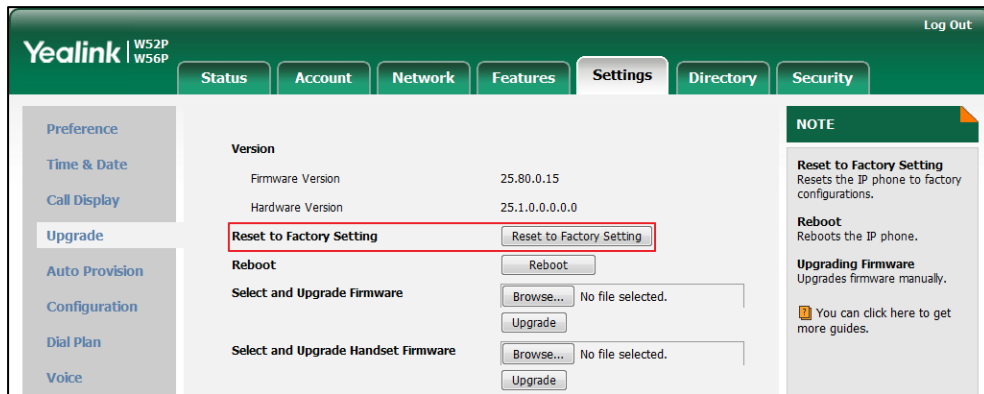
Factory reset and base reset will only reset the settings of the base station to factory defaults. The handset settings will not be reset.

## Scenario Operation I

To reset the base station to factory via web user interface:

1. Click on **Settings->Upgrade**.
2. Click **Reset to Factory Setting**.

The web user interface prompts “Do you want to reset to factory?”.



3. Click **OK**.

## Scenario Operation II

To reset the base station via the handset:

1. Press **OK** to enter the main menu.
2. Select **Settings->System Settings**.
3. Select **Base Reset**, and then press the **OK** soft key.
4. Enter the system PIN (default: 0000), and then press the **Done** soft key.

After startup, all configurations of base station will be reset to factory defaults. Configurations in the 0015655f9d7e-local.cfg file saved on the IP DECT phone will also be cleared. But configurations in the 001565655f9d7e-local.cfg file stored on the provisioning server (tftp://192.168.1.211) will not be cleared after reset.

To retrieve personalized settings of the base station after factory reset:

1. Set the values of the parameters “auto\_provision.custom.sync” and “auto\_provision.custom.protect” to be 1 in the configuration file (y000000000025.cfg or 001565655f9d7e.cfg).
2. Trigger the phone to perform the auto provisioning process.

The IP DECT phone will download the 0015655f9d7e-local.cfg file from the provisioning server, and then update configurations in it during auto provisioning. As a result, the personalized settings of the base station are retrieved after factory reset.

## Scenario D Importing or Exporting the Local Configuration File

The administrator or user can export the local configuration file to check the personalized settings of the base station configured by the user, or import the local configuration file to configure or change settings of the base station.

### Scenario Conditions:

- The MAC address of the IP DECT phone is 0015655f9d7e.
- The current firmware of the base station is 25.80.0.1 or later.
- Provisioning server URL: tftp://192.168.1.211.

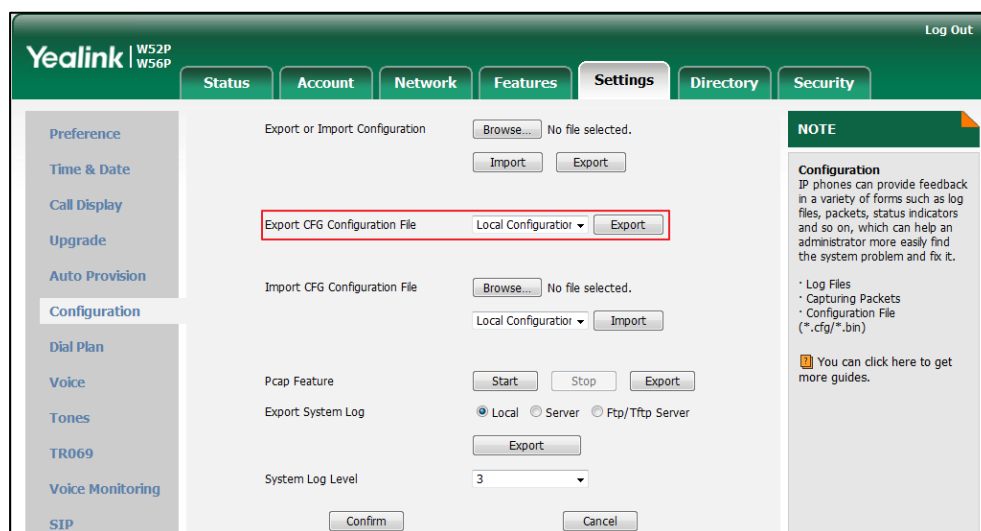
### Note

The <MAC>-local.cfg file can only store personalized settings of the base station. You cannot export or import the handset settings. As the personalized settings of the base station cannot be changed via auto provisioning when the value of the parameter "auto\_provision.custom.protect" is set to 1, it is cautious to change the settings in the <MAC>-local.cfg file before importing it.

### Scenario Operations:

#### To export local configuration file via web user interface:

1. Click on **Settings->Configuration**.
2. Select **Local Configuration** from the **Export CFG Configuration File** pull-down list.
3. Click **Export** to open file download window.
4. Save the 0015655f9d7e-local.cfg file to the local system.



The administrator or user can edit the 0015655f9d7e-local.cfg file after exporting.

#### To import local configuration file via web user interface:

1. Click on **Settings->Configuration**.
2. In the **Local Configuration** field, click **Browse** to locate the 0015655f9d7e-local.cfg



file from your local system.

The screenshot shows the Yealink W52P/W56P Settings page. The 'Configuration' tab is selected. The 'Import CFG Configuration File' section is highlighted with a red box. It contains a 'Browse...' button, a 'Local Configuration' dropdown menu, and an 'Import' button. Other sections include 'Export or Import Configuration', 'Export CFG Configuration File', 'Pcap Feature', 'Export System Log', and 'System Log Level'.

3. Select the **Local Configuration** from the pull-down list.
4. Click **Import**.

The existing local configuration file will be overridden by the imported one after importing. The configurations in the importing 0015655f9d7e-local.cfg file will be saved to the phone flash and take effect.

If the administrator or user deletes the configurations in the 0015655f9d7e-local.cfg file and then import the file to the phone, the IP DECT phone will remain the original configurations. But the configurations can be change via next auto provisioning.

#### Note

If the value of the parameter “auto\_provision.custom.sync” is set to 1, and the 0015655f9d7e-local.cfg file is successfully imported, the imported 0015655f9d7e-local.cfg file will be uploaded to the provisioning server and overrides the existing one on the server.

## Provisioning Server

### Supported Provisioning Protocols

Yealink IP DECT phones perform the auto provisioning function of downloading configuration files, downloading resource files and upgrading firmware. The transfer protocol is used to download files from the provisioning server. The IP DECT phones support several transport protocols for provisioning, including FTP, TFTP, HTTP, and HTTPS protocols. And you can specify the transport protocol in the provisioning server address, for example, http://xxxxxxx. If not specified, the TFTP protocol is used. The provisioning server address can be IP address, domain name or URL. If a user name and password are specified as part of the provisioning server address, for example,

`http://user:pwd@server/dir`, they will be used only if the server supports them.

**Note**

A URL should contain forward slashes instead of back slashes and should not contain spaces. Escape characters are not supported.

If a user name and password are not specified as part of the provisioning server address, the User Name and Password of the provisioning server configured on the phone will be used.

There are two types of FTP methods—active and passive. The IP DECT phones are not compatible with active FTP.

## Setting up the Provisioning Server

The provisioning server can be on the local LAN or anywhere on the Internet. Use the following procedure as a recommendation if this is your first provisioning server setup. For more information on how to set up a provisioning server, refer to [Yealink SIP-T2 Series\\_T19\(P\) E2\\_T4 Series\\_CP860\\_W56P\\_IP\\_Phones\\_Auto\\_Provisioning\\_Guide](#).

**To set up the provisioning server:**

1. Install a provisioning server application or locate a suitable existing server.
2. Create an account and home directory.
3. Set security permissions for the account.
4. Create configuration files and edit them as desired.
5. Copy the configuration files and resource files to the provisioning server.

For more information on how to deploy IP DECT phones using configuration files, refer to [Deploying Phones from the Provisioning Server](#) on page 30.

**Note**

Typically all DECT phones are configured with the same server account, but the server account provides a means of conveniently partitioning the configuration. Give each account a unique home directory on the server and change the configuration on a per-line basis.

## Deploying Phones from the Provisioning Server

The parameters in the new downloaded configuration files will override the duplicate parameters in files downloaded earlier. During auto provisioning, the IP DECT phones download the common configuration file first, and then the MAC-oriented file. Therefore any parameter in the MAC-oriented configuration file will override the same one in the common configuration file.

Before you configure parameters in the configuration files, Yealink recommends that you create new configuration files containing only those parameters that require changes.

**To deploy IP DECT phones from the provisioning server:**

1. Create per-phone configuration files by performing the following steps:
  - a) Obtain a list of phone MAC addresses (the barcode label on the back of the base station or on the outside of the box).
  - b) Create per-phone <MAC>.cfg files by using the MAC-Oriented CFG file from the distribution as templates.
  - c) Edit the parameters in the file as desired.
2. Create new common configuration files by performing the following steps:
  - a) Create y00000000025.cfg files by using the Common CFG file from the distribution as templates.
  - b) Edit the parameters in the file as desired.
3. Copy configuration files to the home directory of the provisioning server.
4. Reboot IP DECT phones to trigger the auto provisioning process.

The IP DECT phones discover the provisioning server address, and then download the configuration files from the provisioning server.

For more information on configuration files, refer to [Configuration Files](#) on page 14. For protecting against unauthorized access, you can encrypt configuration files. For more information on encrypting configuration files, refer to [Encrypting Configuration Files](#) on page 363.

During the auto provisioning process, the IP DECT phone supports the following methods to discover the provisioning server address:

- **PnP:** PnP feature allows the IP DECT phones to discover the provisioning server address by broadcasting the PnP SUBSCRIBE message during startup.
- **DHCP:** DHCP option can be used to provide the address or URL of the provisioning server to the IP DECT phones. When the IP DECT phone requests an IP address using the DHCP protocol, the resulting response may contain option 66 or the custom option (if configured) that contains the provisioning server address.
- **Static:** You can manually configure the server address via handset user interface or web user interface.

For more information on the above methods, refer to [Yealink\\_SIP-T2 Series\\_T19\(P\) E2\\_T4 Series\\_CP860\\_W56P\\_IP\\_Phones\\_Auto\\_Provisioning\\_Guide](#).

## Setting Up DECT Phone Network

In order to get your IP DECT phones running, you must perform basic network setup, such as IP address and subnet mask configuration. You can configure the IPv4 or IPv6 network parameters for the phone. You can also configure the appropriate security (VLAN and/or 802.1X authentication) and Quality of Service (QoS) settings for the IP DECT phone.

This chapter describes how to configure all the network parameters for IP DECT phones, and it provides the following sections:

- [DHCP](#)
- [DHCP Options](#)
- [Configuring Network Parameters Manually](#)
- [PPPoE](#)
- [IPv6 Support](#)
- [Web Server Type](#)
- [VLAN](#)
- [VPN](#)
- [Quality of Service](#)
- [802.1X Authentication](#)

## 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. The IP DECT phones comply with the DHCP specifications documented in [RFC 2131](#). If using DHCP, the IP DECT phones connected to the network become operational without having to be manually assigned IP addresses and additional network parameters.

### Procedure

DHCP can be configured using the configuration files or locally.

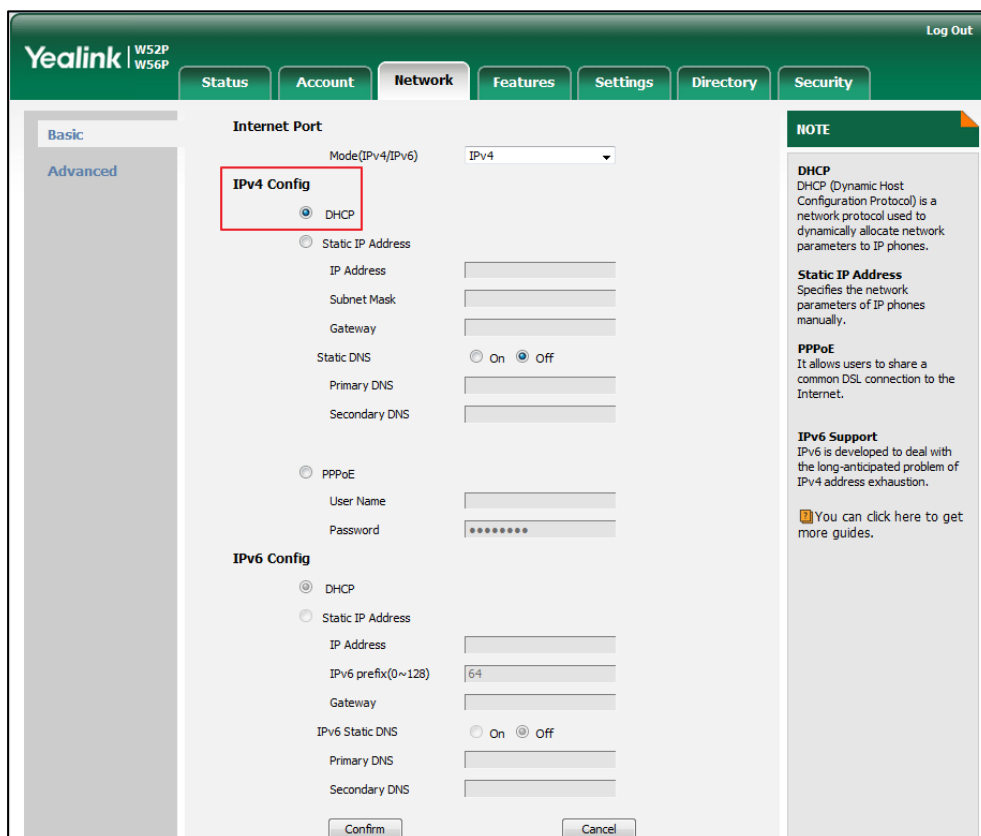
<b>Configuration File</b>	<MAC>.cfg	Configure DHCP on the IP DECT phone. <b>Parameter:</b> network.internet_port.type
<b>Local</b>	Web User Interface	Configure DHCP on the IP DECT phone. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=network&q=load
	Handset User Interface	Configure DHCP on the IP DECT phone.

### Details of Configuration Parameters:

Parameters	Permitted Values	Default
<b>network.internet_port.type</b>	<b>0, 1 or 2</b>	<b>0</b>
<p><b>Description:</b> Configures the Internet (WAN) port type.</p> <p><b>0-DHCP</b> <b>1-PPPoE</b> <b>2-Static IP Address</b></p> <p><b>Note:</b> It works only if the value of the parameter “network.ip_address_mode” is set to 0 (IPv4) or 2 (IPv4 &amp; IPv6). If you change this parameter, the IP DECT phone will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Network-&gt;Basic-&gt;IPv4 Config</p> <p><b>Handset User Interface:</b> OK-&gt;Settings-&gt;System Settings-&gt;Network (default PIN: 0000)-&gt;IPv4-&gt;IP Address Type</p>		

**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 a reboot.
4. Click **OK** to reboot the phone.

**To configure DHCP via handset user interface:**

1. Press **OK** to enter the main menu.
2. Select **Settings->System Settings->Network**.
3. Enter the system PIN (default: 0000), and then press the **Done** soft key.
4. Press **▼** to select **IPv4**, and then press the **OK** soft key.
5. Press **◀** or **▶** to select **DHCP** from the **IP Address Type** field.
6. Press the **Save** soft key to accept the change.

The base station reboots automatically to make settings effective after a period of time.

## Static DNS

Static DNS address(es) can be configured and used when DHCP is enabled.

## Procedure

Static DNS can be configured using the configuration files or locally.

<b>Configuration File</b>	<MAC>.cfg	Configure static DNS address. <b>Parameters:</b> network.static_dns_enable network.primary_dns network.secondary_dns
<b>Local</b>	Web User Interface	Configure static DNS address. <b>Navigate to:</b> http://<phoneIPAddress>/servlet ?p=network&q=load
	Handset User Interface	Configure static DNS address.

### Details of Configuration Parameters:

Parameters	Permitted Values	Default
<b>network.static_dns_enable</b>	<b>0 or 1</b>	<b>0</b>
<p><b>Description:</b> Triggers the static IPv4 DNS feature to on or off. <b>0-Off</b> <b>1-On</b> If it is set to 0 (Off), the IP DECT phone will use the IPv4 DNS obtained from DHCP. If it is set to 1 (On), the IP DECT phone will use manually configured static IPv4 DNS. <b>Note:</b> It works only if the value of the parameter "network.internet_port.type" is set to 0 (DHCP). If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Network-&gt;Basic-&gt;IPv4 Config-&gt;Static IP Address-&gt;Static DNS</p> <p><b>Handset User Interface:</b> OK-&gt;Settings-&gt;System Settings-&gt;Network (default PIN: 0000)-&gt;IPv4-&gt;IP Address Type: DHCP-&gt;DNS Type: Manual</p>		
<b>network.primary_dns</b>	<b>IPv4 address</b>	<b>Blank</b>
<p><b>Description:</b> Configures the primary DNS server.</p>		

Parameters	Permitted Values	Default
<p><b>Example:</b> network.primary_dns = 202.101.103.55</p> <p><b>Note:</b> It works only if the value of the parameter "network.static_dns_enable" is set to 1 (On). If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Network-&gt;Basic-&gt;IPv4 Config-&gt;Static IP Address-&gt;Static DNS-&gt;Primary DNS</p> <p><b>Handset User Interface:</b> OK-&gt;Settings-&gt;System Settings-&gt;Network (default PIN: 0000)-&gt;IPv4-&gt;IP Address Type: DHCP-&gt;DNS Type: Manual-&gt;Primary DNS</p>		
network.secondary_dns	IPv4 address	Blank
<p><b>Description:</b> Configures the secondary DNS server.</p> <p><b>Example:</b> network.secondary_dns = 202.101.103.54</p> <p><b>Note:</b> It works only if the value of the parameter "network.static_dns_enable" is set to 1 (On). If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Network-&gt;Basic-&gt;IPv4 Config-&gt;Static DNS-&gt;Secondary DNS</p> <p><b>Handset User Interface:</b> OK-&gt;Settings-&gt;System Settings-&gt;Network (default PIN: 0000)-&gt;IPv4-&gt;IP Address Type: DHCP-&gt;DNS Type: Manual-&gt;Secondary DNS</p>		

**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. In the **Static DNS** block, mark the **On** radio box.



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

The screenshot shows the Yealink W52P/W56P web interface. The 'Network' tab is selected. Under 'Internet Port', the mode is set to 'IPv4'. In the 'IPv4 Config' section, 'DHCP' is selected. The 'Static DNS' option is turned 'On'. The 'Primary DNS' field contains '202.101.103.55' and the 'Secondary DNS' field contains '202.101.103.54'. Other fields like IP Address, Subnet Mask, Gateway, User Name, and Password are present but empty. A 'NOTE' sidebar on the right contains information about DHCP, Static IP Address, PPPoE, and IPv6 Support.

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

#### To configure static DNS when DHCP is used via handset user interface:

- Press **OK** to enter the main menu.
- Select **Settings->System Settings->Network**.
- Enter the system PIN (default: 0000), and then press the **Done** soft key.
- Press **▼** to select **IPv4**, and then press the **OK** soft key.
- Press **◀** or **▶** to select **Manual** from the **DNS Type** field when **DHCP** is selected from the **IP Address Type** field.
- Enter the valid value in the **Primary DNS** and **Secondary DNS** field respectively.
- Press the **Save** soft key to accept the change.

The base station reboots automatically to make settings effective after a period of time.

## DHCP Options

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 DECT phone with the network. The IP DECT phones broadcast DISCOVER messages to request the network information carried in DHCP options, and the DHCP server responds with specific values in corresponding options.

The following table lists common DHCP options supported by IP DECT 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 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 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 'name' field in the DHCP header has been used for DHCP options.
Boot file Name	67	Identify a boot file when the 'file' field in the DHCP header has been used for DHCP options.

For more information on DHCP options, refer to <http://www.ietf.org/rfc/rfc2131.txt?number=2131> or <http://www.ietf.org/rfc/rfc2132.txt?number=2132>.

If you do not have the ability to configure the DHCP options for discovering the

provisioning server on the DHCP server, an alternate method of automatically discovering the provisioning server address is required. Connecting to the secondary DHCP server that responds to DHCP INFORM queries with a requested provisioning server address is one possibility. For more information, refer to <http://www.ietf.org/rfc/rfc3925.txt?number=3925>.

## DHCP Option 66 and Option 43

Yealink IP DECT phones support obtaining the provisioning server address by detecting DHCP options during startup.

The phone will automatically detect the option 66 and option 43 for obtaining the provisioning server address. DHCP option 66 is used to identify the TFTP server. DHCP option 43 is a vendor-specific option, which is used to transfer the vendor-specific information.

To use DHCP option 66 or DHCP option 43, make sure the DHCP Active feature is enabled.

### Procedure

DHCP active can be configured using the configuration files or locally.

<b>Configuration File</b>	y00000000025.cfg	Configure DHCP active. <b>Parameters:</b> auto_provision.dhcp_option.enable
<b>Local</b>	Web User Interface	Configure DHCP active. <b>Navigate to:</b> <a href="http://&lt;phoneIPAddress&gt;/servlet?parameter=phone-autoprovision&amp;q=load">http://&lt;phoneIPAddress&gt;/servlet?parameter=phone-autoprovision&amp;q=load</a>

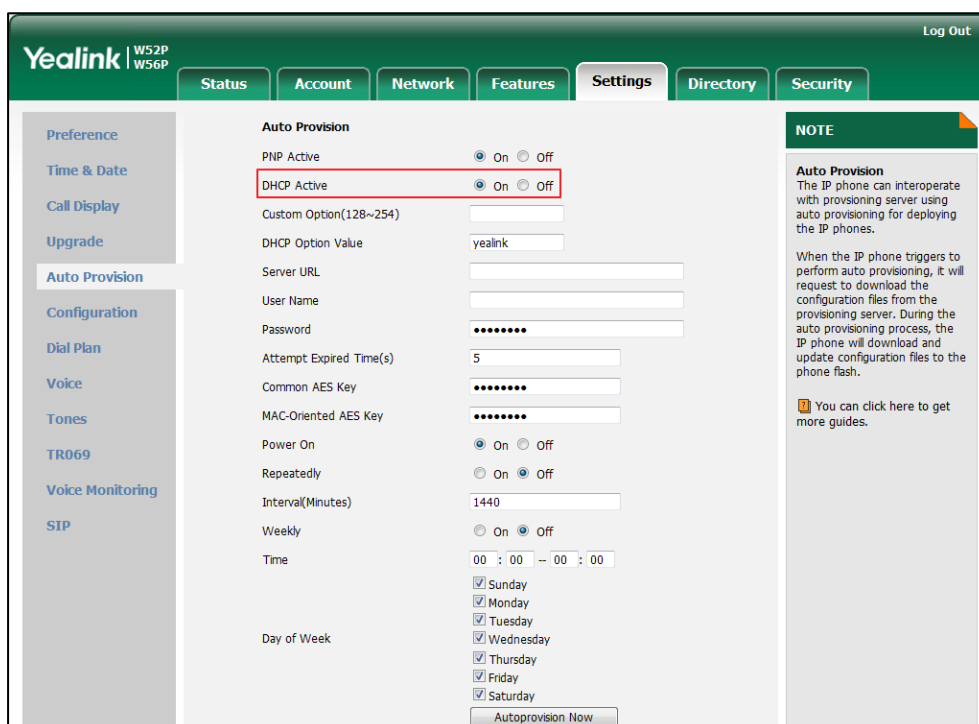
### Details of Configuration Parameters:

Parameters	Permitted Values	Default
auto_provision.dhcp_option.enable	0 or 1	1
<p><b>Description:</b> Triggers the DHCP Option feature to on or off.</p> <p><b>0-Off</b> <b>1-On</b></p> <p>If it is set to 1 (On), the IP DECT phone will obtain the provisioning server address by detecting DHCP options.</p> <p><b>Web User Interface:</b> Settings-&gt;Auto Provision-&gt;DHCP Active</p>		

Parameters	Permitted Values	Default
<b>Handset User Interface:</b>		
None		

To configure the DHCP active feature via web user interface:

1. Click on **Settings->Auto Provision**.
2. Mark the **On** radio box in the **DHCP Active** field.



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

## DHCP Option 42 and Option 2

Yealink IP DECT phones support using the NTP server address offered by DHCP.

DHCP option 42 is used to specify a list of NTP servers available to the client by IP address. NTP servers should be listed in order of preference. DHCP option 2 is used to specify the offset of the client's subnet in seconds from Coordinated Universal Time (UTC).

To update time with the offset time offered by the DHCP server, make sure the DHCP Time feature is enabled at the web path **Settings->Time & Date->DHCP Time**. For more information on how to configure DHCP time feature, refer to [NTP Time Server](#) on page 130.

## DHCP Option 12 Hostname on the IP DECT phone

This option specifies the hostname of the client. The name may or may not be qualified with the local domain name (based on RFC 2132). See RFC 1035 for character restrictions.

### Procedure

DHCP option 12 hostname can be configured using the configuration files or locally.

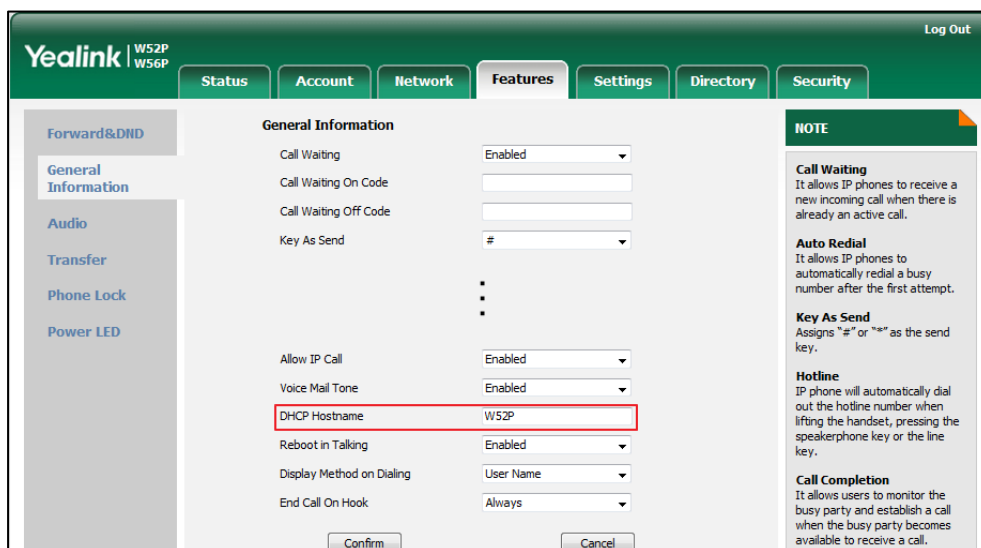
<b>Configuration File</b>	y000000000025.cfg	Configure the DHCP option 12 hostname. <b>Parameters:</b> network.dhcp_host_name
<b>Local</b>	Web User Interface	Configure the DHCP option 12 hostname. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=phone-features&q=load

### Details of Configuration Parameters:

Parameters	Permitted Values	Default
network.dhcp_host_name	String within 99 characters	W52P
<p><b>Description:</b> Configures the DHCP option 12 hostname on the IP DECT phone.</p> <p><b>Note:</b> If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Features-&gt;General Information-&gt;DHCP Hostname</p> <p><b>Handset User Interface:</b> None</p>		

To configure DHCP option 12 hostname on the IP DECT phone via web user interface:

1. Click on **Features->General Information**.
2. Enter the desired host name in the **DHCP Hostname** field.



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

## Configuring Network Parameters Manually

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

<b>Configuration File</b>	<MAC>.cfg	Configure network parameters of the IP DECT phone manually. <b>Parameters:</b> network.internet_port.type
---------------------------	-----------	---

		network.internet_port.ip network.internet_port.mask network.internet_port.gateway network.primary_dns network.secondary_dns
<b>Local</b>	Web User Interface	Configure network parameters of the IP DECT phone manually. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=network&q=load
	Handset User Interface	Configure network parameters of the IP DECT phone manually.

### Details of Configuration Parameters:

Parameters	Permitted Values	Default
<b>network.internet_port.type</b>	<b>0, 1 or 2</b>	<b>0</b>
<p><b>Description:</b> Configures the Internet (WAN) port type.</p> <p><b>0-DHCP</b> <b>1-PPPoE</b> <b>2-Static IP Address</b></p> <p><b>Note:</b> It works only if the value of the parameter "network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 &amp; IPv6). If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Network-&gt;Basic-&gt;IPv4 Config</p> <p><b>Handset User Interface:</b> OK-&gt;Settings-&gt;System Settings-&gt;Network (default PIN: 0000)-&gt;IPv4-&gt;IP Address Type</p>		
<b>network.internet_port.ip</b>	<b>IPv4 address</b>	<b>Blank</b>
<p><b>Description:</b> Configures the IP address.</p> <p><b>Example:</b> network.internet_port.ip = 192.168.1.20</p> <p><b>Note:</b> It works only if the value of the parameter "network.internet_port.type" is set to 2 (Static IP Address). If you change this parameter, the base station will reboot to</p>		

Parameters	Permitted Values	Default
<p>make the change take effect.</p> <p><b>Web User Interface:</b> Network-&gt;Basic-&gt;IPv4 Config-&gt;Static IP Address-&gt;IP Address</p> <p><b>Handset User Interface:</b> OK-&gt;Settings-&gt;System Settings-&gt;Network (default PIN: 0000)-&gt;IPv4-&gt;IP Address Type: Static-&gt;IP Address</p>		
<b>network.internet_port.mask</b>	<b>Subnet Mask</b>	<b>Blank</b>
<p><b>Description:</b> Configures the subnet mask.</p> <p><b>Example:</b> network.internet_port.mask = 255.255.255.0</p> <p><b>Note:</b> It works only if the value of the parameter "network.internet_port.type" is set to 2 (Static IP Address). If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Network-&gt;Basic-&gt;IPv4 Config-&gt;Static IP Address-&gt;Subnet Mask</p> <p><b>Handset User Interface:</b> OK-&gt;Settings-&gt;System Settings-&gt;Network (default PIN: 0000)-&gt;IPv4-&gt;IP Address Type: Static-&gt;Subnet Mask</p>		
<b>network.internet_port.gateway</b>	<b>IPv4 address</b>	<b>Blank</b>
<p><b>Description:</b> Configures the default gateway.</p> <p><b>Example:</b> network.internet_port.gateway = 192.168.1.254</p> <p><b>Note:</b> It works only if the value of the parameter "network.internet_port.type" is set to 2 (Static IP Address). If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Network-&gt;Basic-&gt;IPv4 Config-&gt;Static IP Address-&gt;Gateway</p> <p><b>Handset User Interface:</b> OK-&gt;Settings-&gt;System Settings-&gt;Network (default PIN: 0000)-&gt;IPv4-&gt;IP Address Type: Static-&gt;Default Gateway</p>		
<b>network.primary_dns</b>	<b>IPv4 address</b>	<b>Blank</b>

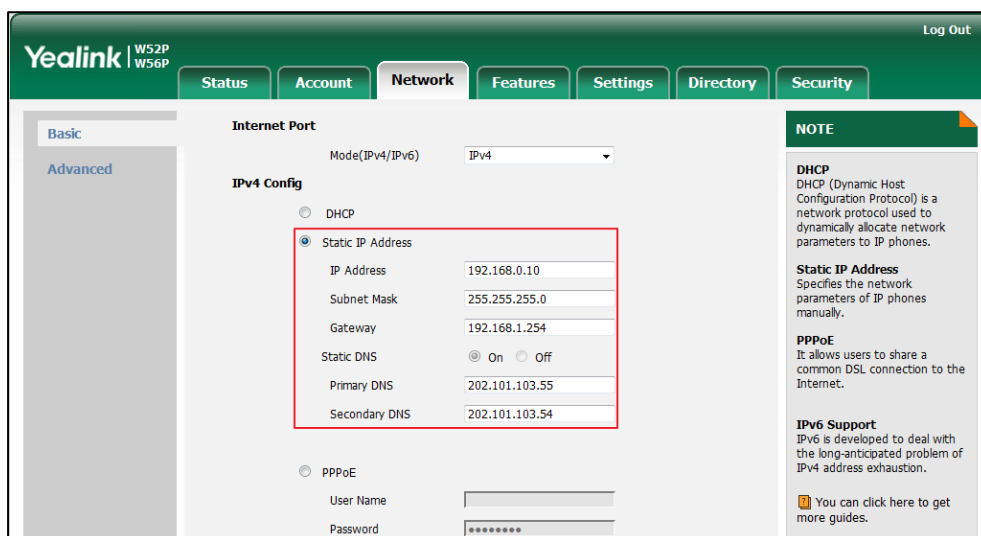


Parameters	Permitted Values	Default
<p><b>Description:</b> Configures the primary DNS server.</p> <p><b>Example:</b> network.primary_dns = 202.101.103.55</p> <p><b>Note:</b> It works only if the value of the parameter "network.internet_port.type" is set to 2 (Static IP Address) or "network.static_dns_enable" is set to 1 (On). If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Network-&gt;Basic-&gt;IPv4 Config-&gt;Static IP Address-&gt;Static DNS-&gt;Primary DNS</p> <p><b>Handset User Interface:</b> OK-&gt;Settings-&gt;System Settings-&gt;Network (default PIN: 0000)-&gt;IPv4-&gt;IP Address Type: Static-&gt;Primary DNS</p>		
network.secondary_dns	IPv4 address	Blank
<p><b>Description:</b> Configures the secondary DNS server.</p> <p><b>Example:</b> network.secondary_dns = 202.101.103.54</p> <p><b>Note:</b> It works only if the value of the paramete "network.internet_port.type" is set to 2 (Static IP Address) or "network.static_dns_enable" is set to 1 (On). If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Network-&gt;Basic-&gt;IPv4 Config-&gt;Static IP Address-&gt;Static DNS-&gt;Secondary DNS</p> <p><b>Handset User Interface:</b> OK-&gt;Settings-&gt;System Settings-&gt;Network (default PIN: 0000)-&gt;IPv4-&gt;IP Address Type: Static-&gt;Secondary DNS</p>		

**To configure a static IP address via web user interface:**

1. Click on **Network->Basic**.
2. In the **Internet Port** block, mark the **Static IP Address** radio box.

3. Enter the valid values in the **IP Address, Subnet Mask, Default Gateway, Primary DNS** and **Secondary DNS** fields.



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

**To configure a static IP address via handset user interface:**

1. Press **OK** to enter the main menu.
2. Select **Settings->System Settings->Network**.
3. Enter the system PIN (default: 0000), and then press the **Done** soft key.
4. Press **◀** or **▶** to select **Static** from the **IP Address Type** field.
5. Enter the valid value in the **IP Address, Subnet Mask, Default Gateway, Primary DNS** and **Secondary DNS** field respectively.
6. Press the **Save** soft key to accept the change.

The base station reboots automatically to make settings effective after a period of time.

## 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 IP DECT phone Internet port. Contact your ISP for the PPPoE user name and password.

## Procedure

PPPoE can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure PPPoE on the IP DECT phone. <b>Parameters:</b> network.internet_port.type
	y000000000025.cfg	Configure the user name and password for PPPoE on the IP DECT phone. <b>Parameters:</b> network.pppoe.user network.pppoe.password
Local	Web User Interface	Configure PPPoE on the IP DECT phone. Configure the user name and password for PPPoE on the IP DECT phone. <b>Navigate to:</b> <a href="http://&lt;phoneIPAddress&gt;/servlet?p=network&amp;q=load">http://&lt;phoneIPAddress&gt;/servlet?p=network&amp;q=load</a>
	Handset User Interface	Configure PPPoE on the IP DECT phone. Configure the user name and password for PPPoE on the IP DECT phone.

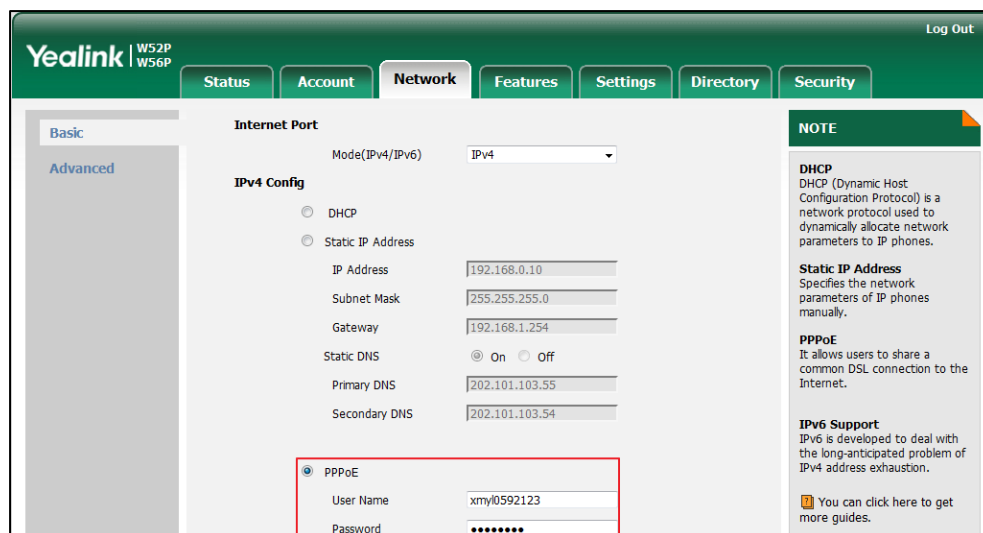
### Details of Configuration Parameters:

Parameters	Permitted Values	Default
network.internet_port.type	0, 1 or 2	0
<p><b>Description:</b> Configures the Internet (WAN) port type.</p> <p><b>0</b>-DHCP <b>1</b>-PPPoE <b>2</b>-Static IP Address</p> <p><b>Note:</b> It works only if the value of the parameter "network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 &amp; IPv6). If you change this parameter, the base station will reboot</p>		

Parameters	Permitted Values	Default
<p>to make the change take effect.</p> <p><b>Web User Interface:</b> Network-&gt;Basic-&gt;IPv4 Config</p> <p><b>Handset User Interface:</b> OK-&gt;Settings-&gt;System Settings-&gt;Network (default PIN: 0000)-&gt;IPv4-&gt;IP Address Type</p>		
network.pppoe.user	String within 32 characters	Blank
<p><b>Description:</b> Configures the username for PPPoE connection.</p> <p><b>Example:</b> network.pppoe.user =Xmyl0592123</p> <p><b>Note:</b> It works only if the value of the parameter "network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 &amp; IPv6), and "network.internet_port.type" is set to 1 (PPPoE). If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Network-&gt;Basic-&gt;IPv4 Config-&gt;PPPoE-&gt;User Name</p> <p><b>Handset User Interface:</b> OK-&gt;Settings-&gt;System Settings-&gt;Network (default PIN: 0000)-&gt;IPv4-&gt;IP Address Type: PPPoE-&gt;PPPoE User</p>		
network.pppoe.password	String within 99 characters	Blank
<p><b>Description:</b> Configures the password for PPPoE connection.</p> <p><b>Example:</b> network.pppoe.password = yealink123</p> <p><b>Note:</b> It works only if the value of the parameter "network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 &amp; IPv6), and "network.internet_port.type" is set to 1 (PPPoE). If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Network-&gt;Basic-&gt;IPv4 Config-&gt;PPPoE-&gt;Password</p> <p><b>Handset User Interface:</b> OK-&gt;Settings-&gt;System Settings-&gt;Network (default PIN: 0000)-&gt;IPv4-&gt;IP Address Type: PPPoE-&gt;PPPoE Password</p>		

### To configure PPPoE via web user interface:

1. Click on **Network->Basic**.
2. In the **PPPoE** block, mark the **PPPoE** radio box.
3. Enter the user name and password in corresponding fields.



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

### To configure PPPoE via handset user interface:

1. Press **OK** to enter the main menu.
2. Select **Settings->System Settings->Network**.
3. Enter the system PIN (default: 0000), and then press the **Done** soft key.
4. Press **▼** to select **IPv4**, and then press the **OK** soft key.
5. Press **◀** or **▶** to select **PPPoE** from the **IP Address Type** field.
6. Enter the valid values in the **PPPoE User** and **PPPoE Password** fields.

You can press **\*#** to enter special characters and press **#a** to switch the input method.

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

The base station reboots automatically to make settings effective after a period of time.

## IPv6 Support

Because Internet Protocol version 4 (IPv4) uses a 32-bit address, it cannot meet the increased demands for unique IP addresses for all devices that connect to the Internet. Therefore, Internet Protocol version 6 (IPv6) is the next generation network layer protocol, which 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. Yealink IP DECT Phone supports IPv4 addressing mode, IPv6 addressing mode, as well as an IPv4 & IPv6 dual stack addressing mode. IPv4 uses a 32-bit address, consisting of four groups of three decimal digits separated by dots; for example, 192.168.1.100. IPv6 uses a 128-bit address, consisting of eight groups of four hexadecimal digits separated by colons; for example, 2026:1234:1:1:215:65ff:fe1f:caa.

VoIP network based on IPv6 can provide end-to-end security capabilities, enhanced Quality of Service (QoS), a set of service requirements to deliver performance guarantee while transporting traffic over the network.

If you configure the network settings on the phone for an IPv6 network, you can set up an IP address for the phone by using SLAAC (ICMPv6) or by manually entering an IP address. Ensure that your network environment supports IPv6. Contact your ISP for more information.

### 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 DECT phone can be statically configured by an administrator.
- **Stateless Address Autoconfiguration (SLAAC)/ICMPv6:** SLAAC is one of the most convenient methods to assign IP addresses to IPv6 nodes. SLAAC requires no manual configuration of the IP DECT phone, minimal (if any) configuration of routers, and no additional servers. To use IPv6 SLAAC, the IP DECT 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 DECT phone to configure itself with IPv6 address, as specified in RFC 4862.

### How the IP DECT phone obtains the IPv6 address and network settings?

The following table lists where the IP DECT phone obtains the IPv6 address and other network settings:

SLAAC (ICMPv6)	How the IP DECT phone obtains the IPv6 address and network settings?
Disabled	You have to manually configure the static IPv6 address and other network settings.
Enabled	The IP DECT phone can obtain the IPv6 address via SLAAC, but the other network settings must be configured manually.

## Procedure

IPv6 can be configured using the following methods.

Configuration File	<MAC>.cfg	Configure the IPv6 address assignment method. <b>Parameters:</b> network.ip_address_mode network.ipv6_internet_port.type network.ipv6_internet_port.ip network.ipv6_prefix network.ipv6_internet_port.gateway
		Configure the IPv6 static DNS address. <b>Parameters:</b> network.ipv6_primary_dns network.ipv6_secondary_dns
		Configure the IPv6 static DNS. <b>Parameter:</b> network.ipv6_static_dns_enable
Local	Web User Interface	Configure the IPv6 address assignment method. Configure the IPv6 static DNS address. Configure the IPv6 static DNS. <b>Navigate to:</b> <a href="http://&lt;phoneIPAddress&gt;/servlet?p=network&amp;q=load">http://&lt;phoneIPAddress&gt;/servlet?p=network&amp;q=load</a>
	Handset User Interface	Configure the IPv6 address assignment method. Configure the IPv6 static DNS address. Configure the IPv6 static DNS.

### Details of Configuration Parameters:

Parameters	Permitted Values	Default
network.ip_address_mode	0, 1 or 2	0

Parameters	Permitted Values	Default
<p><b>Description:</b> Configures the IP address mode.</p> <p><b>0</b>-IPv4 <b>1</b>-IPv6 <b>2</b>-IPv4 &amp; IPv6</p> <p><b>Note:</b> If you change this parameter, the IP DECT phone will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Network-&gt;Basic-&gt;Internet Port-&gt;Mode(IPv4/IPv6)</p> <p><b>Handset User Interface:</b> OK-&gt;Settings-&gt;System Settings-&gt;Network (default PIN: 0000)-&gt;IP Mode</p>		
<b>network.ipv6_internet_port.type</b>	<b>0 or 1</b>	<b>0</b>
<p><b>Description:</b> Configures the Internet port type for IPv6.</p> <p><b>0</b>-DHCP <b>1</b>-Static IP Address</p> <p><b>Note:</b> It works only if the value of the parameter "network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 &amp; IPv6). If you change this parameter, the IP DECT phone will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Network-&gt;Basic-&gt;IPv6 Config</p> <p><b>Handset User Interface:</b> OK-&gt;Settings-&gt;System Settings-&gt;Network (default PIN: 0000)-&gt;IPv6-&gt;IP Address Type</p>		
<b>network.ipv6_static_dns_enable</b>	<b>0 or 1</b>	<b>0</b>
<p><b>Description:</b> Triggers the static IPv6 DNS feature to on or off.</p> <p><b>0</b>-Off <b>1</b>-On</p> <p>If it is set to 0 (Off), the IP DECT phone will use the IPv6 DNS obtained from DHCP If it is set to 1 (On), the IP DECT phone will use manually configured static IPv6 DNS.</p> <p><b>Note:</b> It works only if the value of the parameter "network.ipv6_internet_port.type" is set to 0 (DHCP). If you change this parameter, the IP DECT phone will reboot to</p>		



Parameters	Permitted Values	Default
<p>make the change take effect.</p> <p><b>Web User Interface:</b> Network-&gt;Basic-&gt;IPv6 Config-&gt;IPv6 Static DNS</p> <p><b>Handset User Interface:</b> OK-&gt;Settings-&gt;System Settings-&gt;Network (default PIN: 0000)-&gt;IPv6-&gt;IP Address Type: DHCP-&gt;DNS Type: Manual</p>		
<b>network.ipv6_internet_port.ip</b>	<b>IPv6 address</b>	<b>Blank</b>
<p><b>Description:</b> Configures the IPv6 address.</p> <p><b>Example:</b> network.ipv6_internet_port.ip = 2026:1234:1:1:215:65ff:fe1f:caa</p> <p><b>Note:</b> It works only if the value of the parameter "network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 &amp; IPv6), and "network.ipv6_internet_port.type" is set to 1 (Static IP Address). If you change this parameter, the IP DECT phone will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Network-&gt;Basic-&gt;IPv6 Config-&gt;Static IP Address-&gt;IP Address</p> <p><b>Handset User Interface:</b> OK-&gt;Settings-&gt;System Settings-&gt;Network (default PIN: 0000)-&gt;IPv6-&gt;IP Address Type: Static-&gt;IP Address</p>		
<b>network.ipv6_prefix</b>	<b>Integer from 0 to 128</b>	<b>64</b>
<p><b>Description:</b> Configures the IPv6 prefix.</p> <p><b>Note:</b> It works only if the value of the parameter "network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 &amp; IPv6), and "network.ipv6_internet_port.type" is set to 1 (Static IP Address). If you change this parameter, the IP DECT phone will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Network-&gt;Basic-&gt;IPv6 Config-&gt;Static IP Address-&gt;IPv6 Prefix(0~128)</p> <p><b>Handset User Interface:</b> OK-&gt;Settings-&gt;System Settings-&gt;Network (default PIN: 0000)-&gt;IPv6-&gt;IP Address Type: Static-&gt;IPv6 Prefix</p>		

Parameters	Permitted Values	Default
<b>network.ipv6_internet_port.gateway</b>	IPv6 address	Blank
<p><b>Description:</b> Configures the IPv6 default gateway.</p> <p><b>Example:</b> network.ipv6_internet_port.gateway = 3036:1:1:c3c7:c11c:5447:23a6:255</p> <p><b>Note:</b> It works only if the value of the parameter "network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 &amp; IPv6), and "network.ipv6_internet_port.type" is set to 1 (Static IP Address). If you change this parameter, the IP DECT phone will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Network-&gt;Basic-&gt;IPv6 Config-&gt;Static IP Address-&gt;Gateway</p> <p><b>Handset User Interface:</b> OK-&gt;Settings-&gt;System Settings-&gt;Network (default PIN: 0000)-&gt;IPv6-&gt;IP Address Type: Static-&gt;Default Gateway</p>		
<b>network.ipv6_primary_dns</b>	IPv6 address	Blank
<p><b>Description:</b> Configures the primary IPv6 DNS server.</p> <p><b>Example:</b> network.ipv6_primary_dns = 3036:1:1:c3c7: c11c:5447:23a6:256</p> <p><b>Note:</b> It works only if the value of the parameter "network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 &amp; IPv6). In DHCP environment, you also need to make sure the value of the parameter "network.ipv6_static_dns_enable" is set to 1 (On). If you change this parameter, the IP DECT phone will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Network-&gt;Basic-&gt;IPv6 Config-&gt;Static IP Address-&gt;Primary DNS</p> <p><b>Handset User Interface:</b> For DHCP: OK-&gt;Settings-&gt;System Settings-&gt;Network (default PIN: 0000)-&gt;IPv6-&gt;IP Address Type: DHCP-&gt;DNS Type: Manual-&gt;Primary For Static IP address: OK-&gt;Settings-&gt;System Settings-&gt;Network (default PIN: 0000)-&gt;IPv6-&gt;IP Address Type: Static-&gt;Primary DNS</p>		

Parameters	Permitted Values	Default
network.ipv6_secondary_dns	IPv6 address	Blank
<p><b>Description:</b> Configures the secondary IPv6 DNS server.</p> <p><b>Example:</b> network.ipv6_secondary_dns = 2026:1234:1:1:c3c7:c11c:5447:23a6</p> <p><b>Note:</b> It works only if the value of the parameter "network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 &amp; IPv6). In DHCP environment, you also need to make sure the value of the parameter "network.ipv6_static_dns_enable" is set to 1 (On). If you change this parameter, the IP DECT phone will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Network-&gt;Basic-&gt;IPv6 Config-&gt;Static IP Address-&gt;Secondary DNS</p> <p><b>Handset User Interface:</b> For DHCP: OK-&gt;Settings-&gt;System Settings-&gt;Network (default PIN: 0000)-&gt;IPv6-&gt;IP Address Type: DHCP-&gt;DNS Type: Manual-&gt;Secondary DNS For Static IP address: OK-&gt;Settings-&gt;System Settings-&gt;Network (default PIN: 0000)-&gt;IPv6-&gt;IP Address Type: Static-&gt;Secondary DNS</p>		

**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.

- (Optional.) If you mark the **DHCP** radio box, you can configure the static DNS address in the corresponding fields.

The screenshot shows the 'Network' configuration page for a Yealink W52P/W56P phone. The 'Internet Port' is set to 'IPv6'. Under 'IPv4 Config', 'Static IP Address' is selected. Under 'IPv6 Config', 'DHCP' is selected. The 'IPv6 Static DNS' is set to 'On', with 'Primary DNS' as '3036:1:1:c3c7:c11c:5447:2' and 'Secondary DNS' as '2026:1234:1:1:c3c7:c11c:5'. A 'NOTE' sidebar on the right explains DHCP, Static IP Address, PPPoE, and IPv6 Support.

**Internet Port**  
Mode(IPv4/IPv6) IPv6

**IPv4 Config**

- DHCP
- Static IP Address
  - IP Address
  - Subnet Mask
  - Gateway
  - Static DNS  On  Off
    - Primary DNS
    - Secondary DNS
- PPPoE
  - User Name
  - Password

**IPv6 Config**

- DHCP
- Static IP Address
  - IP Address
  - IPv6 prefix(0~128) 64
  - Gateway
  - IPv6 Static DNS  On  Off
    - Primary DNS 3036:1:1:c3c7:c11c:5447:2
    - Secondary DNS 2026:1234:1:1:c3c7:c11c:5

**NOTE**

**DHCP**  
DHCP (Dynamic Host Configuration Protocol) is a network protocol used to dynamically allocate network parameters to IP phones.

**Static IP Address**  
Specifies the network parameters of IP phones manually.

**PPPoE**  
It allows users to share a common DSL connection to the Internet.

**IPv6 Support**  
IPv6 is developed to deal with the long-anticipated problem of IPv4 address exhaustion.

You can click here to get more guides.

Confirm Cancel

- If you mark the **Static IP Address** radio box, configure the IPv6 address and other configuration parameters in the corresponding fields.

The screenshot shows the Yealink W52P/W56P Network configuration interface. The 'Internet Port' dropdown is set to 'IPv6'. Under 'IPv4 Config', 'Static IP Address' is selected. Under 'IPv6 Config', 'Static IP Address' is also selected. The IPv6 fields are filled with: IP Address: 2026:1234:1:1:215:65ff:fe:1, IPv6 prefix: 64, Gateway: 3036:1:1:c3c7:c11c:5447:2, Primary DNS: 3036:1:1:c3c7:c11c:5447:2, and Secondary DNS: 2026:1234:1:1:c3c7:c11c:5-.





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

#### To configure IPv6 address assignment method via handset user interface:

1. Press **OK** to enter the main menu.
2. Select **Settings->System Settings->Network**.
3. Enter the system PIN (default: 0000), press the **Done** soft key.
4. Press **◀** or **▶** to select **IPv6** or **IPv4&IPv6** from the **IP Mode** field.
5. Press **▼** to select **IPv6**, and then press the **OK** soft key.
6. Press **◀** or **▶** to select **Static** from the **IP Address Type** field.
7. Enter the valid value in the **IP Address**, **IPv6 Prefix**, **Default Gateway**, **Primary DNS** and **Secondary DNS** field respectively.
8. Press the **Save** soft key to accept the change.

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

**To configure static DNS when DHCP is used via handset user interface:**

1. Press  to enter the main menu.
2. Select **Settings->System Settings->Network**.
3. Enter the system PIN (default: 0000), press the **Done** soft key.
4. Press  to select **IPv6**, and then press the **OK** soft key.
5. Press  or  to select **Manual** from the **DNS Type** field.
6. Enter the valid value in the **Primary DNS** and **Secondary DNS** field respectively.
7. Press the **Save** soft key to accept the change.

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

## Web Server Type

Web server type determines access protocol of the IP DECT phone's web user interface. The IP DECT 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 pages returned by the web server. Both HTTP and HTTPS port numbers are configurable.

### Procedure

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

<b>Configuration File</b>	y000000000025.cfg	Configure the web access type, HTTP port and HTTPS port. <b>Parameters:</b> wui.http_enable network.port.http wui.https_enable network.port.https
		Configure the quick login web user interface. <b>Parameters:</b> wui.quick_login
<b>Local</b>	Web User Interface	Configure the web access type, HTTP port and HTTPS port. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=network-adv&q=load

### Details of Configuration Parameters:

Parameters	Permitted Values	Default
<b>wui.http_enable</b>	<b>0 or 1</b>	<b>1</b>
<p><b>Description:</b> Enables or disables the user to access web user interface of the IP DECT phone using the HTTP protocol.</p> <p><b>0-Disabled</b> <b>1-Enabled</b></p> <p><b>Note:</b> If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Network-&gt;Advanced-&gt;Web Server-&gt;HTTP</p> <p><b>Handset User Interface:</b> None</p>		
<b>network.port.http</b>	<b>Integer from 1 to 65535</b>	<b>80</b>
<p><b>Description:</b> Configures the HTTP port for the user to access web user interface of the IP DECT phone using the HTTP protocol.</p> <p><b>Note:</b> If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Network-&gt;Advanced-&gt;Web Server-&gt;HTTP Port(1~65535)</p> <p><b>Handset User Interface:</b> None</p>		
<b>wui.https_enable</b>	<b>0 or 1</b>	<b>1</b>
<p><b>Description:</b> Enables or disables the user to access web user interface of the IP DECT phone using the HTTPS protocol.</p> <p><b>0-Disabled</b> <b>1-Enabled</b></p> <p><b>Note:</b> If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Network-&gt;Advanced-&gt;Web Server-&gt;HTTPS</p>		

Parameters	Permitted Values	Default
<b>Handset User Interface:</b> None		
<b>network.port.https</b>	<b>Integer from 1 to 65535</b>	<b>443</b>
<p><b>Description:</b> Configures the HTTPS port for the user to access web user interface of the IP DECT phone using the HTTPS protocol.</p> <p><b>Note:</b> If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Network-&gt;Advanced-&gt;Web Server-&gt;HTTPS Port(1~65535)</p> <p><b>Handset User Interface:</b> None</p>		
<b>wui.quick_login</b>	<b>0 or 1</b>	<b>0</b>
<p><b>Description:</b> Enables or disables the user to quick login the web user interface of the IP DECT phone using https://username:password@IP.</p> <p><b>Example:</b> https://admin:admin@192.168.0.1</p> <p><b>Web User Interface:</b> None</p> <p><b>Handset User Interface:</b> None</p>		

**To configure web server type via web user interface:**

1. Click on **Network->Advanced**.
2. Select the desired value from the pull-down list of **HTTP**.
3. Enter the desired HTTP port number in the **HTTP Port** field.  
The default HTTP port number is 80.
4. Select the desired value from the pull-down list of **HTTPS**.
5. Enter the desired HTTPS port number in the **HTTPS Port** field.



The default HTTPS port number is 443.

The screenshot shows the Yealink W52P/W56P web interface. The 'Network' tab is selected. The 'Web Server' section is highlighted with a red box. The settings for 'Web Server' are as follows:

Service	Status	Port
HTTP	Enabled	80
HTTPS	Enabled	443

Other visible settings include:

- LLDP:** Active, Enabled, Packet Interval (1-3600s): 60
- VLAN:** WAN Port: Active, Disabled; VID (1-4094): 1
- VPN:** Active, Disabled; Upload VPN Config: Upload

A 'NOTE' section on the right provides information about VLAN, NAT Traversal, and Quality of Service (QoS).

6. Click **Confirm** to accept the change.  
A dialog box pops up to prompt that settings will take effect after a reboot.
7. Click **OK** to reboot the 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 DECT phone is to insert tag with VLAN information to the packets generated by the IP DECT phone. When VLAN is properly configured for the ports (Internet port) on the IP DECT phone, the IP DECT 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.

In addition to manual configuration, the IP DECT phone also supports automatic discovery of VLAN via LLDP or DHCP. The assignment takes effect in this order: assignment via LLDP, manual configuration, then assignment via DHCP.

For more information on VLAN, refer to [VLAN Feature on Yealink IP phones](#).

## Procedure

VLAN assignment method can be configured using the configuration files or locally.

<b>Configuration File</b>	y00000000025.cfg	Configure the VLAN assignment method. <b>Parameter:</b> network.vlan.vlan_change.enable
---------------------------	------------------	---

## Details of Configuration Parameters:

Parameters	Permitted Values	Default
network.vlan.vlan_change.enable	0 or 1	0
<p><b>Description:</b> Enables or disables the IP DECT phone to obtain VLAN ID using lower priority of VLAN assignment method or disable VLAN feature when the IP DECT phone cannot obtain VLAN ID using the current VLAN assignment method.</p> <p><b>0</b>-Disabled <b>1</b>-Enabled</p> <p>The priority of each method is: LLDP&gt;Manual&gt;DHCP VLAN.</p> <p>If it is set to 1 (Enabled), the IP DECT phone will attempt to use the lower priority of VLAN assignment method when failing to obtain the VLAN ID using higher priority of VLAN assignment method. If all the methods are attempted, the phone will disable VLAN feature.</p> <p><b>Note:</b> If you change this parameter, the IP DECT phone will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> None</p> <p><b>Handset User Interface:</b> None</p>		

## LLDP

LLDP (Linker Layer Discovery Protocol) is a vendor-neutral Link Layer protocol, which allows IP DECT 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.

When LLDP feature is enabled on IP DECT phones, the IP DECT phones periodically

advertise their own information to the directly connected LLDP-enabled switch. The IP DECT phones can also receive LLDP packets from the connected switch. When the application type is “voice”, the IP DECT phones decide whether to update the VLAN configurations obtained from the LLDP packets. When the VLAN configurations on the IP DECT phones are different from the ones sent by the switch, the IP DECT phones perform an update and reboot. This allows the IP DECT phones to be plugged into any switch, obtain their VLAN IDs, and then start communications with the call control.

## Procedure

LLDP can be configured using the configuration files or locally.

<b>Configuration File</b>	y000000000025.cfg	Configure LLDP. <b>Parameters:</b> network.lldp.enable network.lldp.packet_interval
<b>Local</b>	Web User Interface	Configure LLDP. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=network-adv&q=load

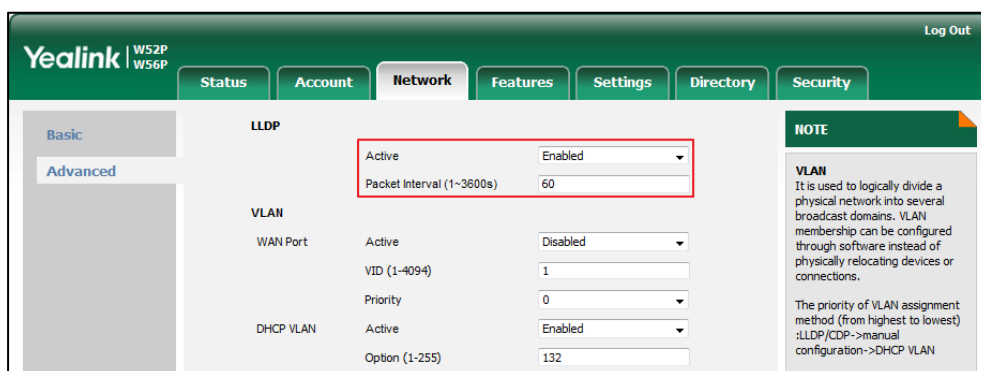
## Details of Configuration Parameters:

Parameters	Permitted Values	Default
<b>network.lldp.enable</b>	<b>0 or 1</b>	<b>1</b>
<p><b>Description:</b> Enables or disables the LLDP (Linker Layer Discovery Protocol) feature on the IP DECT phone.</p> <p><b>0-Disabled</b> <b>1-Enabled</b></p> <p><b>Note:</b> If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Network-&gt;Advanced-&gt;LLDP-&gt;Active</p> <p><b>Handset User Interface:</b> None</p>		
<b>network.lldp.packet_interval</b>	<b>Integer from 1 to 3600</b>	<b>60</b>
<p><b>Description:</b> Configures the interval (in seconds) for the IP DECT phone to send the LLDP (Linker</p>		

Parameters	Permitted Values	Default
Layer Discovery Protocol) request.		
<b>Note:</b> It works only if the value of the parameter "network.lldp.enable" is set to 1 (Enabled). If you change this parameter, the base station will reboot to make the change take effect.		
<b>Web User Interface:</b>		
Network->Advanced->LLDP->Packet Interval (1~3600s)		
<b>Handset User Interface:</b>		
None		

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 settings will take effect after a reboot.
5. Click **OK** to reboot the phone.

## Manual Configuration for VLAN

VLAN is disabled on IP DECT phones by default. You can configure VLAN for the Internet port manually. Before configuring VLAN on the IP DECT phone, you need to obtain the VLAN ID from your network administrator.

### Procedure

VLAN can be configured using the configuration files or locally.

<b>Configuration File</b>	y000000000025.cfg	Configure VLAN for the Internet port manually. <b>Parameters:</b>
---------------------------	-------------------	--

		network.vlan.internet_port_enable network.vlan.internet_port_vid network.vlan.internet_port_priority
<b>Local</b>	Web User Interface	Configure VLAN for the Internet port manually. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=network-adv&q=load

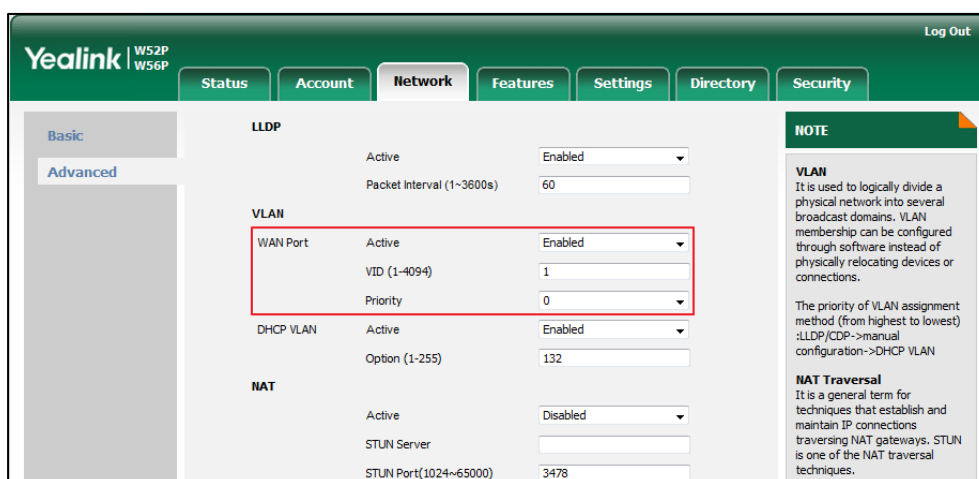
### Details of Configuration Parameters:

Parameters	Permitted Values	Default
network.vlan.internet_port_enable	0 or 1	0
<p><b>Description:</b> Enables or disables VLAN for the Internet (WAN) port. 0-Disabled 1-Enabled</p> <p><b>Note:</b> If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Network-&gt;Advanced-&gt;VLAN-&gt;WAN Port-&gt;Active</p> <p><b>Handset User Interface:</b> None</p>		
network.vlan.internet_port_vid	Integer from 1 to 4094	1
<p><b>Description:</b> Configures VLAN ID for the Internet (WAN) port.</p> <p><b>Note:</b> If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Network-&gt;Advanced-&gt;VLAN-&gt;WAN Port-&gt;VID(1-4094)</p> <p><b>Handset User Interface:</b> None</p>		
network.vlan.internet_port_priority	Integer from 0 to 7	0
<p><b>Description:</b></p>		

Parameters	Permitted Values	Default
<p>Configures VLAN priority for the Internet (WAN) port.</p> <p>7 is the highest priority, 0 is the lowest priority.</p> <p><b>Note:</b> If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b></p> <p>Network-&gt;Advanced-&gt;VLAN-&gt;WAN Port-&gt;Priority</p> <p><b>Handset User Interface:</b></p> <p>None</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 that the settings will take effect after a reboot.
6. Click **OK** to reboot the phone.

## DHCP VLAN

The IP DECT phones support VLAN discovery via DHCP. When the VLAN Discovery method is set to DHCP, the IP DECT 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

DHCP VLAN can be configured using the configuration files or locally.

<b>Configuration File</b>	y000000000025.cfg	Configure DHCP VLAN discovery feature. <b>Parameters:</b> network.vlan.dhcp_enable network.vlan.dhcp_option
<b>Local</b>	Web User Interface	Configure DHCP VLAN discovery feature. <b>Navigate to:</b> <a href="http://&lt;phoneIPAddress&gt;/servlet?p=network-adv&amp;q=load">http://&lt;phoneIPAddress&gt;/servlet?p=network-adv&amp;q=load</a>

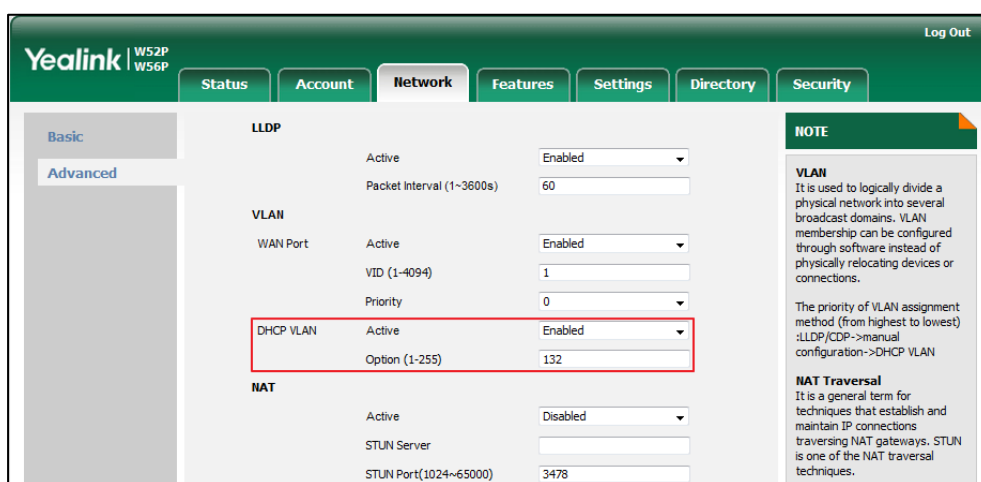
### Details of Configuration Parameters:

Parameters	Permitted Values	Default
network.vlan.dhcp_enable	0 or 1	1
<p><b>Description:</b> Enables or disables DHCP VLAN discovery feature on the IP DECT phone. 0-Disabled 1-Enabled</p> <p><b>Note:</b> If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Network-&gt;Advanced-&gt;VLAN-&gt;DHCP VLAN-&gt;Active</p> <p><b>Handset User Interface:</b> None</p>		
network.vlan.dhcp_option	Integer from 1 to 255	132
<p><b>Description:</b> Configures the DHCP option from which the IP DECT phone will obtain the VLAN settings. You can configure at most five DHCP options and separate them by commas.</p> <p><b>Note:</b> If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b></p>		

Parameters	Permitted Values	Default
Network->Advanced->VLAN->DHCP VLAN->Option (1-255)		
<b>Handset User Interface:</b>		
None		

To configure 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 (1-255)** 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 a reboot.
5. Click **OK** to reboot the phone.

## VPN

VPN (Virtual Private Network) is a secured private network connection built on top of public telecommunication infrastructure, such as the Internet. It has become more prevalent due to benefits of scalability, reliability, convenience and security. VPN provides remote offices or individual users with secure access to their organization's network.

### Types of VPN Access

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.

## VPN Technology

The IP DECT 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 network 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. The IP DECT phones use OpenVPN to achieve VPN feature. To prevent disclosure of private information, tunnel endpoints must authenticate each other before secure VPN tunnel is established. After VPN feature is configured properly on the IP DECT phone, the IP DECT phone acts as a VPN client and uses the certificates to authenticate the VPN server.

To use VPN, the compressed package of VPN-related files should be uploaded to the IP DECT phone in advance. The file format of the compressed package must be \*.tar. The related VPN files are: certificates (ca.crt and client.crt), key (client.key) and the configuration file (vpn.cnf) of the VPN client.

The following table lists the unified directories of the OpenVPN certificates and key in the configuration file (vpn.cnf) for Yealink IP DECT phones:

VPN files	Description	Unified Directories
ca.crt	CA certificate	/config/openvpn/keys/ca.crt
client.crt	Server certificate	/config/openvpn/keys/client.crt
client.key	Private key of the client	/config/openvpn/keys/client.key

For more information, refer to [OpenVPN Feature on Yealink IP phones](#).

## Procedure

VPN can be configured using the configuration files or locally.

<b>Configuration File</b>	y000000000025.cfg	Configure VPN feature and upload a TAR file to the IP DECT phone. <b>Parameters:</b> network.vpn_enable openvpn.url
<b>Local</b>	Web User Interface	Configure VPN feature and upload a TAR package to the IP DECT phone. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p

		=network-adv&q=load
--	--	---------------------

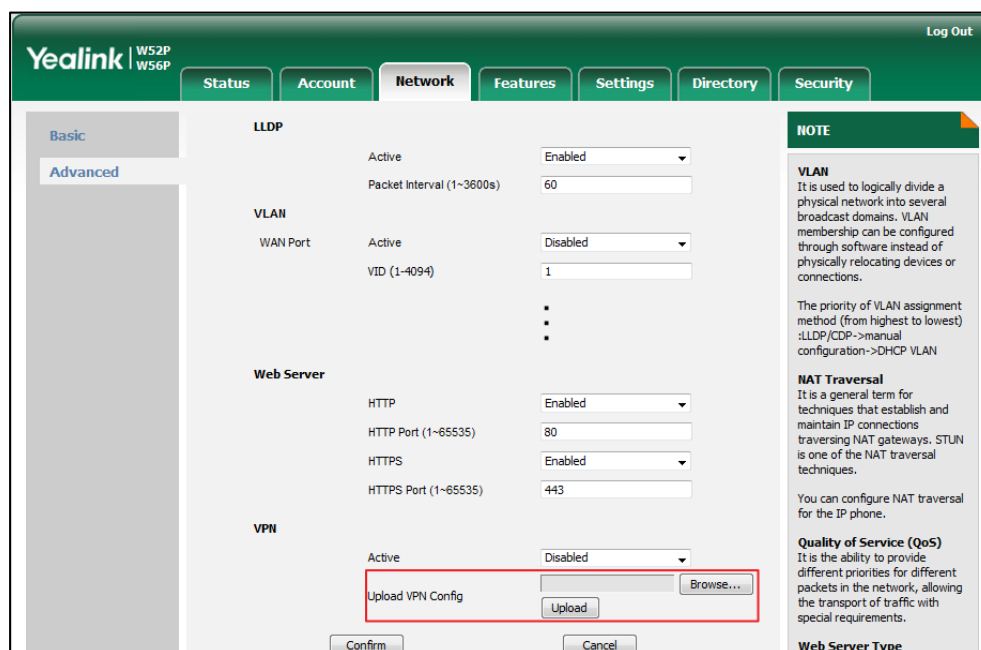
**Details of Configuration Parameters:**

Parameters	Permitted Values	Default
<b>network.vpn_enable</b>	<b>0 or 1</b>	<b>0</b>
<p><b>Description:</b>                      Enables or disables OpenVPN feature on the IP DECT phone.                      0-Disabled                      1-Enabled  <b>Note:</b> If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b>                      Network-&gt;Advanced-&gt;VPN-&gt;Active</p> <p><b>Handset User Interface:</b>                      None</p>		
<b>openvpn.url</b>	<b>URL within 511 characters</b>	<b>Blank</b>
<p><b>Description:</b>                      Configures the access URL of the *.tar file for OpenVPN.</p> <p><b>Example:</b>                      openvpn.url = http://192.168.10.25/OpenVPN.tar</p> <p><b>Web User Interface:</b>                      Network-&gt;Advanced-&gt;VPN-&gt;Upload VPN Config</p> <p><b>Handset User Interface:</b>                      None</p>		

**To upload a TAR file and configure VPN via web user interface:**

1. Click on **Network->Advanced**.
2. Click **Browse** to locate the TAR file from the local system.

- Click **Upload** to upload the TAR file.



The web user interface prompts the message “Import config...”.

- In the **VPN** block, select the desired value from the pull-down list of **Active**.
- Click **Confirm** to accept the change.  
A dialog box pops up to prompt that settings will take effect after a reboot.
- Click **OK** to reboot the phone.

## Quality of Service

Quality of Service (QoS) is the ability to provide different priorities for 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 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.

Four standard PHBs available to construct a DiffServ-enabled network and achieve QoS:

- **ClassSelector 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 (Bandwidth Allocations) 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 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. The IP DECT 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, or 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 DECT phones should be configured with a high transmission priority.

DSCPs for voice and SIP packets can be specified respectively.

### Note

For voice and SIP packets, the IP DECT phone obtains DSCP info from the network policy if LLDP feature is enabled, which takes precedence over manual settings. For more information on LLDP, refer to [LLDP](#) on page 62.

## Procedure

QoS can be configured using the configuration files or locally.

<b>Configuration File</b>	y00000000025.cfg	Configure the DSCPs for voice packets and SIP packets. <b>Parameters:</b> network.qos.rtpots network.qos.signalots
<b>Local</b>	Web User Interface	Configure the DSCPs for voice packets and SIP packets. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=network-adv&q=load

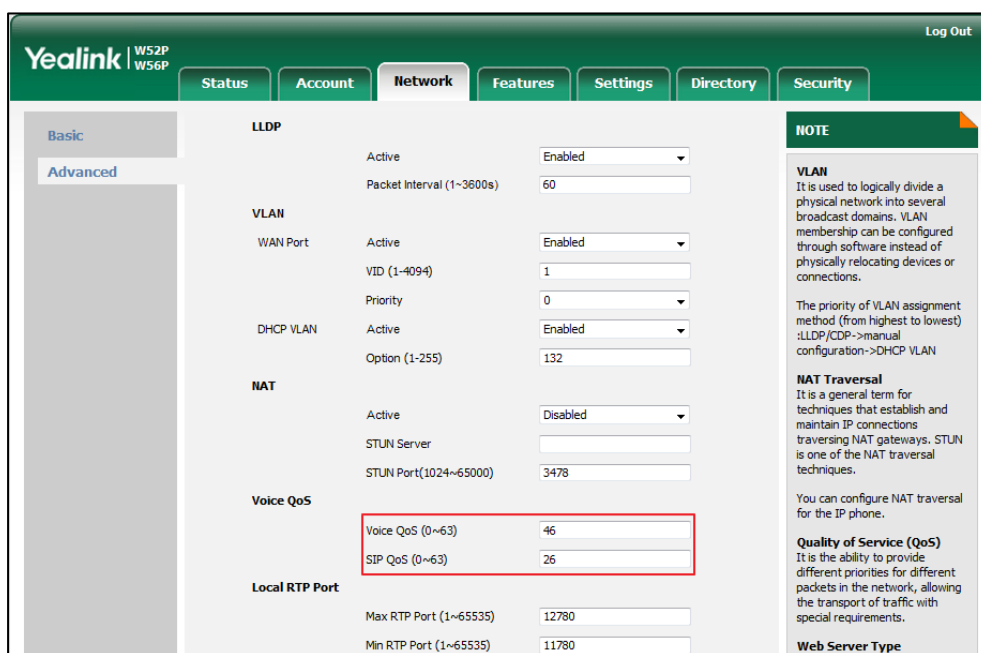
### Details of Configuration Parameters:

Parameters	Permitted Values	Default
network.qos.rtpots	Integer from 0 to 63	46
<p><b>Description:</b> Configures the DSCP (Differentiated Services Code Point) for voice packets. The default DSCP value for RTP packets is 46 (Expedited Forwarding).</p> <p><b>Note:</b> If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Network-&gt;Advanced-&gt;Voice QoS (0-63)</p> <p><b>Handset User Interface:</b> None</p>		
network.qos.signalots	Integer from 0 to 63	26
<p><b>Description:</b> Configures the DSCP (Differentiated Services Code Point) for SIP packets. The default DSCP value for SIP packets is 26 (Assured Forwarding).</p> <p><b>Note:</b> If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b></p>		

Parameters	Permitted Values	Default
Network->Advanced->SIP QoS (0-63)		
<b>Handset User Interface:</b>		
None		

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.



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

## 802.1X Authentication

IEEE802.1X 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/link 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 DECT phone that wishes to attach to the LAN or WLAN. With 802.1X port-based authentication, the IP DECT phone provides credentials, such as username 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 DECT phone is allowed to access resources

located on the protected side of the network.

The DECT phones support protocols EAP-MD5, EAP-TLS, EAP-PEAP/MSCHAPv2, EAP-TTLS/EAP-MSCHAPv2, EAP-PEAP/GTC, EAP-TTLS/EAP-GTC and EAP-FAST for 802.1X authentication.

For more information on 802.1X authentication, refer to [Yealink 802.1X Authentication](#).

## Procedure

802.1X authentication can be configured using the configuration files or locally.

<b>Configuration File</b>	y000000000025.cfg	Configure the 802.1X authentication. <b>Parameters:</b> network.802_1x.mode network.802_1x.identity network.802_1x.md5_password network.802_1x.client_cert_url
<b>Local</b>	Web User Interface	Configure the 802.1X authentication. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=network-adv&q=load

## Details of Configuration Parameters:

Parameters	Permitted Values	Default
network.802_1x.mode	0, 1, 2, 3, 4, 5, 6 or 7	0
<p><b>Description:</b> Configures the 802.1x authentication method.</p> <p><b>0</b>-Disabled <b>1</b>-EAP-MD5 <b>2</b>-EAP-TLS <b>3</b>-EAP-PEAP/MSCHAPv2 <b>4</b>-EAP-TTLS/EAP-MSCHAPv2 <b>5</b>-EAP-PEAP/GTC <b>6</b>-EAP-TTLS/EAP-GTC <b>7</b>-EAP-FAST</p> <p><b>Note:</b> If you change this parameter, the base station will reboot to make the change take effect.</p>		

Parameters	Permitted Values	Default
<p><b>Web User Interface:</b> Network-&gt;Advanced-&gt;802.1x-&gt;802.1x Mode</p> <p><b>Handset User Interface:</b> None</p>		
<b>network.802_1x.identity</b>	<b>String within 32 characters</b>	<b>Blank</b>
<p><b>Description:</b> Configures the user name for 802.1x authentication.</p> <p><b>Example:</b> network.802_1x.identity = admin</p> <p><b>Note:</b> It works only if the value of the parameter "network.802_1x.mode" is set to 1, 2, 3, 4, 5, 6 or 7. If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Network-&gt; Advanced-&gt;802.1x-&gt;Identity</p> <p><b>Handset User Interface:</b> None</p>		
<b>network.802_1x.md5_password</b>	<b>String within 32 characters</b>	<b>Blank</b>
<p><b>Description:</b> Configures the password for 802.1x authentication.</p> <p><b>Example:</b> network.802_1x.md5_password = admin123</p> <p><b>Note:</b> It works only if the value of the parameter "network.802_1x.mode" is set to 1, 2, 3, 4, 5, 6 or 7. If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Network-&gt;Advanced-&gt;802.1x-&gt;MD5 Password</p> <p><b>Handset User Interface:</b> None</p>		
<b>network.802_1x.root_cert_url</b>	<b>URL within 511 characters</b>	<b>Blank</b>
<p><b>Description:</b> Configures the access URL of the CA certificate.</p> <p><b>Example:</b> network.802_1x.root_cert_url = http://192.168.1.10/ca.pem</p>		



Parameters	Permitted Values	Default
<p><b>Note:</b> It works only if the value of the parameter “network.802_1x.mode” is set to 1, 2, 3, 4, 5, 6 or 7. The format of the certificate must be *.pem, *.crt, *.cer or *.der.</p> <p><b>Web User Interface:</b> Network-&gt;Advanced-&gt;802.1x-&gt;CA Certificate</p> <p><b>Handset User Interface:</b> None</p>		
network.802_1x.client_cert_url	URL within 511 characters	Blank
<p><b>Description:</b> Configures the access URL of the device certificate.</p> <p><b>Example:</b> network.802_1x.client_cert_url = http://192.168.1.10/client.pem</p> <p><b>Note:</b> It works only if the value of the parameter “network.802_1x.mode” is set to 2 (EAP-TLS). The format of the certificate must be *.pem.</p> <p><b>Web User Interface:</b> Network-&gt;Advanced-&gt;802.1x-&gt;Device Certificates</p> <p><b>Handset User Interface:</b> None</p>		

**To configure the 802.1X authentication via web user interface:**

1. Click on **Network->Advanced**.
2. In the **802.1x** block, select the desired protocol from the pull-down list of **802.1x Mode**.
  - a) If you select **EAP-MD5**:
    - 1) Enter the username for authentication in the **Identity** field.

- 2) Enter the password for authentication in the **MD5 Password** field.

The screenshot shows the Yealink configuration interface for W52P and W56P models. The 'Network' tab is selected, and the '802.1x' section is highlighted with a red box. The '802.1x Mode' is set to 'EAP-MD5', the 'Identity' is 'yealink', and the 'MD5 Password' field is filled with dots. Other sections include LLDP (Active: Enabled, Packet Interval: 60), CA Certificates, Device Certificates, and VPN (Active: Disabled). A 'NOTE' section on the right provides information about VLAN, NAT Traversal, and Quality of Service (QoS).

**b) If you select EAP-TLS:**

- 1) Enter the username for authentication in the **Identity** field.
- 2) Leave the **MD5 Password** field blank.
- 3) In the **CA Certificates** field, click **Browse** to select the desired CA certificate (\*.pem, \*.crt, \*.cer or \*.der) from your local system.
- 4) In the **Device Certificates** field, click **Browse** to select the desired client (\*.pem or \*.cer) certificate from your local system.

- 5) Click **Upload** to upload the certificates.

The screenshot shows the Yealink W52P/W56P Network Settings page. The 'Network' tab is selected, and the '802.1x' section is highlighted with a red box. The '802.1x' section includes the following fields:

- 802.1x Mode: EAP-TLS (dropdown menu)
- Identity: yealink (text input)
- MD5 Password: [masked with dots] (password input)
- CA Certificates: [Browse... button]
- Device Certificates: [Upload button]

The 'LLDP' section is also visible, with 'Active' set to 'Enabled' and 'Packet Interval (1~3600s)' set to '60'. The 'VPN' section is at the bottom, with 'Active' set to 'Disabled' and 'Upload VPN Config' button.

**NOTE**

**VLAN**  
It 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.

The priority of VLAN assignment method (from highest to lowest): LLDP/CDP->manual configuration->DHCP VLAN

**NAT Traversal**  
It is a general term for techniques that establish and maintain IP connections traversing NAT gateways. STUN is one of the NAT traversal techniques.

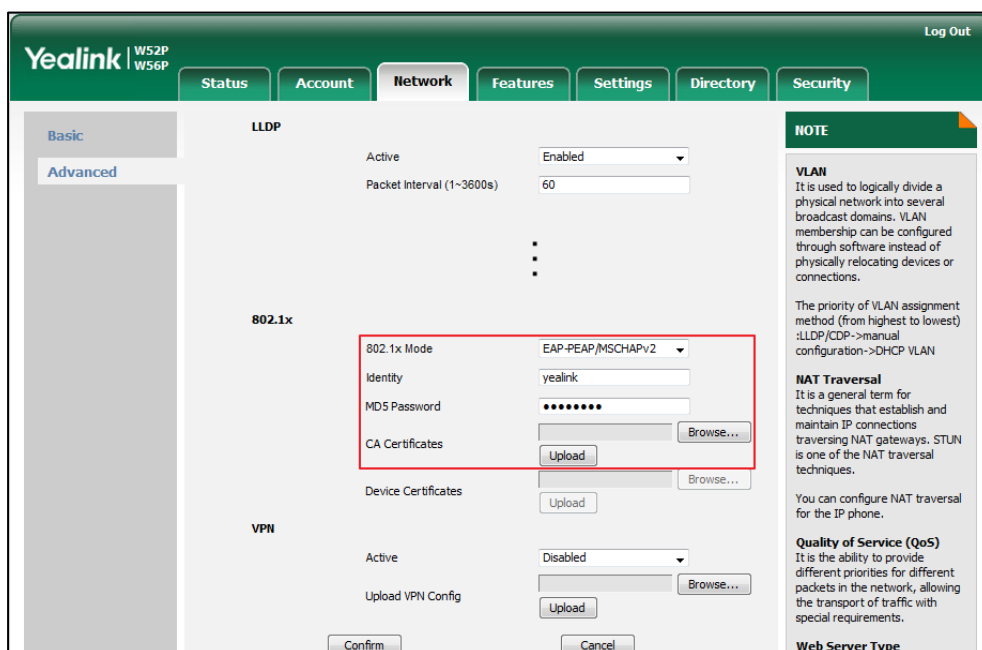
You can configure NAT traversal for the IP phone.

**Quality of Service (QoS)**  
It is the ability to provide different priorities for different packets in the network, allowing the transport of traffic with special requirements.

**Web Server Type**

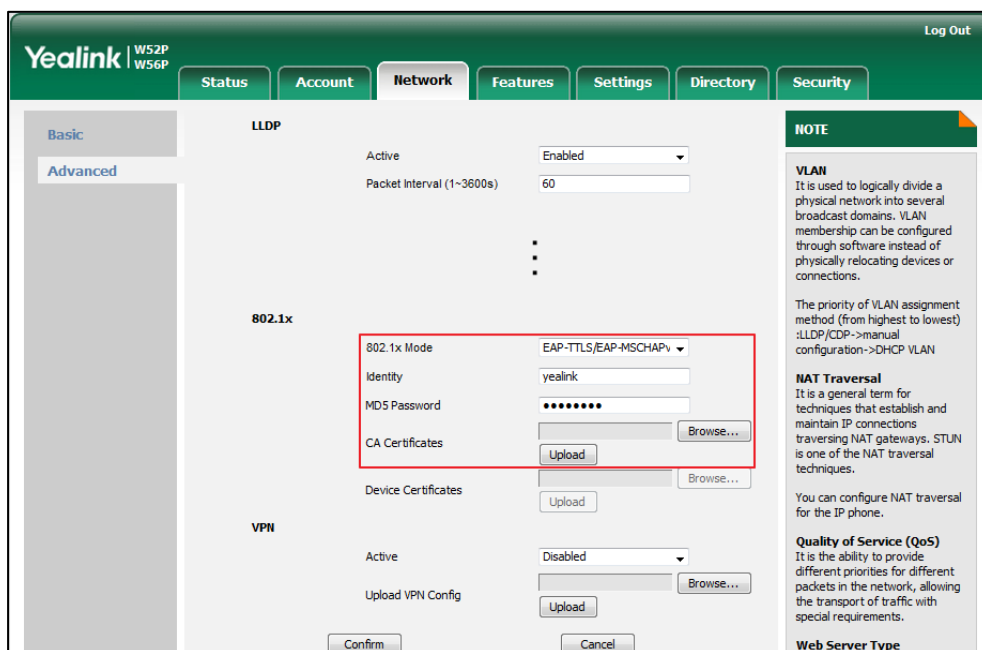
- c) If you select **EAP-PEAP/MSCHAPv2**:
  - 1) Enter the username for authentication in the **Identity** field.
  - 2) Enter the password for authentication in the **MD5 Password** field.
  - 3) In the **CA Certificates** field, click **Browse** to select the desired CA certificate (\*.pem, \*.crt, \*.cer or \*.der) from your local system.

- 4) Click **Upload** to upload the certificate.



- d) If you select **EAP-TTLS/EAP-MSCHAPv2**:

- 1) Enter the username 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 select the desired CA certificate (\*.pem, \*.crt, \*.cer or \*.der) from your local system.
- 4) Click **Upload** to upload the certificate.



- e) If you select **EAP-PEAP/GTC**:

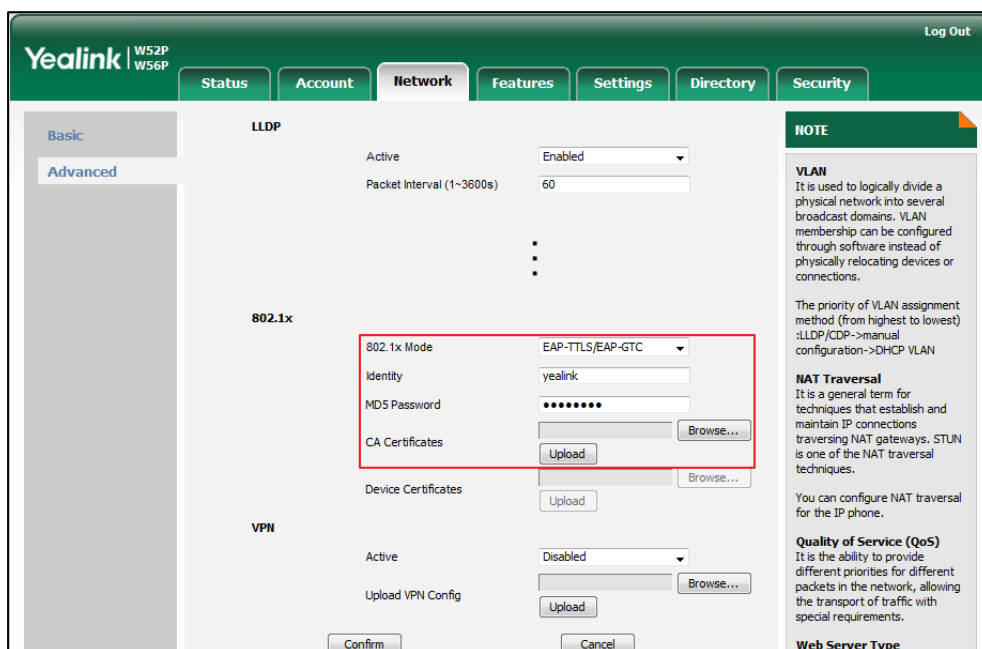
- 1) Enter the username for authentication in the **Identity** field.

- 2) Enter the password for authentication in the **MD5 Password** field.
- 3) In the **CA Certificates** field, click **Browse** to select the desired CA certificate (\*.pem, \*.crt, \*.cer or \*.der) from your local system.

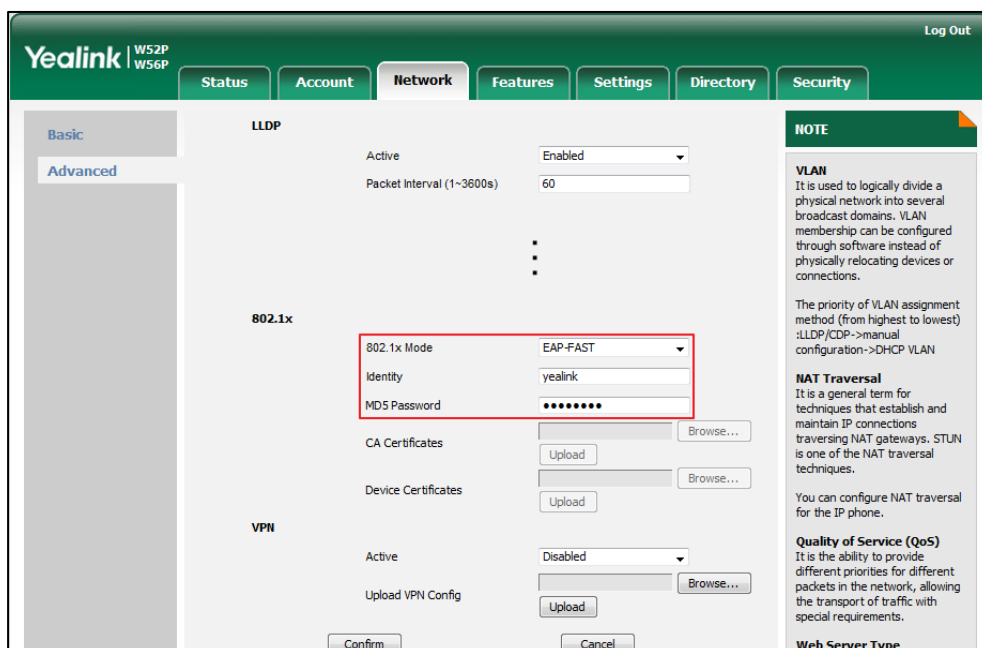
The screenshot shows the Yealink W52P/W56P web interface. The 'Network' tab is selected, and the '802.1x' configuration page is displayed. The '802.1x Mode' is set to 'EAP-PEAP/GTC'. The 'Identity' field contains 'yealink' and the 'MD5 Password' field contains a masked password. The 'CA Certificates' field has an 'Upload' button and a 'Browse...' button. The 'Device Certificates' field has an 'Upload' button and a 'Browse...' button. The 'VPN' section is also visible with 'Active' set to 'Disabled' and an 'Upload VPN Config' button. A 'NOTE' section on the right provides information about VLAN, NAT Traversal, and Quality of Service (QoS).

- 4) Click **Upload** to upload the certificate.
- f) If you select **EAP-TTLS/EAP-GTC**:
- 1) Enter the username 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 select the desired CA certificate (\*.pem, \*.crt, \*.cer or \*.der) from your local system.



- 4) Click **Upload** to upload the certificate.
- g) If you select **EAP-FAST**:
- 1) Enter the username for authentication in the **Identity** field.
  - 2) Enter the password for authentication in the **MD5 Password** field.



- 3) Click **Upload** to upload the certificate.
3. Click **Confirm** to accept the change.
- A dialog box pops up to prompt that settings will take effect after a reboot.

4. Click **OK** to reboot the phone.

## Upgrading Firmware

This section provides information on upgrading the IP DECT phone firmware. Two methods of firmware upgrade:

- Manually, from the local system for a single IP DECT phone.
- Automatically, from the provisioning server for a mass of phones.

### Note

You can download the latest firmware online:  
<http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage>.

Do not unplug the network and power cables when the IP DECT phone is upgrading firmware.

Before upgrading the handset, take notes as follow:

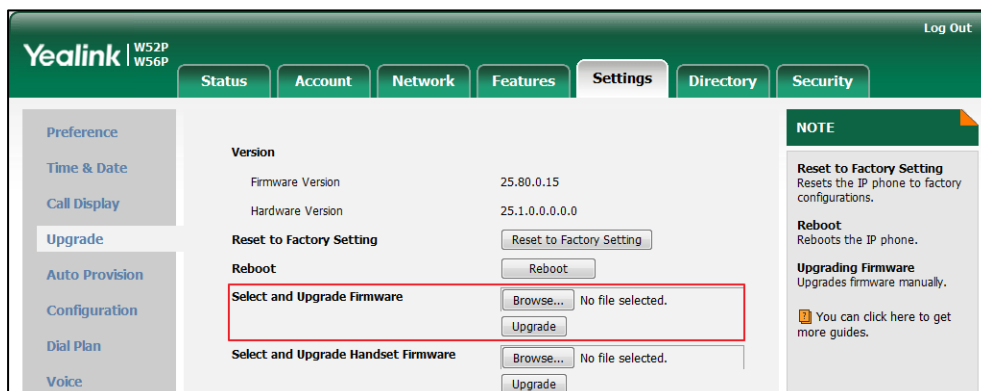
- All the registered handset (when the handset is in idle and the firmware version number is different with the upgrade one) will upgrade simultaneously.
- The handset battery power should not less than 40%.
- You cannot make a call (including emergency calls) during other handsets upgrading.
- If the firmware upgrade is started while the handset is on an internal call, the update will start after the call is completed.

## Upgrading Firmware via Web User Interface

To manually upgrade firmware via web user interface, you need to store firmware to your local system in advance.

**To upgrade base station firmware manually via web user interface:**

1. Click on **Settings->Upgrade**.
2. In the **Select and Upgrade Firmware** field, click **Browse** to locate the firmware file from your local system.

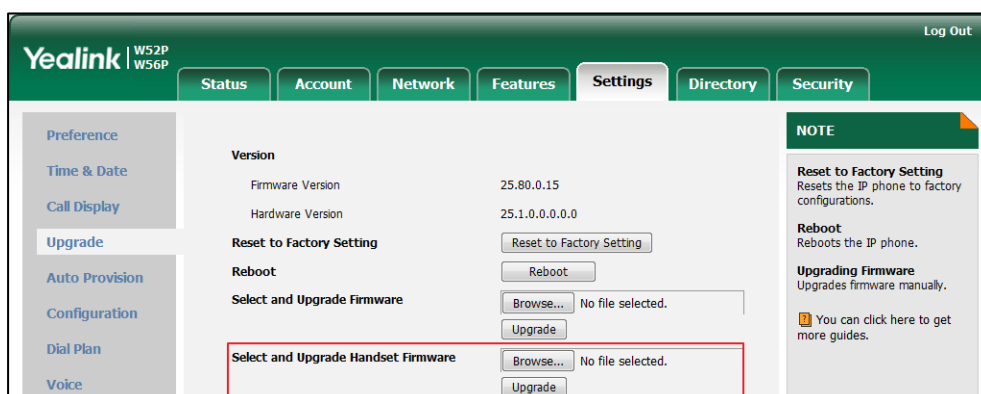


3. Click **Upgrade** to upgrade the firmware of the base station.  
The browser pops up the dialog box "Firmware of the SIP Phone will be updated. It will take 5 minutes to complete. Please don't power off!".
4. Click **OK** to confirm upgrading.  
The upgrading process will take a few minutes. The power indicator LED on the base station flashes during the firmware upgrading process.

You can also upgrade firmware for all the handsets that registered to the base station via web user interface.

**To upgrade handset firmware manually via web user interface:**

1. Click on **Settings->Upgrade**.
2. In the **Select and Upgrade Handset Firmware** field, click **Browse** to locate the firmware file from your local system.



3. Click **Upgrade** to upgrade the firmware of the all handset that registered to the base station.  
The browser pops up the dialog box "Firmware of the SIP Phone will be updated. It will take 5 minutes to complete. Please don't power off!".



- Click **OK** to confirm upgrading.

The handset LCD screen prompts "Upgrading...xx%" (xx ranges from 0 to 100).

If the display does not change after several minutes, try to moving the handset closer to the base station or check the network if disconnected.

**Note** Do not close and refresh the browser when the IP DECT phone is upgrading firmware via web user interface.

## Upgrading Firmware from the Provisioning Server

The IP DECT phones support using FTP, TFTP, HTTP and HTTPS protocols to download configuration files and firmware from the provisioning server, and then upgrade firmware automatically.

The IP DECT phones can download firmware stored on the provisioning server in one of two ways:

- Check for configuration files and then download firmware during startup.
- Automatically check for configuration files and then download firmware at a fixed interval or specific time.

Method of checking for configuration files is configurable.

### Procedure

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

<b>Configuration File</b>	y000000000025.cfg	Configure the way for the IP DECT phone to check for configuration files. <b>Parameters:</b> auto_provision.power_on auto_provision.repeat.enable auto_provision.repeat.minutes auto_provision.weekly.enable auto_provision.weekly.begin_time auto_provision.weekly.end_time auto_provision.weekly.dayofweek
		Specify the access URL of firmware for base station. <b>Parameter:</b> firmware.url

		<p>Specify the access URL of firmware for handset.</p> <p><b>Parameter:</b> over_the_air.url</p>
		<p>Configure the OTA upgrading feature for handset.</p> <p><b>Parameters:</b> over_the_air.base_trigger over_the_air.handset_tip</p>
<b>Local</b>	Web User Interface	<p>Configure the way for the IP DECT phone to check for configuration files.</p> <p><b>Navigate to:</b> http://&lt;phoneIPAddress&gt;/servlet?p=settings-autop&amp;q=load</p> <p>Specify the access URL of firmware for base station.</p> <p><b>Navigate to:</b> http://&lt;phoneIPAddress&gt;/servlet?p=settings-upgrade&amp;q=load</p> <p>Specify the access URL of firmware for handset.</p> <p><b>Navigate to:</b> http://&lt;phoneIPAddress&gt;/servlet?p=settings-upgrade&amp;q=load</p>

**Details of Configuration Parameters:**

Parameters	Permitted Values	Default
auto_provision.power_on	0 or 1	1
<p><b>Description:</b> Triggers the power on feature to on or off.</p> <p>0-Off 1-On</p> <p>If it is set to 1 (On), the IP DECT phone will perform an auto provisioning process when powered on.</p> <p><b>Web User Interface:</b> Settings-&gt;Auto Provision-&gt;Power On</p>		

Parameters	Permitted Values	Default
<b>Handset User Interface:</b> None		
<b>auto_provision.repeat.enable</b>	<b>0 or 1</b>	<b>0</b>
<p><b>Description:</b> Triggers the repeatedly feature to on or off. 0-Off 1-On If it is set to 1 (On), the IP DECT phone will perform an auto provisioning process repeatedly.</p> <p><b>Web User Interface:</b> Settings-&gt;Auto Provision-&gt;Repeatedly</p> <p><b>Handset User Interface:</b> None</p>		
<b>auto_provision.repeat.minutes</b>	<b>Integer from 1 to 43200</b>	<b>1440</b>
<p><b>Description:</b> Configures the interval (in minutes) for the IP DECT phone to perform an auto provisioning process repeatedly. <b>Note:</b> It works only if the value of the parameter "auto_provision.repeat.enable" is set to 1 (On).</p> <p><b>Web User Interface:</b> Settings-&gt;Auto Provision-&gt;Interval(Minutes)</p> <p><b>Handset User Interface:</b> None</p>		
<b>auto_provision.weekly.enable</b>	<b>0 or 1</b>	<b>0</b>
<p><b>Description:</b> Triggers the weekly feature to on or off. 0-Off 1-On If it is set to 1 (On), the IP DECT phone will perform an auto provisioning process weekly.</p> <p><b>Web User Interface:</b> Settings-&gt;Auto Provision-&gt;Weekly</p> <p><b>Handset User Interface:</b></p>		

Parameters	Permitted Values	Default
None		
<b>auto_provision.weekly.begin_time</b>	Time from 00:00 to 23:59	00:00
<p><b>Description:</b> Configures the begin time of the day for the IP DECT phone to perform an auto provisioning process weekly.</p> <p><b>Note:</b> It works only if the value of the parameter "auto_provision.weekly.enable" is set to 1 (On).</p> <p><b>Web User Interface:</b> Settings-&gt;Auto Provision-&gt;Time</p> <p><b>Handset User Interface:</b> None</p>		
<b>auto_provision.weekly.end_time</b>	Time from 00:00 to 23:59	00:00
<p><b>Description:</b> Configures the end time of the day for the IP DECT phone to perform an auto provisioning process weekly.</p> <p><b>Note:</b> It works only if the value of the parameter "auto_provision.weekly.enable" is set to 1 (On).</p> <p><b>Web User Interface:</b> Settings-&gt;Auto Provision-&gt;Time</p> <p><b>Handset User Interface:</b> None</p>		
<b>auto_provision.weekly.dayofweek</b>	0,1,2,3,4,5,6 or a combination of these digits	0123456
<p><b>Description:</b> Configures the days of the week for the IP DECT phone to perform an auto provisioning process weekly.</p> <p><b>0</b>-Sunday <b>1</b>-Monday <b>2</b>-Tuesday <b>3</b>-Wednesday <b>4</b>-Thursday <b>5</b>-Friday <b>6</b>-Saturday</p>		

Parameters	Permitted Values	Default
<p><b>Example:</b>  auto_provision.weekly.dayofweek = 01  It means the IP DECT phone will perform an auto provisioning process every Sunday and Monday.  <b>Note:</b> It works only if the value of the parameter "auto_provision.weekly.enable" is set to 1 (On).  <b>Web User Interface:</b>  Settings-&gt;Auto Provision-&gt;Day of Week  <b>Handset User Interface:</b>  None</p>		
firmware.url	URL within 511 characters	Blank
<p><b>Description:</b>  Configures the access URL of the base station firmware file.  <b>Example:</b>  firmware.url = http://192.168.1.20/25.80.0.1.rom  <b>Note:</b> If you change this parameter, the base station will reboot to make the change take effect.  <b>Web User Interface:</b>  Settings-&gt;Upgrade-&gt;Select and Upgrade Firmware  <b>Handset User Interface:</b>  None</p>		
over_the_air.url	URL within 511 characters	Blank
<p><b>Description:</b>  Configures the access URL of the handset firmware file.  <b>Example:</b>  over_the_air.url = http://192.168.1.20/61.80.0.1.rom  <b>Note:</b> If you change this parameter, the base station will reboot to make the change take effect.  <b>Web User Interface:</b>  Settings-&gt;Upgrade-&gt;Select and Upgrade Handset Firmware  <b>Handset User Interface:</b>  None</p>		
over_the_air.base_trigger	0 or 1	0

Parameters	Permitted Values	Default
<p><b>Description:</b>                      Enables or disables to upgrade the firmware compulsively from the provisioning sever.</p> <p><b>0-Disabled</b>  <b>1-Enabled</b></p> <p>If it is set to 0 (Disabled) and the value of the parameter "over_the_air.handset_tip" is set to 1 (Enabled), it will pop-up a tip on the handset to notify the user to confirm upgrading the firmware or not. If the value of the parameter "over_the_air.handset_tip" is set to 0, you may go to <b>Settings-&gt;Upgrade Firmware</b> on handset to trigger the upgrading manually.</p> <p>If it is set to 1 (Enabled), it will upgrade the firmware compulsively without pop-up a tip on the handset.</p> <p><b>Web User Interface:</b>                      None</p> <p><b>Handset User Interface:</b>                      None</p>		
<b>over_the_air.handset_tip</b>	<b>0 or 1</b>	<b>1</b>
<p><b>Description:</b>                      Enables or disables to pop-up a tip when upgrading the firmware from the provisioning server.</p> <p><b>0-Disabled</b>  <b>1-Enabled</b></p> <p><b>Note:</b> It works only if the value of the parameter "over_the_air.base_trigger" is set to 0 (Disabled).</p> <p><b>Web User Interface:</b>                      None</p> <p><b>Handset User Interface:</b>                      None</p>		

To configure the way for the IP DECT phone to check for configuration files via web user interface:

1. Click on **Settings->Auto Provision**.
2. Make the desired change.

The screenshot displays the Yealink W52P/W56P web interface. The top navigation bar includes 'Status', 'Account', 'Network', 'Features', 'Settings', 'Directory', and 'Security'. The 'Settings' tab is active, and the 'Auto Provision' sub-tab is selected in the left sidebar. The main content area shows the 'Auto Provision' configuration page with the following settings:

- PNP Active:  On  Off
- DHCP Active:  On  Off
- Custom Option(128~254): [Empty text box]
- DHCP Option Value: yealink
- Server URL: [Empty text box]
- User Name: [Empty text box]
- Password: [Masked text box]
- Attempt Expired Time(s): 5
- Common AES Key: [Masked text box]
- MAC-Oriented AES Key: [Masked text box]
- Power On:  On  Off
- Repeatedly:  On  Off
- Interval(Minutes): 1440
- Weekly:  On  Off
- Time: 00 : 00 -- 00 : 00
- Day of Week:  Sunday,  Monday,  Tuesday,  Wednesday,  Thursday,  Friday,  Saturday

At the bottom of the settings area are 'Confirm' and 'Cancel' buttons. A 'NOTE' box on the right side contains the following text:

**NOTE**  
**Auto Provision**  
The IP phone can interoperate with provisioning server using auto provisioning for deploying the IP phones.  
When the IP phone triggers to perform auto provisioning, it will request to download the configuration files from the provisioning server. During the auto provisioning process, the IP phone will download and update configuration files to the phone flash.  
You can click here to get more guides.

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

When the "Power On" is set to **On**, the IP DECT phone will check configuration files stored on the provisioning server during startup and then will download firmware from the server.





## Configuring the Handset

This section provides information on configuring some features for the handset.

### Handset Power Indicator LED

Handset power indicator LED indicates power status and phone status. There are four configuration options for handset 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 handset receives an incoming call.

#### Voice Mail Power Light Flash

Voice Mail Power Light Flash allows the power indicator LED to flash when the handset receives a voice mail.

#### Miss Call Power Light Flash

Miss Call Power Light flash allows the power indicator LED to flash when the handset misses a call.

#### Procedure

The power indicator LED of handset can be configured using the configuration files or locally.

<b>Configuration File</b>	y000000000025.cfg	Configure the handset power indicator LED. <b>Parameters:</b> phone_setting.common_power_led_enable phone_setting.ring_power_led_flash_enable phone_setting.mail_power_led_flash_enable phone_setting.missed_call_power_led_flash.enable
---------------------------	-------------------	---

<b>Local</b>	Web User Interface	<b>Navigate to:</b> <a href="http://&lt;phoneIPAddress&gt;/servlet?p=features-poweredled&amp;q=load">http://&lt;phoneIPAddress&gt;/servlet?p=features-poweredled&amp;q=load</a>
--------------	--------------------	--

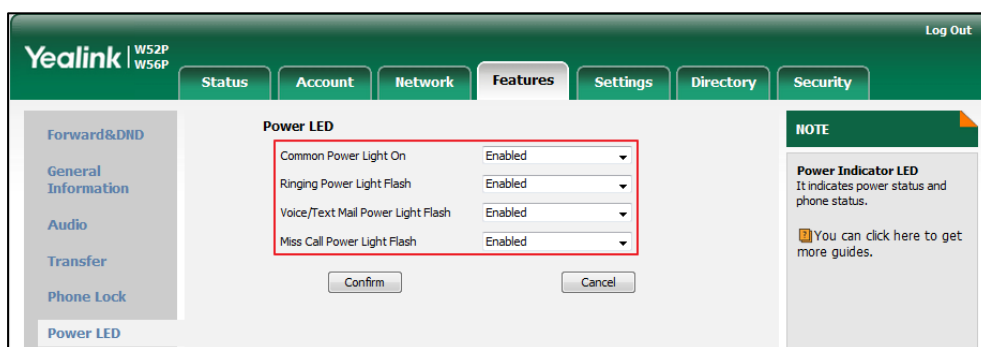
**Details of Configuration Parameters:**

Parameters	Permitted Values	Default
<b>phone_setting.common_power_led_enable</b>	<b>0 or 1</b>	<b>0</b>
<p><b>Description:</b>                      Enables or disables the handset power indicator LED to be turned on when the handset is idle.</p> <p><b>0-Disabled</b> (handset power indicator LED is off)  <b>1-Enabled</b> (handset power indicator LED is solid red)</p> <p><b>Web User Interface:</b>                      Features-&gt;Power LED-&gt;Common Power Light On</p> <p><b>Handset User Interface:</b>                      None</p>		
<b>phone_setting.ring_power_led_flash_enable</b>	<b>0 or 1</b>	<b>1</b>
<p><b>Description:</b>                      Enables or disables the handset power indicator LED to flash when the handset receives an incoming call.</p> <p><b>0-Disabled</b> (handset power indicator LED does not flash)  <b>1-Enabled</b> (handset power indicator LED fast flashes (300ms) red)</p> <p><b>Web User Interface:</b>                      Features-&gt;Power LED-&gt;Ringing Power Light Flash</p> <p><b>Handset User Interface:</b>                      None</p>		
<b>phone_setting.mail_power_led_flash_enable</b>	<b>0 or 1</b>	<b>1</b>
<p><b>Description:</b>                      Enables or disables the handset power indicator LED to flash when the handset receives a voice mail.</p> <p><b>0-Disabled</b> (handset power indicator LED does not flash)  <b>1-Enabled</b> (handset power indicator LED slow flashes (1000ms) red)</p> <p><b>Web User Interface:</b>                      Features-&gt;Power LED-&gt;Voice/Text Mail Power Light Flash</p>		

Parameters	Permitted Values	Default
<b>Handset User Interface:</b> None		
<b>phone_setting.missed_call_power_led_flash.enable</b>	<b>0 or 1</b>	<b>1</b>
<p><b>Description:</b> Enables or disables the handset power indicator LED to flash when the handset misses a call.</p> <p><b>0-Disabled</b> (handset power indicator LED does not flash) <b>1-Enabled</b> (handset power indicator LED slow flashes (1000ms) red)</p> <p><b>Web User Interface:</b> Features-&gt;Power LED-&gt;Miss Call Power Light Flash</p> <p><b>Handset User Interface:</b> None</p>		

To configure the handset 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 **Ringing 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 **Miss Call Power Light Flash**.



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

## Keypad Light

You can enable the keypad light to make the keypad light up when any key is pressed. This helps you distinguish keys from each other in a dark environment.

## Procedure

The keypad's light of handset can be configured using the configuration files or locally.

<b>Configuration File</b>	y000000000025.cfg	Configure the keypad light. <b>Parameters:</b> custom.handset.keypad_light.enable
<b>Local</b>	Handset User Interface	Configure the keypad light.

### Details of Configuration Parameters:

Parameters	Permitted Values	Default
custom.handset.keypad_light.enable	0 or 1	1
<p><b>Description:</b> Enables or disables the handset to turn on the keypad light (digital key, # key, * key, Redirect key and Mute key) when any key is pressed.</p> <p>0-Disabled 1-Enabled</p> <p><b>Note:</b> It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled).</p> <p><b>Web User Interface:</b> None</p> <p><b>Handset User Interface:</b> OK-&gt;Settings-&gt;Display-&gt;Keypad Light</p>		

### To configure keypad light via the handset:

1. Press **OK** to enter the main menu.
2. Select **Settings->Display->Keypad Light**.
3. Press the **Change** soft key to check or uncheck the **Keypad Light** checkbox.

## Advisory Tone

Advisory tones are acoustic signals of your handset, which inform you of different actions and states. The following advisory tones can be configured independently of each other:

- **Keypad Tone:** plays when a user presses any key of the keypad.
- **Confirmation:** plays when a user saves settings or places the handset in the charger cradle.
- **Low Battery:** plays when the capacity of the batteries is low and the handset requires charging.

### Procedure

Advisory tone can be configured using the configuration files or locally.

Configuration File	y000000000025.cfg	Configure keypad's tone on the handset. <b>Parameter:</b> custom.handset.keypad_tone.enable
		Configure confirmation's tone on the handset. <b>Parameter:</b> custom.handset.confirmation_tone.enable
		Configure low battery tone on the handset. <b>Parameter:</b> custom.handset.low_battery_tone.enable
Local	Handset User Interface	Configure keypad's tone on the handset. Configure confirmation's tone on the handset. Configure low battery tone on the handset.

**Details of Configuration Parameters:**

Parameters	Permitted Values	Default
<b>custom.handset.keypad_tone.enable</b>	<b>0 or 1</b>	<b>1</b>
<p><b>Description:</b>                      Enables or disables the handset to play a tone when any key is pressed.                      0-Disabled                      1-Enabled</p> <p><b>Note:</b> It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled) and the silent mode is off.</p> <p><b>Web User Interface:</b>                      None</p> <p><b>Handset User Interface:</b>                      OK-&gt;Settings-&gt;Audio-&gt;Advisory Tones-&gt;Keypad Tone</p>		
<b>custom.handset.confirmation_tone.enable</b>	<b>0 or 1</b>	<b>1</b>
<p><b>Description:</b>                      Enables or disables the handset to play a tone when a user saves settings or places the handset in the charger cradle.                      0-Disabled                      1-Enabled</p> <p><b>Note:</b> It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled) and the silent mode is off.</p> <p><b>Web User Interface:</b>                      None</p> <p><b>Handset User Interface:</b>                      OK-&gt;Settings-&gt;Audio-&gt;Advisory Tones-&gt;Confirmation</p>		
<b>custom.handset.low_battery_tone.enable</b>	<b>0 or 1</b>	<b>1</b>
<p><b>Description:</b>                      Enables or disables the handset to play a tone when the capacity of battery is low.                      0-Disabled                      1-Enabled</p>		

Parameters	Permitted Values	Default
<p><b>Note:</b> It works only if the value of the parameter “auto_provision.handset_configured.enable” is set to 1 (Enabled) and the silent mode is off.</p> <p><b>Web User Interface:</b> None</p> <p><b>Handset User Interface:</b> OK-&gt;Settings-&gt;Audio-&gt;Advisory Tones-&gt;Low Battery</p>		

#### To configure advisory tone via handset user interface:

1. Press **OK** to enter the main menu.
2. Select **Settings->Audio->Advisory Tones**.
3. Press **◀** or **▶** to select the desired value from the **Keypad Tone** field.
4. Press **◀** or **▶** to select the desired value from the **Confirmation** field.
5. Press **◀** or **▶** to select the desired value from the **Low Battery** field.
6. Press the **Save** soft key to accept the change or the **Back** soft key to cancel.

## Backlight

Handset backlight status in the charging state or out of the charging state can be configured independently of each other. If enabled, the backlight is always on. Otherwise, the backlight is turned off after the handset is idle for a period of time. But the backlight is automatically turned on when an incoming call arrives, a key is pressed or the status of handset changes. You can disable the backlight to save power.

### Procedure

Backlight can be configured using the configuration files or locally.

<b>Configuration File</b>	y000000000025.cfg	Configure the back light of the handset LCD screen. <b>Parameters:</b> custom.handset.backlight_in_charger.enable custom.handset.backlight_out_of_charger.enable
<b>Local</b>	Handset User Interface	Configure the backlight of the handset screen.

### Details of Configuration Parameters:

Parameters	Permitted Values	Default
<b>custom.handset.backlight_in_charger.enable</b>	<b>0 or 1</b>	<b>1</b>
<p><b>Description:</b>                      Enables or disables the handset to always turn on the backlight when it is in the charging state.</p> <p><b>0-Disabled</b>  <b>1-Enabled</b></p> <p>If it is set to 0 (Disabled), the backlight will be turned off after the handset is idle for a period of time when it is in the charging state.</p> <p><b>Note:</b> It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled).</p> <p><b>Web User Interface:</b>                      None</p> <p><b>Handset User Interface:</b>                      OK-&gt;Settings-&gt;Display-&gt;Display Backlight-&gt;In Charger</p>		
<b>custom.handset.backlight_out_of_charger.enable</b>	<b>0 or 1</b>	<b>0</b>
<p><b>Description:</b>                      Enables or disables the handset to always turn on the backlight when it is not in the charging state.</p> <p><b>0-Disabled</b>  <b>1-Enabled</b></p> <p>If it is set to 0 (Disabled), the backlight will be turned off after the handset is idle for a period of time when it is not in the charging state.</p> <p><b>Note:</b> It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled).</p> <p><b>Web User Interface:</b>                      None</p> <p><b>Handset User Interface:</b>                      OK-&gt;Settings-&gt;Display-&gt;Display Backlight-&gt;Out Of Charger</p>		

#### To configure the backlight via the handset:

1. Press **OK** to enter the main menu.
2. Select **Settings->Display->Display Backlight**.
3. Press **◀** or **▶** to select the desired value from the **In Charger** field.



4. Press ◀ or ▶ to select the desired value from the **Out Of Charger** field.
5. Press the **Save** soft key to accept the change or the **Back** soft key to cancel.

## Wallpaper

Wallpaper is an image used as the background of the handset idle screen. Users can select an image from handset's built-in background.

### Procedure


Wallpaper can be configured using the configuration files or locally.

<b>Configuration File</b>	y000000000025.cfg	Configure the wallpaper displayed on the handset LCD screen. <b>Parameters:</b> custom.handset.wallpaper
<b>Local</b>	Handset User Interface	Configure the wallpaper of the handset screen.

### Details of Configuration Parameters:

Parameters	Permitted Values	Default
custom.handset.wallpaper	Integer from 1 to 5	1
<p><b>Description:</b> Configures the wallpaper displayed on the handset LCD screen. It will take effect on all handsets that are registered on the base station.</p> <p>1-Wallpaper1 2-Wallpaper2 3-Wallpaper3 4-Wallpaper4 5-Wallpaper5</p> <p><b>Note:</b> It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled).</p> <p><b>Web User Interface:</b> None</p> <p><b>Handset User Interface:</b> OK-&gt;Settings-&gt;Display-&gt;Wallpaper</p>		

**To change the wallpaper for a specific handset via handset user interface:**

1. Press  to enter the main menu.
2. Select **Settings->Display->Wallpaper**.
3. Press **◀** or **▶** to select the desired image.
4. Press **Save** soft key to accept the change.

The handset displays the corresponding wallpaper on the idle screen.

## Screen Saver

The screen saver of the handset is designed to protect your LCD screen by filling it with an analog clock. You can enable the screen saver to protect the LCD screen if you do not use your handset for a long time. When the screen saver is enabled, an analog clock will be activated and appear on the LCD screen if the handset is idle for approximately 10 seconds.

### Procedure

Screen saver can be configured using the configuration files or locally.

<b>Configuration File</b>	y000000000025.cfg	Configure the screensaver of the handset LCD screen. <b>Parameters:</b> custom.handset.screen_saver.enable
<b>Local</b>	Handset User Interface	Configure the screen saver of the handset LCD screen.

### Details of Configuration Parameters:

Parameters	Permitted Values	Default
<b>custom.handset.screen_saver.enable</b>	<b>0 or 1</b>	<b>1</b>
<p><b>Description:</b> Enables or disables screen saver feature.</p> <p><b>0-Disabled</b> <b>1-Enabled</b></p> <p>If it is set to 1 (Enabled), an analog clock will be activated and appear on the LCD screen if no user activity is sensed for approximately 10 seconds. It will take effect on all handset that registered on the base station.</p> <p><b>Note:</b> It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled).</p> <p><b>Web User Interface:</b></p>		

None

**Handset User Interface:**

OK->Settings->Display->Screen Saver

**To configure screen saver for a specific handset via the handset:**

1. Press **OK** to enter the main menu.
2. Select **Settings->Display->Screen Saver**.
3. Press the **Change** soft key to check or uncheck the **Screen Saver** checkbox.

## Handset Name

The handset will be assigned a name by default if successfully registered to the base station. You can personalize the handset name.

### Procedure

Handset name can be configured using the configuration files or locally.

<b>Configuration File</b>	y000000000025.cfg	Configure the handset name of the handset LCD screen. <b>Parameters:</b> handset.X.name
<b>Local</b>	Web User Interface	Configure the handset name of the handset LCD screen. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?parameter=account-handsetname&q=load
	Handset User Interface	Configure the handset name of the handset LCD screen.

### Details of Configuration Parameters:

Parameters	Permitted Values	Default
<b>handset.X.name</b> (X ranges from 1 to 5)	<b>String within 24 characters</b>	<b>Refer to the following content</b>
<p><b>Description:</b> Configures the name of handset X. It will be displayed on the handset LCD screen.</p> <p><b>Default:</b> The handset name for handset 1 is Handset1.</p>		

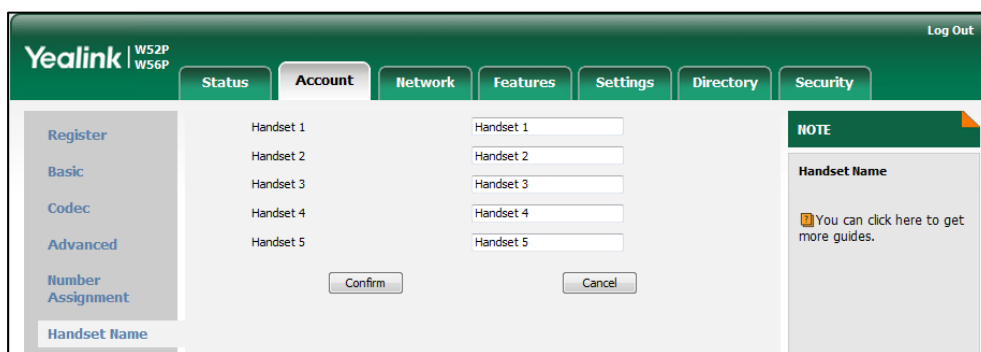
The handset name for handset 2 is Handset2.  
 The handset name for handset 3 is Handset3.  
 The handset name for handset 4 is Handset4.  
 The handset name for handset 5 is Handset5.

**Web User Interface:**  
 Account->Handset Name->Handset X (X range from 1 to 5)

**Handset User Interface:**  
 OK->Settings->Handset Name

**To rename the handset via web user interface:**

1. Click on **Account->Handset Name**.
2. Edit the current name in the **HandsetX** (X is from 1 to 5) field.



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

**To rename the handset via the handset:**

1. Press **OK** to enter the main menu.
2. Select **Settings->Handset Name**.
3. Edit the current name in the **Rename** field.  
 You can press **\*#** to enter special characters and press **# a** to switch among input modes.
4. Press the **Save** soft key to accept the change or **Red Phone** to cancel.

## Language

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

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

Handset	Web User Interface
English	English

Handset	Web User Interface
French	French
Deutsch	German
Italian	Italian
Polish	Polish
Portuguese	Portuguese
Spanish	Spanish
Turkish	Turkish
Swedish	Russian
Russian	

## Loading Language Packs

Languages available for selection depend on language packs currently loaded to the IP DECT phone. You can customize the translation of the existing language on the web user interface. You can also make new languages (not included in the available language list) available for use on the web user interface by loading language packs to the IP DECT phone. Language packs can only be loaded using configuration files.

You can ask the distributor or Yealink FAE for language packs. You can also obtain the language packs online:

<http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage>. For more information on obtaining the language packs, refer to [Obtaining Configuration Files and Resource Files](#) on page 15.

### Note

To modify translation of an existing language, do not rename the language file.

The new added language must be supported by the font library on the IP DECT phone. If the characters in the custom language file are not supported by the DECT phone, the IP DECT phone will display “?” instead.

## Customizing a Language for Web User Interface

The following table lists available languages and associated language packs for the web user interface:

Available Language	Associated Language Pack
English	1.English.js
French	2.French.js
German	3.German.js

Available Language	Associated Language Pack
Italian	4.Italian.js
Polish	5.Polish.js
Portuguese	6.Portuguese.js
Spanish	7.Spanish.js
Turkish	8.Turkish.js
Russian	9.Russian.js

When adding a new language pack for the web user interface, the language pack must be formatted as "Y.name.js" (Y starts from 10, "name" is replaced with the language name). If the language name is the same as the existing one, the existing language file will be overridden by the new uploaded one. We recommend that the name of the new language file should not be the same as the existing languages.

**To customize a language file:**

1. Open the desired language template file (e.g., 1.English.js) using an ASCII editor.
2. Modify the characters within the double quotation marks on the right of the colon. Don't modify the translation item on the left of the colon.

The following shows a portion of the language pack "1.English.js" for the web user interface:

```

1 var _objTrans =
2 {
3
4 " Call Number Filter":"Call Number Filter",
5 " Distinctive Ring Tones":"Distinctive Ring Tones",
6 " Do you want to reboot ?":"Do you want to reboot?",
7 "(800*480)":"(800*480)",
8 "0":"0",
9 "1":"1",
10 "10min":"10min",
11 "1min":"1min",
12 "2":"2",
13 "2min":"2min",
14 "3":"3",
15 "30min":"30min",
16 "4":"4",
17 "404 (Not found)":"404 (Not Found)",
18 "480 (Temporarily not available)":"480 (Temporarily Not Available)",
19 "486 (Busy here)":"486 (Busy Here)",
20 "5":"5",
21 "5min":"5min",
22 "6":"6",
23 "603 (Decline)":"603 (Decline)",
24 "ACD Auto Available Timer(0~120s)":"ACD Auto Available Timer(0~120s)",
25 "ACD Auto Available":"ACD Auto Available",

```

3. Save the language file and place it to the provisioning server (e.g., 192.168.10.25).
4. Specify the access URL of the web user interface language pack in the configuration files.

If you want to add a new language (e.g., Wuilan) to IP DECT phones, prepare the language file named as "10.Wuilan.js" for downloading. After update, you will find a

new language selection “Wuilan” on the web user interface:

**Settings->Preference->Language.**

**Procedure**

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

<b>Configuration File</b>	y00000000025.cfg	Specify the access URL of the custom language pack for web user interface. <b>Parameter:</b> wui_lang.url
		Delete custom language packs of the web user interface. <b>Parameter:</b> wui_lang.delete

**Details of the Configuration Parameter:**

Parameter	Permitted Values	Default
wui_lang.url	URL within 511 characters	Blank
<p><b>Description:</b> Configures the access URL of the custom language pack for the web user interface.</p> <p><b>Example:</b> wui_lang.url = http://192.168.10.25/1.English.js</p> <p>During the auto provisioning process, the IP DECT phone connects to the HTTP provisioning server “192.168.10.25”, and downloads the language pack “1.English.js”. The English language translation will be changed accordingly if you have modified the language template file.</p> <p>If you want to download multiple language packs to the web user interface simultaneously, you can configure as following: wui_lang.url = http://192.168.10.25/1.English.js wui_lang.url = http://192.168.10.25/9.Russian.js</p> <p><b>Web User Interface:</b> None</p> <p><b>Handset User Interface:</b> None</p>		

Parameter	Permitted Values	Default
wui_lang.delete	http://localhost/all or http://localhost/Y.name.js	Blank
<p><b>Description:</b> Delete the specified or all custom web language packs of the web user interface.</p> <p><b>Example:</b> Delete all custom language packs of the web user interface: wui_lang.delete = http://localhost/all Delete a custom language pack of the web user interface (e.g., 9.Russian.js): wui_lang.delete = http://localhost/9.Russian.js</p> <p><b>Web User Interface:</b> None</p> <p><b>Handset User Interface:</b> None</p>		

## Specifying the Language to Use

The default language used on the handset user interface is English. If the language of your web browser is not supported by the IP DECT phone, the web user interface will use English by default. You can specify the language for the handset user interface and web user interface respectively.

### Procedure

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

<b>Configuration File</b>	y000000000025.cfg	Specify the languages for the web user interface. <b>Parameters:</b> lang.wui
		Specify the language for the handset user interface. <b>Parameters:</b> custom.handset.language
<b>Local</b>	Web User Interface	Specify the language for the web user interface. <b>Navigate to:</b> http://10.10.20.27/servlet?p=settin



		gs-preference&q=load
	Handset User Interface	Specify the language for the handset user interface.

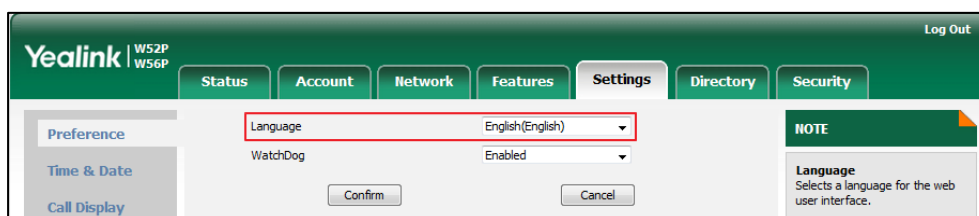
### Details of Configuration Parameters:

Parameters	Permitted Values	Default
lang.wui	Refer to the following content	English
<p><b>Description:</b> Configures the language used on the web user interface.</p> <p><b>Permitted Values:</b> English, French, German, Italian, Polish, Portuguese, Spanish, Turkish, Russian or the custom language name.</p> <p><b>Example:</b> lang.wui = English</p> <p>If you want to use the custom language (e.g., Wuilan) for the IP DECT phone, configure the parameter "lang.wui = Wuilan".</p> <p><b>Note:</b> If the language of your browser is not supported by the IP DECT phone, the web user interface will use English by default.</p> <p><b>Web User Interface:</b> Settings-&gt;Preference-&gt;Language</p> <p><b>Handset User Interface:</b> None</p>		
custom.handset.language	Integer from 0 to 9	0
<p><b>Description:</b> Configures the language of the handset.</p> <p>0-English 1-French 2-Deutsch 3-Italian 4-Polski 5-Portuguese 6-Spanish 7-Turkish 8-Svenska</p>		

Parameters	Permitted Values	Default
<p><b>9-Russian</b></p> <p><b>Note:</b> It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled).</p> <p><b>Web User Interface:</b></p> <p>None</p> <p><b>Handset User Interface:</b></p> <p>OK-&gt;Settings-&gt;Language</p>		

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.  
Text displayed on the web will change to the selected language.

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

1. Press **OK** to enter the main menu.
2. Select **Settings->Language**.
3. Press **▲** or **▼** to highlight the desired language and press the **Select** soft key.  
The LCD screen prompts "Change phone language to xxx?" (xxx is the language you selected).
4. Press the **Yes** soft key to accept the change.  
Text displayed on the handset will change to the selected language.

# Configuring Basic Features

---

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

- Register Power Light Flash
- Account Registration
- Call Display
- Display Method on Dialing
- Number Assignment
- Time and Date
- Input Method
- Key As Send
- Dial Plan
- Auto Dial
- Local Directory
- Search Source in Dialing
- Save Call Log
- Call Waiting
- Auto Answer
- Allow IP Call
- Accept SIP Trust Server Only
- Anonymous Call
- Anonymous Call Rejection
- Do Not Disturb (DND)
- 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](#)
- [Feature Key Synchronization](#)
- [Recent Call in Dialing](#)
- [Call Number Filter](#)
- [Calling Line Identification Presentation](#)
- [Connected Line Identification Presentation](#)
- [Intercom](#)
- [Call Timeout](#)
- [Ringing Timeout](#)
- [Send user=phone](#)
- [SIP Send MAC](#)
- [SIP Send Line](#)
- [Reserve # in User Name](#)
- [Unregister When Reboot](#)
- [100 Reliable Retransmission](#)
- [Reboot in Talking](#)
- [End Call on Hook](#)

## Register Power Light Flash

Register Power Light Flash allows the base power indicator LED to flash when registering an account successfully.

### Procedure

The register power light flash can be configured using the configuration files.

<b>Configuration File</b>	y000000000025.cfg	<p>Configure the register power light flash.</p> <p><b>Parameters:</b></p> <pre>features.registered_power_led_flash.enable</pre>
---------------------------	-------------------	--

**Details of Configuration Parameters:**

Parameters	Permitted Values	Default
<code>features.registered_power_led_flash.enable</code>	0 or 1	1
<p><b>Description:</b> Enables or disables the base power indicator LED to flash when registering an account successfully.</p> <p>0-Disabled (base power indicator LED does not flash) 1-Enabled (base power indicator LED slow flashes (1000ms) red)</p> <p><b>Web User Interface:</b> None</p> <p><b>Handset User Interface:</b> None</p>		

## Account Registration

Registering a SIP account makes it easier for the IP DECT phones to receive an incoming call, dial an outgoing call. The IP DECT phones support SIP server redundancy for account registration. For more information, refer to [Server Redundancy](#) on page 266.

### Procedure

Account registration can be configured using the configuration files or locally.

<b>Configuration File</b>	<MAC>.cfg	<p>Configure the account registration information.</p> <p><b>Parameter:</b></p> <ul style="list-style-type: none"> <li>account.X.enable</li> <li>account.X.label</li> <li>account.X.display_name</li> <li>account.X.auth_name</li> <li>account.X.user_name</li> <li>account.X.password</li> <li>account.X.outbound_proxy_enable</li> <li>account.X.outbound_host</li> <li>account.X.outbound_port</li> <li>account.X.backup_outbound_host</li> <li>account.X.backup_outbound_port</li> </ul>
---------------------------	-----------	--

		<p>Configure the interval for the IP DECT phone to retry to re-register when registration fails.</p> <p><b>Parameter:</b> account.X.reg_fail_retry_interval</p>
<b>Local</b>	Web User Interface	<p>Configure the account registration information.</p> <p><b>Navigate to:</b> http://&lt;phoneIPAddress&gt;/servlet?ρ=account-register&amp;q=load&amp;acc=0</p>
		<p>Configure the interval for the IP DECT phone to retry to re-register when registration fails.</p> <p><b>Navigate to:</b> http://&lt;phoneIPAddress&gt;/servlet?ρ=account-adv&amp;q=load&amp;acc=0</p>

**Details of Configuration Parameters:**

Parameters	Permitted Values	Default
<p><b>account.X.enable</b> (X ranges from 1 to 5)</p>	0 or 1	0
<p><b>Description:</b> Enables or disables the account X. 0-Disabled 1-Enabled</p> <p><b>Web User Interface:</b> Account-&gt;Basic-&gt;Line Active</p> <p><b>Handset User Interface:</b> None</p>		
<p><b>account.X.label</b> (X ranges from 1 to 5)</p>	String within 99 characters	Blank
<p><b>Description:</b> Configures the label to be displayed on the LCD screen for account X.</p> <p><b>Web User Interface:</b> Account-&gt;Basic-&gt;Label</p>		

Parameters	Permitted Values	Default
<b>Handset User Interface:</b> None		
<b>account.X.display_name</b> (X ranges from 1 to 5)	String within 99 characters	Blank
<b>Description:</b> Configures the display name for account X. <b>Web User Interface:</b> Account->Basic->Display Name <b>Handset User Interface:</b> None		
<b>account.X.auth_name</b> (X ranges from 1 to 5)	String within 99 characters	Blank
<b>Description:</b> Configures the user name for register authentication for account X. <b>Web User Interface:</b> Account->Basic->Register Name <b>Handset User Interface:</b> None		
<b>account.X.user_name</b> (X ranges from 1 to 5)	String within 99 characters	Blank
<b>Description:</b> Configures the register user name for account X. <b>Web User Interface:</b> Account->Basic->User Name <b>Handset User Interface:</b> None		
<b>account.X.password</b> (X ranges from 1 to 5)	String within 99 characters	Blank
<b>Description:</b> Configures the password for register authentication for account X. <b>Web User Interface:</b> Account->Basic->Password		

Parameters	Permitted Values	Default
<b>Handset User Interface:</b> None		
<b>account.X.outbound_proxy_enable</b> (X ranges from 1 to 5)	0 or 1	0
<b>Description:</b> Enables or disables the IP DECT phone to send requests to the outbound proxy server for account X.  0-Disabled 1-Enabled  <b>Web User Interface:</b> Account->Basic->Enable Outbound Proxy Server  <b>Handset User Interface:</b> None		
<b>account.X.outbound_host</b> (X ranges from 1 to 5)	IP address or domain name	Blank
<b>Description:</b> Configures the IP address or domain name of the outbound proxy server 1 or account X.  <b>Example:</b> account.1.outbound_host = 10.1.8.11  <b>Note:</b> It works only if the value of the parameter "account.X.outbound_proxy_enable" is set to 1 (Enabled).  <b>Web User Interface:</b> Account->Basic->Outbound Proxy Server 1  <b>Handset User Interface:</b> None		
<b>account.X.outbound_port</b> (X ranges from 1 to 5)	Integer from 0 to 65535	Blank
<b>Description:</b> Configures the port of the outbound proxy server1 for account X.  <b>Example:</b> account.1.outbound_port = 5060  <b>Note:</b> It works only if the value of the parameter "account.X.outbound_proxy_enable" is set to 1 (Enabled).		



Parameters	Permitted Values	Default
<b>Web User Interface:</b> Account->Basic->Outbound Proxy Server 1->Port <b>Handset User Interface:</b> None		
<b>account.X.backup_outbound_host</b> (X ranges from 1 to 5)	<b>IP address or domain name</b>	<b>Blank</b>
<b>Description:</b> Configures the IP address or domain name of the outbound proxy server 2 for account X. <b>Example:</b> account.1.backup_outbound_host = 10.1.8.12 <b>Note:</b> It works only if the value of the parameter "account.X.outbound_proxy_enable" is set to 1 (Enabled). <b>Web User Interface:</b> Account->Register->Outbound Proxy Server 2 <b>Handset User Interface:</b> None		
<b>account.X.backup_outbound_port</b> (X ranges from 1 to 5)	<b>Integer from 0 to 65535</b>	<b>5060</b>
<b>Description:</b> Configures the port of the outbound proxy server 2 for account X. <b>Example:</b> account.1.backup_outbound_host = 5060 <b>Note:</b> It works only if the value of the parameter "account.X.outbound_proxy_enable" is set to 1 (Enabled). <b>Web User Interface:</b> Account->Register->Outbound Proxy Server 2->Port <b>Handset User Interface:</b> None		
<b>account.X.sip_server.Y.address</b> (X ranges from 1 to 5, Y ranges from 1 to 2)	<b>String within 256 characters</b>	<b>Blank</b>
<b>Description:</b> Configures the IP address or domain name of the SIP server Y for account X. <b>Example:</b>		

Parameters	Permitted Values	Default
<p>account.1.sip_server.1.address = yealink.pbx.com</p> <p><b>Web User Interface:</b> Account-&gt;Register-&gt;SIP Server Y-&gt;Server Host</p> <p><b>Handset User Interface:</b> None</p>		
<p><b>account.X.sip_server.Y.port</b> (X ranges from 1 to 5, Y ranges from 1 to 2)</p>	<p>Integer from 0 to 65535</p>	<p>5060</p>
<p><b>Description:</b> Configures the port of the SIP server Y for account X.</p> <p><b>Example:</b> account.1.sip_server.1.port = 5060</p> <p><b>Web User Interface:</b> Account-&gt;Register-&gt;SIP Server Y-&gt;Port</p> <p><b>Handset User Interface:</b> None</p>		
<p><b>account.X.reg_fail_retry_interval</b> (X ranges from 1 to 5)</p>	<p>Integer from 0 to 1800</p>	<p>30</p>
<p><b>Description:</b> Configures the interval (in seconds) for the IP DECT phone to retry to re-register for account X when registration fails.</p> <p><b>Example:</b> account.1.reg_fail_retry_interval = 60</p> <p><b>Web User Interface:</b> Account-&gt;Advanced-&gt;SIP Registration Retry Timer(0~1800)</p> <p><b>Handset User Interface:</b> None</p>		

**To register an account via web user interface:**

1. Click on **Account->Register**.
2. Select the desired account from the pull-down list of **Account**.
3. Select **Enabled** from the pull-down list of **Line Active**.
4. Enter the valid value in the **Label, Display Name, Register Name, User Name, Password** and **SIP Server1/2** field respectively.
5. If you use outbound proxy servers, do the following:
  - 1) Select **Enabled** from the pull-down list of **Enable Outbound Proxy Server**.

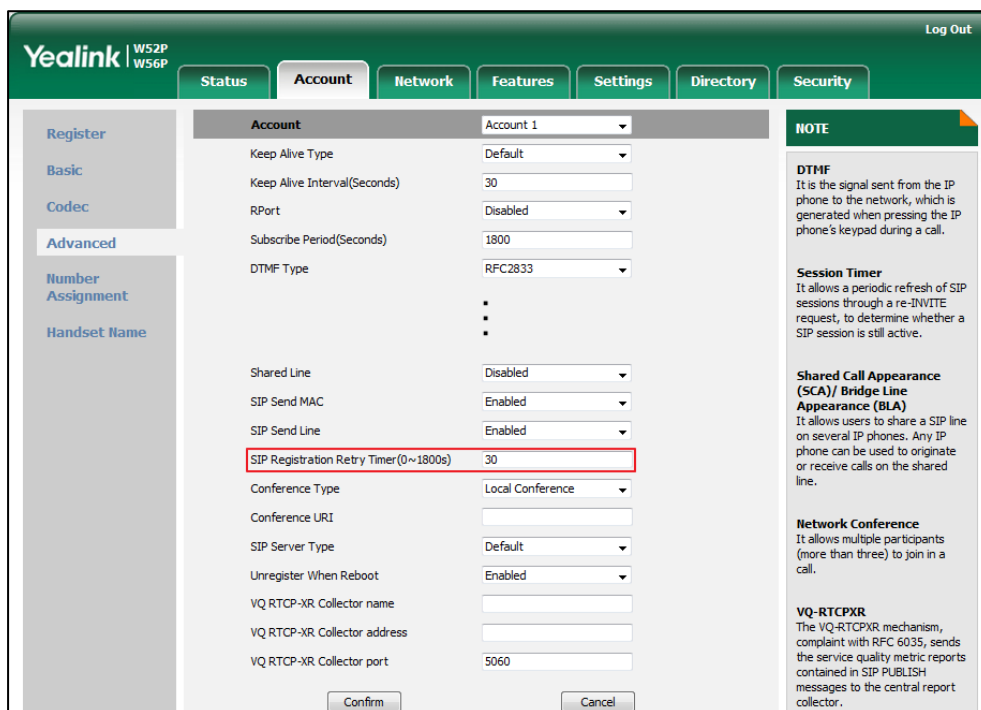
- 2) Enter the desired IP address or domain name in the **Outbound Proxy Server1/2** field and the desired port of the outbound proxy server in the **Port** field respectively.
- 3) Enter the desired interval in the **Proxy Fallback Interval** field.

The screenshot shows the Yealink W52P/W56P web interface. The top navigation bar includes 'Status', 'Account', 'Network', 'Features', 'Settings', 'Directory', and 'Security'. The 'Account' section is selected, showing 'Account 1' as the active account. The 'Register' status is 'Registered'. The 'Line Active' is set to 'Enabled'. The 'Label', 'Display Name', 'Register Name', 'User Name', and 'Password' fields are all set to '4603'. The 'SIP Server 1' section shows 'Server Host' as 'pbx.yealink.com' and 'Port' as '5060'. The 'SIP Server 2' section is empty. The 'Outbound Proxy Server 1' section shows 'Outbound Proxy Server 1' as '10.1.8.11' and 'Port' as '5060'. The 'Outbound Proxy Server 2' section is empty. The 'Proxy Fallback Interval' is set to '3600'. The 'NAT' setting is 'Disabled'. A 'NOTE' section on the right provides information about 'Account Registration', 'Server Redundancy', and 'NAT Traversal'. At the bottom, there are 'Confirm' and 'Cancel' buttons.

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

To configure the interval for re-register when registration fails via web user interface:

1. Click **Account->Advanced**.
2. Enter the desired interval in the **SIP Registration Retry Timer(0~1800s)** field.



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

## Call Display

Display called party information allows the handsets to present the callee identity in addition to the presentation of caller identity when it receives an incoming call.

You can customize the call information to be displayed on the handsets as required. IP DECT phones support five call information display methods: Number+Name, Name, Name+Number, Number or Full Contact Info (display name<sip:xxx@domain.com>).

### Procedure

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

<p><b>Configuration File</b></p>	<p>y000000000025.cfg</p>	<p>Configure display called party information feature.</p> <p><b>Parameter:</b></p> <p>phone_setting.called_party_info_display.enable</p>
----------------------------------	--------------------------	---

		Specify the call information display method. <b>Parameter:</b> phone_setting.call_info_display_method
<b>Local</b>	Web User Interface	Configure display called party information feature. Specify the call information display method. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=settings-calldisplay&q=load

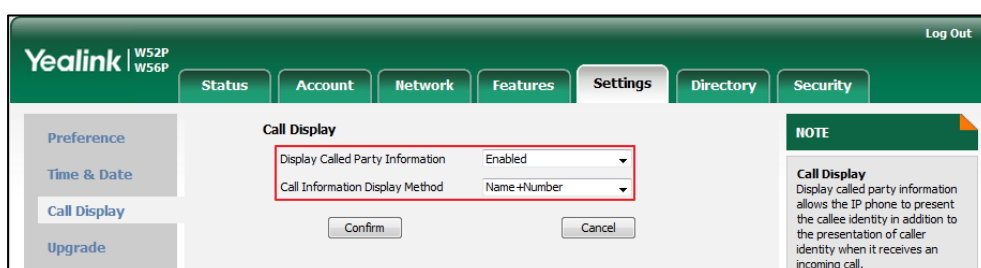
**Details of Configuration Parameters:**

Parameters	Permitted Values	Default
phone_setting.called_party_info_display.enable	0 or 1	1
<p><b>Description:</b> Enables or disables the handset to display the called account information when receiving an incoming call.</p> <p>0-Disabled 1-Enabled</p> <p><b>Web User Interface:</b> Settings-&gt;Call Display-&gt;Display Called Party Information</p> <p><b>Handset User Interface:</b> None</p>		
phone_setting.call_info_display_method	0, 1, 2, 3 or 4	0
<p><b>Description:</b> Specifies the call information display method when the handset receives an incoming call, dials an outgoing call or is during an active call.</p> <p>0-Name+Number 1-Number+Name 2-Name 3-Number 4-Full Contact Info (display name&lt; sip:xxx@domain.com&gt;)</p>		

Parameters	Permitted Values	Default
<b>Web User Interface:</b> Settings->Call Display->Call Information Display Method  <b>Handset User Interface:</b> None		

To configure call display features via web user interface:

1. Click on **Settings->Call Display**.
2. Select the desired value from the pull-down list of **Display Called Party Information**.
3. Select the desired value from the pull-down list of **Call Information Display Method**.



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

## Display Method on Dialing

When the handset is on the pre-dialing, calling or ringing screen, the account information will be displayed on the LCD screen.

You can customize the account information to be displayed on the handsets as required. IP DECT phones support three account information display methods: Label, Display Name or User Name. You can also hide the account information display.

### Procedure

Display method on dialing can be configured using the configuration files or locally.

<b>Configurati on File</b>	y000000000025.cfg	Configure display method on dialing. <b>Parameter:</b> features.caller_name_type_on_dialing
		Hide the account information display. <b>Parameter:</b> account.X.hide_local_number.enable
<b>Local</b>	Web User Interface	Configure display method on dialing. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=features-

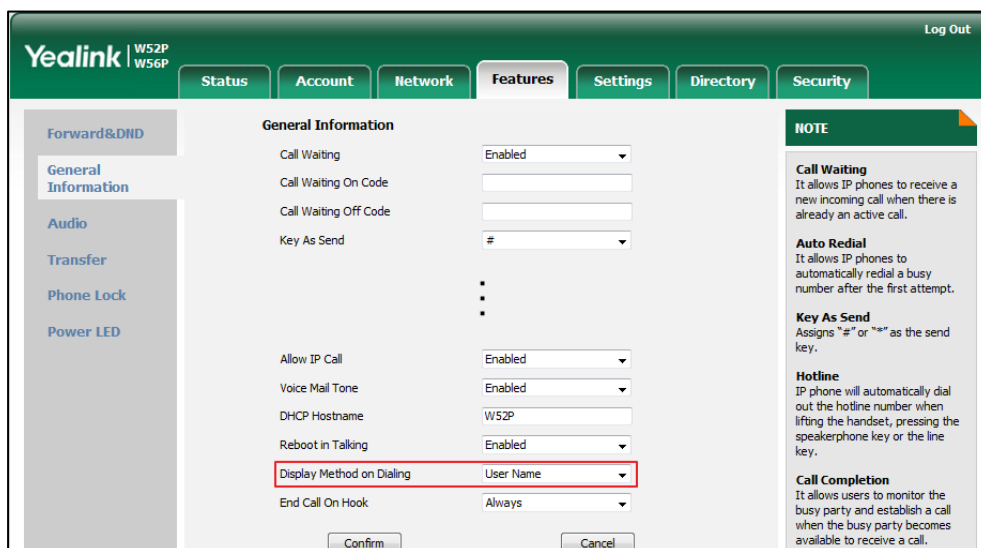
	general&q=load
--	----------------

**Details of Configuration Parameters:**

Parameters	Permitted Values	Default
<b>features.caller_name_type_on_dialing</b>	<b>1, 2 or 3</b>	<b>3</b>
<p><b>Description:</b>                      Configures the account information displayed on the LCD screen when the handset is on the pre-dialing, dialing or ringing screen.</p> <p>1-Label                      2-Display Name                      3-User Name</p> <p><b>Note:</b> It works only if the value of the parameter "account.X.hide_local_number.enable" is set to 0 (Disabled).</p> <p><b>Web User Interface:</b>                      Features-&gt;General Information-&gt;Display Method on Dialing</p> <p><b>Handset User Interface:</b>                      None</p>		
<b>account.X.hide_local_number.enable</b> (X ranges from 1 to 5)	<b>0 or 1</b>	<b>0</b>
<p><b>Description:</b>                      Enables or disables the handset to hide the account information on the pre-dialing, dialing or ringing screen.</p> <p>1-Disabled                      1-Enabled</p> <p>If it is set to 1 (Enabled), the LCD screen will display Line X (X ranges from 1 to 5 for the corresponding account) instead of account information.</p> <p><b>Web User Interface:</b>                      None</p> <p><b>Handset User Interface:</b>                      None</p>		

To configure display method on dialing via web user interface:

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



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

## Number Assignment

After the handset is registered to the base station, you can assign one or more outgoing lines or incoming lines for the handset.

The handset can only use the assigned outgoing line(s) to place calls. When multiple outgoing lines are assigned to the handset, the handset uses the first line as the default outgoing line. You can change the default outgoing line of the handset.

The handset can only receive incoming calls of the assigned incoming line(s). You can assign incoming lines to all handsets registered to the same base station on your handset.

### Procedure

Number Assignment can be configured using the configuration files or locally.

<b>Configuration File</b>	y000000000025.cfg	Configure the incoming lines of the handset. <b>Parameters:</b> handset.X.incoming_lines
		Configure the outgoing lines of the handset. <b>Parameters:</b> handset.X.dial_out_lines



		<p>Configure the dial out default lines of the handset.</p> <p><b>Parameters:</b> handset.X.dial_out_default_line</p>
Local	Web User Interface	<p>Configure the incoming lines of the handset.</p> <p>Configure the outgoing lines of the handset.</p> <p>Configure the number assignment.</p> <p><b>Navigate to:</b> http://&lt;phoneIPAddress&gt;/servlet?p=account-assignment&amp;q=load</p>
	Handset User Interface	<p>Configure the incoming lines of the handset.</p> <p>Configure the outgoing lines of the handset.</p>

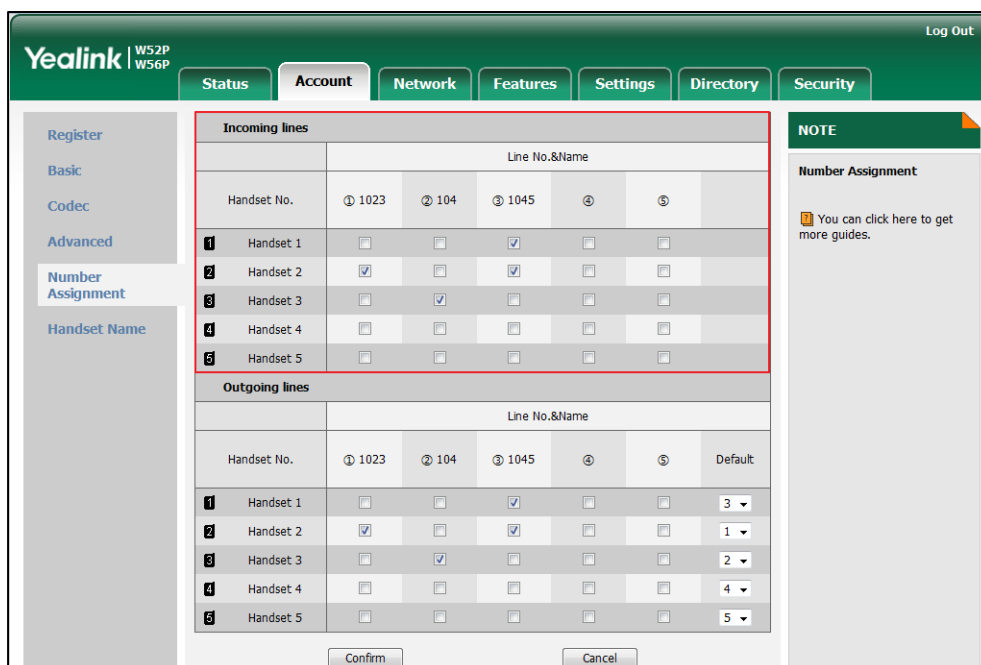
**Details of Configuration Parameters:**

Parameters	Permitted Values	Default
<p><b>handset.X.incoming_lines</b> (X ranges from 1 to 5)</p>	<p><b>Integer from 1 to 5</b></p>	<p><b>Refer to the following content</b></p>
<p><b>Description:</b> Configures the lines to receive incoming calls for handset X. Multiple line IDs are separated by commas.</p> <p><b>Default value:</b> The incoming line for handset 1 is line 1. The incoming line for handset 2 is line 2. The incoming line for handset 3 is line 3. The incoming line for handset 4 is line 4. The incoming line for handset 5 is line 5.</p> <p><b>Web User Interface:</b> Account-&gt;Number Assignment-&gt;Incoming lines</p> <p><b>Handset User Interface:</b> OK-&gt;Settings-&gt;Telephony-&gt;Incoming Lines (Default PIN:0000)-&gt;HandsetX</p>		

Parameters	Permitted Values	Default
<b>handset.X.dial_out_lines</b> (X ranges from 1 to 5)	Integer from 1 to 5	Refer to the following content
<p><b>Description:</b>                      Configures the lines to place outgoing calls for handset X.                      Multiple line IDs are separated by commas.</p> <p><b>Default value:</b>                      The outgoing line for handset 1 is line 1.                      The outgoing line for handset 2 is line 2.                      The outgoing line for handset 3 is line 3.                      The outgoing line for handset 4 is line 4.                      The outgoing line for handset 5 is line 5.</p> <p><b>Web User Interface:</b>                      Account-&gt;Number Assignment-&gt;Outgoing lines</p> <p><b>Handset User Interface:</b>                      None</p>		
<b>handset.X.dial_out_default_line</b> (X is from 1 to 5)	Integer from 1 to 5	Refer to the following content
<p><b>Description:</b>                      Configures the default line to place outgoing calls for handset X.</p> <p><b>Default value:</b>                      The default outgoing line for handset 1 is 1.                      The default outgoing line for handset 2 is 2.                      The default outgoing line for handset 3 is 3.                      The default outgoing line for handset 4 is 4.                      The default outgoing line for handset 5 is 5.</p> <p><b>Note:</b> It works only if the line you want to select to be default outgoing line should be configure as outgoing line for handset X in advance.</p> <p><b>Web User Interface:</b>                      Account-&gt;Number Assignment-&gt;Outgoing lines-&gt;Default</p> <p><b>Handset User Interface:</b>                      OK-&gt;Settings-&gt;Telephony-&gt;Default Line</p>		

**To assign the incoming line of the handset via web user interface:**

1. Click on **Account->Number Assignment**.
2. To assign incoming lines, to check the desired account from **Line No.&Name** field to the corresponding handset in the **Handset No.** field.



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

**To assign the incoming line to handsets via the handset:**

1. Press **OK** to enter the main menu.
2. Select **Settings->Telephony->Incoming Lines**.
3. Enter the system PIN (default: 0000), and then press the **Done** soft key.

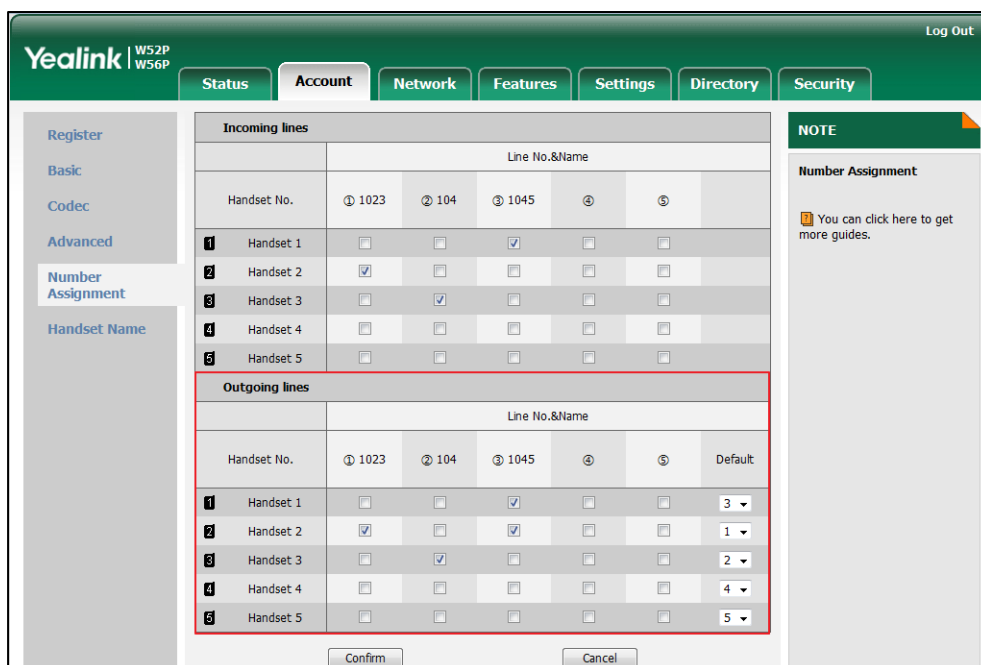
The LCD screen displays all handsets registered to the base station. The handset itself is highlighted and followed by a left arrow.

4. Press **▲** or **▼** to highlight the desired handset, and then press the **OK** soft key.
5. Press **◀** or **▶** to select **Accept** from the desired line fields.
6. Press the **Save** soft key to accept the change.
7. Press the **Back** soft key to return to the previous screen.
8. Repeat steps 5-8 to assign incoming lines for other handsets.

If a line is assigned to multiple handsets as an incoming line, an incoming call to this line will cause these handsets to ring simultaneously, but the incoming call can be only answered by one of them.

To assign the outgoing line of the handset via web user interface:

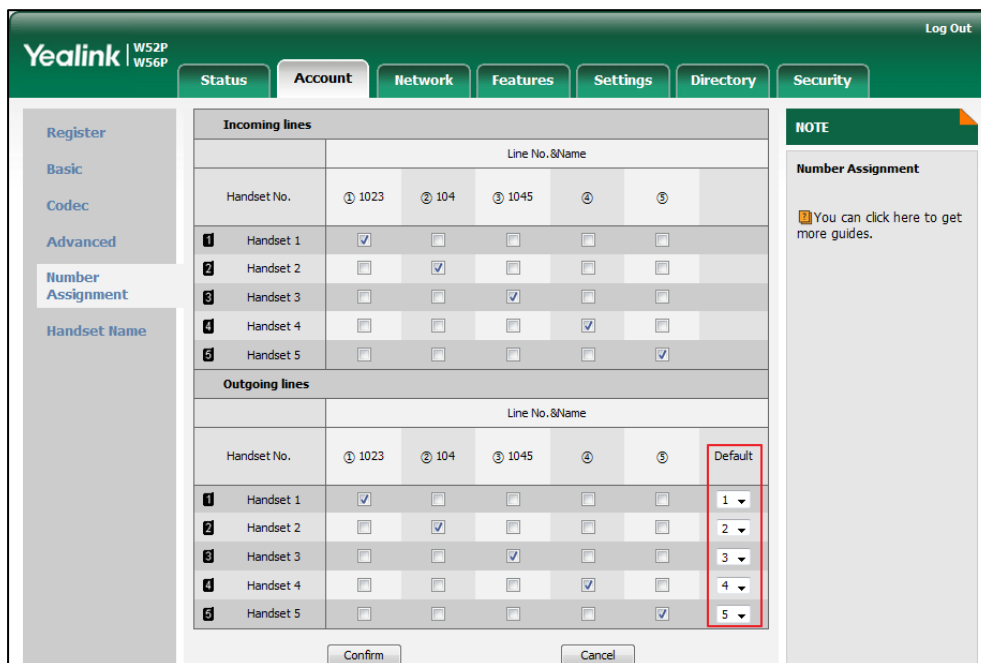
1. Click on **Account->Number Assignment**.
2. To assign outgoing lines, to check the desired account from **Line No.&Name** field to the corresponding handset in the **Handset No.** field.



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

To change the default outgoing line of the handset via web user interface:

1. Click on **Account->Number Assignment**.
2. Select the desired default outgoing line number from the pull-down list of corresponding **Default** field.



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

To change the default outgoing line of the handset via the handset:

1. Press **OK** to enter the main menu.
2. Select **Settings->Telephony->Default Line**.

The LCD screen displays all outgoing lines currently assigned to the handset. The default outgoing line is highlighted and followed by a left arrow.

3. Press **▲** or **▼** to highlight the desired line, and then press the **OK** soft key.  
The default outgoing line is changed successfully.

## Time and Date

The IP DECT phones maintain a local clock and calendar. Time and date are displayed on the idle screen of your handset.

The following table lists available configuration methods for time and date.

Option	Configuration Methods
NTP time server	Configuration Files Web User Interface
Time Zone	Configuration Files

Option	Configuration Methods
	Web User Interface
Time	Web User Interface
Time Format	Configuration Files Web User Interface Handset User Interface
Date	Web User Interface Handset User Interface
Date Format	Configuration Files Web User Interface Handset User Interface
Daylight Saving Time	Configuration Files Web User Interface

## NTP Time Server

A time server is a computer server that reads the actual time from a reference clock and distributes this information to the clients in a network. The Network Time Protocol (NTP) is the most widely used protocol that distributes and synchronizes time in the network.

The IP DECT phones synchronize the time and date automatically from the NTP time server by default. The NTP time server address can be offered by the DHCP server or configured manually. NTP by DHCP Priority feature can configure the priority for the IP DECT phone to use the NTP time server address offered by the DHCP server or configured manually.

### 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 the IP DECT phone to obtain the time and date from the NTP time server, you must set the time zone.

### Procedure

NTP time server and time zone can be configured using the configuration files or locally.

<b>Configuration File</b>	<MAC>.cfg	Configure NTP by DHCP priority feature and DHCP time feature. <b>Parameters:</b> local_time.manual_ntp_srv_prior local_time.dhcp_time
---------------------------	-----------	--

		<p>Configure the NTP server, time zone.</p> <p><b>Parameters:</b></p> <p>local_time.ntp_server1</p> <p>local_time.ntp_server2</p> <p>local_time.interval</p> <p>local_time.time_zone</p> <p>local_time.time_zone_name</p>
<b>Local</b>	Web User Interface	<p>Configure NTP by DHCP priority feature and DHCP time feature.</p> <p>Configure the NTP server, time zone.</p> <p><b>Navigate to:</b></p> <p>http://&lt;phoneIPAddress&gt;/servlet?parameter=settings-datetime&amp;q=load</p>

**Details of Configuration Parameters:**

Parameters	Permitted Values	Default
local_time.manual_ntp_srv_prior	0 or 1	0
<p><b>Description:</b></p> <p>Configures the priority for the IP DECT phone to use the NTP server address offered by the DHCP server.</p> <p>0-High (use the NTP server address offered by the DHCP server preferentially)</p> <p>1-Low (use the NTP server address configured manually preferentially)</p> <p><b>Web User Interface:</b></p> <p>Settings-&gt;Time &amp; Date-&gt;NTP by DHCP Priority</p> <p><b>Handset User Interface:</b></p> <p>None</p>		
local_time.dhcp_time	0 or 1	0
<p><b>Description:</b></p> <p>Enables or disables the IP DECT phone to update time with the offset time offered by the DHCP server.</p> <p>0-Disabled</p> <p>1-Enabled</p> <p><b>Note:</b> It is only available to offset from GMT 0.</p> <p><b>Web User Interface:</b></p> <p>Settings-&gt;Time &amp; Date-&gt;DHCP Time</p>		

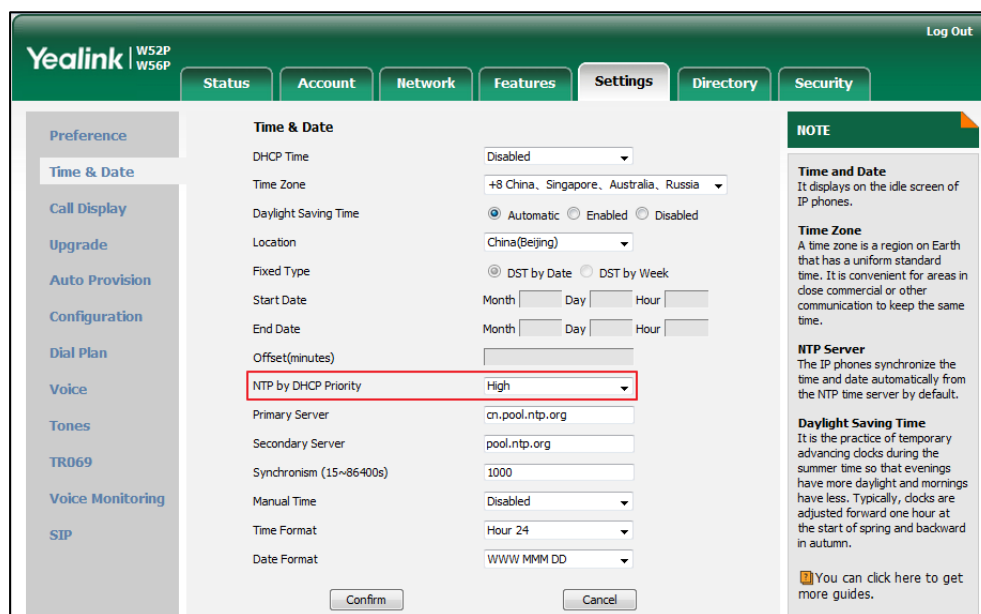
Parameters	Permitted Values	Default
<b>Handset User Interface:</b> None		
<b>local_time.ntp_server1</b>	<b>IP Address or Domain Name</b>	<b>cn.pool.ntp.org</b>
<b>Description:</b> Configures the IP address or the domain name of the NTP server 1.  <b>Example:</b> local_time.ntp_server1 = 192.168.0.5  <b>Web User Interface:</b> Settings->Time & Date->Primary Server  <b>Handset User Interface:</b> None		
<b>local_time.ntp_server2</b>	<b>IP Address or Domain Name</b>	<b>cn.pool.ntp.org</b>
<b>Description:</b> Configures the IP address or the domain name of the NTP server 2. If the NTP server 1 is not configured or cannot be accessed, the IP DECT phone will request the time and date from the NTP server 2.  <b>Example:</b> local_time.ntp_server2 = 192.168.0.6  <b>Web User Interface:</b> Settings->Time & Date->Secondary Server  <b>Handset User Interface:</b> None		
<b>local_time.interval</b>	<b>Integer from 15 to 86400</b>	<b>1000</b>
<b>Description:</b> Configures the interval (in seconds) to update time and date from the NTP server.  <b>Example:</b> local_time.interval = 1000  <b>Web User Interface:</b> Settings->Time & Date->Synchronism (15~86400s)  <b>Handset User Interface:</b> None		



Parameters	Permitted Values	Default
<code>local_time.time_zone</code>	-11 to +14	+8
<p><b>Description:</b> Configures the time zone. For more available time zones, refer to <a href="#">Appendix B: Time Zones</a> on page 405.</p> <p><b>Example:</b> <code>local_time.time_zone = +8</code></p> <p><b>Web User Interface:</b> Settings-&gt;Time &amp; Date-&gt;Time Zone</p> <p><b>Handset User Interface:</b> None</p>		
<code>local_time.time_zone_name</code>	String within 32 characters	China(Beijing)
<p><b>Description:</b> Configures the time zone name. The available time zone names depend on the time zone configured by the parameter "local_time.time_zone". For more information on the available time zone names for each time zone, refer to <a href="#">Appendix B: Time Zones</a> on page 405.</p> <p><b>Example:</b> <code>local_time.time_zone_name = China(Beijing)</code></p> <p><b>Note:</b> It works only if the value of the parameter "local_time.summer_time" is set to 2 (Automatic) and the parameter "local_time.time_zone" should be configured in advance.</p> <p><b>Web User Interface:</b> Settings-&gt;Time &amp; Date-&gt;Location</p> <p><b>Handset User Interface:</b> None</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**.

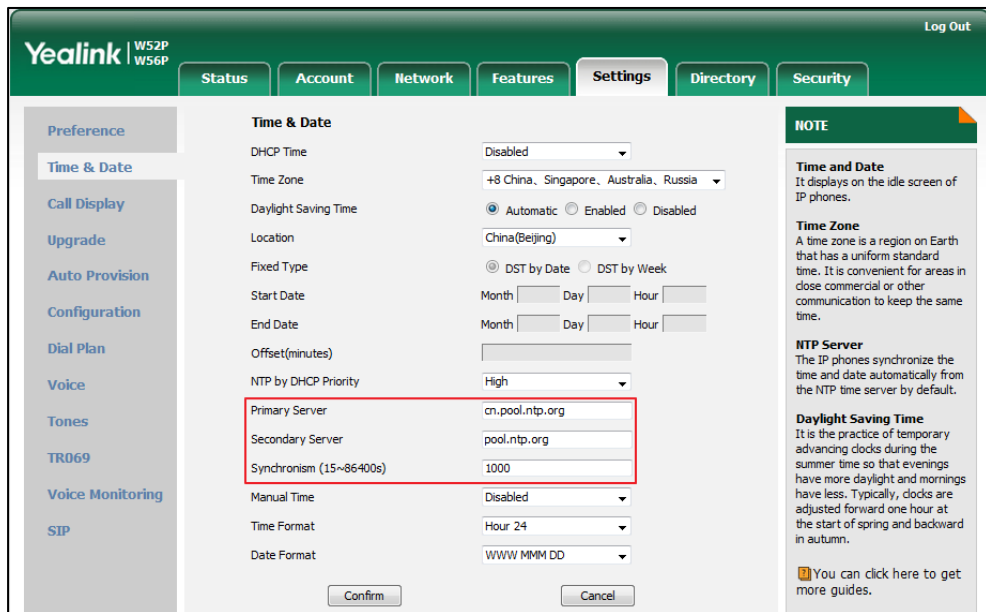


3. Click **Confirm** to accept the change.

To configure the NTP server, time zone 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. Select the desired location from the pull-down list of **Location**.
5. Enter the domain name or IP address in the **Primary Server** and **Secondary Server** field respectively.

- Enter the desired time interval in the **Synchronism (15~86400s)** field.



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

## Time and Date Settings

You can set the time and date manually when IP DECT phones cannot obtain the time and date from the NTP time server. The time and date display can use one of several different formats.

### Procedure

Time and date can be configured using the configuration files or locally.

<b>Configuration File</b>	<MAC>.cfg	Configure the time and date manually. <b>Parameter:</b> local_time.manual_time_enable
		Configure the time and date formats. <b>Parameters:</b> custom.handset.time_format custom.handset.date_format
<b>Local</b>	Web User Interface	Configure the time and date manually. Configure the time and date formats. <b>Navigate to:</b>

		http://<phoneIPAddress>/servlet ?p=settings-datetime&q=load
	Handset User Interface	Configure the time and date formats.

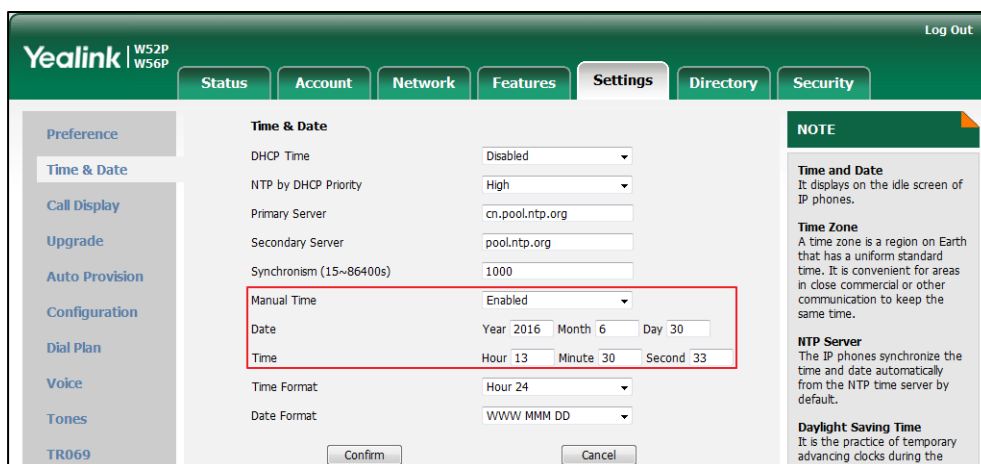
**Details of Configuration Parameters:**

Parameters	Permitted Values	Default
<b>local_time.manual_time_enable</b>	<b>0 or 1</b>	<b>0</b>
<p><b>Description:</b> Enables or disables the IP DECT phone to obtain time and date from manual settings.</p> <p><b>0</b>-Disabled (obtain time and date from NTP server) <b>1</b>-Enabled (obtain time and date from manual settings)</p> <p><b>Web User Interface:</b> Settings-&gt;Time &amp; Date-&gt;Manual Time</p> <p><b>Handset User Interface:</b> None</p>		
<b>custom.handset.time_format</b>	<b>0 or 1</b>	<b>1</b>
<p><b>Description:</b> Configures the time format.</p> <p><b>0</b>-Hour 12 <b>1</b>-Hour 24</p> <p>If it is set to 0 (Hour 12), the time will be displayed in 12-hour format with AM or PM specified.</p> <p>If it is set to 1 (Hour 24), the time will be displayed in 24-hour format (e.g., 2:00 PM displays as 14:00).</p> <p><b>Note:</b> It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled).</p> <p><b>Web User Interface:</b> Settings-&gt;Time &amp; Date-&gt;Time Format</p> <p><b>Handset User Interface:</b> OK-&gt;Settings-&gt;Display-&gt;Time Format</p>		
<b>custom.handset.date_format</b>	<b>0, 1, 2, 3, 4, 5 or 6</b>	<b>0</b>

Parameters	Permitted Values	Default
<p><b>Description:</b> Configures the date format.</p> <p><b>Valid values are:</b>                      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</p> <p><b>Note:</b> “WWW” represents the abbreviation of the week, “DD” represents a two-digit day, “MMM” represents the first three letters of the month, “YYYY” represents a four-digit year, and “YY” represents a two-digit year. It works only if the value of the parameter “auto_provision.handset_configured.enable” is set to 1 (Enabled).</p> <p><b>Web User Interface:</b> Settings-&gt;Time &amp; Date-&gt;Date Format</p> <p><b>Handset User Interface:</b> OK-&gt;Settings-&gt;Display-&gt;Time Format</p>		

To configure the time and date manually for all handsets 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 time and date manually for a specific handset:**

1. Press **OK** to enter the main menu.
2. Select **Settings->Date & Time**.
3. Edit the current value in the **Date** and **Time** field respectively.
4. Press the **Save** soft key to accept the change.

The date and time displayed on the LCD screen will change accordingly.

**Note**

Before you configure date and time manually for specify handset, you should enable the **Manual Time** via web user interface first, or it would not take effect.

**To configure the time format for a specific handset:**

1. Press **OK** to enter the main menu.
2. Select **Settings->Display->Time Format**.
3. Press **▲** or **▼** to highlight the desired time format.
4. Press the **Change** soft key.

The radio box of the highlighted time format is marked.

The time format displayed on the LCD screen will be changed accordingly.

**To configure the date format for a specific handset:**

1. Press **OK** to enter the main menu.
2. Select **Settings->Display->Date Format**.
3. Press **▲** or **▼** to highlight the desired date format.
4. Press the **Change** soft key.

The radio box of the selected date format is marked.

The date format displayed on the LCD screen will be changed accordingly.

## 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. By default, the DST is set to Automatic, so it can be adjusted automatically from the current time zone configuration. You can configure DST for the desired area as required.

### Procedure

Daylight saving time can be configured using the configuration files or locally.

<b>Configuration File</b>	<MAC>.cfg	Configure DST. <b>Parameters:</b> local_time.summer_time local_time.dst_time_type local_time.start_time local_time.end_time local_time.offset_time
<b>Local</b>	Web User Interface	Configure DST. <b>Navigate to:</b> http://<phoneIPAddress>/servlet ?p=settings-datettime&q=load

### Details of Configuration Parameters:

Parameters	Permitted Values	Default
<b>local_time.summer_time</b>	<b>0, 1 or 2</b>	<b>2</b>
<p><b>Description:</b> Configures Daylight Saving Time (DST) feature.</p> <p><b>0-Disabled</b> <b>1-Enabled</b> <b>2-Automatic</b></p> <p><b>Note:</b> If there is no available time zone name for the configured time zone, you can set the value of the parameter "local_time.summer_time" to be 1 (Enabled), and configure the DST time manually.</p> <p><b>Web User Interface:</b> Settings-&gt;Time &amp; Date-&gt;Daylight Saving Time</p> <p><b>Handset User Interface:</b> None</p>		
<b>local_time.dst_time_type</b>	<b>0 or 1</b>	<b>0</b>
<p><b>Description:</b> Configures the DST time type.</p> <p><b>0-By Date</b> <b>1-By Week</b></p>		

Parameters	Permitted Values	Default
<p><b>Note:</b> It works only if the value of the parameter "local_time.summer_time" is set to 1 (Enabled).</p> <p><b>Web User Interface:</b> Settings-&gt;Time &amp; Date-&gt;Fixed Type</p> <p><b>Handset User Interface:</b> None</p>		
local_time.start_time	Time	1/1/0
<p><b>Description:</b> Configures the start time of the DST.</p> <p><b>Value formats are:</b></p> <ul style="list-style-type: none"> <li>• Month/Day/Hour (for By Date)</li> <li>• Month/Week of Month/Day of Week/Hour of Day (for By Week)</li> </ul> <p>If "local_time.dst_time_type" is set to 0 (By Date), use the mapping:</p> <p><b>Month:</b> 1=January, 2=February,..., 12=December</p> <p><b>Day:</b>1=the first day in a month,..., 31= the last day in a month</p> <p><b>Hour:</b>0=0am, 1=1am,..., 23=11pm</p> <p>If "local_time.dst_time_type" is set to 1 (By Week), use the mapping:</p> <p><b>Month:</b> 1=January, 2=February,..., 12=December</p> <p><b>Week of Month:</b> 1=the first week in a month,..., 5=the last week in a month</p> <p><b>Day of Week:</b> 1=Monday, 2=Tuesday,..., 7=Sunday</p> <p><b>Hour of Day:</b> 0=0am, 1=1am,..., 23=11pm</p> <p><b>Note:</b> It works only if the value of the parameter "local_time.summer_time" is set to 1 (Enabled).</p> <p><b>Web User Interface:</b> Settings-&gt;Time &amp; Date-&gt;Start Date</p> <p><b>Handset User Interface:</b> None</p>		
local_time.end_time	Time	12/31/23
<p><b>Description:</b> Configures the end time of the DST.</p> <p><b>Value formats are:</b></p> <ul style="list-style-type: none"> <li>• Month/Day/Hour (for DST by Date)</li> <li>• Month/Week of Month/Day of Week/Hour of Day (for DST by Week)</li> </ul>		



Parameters	Permitted Values	Default
<p>If "local_time.dst_time_type" is set to 0 (DST by Date), use the mapping:</p> <p><b>Month:</b> 1=January, 2=February,..., 12=December</p> <p><b>Day:</b> 1=the first day in a month,..., 31= the last day in a month</p> <p><b>Hour:</b> 0=0am, 1=1am,..., 23=11pm</p> <p>If "local_time.dst_time_type" is set to 1 (DST by Week), use the mapping:</p> <p><b>Month:</b> 1=January, 2=February,..., 12=December</p> <p><b>Week of Month:</b> 1=the first week in a month,..., 5=the last week in a month</p> <p><b>Day of Week:</b> 1=Monday, 2=Tuesday,..., 7=Sunday</p> <p><b>Hour of Day:</b> 0=0am, 1=1am,..., 23=11pm</p> <p><b>Note:</b> It works only if the value of the parameter "local_time.summer_time" is set to 1 (Enabled).</p> <p><b>Web User Interface:</b> Settings-&gt;Time &amp; Date-&gt;End Date</p> <p><b>Handset User Interface:</b> None</p>		
local_time.offset_time	Integer from -300 to 300	Blank
<p><b>Description:</b> Configures the offset time (in minutes) of DST.</p> <p><b>Note:</b> It works only if the value of the parameter "local_time.summer_time" is set to 1 (Enabled).</p> <p><b>Web User Interface:</b> Settings-&gt;Time &amp; Date-&gt;Offset(minutes)</p> <p><b>Handset User Interface:</b> None</p>		

**To configure the 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 name or IP address in the **Primary Server** and **Secondary Server** field respectively.
5. Enter the desired time interval in the **Synchronism(15~86400s)** field.
6. Mark the **Enabled** radio box in the **Daylight Saving Time** field.
  - 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.

The screenshot shows the 'Time & Date' configuration page. The 'Fixed Type' field has 'DST by Week' selected. The 'End Date' field is set to Month 4, Day 6, Hour 2. A red box highlights the Time Zone, Daylight Saving Time, Fixed Type, Start Date, End Date, and Offset fields.

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

The screenshot shows the 'Time & Date' configuration page. The 'Fixed Type' field has 'DST by Week' selected. The 'Start Date' and 'End Date' fields are set to January, First in Month, Sunday, 00:00. A red box highlights the Time Zone, Daylight Saving Time, Fixed Type, Start Date, End Date, and Offset fields.

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

**Note** If the location you select does not use daylight saving time, the fields of Start Date, End Date and Offset will be left blank.

## Customizing an AutoDST Template File

The time zone and corresponding DST pre-configurations exist in the AutoDST file. If the DST is set to Automatic, the IP DECT phone obtains the DST configuration from the AutoDST file. You can customize the AutoDST file if required. The AutoDST file allows you to add or modify time zone and DST settings for your area each year.

Before customizing, you need to obtain the AutoDST file. You can ask the distributor or Yealink FAE for DST template. You can also obtain the DST template online:

<http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage>. For more information on obtaining the template file, refer to [Obtaining Configuration Files and Resource Files](#) on page 15.

The following table lists description of each element in the template file:

Element	Type	Values	Description
<b>DSTData</b>	required	no	File root element
<b>DST</b>	required	no	Time Zone item's root element
<b>szTime</b>	required	[+/-][X]:[Y], X=0~14, Y=0~59	Time Zone
<b>szZone</b>	required	String (if the content is more than one city, it is the best to keep their daylight saving time the same)	Time Zone name
<b>iType</b>	optional	0/1 0: DST by Date 1: DST by Week	DST time type (This item is needed if you want to configure DST.)
<b>szStart</b>	optional	<b>Month/Day/Hour</b> (for <b>iType=0</b> ) Month: 1~12 Day: 1~31 Hour: 0 (midnight)~23 <b>Month/Week of Month/Day of Week/Hour of Day</b> (for <b>iType=1</b> ) Month: 1~12 Week of Month: 1~5 (the last week) Day of Week: 1~7 Hour of Day: 0 (midnight)~23	Start time of the DST
<b>szEnd</b>	optional	Same as szStart	End time of the DST
<b>szOffset</b>	optional	Integer from -300 to 300	The offset time (in minutes) of DST

**When customizing an AutoDST file, learn the following:**

- <DSTData> indicates the start of a template and </DSTData> indicates the end of a template.
- Add or modify time zone and DST settings between <DSTData> and </DSTData>.
- The display order of time zone is corresponding to the szTime order specified in the AutoDST.xml file.
- If the start time of DST is greater than the end time, the valid time of DST is from the start time of this year to the end time of the next year.

**Customizing an AutoDST file:**

1. Open the AutoDST file using an ASCII editor.
2. Add or modify time zone and DST settings as you want in the AutoDST file.

**Example 1:**

To modify the DST settings for the existing time zone "+5 Pakistan(Islamabad)" and add DST settings for the existing time zone "+5:30 India(Calcutta)".

```

AutoDST.xml x
0 10 20 30 40 50 60 70 80 90 100 110
<DST szTime="+3:30" szZone="Iran (Teheran)" iType="0" szStart="3/22/0" szEnd="9/22/0" szOffset="60"/>
<DST szTime="+4" szZone="Armenia (Yerevan)" iType="1" szStart="3/5/7/2" szEnd="10/5/7/3" szOffset="60"/>
<DST szTime="+4" szZone="Azerbaijan (Baku)" iType="1" szStart="3/5/7/4" szEnd="10/5/7/5" szOffset="60"/>
<DST szTime="+4" szZone="Georgia (Tbilisi)" />
<DST szTime="+4" szZone="Kazakhstan (Aktau)" />
<DST szTime="+4" szZone="Russia (Samara)" />
<DST szTime="+4:30" szZone="Afghanistan (Kabul)" />
<DST szTime="+5" szZone="Kazakhstan (Aqtobe)" />
<DST szTime="+5" szZone="Kyrgyzstan (Bishkek)" />
<DST szTime="+5" szZone="Pakistan (Islamabad)" iType="0" szStart="4/15/0" szEnd="11/1/0" szOffset="60"/>
<DST szTime="+5" szZone="Russia (Chelyabinsk)" />
<DST szTime="+5:30" szZone="India (Calcutta)" iType="1" szStart="9/5/7/3" szEnd="4/1/7/2" szOffset="60"/>
<DST szTime="+5:45" szZone="Nepal (Katmandu)" />
<DST szTime="+6" szZone="Kazakhstan (Astana, Almaty)" />
<DST szTime="+6" szZone="Russia (Novosibirsk, Omsk)" />
<DST szTime="+6:30" szZone="Myanmar (Naypyitaw)" />
<DST szTime="+7" szZone="Russia (Krasnoyarsk)" />
<DST szTime="+7" szZone="Thailand (Bangkok)" />
<DST szTime="+8" szZone="China (Beijing)" />
<DST szTime="+8" szZone="Singapore (Singapore)" />
    
```

**Example 2:**

Add a new time zone (+6 Paradise) with daylight saving time 30 minutes.

```

AutoDST.xml x
10 20 30 40 50 60 70 80 90
<DST szTime="+4:30" szZone="Afghanistan (Kabul)" />
<DST szTime="+5" szZone="Kazakhstan (Aqtobe)" />
<DST szTime="+5" szZone="Kyrgyzstan (Bishkek)" />
<DST szTime="+5" szZone="Pakistan (Islamabad)" iType="0" szStart="4/15/0" szEnd="11/1/0" />
<DST szTime="+5" szZone="Russia (Chelyabinsk)" />
<DST szTime="+5:30" szZone="India (Calcutta)" />
<DST szTime="+5:45" szZone="Nepal (Katmandu)" />
<DST szTime="+6" szZone="Paradise" iType="1" szStart="3/5/7/2" szEnd="10/5/7/3" szOffset="30"/>
<DST szTime="+6" szZone="Kazakhstan (Astana, Almaty)" />
<DST szTime="+6" szZone="Russia (Novosibirsk, Omsk)" />
<DST szTime="+6:30" szZone="Myanmar (Naypyitaw)" />
<DST szTime="+7" szZone="Russia (Krasnoyarsk)" />
<DST szTime="+7" szZone="Thailand (Bangkok)" />
<DST szTime="+8" szZone="China (Beijing)" />
<DST szTime="+8" szZone="Singapore (Singapore)" />
<DST szTime="+8" szZone="Australia (Perth)" iType="1" szStart="10/1/7/2" szEnd="3/5/7/3" />
<DST szTime="+8" szZone="Russia (Irkutsk, Ulan-Ude)" />
<DST szTime="+8:45" szZone="Eucla" />
<DST szTime="+9" szZone="Korea (Seoul)" />
<DST szTime="+9" szZone="Japan (Tokyo)" />
<DST szTime="+9" szZone="Russia (Yakutsk, Chita)" />
<DST szTime="+9:30" szZone="Australia (Adelaide)" iType="1" szStart="10/1/7/2" szEnd="4/1/7/3" />
<DST szTime="+9:30" szZone="Australia (Darwin)" />
<DST szTime="+10" szZone="Australia (Sydney, Melbourne, Canberra)" iType="1" szStart="10/1/7/2" />
<DST szTime="+10" szZone="Australia (Brisbane)" />
    
```

3. Save this file and place it to the provisioning server (e.g., 192.168.1.100).
4. Specify the access URL of the AutoDST file in the configuration files.

### Procedure

The access URL of the AutoDST file can be specified using the configuration files.

<b>Configuration File</b>	<MAC>.cfg	Specify the access URL of the AutoDST file. <b>Parameters:</b> auto_dst.url
---------------------------	-----------	---

### Details of Configuration Parameters:

Parameters	Permitted Values	Default
auto_dst.url	URL within 511 characters	Blank
<p><b>Description:</b> Configures the access URL of the AutoDST file (AutoDST.xml).</p> <p><b>Example:</b> auto_dst.url = tftp://192.168.1.100/AutoDST.xml</p> <p>During the auto provisioning process, the IP DECT phone connects to the provisioning server "192.168.1.100", and downloads the AutoDST file "AutoDST.xml".</p> <p><b>Note:</b> It works only if the value of the parameter "local_time.summer_time" is set to 2 (Automatic).</p> <p><b>Web User Interface:</b> None</p> <p><b>Handset User Interface:</b> None</p>		

## Input Method

### Specifying the Default Input Method

In addition to customizing the input method file, you can also specify the default input method for the IP DECT phone when searching for contacts.

## Procedure


Specify the default input methods using the configuration files.

<b>Configuration File</b>	y000000000025.cfg	Specify the default input method when searching for contacts. <b>Parameter:</b> directory.search_default_input_method
---------------------------	-------------------	---

### Details of Configuration Parameters:

Parameters	Permitted Values	Default
directory.search_default_input_method	Integer from 1 to 12	1
<p><b>Description:</b> Configures the default input method when the user searches for contacts in the Local Directory, LDAP, Remote Phone Book or Blacklist.</p> <p>1-Abc 2-123 3-ABC 4-abc 5-ABΓ 6-AAÄÅ 7-aäå 8-SŠŠ 9-sšš 10-aбв 11-AEB 12-גבא</p> <p><b>Example:</b> directory.search_default_input_method = 1</p> <p><b>Note:</b> It works only when the corresponding input method is enabled via the handset at the path: <b>OK-&gt;Settings-&gt;Display-&gt;Input Method.</b></p> <p><b>Web User Interface:</b> None</p> <p><b>Handset User Interface:</b> None</p>		

To configure the input method via the handset:

1. Press  to enter the main menu.
2. Select **Settings->Display->Input Method**.  
The LCD screen displays all available input methods.
3. Press **▲** or **▼** to highlight the desired input method.
4. Press the **Change** soft key to check or uncheck the checkbox.

## Key As Send

Key as send allows assigning the pound key or asterisk key as the send key.

### Procedure

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

<b>Configuration File</b>	y000000000025.cfg	Configure a send key. <b>Parameter:</b> features.key_as_send
<b>Local</b>	Web User Interface	Configure a send key. <b>Navigate to:</b> http://<phoneIPAddress>/servlet ?p=features-general&q=load

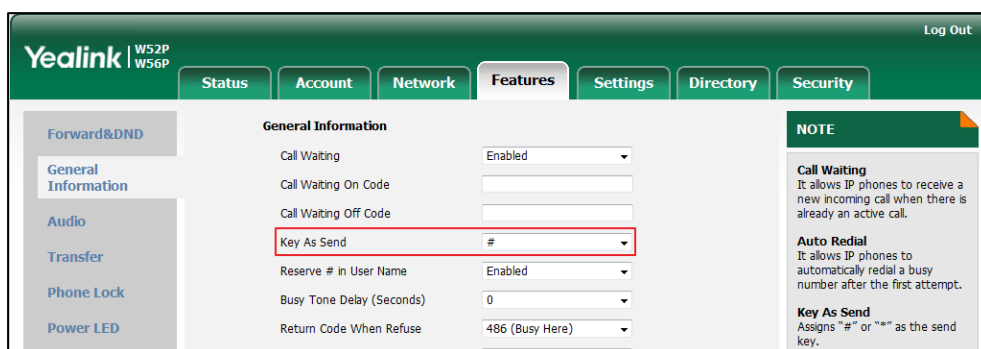
### Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.key_as_send	0, 1 or 2	1
<p><b>Description:</b> Configures the “#” key or “*” key as the send key.</p> <p><b>0-Disabled</b> <b>1-# key</b> <b>2-* key</b></p> <p>If it is set to 0 (Disabled), neither “#” key nor “*” key can be used as the 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.</p> <p><b>Web User Interface:</b> Features-&gt;General Information-&gt;Key As Send</p> <p><b>Handset User Interface:</b></p>		

Parameters	Permitted Values	Default
None		

To configure key as send via web user interface:

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



3. Click **Confirm** to accept the change or the **Cancel** soft key to cancel.

## 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 DECT phone dial plan. Dial plan is a string of characters that governs the way for IP DECT phones to process the inputs received from the IP DECT phone’s keypads. The IP DECT 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 DECT phone will replace the number with "90012354599". "\$1" means 3 digits in the first parenthesis, that is, "235". "\$2" means 2 digits in the second parenthesis, that is, "99".

## Replace Rule

Replace rule is an alternative string that replaces the numbers entered by the user. The IP DECT 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 how to customize a replace rule template, refer to [Customizing Replace Rule Template File](#) on page 151.

### Procedure

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

<b>Configuration File</b>	y000000000025.cfg	Create the replace rule for the IP DECT phone. <b>Parameters:</b> dialplan.replace.prefix.X dialplan.replace.replace.X dialplan.replace.line_id.X
<b>Local</b>	Web User Interface	Create the replace rule for the IP

		<p>DECT phone.</p> <p><b>Navigate to:</b></p> <p>http://&lt;phoneIPAddress&gt;/servlet ?p=settings-dialplan&amp;q=load</p>
--	--	--

**Details of Configuration Parameters:**

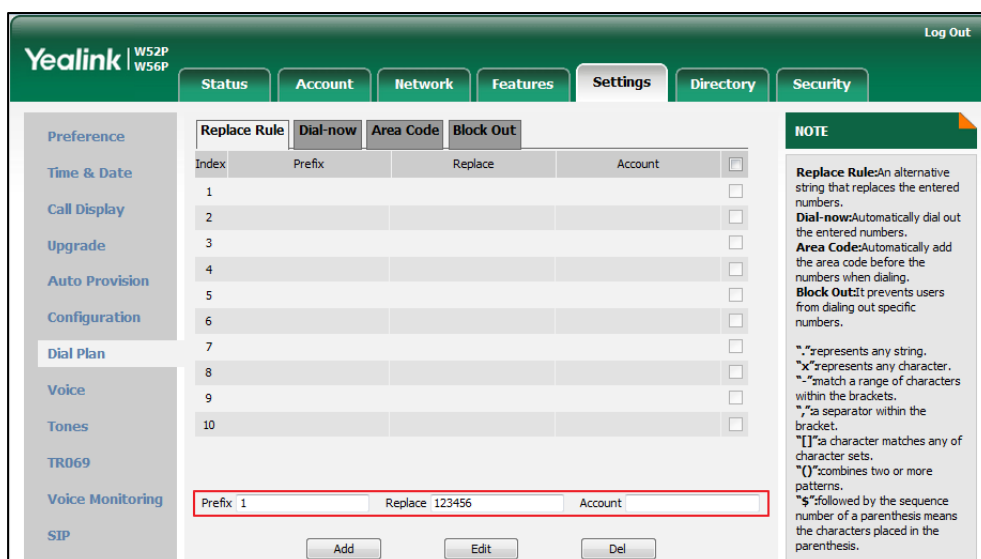
Parameters	Permitted Values	Default
<p><b>dialplan.replace.prefix.X</b> (X ranges from 1 to 100)</p>	<p>String within 32 characters</p>	<p>Blank</p>
<p><b>Description:</b> Configures the entered number to be replaced.</p> <p><b>Example:</b> dialplan.replace.prefix.1 = 1</p> <p><b>Web User Interface:</b> Settings-&gt;Dial Plan-&gt;Replace Rule-&gt;Prefix</p> <p><b>Handset User Interface:</b> None</p>		
<p><b>dialplan.replace.replace.X</b> (X ranges from 1 to 100)</p>	<p>String within 32 characters</p>	<p>Blank</p>
<p><b>Description:</b> Configures the alternate number to replace the entered number.</p> <p><b>Example:</b> dialplan.replace.prefix.1 = 1 and dialplan.replace.replace.1 = 123456</p> <p>When you enter the number "1" and press the send key, the entered number "1" will be replaced by the number "123456".</p> <p><b>Web User Interface:</b> Settings-&gt;Dial Plan-&gt;Replace Rule-&gt;Replace</p> <p><b>Handset User Interface:</b> None</p>		
<p><b>dialplan.replace.line_id.X</b> (X ranges from 1 to 100)</p>	<p>Integer from 0 to 5</p>	<p>Blank (for all lines)</p>
<p><b>Description:</b> Configures the desired line to apply the replace rule. The digit 0 stands for all lines. If it is left blank, the replace rule will apply to all lines on the IP DECT phone.</p> <p><b>Example:</b> dialplan.replace.line_id.1 = 1,2</p>		

Parameters	Permitted Values	Default
<p><b>Note:</b> Multiple line IDs are separated by commas.</p> <p><b>Web User Interface:</b> Settings-&gt;Dial Plan-&gt;Replace Rule-&gt;Account</p> <p><b>Handset User Interface:</b> None</p>		

**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.
4. Enter the desired line ID in the **Account** field or leave it blank.

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



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

## Customizing Replace Rule Template File

The replace rule template helps with the creation of multiple replace rules.

You can ask the distributor or Yealink FAE for replace rule template. You can also obtain the replace rule template online:

<http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage>. For more information on obtaining the replace rule template, refer to [Obtaining Configuration Files and Resource Files](#) on page 15.

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.
- When specifying the desired line(s) to apply the replace rule, the valid values are 0 and line ID. Multiple line IDs are separated by commas.
- At most 100 replace rules can be added to the IP DECT phone.

The expression syntax in the replace rule template is the same as that introduced in the section [Dial Plan](#) on page 148.

**To customize a replace rule template:**

1. Open the template file using an ASCII editor.
2. Create replace rules between <DialRule> and </DialRule>.

**For example:**

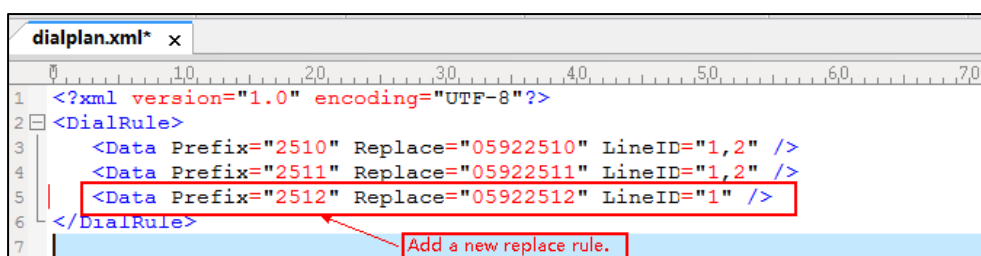
```
<Data Prefix="2512" Replace="05922512" LineID="1" />
```

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 you leave it blank or enter 0, this replace rule will apply to all lines.



If you want to change the replace rule, specify the values within double quotes.

3. Save the change and place this file to the provisioning server.
4. Specify the access URL of the replace rule template in the configuration files.

**Procedure**

Specify the access URL of the replace rule template using configuration files.

<p><b>Configuration File</b></p>	<p>y000000000025.cfg</p>	<p>Specify the access URL of the replace rule template.</p> <p><b>Parameter:</b></p> <p>dialplan_replace_rule.url</p>
----------------------------------	--------------------------	---

**Details of Configuration Parameters:**

Parameters	Permitted Values	Default
dialplan_replace_rule.url	URL within 511 characters	Blank
<p><b>Description:</b> Configures the access URL of the replace rule template file.</p> <p><b>Example:</b> dialplan_replace_rule.url = http://192.168.10.25/dialplan.xml</p> <p>During the auto provisioning process, the IP DECT phone connects to the provisioning server "192.168.10.25", and downloads the replace rule file "dialplan.xml".</p> <p><b>Web User Interface:</b> None</p> <p><b>Handset User Interface:</b> None</p>		

## Dial-now

Dial-now is a string used to match numbers entered by the user. When entered numbers match the predefined dial-now rule, the IP DECT phone will automatically dial out the numbers without pressing the send key. The IP DECT 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 how to customize a dial-now template, refer to [Customizing Dial-now Template File](#) on page 156.

### Delay Time for Dial-now Rule

The IP DECT phone 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.

<b>Configuration File</b>	y000000000025.cfg	Create the dial-now rule for the IP DECT phone. <b>Parameters:</b> dialplan.dialnow.rule.X dialplan.dialnow.line_id.X
		Configure the delay time for the dial-now rule. <b>Parameters:</b>

		phone_setting.dialnow_delay
<b>Local</b>	Web User Interface	Create the dial-now rule for the IP DECT phone. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=settings-dialplan&q=load
		Configure the delay time for the dial-now rule. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=features-general&q=load

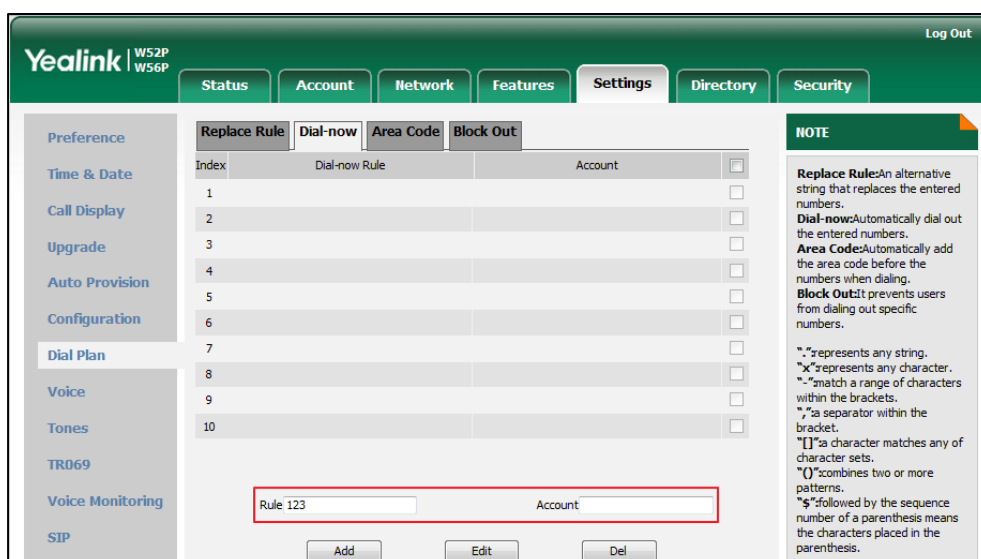
**Details of Configuration Parameters:**

Parameters	Permitted Values	Default
<b>dialplan.dialnow.rule.X</b> (X ranges from 1 to 100)	<b>String within 511 characters</b>	<b>Blank</b>
<p><b>Description:</b> Configures the dial-now rule (the string used to match the numbers entered by the user). When entered numbers match the predefined dial-now rule, the IP DECT phone will automatically dial out the numbers without pressing the send key.</p> <p><b>Example:</b> dialplan.dialnow.rule.1 = 123</p> <p><b>Web User Interface:</b> Settings-&gt;Dial Plan-&gt;Dial-now-&gt;Rule</p> <p><b>Handset User Interface:</b> None</p>		
<b>dialplan.dialnow.line_id.X</b> (X ranges from 1 to 100)	<b>Integer from 0 to 5</b>	<b>Blank (for all lines)</b>
<p><b>Description:</b> Configures the desired line to apply the dial-now rule. The digit 0 stands for all lines. If it is left blank, the dial-now rule will apply to all lines on the IP DECT phone.</p> <p><b>Example:</b> dialplan.dialnow.line_id.1 = 1,2</p> <p><b>Web User Interface:</b> Settings-&gt;Dial Plan-&gt;Dial-now-&gt;Account</p> <p><b>Handset User Interface:</b></p>		

Parameters	Permitted Values	Default
None		
phone_setting.dialnow_delay	Integer from 0 to 14	1
<p><b>Description:</b></p> <p>Configures the delay time (in seconds) for the dial-now rule.</p> <p>When entered numbers match the predefined dial-now rule, the IP DECT phone will automatically dial out the entered number after the designated delay time.</p> <p>If it is set to 0, the IP DECT phone will automatically dial out the entered number immediately.</p> <p><b>Web User Interface:</b></p> <p>Features-&gt;General Information-&gt;Time-Out for Dial-Now Rule</p> <p><b>Handset User Interface:</b></p> <p>None</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 this field blank or enter 0, the dial-now rule will apply to all accounts on the IP DECT 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**.
2. Enter the desired time within 0-14 (in seconds) in the **Time-Out for Dial-Now Rule** field.

The screenshot shows the Yealink W52P/W56P web interface. The 'Features' tab is selected, and the 'General Information' sub-tab is active. The 'Time-Out for Dial-Now Rule' field is highlighted with a red box and contains the value '1'. Other fields include 'Call Waiting' (Enabled), 'Call Waiting On Code', 'Call Waiting Off Code', 'Key As Send' (#), 'Reserve # in User Name' (Enabled), 'Busy Tone Delay (Seconds)' (0), 'Return Code When Refuse' (486 (Busy Here)), 'Return Code When DND' (480 (Temporarily Unavail)), 'Feature Key Synchronization' (Disabled), and 'RFC 2543 Hold' (Disabled). A 'NOTE' sidebar on the right provides details for 'Call Waiting', 'Auto Redial', 'Key As Send', and 'Hotline'.

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

## Customizing Dial-now Template File

The dial-now template helps with the creation of multiple dial-now rules. After setup, place the dial-now template to the provisioning server and specify the access URL in the configuration files.

You can ask the distributor or Yealink FAE for dial-now template. You can also obtain the dial-now template online:

<http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage>. For more information on obtaining the dial-now template, refer to [Obtaining Configuration Files and Resource Files](#) on page 15.

When editing a dial-now template, learn the following:

- <DialNow> indicates the start of a template and </DialNow> indicates the end of a template.
- When specifying the desired line(s) for the dial-now rule, the valid values are 0 and line ID. Multiple line IDs are separated by commas.
- At most 100 rules can be added to the IP DECT phone.

The expression syntax in the dial-now rule template is the same as that introduced in the section [Dial Plan](#) on page 148.



**To customize a dial-now template:**

1. Open the template file using an ASCII editor.
2. Create dial-now rules between <DialNow> and </DialNow>.

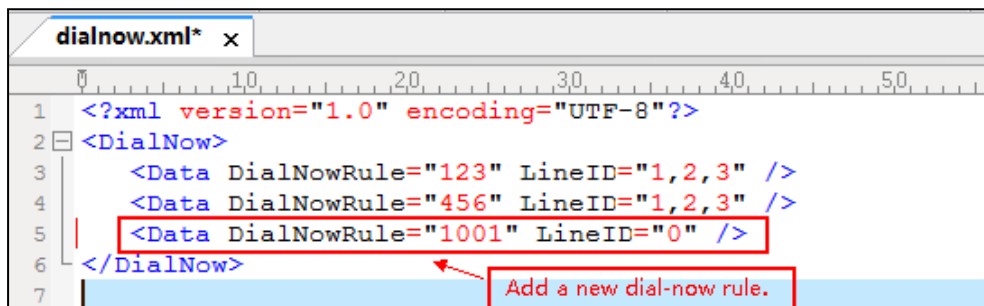
**For example:**

```
<Data DialNowRule="1001" LineID="0" />
```

Where:

DialNowRule="" specifies the dial-now rule.

LineID="" specifies the desired line(s) for this rule. When you leave it blank or enter 0, this dial-now rule will apply to all lines.



If you want to change the dial-now rule, specify the values within double quotes.

3. Save the change and place this file to the provisioning server.
4. Specify the access URL of the dial-now template.

**Procedure**

Specify the access URL of the dial-now template using configuration files.

<b>Configuration File</b>	y000000000025.cfg	Configure the access URL of the dial-now template. <b>Parameter:</b> dialplan_dialnow.url
---------------------------	-------------------	---

**Details of Configuration Parameters:**

Parameters	Permitted Values	Default
dialplan_dialnow.url	URL within 511 characters	Blank
<p><b>Description:</b> Configures the access URL of the dial-now rule template file.</p> <p><b>Example:</b> dialplan_dialnow.url = http://192.168.10.25/dialnow.xml</p> <p>During the auto provisioning process, the IP DECT phone connects to the provisioning</p>		

Parameters	Permitted Values	Default
server "192.168.10.25", and downloads the dial-now rule file "dialnow.xml". <b>Web User Interface:</b> None <b>Handset User Interface:</b> None		

## Area Code

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

### Procedure

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

<b>Configuration File</b>	y000000000025.cfg	Create the area code rule and specify the maximum and minimum lengths of entered numbers. <b>Parameters:</b> dialplan.area_code.code dialplan.area_code.min_len dialplan.area_code.max_len dialplan.area_code.line_id
<b>Local</b>	Web User Interface	Create the area code rule and specify the maximum and minimum lengths of entered numbers. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=settings-dialplan&q=load

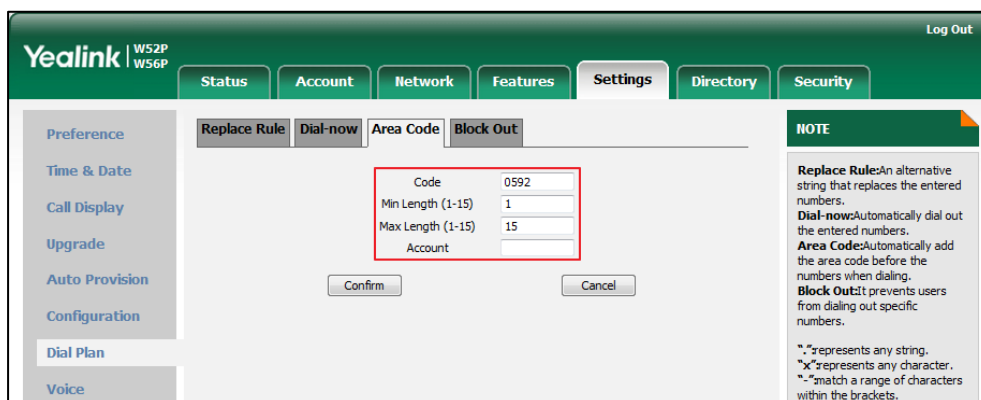
### Details of Configuration Parameters:

Parameters	Permitted Values	Default
dialplan.area_code.code	String within 16 characters	Blank
<p><b>Description:</b> Configures the area code to be added before the entered numbers when dialing out.</p> <p><b>Example:</b> dialplan.area_code.code = 0592</p> <p><b>Note:</b> The length of the entered number must be between the minimum length configured by the parameter "dialplan.area_code.min_len" and the maximum length configured by the parameter "dialplan.area_code.max_len".</p> <p><b>Web User Interface:</b> Settings-&gt;Dial Plan-&gt;Area Code-&gt;Code</p> <p><b>Handset User Interface:</b> None</p>		
dialplan.area_code.min_len	Integer from 1 to 15	1
<p><b>Description:</b> Configures the minimum length of the entered numbers.</p> <p><b>Web User Interface:</b> Settings-&gt;Dial Plan-&gt;Area Code-&gt;Min Length (1-15)</p> <p><b>Handset User Interface:</b> None</p>		
dialplan.area_code.max_len	Integer from 1 to 15	15
<p><b>Description:</b> Configures the maximum length of the entered numbers.</p> <p><b>Note:</b> The value must be larger than the minimum length.</p> <p><b>Web User Interface:</b> Settings-&gt;Dial Plan-&gt;Area Code-&gt;Max Length (1-15)</p> <p><b>Handset User Interface:</b> None</p>		
dialplan.area_code.line_id	Integer from 0 to 5	Blank (for all lines)
<p><b>Description:</b></p>		

Parameters	Permitted Values	Default
<p>Configures the desired line to apply the area code rule. The digit 0 stands for all lines. If it is left blank, the area code rule will apply to all lines on the IP DECT phone.</p> <p><b>Example:</b> dialplan.area_code.line_id = 1</p> <p><b>Note:</b> Multiple line IDs are separated by commas.</p> <p><b>Web User Interface:</b> Settings-&gt;Dial Plan-&gt;Area Code-&gt;Account</p> <p><b>Handset User Interface:</b> None</p>		

**To configure an area code rule via web user interface:**

1. Click on **Settings->Dial Plan->Area Code**.
2. Enter the 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 this field blank or enter 0, the area code rule will apply to all accounts on the IP DECT 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 predefined block out rule, the LCD screen prompts "forbidden number". IP DECT phones support up to 10 block out rules.

## Procedure

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

<b>Configuration File</b>	y000000000025.cfg	Create the block out rule for the IP DECT phone. <b>Parameters:</b> dialplan.block_out.number.X dialplan.block_out.line_id.X
<b>Local</b>	Web User Interface	Create the block out rule for the IP DECT phone. <b>Navigate to:</b> http://<phoneIPAddress>/servlet ?p=settings-dialplan&q=load

### Details of Configuration Parameters:

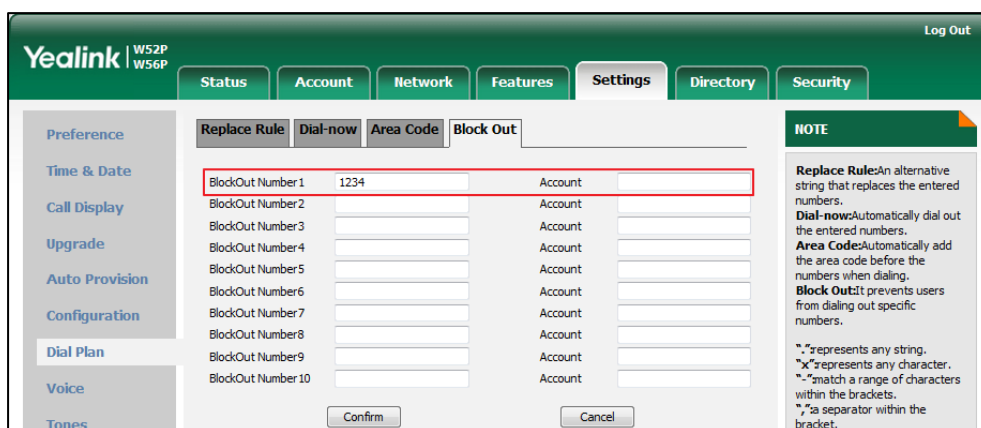
Parameters	Permitted Values	Default
<b>dialplan.block_out.number.X</b> (X ranges from 1 to 10)	<b>String within 32 characters</b>	<b>Blank</b>
<p><b>Description:</b> Configures the block out numbers.</p> <p><b>Example:</b> dialplan.block_out.number.1 = 4321</p> <p>When you dial the number "4321" on your phone, the dialing will fail and the LCD screen will prompt "forbidden number".</p> <p><b>Web User Interface:</b> Settings-&gt;Dial Plan-&gt;Block Out-&gt;BlockOut NumberX</p> <p><b>Handset User Interface:</b> None</p>		
<b>dialplan.block_out.line_id.X</b> (X ranges from 1 to 10)	<b>Integer from 0 to 5</b>	<b>Blank (for all lines)</b>
<p><b>Description:</b> Configures the desired line to apply the block out rule. The digit 0 stands for all lines. If it is left blank, the block out rule will apply to all lines on the IP DECT phone.</p> <p><b>Example:</b> dialplan.block_out.line_id.1 = 1,2,3</p> <p><b>Note:</b> Multiple line IDs are separated by commas.</p>		

Parameters	Permitted Values	Default
<b>Web User Interface:</b> Settings->Dial Plan->Block Out->Account  <b>Handset User Interface:</b> None		

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 NumberX** field.
3. Enter the desired line ID in the **Account** field or leave it blank.

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



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

## Auto Dial

The IP DECT phones support dial out a pre-configured number first when the user places a call automatically. Dials out a call using the account with this feature enabled. The SIP server may then prompt the user to enter an activation code for call service. Only if the user enters a valid activation code, the IP DECT phone will use this account to dial out a call successfully.

Auto dial feature is configurable on a per-line basis and depends on support from a SIP server.

### Procedure

Auto dial can be configured using the configuration files.

<b>Configuration File</b>	y000000000025.cfg	Configure auto dial feature. <b>Parameter:</b> account.X.auto_dial_enable
		Specify the number that the phone first dials out. <b>Parameter:</b> account.X.auto_dial_num

### Details of Configuration Parameters:

Parameter	Permitted Values	Default
<b>account.X.auto_dial_enable</b>	<b>0 or 1</b>	<b>0</b>
<p><b>Description:</b> Enables or disables the phone to automatically dial out a pre-configured number first when the user places a call using the account X.</p> <p>0-Disabled 1-Enabled</p> <p>If it is set to 1 (Enabled), the phone will automatically dial out the pre-configured number (configured by the parameter "account.X.auto_dial_num") before dialing a call.</p> <p><b>Note:</b> The server may prompt the user to enter an activation code to use this account for call service. This feature requires support from the SIP server.</p> <p><b>Web User Interface:</b> None</p> <p><b>Handset User Interface:</b> None</p>		
<b>account.X.auto_dial_num</b>	<b>String within 32 characters</b>	<b>Blank</b>
<p><b>Description:</b> Configures the number that the phone automatically dials out first when the user places a call.</p> <p><b>Note:</b> It works only if the value of the parameter "account.X.auto_dial_enable" is set to 1 (Enabled).</p> <p><b>Web User Interface:</b> None</p>		

Parameter	Permitted Values	Default
<b>Handset User Interface:</b>		
None		

## Local Directory

You can store the frequently used contacts in the handset's local directory, where names and numbers can be freely added, deleted and edited. You can store up to 100 contacts per handset, each with a name, a mobile number and an office number. Yealink IP DECT phones support both \*.xml and \*.csv format contact files.

### Procedure

Local Directory can be configured using the configuration files or locally.

<b>Configuration File</b>	y000000000025.cfg	Specify the access URL of the directory template file. <b>Parameter:</b> handset.X.contact_list.url
<b>Local</b>	Web User Interface	Configure the Directory. <b>Navigate to:</b> http://<phoneIPAddress>/servlet ?p=contactsbasic&q=load

### Details of the Configuration Parameter:

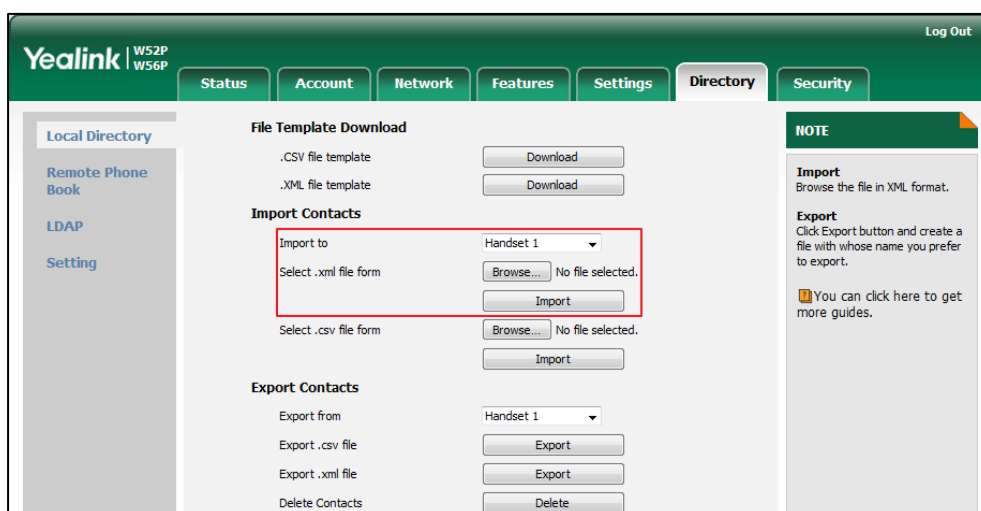
Parameter	Permitted Values	Default
<b>handset.X.contact_list.url</b> (X ranges from 1 to 5)	<b>URL within 511 characters</b>	<b>Blank</b>
<p><b>Description:</b> Configures the access URL of the contact file of handset X. The format of the file must be *.xml.</p> <p><b>Example:</b> handset.1.contact_list.url= http://192.168.1.20/favorite_setting.xml</p> <p>During the auto provisioning process, the IP DCET phone connects to the provisioning server "192.168.1.20", and downloads the directory file "favorite_setting.xml".</p> <p><b>Web User Interface:</b> Directory-&gt;Local Directory-&gt;Import Contacts</p> <p><b>Handset User Interface:</b></p>		



Parameter	Permitted Values	Default
None		

To import an XML contact list file via web user interface:

1. Click on **Directory->Local Directory**.
2. Select the desired handset from the pull-down list of **Import to**.
3. Click **Browse** to locate a contact list file (the file format must be \*.xml) from your local system.

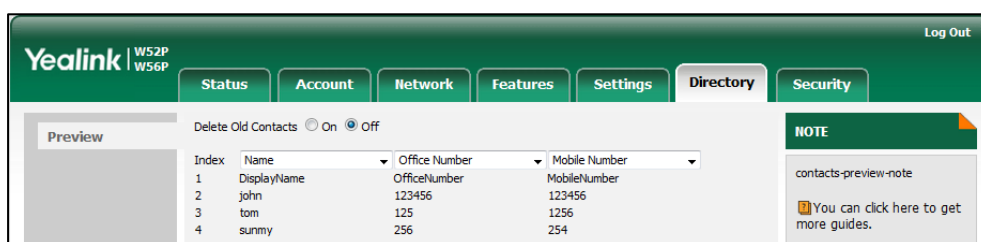


4. Click **Import** to import the contact list.
5. Click **OK** to complete importing the contact list.

To import a CSV contact list file via web user interface:

1. Click on **Directory->Local Directory**.
2. Select the desired handset from the pull-down list of **Import to**.
3. Click **Browse** to locate a contact list file (the file format must be \*.csv) from your local system.
4. Click **Import** to import the contact list.
5. (Optional.) Mark the **On** radio box in the **Delete Old Contacts** field.  
It will delete all existing contacts while importing the contact list.
6. Select the contact information you want to import into the local directory from the pull-down list of **Index**.

At least one item should be selected to be imported into the local directory.



7. Click **Import** to complete importing the contact list.

**To export a contact list via web user interface:**

1. Click on **Directory->Local Directory**.
2. In **Export Contacts** block, click **Export** from the **Export.xml file** (or **Export.csv file**) field.
3. Click **Save** to save the contact list to your local system.

**To delete contacts via web user interface:**

1. Click on **Directory->Local Directory**.
2. In **Export Contacts** block, click **Delete** from the **Delete Contacts** field.

## Customizing a Directory Template File

You can add contacts one by one on the IP DECT phone directly. You can also add multiple contacts at a time and/or share contacts between IP DECT 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. The existing local contacts on the IP DECT phones will be overridden by the downloaded local contacts.

You can ask the distributor or Yealink FAE for local contact template. You can also obtain the local contact template online:

<http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage>. For more information on obtaining the local contact file, refer to [Obtaining Configuration Files and Resource Files](#) on page 15.

The following table lists meaning of each variable in the local contact template file:

Element	Values	Description
<b>root_contact</b>	no	Contact list’s root element.
<b>contact</b>	no	Contact’s root element.
<b>display_name</b>	String	An element of contact. Contact name. <b>Note:</b> This value cannot be blank or duplicated.
<b>office_number</b>	String	Office number of the

Element	Values	Description
		contact.
mobile_number	String	Mobile number of the contact.

#### To customize a local contact file:

1. Open the template file using an ASCII editor.
2. 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=""/>
```

For example, configure the local directory list, edit the values within double quotes in the following strings:

```
<contact display_name="Lily" office_number="1020" mobile_number="1021"/>
```

```
<?xml version='1.0' encoding='utf-8' ?>
<root_contact>
  <contact display_name="" office_number="" mobile_number=""/>
</root_contact>
```

3. Save the change and place this file to the provisioning server.
4. Specify the access URL of the custom local contact template in the configuration files.

For example:

```
handset.1.contact_list.url = tftp://192.168.10.25/contact.xml
```

During the auto provisioning process, the IP DECT phone connects to the provisioning server "192.168.10.25", and downloads the contact file "contact.xml".

## Search Source in Dialing

Search source list in dialing allows the IP DECT phone to automatically search entries from the search source list based on the entered string, and display results on the pre-dialing screen. The user can select the desired entry to dial out quickly. The search source list can be Local Directory, History, Remote Phone Book and LDAP. The search source list can be configured using a supplied super search template file (super\_search.xml).

## Customizing a Super Search Template File

You can ask the distributor or Yealink FAE for super search template. You can also obtain the super search template online:

<http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage>. For more information on obtaining the super search template, refer to [Obtaining Configuration Files and Resource Files](#) on page 15.

The following table lists meaning of each variable in the super search template file:

Element	Values	Description
root_super_search	No	File root element
Item	No	Super search list's root element
id_name	local_directory_search calllog_search remote_directory_search ldap_search Network_directory_search	The directory list (For example, "local_directory_search" for the local directory list). <b>Note:</b> Do not edit this field.
display_name	Local Contacts History Remote Phone Book LDAP Network Directories	The display name of the directory list. <b>Note:</b> We recommend you do not edit this field.
Priority	1, 2, 3, 4 and 5. 1 is the highest priority, 5 is the lowest.	The priority of the search results.
Enable	0/1, 0: Disabled 1: Enabled	Enable or disable the IP DECT phone to search the desired directory list.

**Customizing a super search template:**

1. Open the template file using an ASCII editor.
2. For each directory list that you want to configure, edit the corresponding string in the file. For example, configure the local directory list, edit the values within double quotes in the following strings:

```
<item id_name="local_directory_search" display_name="Local Contacts"
priority="1" enable="1"/>
```

```
super_search.xml x
1 <root super_search>
2   <item id_name="local_directory_search" display_name="Local Contacts" priority="1" enable="1" />
3   <item id_name="calllog_search" display_name="History" priority="2" enable="1" />
4   <item id_name="remote_directory_search" display_name="Remote Phone book" priority="3" enable="0" />
5   <item id_name="ldap_search" display_name="LDAP" priority="4" enable="0" />
6 </root_super_search>
7
```

3. Save the change and place this file to the provisioning server (e.g., 192.168.1.20).
4. Specify the access URL of the custom super search template file in the configuration files (e.g., super\_search.url = http://192.168.1.20/super\_search.xml).

### Procedure





Search source list in dialing can be configured using the configuration files or locally.

<b>Configuration File</b>	y000000000025.cfg	Specify the access URL of the super search template file. <b>Parameter:</b> super_search.url
<b>Local</b>	Web User Interface	Configure the search source list in dialing. <b>Navigate to:</b> http://<phoneIPAddress>/servlet ?p=contacts-favorite&q=load

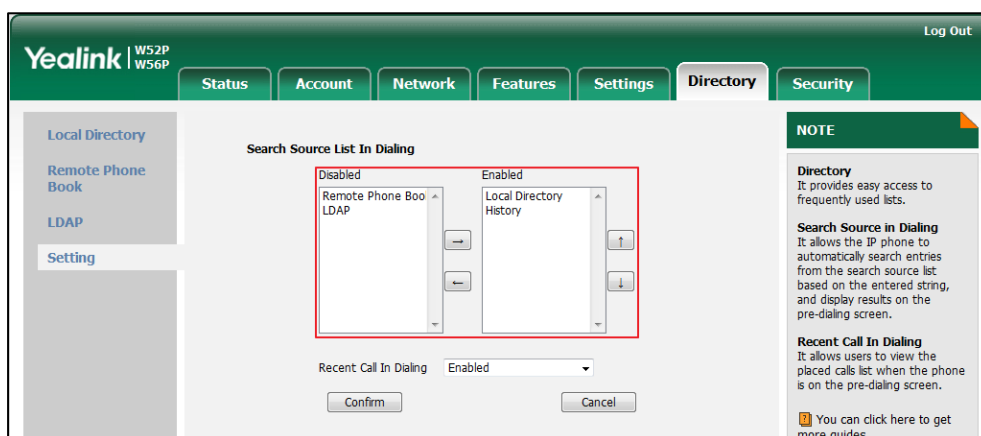
### Details of the Configuration Parameter:

Parameter	Permitted Values	Default
super_search.url	URL within 511 characters	Blank
<p><b>Description:</b> Configures the access URL of the super search template file.</p> <p><b>Example:</b> super_search.url = http://192.168.1.20/super_search.xml</p> <p>During the auto provisioning process, the IP DECT phone connects to the provisioning server "192.168.1.20", and downloads the super search template file "super_search.xml".</p> <p><b>Web User Interface:</b> Directory-&gt;Setting-&gt;Search Source List In Dialing</p> <p><b>Handset User Interface:</b> None</p>		

### To configure search source list in dialing via web user interface:

1. Click on **Directory->Setting**.
2. In the **Search Source List In Dialing** block, select the desired list from the **Disabled** column and then click .  
The selected list appears in the **Enabled** column.
3. Repeat the step 2 to add more lists to the **Enabled** column.
4. To remove a list from the **Enabled** column, select the desired list and then click .
5. To adjust the display order of search results, select the desired list and then click  or .

The LCD screen displays the search results in the adjusted order.



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

## Save Call Log

Call log contains call information such as remote party identification, time and date, and call duration. It can be used to redial previous outgoing calls, return incoming calls, and save contact information from call log lists to the contact directory.

The IP DECT phones maintain a local call log. Call log consists of four lists: Missed Calls, Placed Calls and Received Calls. Each call log list supports up to 100 entries. To store call information, you must enable save call log feature in advance.

### Procedure

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

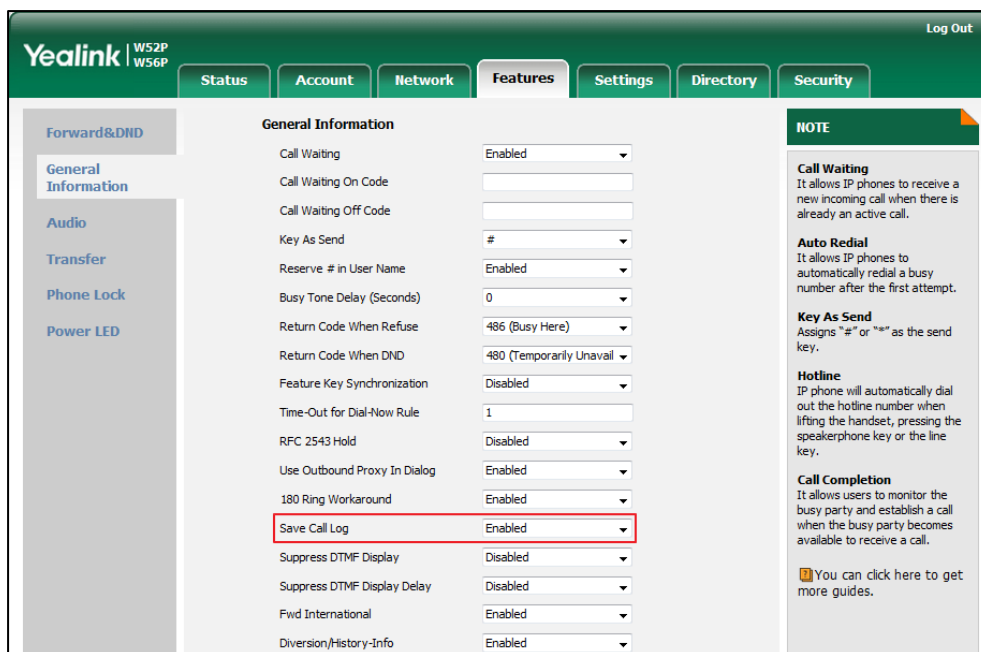
<b>Configuration File</b>	y00000000025.cfg	Configure call log feature. <b>Parameter:</b> features.save_call_history
		Configure call log display method. <b>Parameter:</b> features.cumulative_display_call_log.enable
<b>Local</b>	Web User Interface	Configure call log feature. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=features-general&q=load

**Details of the Configuration Parameter:**

Parameter	Permitted Values	Default
<b>features.save_call_history</b>	<b>0 or 1</b>	<b>1</b>
<p><b>Description:</b>            Enables or disables the IP DECT phone to save the call log.  <b>0-Disabled</b>  <b>1-Enabled</b>            If it is set to 0 (Disabled), the IP DECT phone cannot log the missed calls, placed calls and received calls in the call log lists.</p> <p><b>Web User Interface:</b>            Features-&gt;General Information-&gt;Save Call Log</p> <p><b>Handset User Interface:</b>            None</p>		
<b>features.cumulative_display_call_log.enable</b>	<b>0 or 1</b>	<b>1</b>
<p><b>Description:</b>            Enables or disables the IP DECT phone to display the same call log of a day cumulative.  <b>0-Disabled</b>  <b>1-Enabled</b>            If it is set to 0 (Disabled), the same call log will display in a list respectively.            If it is set to 1 (Enabled), the same call log of a day will display cumulatively.</p> <p><b>Web User Interface:</b>            None</p> <p><b>Handset User Interface:</b>            None</p>		

To configure call log feature 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.

## Call Waiting

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

### Procedure

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

<b>Configuration File</b>	y00000000025.cfg	Configure call waiting and call waiting tone. <b>Parameters:</b> call_waiting.enable call_waiting.tone call_waiting.on_code call_waiting.off_code
<b>Local</b>	Web User Interface	Configure call waiting and call



		waiting tone. <b>Navigate to:</b> http://<phoneIPAddress>/servlet ?p=features-general&q=load
	Handset User Interface	Configure call waiting and call waiting tone.

**Details of Configuration Parameters:**

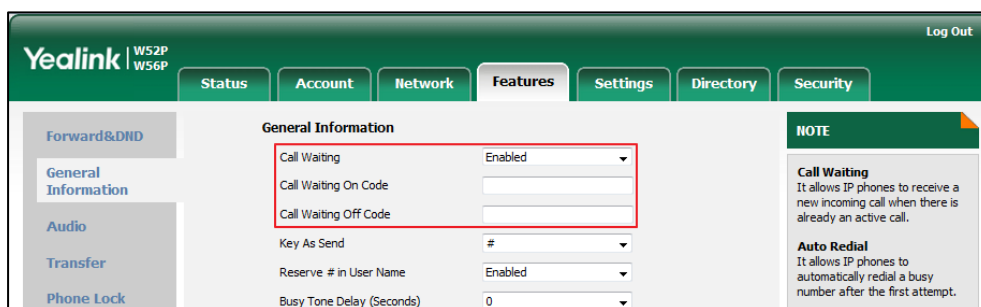
Parameters	Permitted Values	Default
<b>call_waiting.enable</b>	<b>0 or 1</b>	<b>1</b>
<p><b>Description:</b> Enables or disables call waiting feature.</p> <p><b>0-Disabled</b> <b>1-Enabled</b></p> <p>If it is set to 0 (Disabled), a new incoming call is automatically rejected by the IP DECT phone with a busy message while during a call.</p> <p>If it is set to 1 (Enabled), the LCD screen will present a new incoming call while during a call.</p> <p><b>Web User Interface:</b> Features-&gt;General Information-&gt;Call Waiting</p> <p><b>Handset User Interface:</b> OK-&gt;Call Features-&gt;Call Waiting-&gt;Status</p>		
<b>call_waiting.tone</b>	<b>0 or 1</b>	<b>1</b>
<p><b>Description:</b> Enables or disables the IP DECT phone to play the call waiting tone when the IP DECT phone receives an incoming call during a call.</p> <p><b>0-Disabled</b> <b>1-Enabled</b></p> <p>If it is set to 1 (Enabled), the IP DECT phone will perform an audible indicator when receiving a new incoming call during a call.</p> <p><b>Note:</b> It works only if the value of the parameter "call_waiting.enable" is set to 1 (Enabled).</p> <p><b>Web User Interface:</b> Features-&gt;Audio-&gt;Call Waiting Tone</p> <p><b>Handset User Interface:</b></p>		

Parameters	Permitted Values	Default
OK->Call Features->Call Waiting->Tone		
<b>call_waiting.on_code</b>	<b>String within 32 characters</b>	<b>Blank</b>
<p><b>Description:</b> Configures the call waiting on code to activate the server-side call waiting feature. The IP DECT phone will send the call waiting on code to the server when you activate call waiting feature on the IP DECT phone.</p> <p><b>Example:</b> call_waiting.on_code = *71</p> <p><b>Web User Interface:</b> Features-&gt;General Information-&gt;Call Waiting On Code</p> <p><b>Handset User Interface:</b> None</p>		
<b>call_waiting.off_code</b>	<b>String within 32 characters</b>	<b>Blank</b>
<p><b>Description:</b> Configures the call waiting off code to deactivate the server-side call waiting feature. The IP DECT phone will send the call waiting off code to the server when you deactivate call waiting feature on the IP DECT phone.</p> <p><b>Example:</b> call_waiting.off_code = *72</p> <p><b>Web User Interface:</b> Features-&gt;General Information-&gt;Call Waiting Off Code</p> <p><b>Handset User Interface:</b> None</p>		

**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.

- (Optional.) Enter the call waiting off code in the **Call Waiting Off Code** field.



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

**To configure call waiting feature via the handset:**

- Press **OK** to enter the main menu.
- Select **Call Features->Call Waiting**.
- Press **◀** or **▶** to select the desired value from the **Status** field.
- Press **◀** or **▶** to select the desired value from the **Tone** field.
- Press the **Save** soft key to accept the change or the **Back** soft key to cancel.

## Auto Answer

Auto answer allows IP DECT phones to automatically answer an incoming call. The IP DECT phones will not automatically answer the incoming call during a call even if auto answer is enabled. Auto answer is configurable on a per-line basis.

### Procedure

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

<b>Configuration File</b>	y00000000025.cfg	Configure auto answer. <b>Parameter:</b> custom.handset.auto_answer.enable
<b>Local</b>	Handset User Interface	Configure auto answer.

### Details of Configuration Parameters:

Parameters	Permitted Values	Default
custom.handset.auto_answer.enable	0 or 1	1
<b>Description:</b> Enables or disables a user to answer incoming calls by lifting the handset from the charger cradle without having to press the off-hook key.		

Parameters	Permitted Values	Default
<p><b>0</b>-Disabled  <b>1</b>-Enabled</p> <p>If it is set to 1 (Enabled), the IP DECT phone can automatically answer an incoming call.</p> <p><b>Note:</b> It works if the handset is placed in the charger cradle and the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled).</p> <p><b>Web User Interface:</b>  None</p> <p><b>Handset User Interface:</b>  OK-&gt;Settings-&gt;Telephony-&gt;Auto Answer</p>		

**To configure auto answer via the handset:**

1. Press **OK** to enter the main menu.
2. Select **Settings->Telephony->Auto Answer**.
3. Press the **Change** soft key to check or uncheck the **Auto Answer** checkbox.

## Allow IP Call

Allow IP Call feature allows IP DECT phones to receive or place an IP address call. You can neither receive nor place an IP address call if allow IP call feature is disabled.

### Procedure

Allow IP call can be configured using the configuration files or locally.

<b>Configuration File</b>	y000000000025.cfg	Configure allow IP call. <b>Parameter:</b> features.direct_ip_call_enable
<b>Local</b>	Web User Interface	Configure allow IP call. <b>Navigate to:</b> http://<phoneIPAddress>/servlet ?p=features-general&q=load

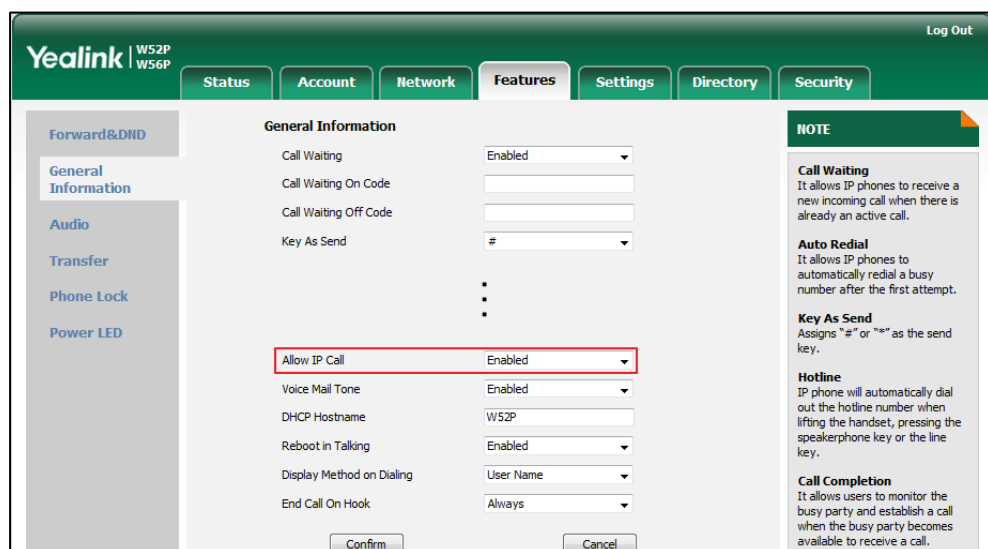
### Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.direct_ip_call_enable	0 or 1	1
<b>Description:</b>		

Parameters	Permitted Values	Default
<p>Enables or disables allow IP address call.</p> <p><b>0-Disabled</b></p> <p><b>1-Enabled</b></p> <p><b>Note:</b> If you want to receive an IP address call, make sure the value of the parameter "sip.trust_ctrl" is set to 0 (Disabled).</p> <p><b>Web User Interface:</b></p> <p>Feature-&gt;General Information-&gt;Allow IP Call</p> <p><b>Handset User Interface:</b></p> <p>None</p>		

To configure allow IP call feature via web user interface:

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



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

## Accept SIP Trust Server Only

Accept SIP trust server only enables the IP DECT phones to only accept the SIP message from your SIP server and outbound proxy server. It can prevent the phone receiving ghost calls from random numbers like 100, 1000, etc. To stop this from happening, you also need to disable allow IP call feature. For more information on allow IP call, refer to [Allow IP Call](#) on page 176.

## Procedure

Accept SIP trust server can be configured using the configuration files or locally.

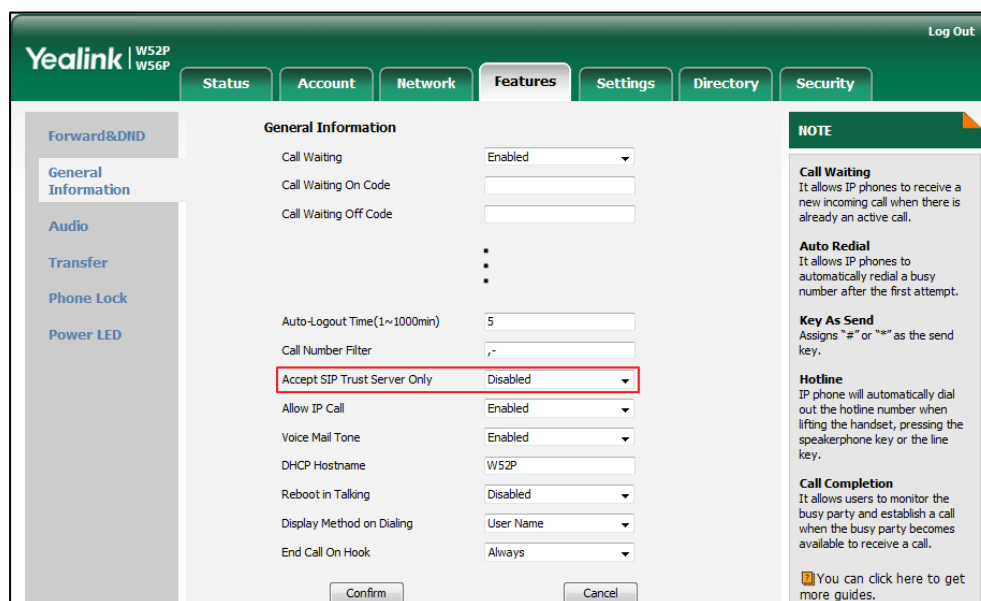
<b>Configuration File</b>	y000000000025.cfg	Configure accept SIP trust server. <b>Parameter:</b> sip.trust_ctrl
<b>Local</b>	Web User Interface	Configure accept SIP trust server. <b>Navigate to:</b> http://<phoneIPAddress>/servlet ?p=features-general&q=load

### Details of Configuration Parameters:

Parameters	Permitted Values	Default
sip.trust_ctrl	0 or 1	0
<p><b>Description:</b> Enables or disables the IP DECT phone to only accept the SIP message from the SIP and outbound proxy server.</p> <p>0-Disabled 1-Enabled</p> <p><b>Web User Interface:</b> Features-&gt;General Information-&gt;Accept SIP Trust Server Only</p> <p><b>Handset User Interface:</b> None</p>		

To configure accept SIP trust server only feature via web user interface:

1. Click on **Features->General Information**.
2. Select the desired value from the pull-down list of **Accept SIP Trust Server Only**.



3. Click **Confirm** 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. Anonymous call is configurable on a per-line basis.

Example of anonymous SIP header:

```
Via: SIP/2.0/UDP 10.3.20.14:5060;branch=z9hG4bK3074920774
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=131654239
To: <sip:1006@10.3.5.199:5060>
Call-ID: 0_288363101@10.3.20.14
CSeq: 1 INVITE
Contact: <sip:1009@10.3.20.14:5060>
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 W52P 25.80.0.10
Allow-Events: talk,hold,conference,refer,check-sync
P-Preferred-Identity: <sip:1009@10.3.5.199>
Privacy: id
Content-Length: 302
```

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

### Procedure

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

<b>Configuration File</b>	<MAC>.cfg	Configure anonymous call. <b>Parameters:</b> features.provision_anonymous_call_on_gui.enable account.X.anonymous_call account.X.send_anonymous_code account.X.anonymous_call_oncode account.X.anonymous_call_offcode
<b>Local</b>	Web User Interface	Configure anonymous call. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=account-basic&q=load&acc=0
	Handset User Interface	Configure anonymous call.

### Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.provision_anonymous_call_on_gui.enable	0 or 1	1
<b>Description:</b> Enables or disables to display the anonymous call setting on the handset. 0-Disabled 1-Enabled <b>Web User Interface:</b> None <b>Handset User Interface:</b> None		
account.X.anonymous_call (X ranges from 1 to 5)	0 or 1	0



Parameters	Permitted Values	Default
<p><b>Description:</b> Triggers the anonymous call feature to on or off for account X.</p> <p><b>0-Off</b> <b>1-On</b></p> <p>If it is set to 1 (On), the IP DECT 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><b>Web User Interface:</b> Account-&gt;Basic-&gt;Local Anonymous</p> <p><b>Handset User Interface:</b> OK-&gt;Call Features-&gt;Anonymous Call-&gt;Line X-&gt;Status (only display when the parameter "features.provision_anonymous_call_on_gui.enable" is set to 1 (Enabled))</p>		
<p><b>account.X.send_anonymous_code</b> (X ranges from 1 to 5)</p>	<p><b>0 or 1</b></p>	<p><b>0</b></p>
<p><b>Description:</b> Configures the IP DECT phone to send anonymous on/off code to activate/deactivate the server-side anonymous call feature for account X.</p> <p><b>0-Off Code</b> <b>1-On Code</b></p> <p>If it is set to 0 (Off Code), the IP DECT phone will send anonymous off code to the server when you activate/deactivate the anonymous call feature.</p> <p>If it is set to 1 (On Code), the IP DECT phone will send anonymous on code to the server when you activate/deactivate the anonymous call feature.</p> <p><b>Web User Interface:</b> Account-&gt;Basic-&gt;Send Anonymous Code</p> <p><b>Handset User Interface:</b> None</p>		
<p><b>account.X.anonymous_call_oncode</b> (X ranges from 1 to 5)</p>	<p><b>String within 32 characters</b></p>	<p><b>Blank</b></p>
<p><b>Description:</b> Configures the anonymous call on code to activate the server-side anonymous call feature for account X.</p> <p><b>Example:</b> account.1.anonymous_call_oncode = *72</p>		

Parameters	Permitted Values	Default
<p><b>Note:</b> It works only if the value of the parameter "account.X.send_anonymous_code" is set to 1 (On Code).</p> <p><b>Web User Interface:</b> Account-&gt;Basic-&gt;Send Anonymous Code-&gt;On Code</p> <p><b>Handset User Interface:</b> None</p>		
<p><b>account.X.anonymous_call_offcode</b> (X ranges from 1 to 5)</p>	<p>String within 32 characters</p>	<p>Blank</p>
<p><b>Description:</b> Configures the anonymous call off code to deactivate the server-side anonymous call feature for account X.</p> <p><b>Example:</b> account.1.anonymous_call_offcode = *73</p> <p><b>Note:</b> It works only if the value of the parameter "account.X.send_anonymous_code" is set to 0 (Off Code).</p> <p><b>Web User Interface:</b> Account-&gt;Basic-&gt;Send Anonymous Code-&gt;Off Code</p> <p><b>Handset User Interface:</b> None</p>		

**To configure anonymous call feature for a specific line via web user interface:**

1. Click on **Account->Basic**.
2. Select the desired account from the pull-down list of **Account**.
3. Select the desired value from the pull-down list of **Local Anonymous**.
4. Select the desired value from the pull-down list of **Send Anonymous Code**.
5. (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 W52P/W56P web interface. The 'Account' tab is selected, and the 'Account 1' dropdown is visible. The 'Local Anonymous' dropdown is set to 'On', and the 'Send Anonymous Code' dropdown is set to 'On Code'. The 'Off Code' field is empty. A red box highlights the 'Local Anonymous' and 'Send Anonymous Code' sections. A 'NOTE' sidebar on the right explains 'Anonymous Call' and 'Anonymous Call Rejection' features.

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

#### To configure anonymous call feature for a specific line via the handset:

- Press **OK** to enter the main menu.
- Select **Call Features->Anonymous Call**.

The LCD screen displays the outgoing lines currently assigned to the handset. The default outgoing line is highlighted and followed by a left arrow.

- Press **▲** or **▼** to highlight the desired line, and then press the **OK** soft key.
- Press **◀** or **▶** to select the desired value from the **Status** field.
- Press the **OK** soft key to accept the change.

## Anonymous Call Rejection

Anonymous call rejection allows IP DECT phones to automatically reject incoming calls from callers whose identity has been deliberately concealed. The anonymous caller's phone LCD screen presents "Anonymity Disallowed". Anonymous call rejection is configurable on a per-line basis.

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

## Procedure

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

<b>Configuration File</b>	<MAC>.cfg	Configure anonymous call rejection. <b>Parameters:</b> account.X.reject_anonymous_call account.X.send_anonymous_rejection_code account.X.anonymous_reject_oncode account.X.anonymous_reject_offcode
<b>Local</b>	Web User Interface	Configure anonymous call rejection. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=account-basic&q=load&acc=0
	Handset User Interface	Configure anonymous call rejection.

### Details of Configuration Parameters:

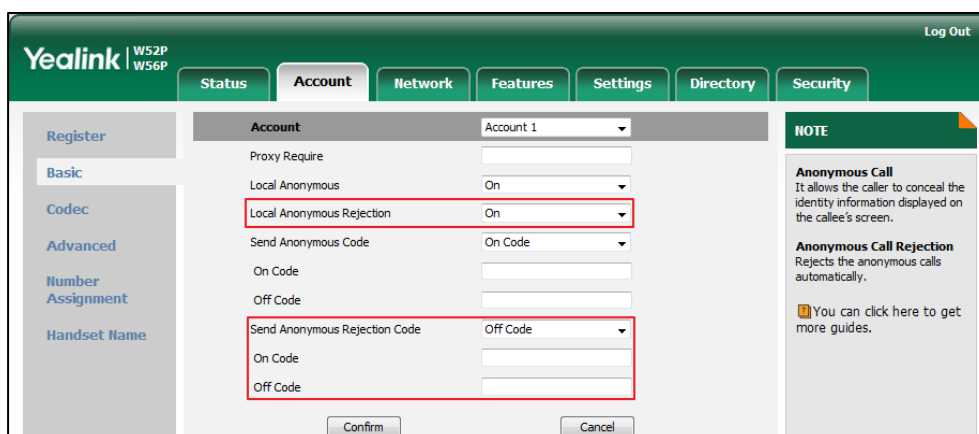
Parameters	Permitted Values	Default
<b>account.X.reject_anonymous_call</b> (X ranges from 1 to 5)	<b>0 or 1</b>	<b>0</b>
<p><b>Description:</b> Triggers the anonymous call rejection feature to on or off for account X.</p> <p><b>0-Off</b> <b>1-On</b></p> <p>If it is set to 1 (On), the IP DECT phone will automatically reject incoming calls from users enabled anonymous call feature. The anonymous user's phone LCD screen presents "Forbidden".</p> <p><b>Web User Interface:</b> Account-&gt;Basic-&gt;Local Anonymous Rejection</p> <p><b>Handset User Interface:</b> OK-&gt;Call Features-&gt;Anon.Call Rejection-&gt;Line X-&gt;Status</p>		
<b>account.X.send_anonymous_rejection_code</b> (X ranges from 1 to 5)	<b>0 or 1</b>	<b>0</b>
<p><b>Description:</b> Configures the IP DECT phone to send anonymous rejection on/off code to activate/deactivate the server-side anonymous call rejection feature for account X.</p>		

Parameters	Permitted Values	Default
<p><b>0-Off code</b>  <b>1-On code</b></p> <p>If it is set to 0 (Off Code), the IP DECT phone will send anonymous rejection off code to the server when you deactivate the anonymous call rejection feature.</p> <p>If it is set to 1 (On Code), the IP DECT phone will send anonymous rejection on code to the server when you activate the anonymous call rejection feature.</p> <p><b>Web User Interface:</b>  Account-&gt;Basic-&gt;Send Anonymous Rejection Code</p> <p><b>Handset User Interface:</b>  None</p>		
<p><b>account.X.anonymous_reject_oncode</b>  (X ranges from 1 to 5)</p>	<p><b>String within 32 characters</b></p>	<p><b>Blank</b></p>
<p><b>Description:</b>  Configures the anonymous call rejection on code to activate the server-side anonymous call rejection feature for account X.</p> <p><b>Example:</b>  account.1.anonymous_reject_oncode = *74</p> <p><b>Note:</b> It works only if the value of the parameter "account.X.send_anonymous_rejection_code" is set to 1 (On Code).</p> <p><b>Web User Interface:</b>  Account-&gt;Basic-&gt;Send Anonymous Rejection Code-&gt;On Code</p> <p><b>Handset User Interface:</b>  None</p>		
<p><b>account.X.anonymous_reject_offcode</b>  (X ranges from 1 to 5)</p>	<p><b>String within 32 characters</b></p>	<p><b>Blank</b></p>
<p><b>Description:</b>  Configures the anonymous call rejection off code to deactivate the server-side anonymous call rejection feature for account X.</p> <p><b>Example:</b>  account.1.anonymous_reject_offcode = *75</p> <p><b>Note:</b> It works only if the value of the parameter "account.X.send_anonymous_rejection_code" is set to 0 (Off Code).</p> <p><b>Web User Interface:</b>  Account-&gt;Basic-&gt;Send Anonymous Rejection Code-&gt;Off Code</p> <p><b>Handset User Interface:</b></p>		

Parameters	Permitted Values	Default
None		

To configure anonymous call rejection feature for a specific line via web user interface:

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



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

To configure anonymous call rejection feature for a specific line via the handset:

1. Press **OK** to enter the main menu.
2. Select **Settings->Anon.Call Rejection**.  
The LCD screen displays the incoming lines currently assigned to the handset.
3. Press **▲** or **▼** to highlight the desired line, and then press the **OK** soft key.
4. Press **◀** or **▶** to select the desired value from the **Status** field.
5. Press the **OK** soft key to accept the change.

## Do Not Disturb (DND)

DND allows IP DECT phones to ignore incoming calls. DND feature can be configured on a phone or a per-line basis depending on the DND mode.

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

### Procedure

DND can be configured using the configuration files or locally.

<b>Configuration File</b>	<MAC>.cfg	Configure DND feature. <b>Parameters:</b> account.X.dnd.enable account.X.dnd.on_code account.X.dnd.off_code
	y000000000025.cfg	Configure the DND refuse code. <b>Parameter:</b> features.dnd_refuse_code
<b>Local</b>	Web User Interface	Configure DND feature. <b>Navigate to:</b> http://<phoneIPAddress>/servlet? p=features-forward&q=load
		Specify the return code and the reason of the SIP response message when DND is enabled. <b>Navigate to:</b> http://<phoneIPAddress>/servlet? p=features-general&q=load
	Handset User Interface	Configure DND feature.

### Details of Configuration Parameters:

Parameters	Permitted Values	Default
<b>account.X.dnd.enable</b> (X ranges from 1 to 5)	<b>0 or 1</b>	<b>0</b>
<p><b>Description:</b> Triggers DND feature to on or off for account X.</p> <p><b>0-Off</b> <b>1-On</b></p> <p>If it is set to 1 (On), the IP DECT phone will reject incoming calls on account X.</p> <p><b>Web User Interface:</b> Features-&gt;Forward&amp;DND-&gt;DND-&gt;DND Status</p> <p><b>Handset User Interface:</b> OK-&gt;Call Features-&gt;Do Not Disturb-&gt;LineX-&gt;Status</p>		

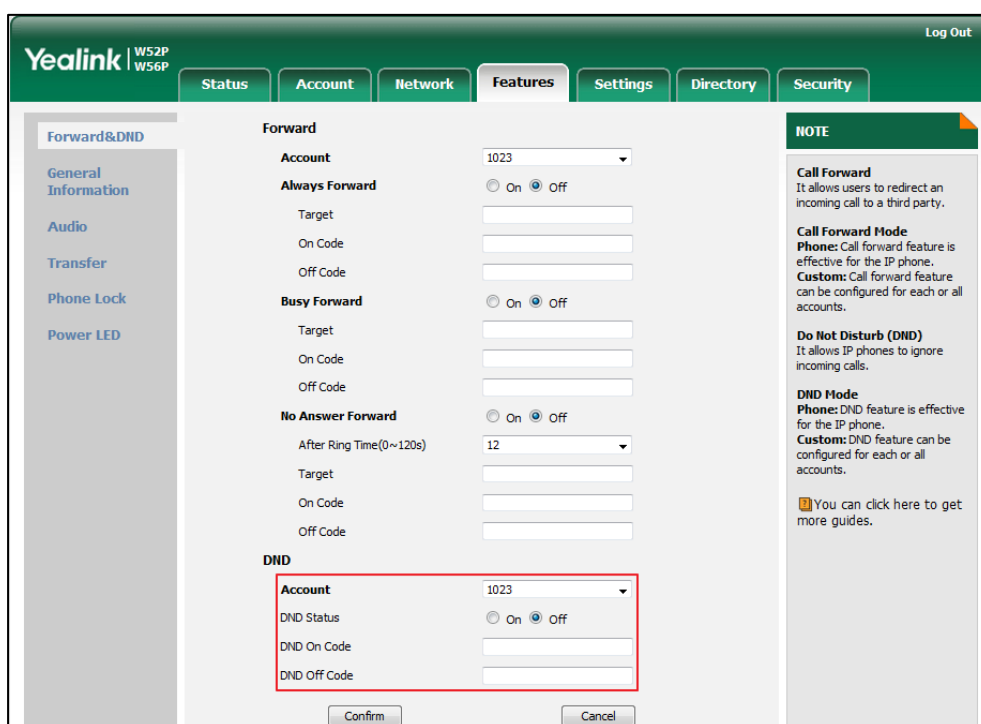
Parameters	Permitted Values	Default
<b>account.X.dnd.on_code</b> (X ranges from 1 to 5)	<b>String within 32 characters</b>	<b>Blank</b>
<p><b>Description:</b>                      Configures the DND on code to activate the server-side DND feature for account X. The IP DECT phone will send the DND on code to the server when you activate DND feature for account X on the IP DECT phone.</p> <p><b>Example:</b>                      account.1.dnd.on_code = *73</p> <p><b>Web User Interface:</b>                      Features-&gt;Forward&amp;DND-&gt;DND-&gt;DND On Code</p> <p><b>Handset User Interface:</b>                      None</p>		
<b>account.X.dnd.off_code</b> (X ranges from 1 to 5)	<b>String within 32 characters</b>	<b>Blank</b>
<p><b>Description:</b>                      Configures the DND off code to deactivate the server-side DND feature for account X. The IP DECT phone will send the DND off code to the server when you deactivate DND feature for account X on the IP DECT phone.</p> <p><b>Example:</b>                      account.1.dnd.off_code = *74</p> <p><b>Web User Interface:</b>                      Features-&gt;Forward&amp;DND-&gt;DND-&gt;DND Off Code</p> <p><b>Handset User Interface:</b>                      None</p>		
<b>features.dnd_refuse_code</b>	<b>404, 480, 486 or 603</b>	<b>480</b>
<p><b>Description:</b>                      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.</p> <p><b>404-Not Found</b></p> <p><b>480-Temporarily Unavailable</b></p> <p><b>486-Busy Here</b></p> <p><b>603-Decline</b></p> <p>If it is set to 486 (Busy here), the caller's phone LCD screen will display the reason "Busy here" when the callee enables DND feature.</p>		



Parameters	Permitted Values	Default
<b>Web User Interface:</b>		
Features->General Information->Return Code When DND		
<b>Handset User Interface:</b>		
None		

To configure DND for a specific line via web user interface:

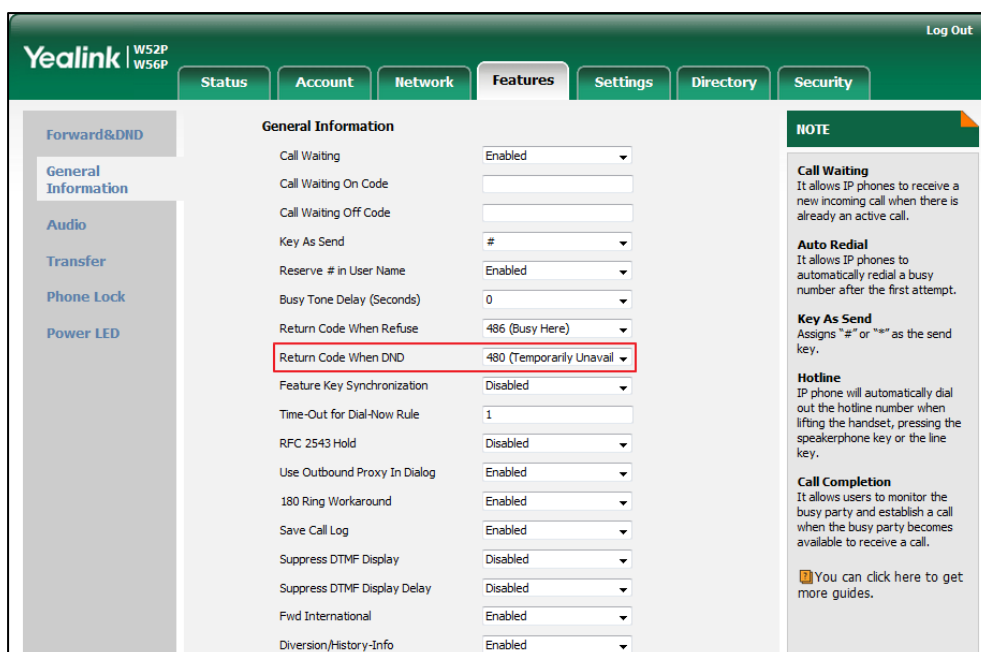
1. Click on **Features->Forward&DND->DND**.
2. Select the desired line from the pull-down list of **Account** field.
3. Mark the desired radio box in the **DND Status** field.
4. Enter the DND on code and off code in the **DND On Code** and **DND Off Code** field respectively.



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

To configure return code when DND via web user interface:

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



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

To activate DND mode for a specific line via the handset:

1. Press **OK** to enter the main menu.
2. Select **Call Features->Do Not Disturb**.  
The LCD screen displays the incoming lines currently assigned to the handset.
3. Press **▲** or **▼** to highlight the desired line, and then press the **OK** soft key.
4. Press **◀** or **▶** to select **Enabled** from the **Status** field.
5. Press the **OK** 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.

<b>Configuration File</b>	y00000000025.cfg	Configure busy tone delay. <b>Parameter:</b> features.busy_tone_delay
---------------------------	------------------	---

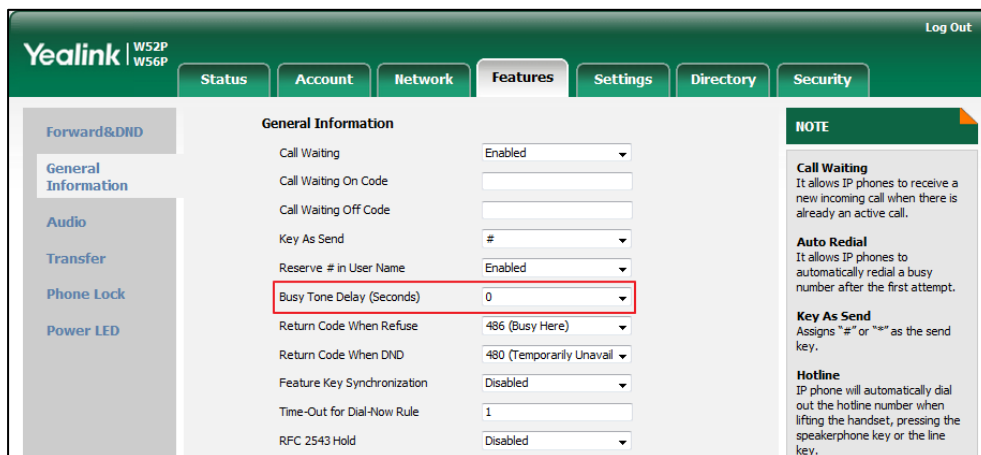
Local	Web User Interface	Configure busy tone delay. <b>Navigate to:</b> http://<phoneIPAddress>/servlet ?p=features-general&q=load
-------	--------------------	--

**Details of the Configuration Parameter:**

Parameter	Permitted Values	Default
features.busy_tone_delay	0, 3 or 5	0
<p><b>Description:</b>                      Configures the duration time (in seconds) for the busy tone.                      When one party releases the call, a busy tone is audible to the other party indicating that the call connection breaks.</p> <p><b>0-0s</b>  <b>3-3s</b>  <b>5-5s</b></p> <p>If it is set to 3 (3s), a busy tone is audible for 3 seconds on the IP DECT phone.</p> <p><b>Web User Interface:</b>                      Features-&gt;General Information-&gt;Busy Tone Delay (Seconds)</p> <p><b>Handset User Interface:</b>                      None</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 the refused call. The caller's phone LCD screen displays the reason according to the received return code. Available return codes and reasons are:

- 404 (Not Found)
- 480 (Temporarily Unavailable)
- 486 (Busy Here)
- 603 (Decline)

### Procedure

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

<b>Configuration File</b>	y000000000025.cfg	Specify the return code and the reason of the SIP response message when refusing a call. <b>Parameter:</b> features.normal_refuse_code
<b>Local</b>	Web User Interface	Specify the return code and the reason of the SIP response message when refusing a call. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=features-general&q=load

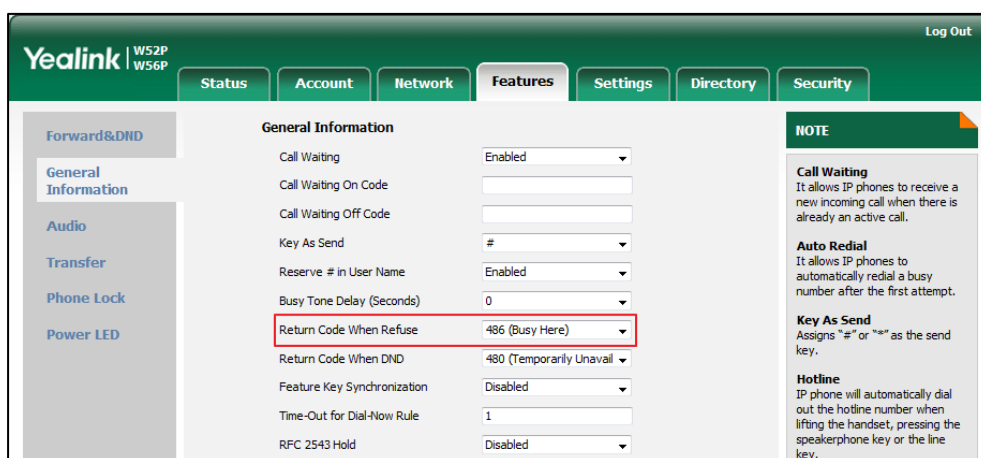
### Details of the Configuration Parameter:

Parameter	Permitted Values	Default
features.normal_refuse_code	404, 480, 486 or 603	486
<p><b>Description:</b></p> <p>Configures a return code and reason of SIP response messages when the IP DECT phone rejects an incoming call. A specific reason is displayed on the caller's phone LCD screen.</p> <p><b>404</b>-Not Found</p> <p><b>480</b>-Temporarily Unavailable</p> <p><b>486</b>-Busy Here</p> <p><b>603</b>-Decline</p> <p>If it is set to 486 (Busy Here), the caller's phone LCD screen will display the message</p>		

Parameter	Permitted Values	Default
"Busy Here" when the callee rejects the incoming call. <b>Web User Interface:</b> Features->General Information->Return Code When Refuse <b>Handset User Interface:</b> None		

To specify the return code and the reason 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 ring back tone and begins to play the media received. 180 ring workaround allows IP DECT phones to resume and play the local ring back tone upon a subsequent 180 message received.

## Procedure

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

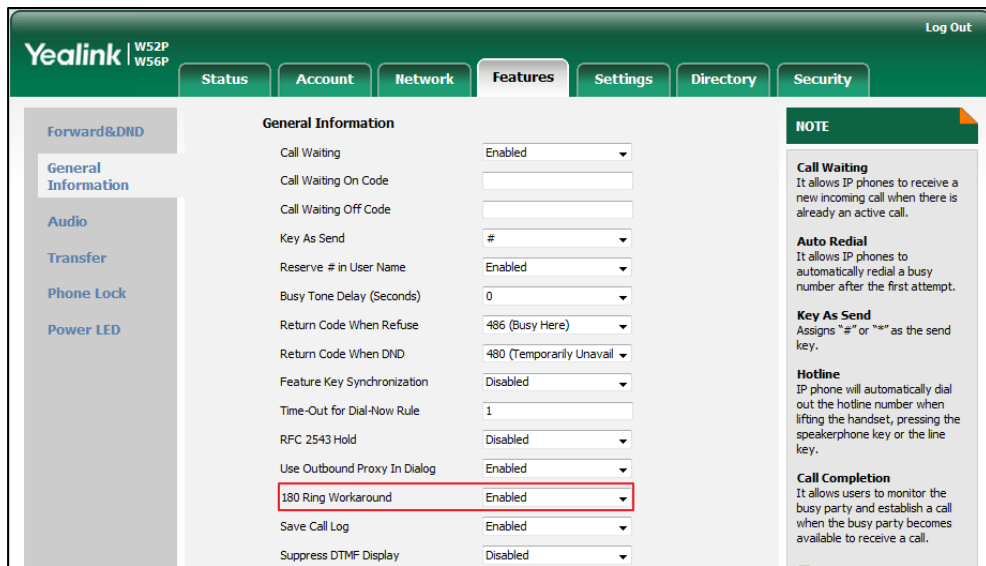
<b>Configuration File</b>	y000000000025.cfg	Configure 180 ring workaround. <b>Parameter:</b> phone_setting.is_deal180
<b>Local</b>	Web User Interface	Configure 180 ring workaround. <b>Navigate to:</b> http://<phoneIPAddress>/servlet ?p=features-general&q=load

### Details of the Configuration Parameter:

Parameter	Permitted Values	Default
phone_setting.is_deal180	0 or 1	1
<p><b>Description:</b> Enables or disables the IP DECT phone to deal with the 180 SIP message received after the 183 SIP message.</p> <p><b>0-Disabled</b> <b>1-Enabled</b></p> <p>If it is set to 1 (Enabled), the IP DECT phone will resume and play the local ring back tone upon a subsequent 180 message received.</p> <p><b>Web User Interface:</b> Features-&gt;General Information-&gt;180 Ring Workaround</p> <p><b>Handset User Interface:</b> None</p>		

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 DECT phone is configured to use an outbound proxy server within a dialog, all SIP request messages from the IP DECT phone will be sent to the outbound proxy server forcibly.

### Note

To use this feature, make sure the outbound server has been correctly configured on the IP DECT phone. For more information on how to configure outbound server, refer to [Account Registration](#) on page 112.

### Procedure

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

<b>Configuration File</b>	y000000000025.cfg	Specify whether to use outbound proxy in a dialog. <b>Parameter:</b> sip.use_out_bound_in_dialog
<b>Local</b>	Web User Interface	Specify whether to use outbound proxy in a dialog. <b>Navigate to:</b> http://<phoneIPAddress>/servlet

		?p=features-general&q=load
--	--	----------------------------

**Details of the Configuration Parameter:**

Parameter	Permitted Values	Default
<b>sip.use_out_bound_in_dialog</b>	<b>0 or 1</b>	<b>1</b>

**Description:**  
 Enables or disables the IP DECT phone to send all SIP requests to the outbound proxy server forcibly in a dialog.

**0-Disabled**  
**1-Enabled**

If it is set to 0 (Disabled), only the new SIP request messages from the IP DECT phone will be sent to the outbound proxy server in a dialog.

If it is set to 1 (Enabled), all the SIP request messages from the IP DECT phone will be forced to send to the outbound proxy server in a dialog.

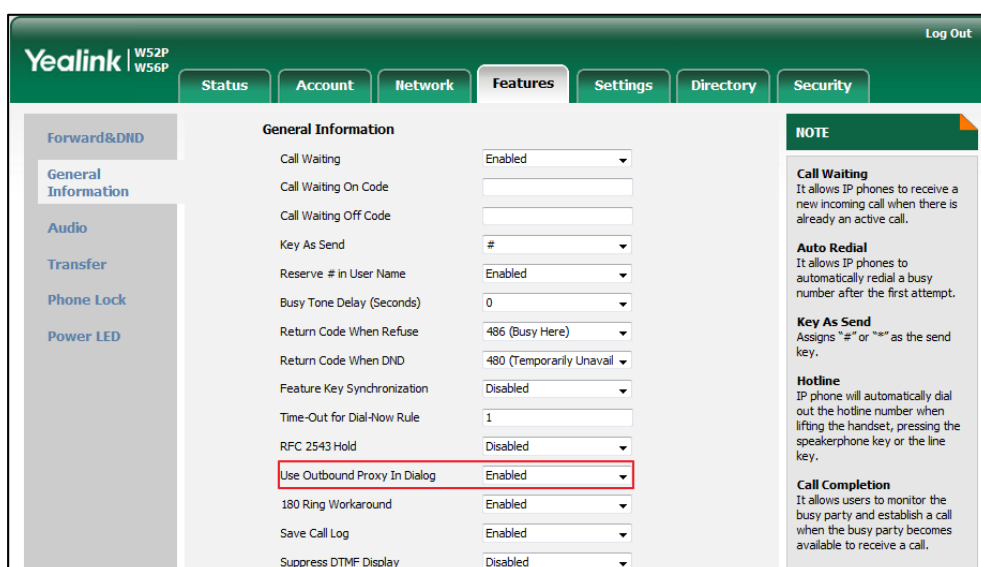
**Note:** It works only if the value of the parameter "account.X.outbound\_proxy\_enable" is set to 1 (Enabled) and the outbound server address has been correctly configured on the phone.

**Web User Interface:**  
 Features->General Information->Use Outbound Proxy In Dialog

**Handset User Interface:**  
 None

**To configure use outbound proxy in 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](#). These session timers are configurable on IP DECT phones.

### Timer T1

Timer T1 is an estimate of the Round Trip Time (RTT) of transactions between a SIP client and SIP server.

### Timer T2

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.

#### Example:

The user registers a SIP account for the IP DECT phone and then set the value of Timer T1, Timer T2 respectively (Timer T1: 0.5, Timer T2: 4). The SIP registration request message will be re-transmitted between the IP DECT phone and SIP server. The re-transmitting and doubling of Timer T1 (0.5) will continue until the retransmitting time reaches the Timer T2 (4). The total registration request retry time will be less than 64 times of T1 ( $64 * 0.5 = 32$ ). The re-transmitting interval in sequence is: 0.5s, 1s, 2s, 4s, 4s, 4s, 4s, 4s, 4s and 4s.

### Timer T4

Timer T4 represents the time the network will take to clear messages between the SIP client and server.

### Procedure

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

<b>Configuration File</b>	y000000000025.cfg	Configure SIP session timer. <b>Parameters:</b> sip.timer_t1 sip.timer_t2 sip.timer_t4
<b>Local</b>	Web User Interface	Configure SIP session timer. <b>Navigate to:</b> <a href="http://&lt;phoneIPAddress&gt;/servlet?p=settings-sip&amp;q=load">http://&lt;phoneIPAddress&gt;/servlet?p=settings-sip&amp;q=load</a>

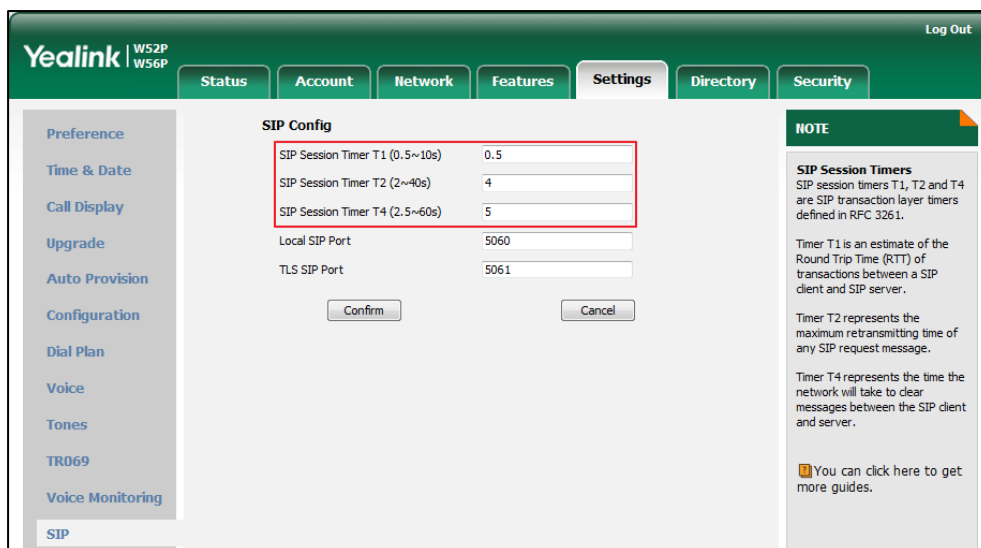
**Details of Configuration Parameters:**

Parameters	Permitted Values	Default
<b>sip.timer_t1</b>	<b>Float from 0.5 to 10</b>	<b>0.5</b>
<p><b>Description:</b> 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.</p> <p><b>Web User Interface:</b> Settings-&gt;SIP-&gt;SIP Session TimerT1 (0.5~10s)</p> <p><b>Handset User Interface:</b> None</p>		
<b>sip.timer_t2</b>	<b>Float from 2 to 40</b>	<b>4</b>
<p><b>Description:</b> Configures the SIP session timer T2 (in seconds) for account X. Timer T2 represents the maximum retransmitting time of any SIP request message.</p> <p><b>Web User Interface:</b> Account-&gt;Advanced-&gt;SIP Session Timer T2 (seconds)</p> <p><b>Handset User Interface:</b> None</p>		
<b>sip.timer_t4</b>	<b>Float from 2.5 to 60</b>	<b>5</b>
<p><b>Description:</b> Configures the SIP session timer T4 (in seconds) for account X. T4 represents the maximum duration a message will remain in the network.</p> <p><b>Web User Interface:</b> Settings-&gt;SIP-&gt;SIP Session Timer T4 (2.5~60s)</p> <p><b>Handset User Interface:</b> None</p>		

**To configure session timer via web user interface:**

1. Click on **Settings->SIP**.
2. Enter the desired value in the **SIP Session Timer T1 (0.5~10s)** field.  
The default value is 0.5s.
3. Enter the desired value in the **SIP Session Timer T2 (2~40s)** field.  
The default value is 4s.

- Enter the desired value in the **SIP Session Timer T4 (2.5~60s)** field.  
The default value is 5s.



- 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. The IP DECT 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/UPDATE request at or before the negotiated session expiration.

### Procedure

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

<b>Configuration File</b>	<MAC>.cfg	Configure session timer. <b>Parameters:</b> account.X.session_timer.enable account.X.session_timer.expires account.X.session_timer.refresher
<b>Local</b>	Web User Interface	Configure session timer. <b>Navigate to:</b> http://<phoneIPAddress>/servlet ?p=account-adv&q=load&acc=0

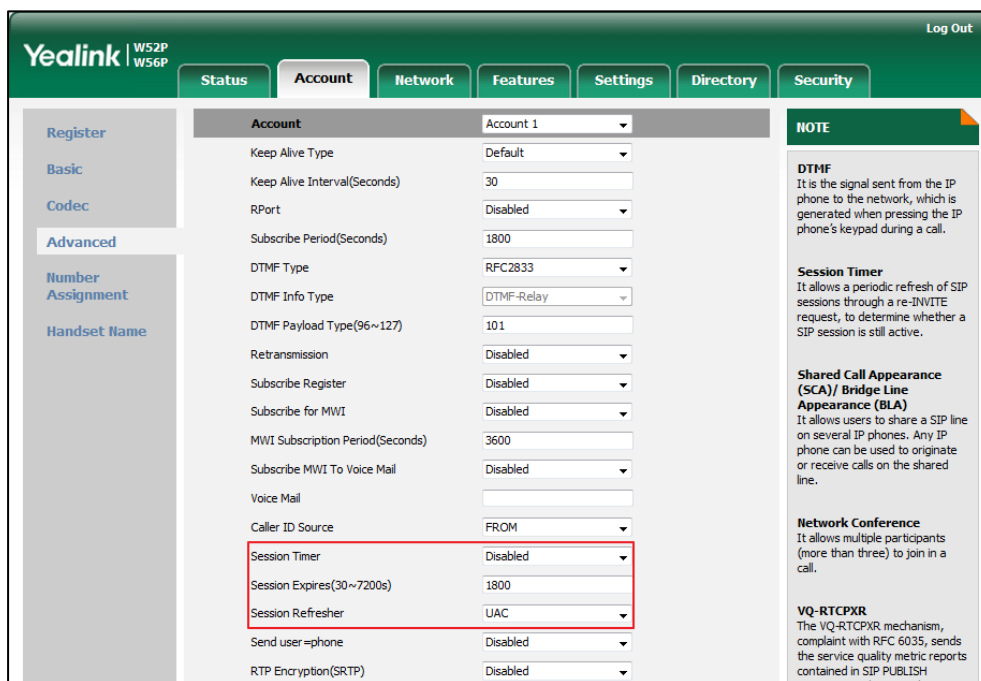
**Details of Configuration Parameters:**

Parameters	Permitted Values	Default
<b>account.X.session_timer.enable</b>	<b>0 or 1</b>	<b>0</b>
<p><b>Description:</b>                      Enables or disables the session timer for account X.  <b>0-Disabled</b>  <b>1-Enabled</b>                      If it is set to 1 (Enabled), the IP DECT phone will send periodic UPDATE requests to refresh the session during a call.</p> <p><b>Web User Interface:</b>                      Account-&gt;Advanced-&gt;Session Timer</p> <p><b>Handset User Interface:</b>                      None</p>		
<b>account.X.session_timer.expires</b>	<b>Integer from 30 to 7200</b>	<b>1800</b>
<p><b>Description:</b>                      Configures the interval (in seconds) for refreshing the SIP session during a call for account X. For example, an UPDATE will be sent after 50% of its value has elapsed. If it is set to 1800 (1800s), the IP DECT phone will refresh the session during a call before 900 seconds.</p> <p><b>Example:</b>                      account.1.session_timer.expires = 1800</p> <p><b>Note:</b> It works only if the value of the parameter "account.X.session_timer.enable" is set to 1 (Enabled).</p> <p><b>Web User Interface:</b>                      Account-&gt;Advanced-&gt;Session Expires(30~7200s)</p> <p><b>Handset User Interface:</b>                      None</p>		
<b>account.X.session_timer.refresher</b>	<b>0 or 1</b>	<b>0</b>
<p><b>Description:</b>                      Configures the function of the endpoint who initiates the SIP request for account X.  <b>0-UAC</b>  <b>1-UAS</b></p> <p><b>Note:</b> It works only if the value of the parameter "account.X.session_timer.enable" is</p>		

Parameters	Permitted Values	Default
set to 1 (Enabled).		
<b>Web User Interface:</b>		
Account->Advanced->Session Refresher		
<b>Handset User Interface:</b>		
None		

**To configure session timer via web user interface:**

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



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

## Call Hold

Call hold provides a service of placing an active call on hold. When a call is placed on hold, the IP DECT phones send an INVITE request with HOLD SDP to request remote parties to stop sending media and to inform them that they are being held. The IP DECT 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). Call hold tone allows IP DECT phones to play a warning tone at regular intervals when there is a call on hold. The warning tone is played through the speakerphone.

### Procedure

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

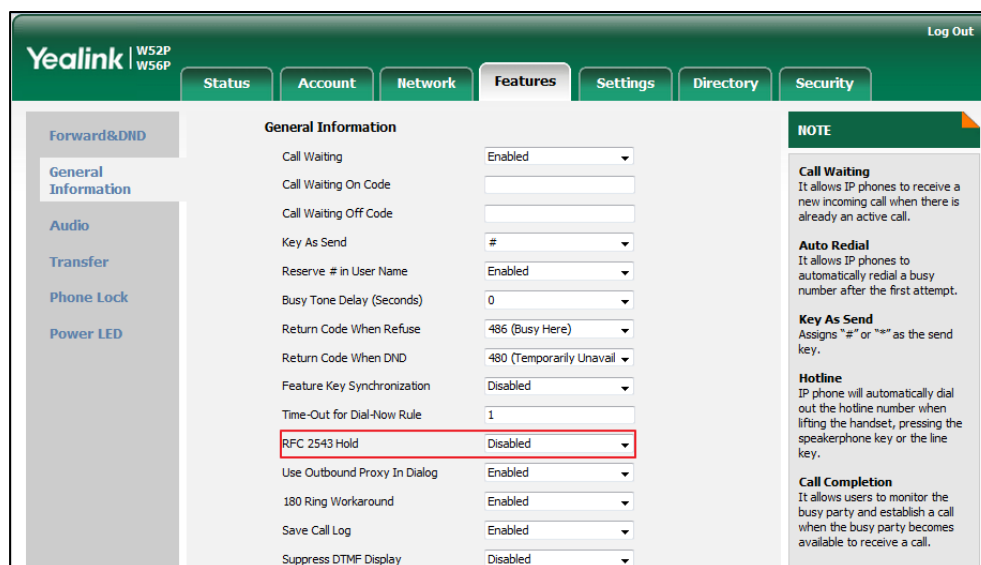
<b>Configuration File</b>	y000000000025.cfg	Specify whether RFC 2543 (c=0.0.0.0) outgoing hold signaling is used. <b>Parameter:</b> sip.rfc2543_hold
<b>Local</b>	Web User Interface	Specify whether RFC 2543 (c=0.0.0.0) outgoing hold signaling is used. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=phone-features&q=load

### Details of Configuration Parameters:

Parameters	Permitted Values	Default
sip.rfc2543_hold	0 or 1	0
<p><b>Description:</b> Enables or disables the IP DECT phone to use RFC 2543 (c=0.0.0.0) outgoing hold signaling.</p> <p><b>0-Disabled</b> <b>1-Enabled</b></p> <p>If it is set to 0 (Disabled), SDP media direction attributes (such as a=sendonly) per RFC 3264 is used when placing a call on hold.</p> <p>If it is set to 1 (Enabled), SDP media connection address c=0.0.0.0 per RFC 2543 is used when placing a call on hold.</p> <p><b>Web User Interface:</b> Features-&gt;General Information-&gt;RFC 2543 Hold</p> <p><b>Handset User Interface:</b> None</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.

## Call Forward

Call forward allows users to redirect an incoming call to a third party. The IP DECT 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 call immediately.
- **Busy Forward**--Forward the incoming call when the IP DECT phone or the specified account is busy.
- **No Answer Forward**--Forward the incoming call after a period of ring time.

Call forward can be configured on a phone or a per-line basis depending on the call forward mode.

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

## Procedure

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

Configuration File	<MAC>.cfg	<p>Configure call forward in custom mode.</p> <p><b>Parameters:</b></p> <p>account.X.always_fwd.enable  account.X.always_fwd.target  account.X.always_fwd.on_code  account.X.always_fwd.off_code  account.X.busy_fwd.enable  account.X.busy_fwd.target  account.X.busy_fwd.on_code  account.X.busy_fwd.off_code  account.X.timeout_fwd.enable  account.X.timeout_fwd.target  account.X.timeout_fwd.timeout  account.X.timeout_fwd.on_code  account.X.timeout_fwd.off_code</p>
		<p>Configure diversion/history-info feature.</p> <p><b>Parameter:</b></p> <p>features.fwd_diversion_enable</p>
		<p>Configure forward international.</p> <p><b>Parameter:</b></p> <p>forward.international.enable</p>
Local	Web User Interface	<p>Configure call forward.</p> <p><b>Navigate to:</b></p> <p>http://&lt;phoneIPAddress&gt;/servlet?p=features-general&amp;q=load</p>
		<p>Configure diversion/history-info feature.</p> <p>Configure forward international.</p> <p><b>Navigate to:</b></p> <p>http://&lt;phoneIPAddress&gt;/servlet?p=features-general&amp;q=load</p>
	Handset User Interface	Configure call forward.



### Details of Configuration Parameters:

Parameters	Permitted Values	Default
<b>account.X.always_fwd.enable</b> (X ranges from 1 to 5)	0 or 1	0
<p><b>Description:</b> Triggers always forward feature to on or off for account X.</p> <p>0-Off 1-On</p> <p>If it is set to 1 (On), incoming calls to the account X are forwarded to the destination number immediately.</p> <p><b>Web User Interface:</b> Features-&gt;Forward&amp;DND-&gt;Forward-&gt;Always Forward-&gt;On/Off</p> <p><b>Handset User Interface:</b> OK-&gt;Call Features-&gt;Call Forward-&gt;LineX-&gt;Always(Disabled/Enabled)-&gt;Status</p>		
<b>account.X.always_fwd.target</b> (X ranges from 1 to 5)	String within 32 characters	Blank
<p><b>Description:</b> Configures the destination number of the always forward for account X.</p> <p><b>Example:</b> account.1.always_fwd.target = 1003</p> <p><b>Web User Interface:</b> Features-&gt;Forward&amp;DND-&gt;Forward-&gt;Always Forward-&gt;Target</p> <p><b>Handset User Interface:</b> OK-&gt;Call Features-&gt;Call Forward-&gt;LineX-&gt;Always(Enabled)-&gt;Target</p>		
<b>account.X.always_fwd.on_code</b> (X ranges from 1 to 5)	String within 32 characters	Blank
<p><b>Description:</b> Configures the always forward on code to activate the server-side always forward feature for account X. The IP DECT phone will send the always forward on code and the pre-configured destination number to the server when you activate always forward feature for account X on the IP DECT phone.</p> <p><b>Example:</b> account.1.always_fwd.on_code = *72</p> <p><b>Web User Interface:</b> Features-&gt;Forward&amp;DND-&gt;Forward-&gt;Always Forward-&gt;On Code</p>		

Parameters	Permitted Values	Default
<p><b>Handset User Interface:</b> None</p>		
<p><b>account.X.always_fwd.off_code</b> (X ranges from 1 to 5)</p>	<p><b>String within 32 characters</b></p>	<p><b>Blank</b></p>
<p><b>Description:</b> Configures the always forward off code to deactivate the server-side always forward feature for account X. The IP DECT phone will send the always forward off code to the server when you deactivate always forward feature for account X on the IP DECT phone.</p> <p><b>Example:</b> account.1.always_fwd.off_code= *73</p> <p><b>Web User Interface:</b> Features-&gt;Forward&amp;DND-&gt;Forward-&gt;Always Forward-&gt;Off Code</p> <p><b>Handset User Interface:</b> None</p>		
<p><b>account.X.busy_fwd.enable</b> (X ranges from 1 to 5)</p>	<p><b>0 or 1</b></p>	<p><b>0</b></p>
<p><b>Description:</b> Triggers busy forward feature to on or off for account X.</p> <p><b>0-Off</b> <b>1-On</b></p> <p>If it is set to 1 (On), incoming calls to the account X are forwarded to the destination number when the callee is busy.</p> <p><b>Web User Interface:</b> Features-&gt;Forward&amp;DND-&gt;Forward-&gt;Busy Forward-&gt;On/Off</p> <p><b>Handset User Interface:</b> OK-&gt;Call Features-&gt;Call Forward-&gt;LineX-&gt;Busy(Disabled/Enabled)-&gt;Status</p>		
<p><b>account.X.busy_fwd.target</b> (X ranges from 1 to 5)</p>	<p><b>String within 32 characters</b></p>	<p><b>Blank</b></p>
<p><b>Description:</b> Configures the destination number of the busy forward for account X.</p> <p><b>Example:</b> account.1.busy_fwd.target = 3602</p> <p><b>Web User Interface:</b></p>		

Parameters	Permitted Values	Default
Features->Forward&DND->Forward->Busy Forward->Target <b>Handset User Interface:</b> OK->Call Features->Call Forward->LineX->Busy(Enabled)->Target		
<b>account.X.busy_fwd.on_code</b> (X ranges from 1 to 5)	<b>String within 32 characters</b>	<b>Blank</b>
<b>Description:</b> Configures the busy forward on code to activate the server-side busy forward feature for account X. The IP DECT phone will send the busy forward on code and the pre-configured destination number to the server when you activate busy forward feature for account X on the IP DECT phone. <b>Example:</b> account.1.busy_fwd.on_code = *74 <b>Web User Interface:</b> Features->Forward&DND->Forward->No Answer Forward->On Code <b>Handset User Interface:</b> None		
<b>account.X.busy_fwd.off_code</b> (X ranges from 1 to 5)	<b>String within 32 characters</b>	<b>Blank</b>
<b>Description:</b> Configures the busy forward off code to deactivate the server-side busy forward feature for account X. The IP DECT phone will send the busy forward off code to the server when you deactivate busy forward feature for account X on the IP DECT phone. <b>Example:</b> account.1.busy_fwd.off_code = *75 <b>Web User Interface:</b> Features->Forward&DND->Forward->No Answer Forward->Off Code <b>Handset User Interface:</b> None		
<b>account.X.timeout_fwd.enable</b> (X ranges from 1 to 5)	<b>0 or 1</b>	<b>0</b>
<b>Description:</b> Triggers no answer forward feature to on or off for account X. <b>0-Off</b> <b>1-On</b>		

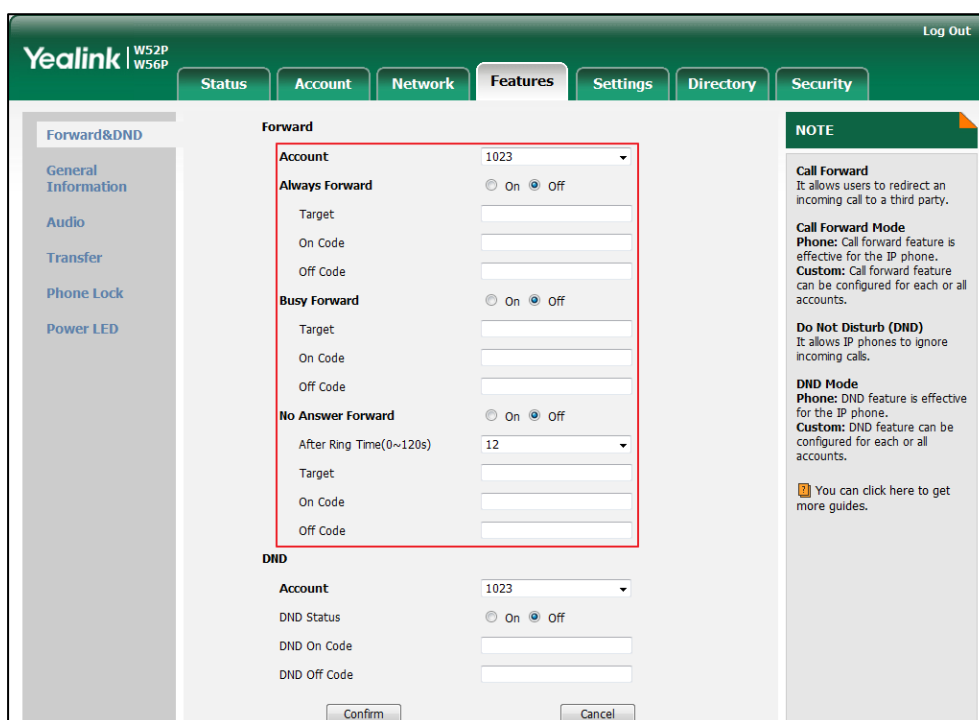
Parameters	Permitted Values	Default
<p>If it is set to 1 (On), incoming calls to the account X are forwarded to the destination number after a period of ring time.</p> <p><b>Web User Interface:</b> Features-&gt;Forward&amp;DND-&gt;Forward-&gt;No Answer Forward-&gt;On/Off</p> <p><b>Handset User Interface:</b> OK-&gt;Call Features-&gt;Call Forward-&gt;LineX-&gt;No Answer(Disabled/Enabled)-&gt;Status</p>		
<p><b>account.X.timeout_fwd.target</b> (X ranges from 1 to 5)</p>	<p><b>String within 32 characters</b></p>	<p><b>Blank</b></p>
<p><b>Description:</b> Configures the destination number of the no answer forward for account X.</p> <p><b>Example:</b> account.1.timeout_fwd.target = 3603</p> <p><b>Web User Interface:</b> Features-&gt;Forward&amp;DND-&gt;Forward-&gt;No Answer Forward-&gt;Target</p> <p><b>Handset User Interface:</b> OK-&gt;Call Features-&gt;Call Forward-&gt;LineX-&gt;No Answer(Enabled)-&gt;Target</p>		
<p><b>account.X.timeout_fwd.timeout</b> (X ranges from 1 to 5)</p>	<p><b>Integer from 0 to 20</b></p>	<p><b>2</b></p>
<p><b>Description:</b> Configures ring times (N) to wait before forwarding incoming calls for account X. Incoming calls will be forwarded when not answered after N*6 seconds.</p> <p><b>Web User Interface:</b> Features-&gt;Forward&amp;DND-&gt;Forward-&gt;No Answer Forward-&gt;After RingTime(0~120s)</p> <p><b>Handset User Interface:</b> OK-&gt;Call Features-&gt;Call Forward-&gt;LineX-&gt;No Answer(Enabled)-&gt;After Ring Time</p>		
<p><b>account.X.timeout_fwd.on_code</b> (X ranges from 1 to 5)</p>	<p><b>String within 32 characters</b></p>	<p><b>Blank</b></p>
<p><b>Description:</b> Configures the no answer forward on code to activate the server-side no answer forward feature for account X. The IP DECT phone will send the no answer forward on code and the pre-configured destination number to the server when you activate no answer forward feature for account X on the IP DECT phone.</p> <p><b>Example:</b> account.1.timeout_fwd.on_code = *76</p>		

Parameters	Permitted Values	Default
<b>Web User Interface:</b> Features->Forward&DND->Forward->No Answer Forward->On Code <b>Handset User Interface:</b> None		
<b>account.X.timeout_fwd.off_code</b> (X ranges from 1 to 5)	String within 32 characters	Blank
<b>Description:</b> Configures the no answer forward off code to deactivate the server-side no answer forward feature for account X. The IP DECT phone will send the no answer forward off code to the server when you deactivate no answer forward feature for account X on the IP DECT phone. <b>Example:</b> account.1.timeout_fwd.off_code = *77 <b>Web User Interface:</b> Features->Forward&DND->Forward->No Answer Forward->Off Code <b>Handset User Interface:</b> None		
<b>features.fwd_diversion_enable</b>	0 or 1	1
<b>Description:</b> Enables or disables the IP DECT phone to present the diversion information when an incoming call is forwarded to your IP DECT phone. 0-Disabled 1-Enabled <b>Web User Interface:</b> Features->General Information->Diversion/History-Info <b>Handset User Interface:</b> None		
<b>forward.international.enable</b>	0 or 1	1
<b>Description:</b> Enables or disables the IP DECT phone to forward incoming calls to international numbers (the prefix is 00). 0-Disabled 1-Enabled		

Parameters	Permitted Values	Default
<b>Web User Interface:</b>		
Features->General Information->Fwd International		
<b>Handset User Interface:</b>		
None		

To configure call forward via web user interface:

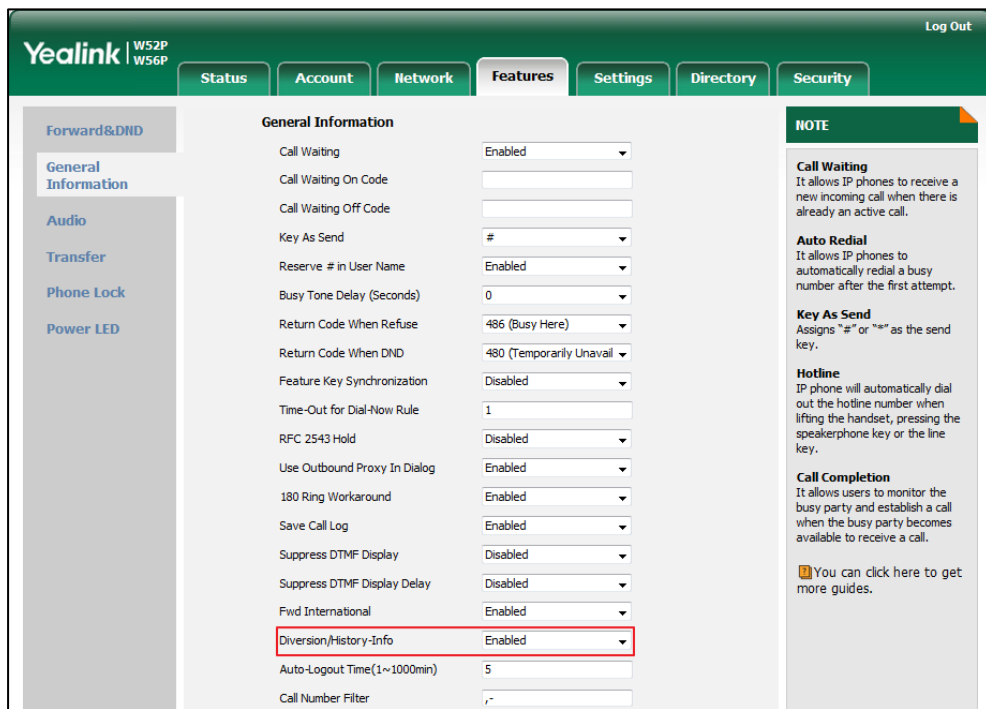
1. Click on **Features->Forward&DND**.
2. In the **Forward** block, mark the desired radio box in the **Mode** field.
  - 1) Mark the desired radio box in the **Always/Busy/No Answer Forward** field.
  - 2) Enter the destination number you want to forward in the **Target** field.
  - 3) (Optional.) Enter 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).



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

To configure Diversion/History-Info feature via web user interface:

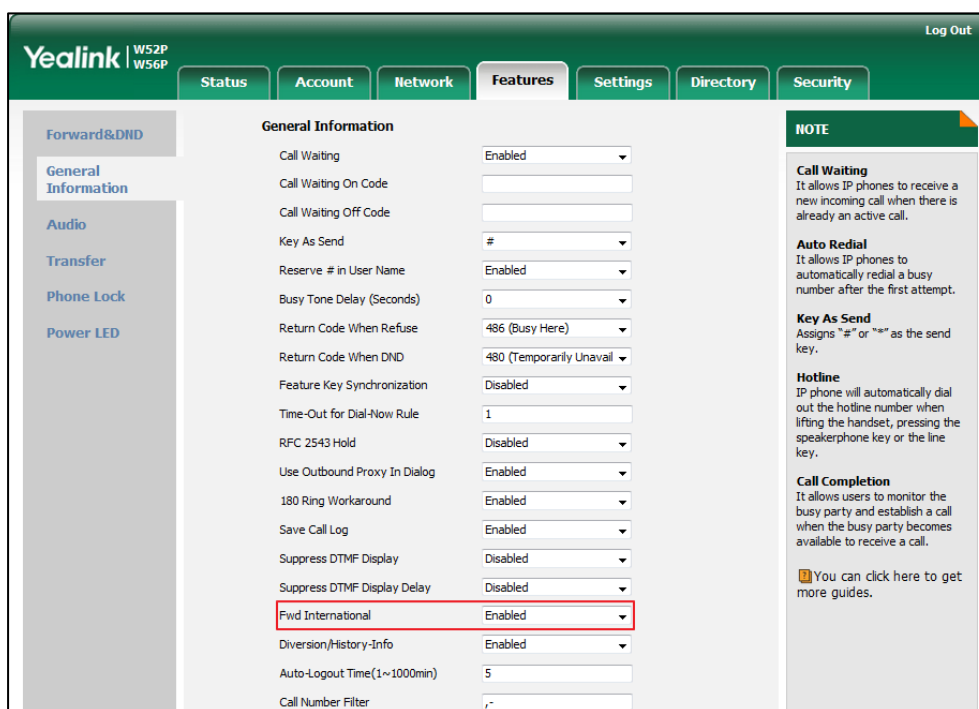
1. Click on **Features->General Information**.
2. Select the desired value from the pull-down list of **Diversion/History-Info**.



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

**To configure forward international 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 enable call forward feature for a specific line via the handset:**

1. Press **OK** to enter the main menu.
2. Select **Call Features->Call Forward**.  
The LCD screen displays the incoming lines currently assigned to the handset.
3. Press **▲** or **▼** to highlight the desired line, and then press the **OK** soft key.
4. Press **▲** or **▼** to highlight the desired forwarding type, and then press the **OK** soft key.
5. Press **◀** or **▶** to select **Enabled** from the **Status** field.
6. Enter the destination number you want to forward incoming calls to in the **Target** field.
7. Press **◀** or **▶** to select the desired ring time to wait before forwarding from the **After Ring Time** field (only available for No Answer Forward).
8. Press the **Save** soft key to accept the change.



## Call Transfer

Call transfer enables IP DECT phones to transfer an existing call to another party. The IP DECT 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 ring back 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. Blind transfer on hook and attended transfer on hook features allow the IP DECT phone to complete the transfer through on-hook.

When a user performs a semi-attended transfer, semi-attended transfer feature determines whether to display the prompt **"Missed Call(s)"**, handset's LCD screen indicate the number of the missed calls.

### Procedure

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

<b>Configuration File</b>	y00000000025.cfg	Specify whether to complete the transfer through on-hook. <b>Parameters:</b> transfer.blind_tran_on_hook_enable transfer.on_hook_trans_enable
		Configure semi-attended transfer feature. <b>Parameter:</b> transfer.semi_attend_tran_enable
<b>Local</b>	Web User Interface	Specify whether to complete the transfer through on-hook. Configure semi-attended transfer feature. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=features-transfer&q=load

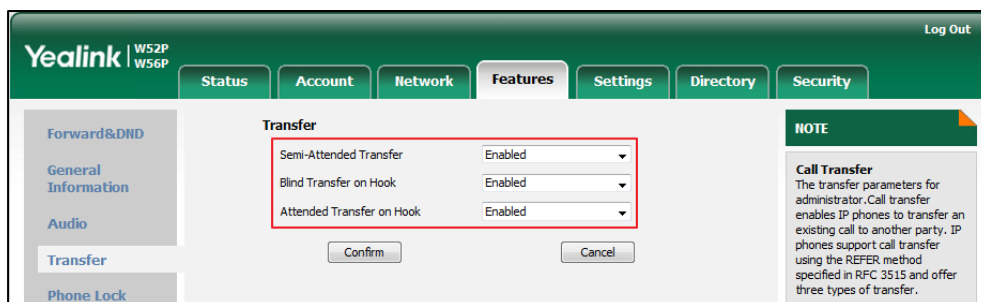
## Details of Configuration Parameters:

Parameters	Permitted Values	Default
<b>transfer.blind_tran_on_hook_enable</b>	<b>0 or 1</b>	<b>1</b>
<p><b>Description:</b> Enables or disables the phone to complete the blind transfer through on-hook besides pressing the <b>TRAN</b> key on the handset (Blind transfer means transfer a call directly to another party without consulting).</p> <p><b>0</b>-Disabled <b>1</b>-Enabled</p> <p><b>Web User Interface:</b> Features-&gt;Transfer-&gt;Blind Transfer On Hook</p> <p><b>Handset User Interface:</b> None</p>		
<b>transfer.on_hook_trans_enable</b>	<b>0 or 1</b>	<b>1</b>
<p><b>Description:</b> Enables or disables the phone to complete the attended transfer through on-hook besides pressing the <b>TRAN</b> key on the handset (Attended transfer means transfer a call with prior consulting).</p> <p><b>0</b>-Disabled <b>1</b>-Enabled</p> <p><b>Web User Interface:</b> Features-&gt;Transfer-&gt;Attended Transfer On Hook</p> <p><b>Handset User Interface:</b> None</p>		
<b>transfer.semi_attend_tran_enable</b>	<b>0 or 1</b>	<b>1</b>
<p><b>Description:</b> Enables or disables the transfer-to party's phone not to prompt a missed call on the LCD screen before displaying the caller ID when completing a semi-attended transfer.</p> <p><b>0</b>-Disabled <b>1</b>-Enabled</p> <p><b>Web User Interface:</b> Features-&gt;Transfer-&gt;Semi-Attended Transfer</p> <p><b>Handset User Interface:</b></p>		

Parameters	Permitted Values	Default
None		

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-Attended Transfer**, **Blind Transfer on Hook** and **Attended 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). The IP DECT 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.

<b>Configuration File</b>	<MAC>.cfg	Configure network conference. <b>Parameters:</b> account.X.conf_type account.X.conf_uri
<b>Local</b>	Web User Interface	Configure network conference. <b>Navigate to:</b> http://<phoneIPAddress>/servlet ?p=account-adv&q=load&acc=0

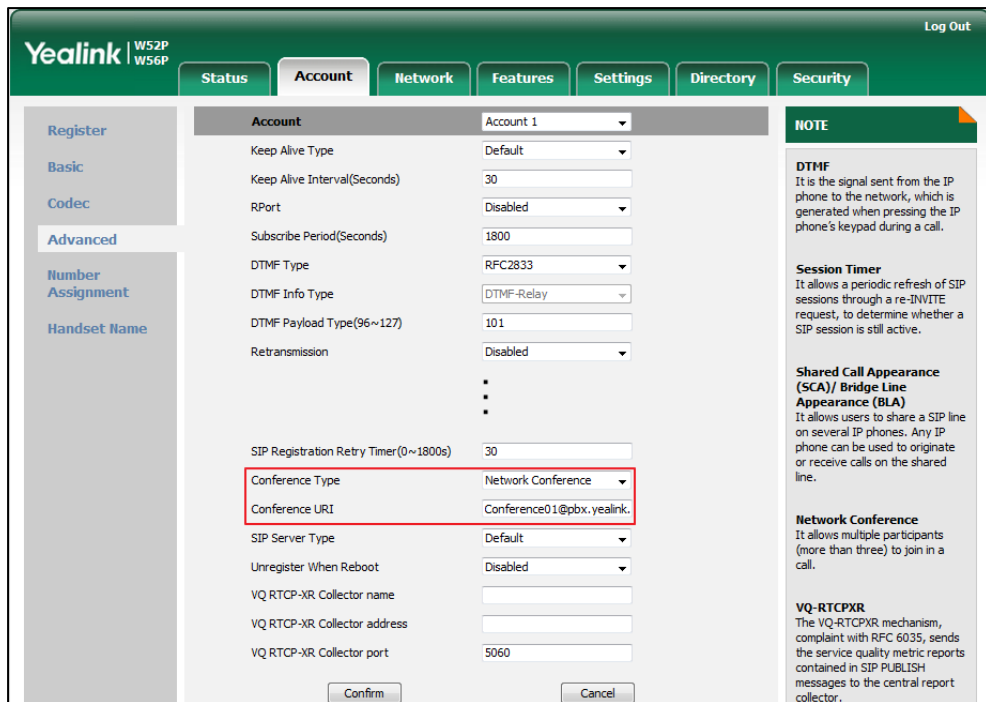
**Details of Configuration Parameters:**

Parameters	Permitted Values	Default
<b>account.X.conf_type</b> (X ranges from 1 to 5)	<b>0 or 2</b>	<b>0</b>
<p><b>Description:</b>                      Configures the network conference type for account X.</p> <p><b>0</b>-Local Conference  <b>2</b>-Network Conference</p> <p>If it is set to 0 (Local Conference), conferences are set up on the IP DECT phone locally.</p> <p>If it is set to 2 (Network Conference), conferences are set up by the server.</p> <p><b>Web User Interface:</b>                      Account-&gt;Advanced-&gt;Conference Type</p> <p><b>Handset User Interface:</b>                      None</p>		
<b>account.X.conf_uri</b> (X ranges from 1 to 5)	<b>SIP URI within 511 characters</b>	<b>Blank</b>
<p><b>Description:</b>                      Configures the network conference URI for account X.</p> <p><b>Example:</b>                      account.1.conf_uri = Conference01@pbx.yealink.com</p> <p><b>Note:</b> It works only if the value of the parameter "account.X.conf_type" is set to 2 (Network Conference).</p> <p><b>Web User Interface:</b>                      Account-&gt;Advanced-&gt;Conference URI</p> <p><b>Handset User Interface:</b>                      None</p>		

**To configure the network conference via web user interface:**

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

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



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

## Feature Key Synchronization

Feature key synchronization provides the capability to synchronize the status of the following features between the IP DECT phone and the server:

- Do Not Disturb (DND)
- Call Forwarding Always (CFA)
- Call Forwarding Busy (CFB)
- Call Forwarding No Answer (CFNA)

### Procedure

Feature key synchronization can be configured using the configuration files or locally.

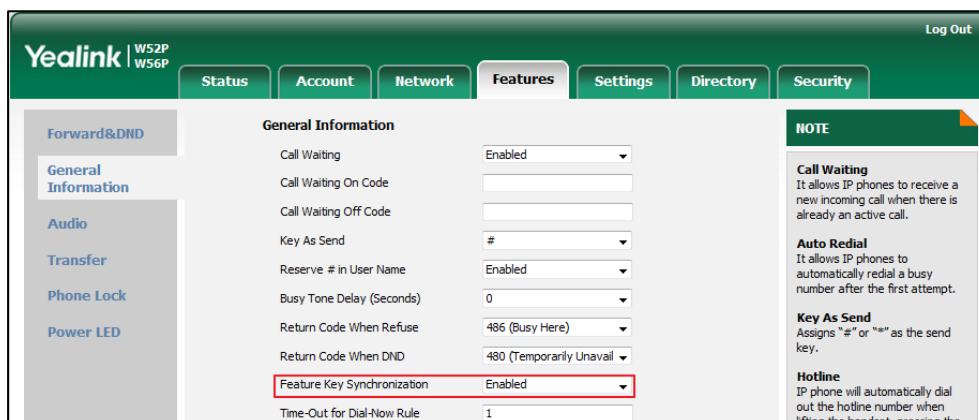
<b>Configuration File</b>	y000000000025.cfg	Configure feature key synchronization. <b>Parameter:</b> bw.feature_key_sync
<b>Local</b>	Web User Interface	Configure feature key synchronization. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=features-general&q=load

### Details of Configuration Parameter:

Parameters	Permitted Values	Default
bw.feature_key_sync	0 or 1	0
<p><b>Description:</b>                      Enables or disables feature key synchronization.                      0-Disabled                      1-Enabled</p> <p><b>Web User Interface:</b>                      Features-&gt;General Information-&gt;Feature Key Synchronization</p> <p><b>Handset User Interface:</b>                      None</p>		

To configure feature key synchronization via web user interface:

1. Click on **Features->General Information**.
2. Select **Enabled** from the pull-down list of **Feature Key Synchronization**.



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

## Recent Call in Dialing

Recent call in dialing feature allows users to view the placed calls list when the phone is on the pre-dialing screen.

### Procedure

Recent call in dialing can be configured using the configuration files or locally.

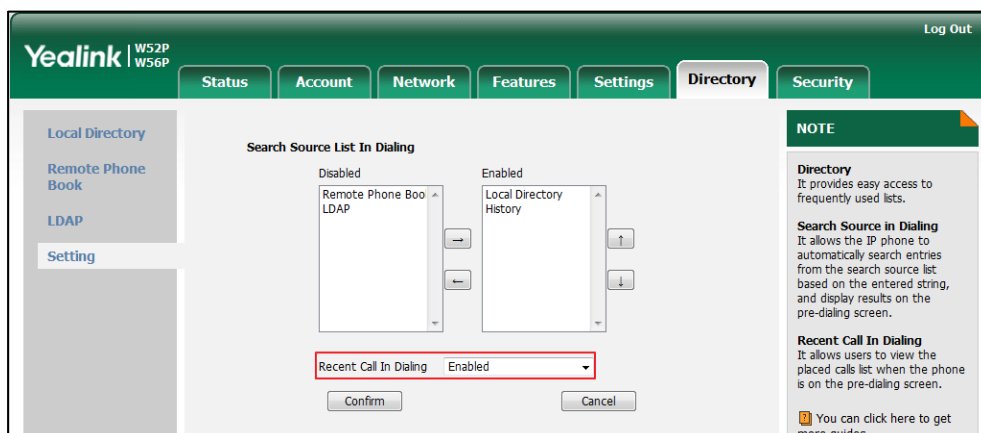
<b>Configuration File</b>	y000000000025.cfg	Configure recent call in dialing feature. <b>Parameters:</b> super_search.recent_call
<b>Local</b>	Web User Interface	Configure recent call in dialing feature. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=contacts-favorite&q=load

### Details of Configuration Parameters:

Parameters	Permitted Values	Default
super_search.recent_call	0 or 1	0
<p><b>Description:</b> Enables or disables recent call in dialing feature.</p> <p>0-Disabled 1-Enabled</p> <p>If it is set to 1 (Enabled), you can see the placed calls list when the handset is on the pre-dialing screen.</p> <p><b>Web User Interface:</b> Directory-&gt;Setting-&gt;Recent Call In Dialing</p> <p><b>Handset User Interface:</b> None</p>		

To configure recent call in dialing via web user interface:

1. Click on **Directory**->**Setting**.
2. Select the desired value from the pull-down list of **Recent Call In Dialing**.



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

## Call Number Filter

Call number filter feature allows IP DECT phone to automatically filter designated characters when dialing.

### Procedure

Call number filter can be configured using the configuration files or locally.

<b>Configuration File</b>	y000000000025.cfg	Configure the characters the IP DECT phone filters when dialing. <b>Parameters:</b> features.call_num_filter
<b>Local</b>	Web User Interface	Configure the characters the IP DECT phone filters when dialing. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=features-general&q=load



**Details of Configuration Parameters:**

Parameters	Permitted Values	Default
features.call_num_filter	String within 99 characters	,-

**Description:**  
 Configures the characters the IP DECT phone filters when dialing.  
 If the dialed number contains configured characters, the IP DECT phone will automatically filter these characters when dialing.

**Example:**  
 features.call\_num\_filter = ,(%!  
 If you dial 1010%, the IP DECT phone will filter the character % and dial out 1010.

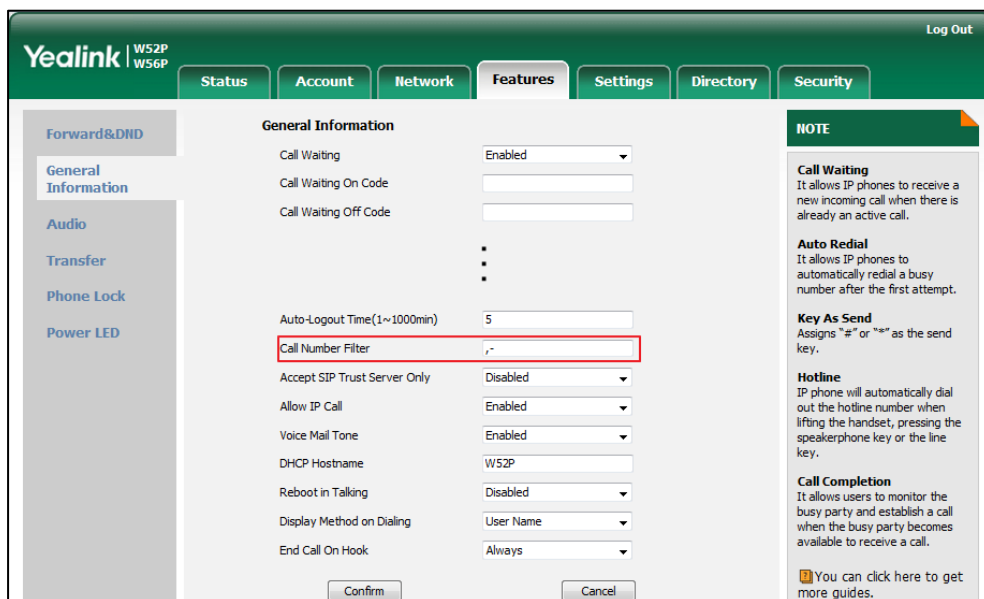
**Note:** If it is left blank, the IP DECT phone will not automatically filter any characters when dialing. If you want to filter just a space, you have to set the value to " ," (a space first followed by a comma).

**Web User Interface:**  
 Features->General Information->Call Number Filter

**Handset User Interface:**  
 None

To configure the characters the IP DECT phone filters via web user interface:

1. Click on **Feature->General Information**.
2. Enter the desired characters in the **Call Number Filter** field.



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

## Calling Line Identification Presentation

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

### Note

If the caller already exists in the local directory, the local contact name assigned to the caller should be preferentially displayed and stored in the call log.

The following sessions show the enhancements of calling line identification presentation according to the calling line identification source configured on the IP DECT phones.

### Caller ID source = FROM

- 1) The IP DECT phone checks Privacy: id header preferentially, if there is a Privacy: id in the INVITE request, the calling line identification information will be hidden and the IP DECT phone LCD screen presents anonymous.
- 2) If there is not any Privacy: id header in the INVITE request, the IP DECT phone checks and presents the caller identification from the P-Preferred-Identity header.
- 3) If there is not P-Preferred-Identity header in the INVITE request, the IP DECT phone presents the caller identification derived from the FROM header.

### Caller ID source = PAI

- 1) The IP DECT phone checks Privacy: id header preferentially, if there is a Privacy: id in the INVITE request, the caller identification information will be hidden and the IP DECT phone LCD screen presents anonymous.
- 2) If there is not any Privacy: id header in the INVITE request, the IP DECT phone checks and presents the caller identification from the P-Preferred-Identity header.
- 3) If there is not P-Preferred-Identity header in the INVITE request, the IP DECT phone checks and presents the caller identification from the P-Asserted-Identity header.

### Caller ID source = PAI-FROM

- 1) The IP DECT phone checks Privacy: id header preferentially, if there is a Privacy: id in the INVITE request, the caller identification information will be hidden and the IP DECT phone LCD screen presents anonymous.
- 2) If there is not any Privacy: id header in the INVITE request, the IP DECT phone checks and presents the caller identification from the P-Preferred-Identity header.
- 3) If there is not P-Preferred-Identity header in the INVITE request, the IP DECT phone

checks and presents the caller identification from the P-Asserted-Identity header.

- 4) If there is not P-Asserted-Identity header in the INVITE request, the IP DECT phone presents the caller identification derived from the FROM header.

### **Caller ID source = RPID-FROM**

- 1) The IP DECT phone checks Privacy: id header preferentially, if there is a Privacy: id in the INVITE request, the caller identification information will be hidden and the IP DECT phone LCD screen presents anonymous.
- 2) If there is not any Privacy: id header in the INVITE request, the IP DECT phone checks and presents the caller identification from the P-Preferred-Identity header.
- 3) If there is not P-Preferred-Identity header in the INVITE request, the IP DECT phone checks and presents the caller identification from the Remote-Party-ID header.
- 4) If there is not Remote-Party-ID header in the INVITE request, the IP DECT phone presents the caller identification derived from the FROM header.

### **Caller ID source =PAI-RPID-FROM**

- 1) The IP DECT phone checks Privacy: id header preferentially, if there is a Privacy: id in the INVITE request, the caller identification information will be hidden and the IP DECT phone LCD screen presents anonymous.
- 2) If there is not any Privacy: id header in the INVITE request, the IP DECT phone checks and presents the caller identification from the P-Preferred-Identity header.
- 3) If there is not P-Preferred-Identity header in the INVITE request, the IP DECT phone checks and presents the caller identification from the P-Asserted-Identity header.
- 4) If there is not P-Asserted-Identity header in the INVITE request, the IP DECT phone checks and presents the caller identification from the Remote-Party-ID header.
- 5) If there is not Remote-Party-ID header in the INVITE request, the IP DECT phone presents the caller identification derived from the FROM header.

### **Caller ID source =RPID-PAI-FROM**

- 1) The IP DECT phone checks Privacy: id header preferentially, if there is a Privacy: id in the INVITE request, the caller identification information will be hidden and the IP DECT phone LCD screen presents anonymous.
- 2) If there is not any Privacy: id header in the INVITE request, the IP DECT phone checks and presents the caller identification from the P-Preferred-Identity header.
- 3) If there is not P-Preferred-Identity header in the INVITE request, the IP DECT phone checks and presents the caller identification from the Remote-Party-ID header.
- 4) If there is not Remote-Party-ID header in the INVITE request, the IP DECT phone checks and presents the caller identification from the P-Asserted-Identity header.
- 5) If there is not P-Asserted-Identity in the INVITE request, the IP DECT phone presents the caller identification derived from the FROM header.

For more information on calling line identification presentation, refer to [Calling and Connected Line Identification Presentation on Yealink IP Phones](#).

### Procedure

CLIP can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure the presentation of the caller identity. <b>Parameter:</b> account.X.cid_source
		Specify whether to process Privacy header field. <b>Parameter:</b> account.X.cid_source_privacy
		Specify whether to process the P-Preferred-Identity (PPI) header for caller identity presentation. <b>Parameter:</b> account.X.cid_source_ppi
Local	Web User Interface	Configure the presentation of the caller identity. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

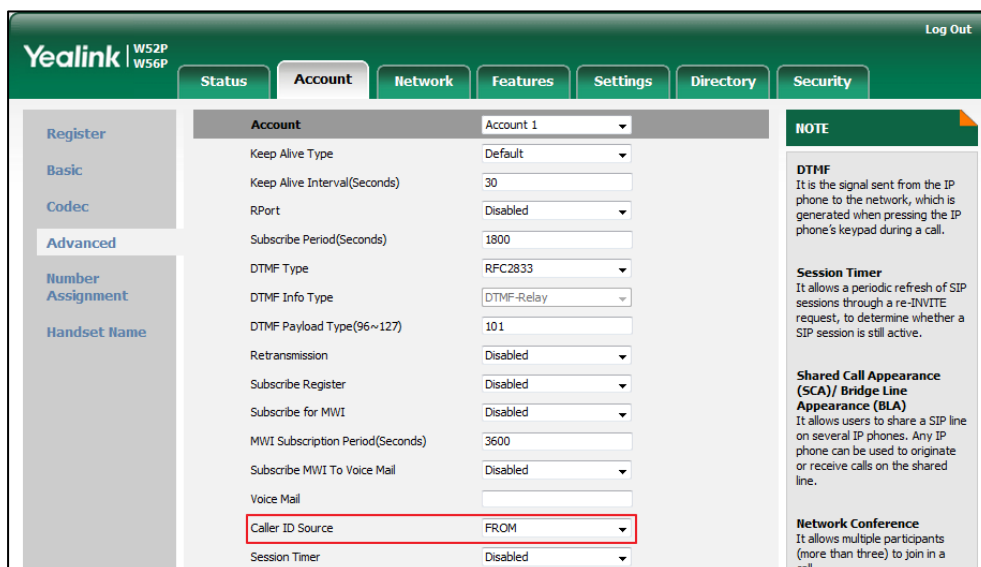
### Details of the Configuration Parameter:

Parameter	Permitted Values	Default
account.X.cid_source (X ranges from 1 to 5)	0, 1, 2, 3, 4 or 5	0
<b>Description:</b> Configures the presentation of the caller identity when receiving an incoming call for account X. 0-FROM 1-PAI 2-PAI-FROM 3-RPID-PAI-FROM		

Parameter	Permitted Values	Default
<p>4-PAI-RPID-FROM</p> <p>5-RPID-FROM</p> <p><b>Web User Interface:</b></p> <p>Account-&gt;Advanced-&gt;Caller ID Header</p> <p><b>Handset User Interface:</b></p> <p>None</p>		
<p><b>account.X.cid_source_privacy</b></p> <p>(X ranges from 1 to 5)</p>	<p>0 or 1</p>	<p>1</p>
<p><b>Description:</b></p> <p>Enables or disables the IP DECT phone to process Privacy header field in the SIP message for account X.</p> <p>0-Disabled</p> <p>1-Enabled</p> <p><b>Web User Interface:</b></p> <p>None</p> <p><b>Handset User Interface:</b></p> <p>None</p>		
<p><b>account.X.cid_source_ppi</b></p> <p>(X ranges from 1 to 5)</p>	<p>0 or 1</p>	<p>1</p>
<p><b>Description:</b></p> <p>Enables or disables the IP DECT phone to process the P-Preferred-Identity (PPI) header for caller identity presentation when receiving an incoming call for account X.</p> <p>0-Disabled</p> <p>1-Enabled</p> <p><b>Web User Interface:</b></p> <p>None</p> <p><b>Handset User Interface:</b></p> <p>None</p>		

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

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



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

## Connected Line Identification Presentation

Connected Line Identification Presentation (COLP) allows IP DECT phones to display the identity of the connected party specified for outgoing calls. IP DECT phones 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 RFC4916. Connected line identification presentation is also known as Called line identification presentation. In some cases, the remote party will be different from the called line identification presentation due to call diversion.

### Note

If the callee already exists in the local directory, the local contact name assigned to the callee should be preferentially displayed.

The following sessions show the enhancements of connected line identification according to the connected line identification source configured on the IP DECT phones.

### Connected Line Identification source = PAI-RPID

- 1) The IP DECT phone checks Privacy: id header preferentially, if there is a Privacy: id in the 18X or 200OK response, the connected line identification information will be hidden and the IP DECT phone LCD screen presents anonymous.
- 2) If there is not any Privacy: id header in the 18X or 200OK response, the IP DECT

phone checks and presents the connected line identification from the P-Asserted-Identity header.

- 3) If there is not P-Asserted-Identity header in the 18X or 200OK response, the IP DECT phone presents the connected line identification from the Remote-Party-ID header. If no, the IP DECT phone presents the connected line identification according to the dialed digits.

### Connected Line Identification source =Dialed digits

Yealink IP DECT phones present the connected line identification according to the dialed digits.

### Connected Line Identification source =RFC4916

Yealink IP DECT phones support to present the connected line identification from UPDATE message following the RFC 4916.

- 1) The IP DECT phone receives an UPDATE message during a call, the connected line identification on the LCD screen should be refreshed according the FROM SIP carried in the UPDATE message.

For more information on connected line identification presentation, refer to [Calling and Connected Line Identification Presentation on Yealink IP Phones](#).

### Procedure

COLP can be configured only using the configuration files.

<b>Configuration File</b>	<MAC>.cfg	Configure the presentation of the callee’s identity. <b>Parameter:</b> account.X.cp_source
		Specify whether to process Privacy header field. <b>Parameter:</b> account.X.cid_source_privacy

### Details of the Configuration Parameter:

Parameter	Permitted Values	Default
account.X.cp_source	0, 1 or 2	0
<b>Description:</b> Configures the presentation of the callee’s identity for account X.		

Parameter	Permitted Values	Default
<p><b>0</b>-PAI-RPID</p> <p><b>1</b>-Dialed Digits</p> <p><b>2</b>-RFC4916</p> <p><b>Note:</b> When the RFC 4916 is enabled on the IP DECT phone, the caller sends the SIP request message which contains the from-change tag in the Supported header. The caller then receives an UPDATE message from the callee, and displays the identity in the "From" header.</p> <p><b>Web User Interface:</b></p> <p>None</p> <p><b>Handset User Interface:</b></p> <p>None</p>		
<p><b>account.X.cid_source_privacy</b></p>	<p><b>0 or 1</b></p>	<p><b>1</b></p>
<p><b>Description:</b></p> <p>Enables or disables the IP DECT phone to process Privacy header field in the SIP message for account X.</p> <p><b>0</b>-Disabled</p> <p><b>1</b>-Enabled</p> <p><b>Web User Interface:</b></p> <p>None</p> <p><b>Handset User Interface:</b></p> <p>None</p>		

## Intercom

Intercom is a useful feature in an office environment to quickly connect with the operator or the secretary. You can make internal intercom calls and external intercom calls on the phone. Internal intercom calls are made between handsets registered to the same base station. External intercom calls can be made by dialing the feature access code followed by the number. External intercom calls depend on support from a SIP server. The handset can automatically answer an incoming external intercom call and play warning tone only when there is only one handset subscribed and no call in progress on the handset.

To automatically answer an incoming internal intercom call, you need to enable auto intercom feature on the handset. The following configuration types of auto intercom feature are available for selection:

- **On (Beep On):** Auto intercom feature is on. The handset will answer an incoming



internal intercom call automatically and play a warning tone.

- **On (Beep Off):** Auto intercom feature is on. The handset will answer an incoming internal intercom call automatically without a warning tone.
- **Off:** Auto intercom feature is off. You need to answer an incoming internal intercom call by pressing the **Accept** soft key.

### Procedure

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

<b>Configuration File</b>	y000000000025.cfg	Configure incoming intercom call feature. <b>Parameters:</b> features.intercom.headset_prior.enable custom.handset.auto_intercom
<b>Local</b>	Handset User Interface	Configure incoming intercom call feature for specified handset.

### Details of Configuration Parameters:

Parameters	Permitted Values	Default
<b>features.intercom.headset_prior.enable</b>	<b>0 or 1</b>	<b>1</b>
<b>Description:</b> Configures the channel mode when an incoming intercom call is answered through the handset. The headset should be connected in advance. 0-Speaker Mode 1-Headset Mode <b>Web User Interface:</b> None <b>Handset User Interface:</b> None		
<b>custom.handset.auto_intercom</b>	<b>0, 1 or 2</b>	<b>0</b>
<b>Description:</b> Configures whether the IP DECT phone automatically answers an incoming internal intercom call and plays a warning tone. 0-Off 1-On(Beep Off)		

Parameters	Permitted Values	Default
<p><b>2-On(Beep On)</b></p> <p>If it is set to 0, users need to answer incoming internal intercom calls manually.</p> <p>If it is set to 1, the handset will answer an incoming internal intercom call automatically without a warning tone.</p> <p>If it is set to 2, the handset will answer an incoming internal intercom call automatically and play a warning tone. It works when the silence mode is off.</p> <p><b>Note:</b> It works only if the value of the parameter “auto_provision.handset_configured.enable” is set to 1 (Enabled).</p> <p><b>Web User Interface:</b></p> <p>None</p> <p><b>Handset User Interface:</b></p> <p>OK-&gt;Settings-&gt;Telephony-&gt;Auto Intercom</p>		

**To configure auto intercom for specify handset:**

1. Press **OK** to enter the main menu.
2. Select **Settings->Telephony->Auto Intercom**.  
The LCD screen displays three configuration types.
3. Press **▲** or **▼** to highlight the desired configuration type.
4. Press the **Change** soft key.  
The radio box of the selected configuration type is marked.

## Call Timeout

Call timeout defines a specific period of time within which the IP DECT phone will cancel the dialing if the call is not answered.

**Procedure**

Call timeout can only be configured using the configuration files.

<b>Configuration File</b>	y000000000025.cfg	<p>Configure the duration time (in seconds) in the ring back state.</p> <p><b>Parameters:</b></p> <p>phone_setting.ringback_timeout</p>
---------------------------	-------------------	---

**Details of the Configuration Parameter:**

Parameter	Permitted Values	Default
phone_setting.ringback_timeout	Integer from 0 to 3600	180
<b>Description:</b> Configures the duration time (in seconds) in the ring back state. If it is set to 180, the phone will cancel the dialing if the call is not answered within 180 seconds. <b>Web User Interface:</b> None <b>Handset User Interface:</b> None		

## Ringling Timeout

Ringling timeout defines a specific period of time within which the IP DECT phone will stop ringling if the call is not answered.

**Procedure**

Ringling timeout can only be configured using the configuration files.

<b>Configuration File</b>	y00000000025.cfg	Configure the duration time (in seconds) in the ringling state. <b>Parameters:</b> phone_setting.ringling_timeout
---------------------------	------------------	---

**Details of the Configuration Parameter:**

Parameter	Permitted Values	Default
phone_setting.ringling_timeout	Integer from 0 to 3600	180
<b>Description:</b> Configures the duration time (in seconds) in the ringling state. If it is set to 180, the phone will stop ringling if the call is not answered within 180 seconds. <b>Web User Interface:</b> None <b>Handset User Interface:</b>		

Parameter	Permitted Values	Default
None		

## Send user=phone

When placing a call, the IP DECT phone will send an INVITE request to the proxy server. Send user=phone feature allows adding user=phone to the SIP header of the INVITE message.

Example of a SIP INVITE message:

```

INVITE sip:101@10.3.5.199:5060;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.3.20.6:5060;branch=z9hG4bK2475812834
From: "1010" <sip:1010@10.3.5.199:5060>;tag=3747068208
To: <sip:101@10.3.5.199:5060;user=phone>
Call-ID: 0_4008470062@10.3.20.6
CSeq: 1 INVITE
Contact: <sip:1010@10.3.20.6:5060>
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 W52P 25.80.0.10
Allow-Events: talk,hold,conference,refer,check-sync
Content-Length: 300
    
```

### Procedure

Send user=phone can be configured using the configuration files or locally.

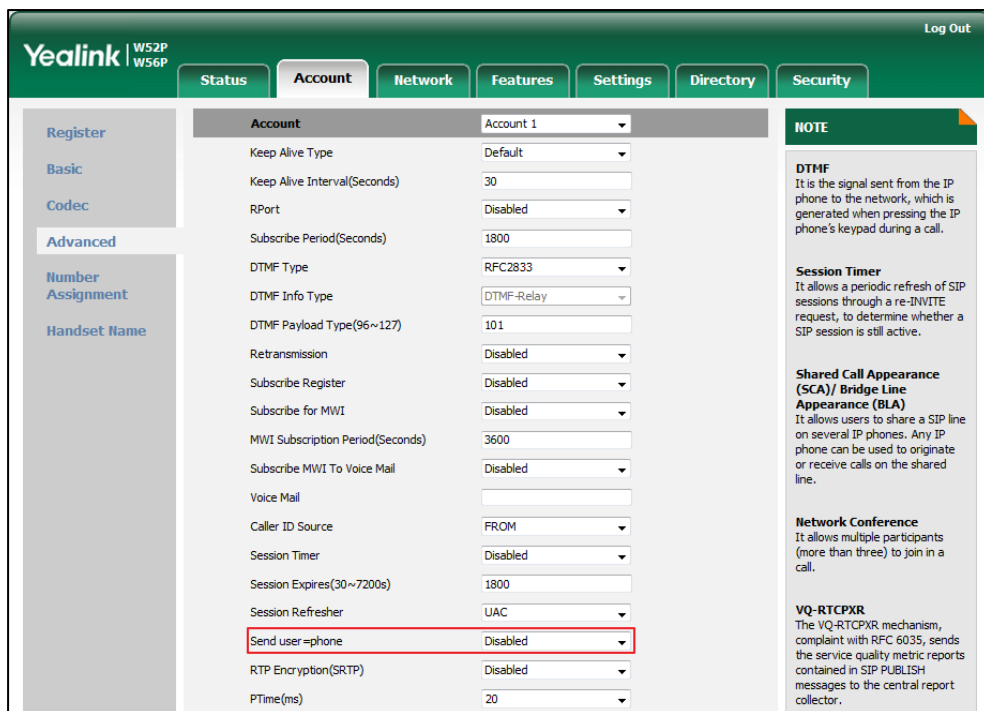
<b>Configuration File</b>	<MAC>.cfg	Configure send user=phone feature on a per-line basis. <b>Parameters:</b> account.X.enable_user_equal_phone
<b>Local</b>	Web User Interface	Configure send user=phone feature on a per-line basis. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

**Details of the Configuration Parameter:**

Parameter	Permitted Values	Default
<b>account.X.enable_user_equal_phone</b> (X ranges from 1 to 5)	<b>0 or 1</b>	<b>0</b>
<p><b>Description:</b> Enables or disables the IP DECT phone to add “user=phone” to the SIP header of the INVITE message for account X.</p> <p><b>0-Disabled</b> <b>1-Enabled</b></p> <p><b>Web User Interface:</b> Account-&gt;Advanced-&gt;Use user=phone</p> <p><b>Handset User Interface:</b> None</p>		

**To configure send user=phone feature via web user interface:**

1. Click on **Account->Advanced**.
2. Select the desired account from the pull-down list of **Account**.
3. Select the desired value from the pull-down list of **Send user=phone**.



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

## SIP Send MAC

The IP DECT phone can send the MAC address in the REGISTER message. SIP send MAC allow adding "Mac:<PhoneMACAddress>" (e.g., Mac: 00:15:65:74:b1:50) to the SIP header of the REGISTER message.

Example of a SIP REGISTER message:

```
REGISTER sip:10.3.5.199:5060 SIP/2.0
Via: SIP/2.0/UDP 10.3.20.14:5060;branch=z9hG4bK3593117201
From: "11" <sip:11@10.3.5.199:5060>;tag=2788360609
To: "11" <sip:11@10.3.5.199:5060>
Call-ID: 1_1863786852@10.3.20.14
CSeq: 2 REGISTER
Contact: <sip:11@10.3.20.14:5060;line=cc75882e976e208>
Allow: INVITE, INFO, PRACK, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REGISTER, SUBSCRIBE, REFER,
PUBLISH, UPDATE, MESSAGE
Max-Forwards: 70
User-Agent: Yealink W52P 25.80.0.10
Expires: 0
Allow-Events: talk,hold,conference,refer,check-sync
Mac: 00:15:65:5F:9D:7E
Content-Length: 0
```

### Procedure

SIP send MAC can be configured using the configuration files or locally.

<b>Configuration File</b>	<MAC>.cfg	Configure SIP send MAC on a per-line basis. <b>Parameters:</b> account.X.register_mac
<b>Local</b>	Web User Interface	Configure SIP send MAC on a per-line basis. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

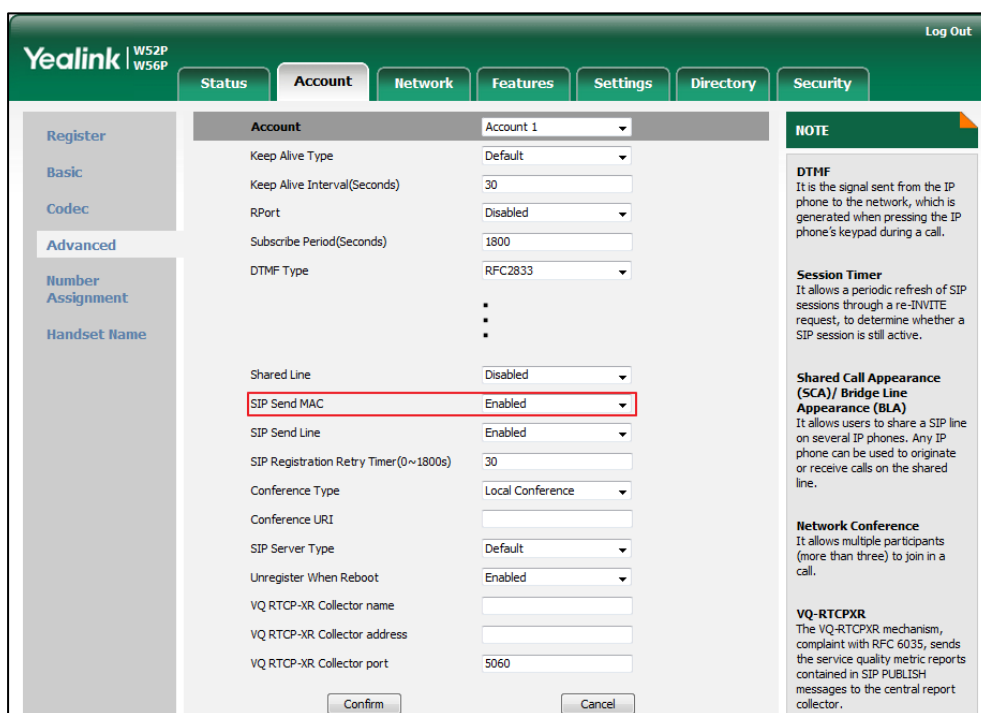
### Details of the Configuration Parameter:

Parameter	Permitted Values	Default
<b>account.X.register_mac</b> (X ranges from 1 to 5)	<b>0 or 1</b>	<b>0</b>

Parameter	Permitted Values	Default
<p><b>Description:</b>                      Enables or disables the IP DECT phone to add MAC address to the SIP header of the REGISTER message for account X.</p> <p>0-Disabled                      1-Enabled</p> <p><b>Web User Interface:</b>                      Account-&gt;Advanced-&gt;SIP Send MAC</p> <p><b>Handset User Interface:</b>                      None</p>		

To configure SIP send MAC feature via web user interface:

1. Click on **Account->Advanced**.
2. Select the desired account from the pull-down list of **Account**.
3. Select the desired value from the pull-down list of **SIP Send MAC**.



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

## SIP Send Line

The IP DECT phone can send the line number in the REGISTER message. SIP send line allow adding "Line:<linenumber>" (e.g., Line: 1) to the SIP header of the REGISTER message. The line number is a number between 0 and 15.

Example of a SIP REGISTER message:

```
REGISTER sip:10.3.5.199:5060 SIP/2.0
Via: SIP/2.0/UDP 10.3.20.14:5060;branch=z9hG4bK3990593443
From: "11" <sip:11@10.3.5.199:5060>;tag=255071842
To: "11" <sip:11@10.3.5.199:5060>
Call-ID: 1_2369214377@10.3.20.14
CSeq: 2 REGISTER
Contact: <sip:11@10.3.20.14:5060;line=1da6aa8d7254654>
Allow: INVITE, INFO, PRACK, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REGISTER, SUBSCRIBE, REFER,
PUBLISH, UPDATE, MESSAGE
Max-Forwards: 70
User-Agent: Yealink W52P 25.80.0.10
Expires: 0
Allow-Events: talk,hold,conference,refer,check-sync
Line: 0
Content-Length: 0
```

## Procedure

SIP send line can be configured using the configuration files or locally.

<b>Configuration File</b>	<MAC>.cfg	Configure SIP send line on a per-line basis. <b>Parameters:</b> account.X.register_line
<b>Local</b>	Web User Interface	Configure SIP send line on a per-line basis. <b>Navigate to:</b> http://<phoneIPAddress>/servlet? p=account-adv&q=load&acc=0

## Details of the Configuration Parameter:

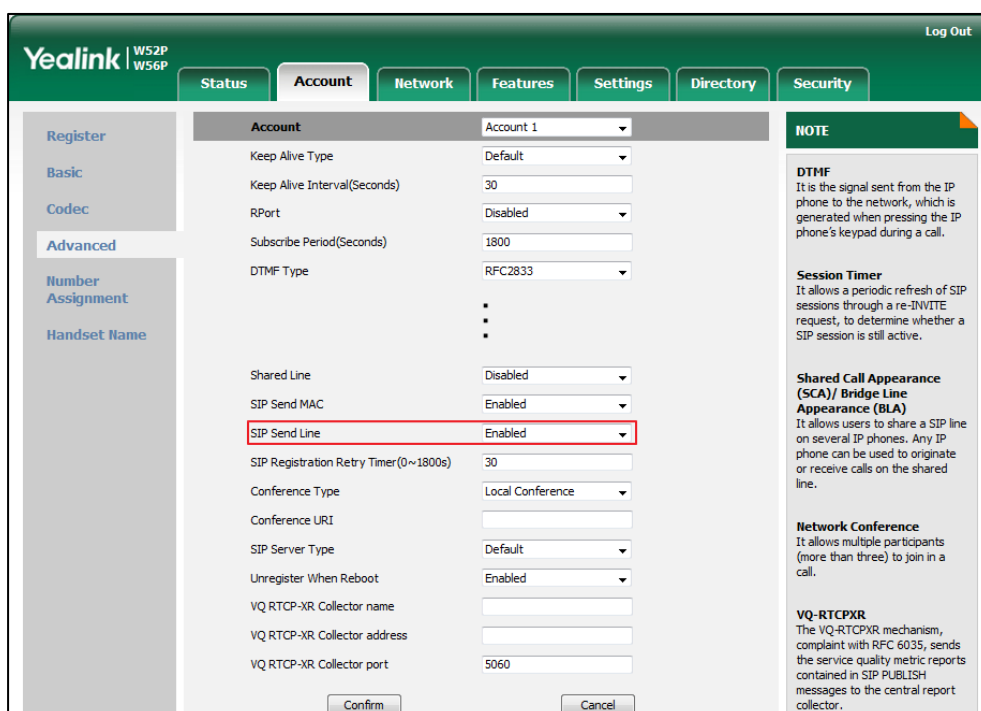
Parameter	Permitted Values	Default
<b>account.X.register_line</b> (X ranges from 1 to 5)	<b>0 or 1</b>	<b>1</b>
<b>Description:</b> Enables or disables the IP DECT phone to add line number to the SIP header of the REGISTER message for account X.  <b>0-Disabled</b> <b>1-Enabled</b>		



Parameter	Permitted Values	Default
<b>Web User Interface:</b>		
Account->Advanced->SIP Send Line		
<b>Handset User Interface:</b>		
None		

To configure SIP send Line feature via web user interface:

1. Click on **Account->Advanced**.
2. Select the desired account from the pull-down list of **Account**.
3. Select the desired value from the pull-down list of **SIP Send Line**.



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

## Reserve # in User Name

Reserve # in User Name feature allows IP DECT phones to reserve “#” in user name. When Reserve # in User Name feature is disabled, “#” will be converted into “%23”. For example, the user registers an account (user name: 1010#) on the phone, the phone will send 1010%23 instead of 1010# in the REGISTER message or INVITE message to SIP server.

Example of a SIP INVITE message:

```
INVITE sip:2@10.3.5.199:5060 SIP/2.0
Via: SIP/2.0/UDP 10.3.20.6:5060;branch=z9hG4bK1867789050
```

```

From: "1010" <sip:1010%23@10.3.5.199:5060>;tag=1945988802
To: <sip:2@10.3.5.199:5060>
Call-ID: 0_2336101648@10.3.20.6
CSeq: 1 INVITE
Contact: <sip:1010%23@10.3.20.6:5060>
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 W52P 25.80.0.10
Allow-Events: talk,hold,conference,refer,check-sync
Content-Length: 300
    
```

### Procedure

Reserve # in User Name can be configured using the configuration files.

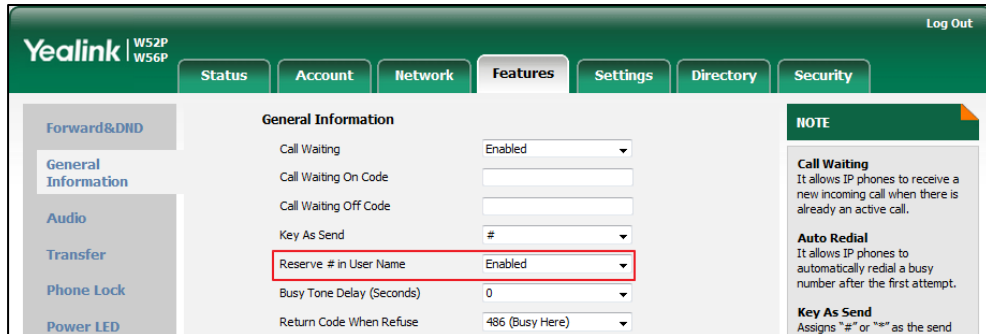
<b>Configuration File</b>	y00000000025.cfg	Configure reserve # in user name. <b>Parameters:</b> sip.use_23_as_pound
<b>Local</b>	Web User Interface	Configure reserve # in user name. <b>Navigate to:</b> http://<phoneIPAddress>servlet? p=features-general&q=load

### Details of the Configuration Parameter:

Parameter	Permitted Values	Default
sip.use_23_as_pound	0 or 1	1
<p><b>Description:</b> Enables or disables the IP DECT phone to reserve the pound sign (#) in the user name. 0-Disabled(convert the pound sign into "%23") 1-Enabled</p> <p><b>Web User Interface:</b> Features-&gt;General Information-&gt;Reserve # in User Name</p> <p><b>Handset User Interface:</b> None</p>		

To configure reserve # in user name feature via web user interface:

1. Click on **Features->General Information**.
2. Select the desired value from the pull-down list of **Reserve # in User Name**.



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

## Unregister When Reboot

Unregister when reboot feature allows the IP DECT phones to unregister first before re-registering the account when finishing a reboot.

### Procedure

Unregister when reboot can be configured using the configuration files or locally.

<b>Configuration File</b>	<MAC>.cfg	Configure unregister when reboot. <b>Parameters:</b> account.X.unregister_on_reboot
<b>Local</b>	Web User Interface	Configure unregister when reboot. <b>Navigate to:</b> http://<phoneIPAddress>/servlet? p=account-adv&q=load&acc=0

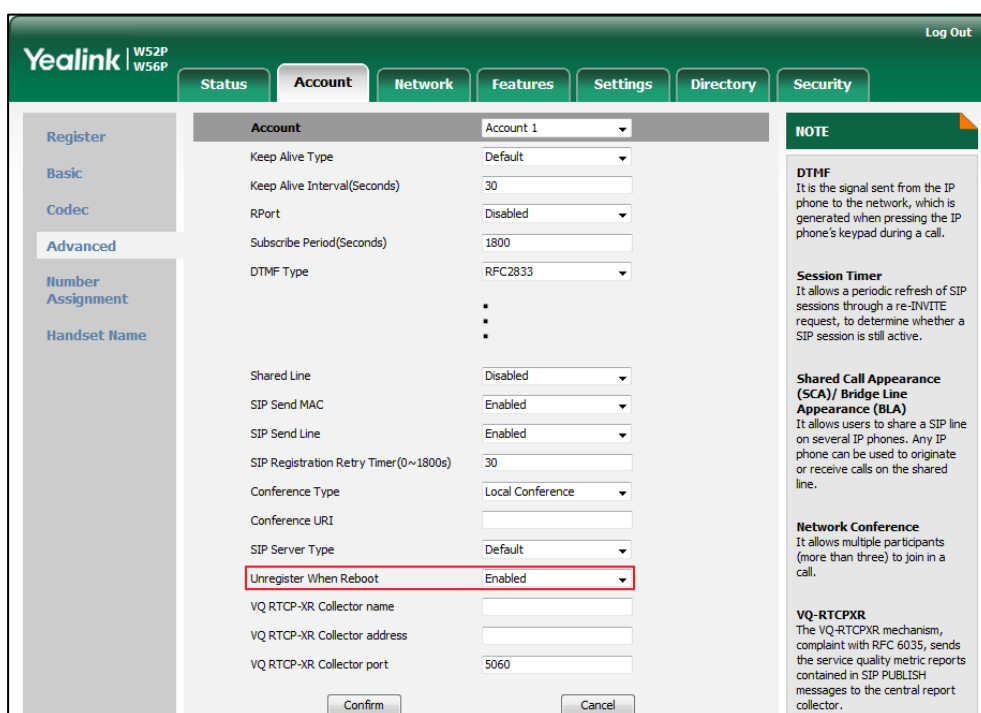
### Details of the Configuration Parameter:

Parameter	Permitted Values	Default
<b>account.X.unregister_on_reboot</b> (X ranges from 1 to 5)	<b>0 or 1</b>	<b>0</b>
<b>Description:</b> Enables or disables the IP DECT phone to unregister first before re-registering		

Parameter	Permitted Values	Default
account X when finishing a reboot.		
0-Disabled		
1-Enabled		
<b>Web User Interface:</b>		
Account->Advanced->Unregister When Reboot		
<b>Handset User Interface:</b>		
None		

To configure unregister when reboot via web user interface:

1. Click on **Account->Advanced**.
2. Select the desired account from the pull-down list of **Account**.
3. Select the desired value from the pull-down list of **Unregister When Reboot**.



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

## 100 Reliable Retransmission

As described in [RFC3262](#), 100rel tag is for reliability of provisional responses. When present in a Supported header, it indicates that the IP DECT phone can send or receive reliable provisional responses. When present in a Require header in a reliable provisional response, it indicates that the response is to be sent reliably.

Example of a SIP INVITE message:

```

INVITE sip:1024@pbx.yealink.com:5060 SIP/2.0
Via: SIP/2.0/UDP 10.3.6.197:5060;branch=z9hG4bK1708689023
From: "1025" <sip:1025@pbx.yealink.com:5060>;tag=1622206783
To: <sip:1024@pbx.yealink.com:5060>
Call-ID: 0_537569052@10.3.6.197
CSeq: 2 INVITE
Contact: <sip:1025@10.3.6.197:5060>
Authorization: Digest username="1025", realm="pbx.yealink.com",
nonce="BroadWorksXi5stub71Ts2nb05BW", uri="sip:1024@pbx.yealink.com:5060",
response="f7e9d35c55af45b3f89beae95e913171", algorithm=MD5, cnonce="0a4f113b", qop=auth,
nc=00000001
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 W52P 25.80.0.10
Supported: 100rel
Allow-Events: talk,hold,conference,refer,check-sync
Content-Length: 302
    
```

### Procedure

100 Reliable Retransmission can be configured using the configuration files or locally.

<b>Configuration File</b>	<MAC>.cfg	Configure the 100 reliable retransmission feature. <b>Parameters:</b> account.X.100rel_enable
<b>Local</b>	Web User Interface	Configure the 100 reliable retransmission feature. <b>Navigate to:</b> http://<phoneIPAddress>/servlet? p=account-adv&q=load&acc=0

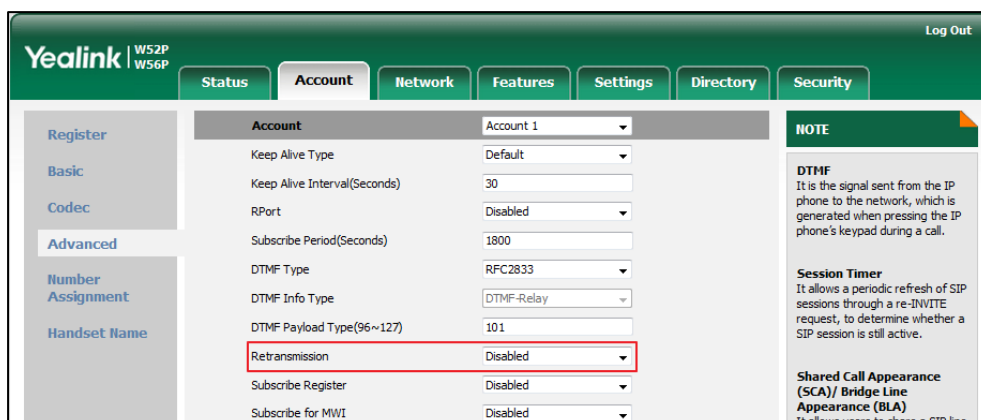
### Details of the Configuration Parameter:

Parameter	Permitted Values	Default
<b>account.X.100rel_enable</b> (X ranges from 1 to 5)	<b>0 or 1</b>	<b>0</b>
<b>Description:</b> Enables or disables the 100 reliable retransmission feature for account X.		

Parameter	Permitted Values	Default
0-Disabled 1-Enabled		
<b>Web User Interface:</b> Account->Advanced->Retransmission		
<b>Handset User Interface:</b> None		

To configure 100 reliable retransmission via web user interface:

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



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

## Reboot in Talking

Reboot in talking feature allows base station to reboot during an active call when it receives packets.

### Procedure

Reboot in talking can be configured using the configuration files or locally.

<b>Configuration File</b>	y000000000025.cfg	Configure reboot in talking. <b>Parameter:</b> features.reboot_in_talk_enable
<b>Local</b>	Web User Interface	Configure reboot in talking. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=f

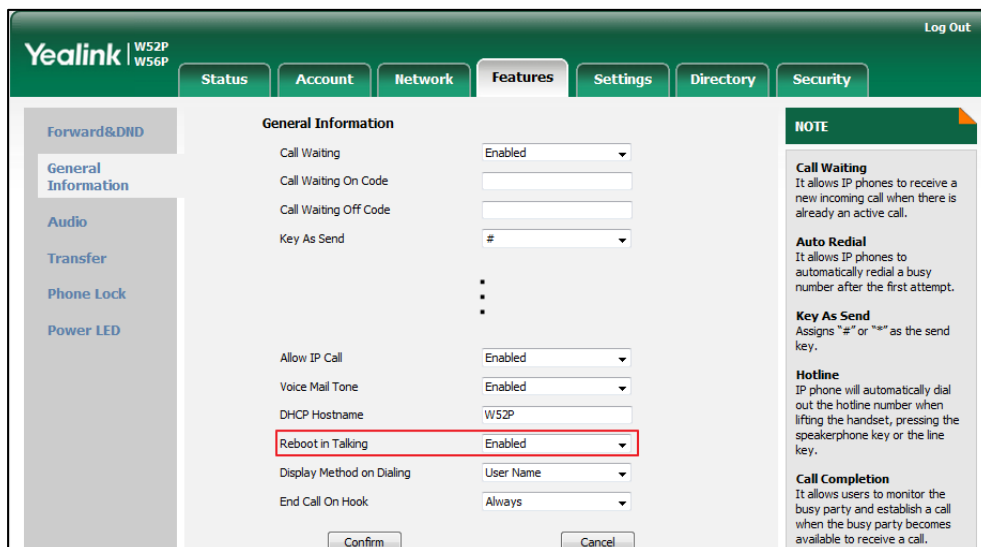
		eatures-general&q=load
--	--	------------------------

**Details of Configuration Parameters:**

Parameter	Permitted Values	Default
features.reboot_in_talk_enable	0 or 1	0
<p><b>Description:</b>                      Enables or disables the base station to reboot during a call when it receives a reboot packet.                      0-Disabled                      1-Enabled</p> <p><b>Web User Interface:</b>                      Features-&gt;General Information-&gt;Reboot in Talking</p> <p><b>Handset User Interface:</b>                      None</p>		

**To configure reboot in talking via web user interface:**

1. Click on **Features->General Information**.
2. Select the desired value from the pull-down list of **Reboot in Talking** field.



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

## End Call on Hook

End call on hook feature allows ending a call when placing the handset into the charger cradle.

### Procedure

End call on hook can be configured using the configuration files or locally.

<b>Configuration File</b>	y000000000025.cfg	Configure end call on hook. <b>Parameter:</b> phone_setting.end_call_on_hook.enable
<b>Local</b>	Web User Interface	Configure end call on hook. <b>Navigate to:</b> <a href="http://&lt;phoneIPAddress&gt;/servlet?p=features-general&amp;q=load">http://&lt;phoneIPAddress&gt;/servlet?p=features-general&amp;q=load</a>

### Details of Configuration Parameters:

Parameter	Permitted Values	Default
phone_setting.end_call_on_hook.enable	0 or 1	1
<p><b>Description:</b> Enables or disables to end a call when placing the handset into the charger cradle.</p> <p><b>0</b>-Never <b>1</b>-Always</p> <p><b>Web User Interface:</b> Features-&gt;General Information-&gt;End Call On Hook</p> <p><b>Handset User Interface:</b> None</p>		



To configure end call on hook via web user interface:

1. Click on **Features->General Information**.
2. Select the desired value from the pull-down list of **End Call On Hook** field.

The screenshot displays the Yealink W52P/W56P web interface. The top navigation bar includes 'Status', 'Account', 'Network', 'Features', 'Settings', 'Directory', and 'Security'. The 'Features' tab is active, and the 'General Information' sub-tab is selected. The left sidebar lists various configuration categories: Forward&DND, General Information (highlighted), Audio, Transfer, Phone Lock, and Power LED. The main content area shows the 'General Information' configuration table:

General Information	
Call Waiting	Enabled
Call Waiting On Code	
Call Waiting Off Code	
Key As Send	#
	.
	.
	.
Allow IP Call	Enabled
Voice Mail Tone	Enabled
DHCP Hostname	W52P
Reboot in Talking	Enabled
Display Method on Dialing	User Name
<b>End Call On Hook</b>	<b>Always</b>

At the bottom of the configuration area are 'Confirm' and 'Cancel' buttons. On the right side, there is a 'NOTE' section with the following text:

**Call Waiting**  
It allows IP phones to receive a new incoming call when there is already an active call.

**Auto Redial**  
It allows IP phones to automatically redial a busy number after the first attempt.

**Key As Send**  
Assigns "#" or "\*" as the send key.

**Hotline**  
IP phone will automatically dial out the hotline number when lifting the handset, pressing the speakerphone key or the line key.

**Call Completion**  
It allows users to monitor the busy party and establish a call when the busy party becomes available to receive a call.

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



# Configuring Advanced Features

---

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

- [Remote Phone Book](#)
- [Lightweight Directory Access Protocol \(LDAP\)](#)
- [Shared Call Appearance \(SCA\)](#)
- [Message Waiting Indicator](#)
- [Server Redundancy](#)
- [Static DNS Cache](#)
- [Quality of Service](#)
- [Network Address Translation](#)
- [Real-Time Transport Protocol](#)
- [TR-069 Device Management](#)

## 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 DECT phone can establish a connection with the remote server and download the phone book, and then display the remote phonebook entries on the handset user interface. The IP DECT phones support up to 5 remote phone books. Remote phonebook is customizable.

Incoming/Outgoing Call Lookup allows the IP DECT phones to search the entry names from the remote phone book for incoming/outgoing calls. Update Time Interval specifies how often IP DECT phones refresh the local cache of the remote phone book.

## Procedure

Remote phonebook can be configured using the configuration files or locally.

<b>Configuration File</b>	y00000000025.cfg	<p>Specify the access URL and the display name of the remote phone book.</p> <p><b>Parameters:</b></p> <p>remote_phonebook.data.X.url                      remote_phonebook.data.X.name                      remote_phonebook.display_name</p>
		<p>Specify whether to query the entry name from the remote phone book for outgoing/incoming calls.</p> <p><b>Parameter:</b></p> <p>features.remote_phonebook.enable</p>
		<p>Specify how often the IP DECT phone refreshes the local cache of the remote phone book.</p> <p><b>Parameter:</b></p> <p>features.remote_phonebook.flash_time</p>
		<p>Specify whether to refresh the local cache of the remote phone book at a time when accessing the remote phone book.</p> <p><b>Parameter:</b></p> <p>features.remote_phonebook.enter_update_enable</p>
<b>Local</b>	Web User Interface	<p>Specify the access URL and the display name of the remote phone book.</p> <p>Specify whether to query the entry name from the remote phonebook for outgoing/incoming calls.</p> <p>Specify how often the IP DECT phone refreshes the local cache of the remote phone book.</p> <p><b>Navigate to:</b></p> <p>http://&lt;phoneIPAddress&gt;/servlet?p=contacts-remote&amp;q=load</p>

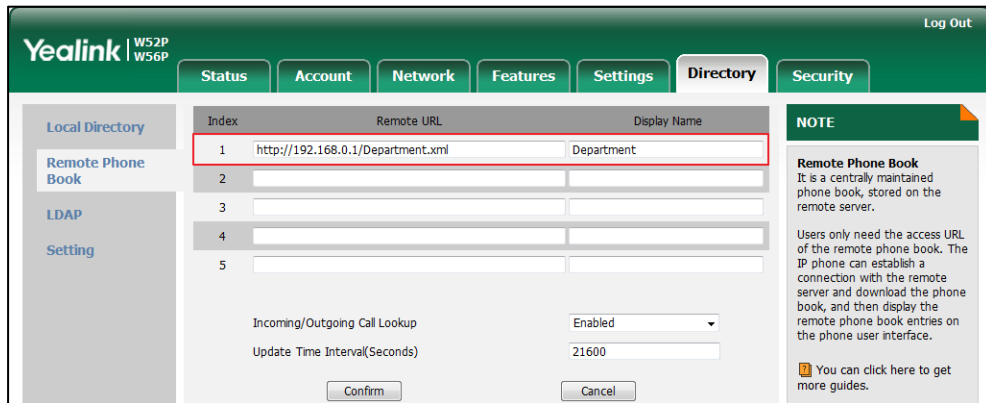
## Details of Configuration Parameters:

Parameters	Permitted Values	Default
<b>remote_phonebook.data.X.url</b> (X ranges from 1 to 5)	<b>URL within 511 characters</b>	<b>Blank</b>
<b>Description:</b> Configures the access URL of the remote phone book. <b>Example:</b> remote_phonebook.data.1.url = http://192.168.1.20/phonebook.xml <b>Web User Interface:</b> Directory->Remote Phone Book->Remote URL <b>Handset User Interface:</b> None		
<b>remote_phonebook.data.X.name</b> (X ranges from 1 to 5)	<b>String within 99 characters</b>	<b>Blank</b>
<b>Description:</b> Configures the display name of the remote phone book item. <b>Example:</b> remote_phonebook.data.1.name = Xmyl <b>Web User Interface:</b> Directory->Remote Phone Book->Display Name <b>Handset User Interface:</b> None		
<b>remote_phonebook.display_name</b>	<b>String within 99 characters</b>	<b>Blank</b>
<b>Description:</b> Configures the display name of the remote phone book. <b>Example:</b> remote_phonebook.display_name = Friends "Friends" will be displayed on the handset LCD screen at the path <b>OK-&gt;Directory</b> . If it is left blank, Remote Phone Book will be the display name. <b>Web User Interface:</b> None <b>Handset User Interface:</b> None		

Parameters	Permitted Values	Default
<b>features.remote_phonebook.enable</b>	0 or 1	0
<p><b>Description:</b>                      Enables or disables the IP DECT phone to perform a remote phone book search for an incoming or outgoing call and display the matched results on the LCD screen.                      0-Disabled                      1-Enabled</p> <p><b>Web User Interface:</b>                      Directory-&gt;Remote Phone Book-&gt;Incoming/Outgoing Call Lookup</p> <p><b>Handset User Interface:</b>                      None</p>		
<b>features.remote_phonebook.flash_time</b>	0, Integer from 3600 to 1296000	21600
<p><b>Description:</b>                      Configures how often to refresh the local cache of the remote phone book. If it is set to 3600, the IP DECT phone will refresh the local cache of the remote phone book every 3600 seconds.  <b>Note:</b> If it is set to 0, the IP DECT phone will refresh the local cache of the remote phone book a periodically.</p> <p><b>Web User Interface:</b>                      Directory-&gt;Remote Phone Book-&gt;Update Time Interval(Seconds)</p> <p><b>Handset User Interface:</b>                      None</p>		
<b>features.remote_phonebook.enter_update_enable</b>	0 or 1	0
<p><b>Description:</b>                      Enables or disables the IP DECT phone to refresh the local cache of the remote phone book at a time when accessing the remote phone book.                      0-Disabled                      1-Enabled</p> <p><b>Web User Interface:</b>                      None</p> <p><b>Handset User Interface:</b>                      None</p>		

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

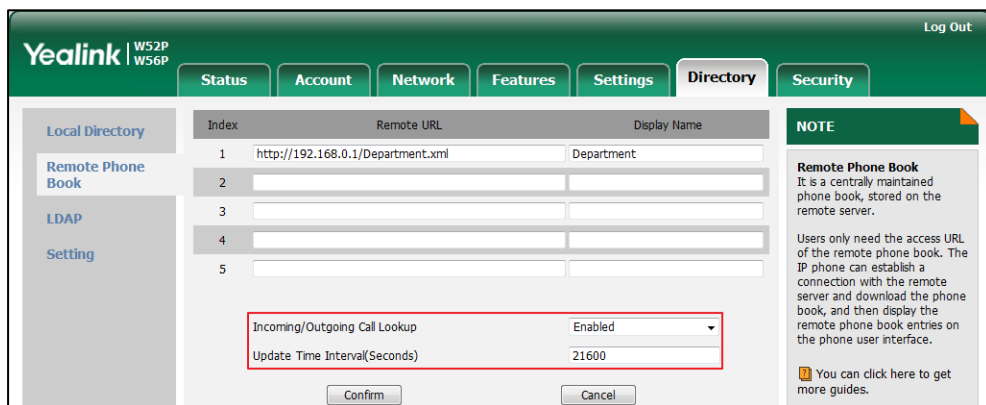
1. Click on **Directory->Remote Phone Book**.
2. Enter the access URL in the **Remote URL** field.
3. Enter the name in the **Display Name** field.



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

To configure incoming/outgoing call lookup and update time interval via web user interface:

1. Click on **Directory->Remote Phone Book**.
2. Select the desired value from the pull-down list of **Incoming/Outgoing Call Lookup**.
3. Enter the desired time in the **Update Time Interval(Seconds)** field.



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

## Lightweight Directory Access Protocol (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 DECT phones can be configured to interface with a corporate directory server that supports LDAP version 2 or 3. The following LDAP servers are supported:

- Microsoft Active Directory

- Sun ONE Directory Server
- Open LDAP Directory Server
- Microsoft Active Directory Application Mode (ADAM)

The biggest plus for LDAP is that users can access the central LDAP directory of the corporation using IP DECT phones. Therefore they do not have to maintain the directory locally. Users can search and dial out from the LDAP directory, and save LDAP entries to the local directory. LDAP entries displayed on the IP DECT phone are read only, which cannot be added, edited or deleted by users. When an LDAP server is properly configured, the IP DECT 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" can be used to select the desired entry or group, and return the desired information.

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

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

### LDAP Attributes

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

Abbreviation	Name	Description
gn	givenName	First name
cn	commonName	LDAP attribute is 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

For more information on LDAP, refer to [LDAP Phonebook on Yealink IP Phones](#).



### Procedure

LDAP can be configured using the configuration files or locally.

<p><b>Configuration File</b></p>	<p>y000000000025.cfg</p>	<p>Configure LDAP.</p> <p><b>Parameters:</b></p> <p>ldap.enable                      ldap.name_filter                      ldap.number_filter                      ldap.tls_mode                      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.call_out_lookup                      ldap.ldap_sort                      ldap.incoming_call_special_search.enable</p>
<p><b>Local</b></p>	<p>Web User Interface</p>	<p>Configure LDAP.</p> <p><b>Navigate to:</b></p> <p>http://&lt;phoneIPAddress&gt;/servlet                      ?p=contacts-LDAP&amp;q=load</p>

### Details of Configuration Parameters:

Parameters	Permitted Values	Default
<p>ldap.enable</p>	<p>0 or 1</p>	<p>0</p>
<p><b>Description:</b></p> <p>Enables or disables LDAP feature on the IP DECT phone.</p> <p>0-Disabled                      1-Enabled</p>		

Parameters	Permitted Values	Default
<p><b>Web User Interface:</b> Directory-&gt;LDAP-&gt;Enable LDAP</p> <p><b>Handset User Interface:</b> None</p>		
<p><b>ldap.name_filter</b></p>	<p>String within 99 characters</p>	<p>Blank</p>
<p><b>Description:</b> Configures the search criteria for LDAP contact names look up. The "*" symbol in the filter stands for any character. The "%" symbol in the filter stands for the name prefix entered by the user.</p> <p><b>Example:</b> ldap.name_filter = ( (cn=%)(sn=%)) When the cn or sn of the LDAP contact starts with the entered prefix, the record will be displayed on the LCD screen.</p> <p><b>Web User Interface:</b> Directory-&gt;LDAP-&gt;LDAP Name Filter</p> <p><b>Handset User Interface:</b> None</p>		
<p><b>ldap.number_filter</b></p>	<p>String within 99 characters</p>	<p>Blank</p>
<p><b>Description:</b> Configures the search criteria for LDAP contact numbers look up. The "*" symbol in the filter stands for any number. The "%" symbol in the filter stands for the number prefix entered by the user.</p> <p><b>Example:</b> ldap.number_filter = ( (telephoneNumber=%)(mobile=%)(ipPhone=%)) When the number prefix of the telephone Number, mobile or ipPhone of the contact record matches the search criteria, the record will be displayed on the LCD screen.</p> <p><b>Web User Interface:</b> Directory-&gt;LDAP-&gt;LDAP Number Filter</p> <p><b>Handset User Interface:</b> None</p>		
<p><b>ldap.tls_mode</b></p>	<p>0, 1 or 2</p>	<p>0</p>
<p><b>Description:</b></p>		

Parameters	Permitted Values	Default
<p>Configures the connection mode between the LDAP server and the IP DECT phone.</p> <p><b>0-LDAP</b>—Unencrypted connection between LDAP server and the IP DECT phone (port 389 is used by default).</p> <p><b>1-LDAP TLS Start</b>—TLS/SSL connection between LDAP server and the IP DECT phone (port 389 is used by default).</p> <p><b>2-LDAPs</b>—TLS/SSL connection between LDAP server and the IP DECT phone (port 636 is used by default).</p> <p><b>Web User Interface:</b> Directory-&gt;LDAP-&gt;LDAP TLS Mode</p> <p><b>Handset User Interface:</b> None</p>		
<b>ldap.host</b>	<b>IP address or domain name</b>	<b>Blank</b>
<p><b>Description:</b> Configures the IP address or domain name of the LDAP server.</p> <p><b>Example:</b> ldap.host = 192.168.1.20</p> <p><b>Web User Interface:</b> Directory-&gt;LDAP-&gt;Server Address</p> <p><b>Handset User Interface:</b> None</p>		
<b>ldap.port</b>	<b>Integer from 1 to 65535</b>	<b>389</b>
<p><b>Description:</b> Configures the port of the LDAP server.</p> <p><b>Example:</b> ldap.port = 389</p> <p><b>Web User Interface:</b> Directory-&gt;LDAP-&gt;Port</p> <p><b>Handset User Interface:</b> None</p>		
<b>ldap.base</b>	<b>String within 99 characters</b>	<b>Blank</b>
<p><b>Description:</b> Configures the LDAP search base which corresponds to the location of the LDAP</p>		

Parameters	Permitted Values	Default
<p>phonebook from which the LDAP search request begins. The search base narrows the search scope and decreases directory search time.</p> <p><b>Example:</b></p> <p>ldap.base = dc=yealink,dc=cn</p> <p><b>Web User Interface:</b></p> <p>Directory-&gt;LDAP-&gt;Base</p> <p><b>Handset User Interface:</b></p> <p>None</p>		
ldap.user	String within 99 characters	Blank
<p><b>Description:</b></p> <p>Configures the user name used to login the LDAP server.</p> <p>This parameter can be left blank in case the server allows anonymous to login. Otherwise you will need to provide the username to login the LDAP server.</p> <p><b>Example:</b></p> <p>ldap.user = cn=manager,dc=yealink,dc=cn</p> <p><b>Web User Interface:</b></p> <p>Directory-&gt;LDAP-&gt;Username</p> <p><b>Handset User Interface:</b></p> <p>None</p>		
ldap.password	String within 99 characters	Blank
<p><b>Description:</b></p> <p>Configures the password to login the LDAP server.</p> <p>This parameter can be left blank in case the server allows anonymous to login. Otherwise you will need to provide the password to login the LDAP server.</p> <p><b>Example:</b></p> <p>ldap.password = secret</p> <p><b>Web User Interface:</b></p> <p>Directory-&gt;LDAP-&gt;Password</p> <p><b>Handset User Interface:</b></p> <p>None</p>		
ldap.max_hits	Integer from 1 to 32000	50
<p><b>Description:</b></p>		

Parameters	Permitted Values	Default
<p>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.</p> <p><b>Example:</b> ldap.max_hits = 50</p> <p><b>Web User Interface:</b> Directory-&gt;LDAP-&gt;Max Hits (1~32000)</p> <p><b>Handset User Interface:</b> None</p>		
ldap.name_attr	String within 99 characters	Blank
<p><b>Description:</b> 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 spaces.</p> <p><b>Example:</b> ldap.name_attr = cn sn</p> <p>This requires the "cn" and "sn" attributes set for each contact record on the LDAP server.</p> <p><b>Web User Interface:</b> Directory-&gt;LDAP-&gt;LDAP Name Attributes</p> <p><b>Handset User Interface:</b> None</p>		
ldap.numb_attr	String within 99 characters	Blank
<p><b>Description:</b> 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 spaces.</p> <p><b>Example:</b> ldap.numb_attr = mobile ipPhone</p> <p>This requires the "mobile" and "ipPhone" attributes set for each contact record on the LDAP server.</p> <p><b>Web User Interface:</b></p>		

Parameters	Permitted Values	Default
Directory->LDAP->LDAP Number Attributes <b>Handset User Interface:</b> None		
<b>ldap.display_name</b>	String within 99 characters	Blank
<b>Description:</b> Configures the display name of the contact record displayed on the LCD screen. The value must start with “%” symbol. <b>Example:</b> ldap.display_name = %cn The cn of the contact record is displayed on the LCD screen. <b>Web User Interface:</b> Directory->LDAP->LDAP Display Name <b>Handset User Interface:</b> None		
<b>ldap.version</b>	2 or 3	3
<b>Description:</b> Configures the LDAP protocol version supported by the IP DECT phone. Make sure the protocol value corresponds with the version assigned on the LDAP server. <b>Web User Interface:</b> Directory->LDAP->Protocol <b>Handset User Interface:</b> None		
<b>ldap.call_in_lookup</b>	0 or 1	0
<b>Description:</b> Enables or disables the IP DECT phone to perform an LDAP search when receiving an incoming call. 0-Disabled 1-Enabled <b>Web User Interface:</b> Directory->LDAP->LDAP Lookup For Incoming Call <b>Handset User Interface:</b> None		

Parameters	Permitted Values	Default
<b>ldap.call_out_lookup</b>	<b>0 or 1</b>	<b>1</b>
<p><b>Description:</b> Enables or disables the IP DECT phone to perform an LDAP search when placing a call.</p> <p><b>0-Disabled</b> <b>1-Enabled</b></p> <p><b>Web User Interface:</b> Directory-&gt;LDAP-&gt;LDAP Lookup For Callout</p> <p><b>Handset User Interface:</b> None</p>		
<b>ldap.ldap_sort</b>	<b>0 or 1</b>	<b>0</b>
<p><b>Description:</b> Enables or disables the IP DECT phone to sort the search results in alphabetical order or numerical order.</p> <p><b>0-Disabled</b> <b>1-Enabled</b></p> <p><b>Web User Interface:</b> Directory-&gt;LDAP-&gt;LDAP Sorting Results</p> <p><b>Handset User Interface:</b> None</p>		
<b>ldap.incoming_call_special_search.enable</b>	<b>0 or 1</b>	<b>0</b>
<p><b>Description:</b> Enables or disables the IP DECT phone to search the telephone numbers starting with "+" symbol and "00" from the LDAP server if the incoming phone number starts with "+" or "00". When completing the LDAP search, the all search results will be displayed on the LCD screen.</p> <p><b>0-Disabled</b> <b>1-Enabled</b></p> <p>For example, If the phone receives an incoming call from the phone number 0044123456789, it will search 0044123456789 from the LDAP sever first, if no result found, it will search +44123456789 from the server again. The phone will display all the search results.</p> <p><b>Note:</b> It works only if the value of the parameter "ldap.call_in_lookup" is set to 1 (Enabled). You may need to set the value of the parameter "ldap.name_filter" to be</p>		

Parameters	Permitted Values	Default
( (cn=%)(sn=%)(telephoneNumber=%)(mobile=%)) for searching the telephone numbers starting with "+" symbol. <b>Web User Interface:</b> None <b>Handset User Interface:</b> None		

## Shared Call Appearance (SCA)

SCA allows users to share an extension which can be registered on two or more IP DECT phones at the same time. For more information on how to register accounts, refer to [Account Registration](#) on page 113.

Any IP DECT phone can be used to originate or receive calls on the shared line. An incoming call can be presented to multiple phones simultaneously. The incoming call can be answered on any IP DECT phone but not all. A call that is active on one IP DECT phone will be presented visually to other IP DECT phones that share the call appearance.

The IP DECT phones support SCA using a SUBSCRIBE/NOTIFY mechanism as specified in [RFC 3265](#). The events used are:

- "call-info" for call appearance state notification
- "line-seize" for the IP DECT phone to ask to seize the line

SCA allows users to barge in an active call.

If the call is placed on public hold, the held call is available for any shared line to retrieve. If the call is placed on private hold, the held call is only available for the hold party to retrieve.

### Procedure

SCA can be configured using the configuration files or locally.

<b>Configuration File</b>	<MAC>.cfg	Configure the registration line type. <b>Parameters:</b> account.X.shared_line
		Configure the barge in soft key. <b>Parameters:</b> features.display_sca_barge_in.enable



<p><b>Local</b></p>	<p>Web User Interface</p>	<p>Configure the registration line type.  <b>Navigate to:</b>  <a href="http://&lt;phoneIPAddress&gt;/servlet?p=account-adv&amp;q=load&amp;acc=0">http://&lt;phoneIPAddress&gt;/servlet?p=account-adv&amp;q=load&amp;acc=0</a></p>
---------------------	---------------------------	--

**Details of Configuration Parameters:**

Parameters	Permitted Values	Default
<p><b>account.X.shared_line</b> (X ranges from 1 to 5)</p>	<p>0 or 1</p>	<p>0</p>
<p><b>Description:</b>                      Enables or disables BroadSoft shared call appearance feature.                      0-Disabled                      1-Shared Call Appearance  <b>Web User Interface:</b>                      Account-&gt;Advanced-&gt;Shared Line  <b>Handset User Interface:</b>                      None</p>		
<p><b>features.display_sca_barge_in.enable</b></p>	<p>0 or 1</p>	<p>1</p>
<p><b>Description:</b>                      Enables or disables the barge in soft key to display during an SCA call.                      0-Disabled                      1-Enabled  <b>Web User Interface:</b>                      None  <b>Handset User Interface:</b>                      None</p>		

To configure the shared line feature via web user interface:

1. Click on **Account->Advanced**.
2. Select **Shared Call Appearance** form the pull-down list of **Shared Line** field.

The screenshot shows the Yealink W52P/W56P web user interface. The 'Account' tab is active, and the 'Advanced' sub-tab is selected. The 'Shared Line' field is highlighted with a red box, and its dropdown menu is open, showing 'Shared Call Appearance' selected. The interface includes a sidebar with navigation options like Register, Basic, Codec, Advanced, Number Assignment, and Handset Name. A 'NOTE' section on the right provides details about DTMF, Session Timer, Shared Call Appearance (SCA)/ Bridge Line Appearance (BLA), Network Conference, and VQ-RTCPXR.

3. Click **Confirm** 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. When receiving a new voice mail, the voice mail icon appears on the LCD screen. IP DECT phones support both solicited and unsolicited MWI.

### Unsolicited MWI

Unsolicited MWI is a server related feature. The IP DECT 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.

### Solicited MWI

For solicited MWI, you must enable MWI subscription feature on IP DECT phones. The IP DECT phones support subscribing the MWI messages to the account or the voice mail number.

## Procedure

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

<b>Configuration File</b>	<MAC>.cfg	Configure subscribe for MWI. <b>Parameters:</b> account.X.subscribe_mwi account.X.subscribe_mwi_expires
		Configure subscribe MWI to voice mail. <b>Parameters:</b> account.X.subscribe_mwi_to_vm
		Configure the voice mail number for account X. <b>Parameter:</b> voice_mail.number.X
<b>Local</b>	Web User Interface	Configure subscribe for MWI. Configure subscribe MWI to voice mail. Configure the voice mail number for account X. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0
	Handset User Interface	Configure the voice mail number for account X.

### Details of Configuration Parameters:

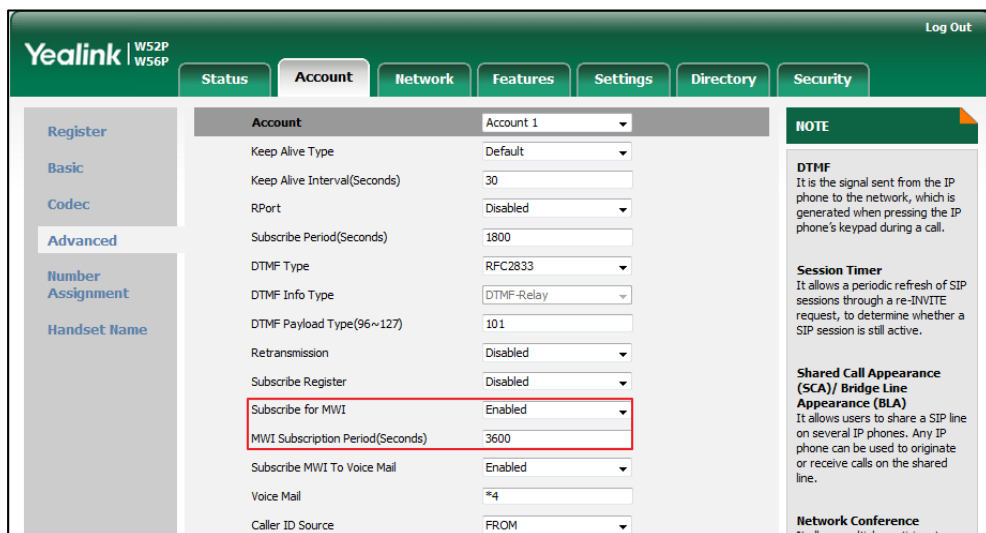
Parameters	Permitted Values	Default
<b>account.X.subscribe_mwi</b> (X ranges from 1 to 5)	<b>0 or 1</b>	<b>0</b>
<p><b>Description:</b></p> <p>Enables or disables the IP DECT phone to subscribe the message waiting indicator for account X.</p> <p><b>0</b>-Disabled <b>1</b>-Enabled</p> <p>If it is set to 1 (Enabled), the IP DECT phone will send a SUBSCRIBE message to the server for message-summary updates.</p>		

Parameters	Permitted Values	Default
<p>If it is set to 0 (Disabled), the server automatically sends a message-summary NOTIFY in a new dialog each time the MWI status changes. (This requires server support)</p> <p><b>Web User Interface:</b> Account-&gt;Advanced-&gt;Subscribe for MWI</p> <p><b>Handset User Interface:</b> None</p>		
<p><b>account.X.subscribe_mwi_expires</b> (X ranges from 1 to 5)</p>	<p>Integer from 0 to <b>84600</b></p>	<p><b>3600</b></p>
<p><b>Description:</b> Configures MWI subscribe expiry time (in seconds) for account X. The IP DECT phone is able to successfully refresh the SUBSCRIBE for message-summary events before expiration of the subscription dialog.</p> <p><b>Note:</b> It works only if the value of the parameter "account.X.subscribe_mwi" is set to 1 (Enabled).</p> <p><b>Web User Interface:</b> Account-&gt;Advanced-&gt;MWI Subscription Period (Seconds)</p> <p><b>Handset User Interface:</b> None</p>		
<p><b>account.X.subscribe_mwi_to_vm</b> (X ranges from 1 to 5)</p>	<p><b>0 or 1</b></p>	<p><b>0</b></p>
<p><b>Description:</b> Enables or disables the IP DECT phone to subscribe the message waiting indicator to the voice mail number for account X.</p> <p><b>0-Disabled</b> <b>1-Enabled</b></p> <p><b>Note:</b> It works only if the value of the parameters "account.X.subscribe_mwi" is set to 1 (Enabled) and "voice_mail.number.X" is configured.</p> <p><b>Web User Interface:</b> Account-&gt;Advanced-&gt;Subscribe MWI To Voice Mail</p> <p><b>Handset User Interface:</b> None</p>		
<p><b>voice_mail.number.X</b> (X ranges from 1 to 5)</p>	<p>String within 99 characters</p>	<p><b>Blank</b></p>
<p><b>Description:</b></p>		

Parameters	Permitted Values	Default
<p>Configures the voice mail number for account X.</p> <p><b>Example:</b></p> <p>voice_mail.number.1 = 1234</p> <p><b>Web User Interface:</b></p> <p>Account-&gt;Advanced-&gt;Voice Mail</p> <p><b>Handset User Interface:</b></p> <p>OK-&gt;Voice Mail-&gt;Set Voice Mail-&gt;LineX-&gt;Number</p>		

**To configure subscribe for MWI via web user interface:**

1. Click on **Account->Advanced**.
2. Select the desired account from the pull-down list of **Account**.
3. Select the desired value from the pull-down list of **Subscribe for MWI**.
4. Enter the period time in the **MWI Subscription Period(Seconds)** field.

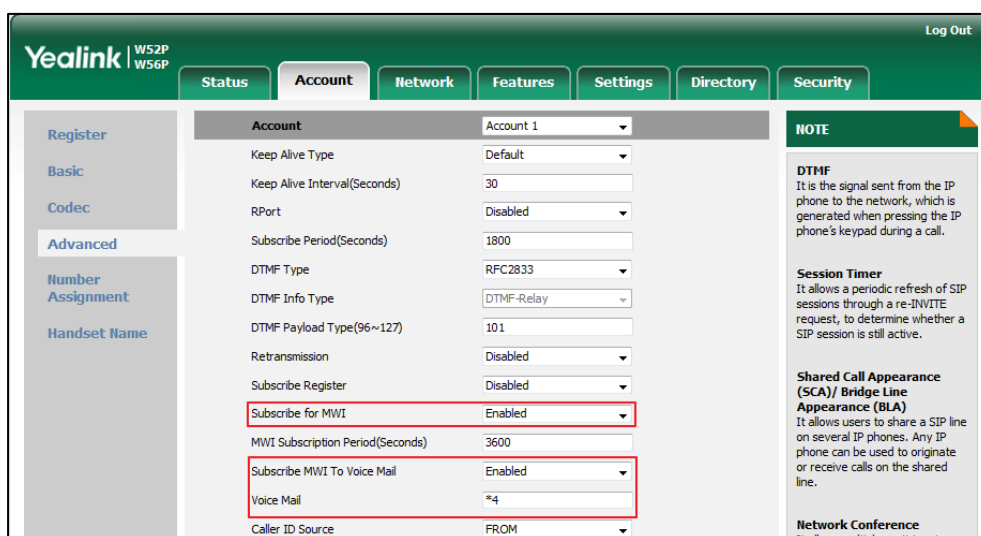


5. Click **Confirm** to accept the change.

**To configure subscribe MWI to voice mail via web user interface:**

1. Click on **Account->Advanced**.
2. Select the desired account from the pull-down list of **Account**.
3. Select **Enabled** from the pull-down list of **Subscribe for MWI**.
4. Select the desired value from the pull-down list of **Subscribe MWI To Voice Mail**.

5. Enter the desired voice number in the **Voice Mail** field.



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

## Server Redundancy

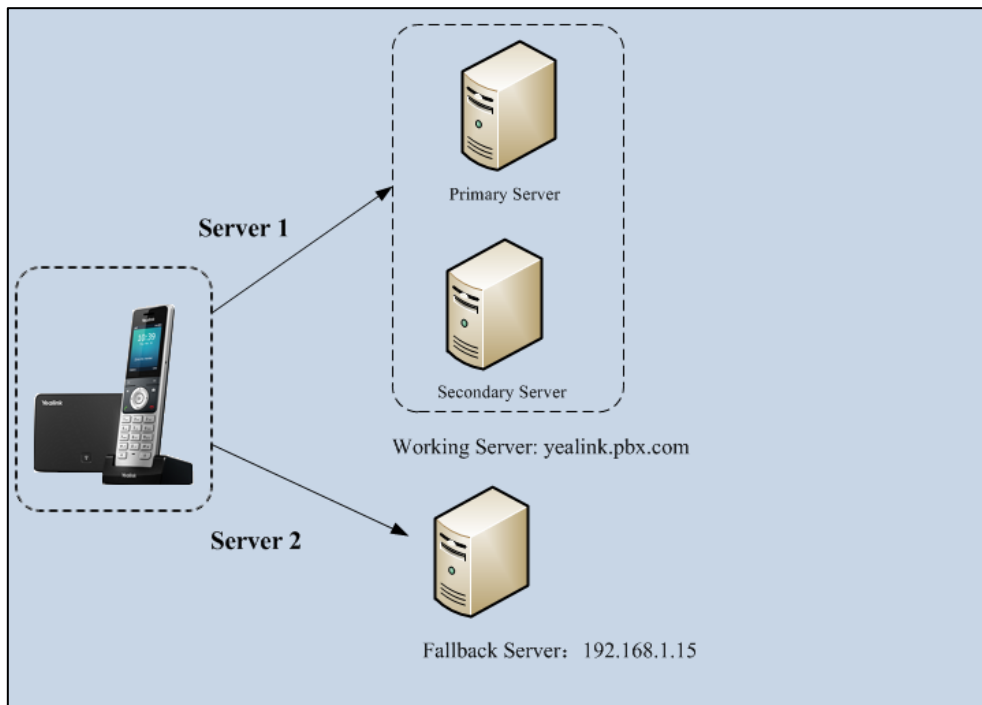
Server redundancy is often required in VoIP deployments to ensure continuity of phone service, for events where the server needs to be taken offline for maintenance, the server fails, or the connection between the IP DECT phone and the server fails.

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 mechanism from the primary to the secondary server.
- **Fallback:** In this mode, a second less featured call server with SIP capability takes over call control to provide basic calling capability, but without some advanced features (for example, shared line, call recording and MWI) offered by the working server. The IP DECT phones support configuration of two 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 DECT phone may be configured is shown as below. In the example, server redundancy for fallback and failover purposes is deployed. Two separate 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: yealink.pbx.com. DNS mechanism is used such that the working server is resolved to multiple servers for failover purpose. The working server is deployed in redundant pairs, designated as primary and secondary servers. The primary server has 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 IP address of the fallback server. For example, 192.168.1.15. A fallback server offers less functionality than the working server.

## Phone Registration

Registration method of the failover mode:

The IP DECT phone must always register to the primary server first except in failover conditions. If this is unsuccessful, the phone will re-register as many times as configured until the registration is successful. When the primary server registration is unavailable, the secondary server will serve as the working server.

Registration methods of the fallback mode include:

- **Concurrent registration (default):** The IP DECT 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 (for example, shared lines, call recording and MWI) offered by the working server. It is not applicable to outbound proxy servers.

- **Successiveregistration:** The IP DECT phone only registers to one server at a time. The IP DECT phone first registers to the working server. In a failure situation, the IP DECT phone registers to the fallback server.

For more information on server redundancy, refer to [Server Redundancy on Yealink IP phones](#).

## Procedure

Server redundancy can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	<p>Configure the SIP server redundancy.</p> <p><b>Parameters:</b></p> <p>account.X.sip_server.Y.address</p> <p>account.X.sip_server.Y.port</p> <p>account.X.sip_server.Y.expires</p> <p>account.X.sip_server.Y.retry_counts</p>
		<p>Configure the outbound proxy server redundancy.</p> <p><b>Parameters:</b></p> <p>account.X.outbound_proxy_enable</p> <p>account.X.outbound_host</p> <p>account.X.outbound_port</p>
		<p><b>Fallback Mode:</b></p> <p>account.X.fallback.redundancy_type</p> <p>account.X.fallback.timeout</p>
		<p><b>Failover Mode:</b></p> <p>account.X.sip_server.Y.failback_mode</p> <p>account.X.sip_server.Y.failback_timeout</p> <p>account.X.sip_server.Y.register_on_enable</p>
Local	Web User Interface	<p>Configure the server redundancy on the IP DECT phone.</p> <p><b>Navigate to:</b></p> <p>http://&lt;phoneIPAddress&gt;/servlet?p=account-register&amp;q=load&amp;acc=0</p>



**Details of Configuration Parameters:**

Parameters	Permitted Values	Default
<b>account.X.sip_server.Y.address</b> (X ranges from 1 to 5, Y ranges from 1 to 2)	<b>String within 256 characters</b>	<b>Blank</b>
<p><b>Description:</b> Configures the IP address or domain name of the SIP server Y for account X.</p> <p><b>Example:</b> account.1.sip_server.1.address = yealink.pbx.com</p> <p><b>Web User Interface:</b> Account-&gt;Register-&gt;SIP Server Y-&gt;Server Host</p> <p><b>Handset User Interface:</b> None</p>		
<b>account.X.sip_server.Y.port</b> (X ranges from 1 to 5, Y ranges from 1 to 2)	<b>Integer from 0 to 65535</b>	<b>5060</b>
<p><b>Description:</b> Configures the port of the SIP server Y for account X.</p> <p><b>Example:</b> account.1.sip_server.1.port = 5060</p> <p><b>Web User Interface:</b> Account-&gt;Register-&gt;SIP Server Y-&gt;Port</p> <p><b>Handset User Interface:</b> None</p>		
<b>account.X.sip_server.Y.expires</b> (X ranges from 1 to 5, Y ranges from 1 to 2)	<b>Integer from 30 to 2147483647</b>	<b>3600</b>
<p><b>Description:</b> Configures the registration expiration time (in seconds) of the SIP server Y for account X.</p> <p><b>Example:</b> account.1.sip_server.1.expires = 3600</p> <p><b>Web User Interface:</b> Account-&gt;Register-&gt;SIP Server Y-&gt;Server Expires</p> <p><b>Handset User Interface:</b> None</p>		
<b>account.X.sip_server.Y.retry_counts</b>	<b>Integer from 0 to 20</b>	<b>3</b>

Parameters	Permitted Values	Default
(X ranges from 1 to 5, Y ranges from 1 to 2)		
<p><b>Description:</b> Configures the retry times for the IP DECT phone to resend requests when the SIP server Y is unavailable or there is no response from the SIP server Y for account X.</p> <p><b>Web User Interface:</b> Account-&gt;Register-&gt;SIP Server Y-&gt;Server Retry Counts</p> <p><b>Handset User Interface:</b> None</p>		
<p><b>account.X.sip_server.Y.register_on_enable</b> (X ranges from 1 to 5, Y ranges from 1 to 2)</p>	<p><b>0 or 1</b></p>	<p><b>0</b></p>
<p><b>Description:</b> Enables or disables the IP DECT phone to send registration requests to the secondary server for account X when encountering a failover.</p> <p><b>0-Disabled</b> <b>1-Enabled</b></p> <p><b>Web User Interface:</b> None</p> <p><b>Handset User Interface:</b> None</p>		
<p><b>account.X.outbound_proxy_enable</b> (X ranges from 1 to 5)</p>	<p><b>0 or 1</b></p>	<p><b>0</b></p>
<p><b>Description:</b> Enables or disables the IP DECT phone to send requests to the outbound proxy server for account X.</p> <p><b>0-Disabled</b> <b>1-Enabled</b></p> <p><b>Web User Interface:</b> Account-&gt;Register-&gt;Enable Outbound Proxy Server</p> <p><b>Handset User Interface:</b> None</p>		
<p><b>account.X.outbound_host</b> (X ranges from 1 to 5)</p>	<p><b>IP address or domain name</b></p>	<p><b>Blank</b></p>
<p><b>Description:</b> Configures the IP address or domain name of the outbound proxy server 1 for</p>		

Parameters	Permitted Values	Default
account X. <b>Note:</b> It works only if the value of the parameter "account.X.outbound_proxy_enable" is set to 1 (Enabled). <b>Web User Interface:</b> Account->Register->Outbound Proxy Server 1 <b>Handset User Interface:</b> None		
<b>account.X.outbound_port</b> (X ranges from 1 to 5)	<b>Integer from 0 to 65535</b>	<b>5060</b>
<b>Description:</b> Configures the port of the outbound proxy server 1 for account X. <b>Example:</b> account.1.outbound_port = 5060 <b>Note:</b> It works only if the value of the parameter "account.X.outbound_proxy_enable" is set to 1 (Enabled). <b>Web User Interface:</b> Account->Register->Outbound Proxy Server 1->Port <b>Handset User Interface:</b> None		
<b>account.X.backup_outbound_host</b> (X ranges from 1 to 5)	<b>IP address or domain name</b>	<b>Blank</b>
<b>Description:</b> Configures the IP address or domain name of the outbound proxy server 2 for account X. <b>Note:</b> It works only if the value of the parameter "account.X.outbound_proxy_enable" is set to 1 (Enabled). <b>Web User Interface:</b> Account->Register->Outbound Proxy Server 2 <b>Handset User Interface:</b> None		
<b>account.X.backup_outbound_port</b> (X ranges from 1 to 5)	<b>Integer from 0 to 65535</b>	<b>5060</b>
<b>Description:</b> Configures the port of the outbound proxy server 2 for account X.		

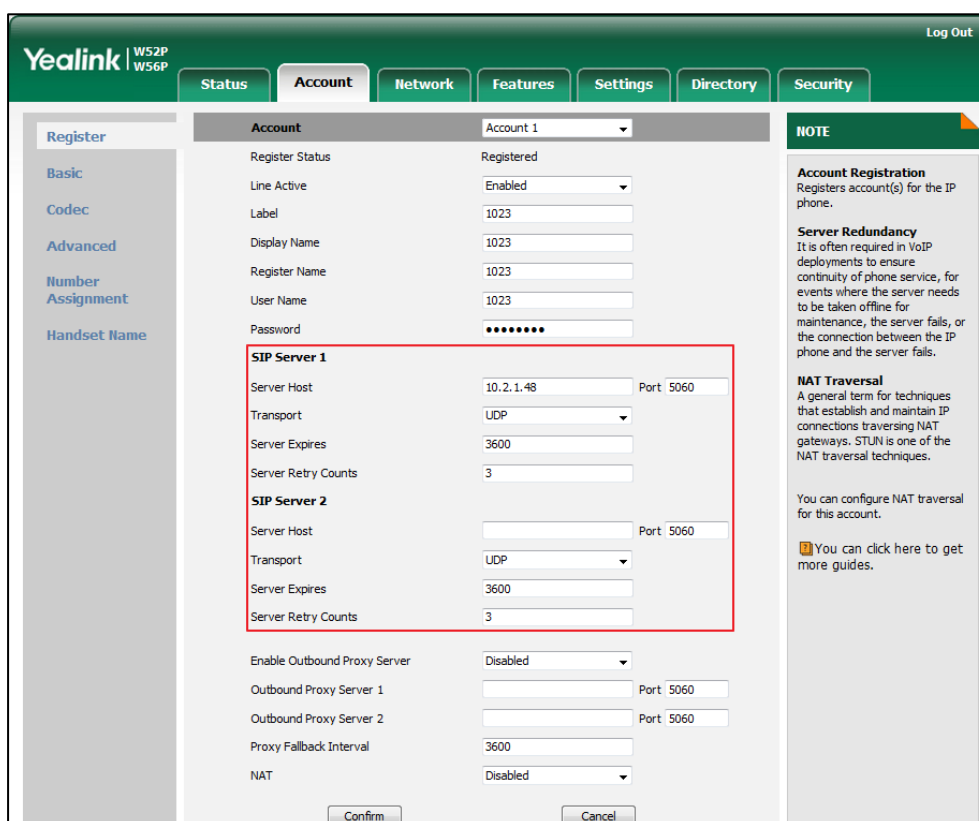
Parameters	Permitted Values	Default
<p><b>Example:</b>  account.1.backup_outbound_port = 5060</p> <p><b>Note:</b> It works only if the value of the parameter "account.X.outbound_proxy_enable" is set to 1 (Enabled).</p> <p><b>Web User Interface:</b>  Account-&gt;Register-&gt;Outbound Proxy Server 2-&gt;Port</p> <p><b>Handset User Interface:</b>  None</p>		
<p><b>account.X.fallback.redundancy_type</b>  (X ranges from 1 to 5)</p>	<p>0 or 1</p>	<p>0</p>
<p><b>Description:</b>  Configures the registration mode for the IP DECT phone in fallback mode.</p> <p>0-Concurrent Registration  1-Successive Registration</p> <p><b>Note:</b> It is not applicable to outbound proxy servers.</p> <p><b>Web User Interface:</b>  None</p> <p><b>Handset User Interface:</b>  None</p>		
<p><b>account.X.fallback.timeout</b>  (X ranges from 1 to 5)</p>	<p>Integer from 10 to  2147483647</p>	<p>120</p>
<p><b>Description:</b>  Configures the time interval (in seconds) for the IP DECT phone to detect whether the working server is available by sending the registration request for account X after the fallback server takes over call control.</p> <p><b>Note:</b> It works only if the value of the parameter "account.X.fallback.redundancy_type" is set to 1 (Successive registration).</p> <p><b>Web User Interface:</b>  None</p> <p><b>Handset User Interface:</b>  None</p>		
<p><b>account.X.outbound_proxy_fallback_interval</b>  (X ranges from 1 to 5, Y ranges from 1 to 2)</p>	<p>Integer from 0 to  65535</p>	<p>3600</p>
<p><b>Description:</b></p>		

Parameters	Permitted Values	Default
<p>Configures the time interval (in seconds) for the IP DECT phone to detect whether the working outbound proxy server is available by sending the registration request after the fallback server takes over call control.</p> <p><b>Example:</b></p> <p>account.1.outbound_proxy_fallback_interval = 3600</p> <p><b>Note:</b> It is only applicable to outbound proxy servers.</p> <p><b>Web User Interface:</b></p> <p>Account-&gt;Register-&gt;Proxy Fallback Interval</p> <p><b>Handset User Interface:</b></p> <p>None</p>		
<p><b>account.X.sip_server.Y.fallback_mode</b> (X ranges from 1 to 5, Y ranges from 1 to 2)</p>	<p><b>0, 1, 2 or 3</b></p>	<p><b>0</b></p>
<p><b>Description:</b></p> <p>Configures the mode for the IP DECT phone to retry the primary server in failover for account X.</p> <p><b>0-newRequests:</b> all requests are sent to the primary server first, regardless of the last server that was used.</p> <p><b>1-DNSTTL:</b> the IP DECT phone will send requests to the last registered server first. If the time defined by DNSTTL on the registered server expires, the phone will retry to send requests to the primary server.</p> <p><b>2-Registration:</b> the IP DECT phone will send requests to the last registered server first. If the registration expires, the phone will retry to send requests to the primary server.</p> <p><b>3-duration:</b> the IP DECT phone will send requests to the last registered server first. If the time defined by the “account.X.sip_server.Y.fallback_timeout” parameter expires, the phone will retry to send requests to the primary server.</p> <p><b>Web User Interface:</b></p> <p>None</p> <p><b>Handset User Interface:</b></p> <p>None</p>		
<p><b>account.X.sip_server.Y.fallback_timeout</b> (X ranges from 1 to 16, Y ranges from 1 to 2)</p>	<p><b>0, Integer from 60 to 65535</b></p>	<p><b>3600</b></p>
<p><b>Description:</b></p> <p>Configures the time (in seconds) for the phone to retry to send requests to the primary server after failing over to the current working server for account X.</p> <p>If you set the parameter to 0, the IP DECT phone will not send requests to the primary server until a failover event occurs with the current working server.</p>		

Parameters	Permitted Values	Default
<p>If you set the parameter between 1 and 59, the timeout will be 60 seconds.</p> <p><b>Note:</b> It works only if the value of the parameter "account.X.sip_server.Y.failback_mode" is set to 3 (duration).</p> <p><b>Web User Interface:</b></p> <p>None</p> <p><b>Handset User Interface:</b></p> <p>None</p>		

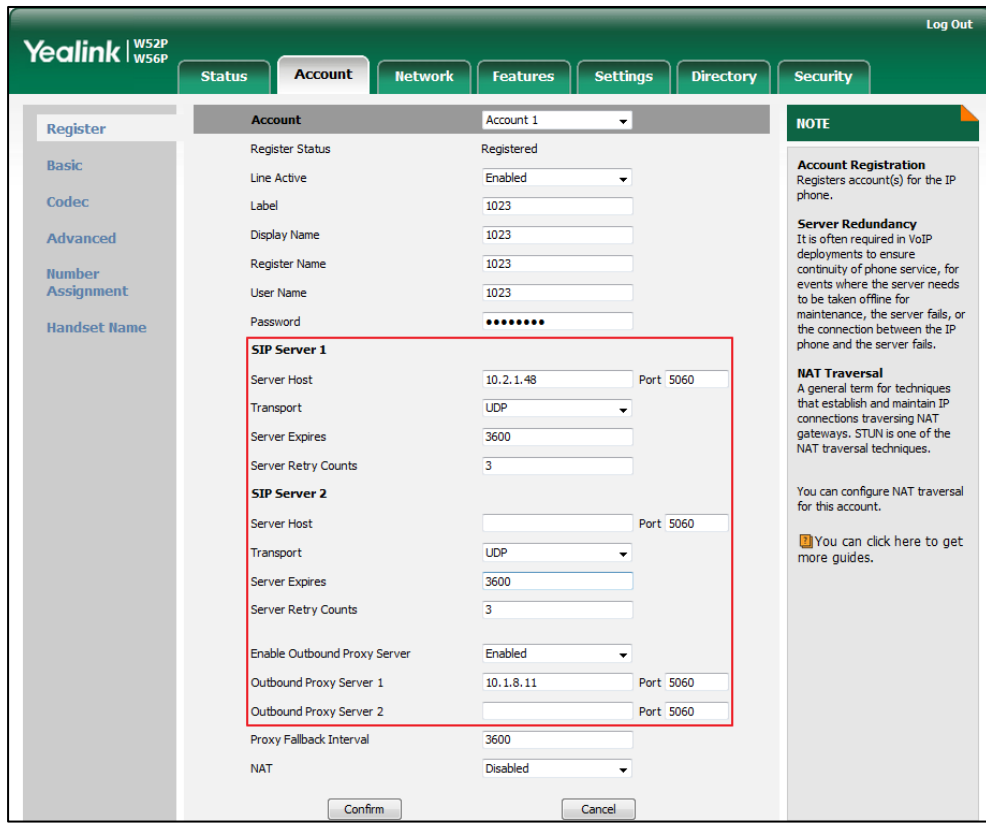
To configure server redundancy for fallback purpose via web user interface:

1. Click on **Account->Register**.
2. Select the desired account from the pull-down list of **Account**.
3. Configure registration parameters of the selected account in the corresponding fields.
4. Configure parameters of SIP server 1 and SIP server 2 in the corresponding fields.



5. If you use outbound proxy servers, do the following:
  - 1) Select **Enabled** from the pull-down list of **Enable Outbound Proxy Server**.

- 2) Configure parameters of outbound proxy server 1 and outbound proxy server 2 in the corresponding fields.



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

**To configure server redundancy for failover purpose via web user interface:**

1. Click on **Account->Register**.
2. Select the desired account from the pull-down list of **Account**.
3. Configure registration parameters of the selected account in the corresponding fields.
4. Configure parameters of the SIP server 1 or SIP server 2 in the corresponding fields.  
You must set the port of SIP server to 0 for NAPTR, SRV and A queries.

5. Select **DNS-NAPTR** from the pull-down list of **Transport**.

The screenshot shows the Yealink W52P/W56P web interface. The 'Account' tab is selected, and the 'Account 1' configuration page is displayed. The 'SIP Server 1' section is highlighted with a red box, showing the following fields:

Field	Value
Server Host	10.2.1.48
Port	5060
Transport	UDP
Server Expires	3600
Server Retry Counts	3

The 'SIP Server 2' section is also visible below it, with the following fields:

Field	Value
Server Host	
Port	5060
Transport	UDP
Server Expires	3600
Server Retry Counts	3

Other fields in the 'SIP Server 1' section include: Register Status (Registered), Line Active (Enabled), Label (1023), Display Name (1023), Register Name (1023), User Name (1023), and Password (masked with dots).

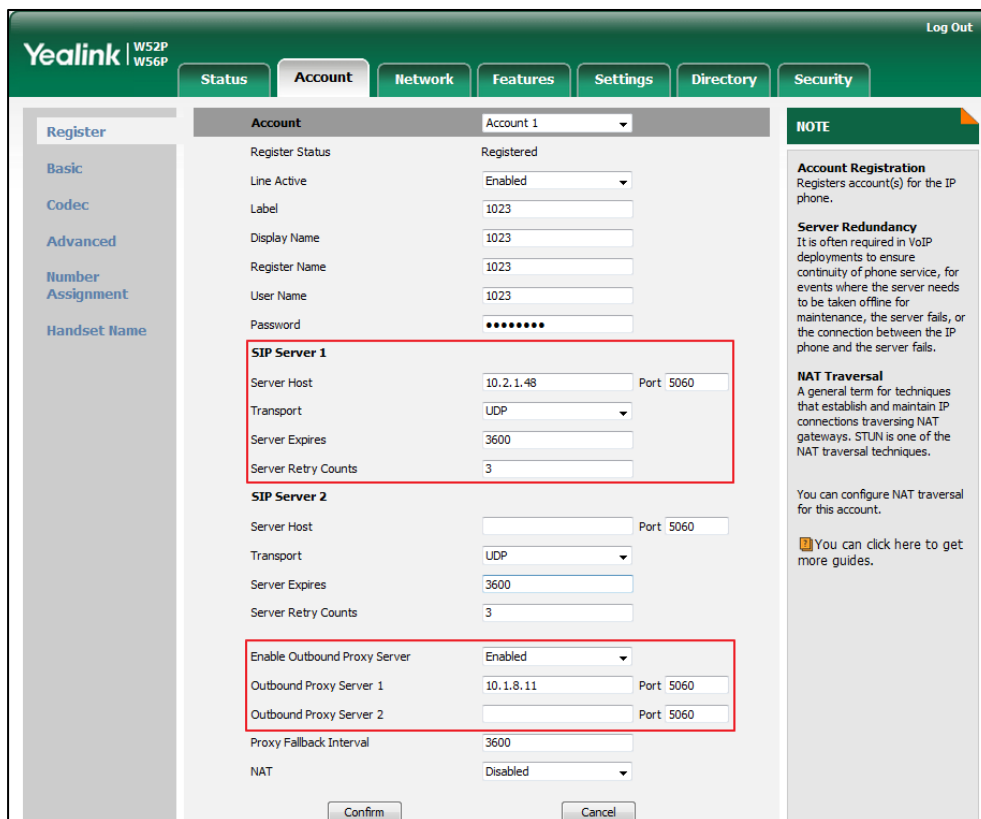
The 'SIP Server 2' section includes: Enable Outbound Proxy Server (Enabled), Outbound Proxy Server 1 (10.1.8.11), Outbound Proxy Server 2 (empty), Proxy Fallback Interval (3600), and NAT (Disabled).

Buttons for 'Confirm' and 'Cancel' are located at the bottom of the form.

6. If you use outbound proxy servers, do the following:
  - 1) Select **Enabled** from the pull-down list of **Enable Outbound Proxy Server**.
  - 2) Configure parameters of outbound proxy server 1/2 in the corresponding fields.



You must set the port of outbound proxy server to 0 for NAPTR, SRV and A queries.



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

## Server Domain Name Resolution

If a domain name is configured for a server, the IP address(es) associated with that domain name will be resolved through DNS as specified by RFC 3263. The DNS query involves NAPTR, SRV and A queries, which allows the IP DECT phone to adapt to various deployment environments. The IP DECT phone performs NAPTR query for the NAPTR pointer and transport protocol (UDP, TCP and TLS), the SRV query on the record returned from the NAPTR for the target domain name and the port number, and the A query for the IP addresses.

If an explicit port (except 0) is specified, a query will be performed only. If a server port is set to 0 and the transport type is set to DNS-NAPTR, NAPTR and SRV queries will be tried before falling to A query. If no port is found through the DNS query, 5060 will be used.

The following details the procedures of DNS query for the IP DECT phone to resolve the domain name (e.g., yealink.pbx.com) of working server into the IP address, port and transport protocol.

### NAPTR (Naming Authority Pointer)

First, the IP DECT phone sends NAPTR query to get the NAPTR pointer and transport protocol. Example of NAPTR records:

	order	pref	flags	service	regexp	replacement
IN NAPTR	90	50	"s"	"SIP+D2T"	""	_sip._tcp.yealink.pbx.com
IN NAPTR	100	50	"s"	"SIP+D2U"	""	_sip._udp.yealink.pbx.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: 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 DECT 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.yealink.pbx.com". If the flag of the NAPTR record returned is empty, the IP DECT phone will perform NAPTR query again according to the previous NAPTR query result.

### SRV (Service Location Record)

The IP DECT phone performs an 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.yealink.pbx.com
IN SRV	0	2	5060	server2.yealink.pbx.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 DECT phone uses this port. If the Target is not a numeric IP address, the IP DECT phone performs an A query. So in this case, the IP DECT phone uses "server1.yealink.pbx.com" and "server2.yealink.pbx.com" for the A query.

#### A (Host IP Address)

The IP DECT phone performs an A query for the IP address of each target host name.

Example of A records:

```
Server1.yealink.pbx.com IN A 192.168.1.13
```

```
Server2.yealink.pbx.com IN A 192.168.1.14
```

The IP DECT phone picks the IP address "192.168.1.14" first.

### Outgoing Call When the Working Server Connection Fails

When a user initiates a call, the IP DECT 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 DECT 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.

<b>Configuration File</b>	<MAC>.cfg	Configure the transport type on the IP DECT phone. <b>Parameters:</b> account.X.sip_server.Y.transport_type account.X.naptr_build
<b>Local</b>	Web User Interface	Configure the transport type on the IP DECT phone. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=account-register&q=load&acc=0

### Details of Configuration Parameters:

Parameters	Permitted Values	Default
<b>account.X.sip_server.Y.transport_type</b> (X ranges from 1 to 5, Y ranges from 1 to 2)	<b>0, 1, 2 or 3</b>	<b>0</b>
<p><b>Description:</b> Configures the type of transport protocol for account X.</p> <p><b>0-UDP</b> <b>1-TCP</b> <b>2-TLS</b> <b>3-DNS-NAPTR</b></p> <p>If the value of the parameter is set to 3 (DNS-NAPTR) and no server port is given, the IP DECT phone performs the DNS NAPTR and SRV queries for the service type and port.</p> <p><b>Web User Interface:</b> Account-&gt;Register-&gt;SIP Server Y-&gt;Transport</p> <p><b>Handset User Interface:</b> None</p>		
<b>account.X.naptr_build</b>	<b>0 or 1</b>	<b>0</b>

Parameters	Permitted Values	Default
(X ranges from 1 to 5)		
<p><b>Description:</b> Configures the way of SRV query for the IP DECT phone to be performed when no result is returned from NAPTR query for account X.</p> <p><b>0</b>-SRV query using UDP only <b>1</b>-SRV query using UDP, TCP and TLS</p> <p><b>Web User Interface:</b> None</p> <p><b>Handset User Interface:</b> None</p>		

## Static DNS Cache

Failover redundancy can only be utilized when the configured domain name of the server is resolved to multiple IP addresses. If the IP DECT phone is not configured with a DNS server, or the DNS query returns no result from a DNS server, you can configure a set of DNS NAPTR/SRV/A records into the IP DECT phone. The IP DECT phone will attempt to resolve the domain name of the SIP server with static DNS cache.

When the IP DECT phone is configured with a DNS server, the IP DECT phone will behave as follows to resolve domain name of the server:

- The IP DECT phone performs a DNS query to resolve the domain name from the DNS server.
- If the DNS query returns no results for the domain name, or the returned record cannot be contacted, the values in the static DNS cache (if configured) are used when their configured time intervals are not elapsed.
- If the configured time interval is elapsed, the IP DECT phone will attempt to perform a DNS query again.
- If the DNS query returns a result, the IP DECT phone will use the returned record and ignore the statically configured cache values.

When the IP DECT phone is not configured with a DNS server, it will behave as follow:

- The IP DECT phone attempts to resolve the domain name within the static DNS cache.
- The IP DECT phone will always use the results returned from the static DNS cache.

The IP DECT phones can be configured to use static DNS cache preferentially. Static DNS cache is configurable on a per-line basis.

## Procedure

Static DNS cache can be configured only using the configuration files.

<b>Configuration File</b>	y00000000025.cfg	<p>Configure NAPTR/SRV/A records.</p> <p><b>Parameters:</b></p> <p>dns_cache_naptr.X.name          dns_cache_naptr.X.flags          dns_cache_naptr.X.order          dns_cache_naptr.X.preference          dns_cache_naptr.X.replace          dns_cache_naptr.X.service          dns_cache_naptr.X.ttl          dns_cache_srv.X.name          dns_cache_srv.X.port          dns_cache_srv.X.priority          dns_cache_srv.X.target          dns_cache_srv.X.weight          dns_cache_srv.X.ttl          dns_cache_a.X.name          dns_cache_a.X.ip          dns_cache_a.X.ttl</p>
	<MAC>.cfg	<p>Configure the IP DECT phone whether to cache the additional DNS records.</p> <p><b>Parameter:</b></p> <p>account.X.dns_cache_type</p>
		<p>Configure the IP DECT phone whether to use static DNS cache preferentially.</p> <p><b>Parameter:</b></p> <p>account.X.static_cache_pri</p>

## Details of Configuration Parameters:

Parameters	Permitted Values	Default
<b>dns_cache_naptr.X.name</b> (X ranges from 1 to 12)	<b>Domain name</b>	<b>Blank</b>
<p><b>Description:</b> Configures the domain name to which NAPTR record X refers.</p> <p><b>Example:</b> dns_cache_naptr.1.name = yealink.pbx.com</p> <p><b>Web User Interface:</b> None</p> <p><b>Handset User Interface:</b> None</p>		
<b>dns_cache_naptr.X.flags</b> (X ranges from 1 to 12)	<b>S, A, U or P</b>	<b>Blank</b>
<p><b>Description:</b> Configures the flag of NAPTR record X (Always "S" for SIP, which means to do an SRV lookup on whatever is in the replacement field).</p> <p><b>S</b>-Do an SRV lookup next <b>A</b>-Do an A lookup next <b>U</b>-No need to do a DNS query next <b>P</b>-Service custom by the user</p> <p><b>Example:</b> dns_cache_naptr.1.flags = S</p> <p><b>Web User Interface:</b> None</p> <p><b>Handset User Interface:</b> None</p>		
<b>dns_cache_naptr.X.order</b> (X ranges from 1 to 12)	<b>Integer from 0 to 65535</b>	<b>0</b>
<p><b>Description:</b> Configures the order of NAPTR record X. NAPTR record with lower order is more preferred.</p> <p><b>Example:</b> dns_cache_naptr.1.order = 90</p> <p><b>Web User Interface:</b></p>		

Parameters	Permitted Values	Default
<p>None</p> <p><b>Handset User Interface:</b></p> <p>None</p>		
<p><b>dns_cache_naptr.X.preference</b> (X ranges from 1 to 12)</p>	<p>Integer from 0 to 65535</p>	<p>0</p>
<p><b>Description:</b></p> <p>Configures the preference of NAPTR record X. NAPTR record with lower preference is more preferred.</p> <p><b>Example:</b></p> <p>dns_cache_naptr.1.preference = 50</p> <p><b>Web User Interface:</b></p> <p>None</p> <p><b>Handset User Interface:</b></p> <p>None</p>		
<p><b>dns_cache_naptr.X.replace</b> (X ranges from 1 to 12)</p>	<p>Domain name</p>	<p>Blank</p>
<p><b>Description:</b></p> <p>Configures a domain name to be used for the next SRV query in NAPTR record X.</p> <p><b>Example:</b></p> <p>dns_cache_naptr.1.replace = _sip._tcp.yealink.pbx.com</p> <p><b>Web User Interface:</b></p> <p>None</p> <p><b>Handset User Interface:</b></p> <p>None</p>		
<p><b>dns_cache_naptr.X.service</b> (X ranges from 1 to 12)</p>	<p>String within 32 characters</p>	<p>Blank</p>
<p><b>Description:</b></p> <p>Configures the transport protocol available for the server in NAPTR record X.</p> <p><b>SIP+D2U:</b> SIP over UDP</p> <p><b>SIP+D2T:</b> SIP over TCP</p> <p><b>SIP+D2S:</b> SIP over SCTP</p> <p><b>SIPS+D2T:</b> SIPS over TCP</p> <p><b>Example:</b></p> <p>dns_cache_naptr.1.service = SIP+D2T</p>		



Parameters	Permitted Values	Default
<b>Web User Interface:</b> None <b>Handset User Interface:</b> None		
<b>dns_cache_naptr.X.ttl</b> (X ranges from 1 to 12)	<b>Integer from 30 to 2147483647</b>	<b>300</b>
<b>Description:</b> Configures the time interval (in seconds) that NAPTR record X may be cached before the record should be consulted again. <b>Example:</b> dns_cache_naptr.1.ttl = 3600 <b>Web User Interface:</b> None <b>Handset User Interface:</b> None		
<b>dns_cache_srv.X.name</b> (X ranges from 1 to 12)	<b>Domain name</b>	<b>Blank</b>
<b>Description:</b> Configures the domain name in SRV record X. <b>Example:</b> dns_cache_srv.1.name = _sip._tcp.yealink.pbx.com <b>Web User Interface:</b> None <b>Handset User Interface:</b> None		
<b>dns_cache_srv.X.port</b> (X ranges from 1 to 12)	<b>Integer from 0 to 65535</b>	<b>0</b>
<b>Description:</b> Configures the port to be used in SRV record X. <b>Example:</b> dns_cache_srv.1.port = 5060 <b>Web User Interface:</b> None <b>Handset User Interface:</b>		

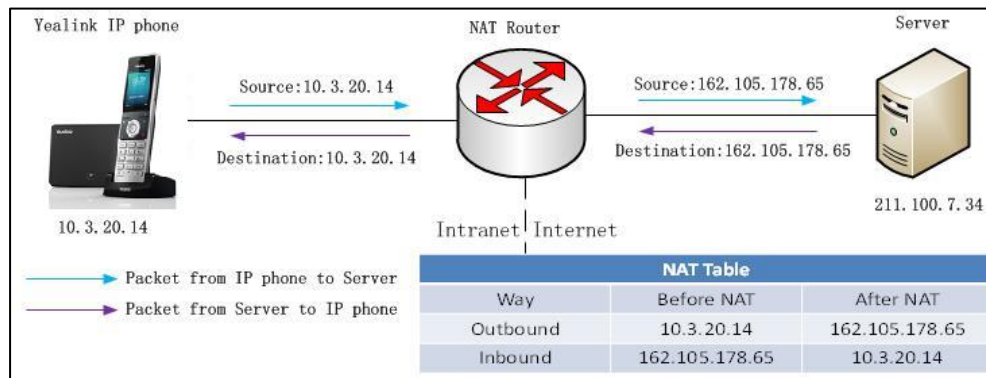
Parameters	Permitted Values	Default
None		
<b>dns_cache_srv.X.priority</b> (X ranges from 1 to 12)	Integer from 0 to 65535	0
<b>Description:</b> Configures the priority for the target host in SRV record X. Lower priority is more preferred. <b>Web User Interface:</b> None <b>Handset User Interface:</b> None		
<b>dns_cache_srv.X.target</b> (X ranges from 1 to 12)	Domain name	Blank
<b>Description:</b> Configures the domain name of the target host for an A query in SRV record X. <b>Example:</b> dns_cache_srv.1.target = server1.yealink.pbx.com <b>Web User Interface:</b> None <b>Handset User Interface:</b> None		
<b>dns_cache_srv.X.weight</b> (X ranges from 1 to 12)	Integer from 0 to 65535	0
<b>Description:</b> Configures the weight of the target host in SRV record X. When priorities are equal, weight is used to differentiate the preference. Higher weight is more preferred. <b>Example:</b> dns_cache_srv.1.weight = 1 <b>Web User Interface:</b> None <b>Handset User Interface:</b> None		
<b>dns_cache_srv.X.ttl</b> (X ranges from 1 to 12)	Integer from 30 to 2147483647	300

Parameters	Permitted Values	Default
<p><b>Description:</b> Configures the time interval (in seconds) that SRV record X may be cached before the record should be consulted again.</p> <p><b>Example:</b> dns_cache_srv.1.ttl = 3600</p> <p><b>Web User Interface:</b> None</p> <p><b>Handset User Interface:</b> None</p>		
<p><b>dns_cache_a.X.name</b> (X ranges from 1 to 12)</p>	<p><b>Domain name</b></p>	<p><b>Blank</b></p>
<p><b>Description:</b> Configures the domain name in A record X.</p> <p><b>Example:</b> dns_cache_a.1.name = yealink.pbx.com</p> <p><b>Web User Interface:</b> None</p> <p><b>Handset User Interface:</b> None</p>		
<p><b>dns_cache_a.X.ip</b> (X ranges from 1 to 12)</p>	<p><b>IP address</b></p>	<p><b>Blank</b></p>
<p><b>Description:</b> Configures the IP address that the domain name in A record X maps to.</p> <p><b>Example:</b> dns_cache_a.1.ip = 192.168.1.13</p> <p><b>Web User Interface:</b> None</p> <p><b>Handset User Interface:</b> None</p>		
<p><b>dns_cache_a.X.ttl</b> (X ranges from 1 to 12)</p>	<p><b>Integer from 30 to 2147483647</b></p>	<p><b>300</b></p>
<p><b>Description:</b> Configures the time interval (in seconds) that A record X may be cached before the record should be consulted again.</p>		

Parameters	Permitted Values	Default
<p><b>Example:</b> dns_cache_a.1.ttl = 3600</p> <p><b>Web User Interface:</b> None</p> <p><b>Handset User Interface:</b> None</p>		
<p><b>account.X.dns_cache_type</b> (X ranges from 1 to 5)</p>	<p><b>0, 1 or 2</b></p>	<p><b>1</b></p>
<p><b>Description:</b> Configures whether the IP DECT phone uses the DNS cache for domain name resolution of the server and caches the additional DNS records for account X.</p> <p><b>0</b>-Perform real-time DNS query rather than using DNS cache. <b>1</b>-Use DNS cache, but do not cache the additional DNS records. <b>2</b>-Use DNS cache and cache the additional DNS records.</p> <p><b>Example:</b> account.1.dns_cache_type = 1</p> <p><b>Web User Interface:</b> None</p> <p><b>Handset User Interface:</b> None</p>		
<p><b>account.X.static_cache_pri</b></p>	<p><b>0 or 1</b></p>	<p><b>0</b></p>
<p><b>Description:</b> Configures whether preferentially to use the static DNS cache for domain name resolution of the server for account X.</p> <p><b>0</b>-Use domain name resolution from the DNS server preferentially <b>1</b>-Use static DNS cache preferentially</p> <p><b>Example:</b> account.1.static_cache_pri = 1</p> <p><b>Web User Interface:</b> None</p> <p><b>Handset User Interface:</b> None</p>		

## 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. NAT ensures security since each outgoing or incoming request must first go through a translation process.



## NAT Types

### Symmetrical NAT

In symmetrical NAT, the NAT router stores the address and port where the packet was sent. Only packets coming from this address and port are forwarded back to the private address.

### Full Cone NAT

In full cone NAT, all packets from a private address (e.g., iAddr: port1) to public network will be sent through a public address (e.g., eAddr: port2). Packets coming from the address of any server to eAddr: port2 will be forwarded back to the private address (e.g., iAddr: port1).

### Address Restricted Cone NAT

Restricted cone NAT works similar like full cone NAT. A public host (hAddr:any) can send packets to iAddr: port1 through eAddr: port2 only if iAddr: port1 has previously sent a packet to hAddr: any. "Any" means the port number doesn't matter.

### Port Restricted Cone NAT

Port restricted cone NAT works similar like full cone NAT. A public host (hAddr:hPort) can send packets to iAddr: port1 through eAddr: port2 only if iAddr: port1 has previously sent a packet to hAddr: hPort.

## NAT Traversal

In the VoIP environment, NAT breaks end-to-end connectivity.

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 DECT 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 DECT phone can be configured to act as a STUN client, to send 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.

### SIP Ports for NAT Traversal

You can configure the SIP ports on the IP DECT phone. Previously, the IP DECT phone used default values (5060 for UDP/TCP). In the configuration files, you can use the following parameters to configure the SIP and TLS source ports:

- Local SIP Port
- TLS SIP Port

If NAT is disabled, the port number shows in the Via and Contact SIP headers of SIP messages. If NAT is enabled, the phone uses the NAT port number (and NAT IP address) in the Via and Contact SIP headers of SIP messages, but still use the configured source port.

### Procedure

NAT traversal and STUN server can be configured using the configuration files or locally.

<p><b>Configuration File</b></p>	<p>y000000000025.cfg</p>	<p>Configure NAT traversal and STUN server on a phone basis.</p> <p><b>Parameters:</b></p> <p>sip.nat_stun.enable</p> <p>sip.nat_stun.server</p> <p>sip.nat_stun.port</p>
----------------------------------	--------------------------	---

		<p>Configure local SIP port and TLS SIP port.</p> <p><b>Parameters:</b></p> <p>sip.listen_port</p> <p>sip.tls_listen_port</p>
	<MAC>.cfg	<p>Configure NAT traversal on a per-line basis.</p> <p><b>Parameters:</b></p> <p>account.X.nat.nat_traversal</p>
Local	Web User Interface	<p>Configure NAT traversal and STUN server on a phone basis.</p> <p><b>Navigate to:</b></p> <p>http://&lt;phoneIPAddress&gt;/servlet?p=network-adv&amp;q=load</p>
		<p>Configure local SIP port and TLS SIP port.</p> <p><b>Navigate to:</b></p> <p>http://&lt;phoneIPAddress&gt;/servlet?p=account-adv&amp;q=load&amp;acc=0</p>
		<p>Configure NAT traversal on a per-line basis.</p> <p><b>Navigate to:</b></p> <p>http://&lt;phoneIPAddress&gt;/servlet?p=account-register&amp;q=load&amp;acc=0</p>

**Details of Configuration Parameters:**

Parameters	Permitted Values	Default
sip.nat_stun.enable	0 or 1	0
<p><b>Description:</b></p> <p>Enables or disables the STUN (Simple Traversal of UDP over NATs) feature on the IP DECT phone.</p> <p><b>0</b>-Disabled</p> <p><b>1</b>-Enabled</p> <p><b>Note:</b> If you change this parameter, the base station will reboot to make the change</p>		

Parameters	Permitted Values	Default
take effect. <b>Web User Interface:</b> Network->Advanced->NAT->Active <b>Handset User Interface:</b> None		
sip.nat_stun.server	IP address or domain name	Blank
<b>Description:</b> Configures the IP address or the domain name of the STUN (Simple Traversal of UDP over NATs) server. <b>Example:</b> sip.nat_stun.server = 218.107.220.201 <b>Note:</b> If you change this parameter, the base station will reboot to make the change take effect. <b>Web User Interface:</b> Network->Advanced->NAT->STUN Server <b>Handset User Interface:</b> None		
sip.nat_stun.port	Integer from 1024 to 65000	3478
<b>Description:</b> Configures the port of the STUN (Simple Traversal of UDP over NATs) server. <b>Example:</b> sip.nat_stun.port= 3478 <b>Note:</b> If you change this parameter, the base station will reboot to make the change take effect. <b>Web User Interface:</b> Network->Advanced->NAT->STUN Port(1024~65000) <b>Handset User Interface:</b> None		
account.X.nat.nat_traversal (X ranges from 1 to 5)	0 or 1	0
<b>Description:</b> Enables or disables the NAT traversal for account X. 0-Disabled		



Parameters	Permitted Values	Default
<b>1-STUN</b> <b>Web User Interface:</b> Account->Register->NAT <b>Handset User Interface:</b> None		
<b>sip.listen_port</b>	<b>Integer from 1024 to 65535</b>	<b>5060</b>
<b>Description:</b> Configures the local SIP port. <b>Web User Interface:</b> Settings->SIP->Local SIP Port <b>Handset User Interface:</b> None		
<b>sip.tls_listen_port</b>	<b>Integer from 1024 to 65535</b>	<b>5061</b>
<b>Description:</b> Configures the local TLS listen port. <b>Web User Interface:</b> Settings->SIP->TLS SIP Port <b>Handset User Interface:</b> None		

To configure NAT traversal and STUN server via web user interface:

1. Click on **Network->Advanced**.
2. In the **NAT** block, select the desired value from the pull-down list of **Active**.
3. Enter the IP address or the domain name of the STUN server in the **STUN Server** field.

- Enter the port of the STUN server in the **STUN Port(1024-65000)** field.

The screenshot shows the Yealink W52P/W56P web interface. The 'Network' tab is selected. The 'NAT' section is highlighted with a red box, showing the following settings:

Active	Disabled
STUN Server	
STUN Port(1024~65000)	3478

The 'NOTE' section on the right contains the following information:

**VLAN**  
It 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.

The priority of VLAN assignment method (from highest to lowest): LLDP/CDP->manual configuration->DHCP VLAN

**NAT Traversal**  
It is a general term for techniques that establish and maintain IP connections traversing NAT gateways. STUN is one of the NAT traversal techniques.

You can configure NAT traversal for the IP phone.

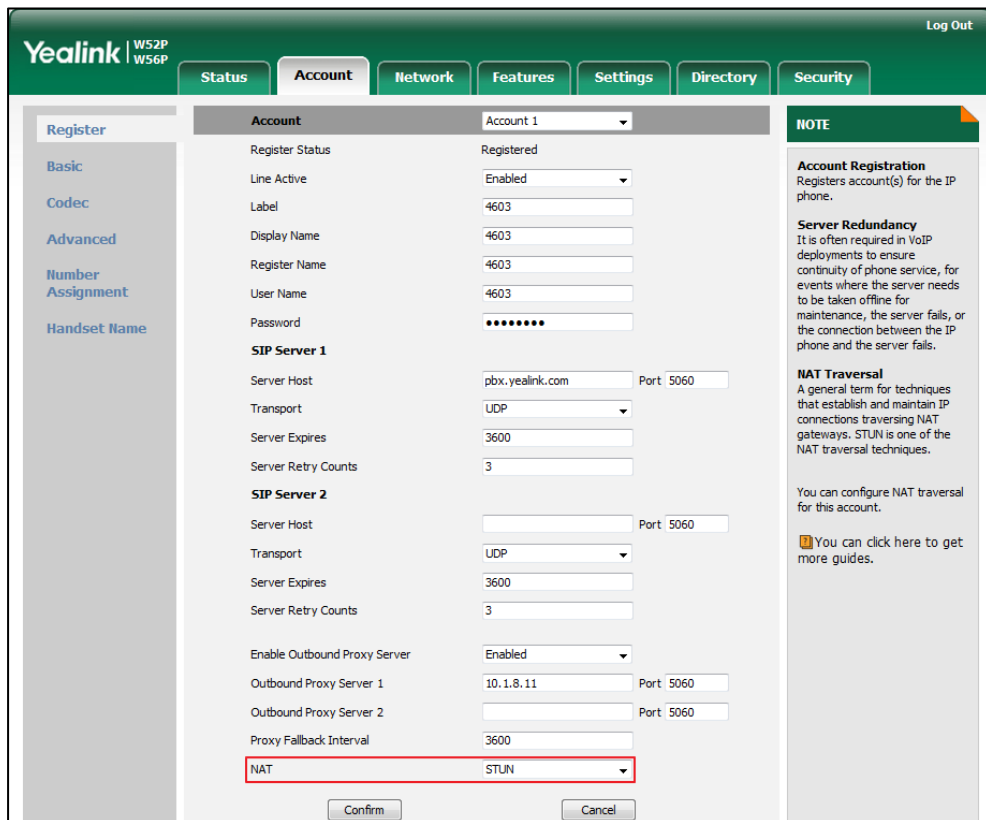
**Quality of Service (QoS)**  
It is the ability to provide different priorities for different

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

**To configure NAT traversal and STUN server via web user interface:**

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

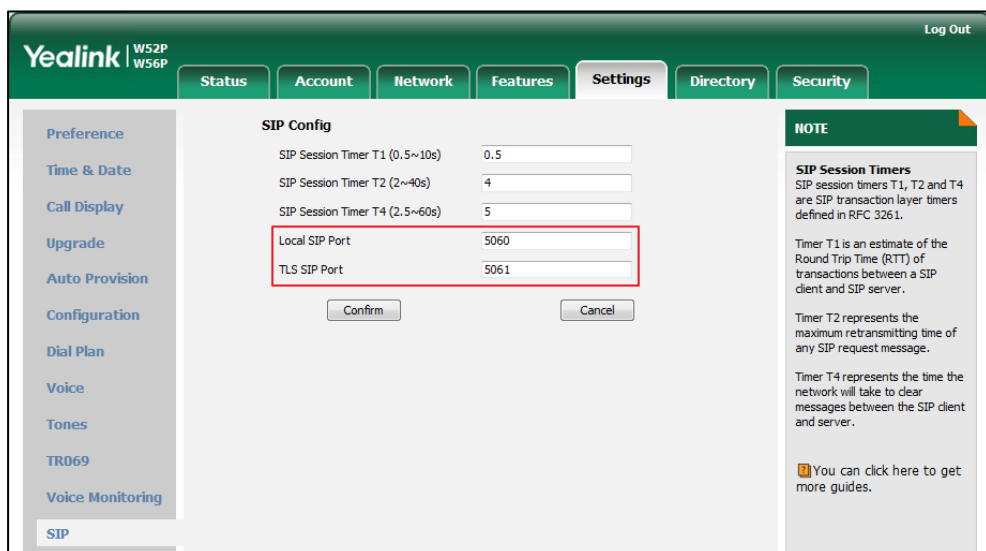
3. Select **STUN** from the pull-down list of **NAT**.



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

To configure local SIP port and TLS SIP port via web user interface:

1. Click on **Settings->SIP**.
2. Enter the desired local SIP port in the **Local SIP Port** field.
3. Enter the desired TLS SIP port in the **TLS SIP Port** field.



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

## Keep Alive

The IP DECT phones can send keep-alive packets to NAT device for keeping the communication port open.

### Procedure

Keep alive feature can be configured using the configuration files or locally.

<b>Configuration File</b>	<MAC>.cfg	Configure the type of keep-alive packets on a per-line basis. <b>Parameters:</b> account.X.nat.udp_update_enable
		Configure the keep-alive interval on a per-line basis. <b>Parameters:</b> account.X.nat.udp_update_time
<b>Local</b>	Web User Interface	Configure the type of keep-alive packets on a per-line basis. Configure the keep-alive interval on a per-line basis. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

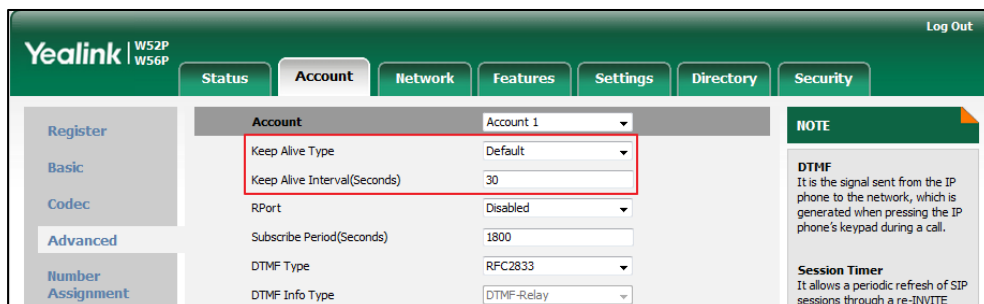
### Details of Configuration Parameters:

Parameters	Permitted Values	Default
<b>account.X.nat.udp_update_enable</b> (X ranges from 1 to 5)	<b>0, 1, 2 or 3</b>	<b>1</b>
<p><b>Description:</b> Configures the type of keep-alive packets sent by the IP DECT phone to the NAT device to keep the communication port open so that NAT can continue to function for account X.</p> <p><b>0-Disabled</b> <b>1-Default</b> (the IP DECT phone sends UDP packets to the server) <b>2-Options</b> (the IP DECT phone sends SIP OPTIONS packets to the server) <b>3-Notify</b> (the IP DECT phone sends SIP NOTIFY packets to the server)</p> <p><b>Web User Interface:</b> Account-&gt;Advanced-&gt;Keep Alive Type</p>		

Parameters	Permitted Values	Default
<b>Handset User Interface:</b> None		
<b>account.X.nat.udp_update_time</b>	<b>Integer from 15 to 2147483647</b>	<b>30</b>
<p><b>Description:</b> Configures the keep-alive interval (in seconds) for account X.</p> <p><b>Example:</b> account.1.nat.udp_update_time = 60</p> <p><b>Note:</b> It works only if the value of the parameter "account.X.nat.udp_update_enable" is set to 1, 2 or 3.</p> <p><b>Web User Interface:</b> Account-&gt;Advanced-&gt;UDP Keep Alive Interval(Seconds)</p> <p><b>Handset User Interface:</b> None</p>		

To configure the type of keep-alive packets and keep-alive interval via web user interface:

1. Click on **Account->Advanced**.
2. Select the desired account from the pull-down list of **Account**.
3. Select the desired value from the pull-down list of **Keep Alive Type**.
4. Enter the keep-alive interval in the **UDP Keep Alive Interval(Seconds)** field.



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

## Rport

Rport in [RFC 3581](#), allows a client to request that the server sends the response back to the source port from which the request came. Rport feature depends on support from a SIP server.

## Procedure

Rport feature can be configured using the configuration files or locally.

<b>Configuration File</b>	<MAC>.cfg	Configure NAT Rport feature for account. <b>Parameters:</b> account.X.nat.rport
<b>Local</b>	Web User Interface	Configure NAT Rport feature for account. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?parameter=account-adv&q=load&acc=0

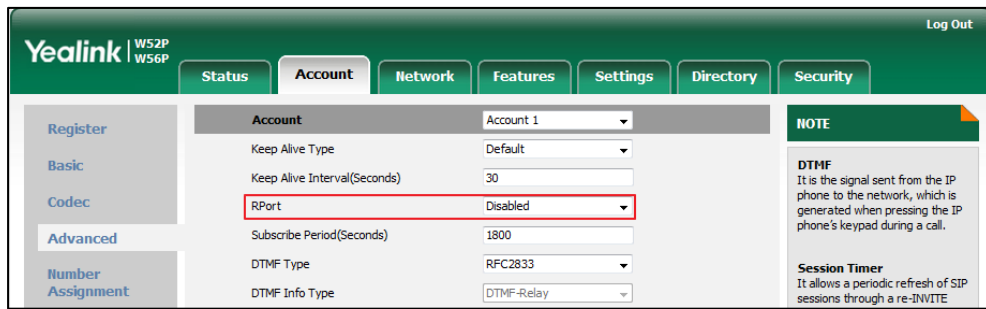
### Details of Configuration Parameters:

Parameters	Permitted Values	Default
<b>account.X.nat.rport</b> (X ranges from 1 to 5)	0, 1 or 2	0
<p><b>Description:</b> Enables or disables NAT Rport feature for account X.</p> <p><b>0-Disabled</b> <b>1-Enabled</b> <b>2-enable direct process</b></p> <p><b>Web User Interface:</b> Account-&gt;Advanced-&gt;RPort</p> <p><b>Handset User Interface:</b> None</p>		

To configure Rport feature via web user interface:

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

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



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

## Real-Time Transport Protocol

The Real-time Transport Protocol (RTP) is a network protocol for delivering audio and video over IP networks. The UDP port used for RTP streams is traditionally an even-numbered port. For example, the default RTP min port on the IP DECT phones is 11780. The first voice patch sends RTP on port 11780. Additional calls would then use ports 11782, 11784, 11786, etc. up to the max port.

### Procedure

RTP port can be configured using the configuration files or locally.

<b>Configuration File</b>	y00000000025.cfg	Configure RTP port. <b>Parameters:</b> network.port.max_rtpport network.port.min_rtpport
<b>Local</b>	Web User Interface	Configure RTP port. <b>Navigate to:</b> http://<phoneIPAddress>/serv let?p=network-adv&q=load

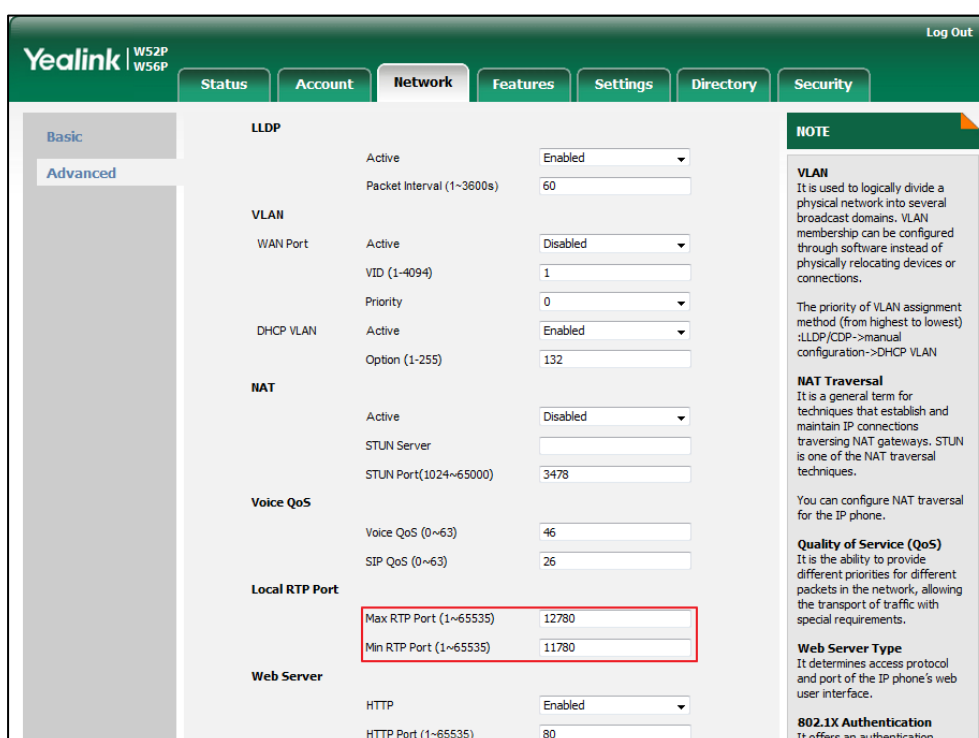
### Details of Configuration Parameters:

Parameters	Permitted Values	Default
network.port.max_rtpport	Integer from 1 to 65535	12780
<p><b>Description:</b> Configures the maximum local RTP port.</p> <p><b>Note:</b> The value of the maximum local RTP port cannot be less than that of the minimum local RTP port. If you change this parameter, the base station will reboot</p>		

Parameters	Permitted Values	Default
to make the change take effect. <b>Web User Interface:</b> Network->Advanced->Local RTP Port->Max RTP Port(1~65535) <b>Handset User interface:</b> None		
<b>network.port.min_rtpport</b>	<b>Integer from 1 to 65535</b>	<b>11780</b>
<b>Description:</b> Configures the minimum local RTP port. <b>Note:</b> If you change this parameter, the base station will reboot to make the change take effect. <b>Web User Interface:</b> Network->Advanced->Local RTP Port->Min RTP Port(1~65535) <b>Handset User interface:</b> None		

To configure the minimum and maximum RTP port via web user interface:

1. Click on **Network->Advanced**.
2. In the **Local RTP Port** block, enter the max and min RTP port in the **Max RTP Port(1~65535)** and **Min RTP Port(1~65535)** field respectively.





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

## 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

The following table provides a description of RPC methods supported by IP DECT 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. File types supported by IP DECT phones are: <ul style="list-style-type: none"> <li>• Firmware Image</li> </ul>

RPC Method	Description
	<ul style="list-style-type: none"> <li>Configuration File</li> </ul>
Upload	<p>This method is used to cause the CPE to upload a specified file to the designated location.</p> <p>File types supported by IP DECT phones are:</p> <ul style="list-style-type: none"> <li>Configuration File</li> <li>Log File</li> </ul>
ScheduleInform	<p>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.</p>
FactoryReset	<p>This method resets the CPE to its factory default state.</p>
TransferComplete	<p>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.</p>
AddObject	<p>This method is used to add a new instance of an object defined on the CPE.</p>
DeleteObject	<p>This method is used to remove a particular instance of an object.</p>

For more information on TR-069, refer to [Yealink TR-069 Technote](#).

### Procedure

TR-069 can be configured using the configuration files or locally.

<p><b>Configuration File</b></p>	<p>y000000000025.cfg</p>	<p>Configure TR-069 feature.</p> <p><b>Parameters:</b></p> <p>managementserver.enable</p> <p>managementserver.username</p> <p>managementserver.password</p> <p>managementserver.url</p> <p>managementserver.connection_request_username</p> <p>managementserver.connection_request_password</p> <p>managementserver.periodic_inform_enable</p> <p>managementserver.periodic_inform_interval</p>
----------------------------------	--------------------------	---

Local	Web User Interface	Configure TR-069 feature. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=phone-tr069&q=load
-------	--------------------	--

**Details of Configuration Parameters:**

Parameters	Permitted Values	Default
managementserver.enable	0 or 1	0
<p><b>Description:</b>                      Enables or disables the TR-069 feature.</p> <p>0-Disabled                      1-Enabled</p> <p><b>Web User Interface:</b>                      Settings-&gt;TR069-&gt;Enable TR069</p> <p><b>Handset User Interface:</b>                      None</p>		
managementserver.username	String within 128 characters	Blank
<p><b>Description:</b>                      Configures the user name for the IP DECT phone to authenticate with the ACS (Auto Configuration Servers).                      Leave it blank if no authentication is required.</p> <p><b>Example:</b>                      managementserver.username = tr69</p> <p><b>Web User Interface:</b>                      Settings-&gt;TR069-&gt;ACS Username</p> <p><b>Handset User Interface:</b>                      None</p>		
managementserver.password	String within 64 characters	Blank
<p><b>Description:</b>                      Configures the password for the IP DECT phone to authenticate with the ACS (Auto Configuration Servers).                      Leave it blank if no authentication is required.</p> <p><b>Example:</b></p>		

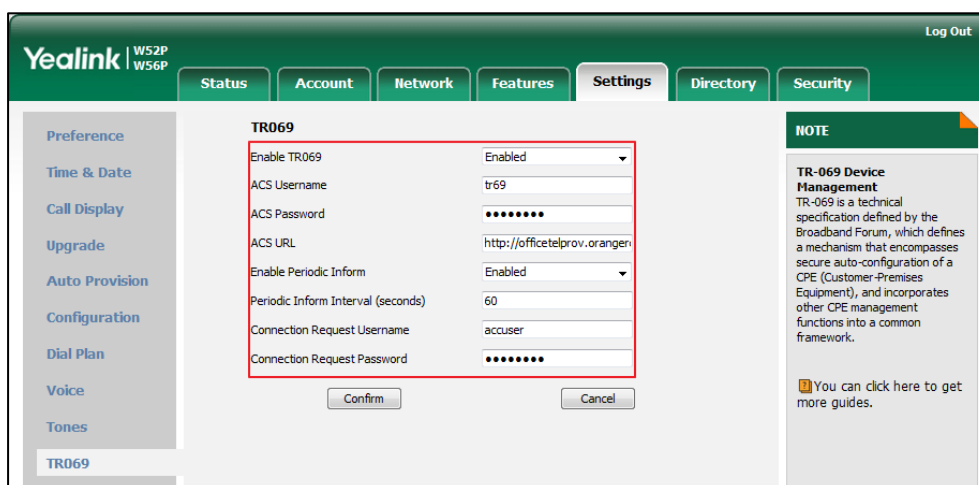
Parameters	Permitted Values	Default
<p>managementserver.password = tr69</p> <p><b>Web User Interface:</b> Settings-&gt;TR069-&gt;ACS Password</p> <p><b>Handset User Interface:</b> None</p>		
managementserver.url	URL within 511 characters	Blank
<p><b>Description:</b> Configures the access URL of the ACS (Auto Configuration Servers).</p> <p><b>Example:</b> managementserver.url =http://officetelprov.orangero.net:8080/ftacs-digest/ACS</p> <p><b>Web User Interface:</b> Settings-&gt;TR069-&gt;ACS URL</p> <p><b>Handset User Interface:</b> None</p>		
managementserver.connection_request_username	String within 128 characters	Blank
<p><b>Description:</b> Configures the user name for the IP DECT phone to authenticate the incoming connection requests.</p> <p><b>Example:</b> managementserver.connection_request_username = accuser</p> <p><b>Web User Interface:</b> Settings-&gt;TR069-&gt;Connection Request Username</p> <p><b>Handset User Interface:</b> None</p>		
managementserver.connection_request_password	String within 64 characters	Blank
<p><b>Description:</b> Configures the password for the IP DECT phone to authenticate the incoming connection requests.</p> <p><b>Example:</b> managementserver.connection_request_password = acspwd</p> <p><b>Web User Interface:</b> Settings-&gt;TR069-&gt;Connection Request Password</p>		

Parameters	Permitted Values	Default
<b>Handset User Interface:</b> None		
<b>managementserver.periodic_inform_enable</b>	<b>0 or 1</b>	<b>1</b>
<p><b>Description:</b> Enables or disables the IP DECT phone to periodically report its configuration information to the ACS (Auto Configuration Servers).</p> <p><b>0-Disabled</b> <b>1-Enabled</b></p> <p><b>Web User Interface:</b> Settings-&gt;TR069-&gt;Enable Periodic Inform</p> <p><b>Handset User Interface:</b> None</p>		
<b>managementserver.periodic_inform_interval</b>	<b>Integer from 5 to 4294967295</b>	<b>60</b>
<p><b>Description:</b> Configures the interval (in seconds) for the IP DECT phone to report its configuration to the ACS (Auto Configuration Servers).</p> <p><b>Note:</b> It works only if the value of the parameter "managementserver.periodic_inform_enable" is set to 1 (Enabled).</p> <p><b>Web User Interface:</b> Settings-&gt;TR069-&gt;Periodic Inform Interval (seconds)</p> <p><b>Handset User Interface:</b> None</p>		

**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 DECT phone in the **Connection Request Username** and **Connection Request Password** fields.



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

---

# Configuring Audio Features

---

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

- [Tones](#)
- [Voice Mail Tone](#)
- [Audio Codecs](#)
- [Acoustic Clarity Technology](#)

## Tones

When receiving a message, the IP DECT 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 DECT phone. The default tones used on IP DECT phones are the US tone sets. Available tone sets for IP DECT 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 IP DECT phones for the following conditions.

Condition	Description
Dial	When in the pre-dialing interface
Ring Back	Ring-back tone
Busy	When the callee is busy
Call Waiting	Call waiting tone

### Procedure

Tones can be configured using the configuration files or locally.

<b>Configuration File</b>	y00000000025.cfg	Configure the tones for the IP DECT phone. <b>Parameters:</b> voice.tone.country voice.tone.dial voice.tone.ring voice.tone.busy voice.tone.callwaiting
<b>Local</b>	Web User Interface	Configure the tones for the IP DECT phone. <b>Navigate to:</b> <a href="http://&lt;phoneIPAddress&gt;/servlet?p=settings-tones&amp;q=load">http://&lt;phoneIPAddress&gt;/servlet?p=settings-tones&amp;q=load</a>



### Details of Configuration Parameters:

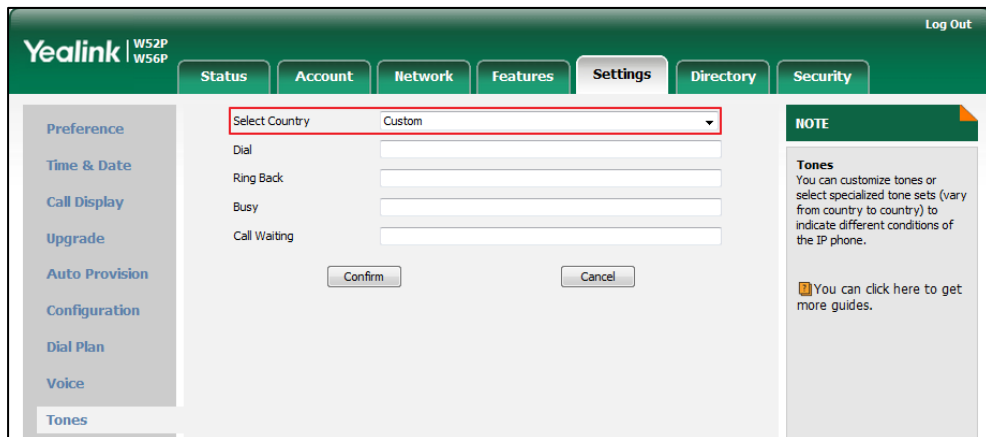
Parameters	Permitted Values	Default
voice.tone.country	Refer to the following content	Custom
<p><b>Description:</b> Configures the country tone for the IP DECT phone.</p> <p><b>Permitted Values:</b> Custom, Australia, Austria, Brazil, Belgium, Chile, China, Czech, Czech ETSI, Denmark, Finland, France, Germany, Great Britain, Greece, Hungary, Lithuania, India, Italy, Japan, Mexico, New Zealand, Netherlands, Norway, Portugal, Spain, Switzerland, Sweden, Russia, United States.</p> <p><b>Example:</b> voice.tone.country=Custom</p> <p><b>Web User Interface:</b> Settings-&gt;Tones-&gt;Select country</p> <p><b>Handset User Interface:</b> None</p>		
voice.tone.dial	String	Blank
<p><b>Description:</b> Customizes the dial tone.</p> <p>tonelist = element[,element] [,element]...</p> <p><b>element</b> = [!]<b>Freq1</b>[+<b>Freq2</b>][+<b>Freq3</b>][+<b>Freq4</b>] /<b>Duration</b></p> <p><b>Freq:</b> the frequency of the tone (ranges from 200 to 4000Hz). If it is set to 0Hz, it means the tone is not played.</p> <p><b>Duration:</b> the duration (in milliseconds) of the dial tone, ranges from 0 to 30000ms.</p> <p>You can configure at most eight different tones for one condition, and separate them by commas. (e.g., 250/200,0/1000,200+300/500,600+700+800+1000/2000).</p> <p>If you want the IP DECT phone to play tones once, add an exclamation mark “!” before tones (e.g., !250/200,0/1000,200+300/500,600+700+800+1000/2000).</p> <p><b>Note:</b> It works only if the value of the parameter “voice.tone.country” is set to Custom.</p> <p><b>Web User Interface:</b> Settings-&gt;Tones-&gt;Dial</p> <p><b>Handset User Interface:</b> None</p>		

Parameters	Permitted Values	Default
<b>voice.tone.ring</b>	<b>String</b>	<b>Blank</b>
<p><b>Description:</b>                      Customizes the ring back tone.                      The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial".  <b>Note:</b> It works only if the value of the parameter "voice.tone.country" is set to Custom.  <b>Web User Interface:</b>                      Settings-&gt;Tones-&gt;Ring back  <b>Handset User interface:</b>                      None</p>		
<b>voice.tone.busy</b>	<b>String</b>	<b>Blank</b>
<p><b>Description:</b>                      Customizes the tone when the callee is busy.                      The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial".  <b>Note:</b> It works only if the value of the parameter "voice.tone.country" is set to Custom.  <b>Web User Interface:</b>                      Settings-&gt;Tones-&gt;Busy  <b>Handset User interface:</b>                      None</p>		
<b>voice.tone.callwaiting</b>	<b>String</b>	<b>Blank</b>
<p><b>Description:</b>                      Customizes the call waiting tone.                      The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial".  <b>Note:</b> It works only if the value of the parameter "voice.tone.country" is set to Custom.  <b>Web User Interface:</b>                      Settings-&gt;Tones-&gt;Call Waiting  <b>Handset User interface:</b>                      None</p>		

To configure tones via web user interface:

1. Click on **Settings->Tones**.
2. Select the desired value from the pull-down list of **Select Country**.

If you select **Custom**, you can customize a tone for each condition of the IP DECT phone.



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

## Voice Mail Tone

Voice mail tone feature allows the IP DECT phone to play a warning tone when receiving a new voice mail.

### Procedure

Voice mail tone can be configured using the configuration files or locally.

<b>Configuration File</b>	y00000000025.cfg	Configure whether to play a warning tone when the IP DECT phone receives a new voice mail. <b>Parameters:</b> features.voice_mail_tone_enable
<b>Local</b>	Web User Interface	Configure whether to play a warning tone when the IP DECT phone receives a new voice mail. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=settings-tones&q=load

### Details of the Configuration Parameter:

Parameter	Permitted Values	Default
features.voice_mail_tone_enable	0 or 1	1

**Description:**  
 Enables or disables the IP DECT phone to play a warning tone when it receives a new voice mail.

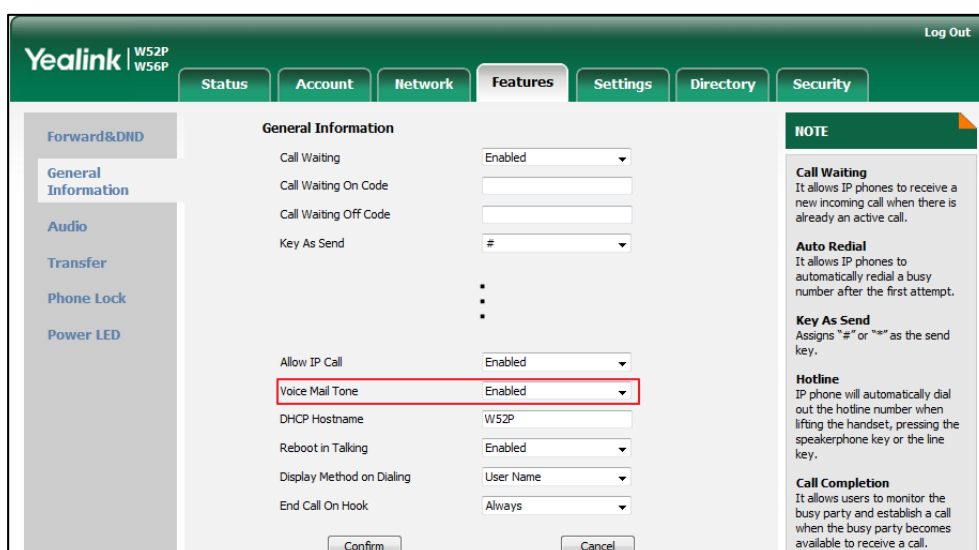
**0-Disabled**  
**1-Enabled**

**Web User Interface:**  
 Features->General Information->Voice Mail Tone

**Handset User interface:**  
 None

#### To configure voice mail tone via web user interface:

1. Click on **Features->General Information**.
2. Select the desired value from the pull-down list of **Voice Mail Tone**.



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 audio codec that the phone uses to establish a call should be supported by the SIP server. When placing a call, the IP DECT phone will offer the enabled audio codec list to the server and then use the audio codec negotiated with the called party according to the priority.

The following table summarizes the supported audio codecs on IP DECT phones:

Codec	Algorithm	Reference	Bit Rate	Sample Rate	Packetization Time
PCMA	G.711 a-law	RFC 3551	64 Kbps	8 Ksps	20ms
PCMU	G.711 u-law	RFC 3551	64 Kbps	8 Ksps	20ms
G723_53/ G723_63	G.723.1	RFC 3951	5.3kbps 6.3kbps	8 Ksps	30ms
G729	G.729	RFC 3551	8 Kbps	8 Ksps	20ms
G722	G.722	RFC 3551	64 Kbps	16 Ksps	20ms
G726-32	G.726	RFC 3551	32 Kbps	8 Ksps	20ms
iLBC	iLBC	RFC 3952	13.33 Kbps 15.2 Kbps	8 Ksps	20ms 30ms

## 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.

Codecs and priorities of these codecs are configurable on a per-line basis. The attribute "rtpmap" 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
G722	Configuration Files Web User Interface	1	9
PCMU	Configuration Files Web User Interface	2	0
PCMA	Configuration Files	3	8

Codec	Configuration Methods	Priority	RTPmap
	Web User Interface		
G729	Configuration Files Web User Interface	4	18
G723_53	Configuration Files Web User Interface	0	4
G723_63	Configuration Files Web User Interface	0	4
G726-32	Configuration Files Web User Interface	0	102
iLBC	Configuration Files Web User Interface	0	106

### Procedure

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

<b>Configuration File</b>	<MAC>.cfg	<p>Configure the codecs to use on a per-line basis.</p> <p><b>Parameters:</b></p> <p>account.X.codec.Y.enable account.X.codec.Y.payload_type</p>
		<p>Configure the priority and rtpmap for the enabled codec.</p> <p><b>Parameters:</b></p> <p>account.X.codec.Y.priority account.X.codec.Y.rtpmap</p>
		<p>Configure the ptime.</p> <p><b>Parameter:</b></p> <p>account.X.ptime</p>
<b>Local</b>	Web User Interface	<p>Configure the codecs to use on a per-line basis.</p> <p>Configure the priority for the enabled codec.</p> <p><b>Navigate to:</b></p> <p>http://&lt;phoneIPAddress&gt;/servlet?p=account-codec&amp;q=load&amp;acc=0</p>

		Configure the ptime. <b>Navigate to:</b> <a href="http://&lt;phoneIPAddress&gt;/servlet?p=account-adv&amp;q=load&amp;acc=0">http://&lt;phoneIPAddress&gt;/servlet? p=account-adv&amp;q=load&amp;acc=0</a>
--	--	---

### Details of Configuration Parameters:





Parameters	Permitted Values	Default
<b>account.X.codec.Y.enable</b> (X ranges from 1 to 5, Y ranges from 1 to 8)	0 or 1	Refer to the following content
<p><b>Description:</b>            Enables or disables the specified codec for account X.</p> <p><b>0-Disabled</b>  <b>1-Enabled</b></p> <p><b>Default:</b>            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> <p><b>Example:</b>            account.1.codec.1.enable = 1            It means that the codec PCMU is enabled on the account 1.</p> <p><b>Web User Interface:</b>            Account-&gt;Codec</p> <p><b>Handset User Interface:</b>            None</p>		
<b>account.X.codec.Y.payload_type</b> (X ranges from 1 to 5, Y ranges from 1 to 8)	Refer to the following content	Refer to the following content
<p><b>Description:</b>            Configures the codec for account X.</p> <p><b>Permitted Values:</b>            PCMU, PCMA, G723_53, G723_63, G729, G722, G726-32, iLBC</p>		

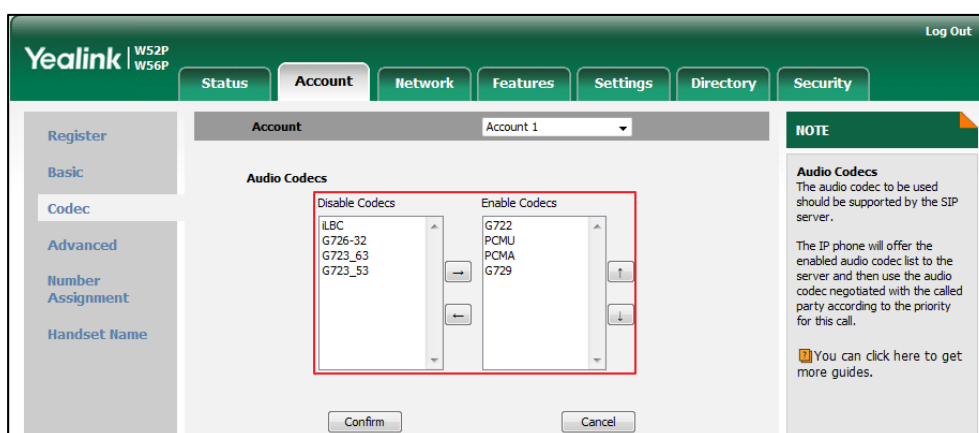
Parameters	Permitted Values	Default
<p><b>Default:</b>                      When Y=1, the default value is PCMU;                      When Y=2, the default value is PCMA;                      When Y=3, the default value is G723_53;                      When Y=4, the default value is G723_63;                      When Y=5, the default value is G729;                      When Y=6, the default value is G722;                      When Y=7, the default value is G726-32;                      When Y=8, the default value is iLBC;</p> <p><b>Example:</b>                      account.1.codec.1.payload_type = PCMU</p> <p><b>Web User Interface:</b>                      Account-&gt;Codec</p> <p><b>Handset User Interface:</b>                      None</p>		
<p><b>account.X.codec.Y.priority</b>                      (X ranges from 1 to 5, Y ranges from 1 to 8)</p>	<p><b>Integer from 0 to 10</b></p>	<p><b>Refer to the following content</b></p>
<p><b>Description:</b>                      Configures the priority of the enabled codec for account X.                      When Y=1, the default value is 2;                      When Y=2, the default value is 3;                      When Y=3, the default value is 4;                      When Y=4, the default value is 0;                      When Y=5, the default value is 4;                      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> <p><b>Example:</b>                      account.1.codec.1.priority = 2</p> <p><b>Web User Interface:</b>                      Account-&gt;Codec</p> <p><b>Handset User Interface:</b>                      None</p>		



Parameters	Permitted Values	Default
<b>account.X.codec.Y.rtpmap</b> (X ranges from 1 to 5, Y ranges from 1 to 8)	<b>Integer</b> <b>from 0 to 127</b>	<b>Refer to the following content</b>
<p><b>Description:</b>            Configures the rtpmap of the audio codec for account X.            When Y=1, the default value is 0;            When Y=2, the default value is 8;            When Y=3, the default value is 4;            When Y=4, the default value is 4;            When Y=5, the default value is 18;            When Y=6, the default value is 9;            When Y=7, the default value is 102;            When Y=8, the default value is 106;</p> <p><b>Example:</b>            account.1.codec.1.rtpmap = 0</p> <p><b>Web User Interface:</b>            None</p> <p><b>Handset User Interface:</b>            None</p>		
<b>account.X.ptime</b> (X ranges from 1 to 5)	<b>0, 10, 20, 30, 40, 50 or 60</b>	<b>20</b>
<p><b>Description:</b>            Configures the ptime (in milliseconds) for the codec for account X.</p> <p><b>0-Disabled</b></p> <p><b>10-10</b></p> <p><b>20-20</b></p> <p><b>30-30</b></p> <p><b>40-40</b></p> <p><b>50-50</b></p> <p><b>60-60</b></p> <p><b>Web User Interface:</b>            Account-&gt;Advanced-&gt;PTime(ms)</p> <p><b>Handset User Interface:</b>            None</p>		

To configure the codecs to use and adjust the priority of the enabled codecs on a per-line basis via web user interface:

1. Click on **Account->Codec**.
2. Select the desired account from the pull-down list of **Account**.
3. Select the desired codec from the **Disable Codecs** column and then click  .  
The selected codec appears in the **Enable Codecs** column.
4. Repeat the step 4 to add more codecs to the **Enable Codecs** column.
5. To remove the codec from the **Enable Codecs** column, select the desired codec and then click  .
6. To adjust the priority of codecs, select the desired codec and then click  or  .



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

To configure the ptime for the account via web user interface:

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

3. Select the desired value from the pull-down list of **PTime(ms)**.

The screenshot shows the Yealink configuration web interface for a W52P/W56P device. The 'Account' tab is selected, and the 'Account 1' configuration page is displayed. The 'PTime(ms)' field is highlighted with a red box, showing a value of 20. Other fields include 'Keep Alive Type' (Default), 'Keep Alive Interval(Seconds)' (30), 'Send user=phone' (Disabled), 'RTP Encryption(SRTP)' (Disabled), 'Shared Line' (Disabled), 'SIP Send MAC' (Enabled), 'SIP Send Line' (Enabled), 'SIP Registration Retry Timer(0~1800s)' (30), 'Conference Type' (Local Conference), 'Conference URI' (empty), 'SIP Server Type' (Default), 'Unregister When Reboot' (Enabled), 'VQ RTCP-XR Collector name' (empty), 'VQ RTCP-XR Collector address' (empty), and 'VQ RTCP-XR Collector port' (5060). A 'NOTE' section on the right provides details about DTMF, Session Timer, Shared Call Appearance (SCA)/ Bridge Line Appearance (BLA), Network Conference, and VQ-RTCPXR.

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

## Acoustic Clarity Technology

## Background Noise Suppression

Background noise suppression (BNS) is designed primarily for hands-free operation and reduces background noise to enhance communication in noisy environments.

## Automatic Gain Control

Automatic Gain Control (AGC) is applicable to hands-free operation and is used to keep audio output at nearly a constant level by adjusting the gain of signals in certain circumstances. This increases the effective user-phone radius and helps with the intelligibility of talkers.

## 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.

<b>Configuration File</b>	y000000000025.cfg	Configure VAD. <b>Parameter:</b> voice.vad
<b>Local</b>	Web User Interface	Configure VAD. <b>Navigate to:</b> <a href="http://&lt;phoneIPAddress&gt;/servlet?p=settings-voice&amp;q=load">http://&lt;phoneIPAddress&gt;/servlet?p=settings-voice&amp;q=load</a>

### Details of the Configuration Parameter:

Parameter	Permitted Values	Default
voice.vad	0 or 1	0
<p><b>Description:</b> Enables or disables the VAD (Voice Activity Detection) feature on the IP DECT phone.</p> <p><b>0</b>-Disabled <b>1</b>-Enabled</p> <p><b>Web User Interface:</b> Settings-&gt;Voice-&gt;Echo Cancellation-&gt;VAD</p> <p><b>Handset User Interface:</b> None</p>		

To configure VAD via web user interface:

1. Click on **Settings->Voice**.
2. Select the desired value from the pull-down list of **VAD**.

The screenshot shows the Yealink W52P/W56P web interface. The 'Settings' tab is active, and the 'Voice' sub-tab is selected. Under 'Echo Cancellation', the 'VAD' dropdown menu is highlighted with a red box and set to 'Disabled'. Below it, 'CNG' is set to 'Enabled'. Under 'JITTER BUFFER', 'Type' is set to 'Adaptive' (selected with a radio button), and 'Fixed' is unselected. The 'Min Delay' is set to 60, 'Max Delay' is 240, and 'Normal' is 120. There are 'Confirm' and 'Cancel' buttons at the bottom. On the right, a 'NOTE' section explains:
 

- Acoustic Echo Cancellation (AEC)**: It is used to reduce acoustic echo from a voice call to provide natural full-duplex communication patterns.
- Voice Activity Detection (VAD)**: It is used in speech processing to detect the presence or absence of human speech.
- Comfort Noise Generation (CNG)**: It is used to generate background noise for voice.

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.

### Note

VAD is used to send CN packets when phone detect a "silence" period; CNG is used to generate comfortable noise when phone receives CN packets from the other side.

For example, A is talking with B.

A: VAD=1, CNG=1

B: VAD=0, CNG=1

If A mutes the call, since VAD=1, A will send CN packets to B. When receiving CN packets, B will generate comfortable noise.

If B mutes the call, since VAD=0, B will not send CN packets to A. So even if CNG=1 (B), A will not hear comfortable noise.

## Procedure

CNG can be configured using the configuration files or locally.

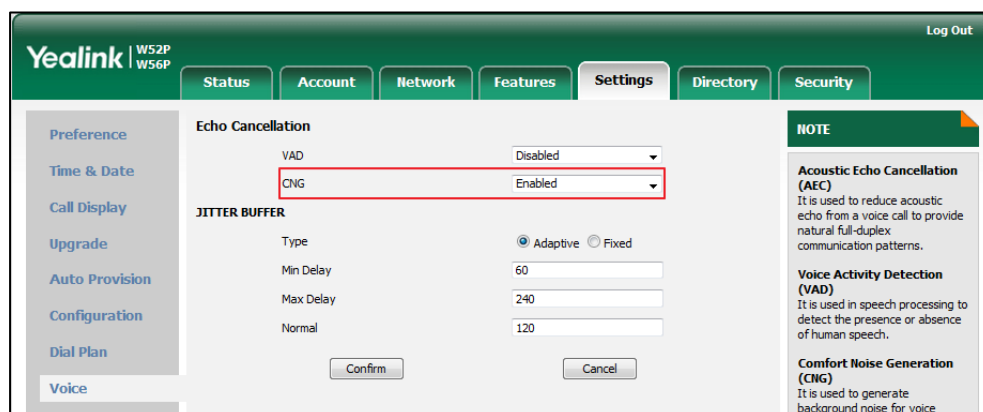
<b>Configuration File</b>	y00000000025.cfg	Configure CNG. <b>Parameter:</b> voice.cng
<b>Local</b>	Web User Interface	Configure CNG. <b>Navigate to:</b> http://<phoneIPAddress>/ser vlet?p=settings-voice&q=load

### Details of the Configuration Parameter:

Parameter	Permitted Values	Default
voice.cng	0 or 1	1
<p><b>Description:</b> Enables or disables the CNG (Comfortable Noise Generation) feature on the IP DECT phone.</p> <p>0-Disabled 1-Enabled</p> <p><b>Web User Interface:</b> Settings-&gt;Voice-&gt;Echo Cancellation-&gt;CNG</p> <p><b>Handset User Interface:</b> None</p>		

### To configure CNG via web user interface:

1. Click on **Settings->Voice**.
2. Select the desired value from the pull-down list of **CNG**.



- 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. The IP DECT phones support two types of jitter buffers: fixed and adaptive. A fixed jitter buffer adds the fixed delay to voice packets. You can configure the delay time for the static jitter buffer on IP DECT phones. An adaptive 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 DECT phones.

### Procedure

Jitter buffer can be configured using the configuration files or locally.

<b>Configuration File</b>	y000000000025.cfg	Configure the mode of jitter buffer and the delay time for jitter buffer. <b>Parameters:</b> voice.jib.adaptive voice.jib.min voice.jib.max voice.jib.normal
<b>Local</b>	Web User Interface	Configure the mode of jitter buffer and the delay time for jitter buffer. <b>Navigate to:</b> <a href="http://&lt;phoneIPAddress&gt;/servlet?p=settings-voice&amp;q=load">http://&lt;phoneIPAddress&gt;/servlet?p=settings-voice&amp;q=load</a>

### Details of Configuration Parameters:

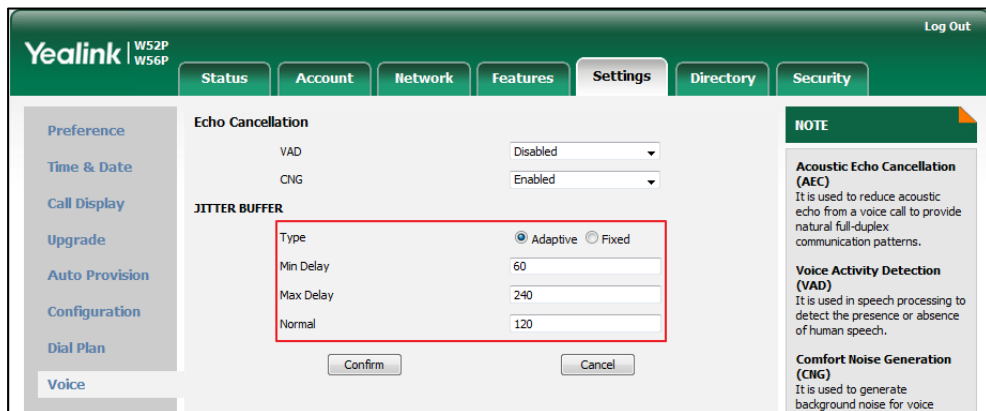
Parameters	Permitted Values	Default
voice.jib.adaptive	0 or 1	1
<b>Description:</b> Configures the type of jitter buffer. <b>0-Fixed</b>		

Parameters	Permitted Values	Default
<p>1-Adaptive</p> <p><b>Web User Interface:</b> Settings-&gt;Voice-&gt;JITTER BUFFER-&gt;Type</p> <p><b>Handset User Interface:</b> None</p>		
voice.jib.min	Integer from 0 to 400	0
<p><b>Description:</b> Configures the minimum delay time (in milliseconds) of jitter buffer.</p> <p><b>Note:</b> It works only if the value of the parameter "voice.jib.adaptive" is set to 1 (Adaptive).</p> <p><b>Web User Interface:</b> Settings-&gt;Voice-&gt;JITTER BUFFER-&gt;Min Delay</p> <p><b>Handset User Interface:</b> None</p>		
voice.jib.max	Integer from 0 to 400	300
<p><b>Description:</b> Configures the maximum delay time (in milliseconds) of jitter buffer.</p> <p><b>Note:</b> It works only if the value of the parameter "voice.jib.adaptive" is set to 1 (Adaptive).</p> <p><b>Web User Interface:</b> Settings-&gt;Voice-&gt;JITTER BUFFER-&gt;Max Delay</p> <p><b>Handset User Interface:</b> None</p>		
voice.jib.normal	Integer from 0 to 400	120
<p><b>Description:</b> Configures the normal delay time (in milliseconds) of jitter buffer.</p> <p><b>Note:</b> It works only if the value of the parameter "voice.jib.adaptive" is set to 0 (Fixed).</p> <p><b>Web User Interface:</b> Settings-&gt;Voice-&gt;JITTER BUFFER-&gt;Normal</p> <p><b>Handset User Interface:</b> None</p>		



**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.  
The valid value ranges from 0 to 400.
4. Enter the maximum delay time for adaptive jitter buffer in the **Max Delay** field.  
The valid value ranges from 0 to 400.
5. Enter the fixed delay time for fixed jitter buffer in the **Normal** field.  
The valid value ranges from 0 to 400.



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

## 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 DECT phone to the network, which is generated when pressing the IP DECT phone’s keypad during a call. Each key pressed on the IP DECT 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
--------	---	---	---	---

## Methods of Transmitting DTMF Digit

Three methods of transmitting DTMF digits on SIP calls:

- **RFC 2833**--DTMF digits are transmitted by RTP Events compliant to RFC2833.
- **INBAND**--DTMF digits are transmitted in the voice band.
- **SIP INFO**--DTMF digits are transmitted by SIP INFO messages.

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

### **RFC2833**

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 RTP Event packets is configurable. IP DECT 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 DECT phone conversation. It uses the same codec as your voice and is audible to 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.

<b>Configuration File</b>	<MAC>.cfg	Configure the method of transmitting DTMF digit and the payload type. <b>Parameters:</b> account.X.dtmf.type account.X.dtmf.dtmf_payload account.X.dtmf.info_type
		Configure the frequency level of DTMF digits. <b>Parameter:</b> features.dtmf.volume
<b>Local</b>	Web User Interface	Configure the method of transmitting DTMF digits and the payload type. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

### Details of Configuration Parameters:

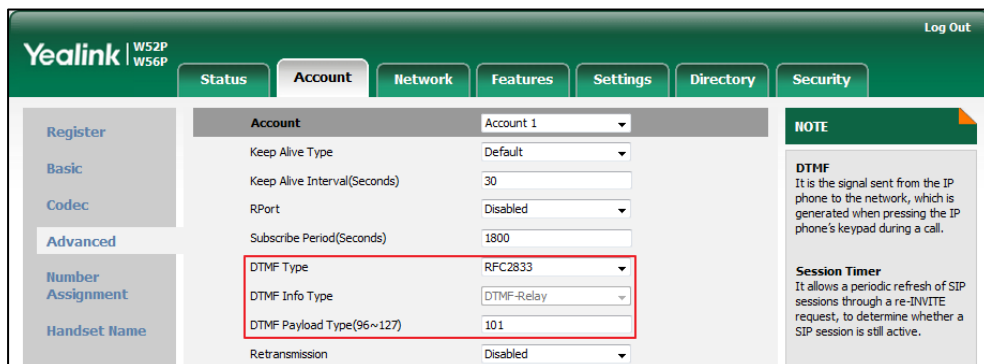
Parameters	Permitted Values	Default
<b>account.X.dtmf.type</b> (X ranges from 1 to 5)	<b>0, 1, 2 or 3</b>	<b>1</b>
<p><b>Description:</b> Configures the DTMF type for account X.</p> <p><b>0</b>-INBAND <b>1</b>-RFC 2833 <b>2</b>-SIP INFO <b>3</b>-RFC2833 + SIP INFO</p> <p>If it is set to 0 (INBAND), DTMF digits are transmitted in the voice band.</p> <p>If it is set to 1 (RFC 2833), DTMF digits are transmitted by RTP Events compliant to RFC2833.</p> <p>If it is set to 2 (SIP INFO), DTMF digits are transmitted by the SIP INFO messages.</p> <p>If it is set to 3 (RFC2833 + SIP INFO), DTMF digits are transmitted by RTP Events</p>		

Parameters	Permitted Values	Default
compliant to RFC2833 and the SIP INFO messages. <b>Web User Interface:</b> Account->Advanced->DTMF Type <b>Handset User Interface:</b> None		
<b>account.X.dtmf.dtmf_payload</b> (X ranges from 1 to 5)	Integer from 96 to 127	101
<b>Description:</b> Configures the value of DTMF payload for account X. <b>Note:</b> It works only if the value of parameter "account.X.dtmf.type" is set to 1 (RFC2833) or 3 (RFC2833 + SIP INFO). <b>Web User Interface:</b> Account->Advanced->DTMF Payload Type(96~127) <b>Handset User Interface:</b> None		
<b>account.X.dtmf.info_type</b> (X ranges from 1 to 5)	1, 2 or 3	1
<b>Description:</b> Configures the DTMF info type. 1-DTMF-Relay 2-DTMF 3-Telephone-Event <b>Note:</b> It works only if the value of parameter "account.X.dtmf.type" is set to 2 (SIP INFO) or 3 (RFC2833 + SIP INFO). <b>Web User Interface:</b> Account->Advanced->DTMF Info Type <b>Handset User Interface:</b> None		
<b>features.dtmf.volume</b>	Integer from -33 to 0	-10
<b>Description:</b> Configures the frequency level of DTMF digits (in db). <b>Web User Interface:</b> None		

Parameters	Permitted Values	Default
<b>Handset User Interface:</b>		
None		

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

1. Click on **Account->Advanced**.
2. Select the desired account from the pull-down list of **Account**.
3. Select the desired value from the pull-down list of **DTMF Type**.  
If **SIP INFO** or **RFC2833 + SIP INFO** is selected, select the desired value from the pull-down list of **DTMF Info Type**.
4. 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.



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

## Suppress DTMF Display

Suppress DTMF display allows IP DECT phones to suppress the display of DTMF digits during an active call. 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.

<b>Configuration File</b>	y00000000025.cfg	Configure suppress DTMF display and suppress DTMF display delay. <b>Parameters:</b> features.dtmf.hide features.dtmf.hide_delay
<b>Local</b>	Web User Interface	Configure suppress DTMF display

		and suppress DTMF display delay. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p =features-general&q=load
--	--	--

**Details of Configuration Parameters:**

Parameters	Permitted Values	Default
<b>features.dtmf.hide</b>	<b>0 or 1</b>	<b>0</b>
<p><b>Description:</b> Enables or disables the IP DECT phone to suppress the display of DTMF digits during an active call. <b>0</b>-Disabled <b>1</b>-Enabled If it is set to 1 (Enabled), the DTMF digits are displayed as asterisks.</p> <p><b>Web User Interface:</b> Features-&gt;General Information-&gt;Suppress DTMF Display</p> <p><b>Handset User Interface:</b> None</p>		
<b>features.dtmf.hide_delay</b>	<b>0 or 1</b>	<b>0</b>
<p><b>Description:</b> Enables or disables the IP DECT phone to display the DTMF digits for a short period before displaying asterisks during an active call. <b>0</b>-Disabled <b>1</b>-Enabled <b>Note:</b> It works only if the value of the parameter "features.dtmf.hide" is set to 1 (Enabled).</p> <p><b>Web User Interface:</b> Features-&gt;General Information-&gt;Suppress DTMF Display Delay</p> <p><b>Handset User Interface:</b> None</p>		

**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**.

The screenshot shows the Yealink configuration interface for a W52P/W56P device. The 'Features' tab is selected, and the 'General Information' section is visible. The 'Suppress DTMF Display Delay' option is highlighted with a red box, showing a dropdown menu set to 'Disabled'. Other options include 'Call Waiting', 'Key As Send', 'Auto Redial', 'Hotline', and 'Call Completion'.

Feature	Value
Call Waiting	Enabled
Call Waiting On Code	
Call Waiting Off Code	
Key As Send	#
Reserve # in User Name	Enabled
Busy Tone Delay (Seconds)	0
Return Code When Refuse	486 (Busy Here)
Return Code When DND	480 (Temporarily Unavail)
Feature Key Synchronization	Disabled
Time-Out for Dial-Now Rule	1
RFC 2543 Hold	Disabled
Use Outbound Proxy In Dialog	Enabled
180 Ring Workaround	Enabled
Save Call Log	Enabled
Suppress DTMF Display	Disabled
Suppress DTMF Display Delay	Disabled
Fwd International	Enabled

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

## Voice Quality Monitoring (VQM)

Voice quality monitoring feature allows the IP DECT phones to generate various quality metrics for listening quality and conversational quality. These metrics can be sent between the phones in RTCP-XR packets. These metrics can also be sent in SIP PUBLISH messages to a central voice quality report collector. Two mechanisms for voice quality monitoring are supported by Yealink IP DECT phones:

- RTCP-XR
- VQ-RTCPXR

## RTCP-XR

The RTCP-XR mechanism, compliant with [RFC 3611-RTP Control Extended Reports \(RTCP XR\)](#), provides the metrics contained in RTCP-XR packets for monitoring the quality of calls. These metrics include network packet loss, delay metrics, analog metrics and voice quality metrics.

## Procedure

RTCP-XR can be configured using the following methods.

<b>Central Provisioning (Configuration File)</b>	y000000000025.cfg	Configure RTCP-XR. <b>Parameters:</b> voice.rtcp_xr.enable phone_setting.rtcp_xr_report.enable
<b>Local</b>	<b>Web User Interface</b>	Configure RTCP-XR. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?parameter=voice_monitoring&q=load

### Details of Configuration Parameters:

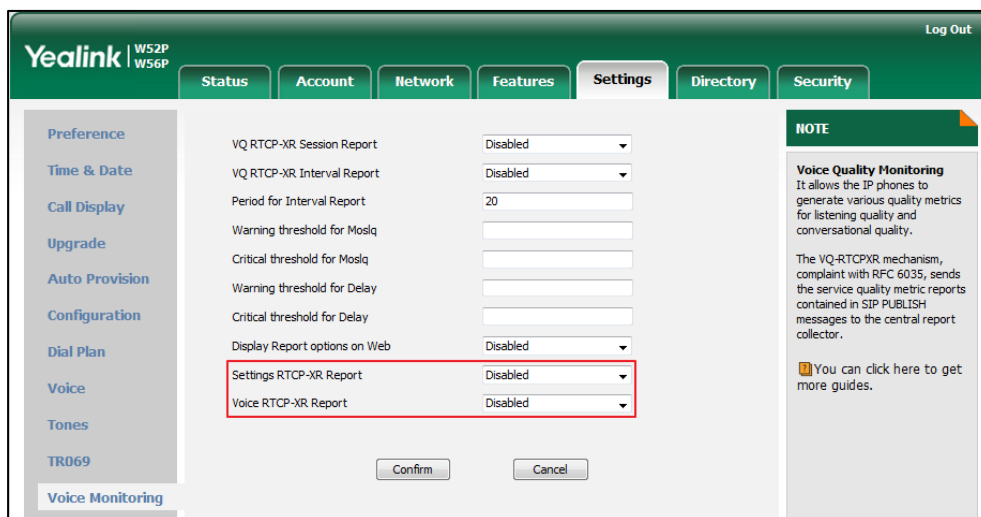
Parameters	Permitted Values	Default
<b>voice.rtcp_xr.enable</b>	<b>0 or 1</b>	<b>0</b>
<p><b>Description:</b></p> <p>Enables or disables the IP DECT phone to send RTCP-XR packets.</p> <p><b>0</b>-Disabled <b>1</b>-Enabled</p> <p><b>Note:</b> If you change this parameter, the IP DECT phone will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Settings-&gt;Voice Monitoring-&gt;Voice RTCP-XR Report</p> <p><b>Handset User Interface:</b> None</p>		
<b>phone_setting.rtcp_xr_report.enable</b>	<b>0 or 1</b>	<b>0</b>
<p><b>Description:</b></p> <p>Enables or disables the IP DECT phone to periodically (every 5 seconds) send RTCP-XR packets to another participating phone during a call for call quality monitoring and diagnosing.</p> <p><b>0</b>-Disabled <b>1</b>-Enabled</p> <p><b>Note:</b> It works only if the value of the parameter "voice.rtcp_xr.enable" is set to 1 (Enabled). If you change this parameter, the IP DECT phone will reboot to make the</p>		



Parameters	Permitted Values	Default
change take effect.		
<b>Web User Interface:</b>		
Settings->Voice Monitoring->Settings RTCP-XR Report		
<b>Handset User Interface:</b>		
None		

To configure RTCP-XR feature via web user interface:

1. Click on **Settings->Voice Monitoring**.
2. Select the desired value from the pull-down list of **Settings RTCP-XR Report**.
3. Select the desired value from the pull-down list of **Voice RTCP-XR Report**.



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

## VQ-RTCPXR

The VQ-RTCPXR mechanism, complaint with [RFC 6035](#), sends the service quality metric reports contained in SIP PUBLISH messages to the central report collector. Three types of quality reports can be enabled:

- **Session:** Generated at the end of a call.
- **Interval:** Generated during a call at a configurable period.
- **Alert:** Generated when the call quality degrades below a configurable threshold.

A wide range of performance metrics are generated in the following three ways:

- Based on current values, such as jitter, jitter buffer max and round trip delay.

- Covers the time period from the beginning of the call until the report is sent, such as network packet loss.
- Computed using other metrics as input, such as listening Mean Opinion Score (MOS-LQ) and conversational Mean Opinion Score (MOS-CQ).

To operate with central report collector, IP DECT phones must be configured to forward their voice quality reports to the specified report collector. You can specify the report collector on a per-line basis.

Users can check the voice quality data of the last call via web user interface or handset user interface. Users can also specify the options of the RTP status to be displayed on the handset user interface. Options of the RTP status to be displayed on the web user interface cannot be specified.

### Procedure

VQ-RTCPXR can be configured using the following methods.

<b>Configuration File</b>	y000000000025.cfg	Configure the generation of session packets. <b>Parameter:</b> phone_setting.vq_rtcpxr.session_report.enable
		Configure the generation of interval packets. <b>Parameters:</b> phone_setting.vq_rtcpxr.interval_report.enable phone_setting.vq_rtcpxr_interval_period
		Configure the generation of alert packets. <b>Parameters:</b> phone_setting.vq_rtcpxr_moslq_threshold_warning phone_setting.vq_rtcpxr_moslq_threshold_critical phone_setting.vq_rtcpxr_delay_threshold_warning phone_setting.vq_rtcpxr_delay_threshold_critical

		<p>Configure the phone to display RTP status showing the voice quality report of the last call on the web user interface.</p> <p><b>Parameter:</b></p> <p>phone_setting.vq_rtcpxr.states_show_on_web.enable</p>
	<MAC>.cfg	<p>Configure the central report collector.</p> <p><b>Parameters:</b></p> <p>account.X.vq_rtcpxr.collector_name  account.X.vq_rtcpxr.collector_server_host  account.X.vq_rtcpxr.collector_server_port</p>
Local	Web User Interface	<p>Configure VQ-RTCPXR.</p> <p>Configure the phone to display RTP status showing the voice quality report of the last call on the web user interface.</p> <p><b>Navigate to:</b></p> <p>http://&lt;phoneIPAddress&gt;/servlet?p=settings-voicemonitoring&amp;q=load</p>
		<p>Configure the central report collector.</p> <p><b>Navigate to:</b></p> <p>http://&lt;phoneIPAddress&gt;/servlet?p=account-adv&amp;q=load&amp;acc=0</p>

**Details of Configuration Parameters:**

Parameters	Permitted Values	Default
phone_setting.vq_rtcpxr.session_report.enable	0 or 1	0
<p><b>Description:</b></p> <p>Enables or disables the IP DECT phone to send a session quality report to the central report collector at the end of each call.</p> <p><b>0-Disabled</b></p> <p><b>1-Enabled</b></p> <p><b>Web User Interface:</b></p> <p>Settings-&gt;Voice Monitoring-&gt;VQ RTCP-XR Session Report</p> <p><b>Handset User Interface:</b></p> <p>None</p>		

Parameters	Permitted Values	Default
<b>phone_setting.vq_rtcpxr.interval_report.enable</b>	0 or 1	0
<p><b>Description:</b>                      Enables or disables the IP DECT phone to send an interval quality report to the central report collector periodically throughout a call.</p> <p>0-Disabled                      1-Enabled</p> <p><b>Web User Interface:</b>                      Settings-&gt;Voice Monitoring-&gt;VQ RTCP-XR Interval Report</p> <p><b>Handset User Interface:</b>                      None</p>		
<b>phone_setting.vq_rtcpxr_interval_period</b>	Integer from 5 to 20	20
<p><b>Description:</b>                      Configures the interval (in seconds) for the IP DECT phone to send an interval quality report to the central report collector periodically throughout a call.</p> <p><b>Note:</b> It works only if the value of the parameter "phone_setting.vq_rtcpxr.interval_report.enable" is set to 1 (Enabled).</p> <p><b>Web User Interface:</b>                      Settings-&gt;Voice Monitoring-&gt;Period for Interval Report</p> <p><b>Handset User Interface:</b>                      None</p>		
<b>phone_setting.vq_rtcpxr_moslq_threshold_warning</b>	15 to 40	Blank
<p><b>Description:</b>                      Configures the threshold value of listening MOS score (MOS-LQ) multiplied by 10. The threshold value of MOS-LQ causes the phone to send a warning alert quality report to the central report collector.</p> <p>For example, a configured value of 35 corresponds to the MOS score 3.5. When the MOS-LQ value computed by the phone is less than or equal to 3.5, the phone will send a warning alert quality report to the central report collector. When the MOS-LQ value computed by the phone is greater than 3.5, the phone will not send a warning alert quality report to the central report collector.</p> <p>If it is set to blank, warning alerts are not generated due to MOS-LQ.</p> <p><b>Web User Interface:</b>                      Settings-&gt;Voice Monitoring-&gt;Warning threshold for Moslq</p>		

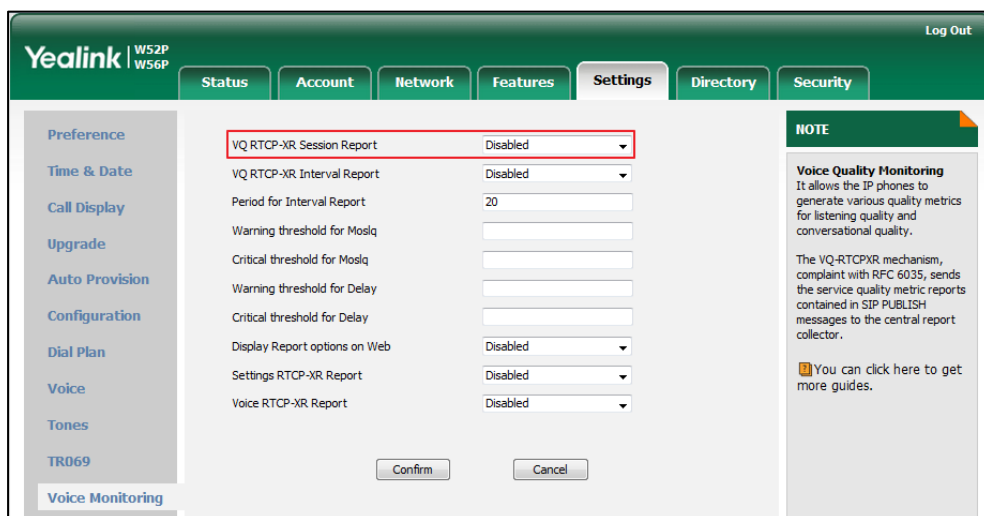
Parameters	Permitted Values	Default
<b>Handset User Interface:</b> None		
<b>phone_setting.vq_rtcpxr_moslq_threshold_critical</b>	<b>15 to 40</b>	<b>Blank</b>
<p><b>Description:</b> Configures the threshold value of listening MOS score (MOS-LQ) multiplied by 10. The threshold value of MOS-LQ causes the phone to send a critical alert quality report to the central report collector.</p> <p>For example, a configured value of 28 corresponds to the MOS score 2.8. When the MOS-LQ value computed by the phone is less than or equal to 2.8, the phone will send a critical alert quality report to the central report collector. When the MOS-LQ value computed by the phone is greater than 2.8, the phone will not send a critical alert quality report to the central report collector.</p> <p>If it is set to blank, critical alerts are not generated due to MOS-LQ.</p> <p><b>Web User Interface:</b> Settings-&gt;Voice Monitoring-&gt;Critical threshold for Moslq</p> <p><b>Handset User Interface:</b> None</p>		
<b>phone_setting.vq_rtcpxr_delay_threshold_warning</b>	<b>10 to 2000</b>	<b>Blank</b>
<p><b>Description:</b> Configures the threshold value of one way delay (in milliseconds) that causes the phone to send a warning alert quality report to the central report collector.</p> <p>For example, If it is set to 500, when the value of one way delay computed by the phone is greater than or equal to 500, the phone will send a warning alert quality report to the central report collector; when the value of one way delay computed by the phone is less than 500, the phone will not send a warning alert quality report to the central report collector.</p> <p>If it is set to blank, warning alerts are not generated due to one way delay. One-way delay includes both network delay and end system delay.</p> <p><b>Web User Interface:</b> Settings-&gt;Voice Monitoring-&gt;Warning threshold for Delay</p> <p><b>Handset User Interface:</b> None</p>		
<b>phone_setting.vq_rtcpxr_delay_threshold_critical</b>	<b>10 to 2000</b>	<b>Blank</b>

Parameters	Permitted Values	Default
<p><b>Description:</b>                      Configures the threshold value of one way delay (in milliseconds) that causes phone to send a critical alert quality report to the central report collector.                      For example, If it is set to 500, when the value of one way delay computed by the phone is greater than or equal to 500, the phone will send a critical alert quality report to the central report collector; when the value of one way delay computed by the phone is less than 500, the phone will not send a critical alert quality report to the central report collector.                      If it is set to blank, critical alerts are not generated due to one way delay. One-way delay includes both network delay and end system delay.</p> <p><b>Web User Interface:</b>                      Settings-&gt;Voice Monitoring-&gt;Critical threshold for Delay</p> <p><b>Handset User Interface:</b>                      None</p>		
<p><b>phone_setting.vq_rtcp.rstates_show_on_web.enable</b></p>	<p>0 or 1</p>	<p>0</p>
<p><b>Description:</b>                      Enables or disables the voice quality data of the last call to be displayed on web interface at path <b>Status-&gt;RTP Status</b>.                      0-Disabled                      1-Enabled</p> <p><b>Web User Interface:</b>                      Settings-&gt;Voice Monitoring-&gt;Display Report options on Web</p> <p><b>Handset User Interface:</b>                      None</p>		
<p><b>account.X.vq_rtcp.collector_name</b>                      (X ranges from 1 to 5)</p>	<p>String within 32 characters</p>	<p>Blank</p>
<p><b>Description:</b>                      Configures the host name of the central report collector that accepts voice quality reports contained in SIP PUBLISH messages for account X.</p> <p><b>Web User Interface:</b>                      Account-&gt;Advanced-&gt;VQ RTCP-XR Collector name</p> <p><b>Handset User Interface:</b>                      None</p>		

Parameters	Permitted Values	Default
<b>account.X.vq_rtcpxr.collector_server_host</b> (X ranges from 1 to 5)	IPv4 address	Blank
<p><b>Description:</b>                      Configures the IP address of the central report collector that accepts voice quality reports contained in SIP PUBLISH messages for account X.</p> <p><b>Web User Interface:</b>                      Account-&gt;Advanced-&gt;VQ RTCP-XR Collector address</p> <p><b>Handset User Interface:</b>                      None</p>		
<b>account.X.vq_rtcpxr.collector_server_port</b> (X ranges from 1 to 5)	Integer from 1 to 65535	5060
<p><b>Description:</b>                      Configures the port of the central report collector that accepts voice quality reports contained in SIP PUBLISH messages for account X.</p> <p><b>Web User Interface:</b>                      Account-&gt;Advanced-&gt;VQ RTCP-XR Collector port</p> <p><b>Handset User Interface:</b>                      None</p>		

To configure session report for VQ-RTCPXR via web user interface:

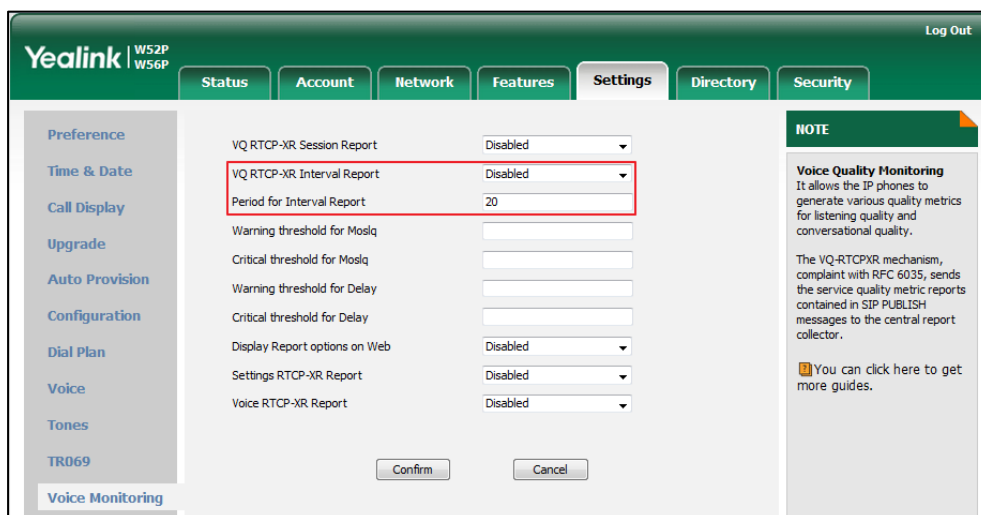
1. Click on **Settings->Voice Monitoring**.
2. Select the desired value from the pull-down list of **VQ RTCP-XR Session Report**.



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

To configure interval report for VQ-RTCPXR via web user interface:

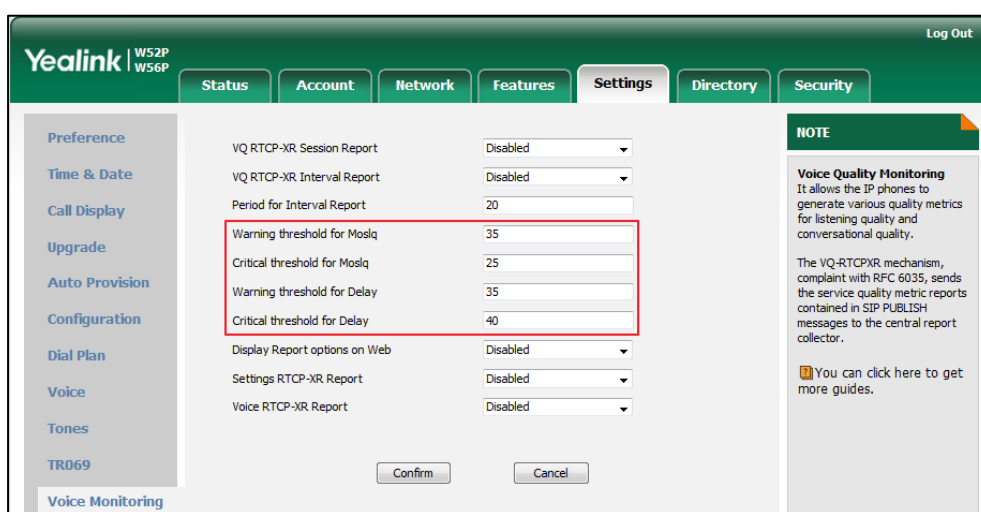
1. Click on **Settings->Voice Monitoring**.
2. Select the desired value from the pull-down list of **VQ RTCP-XR Interval Report**.
3. Enter the desired value in the **Period for Interval Report** field.



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

To configure alert report for VQ-RTCPXR via web user interface:

1. Click on **Settings->Voice Monitoring**.
2. Enter the desired value in the **Warning threshold for Moslq** field.
3. Enter the desired value in the **Critical threshold for Moslq** field.
4. Enter the desired value in the **Warning threshold for Delay** field.
5. Enter the desired value in the **Critical threshold for Delay** field.

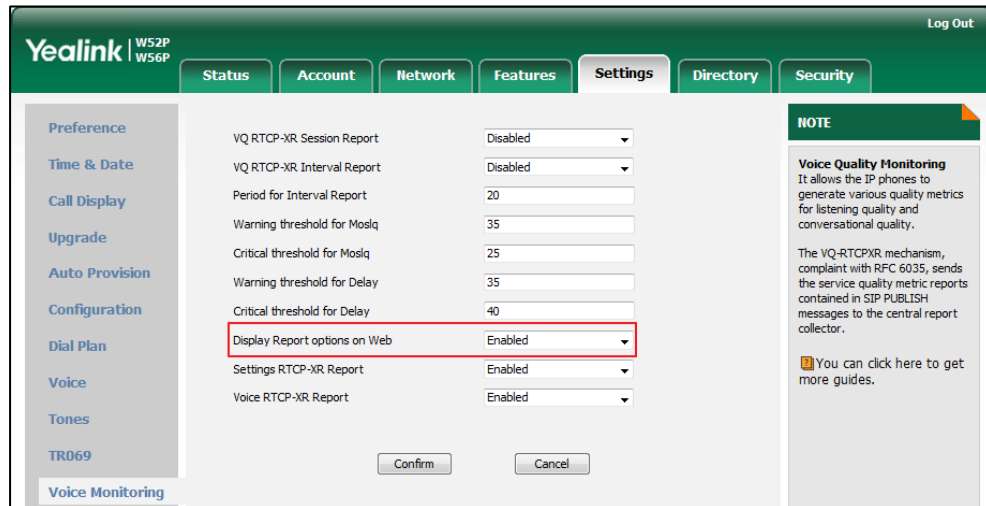


6. Click **Confirm** to accept the change.



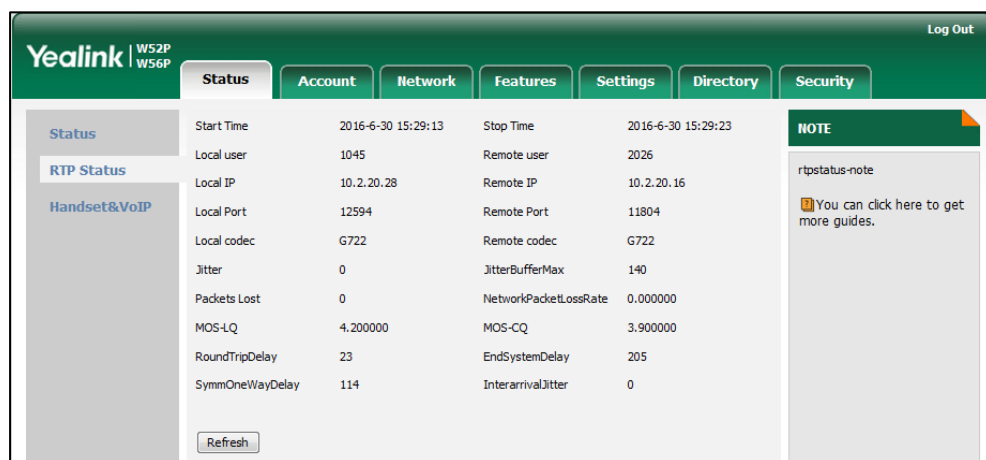
To configure RTP status displayed on the web page via web user interface:

1. Click on **Settings->Voice Monitoring**.
2. Select the desired value from the pull-down list of **Display Report options on Web**.



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

The RTP status will appear on the web user interface at the path: **Status->RTP Status**.



To configure the central report collector via web user interface:

1. Click on **Account->Advanced**.
2. Select the desired account from the pull-down list of **Account**.
3. Enter the host name of the central report collector in the **VQ RTPC-XR Collector name** field.
4. Enter the IP address of the central report collector in the **VQ RTPC-XR Collector address** field.

- Enter the port of the central report collector in the **VQ RTCP-XR Collector port** field.

The screenshot shows the 'Account' settings page for a Yealink W52P/W56P phone. The 'VQ RTCP-XR Collector port' field is highlighted with a red box and contains the value '5060'. The interface includes a navigation menu on the left, a top status bar with 'Log Out', and a 'NOTE' section on the right with technical details about DTMF, Session Timer, Shared Call Appearance (SCA)/ Bridge Line Appearance (BLA), Network Conference, and VQ-RTCPXR.

Field	Value
Account	Account 1
Keep Alive Type	Default
Keep Alive Interval(Seconds)	30
Send user=phone	Disabled
RTP Encryption(SRTP)	Disabled
PTime(ms)	20
Shared Line	Disabled
SIP Send MAC	Enabled
SIP Send Line	Enabled
SIP Registration Retry Timer(0~1800s)	30
Conference Type	Local Conference
Conference URI	
SIP Server Type	Default
Unregister When Reboot	Enabled
VQ RTCP-XR Collector name	
VQ RTCP-XR Collector address	
VQ RTCP-XR Collector port	5060

**NOTE**

**DTMF**  
It is the signal sent from the IP phone to the network, which is generated when pressing the IP phone's keypad during a call.

**Session Timer**  
It allows a periodic refresh of SIP sessions through a re-INVITE request, to determine whether a SIP session is still active.

**Shared Call Appearance (SCA)/ Bridge Line Appearance (BLA)**  
It allows users to share a SIP line on several IP phones. Any IP phone can be used to originate or receive calls on the shared line.

**Network Conference**  
It allows multiple participants (more than three) to join in a call.

**VQ-RTCPXR**  
The VQ-RTCPXR mechanism, compliant with RFC 6035, sends the service quality metric reports contained in SIP PUBLISH messages to the central report collector.

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

# Configuring Security Features

This chapter provides information for making configuration changes for the following security-related features:

- [User Password](#)
- [Administrator Password](#)
- [Auto-Logout Time](#)
- [Base PIN](#)
- [Emergency Number](#)
- [Transport Layer Security](#)
- [Secure Real-Time Transport Protocol](#)
- [Encrypting Configuration Files](#)

## 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 administrator should change the default user password as soon as possible.

### Procedure

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

<b>Configuration File</b>	y000000000025.cfg	Change the user password of the IP DECT phone. <b>Parameter:</b> security.user_password
<b>Local</b>	Web User Interface	Change the user password of the IP DECT phone. <b>Navigate to:</b> <a href="http://&lt;phoneIPAddress&gt;/servlet?p=security&amp;q=load">http://&lt;phoneIPAddress&gt;/servlet?p=security&amp;q=load</a>

### Details of the Configuration Parameter:

Parameter	Permitted Values	Default
security.user_password	String within 32 characters	user

**Description:**  
 Configures the password of the user for phone's web user interface access.  
 The IP DECT phone uses "user" as the default user password.  
 The valid value format is username: new password.

**Example:**  
 security.user\_password = user: 123 means setting the password of user (current user name is "user") to password 123.

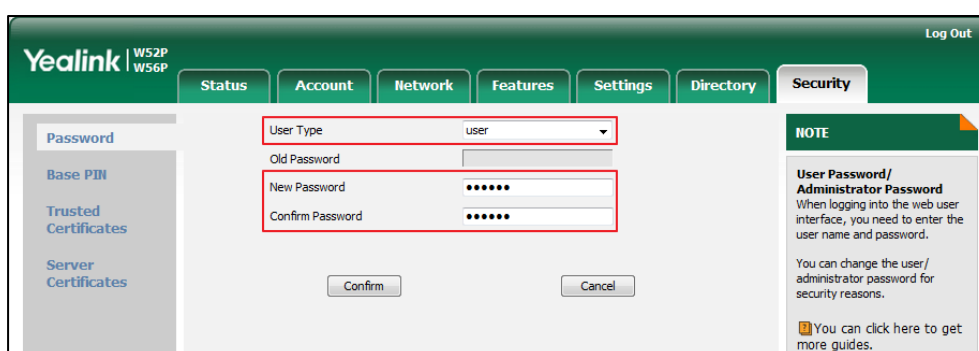
**Note:** The IP DECT phones support ASCII characters 32-126(0x20-0x7E) in passwords. You can set the password to be empty via web user interface only.

**Web User Interface:**  
 Security->Password

**Handset User Interface:**  
 None

#### 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 new password in the **New Password** and **Confirm Password** fields.  
 Valid characters are ASCII characters 32-126(0x20-0x7E) except 58(3A).



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

**Note** If logging into the web user interface of the phone with the user credential, you need to enter the old 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.

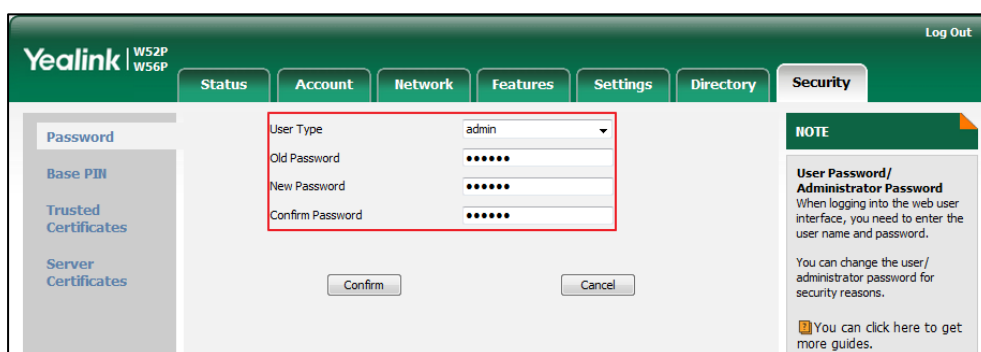
<b>Configuration File</b>	y000000000025.cfg	Change the administrator password. <b>Parameter:</b> security.user_password
<b>Local</b>	Web User Interface	Change the administrator password. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=security&q=load

### Details of the Configuration Parameter:

Parameter	Permitted Values	Default
security.user_password	String within 32 characters	admin
<p><b>Description:</b> Configures the password of the administrator for phone’s web user interface access. The IP DECT phone uses “admin” as the default administrator password.</p> <p><b>Example:</b> security.user_password = admin: 123 means setting the password of administrator (current user name is “admin”) to password 123.</p> <p><b>Note:</b> The IP DECT phones support ASCII characters 32-126(0x20-0x7E) in passwords. You can set the password to be empty via web user interface only.</p> <p><b>Web User Interface:</b> Security-&gt;Password</p> <p><b>Handset User Interface:</b> None</p>		

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 new password in the **New Password** and **Confirm Password** fields.  
Valid characters are ASCII characters 32-126 (0x20-0x7E) except 58 (3A).



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

## Auto-Logout Time

Auto-logout time defines a specific period of time during which the IP DECT phones will automatically log out if you have not performed any actions via web user interface. Once logging out, you must re-enter username and password for web access authentication.

### Procedure

Auto-logout time can be configured using the configuration files or locally.

<b>Configuration File</b>	y00000000025.cfg	Configure auto-logout time. <b>Parameter:</b> features.relog_offtime
<b>Local</b>	Web User Interface	Configure auto-logout time. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=features-general&q=load

**Details of the Configuration Parameter:**

Parameter	Permitted Values	Default
features.relog_offtime	Integer from 1 to 1000	5

**Description:**  
Configures the timeout interval (in minutes) for web access authentication.

**Example:**  
features.relog\_offtime = 5  
If you log into the web user interface and leave it for 5 minutes, it will automatically log out.

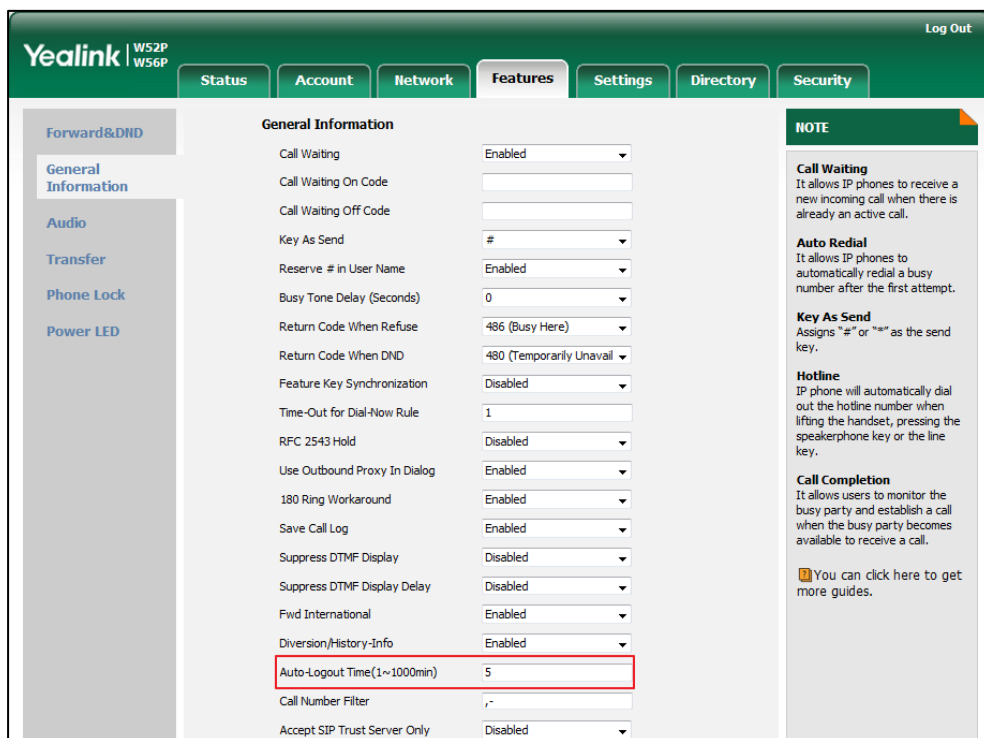
**Note:** If you change this parameter, the base station will reboot to make the change take effect.

**Web User Interface:**  
Features->General Information->Auto-Logout Timeout(1~1000min)

**Handset User Interface:**  
None

**To configure the auto-logout time via web user interface:**

1. Click on **Features->General Information**.
2. Enter the desired auto-logout time in **Auto-Logout Time(1~1000min)** field.



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

## Base PIN

Base PIN is used to lock the IP DECT phone to prevent it from unauthorized use. For menu options, a user must enter the base PIN to unlock it.

### Procedure

Base PIN can be configured using the configuration files or locally.

<b>Configuration File</b>	y000000000025.cfg	Change the base PIN. <b>Parameter:</b> base.pin_code
<b>Local</b>	Web User Interface	Change the base PIN. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=security-base-pin&q=load
	Handset User Interface	Change the base PIN.

### Details of Configuration Parameters:

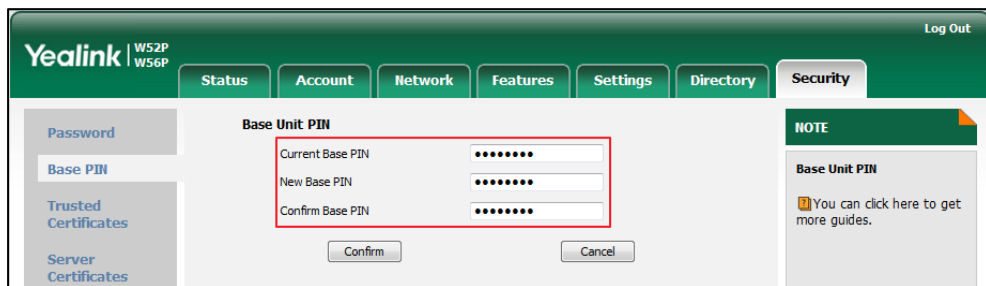
Parameters	Permitted Values	Default
<b>base.pin_code</b>	<b>Integer from 0 to 9999</b>	<b>0000</b>
<p><b>Description:</b> Configures the system PIN of the base station.</p> <p><b>Web User Interface:</b> Security-&gt;Base PIN-&gt;Base Unit PIN</p> <p><b>Handset User Interface:</b> OK-&gt;Settings-&gt;System Settings-&gt;Change Base PIN</p>		

### To configure base PIN via web user interface:

1. Click on **Security->Base PIN**.
2. Enter the current base PIN in the **Current Base PIN** field.



3. Enter new base PIN in the **New Base PIN** and **Confirm Base PIN** fields.



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

**To configure base PIN via handset user interface:**

1. Press **OK** to enter the main menu.
2. Select **Settings->System Settings->Change Base PIN**.
3. Enter the system PIN (default: 0000), and then press the **Done** soft key.
4. Enter the new PIN in the **Enter New PIN** and **Re-enter New PIN** field respectively.
5. Press the **Save** soft key to accept the change.

## Emergency Number

Public telephone networks in countries around the world have a single emergency telephone number (emergency services number), that allows a caller to contact local emergency services for assistance when necessary.

You can specify the emergency numbers for contacting the emergency services in an emergency situation. The emergency telephone number may differ from country to country. It is typically a three-digit number so that it can be easily remembered and dialed quickly. You can dial these numbers when the phone is locked.

### Procedure

Emergency number can be configured using the configuration files or locally.

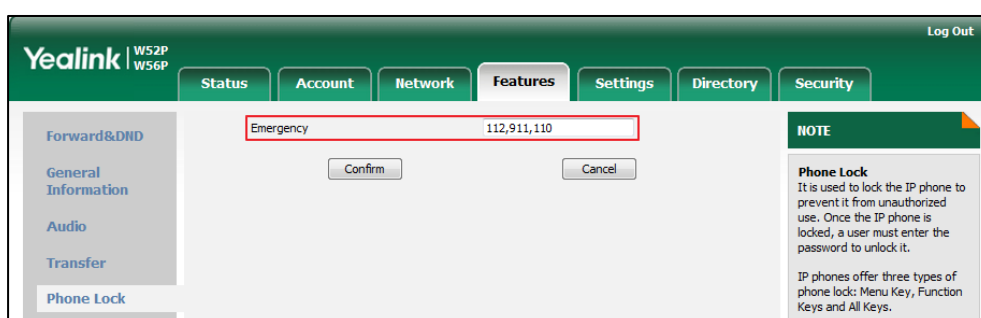
<b>Configuration File</b>	y000000000025.cfg	Configure emergency numbers. <b>Parameter:</b> phone_setting.emergency.number
<b>Local</b>	Web User Interface	Configure emergency numbers. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p= =features-phonelock&q=load

### Details of Configuration Parameters:

Parameters	Permitted Values	Default
phone_setting.emergency.number	String within 99 characters	Blank
<p><b>Description:</b> Configures emergency numbers. Multiple emergency numbers are separated by commas.</p> <p><b>Web User Interface:</b> Features-&gt;Phone Lock-&gt;Emergency</p> <p><b>Handset User Interface:</b> None</p>		

To configure emergency numbers via web user interface:

1. Click on **Features->Phone Lock**.
2. Enter the emergency number in the **Emergency** field.



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

## Transport Layer Security

TLS is a commonly-used protocol for providing communications privacy and managing the security of message transmission, allowing IP DECT 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.

The IP DECT phones support TLS version 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. The IP DECT 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 DECT 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: rnmserver (2244), Seq: 1482, Ack: 437, Len: 586  
 Secure Socket Layer

**Step1:** The IP DECT 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 DECT 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.

The IP DECT 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 appears on the LCD screen after the successful TLS negotiation.

## Certificates

The IP DECT 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 DECT phone requests a TLS connection with a server, the IP DECT phone should verify the certificate sent by the server to decide whether it is trusted based on the trusted certificates list. The IP DECT phone has 30 built-in trusted certificates. You can upload 10 custom certificates at most. The format of the trusted certificate files must be \*.pem, \*.cer, \*.crt and \*.der and the maximum file size is 5MB. For more information on 30 trusted certificates, refer to [Appendix C: Trusted Certificates](#) on page 406.
- **Server Certificate:** When clients request a TLS connection with the IP DECT phone, the IP DECT phone sends the server certificate to the clients for authentication. The IP DECT 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 DECT phone. The old server certificate will be overridden by the new one. The format of the server certificate files must be \*.pem and \*.cer and the maximum file size is 5MB.

- **A unique server certificate:** It is unique to an IP DECT phone (based on the MAC address) and issued by the Yealink Certificate Authority (CA).
- **A generic server certificate:** It issued by the Yealink Certificate Authority (CA). Only if no unique certificate exists, the IP DECT phone may send a generic certificate for authentication.

The IP DECT 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 DECT phone accepts: default certificates, custom certificates or all certificates.

Common Name Validation feature enables the IP DECT phone to mandatorily validate the common name of the certificate sent by the connecting server. And Security verification rules are compliant with RFC 2818.

**Note**

In TLS feature, we use the terms trusted and server certificate. These are also known as CA and device certificates.

Resetting the W56P IP DECT phone to factory defaults will delete custom certificates by default. But this feature is configurable using the configuration files. For more information on the configuration parameter, refer to [Transport Layer Security](#) on page 350.

**Procedure**

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

<b>Configuration File</b>	y00000000025.cfg	Configure TLS on a per-line basis. <b>Parameter:</b> account.X.sip_server.Y.transport_type
		Configure trusted certificates feature. <b>Parameters:</b> security.trust_certificates security.ca_cert security.cn_validation
		Configure server certificates feature. <b>Parameters:</b> security.dev_cert
		Upload the trusted certificates. <b>Parameter:</b> trusted_certificates.url

		<p>Delete all uploaded trusted certificates.</p> <p><b>Parameter:</b> trusted_certificates.delete</p>
		<p>Upload the server certificates.</p> <p><b>Parameter:</b> server_certificates.url</p>
		<p>Delete all uploaded server certificates.</p> <p><b>Parameter:</b> server_certificates.delete</p>
Local	Web User Interface	<p>Configure TLS on a per-line basis.</p> <p><b>Navigate to:</b> http://&lt;phoneIPAddress&gt;/servlet?parameter=account-register&amp;q=load&amp;acc=0</p>
		<p>Configure trusted certificates feature.</p> <p>Upload the trusted certificates.</p> <p><b>Navigate to:</b> http://&lt;phoneIPAddress&gt;/servlet?parameter=security-trusted-certs&amp;q=load</p>
		<p>Configure server certificates feature.</p> <p>Upload the server certificates.</p> <p><b>Navigate to:</b> http://&lt;phoneIPAddress&gt;/servlet?parameter=security-server-certs&amp;q=load</p>

**Details of Configuration Parameters:**

Parameters	Permitted Values	Default
<p><b>account.X.sip_server.Y.transport_type</b> (X ranges from 1 to 5, Y ranges from 1 to 2)</p>	0,1,2 or 3	0
<p><b>Description:</b> Configures the type of transport protocol for account X.</p> <p><b>0-UDP</b> <b>1-TCP</b></p>		

Parameters	Permitted Values	Default
<p>2-TLS 3-DNS-NAPTR</p> <p><b>Web User Interface:</b> Account-&gt;Register-&gt;SIP Server Y-&gt;Transport</p> <p><b>Handset User Interface:</b> None</p>		
<p><b>security.trust_certificates</b></p>	<p><b>0 or 1</b></p>	<p><b>1</b></p>
<p><b>Description:</b> Enables or disables the IP DECT phone to only trust the server certificates in the Trusted Certificates list.</p> <p><b>0-Disabled</b> <b>1-Enabled</b></p> <p>If it is set to 0 (Disabled), the IP DECT phone will trust the server no matter whether the certificate sent by the server is valid or not.</p> <p>If it is set to 1 (Enabled), the IP DECT phone will authenticate the server certificate based on the trusted certificates list. Only when the authentication succeeds, the IP DECT phone will trust the server.</p> <p><b>Note:</b> If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Security-&gt;Trusted Certificates-&gt;Only Accept Trusted Certificates</p> <p><b>Handset User Interface:</b> None</p>		
<p><b>security.ca_cert</b></p>	<p><b>0, 1 or 2</b></p>	<p><b>2</b></p>
<p><b>Description:</b> Configures the type of certificates in the Trusted Certificates list for the IP DECT phone to authenticate for TLS connection.</p> <p><b>0-Default Certificates</b> <b>1-Custom Certificates</b> <b>2-All Certificates</b></p> <p><b>Note:</b> If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Security-&gt;Trusted Certificates-&gt;CA Certificates</p>		

Parameters	Permitted Values	Default
<b>Handset User Interface:</b> None		
<b>security.cn_validation</b>	0 or 1	0
<b>Description:</b> Enables or disables the IP DECT phone to mandatorily validate the CommonName or SubjectAltName of the certificate sent by the server. 0-Disabled 1-Enabled <b>Note:</b> If you change this parameter, the base station will reboot to make the change take effect. <b>Web User Interface:</b> Security->Trusted Certificates->Common Name Validation <b>Handset User Interface:</b> None		
<b>security.dev_cert</b>	0 or 1	0
<b>Description:</b> Configures the type of the device certificates for the IP DECT phone to send for TLS authentication. 0-Default Certificates 1-Custom Certificates <b>Note:</b> If you change this parameter, the base station will reboot to make the change take effect. <b>Web User Interface:</b> Security->Server Certificates->Device Certificates <b>Handset User Interface:</b> None		
<b>trusted_certificates.url</b>	URL within 511 characters	Blank
<b>Description:</b> Configures the access URL of the custom trusted certificate used to authenticate the connecting server. <b>Example:</b> trusted_certificates.url = http://192.168.1.20/tc.crt		

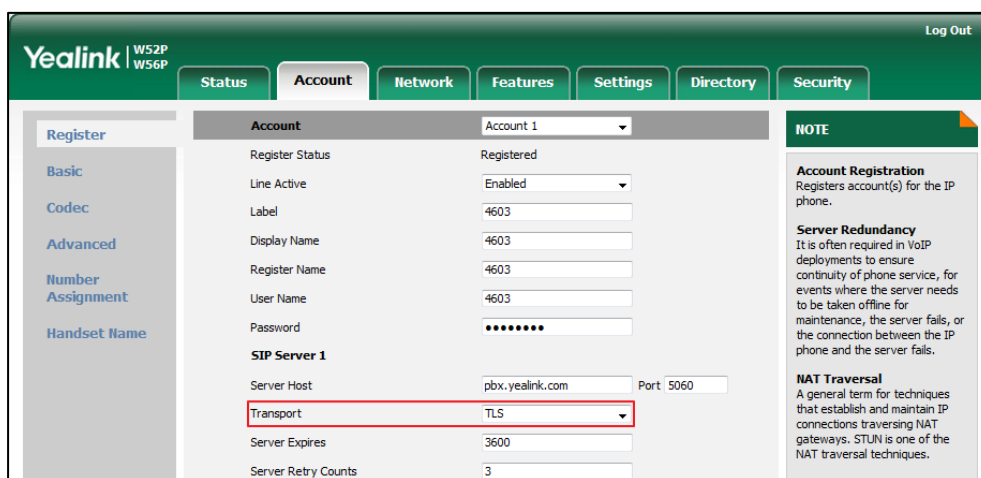


Parameters	Permitted Values	Default
<p><b>Note:</b> The certificate you want to upload must be in *.pem, *.crt, *.cer or *.der format.</p> <p><b>Web User Interface:</b> Security-&gt;Trusted Certificates-&gt;Load trusted certificates file</p> <p><b>Handset User Interface:</b> None</p>		
trusted_certificates.delete	http://localhost/all	Blank
<p><b>Description:</b> Deletes all uploaded trusted certificates.</p> <p><b>Example:</b> trusted_certificates.delete = http://localhost/all</p> <p><b>Web User Interface:</b> None</p> <p><b>Handset User Interface:</b> None</p>		
server_certificates.url	URL within 511 characters	Blank
<p><b>Description:</b> Configures the access URL of the certificate the IP DECT phone sends for authentication.</p> <p><b>Example:</b> server_certificates.url = http://192.168.1.20/ca.pem.</p> <p><b>Note:</b> The certificate you want to upload must be in *.pem or *.cer format.</p> <p><b>Web User Interface:</b> Security-&gt;Server Certificates-&gt;Load server cer file</p> <p><b>Handset User Interface:</b> None</p>		
server_certificates.delete	http://localhost/all	Blank
<p><b>Description:</b> Deletes all uploaded server certificates.</p> <p><b>Example:</b> server_certificates.delete = http://localhost/all</p> <p><b>Web User Interface:</b></p>		

Parameters	Permitted Values	Default
None		
<b>Handset User Interface:</b>		
None		

To configure TLS on a per-line basis via web user interface:

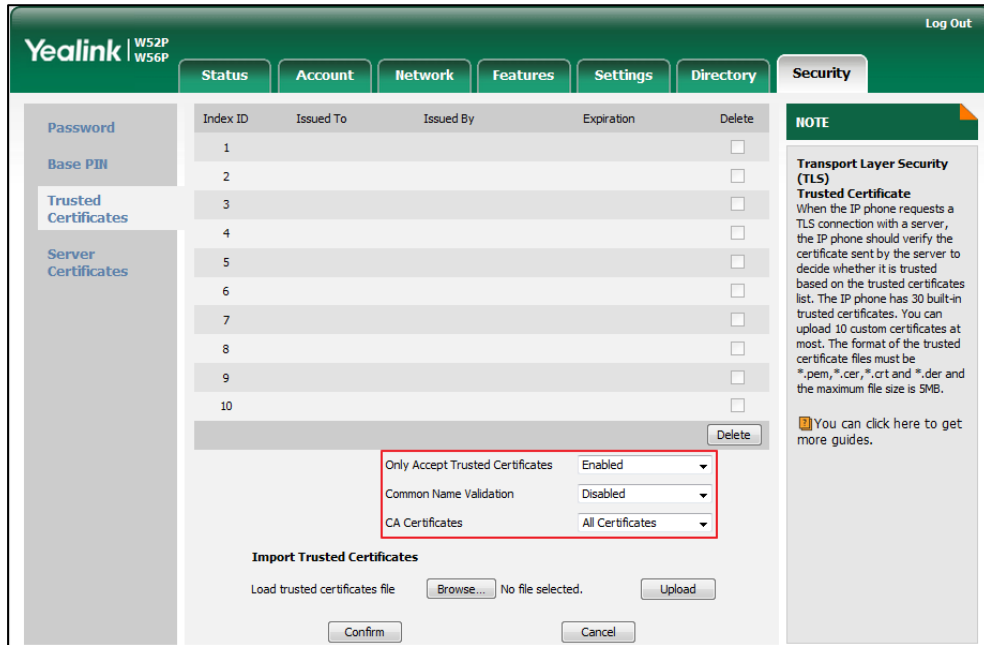
1. Click on **Account->Register**.
2. Select the desired account from the pull-down list of **Account**.
3. Select **TLS** from the pull-down list of **Transport**.



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

To configure the trusted certificates via web user interface:

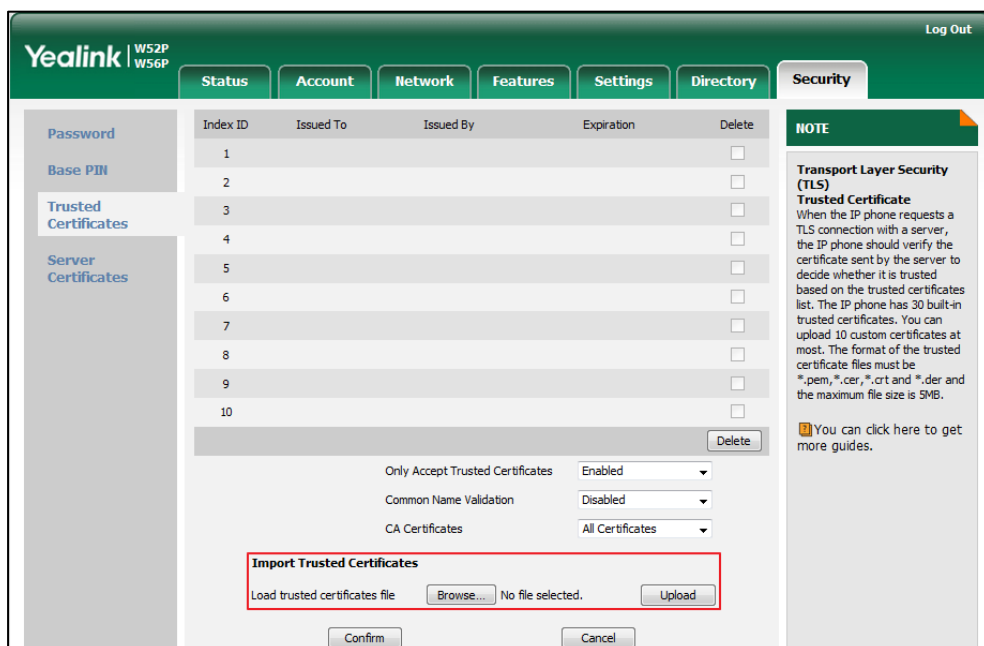
1. Click on **Security->Trusted Certificates**.
2. Select the desired values from the pull-down lists of **Only Accept Trusted Certificates**, **Common Name Validation** and **CA Certificates**.



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

To upload a trusted certificate via web user interface:

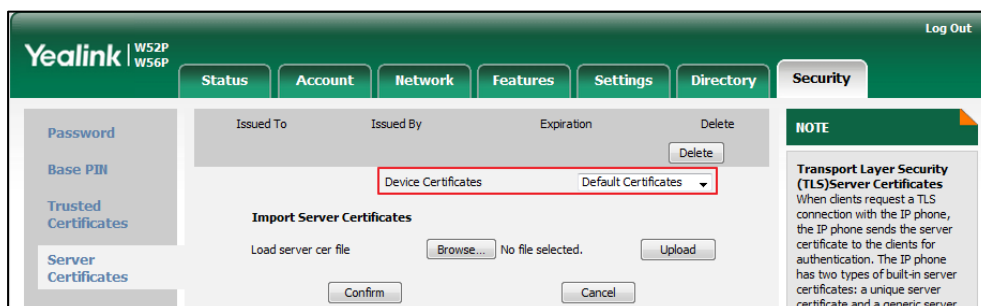
1. Click on **Security->Trusted Certificates**.
2. Click **Browse** to select the certificate (\*.pem, \*.cert, \*.cer or \*.der) from your local system.



3. Click **Upload** to upload the certificate.

To configure the server certificates via web user interface:

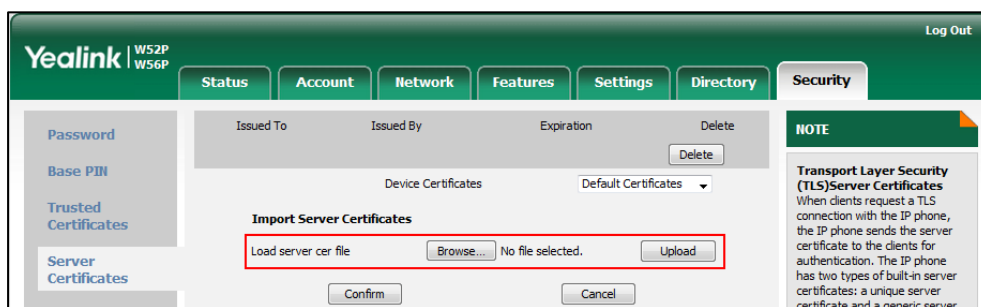
1. Click on **Security->Server Certificates**.
2. Select the desired value from the pull-down list of **Device Certificates**.



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

To upload a server certificate via web user interface:

1. Click on **Security->Server Certificates**.
2. Click **Browse** to select the certificate (\*.pem and \*.cer) from your local system.



3. Click **Upload** to upload the certificate.

A 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 the RTP during IP DECT phone calls to avoid interception and eavesdropping. The parties participating in the call must enable SRTP feature simultaneously. When this feature is enabled on both phones, the type of encryption to utilize for the session is negotiated between the IP DECT phones. This negotiation process is compliant with [RFC 4568](#).

When a user places a call on the enabled SRTP phone, the IP DECT phone sends an INVITE message with the RTP encryption algorithm to the destination phone. As described in [RFC 3711](#), RTP streams may be encrypted using an AES (advanced encryption standard) algorithm.

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:NzFINTUwZDk2OGVIOTc3YzNkYTkWZWVMTM1YWFj
a=crypto:2 AES_CM_128_HMAC_SHA1_32
inline:NzkyM2FjNzQ2ZDgxYjg0MzQwMGVmMGUxMzdmNWFm
a=crypto:3 F8_128_HMAC_SHA1_80 inline:NDIiMWizZGE1ZTAwZjA5ZGFhNjQ5YmEANTMzYzA0
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 is configurable on a per-line basis. When SRTP is enabled on both IP DECT phones, RTP streams will be encrypted, and a lock icon appears on the LCD screen of each IP DECT 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 350.

## Procedure

SRTP can be configured using the configuration files or locally.

<b>Configuration File</b>	<MAC>.cfg	Configure SRTP feature on a per-line basis. <b>Parameter:</b> account.X.srtp_encryption
<b>Local</b>	Web User Interface	Configure SRTP feature on a per-line basis. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

### Details of the Configuration Parameter:

Parameters	Permitted Values	Default
<b>account.X.srtp_encryption</b> (X ranges from 1 to 5)	<b>0, 1 or 2</b>	<b>0</b>
<p><b>Description:</b> Configures whether to use voice encryption service for account X.</p> <p><b>0-Disabled</b> <b>1-Optional</b> <b>2-Compulsory</b></p> <p>If it is set to 1 (Optional), the IP DECT phone will negotiate with the other IP DECT phone what type of encryption to utilize for the session.</p> <p>If it is set to 2 (Compulsory), the IP DECT phone is forced to use SRTP during a call.</p> <p><b>Web User Interface:</b> Account-&gt;Advanced-&gt;RTP Encryption(SRTP)</p> <p><b>Handset User Interface:</b> None</p>		

#### To configure SRTP feature via web user interface:

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

3. Select the desired value from the pull-down list of **RTP Encryption(SRTP)**.

The screenshot shows the Yealink configuration web interface for a W52P/W56P device. The 'Account' tab is selected, and the 'Account 1' configuration page is displayed. The 'RTP Encryption(SRTP)' option is highlighted with a red box and is currently set to 'Disabled'. Other settings include 'Keep Alive Type' (Default), 'Keep Alive Interval(Seconds)' (30), 'Send user=phone' (Disabled), 'PTime(ms)' (20), 'Shared Line' (Disabled), 'SIP Send MAC' (Enabled), 'SIP Send Line' (Enabled), 'SIP Registration Retry Timer(0~1800s)' (30), 'Conference Type' (Local Conference), 'Conference URI' (empty), 'SIP Server Type' (Default), 'Unregister When Reboot' (Enabled), 'VQ RTPC-XR Collector name' (empty), 'VQ RTPC-XR Collector address' (empty), and 'VQ RTPC-XR Collector port' (5060). A 'NOTE' section on the right provides information about DTMF, Session Timer, Shared Call Appearance (SCA)/ Bridge Line Appearance (BLA), Network Conference, and VQ-RTCPXR.

4. 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 supplies a configuration encryption tool for encrypting configuration files. The encryption tool encrypts plaintext y00000000025.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 DECT phone, and generates new files named as <xx\_Security>.enc (xx indicates the name of the configuration file, for example, y00000000025\_Security.enc for y00000000025.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 y00000000025.cfg and <MAC>.cfg file respectively.

**Note** Yealink also supplies a configuration encryption tool (yealinkencrypt) for Linux platform if required. For more information, refer to [Yealink Configuration Encryption Tool User Guide](#).

For security reasons, administrator should upload encrypted configuration files, <y00000000025\_Security>.enc and or <MAC\_Security>.enc files to the root directory of the provisioning server. During auto provisioning, the IP DECT phone requests to download y00000000025.cfg file first. If the downloaded configuration file is encrypted, the IP DECT phone will request to download <y00000000025\_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 DECT phone decrypts y00000000025.cfg file using key2. After decryption, the IP DECT phone resolves configuration files and updates configuration settings onto the IP DECT phone system.

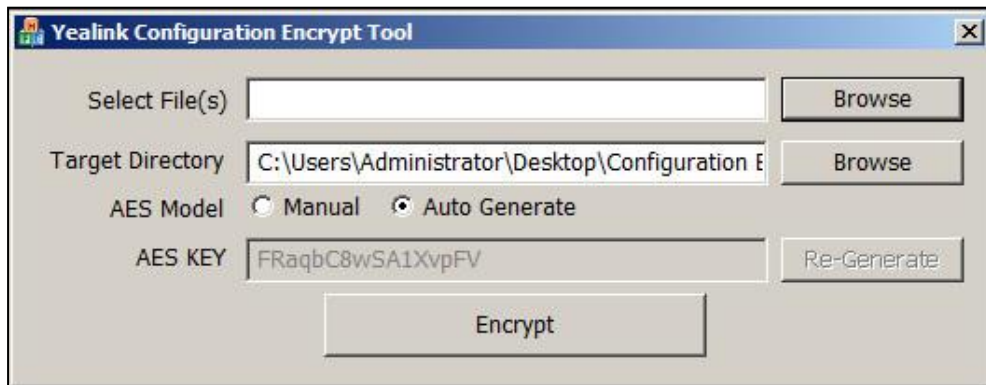
The way the IP DECT phone processes the <MAC>.cfg file is the same to that of the y00000000025.cfg file.

### Procedure to Encrypt Configuration Files

To encrypt the y00000000025.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., y00000000025.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.

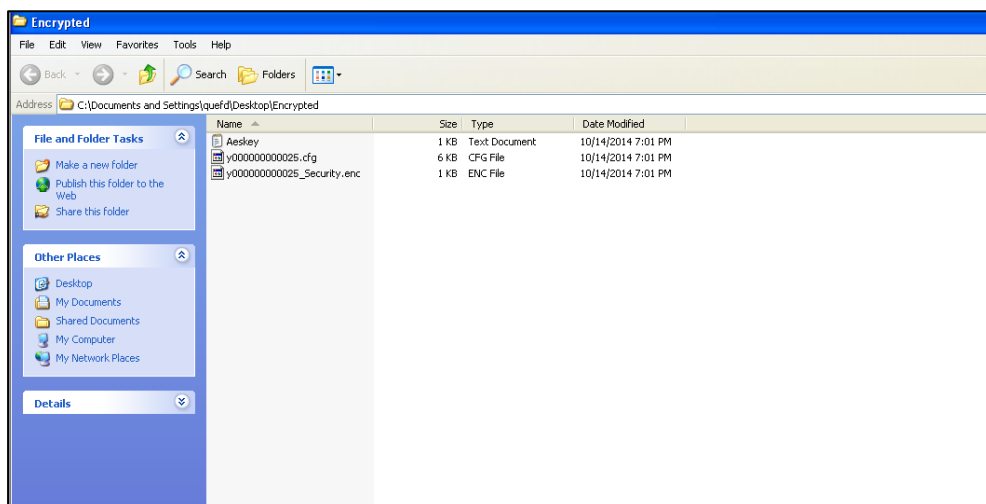
**Note** AES keys must be 16 characters and the supported characters contain: 0 ~ 9, A ~ Z, a ~ z and the following special characters are also supported: # \$ % \* + , - . : = ? @ [ ] ^ \_ { } ~ .

5. Click **Encrypt** to encrypt the configuration file(s).



6. Click **OK**.

The target directory will be automatically opened. You can find the encrypted CFG file(s), encrypted key file(s) and an Aeskey.txt file storing plaintext AES key(s).



### Procedure

Decryption method can be configured using the configuration files.

<b>Configuration File</b>	y000000000025.cfg	Configure the decryption method. <b>Parameter:</b> auto_provision.aes_key_in_file
		Configure AES keys. <b>Parameters:</b>

		auto_provision.aes_key_16.com auto_provision.aes_key_16.mac
<b>Local</b>	Web User Interface	Configure AES keys. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p =settings-autop&q=load

**Details of Configuration Parameters:**

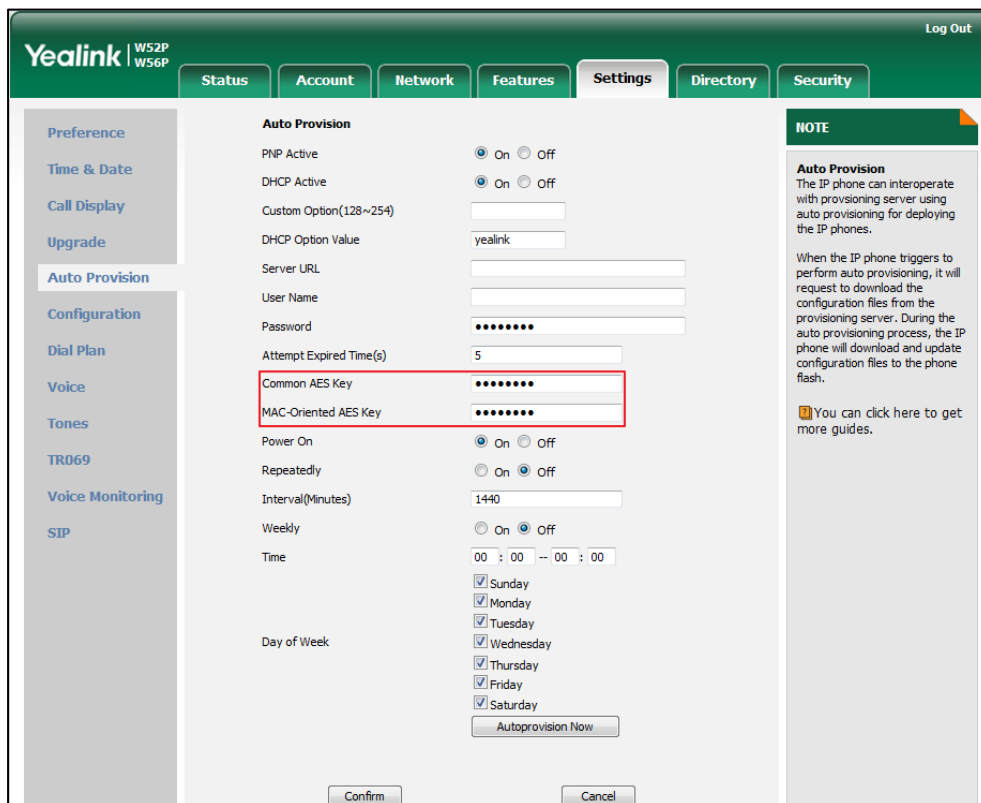
Parameters	Permitted Values	Default
<b>auto_provision.aes_key_in_file</b>	<b>0 or 1</b>	<b>0</b>
<p><b>Description:</b> Enables or disables the IP DECT phone to decrypt configuration files using the encrypted AES keys.</p> <p><b>0-Disabled</b> <b>1-Enabled</b></p> <p>If it is set to 1 (Enabled), the IP DECT phone will download &lt;y00000000025_Security&gt;.enc and &lt;MAC_Security&gt;.enc files during auto provisioning, and then decrypts these files into the plaintext keys (e.g., key2, key3) respectively using the phone built-in key (e.g., key1). The IP DECT 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 DECT phone will decrypt the encrypted configuration files using plaintext AES keys configured on the IP DECT phone.</p> <p><b>Web User Interface:</b> None</p> <p><b>Handset User Interface:</b> None</p>		
<b>auto_provision.aes_key_16.com</b>	<b>16 characters</b>	<b>Blank</b>
<p><b>Description:</b> Configures the plaintext AES key for decrypting the Common CFG file. The valid characters contain: 0 ~ 9, A ~ Z, a ~ z and the following special characters are also supported: # \$ % * + , - . : = ? @ [ ] ^ _ { } ~.</p> <p><b>Example:</b> auto_provision.aes_key_16.com = 0123456789abcdef</p> <p><b>Note:</b> It works only if the value of the parameter "auto_provision.aes_key_in_file" is set to 0 (Disabled).</p>		

Parameters	Permitted Values	Default
<p><b>Web User Interface:</b> Settings-&gt;Auto Provision-&gt;Common AES Key</p> <p><b>Handset User Interface:</b> None</p>		
auto_provision.aes_key_16.mac	16 characters	Blank
<p><b>Description:</b> Configures the plaintext AES key for decrypting the Common CFG file. The valid characters contain: 0 ~ 9, A ~ Z, a ~ z and the following special characters are also supported: # \$ % * + , - . : = ? @ [ ] ^ _ { } ~.</p> <p><b>Example:</b> auto_provision.aes_key_16.com = 0123456789abcdef</p> <p><b>Note:</b> It works only if the value of the parameter "auto_provision.aes_key_in_file" is set to 0 (Disabled).</p> <p><b>Web User Interface:</b> Settings-&gt;Auto Provision-&gt;MAC-Oriented AES Key</p> <p><b>Handset User Interface:</b> None</p>		

To configure 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.

AES keys must be 16 characters and the supported characters contain: 0-9, A-Z, a-z and the following special characters are also supported: # \$ % \* +, - . : = ? @ [ ] ^ \_ { } ~.



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

# Troubleshooting

---

This chapter provides an administrator with general information for troubleshooting some common problems that he (or she) may encounter while using IP DECT phones.

## Troubleshooting Methods

The IP DECT 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 DECT phone.

- [Viewing Log Files](#)
- [Capturing Packets](#)
- [Enabling Watch Dog Feature](#)
- [Analyzing Configuration File](#)

## Viewing Log Files

If your IP DECT phone encounters some problems, commonly the log files are needed. You can configure the phone to periodically upload the log files to the provisioning server (only support a FTP/TFTP as the provisioning server). There are two types of log files on the provisioning server: <mac>-boot.log (e.g., 0015655f9d7e-boot.log) and <mac>-sys.log (0015655f9d7e-sys.log). The <mac>-boot.log file is uploaded to the provisioning server after every boot. The <mac>-sys.log file is uploaded periodically to the provisioning server. 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 6.

In the configuration files, you can use the following parameters to configure system log settings:

- **syslog.log\_level**--Specify the system log level. The following lists the log level of events you can log:
  - 0: system is unusable
  - 1: action must be taken immediately
  - 2: critical condition
  - 3: error conditions
  - 4: warning conditions

5: normal but significant condition

6: informational

- **syslog.mode**-Specify the system log to be exported to the provisioning server, syslog server or local system.
- **syslog.server**-Specify the IP address or domain name of the syslog server to which the log will be exported.
- **syslog.log\_upload\_period**-Specify the period of the log upload (in seconds) to the provisioning server.
- **syslog.ftp.post\_mode**-Specify whether the log files on the provisioning server are overwritten or appended.
- **syslog.ftp.max\_logfile**-Specify the maximum size of the log files on the provisioning server.
- **syslog.ftp.append\_limit\_mode**-Specify the phone to stop log upload or delete the old log when the log on the provisioning server reaches the max size.
- **syslog.bootlog\_upload\_wait\_time**-Specify the waiting time before the phone uploads the log file to the provisioning server.
- **auto\_provision.server.url**-Specify the access URL of the syslog server or provisioning server.

## Configuring the Severity Level of the Log

### Procedure

Severity level can be configured using the configuration files or locally.

<b>Configuration File</b>	y000000000025.cfg	Configure the severity level of the logs to be reported to a log file. <b>Parameters:</b> syslog.log_level
<b>Local</b>	Web User Interface	Configure the severity level of the logs to be reported to a log file. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?parameter=settings-config&q=load

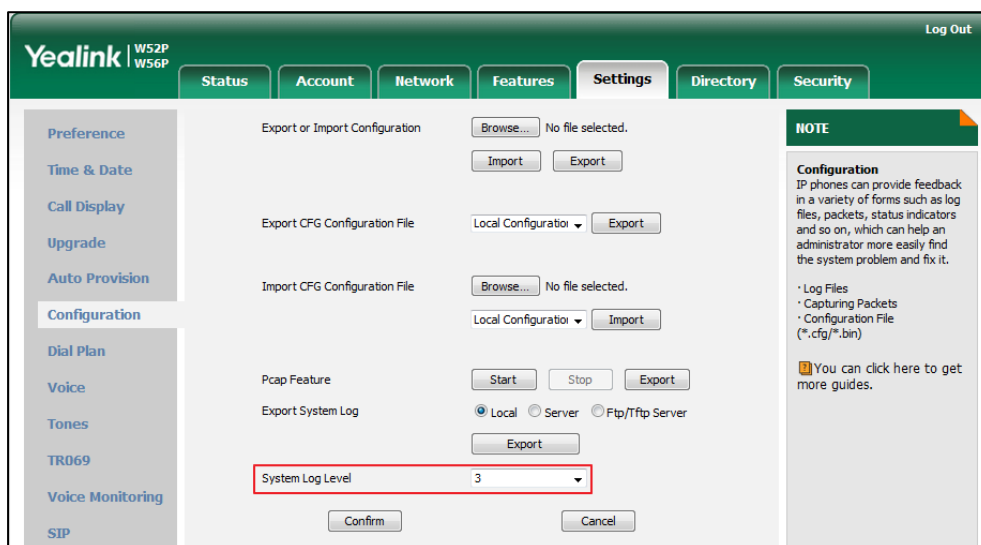
### Details of Configuration Parameters:

Parameters	Permitted Values	Default
syslog.log_level	Integer from 0 to 6	6

Parameters	Permitted Values	Default
<p><b>Description:</b> Configures the detail level of syslog information to be exported.</p> <p><b>0</b>-system is unusable <b>1</b>-action must be taken immediately <b>2</b>-critical condition <b>3</b>-error conditions <b>4</b>-warning conditions <b>5</b>-normal but significant condition <b>6</b>-informational</p> <p><b>Note:</b> If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Settings-&gt;Configuration-&gt;System Log Level</p> <p><b>Handset User Interface:</b> None</p>		

To configure the level of the system log 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.

The system log level is set as 6, the informational level.

**Note** Informational level may make some sensitive information accessible (e.g., password dial number), we recommend that you reset the system log level to 3 after providing the syslog file.

## Exporting the Log File to the Local System

### Procedure

Log setting can be configured using the configuration files or locally.

<b>Configuration File</b>	y000000000025.cfg	Configure the syslog mode. <b>Parameters:</b> syslog.mode
<b>Local</b>	Web User Interface	Configure the syslog mode. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?parameter=settings-config&q=load

### Details of Configuration Parameters:

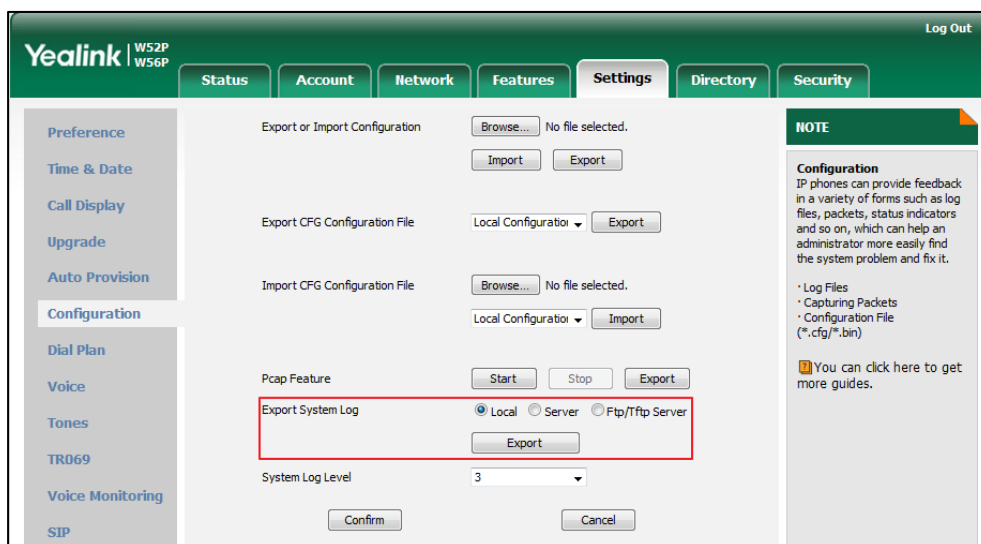
Parameters	Permitted Values	Default
<b>syslog.mode</b>	<b>0, 1 or 2</b>	<b>0</b>
<p><b>Description:</b> Configures the IP DECT phone to export log files to the local system, syslog server or an FTP/TFTP Server (provisioning server).</p> <p><b>0-Local</b> <b>1-Server</b> <b>2-FTP/TFTP Server</b></p> <p><b>Note:</b> If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Settings-&gt;Configuration-&gt;Export System Log</p> <p><b>Handset User Interface:</b> None</p>		

**To export a log file to the local system via web user interface:**

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



2. Mark the **Local** radio box in the **Export System Log** field.  
A dialog box pops up to prompt "Warning: Some settings you changed take effect when you restart your machine! Do you want to reboot now?". The configuration will take effect after a reboot.
3. Click **Export** to open file download window, and then save the file to your local system.



A log file named **syslog.tar** is successfully exported to your local system.

To view the log file on your local system:

1. Extract the combined log files to your local system.
2. Open the folder you extracted to and identify the files you will view.

The following figure shows a portion of a <mac>.log (e.g., 0015655f9d7e.log)-an account registration:

```
Dec 31 08:10:14 sua [531]: DLG <+notice> [000] Message sent: (to dest=10.2.1.48:5060 len=543)
Dec 31 08:10:14 sua [531]: DLG <+info > [000]
Dec 31 08:10:14 sua [531]: DLG <+info > [000] REGISTER sip:10.2.1.48:5060 SIP/2.0^M
Dec 31 08:10:14 sua [531]: DLG <+info > [000] Via: SIP/2.0/UDP 10.10.20.27:5060;branch=z9hG4bK
Dec 31 08:10:14 sua [531]: DLG <+info > [000] From: "1005" <sip:1025@10.2.1.48:5060>;tag=23413
Dec 31 08:10:14 sua [531]: DLG <+info > [000] To: "1005" <sip:1025@10.2.1.48:5060>^M
Dec 31 08:10:14 sua [531]: DLG <+info > [000] Call-ID: 0_2399776309@10.10.20.27^M
Dec 31 08:10:14 sua [531]: DLG <+info > [000] CSeq: 1 REGISTER^M
Dec 31 08:10:14 sua [531]: DLG <+info > [000] Contact: <sip:1025@10.10.20.27:5060>^M
Dec 31 08:10:14 sua [531]: DLG <+info > [000] Allow: INVITE, INFO, PRACK, ACK, BYE, CANCEL, OP
Dec 31 08:10:14 sua [531]: DLG <+info > [000] Max-Forwards: 70^M
Dec 31 08:10:14 sua [531]: DLG <+info > [000] User-Agent: Yealink W52P 25.80.254.48^M
Dec 31 08:10:14 sua [531]: DLG <+info > [000] Expires: 3600^M
Dec 31 08:10:14 sua [531]: DLG <+info > [000] Allow-Events: talk,hold,conference,refer,check-s
Dec 31 08:10:14 sua [531]: DLG <+info > [000] Content-Length: 0^M
Dec 31 08:10:14 sua [531]: DLG <+info > [000] ^M
Dec 31 08:10:14 sua [531]: DLG <+info > [000]
Dec 31 08:10:14 sua [531]: NET <+notice> [000] ===>>> UDP socket 10.2.1.48:5060: send 543 byte
Dec 31 08:10:14 Log [623]: CMDP<+info > Account[0] name[1025] Enable[1] Usable[0]
Dec 31 08:10:14 Log [623]: CMDP<+info > SCA[0] ConfType[0] EnableTls[0]
Dec 31 08:10:14 sua [531]: NET <+notice> [255] <<<<=== UDP socket 10.2.1.48:5060: read 303 byte
Dec 31 08:10:14 sua [531]: SIP <+info > [SIP] match line:name:1025 host:10.2.1.48
Dec 31 08:10:14 sua [531]: DLG <+notice> [000] Message rcv: (from src=10.2.1.48:5060 len=303)
```

## Exporting the Log File to a Syslog Server

### Procedure

Log setting can be configured using the configuration files or locally.

<b>Configuration File</b>	y000000000025.cfg	Configure the syslog mode. <b>Parameters:</b> syslog.mode
		Configure the IP address or domain name of the syslog server where to export the log files. <b>Parameters:</b> syslog.server
<b>Local</b>	Web User Interface	Configure the syslog mode. Configure the IP address or domain name of the syslog server where to export the log files. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?parameter=settings-config&q=load

### Details of Configuration Parameters:

Parameters	Permitted Values	Default
<b>syslog.mode</b>	<b>0, 1 or 2</b>	<b>0</b>
<p><b>Description:</b> Configures the IP DECT phone to export log files to the local system, syslog server or an FTP/TFTP Server (provisioning server).</p> <p><b>0-Local</b> <b>1-Server</b> <b>2-FTP/TFTP Server</b></p> <p><b>Note:</b> If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Settings-&gt;Configuration-&gt;Export System Log</p> <p><b>Handset User Interface:</b> None</p>		

Parameters	Permitted Values	Default
syslog.server	IP address or domain name	Blank

**Description:**  
Configures the IP address or domain name of the syslog server when exporting log to the syslog server.

**Example:**  
syslog.server = 192.168.1.100

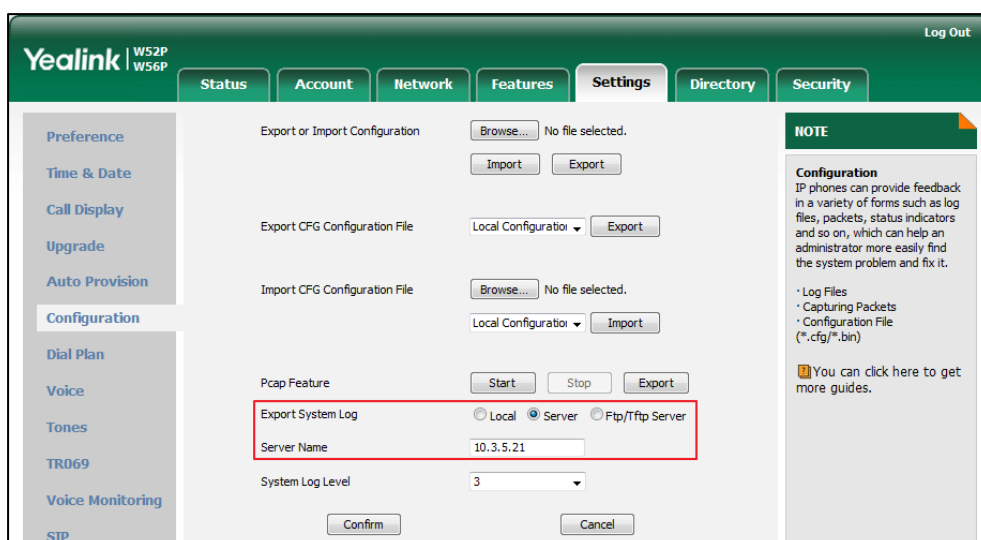
**Note:** It works only if the value of the parameter “syslog.mode” is set to 1 (Server). If you change this parameter, the base station will reboot to make the change take effect.

**Web User Interface:**  
Settings->Configuration->Server Name

**Handset User Interface:**  
None

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.  
For example, the IP address of your syslog server is 10.3.5.21.



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

**To view the log file on your syslog server:**

You can view the system log file in the desired folder on the syslog server. The location of the folder may differ from the syslog server. For more information, refer to the network resources.

The following figure shows a portion of the system log:

```

Aug 27 09:24:03 10.10.20.39 [000] Register: start...
Aug 27 09:24:03 10.10.20.39 [SIP] linestatus lid:0, enable=1, tick=0, old_status:1, new_status:1
Aug 27 09:24:03 10.10.20.39 [SIP] <IPC_p2my>:msg=0x00042103(270595), wparam=0, lparam=0
Aug 27 09:24:03 10.10.20.39 [SIP] <IPC_broa>:msg=0x00040001(262145), wparam=0, lparam=1
Aug 27 09:24:03 10.10.20.39 [000] core get contact nat type:0
Aug 27 09:24:03 10.10.20.39 [000] core get contact nat type:0
Aug 27 09:24:03 10.10.20.39 [000] allocating transaction resource 37 0_1057687278
Aug 27 09:24:03 10.10.20.39 [000] allocating NICT context
Aug 27 09:24:03 10.10.20.39 Line State Change AccountId:0, State:1
Aug 27 09:24:03 10.10.20.39 EtlMsgHandler_NotifyApp ACCOUNT_STATUS_CHANGED(0, 4, 1)!
Aug 27 09:24:03 10.10.20.39 Aug 27 01:24:01 ipvp[520]: IPVP<5+notice> 641.725.333:Message=0x00040001(0x00000
Aug 27 09:24:03 10.10.20.39 Aug 27 01:24:01 ipvp[520]: IPVP<6+info > 641.728.924:unknown msg,0x00040001,frd
Aug 27 09:24:03 10.10.20.39 [000] Message sent: (to dest=10.2.1.48:5060 len=545)
Aug 27 09:24:03 10.10.20.39 [000]
Aug 27 09:24:03 10.10.20.39 [000] REGISTER sip:10.2.1.48:5060 SIP/2.0
Aug 27 09:24:03 10.10.20.39 [000] Via: SIP/2.0/UDP 10.10.20.39:5060;branch=z9hG4bK951979898
Aug 27 09:24:03 10.10.20.39 [000] From: "1012" <sip:1012@10.2.1.48:5060>;tag=2152532079
Aug 27 09:24:03 10.10.20.39 [000] To: "1012" <sip:1012@10.2.1.48:5060>
Aug 27 09:24:03 10.10.20.39 [000] Call-ID: 0_1057687278@10.10.20.39
Aug 27 09:24:03 10.10.20.39 [000] CSeq: 1 REGISTER
Aug 27 09:24:03 10.10.20.39 [000] Contact: <sip:1012@10.10.20.39:5060>
Aug 27 09:24:03 10.10.20.39 [000] Register: get expires:3600
Aug 27 09:24:03 10.10.20.39 [SIP] <IPC_broa>:msg=0x00040001(262145), wparam=0, lparam=2
Aug 27 09:24:03 10.10.20.39 [000] Allow: INVITE, INFO, PRACK, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REGISTER,
Aug 27 09:24:03 10.10.20.39 [255] <<<<=== UDP socket 10.10.20.31:5060: read 681 bytes
Aug 27 09:24:03 10.10.20.39 [000] *****Core event:(0x0043)ECORE_SUBSCRIPTION_NOTIFY *****
Aug 27 09:24:03 10.10.20.39 [000] From: <sip:10111@10.2.1.48:5060>;tag=2198906946
Aug 27 09:24:03 10.10.20.39 OnConfigChangeMsg objMsg.message[262145],objMsg.wParam[0]
    
```

## Exporting the Log File to a Provisioning Server (FTP/TFTP Server)

### Procedure

Log setting can be configured using the configuration files or locally.

<b>Configuration File</b>	y000000000025.cfg	Configure the syslog mode. <b>Parameters:</b> syslog.mode
		Configure the period of the log upload (in seconds) to the provisioning server. <b>Parameters:</b> syslog.log_upload_period
		Configure whether the log files on the provisioning server are overwritten or appended. <b>Parameters:</b> syslog.ftp.post_mode

		<p>Configure the maximum size of the log files on the provisioning server.</p> <p><b>Parameters:</b> syslog.ftp.max_logfile</p> <hr/> <p>Configure the phone to stop log upload or delete the old log when the log on the provisioning server reaches the max size.</p> <p><b>Parameters:</b> syslog.ftp.append_limit_mode</p> <hr/> <p>Configure the waiting time before the phone uploads the log file to the provisioning server.</p> <p><b>Parameters:</b> syslog.bootlog_upload_wait_time</p> <hr/> <p>Configure the access URL of the provisioning server.</p> <p><b>Parameters:</b> auto_provision.server.url</p>
<p><b>Local</b></p>	<p>Web User Interface</p>	<p>Configure the syslog mode.</p> <p>Configure the period of the log upload (in seconds) to the provisioning server.</p> <p>Configure whether the log files on the provisioning server are overwritten or appended.</p> <p>Configure the maximum size of the log files on the provisioning server.</p> <p>Configure the phone to stop log upload or delete the old log when the log on the provisioning server reaches the max size.</p> <p>Configure the waiting time before the phone uploads the log file to the provisioning server.</p> <p><b>Navigate to:</b> http://&lt;phoneIPAddress&gt;/servlet?parameter=settings-config&amp;q=load</p>

		<p>Configure the access URL of the provisioning server.</p> <p><b>Navigate to:</b></p> <p>http://&lt;phoneIPAddress&gt;/servlet?parameter=settings-autop&amp;q=load</p>
--	--	---

**Details of Configuration Parameters:**

Parameters	Permitted Values	Default
<b>syslog.mode</b>	<b>0, 1 or 2</b>	<b>0</b>
<p><b>Description:</b> Configures the IP DECT phone to export log files to the local system, syslog server or an FTP/TFTP Server (provisioning server).</p> <p><b>0</b>-Local <b>1</b>-Server <b>2</b>-FTP/TFTP Server</p> <p><b>Note:</b> If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Settings-&gt;Configuration-&gt;Export System Log</p> <p><b>Handset User Interface:</b> None</p>		
<b>syslog.log_upload_period</b>	<b>Integer from 30 to 2592000</b>	<b>30</b>
<p><b>Description:</b> Configures the period of the log upload (in seconds) to the provisioning server.</p> <p><b>Example:</b> syslog.log_upload_period = 60</p> <p><b>Note:</b> It works only if the value of the parameter "syslog.mode" is set to 2 (FTP/TFTP Server). If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Settings-&gt;Configuration-&gt;Upload Period(30~2592000)s</p> <p><b>Handset User Interface:</b> None</p>		

Parameters	Permitted Values	Default
<b>syslog.ftp.post_mode</b>	<b>1 or 2</b>	<b>1</b>
<p><b>Description:</b>            Configures whether the log files on the provisioning server are overwritten or appended.            1-Post Append            2-Post Stor (not applicable to TFTP Server)            If it is set to 1 (Post Append), the log files on the provisioning server are appended.            If it is set to 2 (Post Stor), the log files on the provisioning server are overwritten.  <b>Note:</b> It works only if the value of the parameter "syslog.mode" is set to 2 (FTP/TFTP Server). If you change this parameter, the base station will reboot to make the change take effect.  <b>Web User Interface:</b>            Settings-&gt;Configuration-&gt;Post Mode  <b>Handset User Interface:</b>            None</p>		
<b>syslog.ftp.max_logfile</b>	<b>Integer from 200 to 65535</b>	<b>512</b>
<p><b>Description:</b>            Configures the maximum size of the log files on the provisioning server.  <b>Example:</b>            syslog.ftp.max_logfile = 511  <b>Note:</b> It works only if the value of the parameter "syslog.mode" is set to 2 (FTP/TFTP Server). If you change this parameter, the base station will reboot to make the change take effect.  <b>Web User Interface:</b>            Settings-&gt;Configuration-&gt;Append Limit Size(200~65535)K  <b>Handset User Interface:</b>            None</p>		
<b>syslog.ftp.append_limit_mode</b>	<b>1 or 2</b>	<b>1</b>
<p><b>Description:</b>            Configures the phone to stop upload log or delete the old log when the log on the provisioning server reaches the max size.            1-Append Delete</p>		

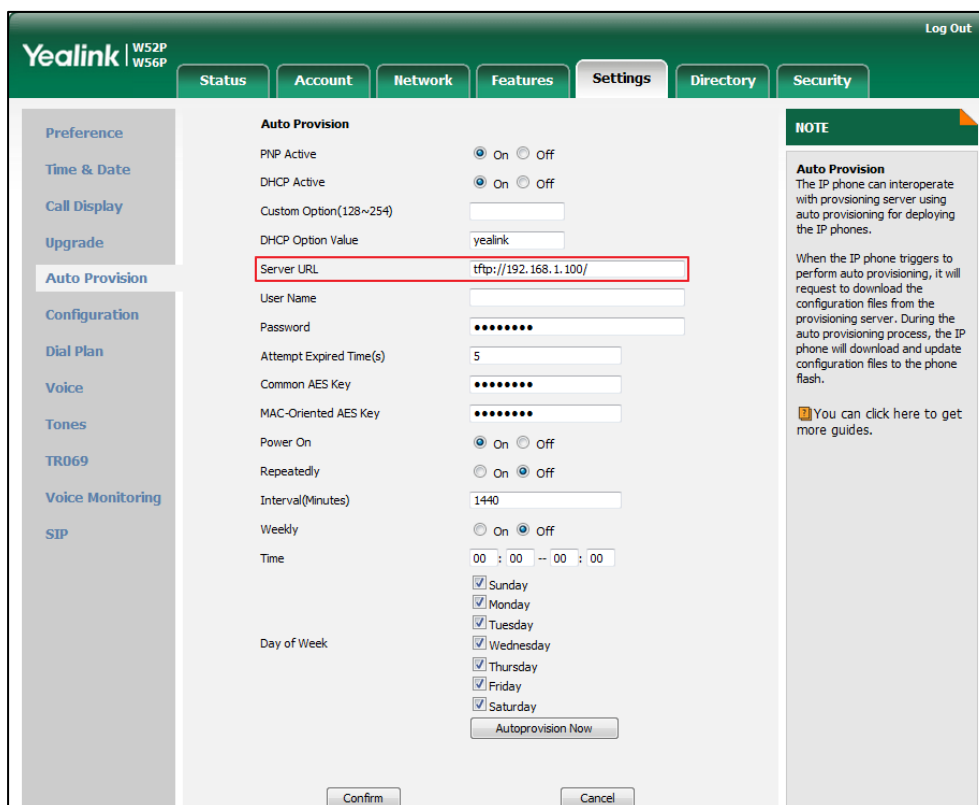
Parameters	Permitted Values	Default
<p><b>2-Append Stop</b></p> <p><b>Note:</b> It works only if the value of the parameter "syslog.mode" is set to 2 (FTP/TFTP Server). If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> Settings-&gt;Configuration-&gt;Append Limit Mode</p> <p><b>Handset User Interface:</b> None</p>		
<b>syslog.bootlog_upload_wait_time</b>	<b>Integer from 1 to 86400</b>	<b>120</b>
<p><b>Description:</b> Configures the waiting time (in seconds) before the phone uploads the log file to the provisioning server.</p> <p><b>Example:</b> syslog.bootlog_upload_wait_time = 121</p> <p><b>Note:</b> It works only if the value of the parameter "syslog.mode" is set to 2 (FTP/TFTP Server). If you change this parameter, the base station will reboot to make the change take effect.</p> <p><b>Web User Interface:</b> None</p> <p><b>Handset User Interface:</b> None</p>		
<b>auto_provision.server.url</b>	<b>URL within 511 characters</b>	<b>Blank</b>
<p><b>Description:</b> Configures the access URL of the provisioning server.</p> <p><b>Example:</b> auto_provision.server.url = tftp://10.3.6.133/</p> <p><b>Web User Interface:</b> Settings-&gt;Auto Provision-&gt;Server URL</p> <p><b>Handset User Interface:</b> None</p>		

**To configure the URL of the provisioning server via web user interface:**

1. Click on **Settings->Auto Provision**.
2. Enter the URL of the FTP/TFTP server in the **Server URL** field.



For example, if the IP address TFTP server is 192.168.1.100, then the URL “tftp://192.168.1.100/” is where the IP DECT phone exports the system log. For more information on TFTP server, refer to [Yealink\\_SIP-T2\\_Series\\_T19\(P\)\\_E2\\_T4\\_Series\\_CP860\\_W56P\\_IP\\_Phones\\_Auto\\_Provisioning\\_Guide](#).

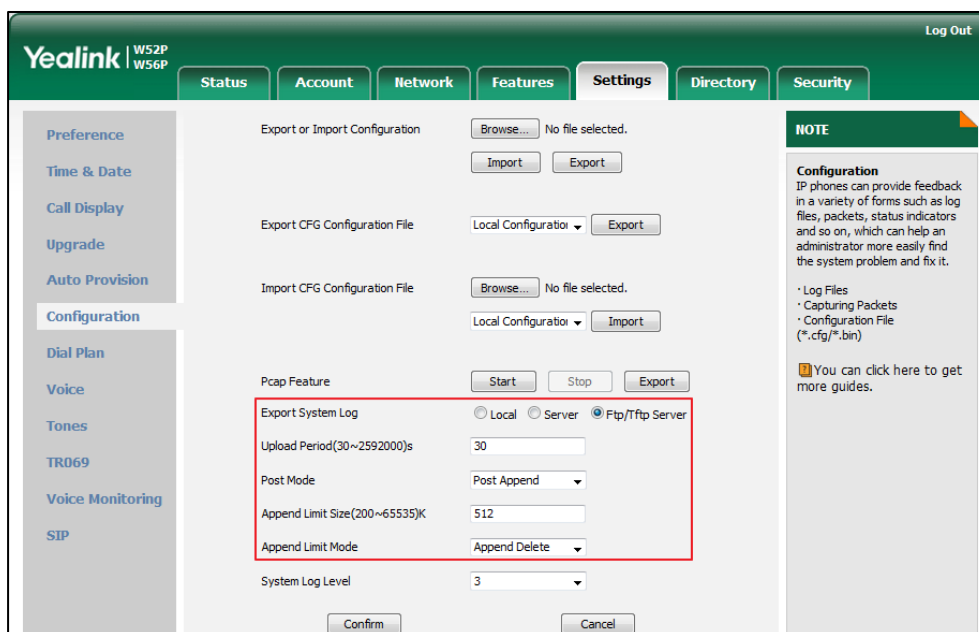


3. Click **Confirm** to accept the change.

**To configure the phone to export the system log to an FTP/TFTP server via web user interface:**

1. Click on **Settings->Configuration**.
2. Mark the **Ftp/Tftp Server** radio box in the **Export System Log** field.
3. Enter the upload period of the log files in the **Upload Period (30~2592000)s** field.
4. Select the desired post mode from the pull-down list of **Post Mode**.
5. Enter the limit size of the log files in the **Append Limit Size (200~65535)K** field.

- Select the desired limit mode from the pull-down list of **Append Limit Mode**.



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

A dialog box pops up to prompt “Do you want to restart your machine?”. The configuration will take effect after a reboot.

- Click **OK** to reboot the phone.

The system log will be exported successfully to the desired FTP/TFTP server after a reboot.

**To view the log file on your FTP/TFTP server:**

You can view the system log file in the root directory folder you have configured on the FTP/TFTP server.

The following figure shows a portion of a <mac>-boot.log (e.g., 0015655f9d7e-boot.log):

```
Dec 31 08:10:13 Log [623]: CNDP<6+info > [SIP] match line:name:1025 host:10.2.1.48
Dec 31 08:10:14 sua [531]: DLG <5+notice> [000] Message rcv: (from src=10.2.1.48:5060 len=303)
Dec 31 08:10:14 sua [531]: DLG <6+info > [000]
Dec 31 08:10:14 sua [531]: DLG <6+info > [000] SIP/2.0 200 OK^M
Dec 31 08:10:14 sua [531]: DLG <6+info > [000] Via: SIP/2.0/UDP 10.10.20.27:5060;branch=z9hG4bK666469922^M
Dec 31 08:10:14 sua [531]: DLG <6+info > [000] Contact: <sip:1005@10.10.20.27:5060>;expires=3600^M
Dec 31 08:10:14 sua [531]: DLG <6+info > [000] From: "1005" <sip:1025@10.2.1.48:5060>;tag=2341321725^M
Dec 31 08:10:14 sua [531]: DLG <6+info > [000] To: "1005" <sip:1025@10.2.1.48:5060>;tag=7341321725^M
Dec 31 08:10:14 sua [531]: DLG <6+info > [000] Call-ID: 0_2399776309@10.10.20.27^M
Dec 31 08:10:14 sua [531]: DLG <6+info > [000] CSeq: 2 REGISTER^M
Dec 31 08:10:14 sua [531]: DLG <6+info > [000] User-Agent: Yealink W52P 25.80.254.48^M
Dec 31 08:10:14 sua [531]: DLG <6+info > [000] Content-Length: 0^M
Dec 31 08:10:14 sua [531]: DLG <6+info > [000] ^M
Dec 31 08:10:14 sua [531]: DLG <6+info > [000]
Dec 31 08:10:14 sua [531]: NET <5+notice> [000] =====>>> UDP socket 10.2.1.48:5060: send 543 bytes
```

The following figure shows a portion of a <mac>-sys.log (e.g., 0015655f9d7e-sys.log):

```

Dec 31 08:10:14 sua [531]: DLG <5+notice> [000] Message sent: (to dest=10.2.1.48:5060 len=543)
Dec 31 08:10:14 sua [531]: DLG <6+info > [000]
Dec 31 08:10:14 sua [531]: DLG <6+info > [000] REGISTER sip:10.2.1.48:5060 SIP/2.0^M
Dec 31 08:10:14 sua [531]: DLG <6+info > [000] Via: SIP/2.0/UDP 10.10.20.27:5060;branch=z9hG4bK
Dec 31 08:10:14 sua [531]: DLG <6+info > [000] From: "1005" <sip:1025@10.2.1.48:5060>;tag=23413
Dec 31 08:10:14 sua [531]: DLG <6+info > [000] To: "1005" <sip:1025@10.2.1.48:5060>^M
Dec 31 08:10:14 sua [531]: DLG <6+info > [000] Call-ID: 0_2399776309@10.10.20.27^M
Dec 31 08:10:14 sua [531]: DLG <6+info > [000] CSeq: 1 REGISTER^M
Dec 31 08:10:14 sua [531]: DLG <6+info > [000] Contact: <sip:1025@10.10.20.27:5060>^M
Dec 31 08:10:14 sua [531]: DLG <6+info > [000] Allow: INVITE, INFO, PRACK, ACK, BYE, CANCEL, OP
Dec 31 08:10:14 sua [531]: DLG <6+info > [000] Max-Forwards: 70^M
Dec 31 08:10:14 sua [531]: DLG <6+info > [000] User-Agent: Yealink W52P 25.80.254.48^M
Dec 31 08:10:14 sua [531]: DLG <6+info > [000] Expires: 3600^M
Dec 31 08:10:14 sua [531]: DLG <6+info > [000] Allow-Events: talk,hold,conference,refer,check-s
Dec 31 08:10:14 sua [531]: DLG <6+info > [000] Content-Length: 0^M
Dec 31 08:10:14 sua [531]: DLG <6+info > [000] ^M
Dec 31 08:10:14 sua [531]: DLG <6+info > [000]
Dec 31 08:10:14 sua [531]: NET <5+notice> [000] ==>>>> UDP socket 10.2.1.48:5060: send 543 byte
Dec 31 08:10:14 Log [623]: CMDP<6+info > Account[0] name[1025] Enable[1] Usable[0]
Dec 31 08:10:14 Log [623]: CMDP<6+info > SCA[0] ConfType[0] EnableTls[0]
Dec 31 08:10:14 sua [531]: NET <5+notice> [255] <<<<=== UDP socket 10.2.1.48:5060: read 303 byte
Dec 31 08:10:14 sua [531]: SIP <6+info > [SIP] match line:name:1025 host:10.2.1.48
Dec 31 08:10:14 sua [531]: DLG <5+notice> [000] Message rcv: (from src=10.2.1.48:5060 len=303)

```

The "6+info" means you got the correct syslog.

## Capturing Packets

You can capture packet in two ways: capturing the packets via web user interface or using the Ethernet software. You can analyze the packet captured for troubleshooting purpose.

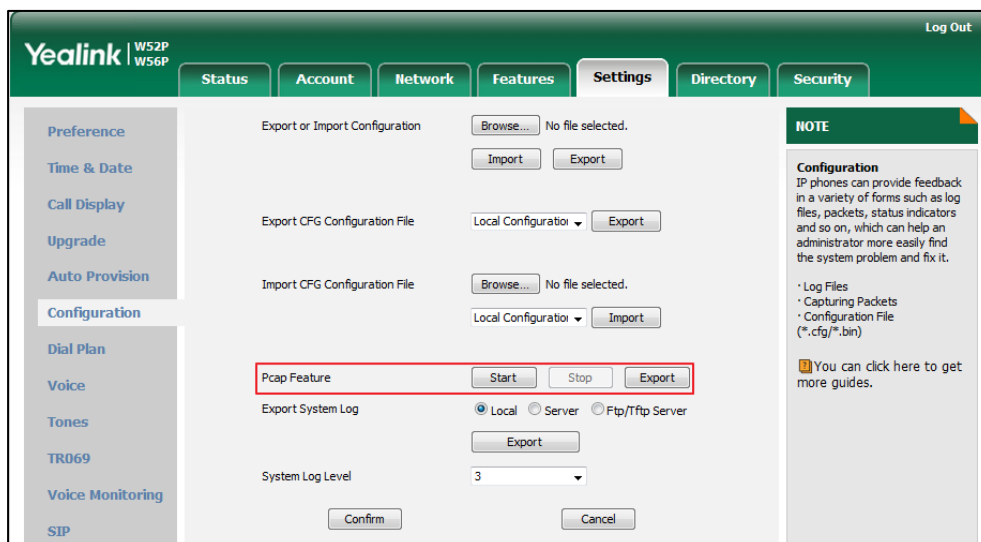
### Capturing the Packets via Web User Interface

For Yealink IP DECT phones, you can export the packets file to the local system and analyze it.

**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.

- Click **Export** to open the file download window, and then save the file to your local system.



## Capturing the Packets Using the Ethernet Software

### Receiving data packets from the HUB

Connect the Internet port of the IP DECT phone and the PC to the same HUB, and then use Sniffer, Ethereal or Wireshark software to capture the signal traffic.

## Enabling Watch Dog Feature

The IP DECT phone provides a troubleshooting feature called “Watch Dog”, which helps you monitor the IP DECT phone status and provides the ability to get stack traces from the last time the IP DECT phone failed. If Watch Dog feature is enabled, the base station will automatically reboot when it detects a fatal failure. This feature can be configured using the configuration files or via web user interface.

### Procedure

Watch Dog can be configured using the configuration files or locally.

<b>Configuration File</b>	y00000000025.cfg	Configure Watch Dog feature. <b>Parameter:</b> watch_dog.enable
<b>Local</b>	Web User Interface	Configure Watch Dog feature. <b>Navigate to:</b>

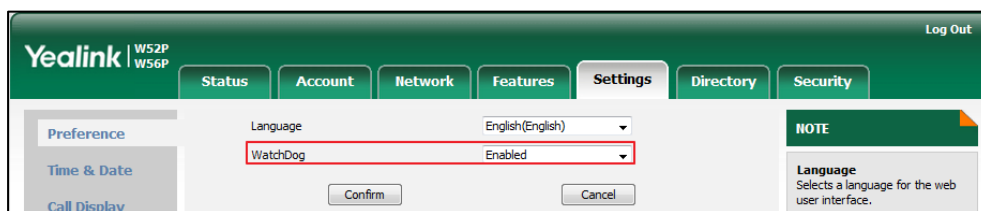
		http://<phoneIPAddress>/servlet?p=settings-preference&q=load
--	--	--

**Details of the Configuration Parameter:**

Parameter	Permitted Values	Default
watch_dog.enable	0 or 1	0
<p><b>Description:</b> Enables or disables the Watch Dog feature.</p> <p>0-Disabled 1-Enabled</p> <p><b>Note:</b> If it is set to 1 (Enabled), the base station will reboot automatically when the system is broken down.</p> <p><b>Web User Interface:</b> Settings-&gt;Preference-&gt;WatchDog</p> <p><b>Handset User Interface:</b> None</p>		

**To configure watch dog feature via web user interface:**

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



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

## Analyzing Configuration File

Wrong configurations may have an impact on your phone use. You can export configuration file to check the current configuration of the IP DECT phone and troubleshoot if necessary. You can also import configuration files for a quick and easy configuration.

Three types of configuration files can be exported to your local system:

- config.bin

- <mac>-all.cfg
- <mac>-local.cfg

We recommend you to edit the exported CFG file instead of the BIN file to change the phone's current settings. For more information on configuration files, refer to [Configuration Files](#) on page 14.

## BIN Configuration Files

The config.bin file is an encrypted file. For more information on config.bin file, contact your Yealink reseller.

### Procedure

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

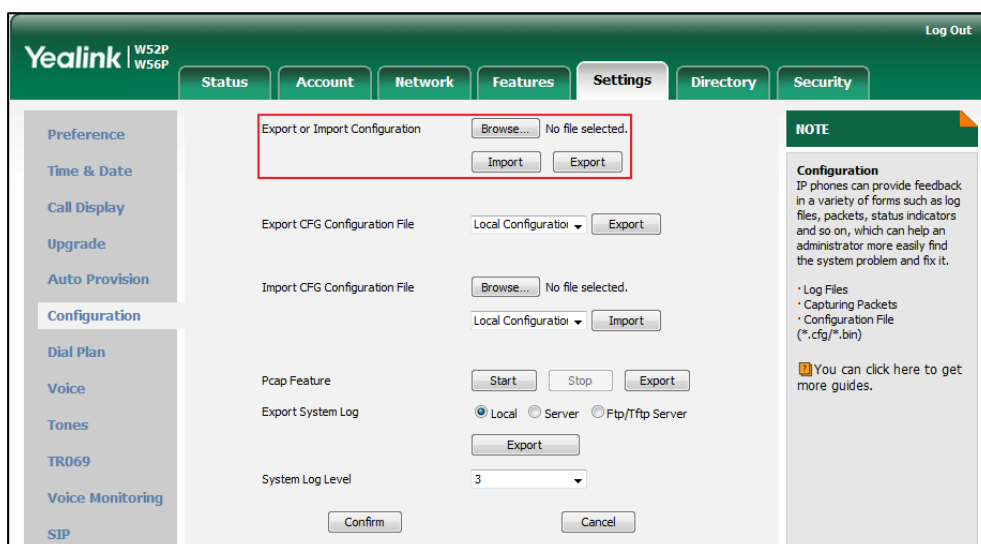
<b>Configuration File</b>	y000000000025.cfg	Specify the access URL for the custom configuration files. <b>Parameter:</b> configuration.url
<b>Local</b>	Web User Interface	Export or import the custom configuration files. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=settings-config&q=load

### Details of the Configuration Parameter:

Parameter	Permitted Values	Default
configuration.url	URL within 511 characters	Blank
<p><b>Description:</b> Configures the access URL for the custom configuration files.</p> <p><b>Note:</b> The file format of custom configuration file must be *.bin.</p> <p><b>Web User Interface:</b> Settings-&gt;Configuration-&gt;Export or Import Configuration</p> <p><b>Handset User Interface:</b> None</p>		

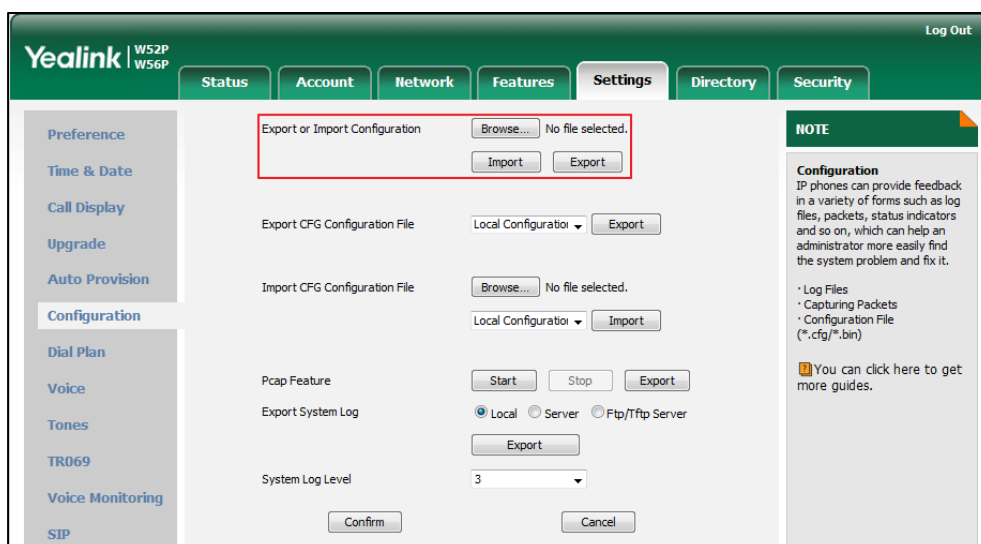
To export BIN configuration files via web user interface:

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.



To import a BIN configuration file via web user interface:

1. Click on **Settings->Configuration**.
2. In the **Export or Import Configuration** block, click **Browse** to locate a BIN configuration file from your local system.



3. Click **Import** to import the configuration file.

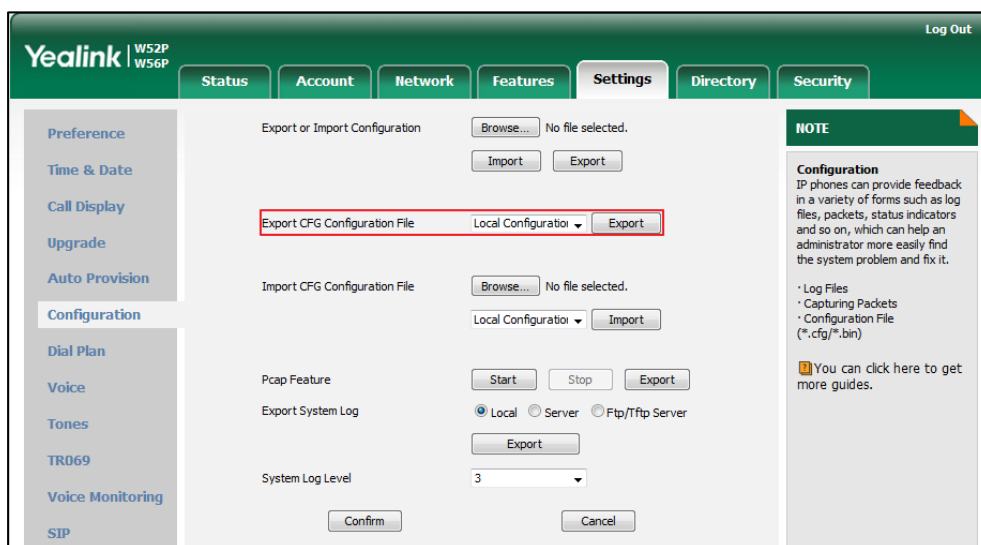
## CFG Configuration Files

The <mac>-all.cfg configuration file contains all changes made via handset user

interface, web user interface and using configuration files. The <mac>-local.cfg configuration file contains changes made via handset user interface and web user interface.

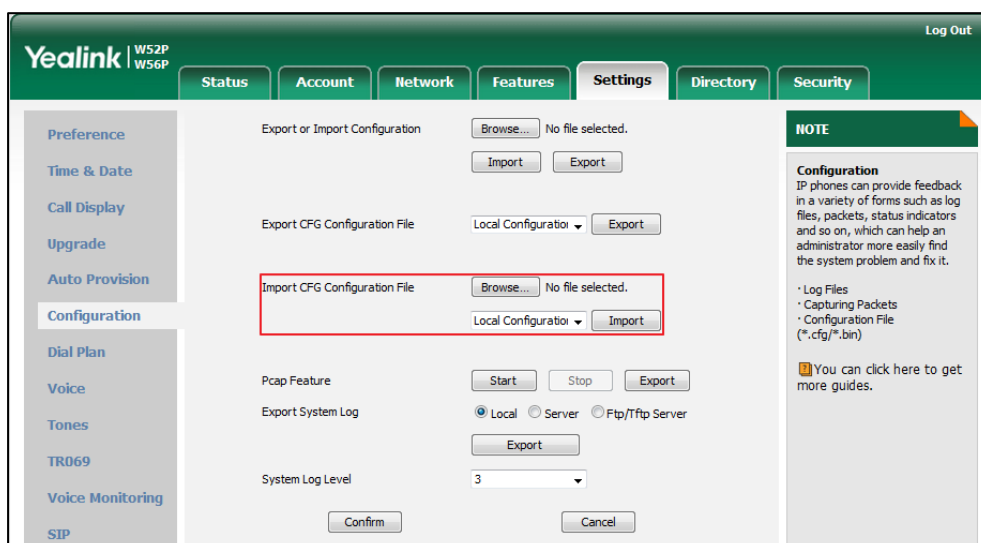
**To export CFG configuration files via web user interface:**

1. Click on **Settings->Configuration**.
2. Select **Local Configuration** or **All Configuration** from the pull-down list of **Export CFG Configuration File**.
3. Click **Export** to open file download window, and then save the file to your local system.



**To import CFG configuration files via web user interface:**

1. Click on **Settings->Configuration**.
2. In the **Import CFG Configuration File** block, click **Browse** to locate a CFG configuration file from your local system.





3. Click **Import** to import the configuration file.

## Troubleshooting Solutions

This section describes solutions to common issues that may occur while using the IP DECT phone. Upon encountering a scenario not listed in this section, contact your Yealink reseller for further support.

### Base Issue

#### Why doesn't the power indicator on the base station light up?

Plug the supplied power adapter to the base station, if the power indicator doesn't light up, it should be a hardware problem. Please contact your vendor or local distributor and send the problem description for help. If you cannot get a support from them, please send a mail which includes problem description, test result, your country and phone's SN to [Support@yealink.com](mailto:Support@yealink.com).

#### Why doesn't the network indicator on the base station slowly flash?

It means that the base station cannot get an IP address. Try connecting the base station to another switch port, if the network indicator still slowly flashes, please try a reset.

#### How to reboot the Base Station remotely?

The base station support remote reboot by a SIP NOTIFY message with "Event: check-sync" header. Whether the base station reboots or not depends on the value of the parameter "sip.notify\_reboot\_enable". If the value is set to 1, or the value is set to 0 and the header of the SIP NOTIFY message contains an additional string "reboot=true", the base station will reboot immediately.

The NOTIFY message is formed as shown:

```
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
```

### Procedure

Changes can only be configured using the configuration files.

<b>Configuration File</b>	y000000000025.cfg	Configure the IP DECT phone behavior when receiving a SIP NOTIFY message which contains the header “Event: check-sync”.  <b>Parameter:</b> sip.notify_reboot_enable
---------------------------	-------------------	--

### Details of the Configuration Parameter:

Parameter	Permitted Values	Default
sip.notify_reboot_enable	0, 1 or 2	1
<p><b>Description:</b> Configure the IP DECT phone behavior when receiving a SIP NOTIFY message which contains the header “Event: check-sync”.</p> <p><b>0</b>-The base station will reboot only if the SIP NOTIFY message contains an additional string “reboot=true”.</p> <p><b>1</b>-The base station will be forced to reboot.</p> <p><b>2</b>-The base station will ignore the SIP NOTIFY message.</p> <p><b>Web User Interface:</b> None</p> <p><b>Handset User Interface:</b> None</p>		

## Register Issue

### Why cannot the handset be registered to the base station?

If the network works normally, you can check the compatibility between base station and handset. There are 2 sets of base stations, complied with the FCC and CE standard respectively. You can check it from the back of the base station. There are also 2 sets of handsets, American and Europe area respectively.

The American area handset is compatible with FCC standard base station.

The Europe area handset is compatible with CE standard base station.

## Display Issue

### Why does the handset prompt the message “Not Subscribed” ?

Check the registration status of your handset. If your handset is not registered to the base station, register it manually.

### Why does the handset prompt the message “Not In Range” ?

- Ensure that the base station is properly plugged into a functional AC outlet.
- Ensure that the handset is not too far from the base station.

### Why does the handset prompt the message “Network unavailable” ?

- Ensure that the Ethernet cable is plugged into the Internet port on the base station and the Ethernet cable is not loose.
- Ensure that the switch or hub in your network is operational.

### Why does the Handset display “No Service” ?

The LCD screen prompts “No Service” message when there is no available SIP account on the W56P IP DECT phone.

Do one of the following:

- Ensure that an account is actively registered on the handset at the path **OK->Status->Line Status**.
- Ensure that the SIP account parameters have been configured correctly.

## Upgrade Issue

### Why doesn't the IP DECT phone upgrade firmware successfully?

Do one of the following:

- Ensure that the target firmware version is not the same as the current one.
- Ensure that the target firmware is applicable to the IP DECT 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 or refreshed when upgrading firmware via web user interface.
- For handset, ensure the handset battery should not less than 40% and is connected to the base station.

## Time and Date Issue

### Why doesn't the handset display time and date correctly?

Check if the IP DECT 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.

## Audio Issue

### How to increase or decrease the volume?

Press ◀ or ▶ on the handset to increase or decrease the ringer volume when the handset is idle, or to adjust the volume of engaged audio device (earpiece, speakerphone or earphone) when there is an active call in progress.

### 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 noises, 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 (e.g., 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.
- The handset is too far from the base station, please move closer and try again.

## Why does the IP DECT phone play the local ringback tone instead of media when placing a long distance number without plus 0?

Ensure that the 180 ring workaround feature is disabled. For more information, refer to [180 Ring Workaround](#) on page 193.

## Why is there no sound when the other party picks up the call?

If the caller and receiver cannot hear anything - there is no sound at all when the other party picks up the call, the possible reason could be: the phone cannot send the real-time transport protocol (RTP) streams, in which audio data is transmitted, to the connected call.

Try to disable the 180 ring workaround feature. For more information, refer to [180 Ring Workaround](#) on page 193.

## Phone Book Issues

### What is the difference between a remote phone book and a local phone book?

A remote phonebook is placed on a server, while a local phonebook is placed on the IP DECT phone flash. A remote phonebook can be used by everyone that can access the server, while a local phonebook can only be used by a specific phone. A remote

phonebook 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.

## Provisioning Issues

### What is auto provisioning?

Auto provisioning refers to the update of IP DECT phones, including update on 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 DECT phones to acquire the provisioning server address. With PnP enabled, the IP DECT 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 DECT phone will be able to download the CFG files from the provisioning server. PnP depends on support from a SIP server.

### Why doesn't the IP DECT phone update the configuration?

Do one of the following:

- Ensure that the configuration is set correctly.
- Reboot the base station. Some configurations require a reboot to take effect.
- Ensure that the configuration is applicable to the IP DECT phone model.
- The configuration may depend on support from a server.

## Resetting Issues

Generally, some common issues may occur while using the IP DECT phone. You can reset your phone to factory configurations after you have tried all troubleshooting suggestions but do not solve the problem. Resetting the phone to factory configurations clears the flash parameters, removes log files, user data, and cached data, and resets the administrator password to admin. All custom settings will be overwritten after resetting.

You can reset the IP DECT phone to default factory configurations. The default factory configurations are the settings that reside on the IP DECT phone after it has left the factory. For more information, refer to [How to reset the IP DECT phone to factory](#)

[configurations?](#) on page 395.

You can also reset the IP DECT phone to custom factory configurations if required. The custom factory configurations are the settings that defined by the user to keep some custom settings after resetting. You have to import the custom factory configuration files in advance. For more information, refer to [How to reset the IP DECT phone to custom factory configurations?](#) on page 396.

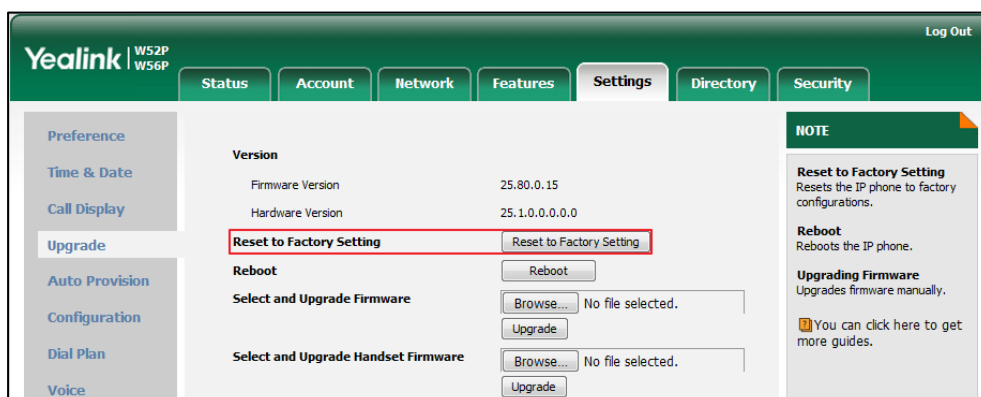
## How to reset the IP DECT phone to factory configurations?

Reset your phone to factory configurations after you have tried all troubleshooting suggestions but do not solve the problem. Note that all custom settings will be overwritten after resetting.

**To reset the IP DECT phone via web user interface:**

1. Click on **Settings->Upgrade**.
2. Click **Reset to Factory Setting** 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 IP DECT phone will be reset to factory successfully after startup.

### Note

Reset of your phone may take a few minutes. Do not power off until the phone starts up successfully.

## How to reset the IP DECT phone to custom factory configurations?

### Procedure

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

<b>Configuration File</b>	y000000000025.cfg	Configure the Custom Factory Configuration feature. <b>Parameters:</b> features.custom_factory_config.enable
		Configure the access URL of the custom factory configuration files. <b>Parameters:</b> custom_factory_configuration.url
<b>Local</b>	Web User Interface	Configure the access URL of the custom factory configuration files. <b>Navigate to:</b> http://<phoneIPAddress>/servlet?p=settings-config&q=load

### Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.custom_factory_config.enable	0 or 1	0
<p><b>Description:</b> Enables or disables the Custom Factory Configuration feature.</p> <p><b>0-Disabled</b> <b>1-Enabled</b></p> <p>If it is set to 1 (Enabled), <b>Import Factory Configuration</b> item will be displayed on the IP DECT phone's web user interface at the path <b>Settings-&gt;Configuration</b>. You can import a custom factory configuration file or delete the user-defined factory configuration via web user interface.</p> <p><b>Web User Interface:</b> None</p> <p><b>Handset User Interface:</b> None</p>		



Parameters	Permitted Values	Default
custom_factory_configuration.url	URL within 511 characters	Blank

**Description:**  
Configures the access URL of the custom factory configuration files.

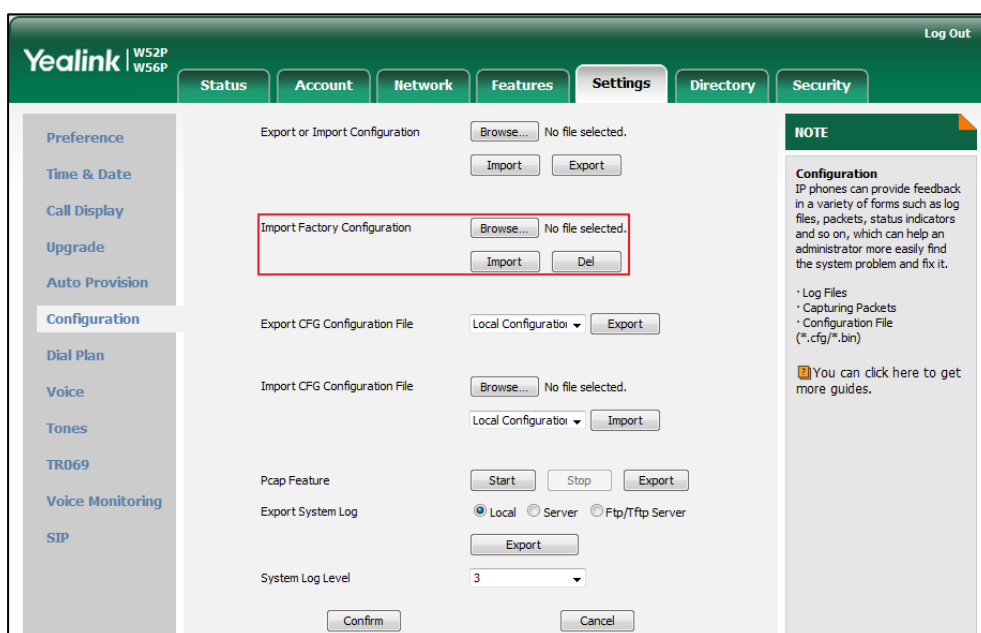
**Note:** It works only if the value of the parameter “features.custom\_factory\_config.enable” is set to 1 (Enabled) and the file format of custom factory configuration file must be \*.bin. If you change this parameter, the base station will reboot to make the change take effect.

**Web User Interface:**  
Settings->Configuration->Import Factory Configuration

**Handset User Interface:**  
None

To import the custom factory configuration files via web user interface:

1. Click on **Settings->Configuration**.
2. Click **Browse** to locate the custom factory configuration file from your local system.



3. Click **Import**.

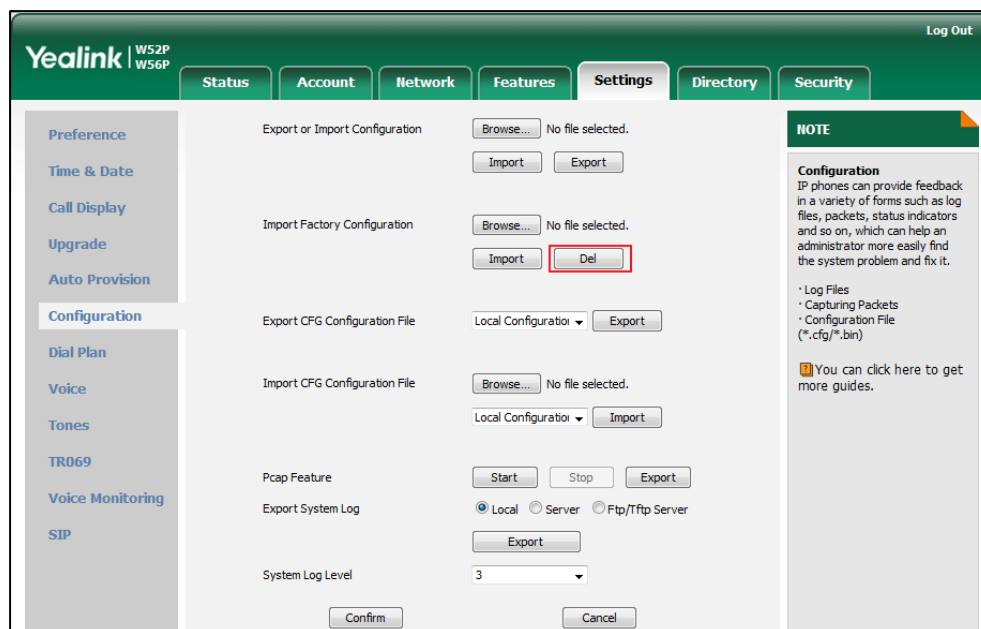
When the custom factory configuration file is imported successfully, you can reset the IP DECT phone to custom factory configurations. For more information on how to reset to factory configuration via web user interface, refer to [How to reset the IP DECT phone to factory configurations?](#) on page 395.

You can delete the user-defined factory configurations via web user interface.

To delete the custom factory configuration files via web user interface:

1. Click on **Settings->Configuration**.
2. Click **Del** in the **Import Factory Configuration** field.

The web user interface prompts the message "Are you sure delete user-defined factory configuration?".



3. Click **OK** to delete the custom factory configuration files.

The imported custom factory file will be deleted. The IP DECT phone will be reset to default factory configurations after resetting.

## Password Issues

### How to restore the administrator password?

Factory reset can restore the original password. All custom settings will be overwritten after reset.

## System Log Issue

### Why can't I export the system log to a provisioning server (FTP/TFTP server)?

Do one of the following:

- Ensure that the FTP/TFTP server is downloaded and installed on your local system.
- Ensure that you have configured the FTP/TFTP server address correctly via web user interface on your IP DECT phone.
- Reboot the base station. The configurations require a reboot to take effect.

### Why can't I export the system log to a syslog server?

Do one of the following:

- Ensure that the syslog server supports saving the syslog files exported from IP DECT phone.
- Ensure that you have configured the syslog server address correctly via web user interface on your IP DECT phone.
- Reboot the base station. The configurations require a reboot to take effect.

## Hardware Issue

### Why is the sending/receiving volume of the headset or handset too low?

Ensure that the headset or handset is not damaged. If the headset or handset is usable, it may be the codec problem on the mainboard.

### Why is there no response when pressing the keys on the keypad?

Do one of the following:

- Ensure that the keypad cables is properly connected and not damaged.

- Check if the keypad surface is clean.

## Other Issues

### How to recognize the area of handset?

To recognize the area of handset via the handset:

1. Press **OK** to enter the main menu.
2. Select **Settings->Handset**.

The LCD screen displays status information of handset status, you can press ▲ or ▼ to scroll through to the **Area** field.

### What is the difference among 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.

### What do "on code" and "off code" mean?

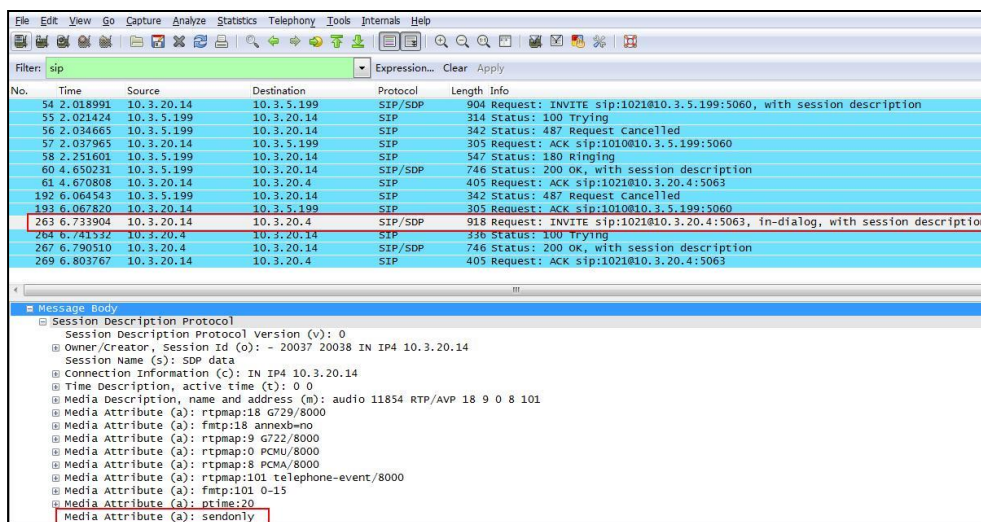
They are codes that the IP DECT phone sends to the server when a certain action takes place. On code is used to activate a feature on the server side, while off code is used to deactivate a feature on the server side.

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 DECT phone, the IP DECT phone sends \*78201 to the server, and then the server will enable Always Forward feature on the server side, hence being able to get the right status of the extension.

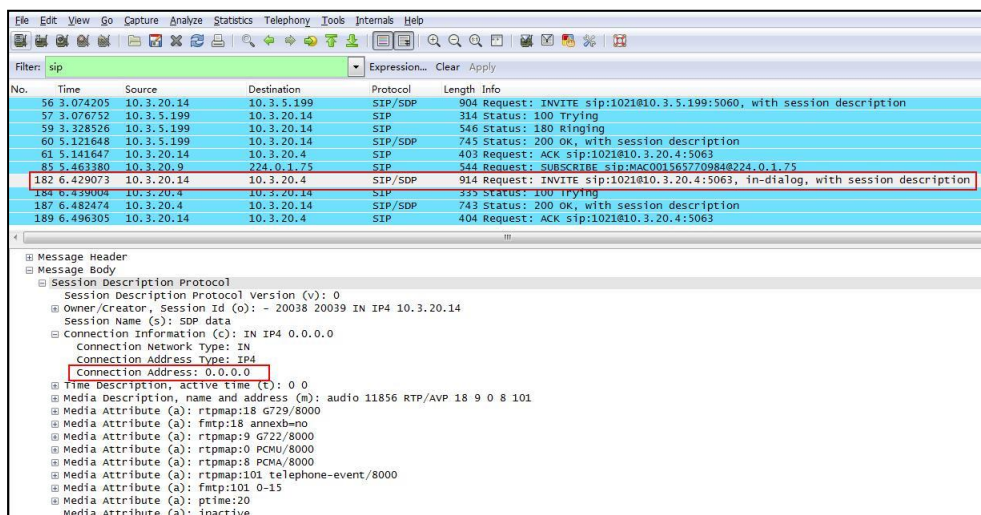
For anonymous call/anonymous call rejection feature, the phone will send either the on code or off code to the server according to the value of Send Anonymous Code/Send Rejection Code. For more information, refer to [Anonymous Call](#) on page 179 and [Anonymous Call Rejection](#) on page 183.

## What is the difference between enabling and disabling the RFC 2543 Hold feature?

Capturing packets after you enable the RFC 2543 Hold feature. SDP media direction attributes (such as a=sendonly) per RFC 2543 is used in the INVITE message when placing a call on hold.



Capturing packets after you disable the RFC 2543 Hold feature. SDP media connection address c=0.0.0.0 per RFC 3264 is used in the INVITE message when placing a call on hold.



For more information on RFC 2543 hold feature, refer to [Call Hold](#) on page 201. For more information on capturing packets, refer to [Capturing Packets](#) on page 383.



---

# 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 provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

**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 DECT 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	Samoa
-10	United States-Hawaii-Aleutian, United States-Alaska-Aleutian
-9:30	French Polynesia
-9	United States-Alaska Time
-8	Canada(Vancouver,Whitehorse), Mexico(Tijuana,Mexicali), United States-Pacific Time
-7	Canada(Edmonton,Calgary),Mexico(Mazatlan,Chihuahua), United States-MST no DST, United States-Mountain Time
-6	Canada-Manitoba(Winnipeg),Chile(Easter Islands),Mexico(Mexico City,Acapulco),United States-Central Time
-5	Bahamas(Nassau),Canada(Montreal,Ottawa,Quebec),Cuba(Havana),United States-Eastern Time
-4:30	Venezuela(Caracas)
-4	Canada(Halifax,Saint John),Chile(Santiago),Paraguay(Asuncion), United Kingdom-Bermuda(Bermuda), United Kingdom(Falkland Islands), Trinidad&Tobago
-3:30	Canada-New Foundland(St.Johns)
-3	Argentina(Buenos Aires),Brazil(DST), Brazil(no DST), Denmark-Greenland(Nuuk)
-2:30	Newfoundland and Labrador
-2	Brazil(no DST)
-1	Portugal(Azores)
0	Denmark-Faroe Islands(Torshavn), GMT, Greenland, Ireland(Dublin), Morocco, Portugal(Lisboa,Porto,Funchal), Spain-Canary Islands(Las Palmas), United Kingdom(London)
+1	Albania(Tirane), Austria(Vienna), Belgium(Brussels), Caicos, Chad, Croatia(Zagreb), Czech Republic(Prague), Denmark(Kopenhagen), France(Paris), Germany(Berlin), Hungary(Budapest), Italy(Rome), Luxembourg(Luxembourg), Macedonia(Skopje), Namibia(Windhoek), Netherlands(Amsterdam), Spain(Madrid)
+2	Estonia(Tallinn), Finland(Helsinki), Gaza Strip(Gaza), Greece(Athens), Israel(Tel Aviv), Jordan(Amman), Latvia(Riga), Lebanon(Beirut), Moldova(Kishinev), Romania(Bucharest), Russia(Kaliningrad), Syria(Damascus), Turkey(Ankara), Ukraine(Kyiv, Odessa)
+3	East Africa Time,Iraq(Baghdad),Russia(Moscow)
+3:30	Iran(Teheran)
+4	Armenia(Yerevan), Azerbaijan(Baku), Georgia(Tbilisi),Kazakhstan(Aktau),Russia(Samara)
+4:30	Afghanistan(Kabul)
+5	Kazakhstan(Aqtobe),Kyrgyzstan(Bishkek),Pakistan(Islamabad),Russia(Chelyabinsk)
+5:30	India(Calcutta)

Time Zone	Time Zone Name
+5:45	Nepal(Katmandu)
+6	Kazakhstan(Astana, Almaty),Russia(Novosibirsk,Omsk)
+6:30	Myanmar(Naypyitaw)
+7	Russia(Krasnoyarsk), Thailand(Bangkok)
+8	Australia(Perth),China(Beijing),Russia(Irkutsk, Ulan-Ude), Singapore(Singapore)
+8:45	Eucla
+9	Japan(Tokyo),Korea(Seoul),Russia(Yakutsk,Chita)
+9:30	Australia(Adelaide), Australia(Darwin)
+10	Australia(Brisbane), Australia(Hobart), Australia(Sydney,Melbourne,Canberra), Russia(Vladivostok)
+10:30	Australia(Lord Howe Islands)
+11	New Caledonia(Noumea),Russia(Srednekolymsk Time)
+11:30	Norfolk Island
+12	New Zealand(Wellington,Auckland),Russia(Kamchatka Time)
+12:45	New Zealand(Chatham Islands)
+13	Tonga(Nukualofa)
+13:30	Chatham Islands
+14	Kiribati

## Appendix C: Trusted Certificates

Yealink IP DECT phones trust the following CAs by default:

- DigiCert High Assurance EV Root CA
- Deutsche Telekom AG Root CA-2
- Equifax Secure Certificate Authority
- Equifax Secure eBusiness CA-1
- Equifax Secure Global eBusiness CA-1
- GeoTrust Global CA
- GeoTrust Global CA2
- GeoTrust Primary CA
- GeoTrust Primary CA G2 ECC
- GeoTrust Universal CA
- GeoTrust Universal CA2
- Thawte Personal Freemail CA
- Thawte Premium Server CA
- Thawte Primary Root CA - G1 (EV)
- Thawte Primary Root CA - G2 (ECC)

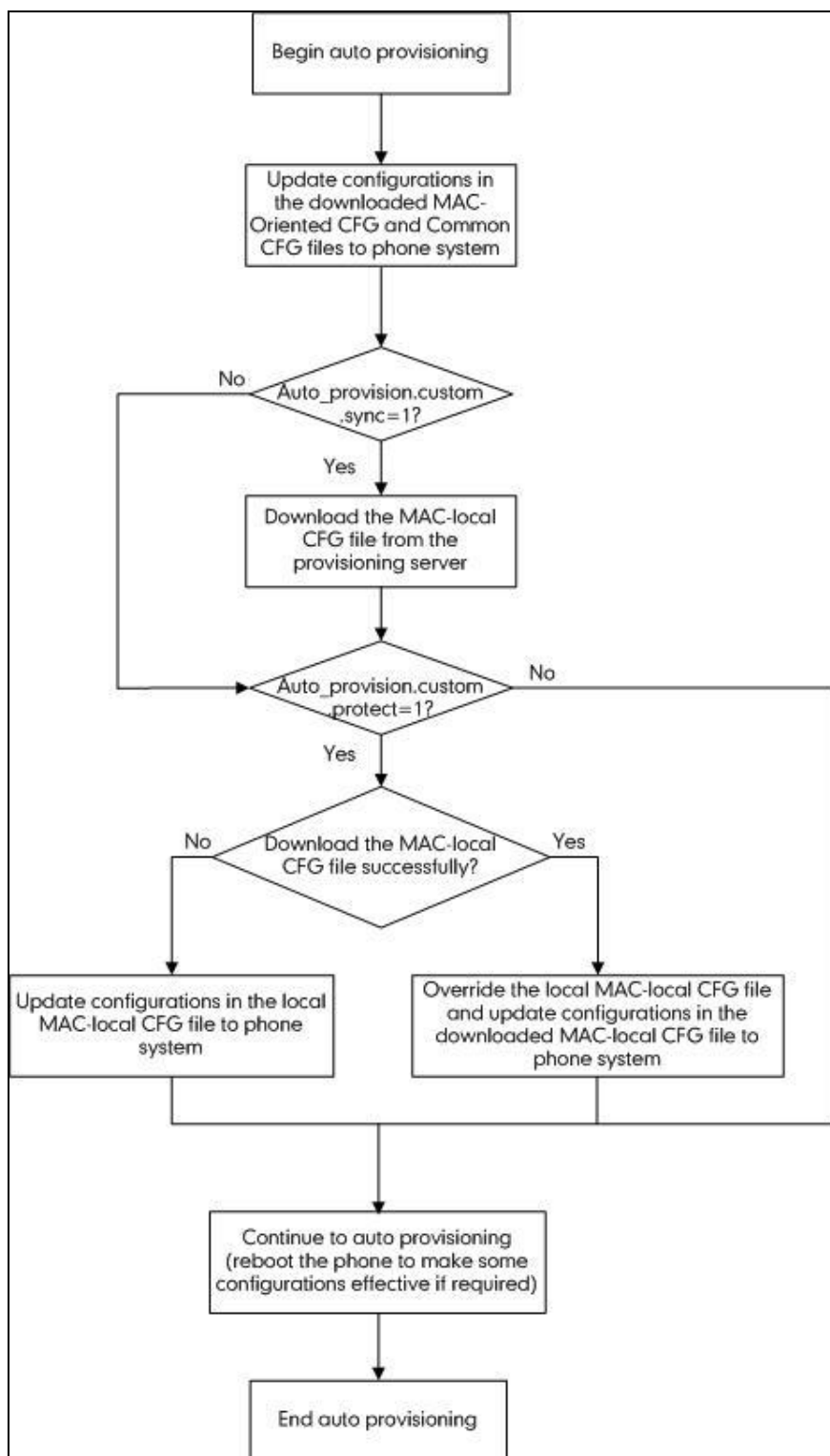
- Thawte Primary Root CA - G3 (SHA256)
- Thawte Server CA
- VeriSign Class 1 Public Primary Certification Authority
- VeriSign Class 1 Public Primary Certification Authority - G2
- VeriSign Class 1 Public Primary Certification Authority - G3
- VeriSign Class 2 Public Primary Certification Authority - G2
- VeriSign Class 2 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority
- VeriSign Class 3 Public Primary Certification Authority - G2
- VeriSign Class 3 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority - G4
- VeriSign Class 3 Public Primary Certification Authority - G5
- VeriSign Class 4 Public Primary Certification Authority - G2
- VeriSign Class 4 Public Primary Certification Authority - G3
- VeriSign Universal Root Certification Authority

**Note**

Yealink endeavors to maintain a built-in list of most common used CA Certificates. Due to memory constraints, we cannot ensure a complete set of certificates. If you are using a certificate from a commercial Certificate Authority not in the list above, you can send a request to your local distributor. At this point, you can upload your particular CA certificate into your phone. For more information on uploading custom CA certificate, refer to [Transport Layer Security](#) on page 350.

## Appendix D: Auto Provisioning Flowchart (Keep user personalized configuration settings)

The following shows auto provisioning flowchart for Yealink IP DECT phones when a user wishes to keep user personalized configuration settings.



## Appendix E: Configurations Defined Never be Saved to <MAC>-local.cfg file

The following tables list all the configurations defined never be saved to <MAC>-local.cfg file.

Item	Configurations
Server Type	account.X.sip_server_type
	account.X.xsi.server_type
Network	network.dhcp_host_name
	network.pppoe.user
	network.pppoe.password
	network.static_dns_enable
	network.ipv6_static_dns_enable
	network.vlan.internet_port_enable
	network.vlan.internet_port_vid
	network.vlan.internet_port_priority
	network.vlan.dhcp_enable
	network.vlan.dhcp_option
	network.port.http
	network.port.https
	network.qos.rtptos
	network.qos.signaltos
	network.802_1x.mode
	network.802_1x.identity
	network.802_1x.md5_password
	network.802_1x.client_cert_url
	network.vpn_enable
	network.ldap.enable
network.ldap.packet_interval	
network.port.max_rtpport	
network.port.min_rtpport	
network.ipv6_prefix	

Item	Configurations
	network.ipv6_internet_port.type
	network.ipv6_internet_port.ip
	network.ipv6_internet_port.gateway
	network.ipv6_primary_dns
	network.ipv6_secondary_dns
	network.ipv6_icmp_v6.enable
	network.internet_port.type
	network.internet_port.ip
	network.internet_port.mask
	network.internet_port.gateway
	network.primary_dns
	network.secondary_dns
Openvpn	openvpn.url
Security	security.user_name.user
	security.user_name.admin
	security.user_name.var
	security.user_password
	security.trust_certificates
	security.ca_cert
	security.dev_cert
	security.cn_validation
	security.var_enable
	trusted_certificates.url
	trusted_certificates.delete
	server_certificates.url
	server_certificates.delete
	wui.https_enable
	wui.http_enable
Log	syslog.mode
	syslog.server
	syslog.log_level

Item	Configurations
Autoprovision	auto_provision.custom.sync
	auto_provision.custom.protect
	auto_provision.custom.upload_method
	auto_provision.power_on
	auto_provision.pnp_enable
	auto_provision.dhcp_option.enable
	auto_provision.dhcp_option.list_user_options
	auto_provision.repeat.enable
	auto_provision.repeat.minutes
	auto_provision.weekly.enable
	auto_provision.weekly.dayofweek
	auto_provision.weekly.begin_time
	auto_provision.weekly.end_time
	auto_provision.server.url
	auto_provision.server.username
	auto_provision.server.password
	auto_provision.attempt_expired_time
	auto_provision.aes_key_16.com
	auto_provision.aes_key_16.mac
	auto_provision.aes_key_in_file
	auto_provision.dhcp_option.option60_value
	auto_provision.reboot_force.enable
	auto_provision.url_wildcard.pn
	autoprovision.X.name
	autoprovision.X.code
	autoprovision.X.user
	autoprovision.X.password
	autoprovision.X.url
	autoprovision.X.com_aes
	autoprovision.X.mac_aes
SIP	sip.notify_reboot_enable

Item	Configurations
	sip.escape_characters.enable sip.listen_mode sip.reserve_characters sip.use_23_as_pound sip.rfc2543_hold account.X.custom_ua sip.reg_surge_prevention sip.send_response_by_request sip.refer_by_header_auto_build sip.tcp_port_random_mode sip.use_out_bound_in_dialog account.X.hoteling.password account.X.xsi.password account.X.password managementserver.connection_request_password managementserver.password
DND&Forward	account.X.always_fwd.enable account.X.always_fwd.target account.X.always_fwd.off_code account.X.always_fwd.on_code account.X.busy_fwd.enable account.X.busy_fwd.target account.X.busy_fwd.off_code account.X.busy_fwd.on_code account.X.timeout_fwd.enable account.X.timeout_fwd.target account.X.timeout_fwd.timeout account.X.timeout_fwd.off_code account.X.timeout_fwd.on_code account.X.dnd.enable account.X.dnd.off_code



Item	Configurations
	account.X.dnd.on_code
	features.fwd_mode
	features.dnd_refuse_code
Feature access code	account.X.anonymous_call_oncode
	account.X.anonymous_call_offcode
	account.X.anonymous_reject_oncode
	account.X.anonymous_reject_offcode
	voice_mail.number.X
Access URL of the xml format resource files/configuration files	custom_mac_cfg.url
	dialplan_replace_rule.url
	remote_phonebook.data.X.url
	web_item_level.url
	trusted_certificates.url
	server_certificates.url
	custom_factory_configuration.url
	configuration.url
	firmware.url
DNS	dns_cache_a.X.name
	dns_cache_a.X.ip
	dns_cache_a.X.ttl
	dns_cache_srv.X.name
	dns_cache_srv.X.port
	dns_cache_srv.X.priority
	dns_cache_srv.X.target
	dns_cache_srv.X.weight
	dns_cache_srv.X.ttl
	dns_cache_naptr.X.name
	dns_cache_naptr.X.flags
	dns_cache_naptr.X.order
	dns_cache_naptr.X.preference
	dns_cache_naptr.X.replace

Item	Configurations
	dns_cache_naptr.X.service
	dns_cache_naptr.X.ttl
Configurations requiring a reboot during auto provisioning	features.relog_offtime
	bw.enable

## Appendix F: SIP (Session Initiation Protocol)

This section describes how Yealink IP DECT 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 2327—SDP: Session Description Protocol
- RFC 2387—The MIME Multipart/Related Content-type
- RFC 2543—SIP: Session Initiation Protocol
- 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 2976—The SIP INFO Method
- 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 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 3398—ISUP to SIP Mapping
- 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: Transport Protocol for Real-Time Applications
- RFC 3555—MIME Type Registration of RTP Payload Formats
- RFC 3581—An Extension to the SIP for Symmetric Response Routing
- RFC 3608—SIP Extension Header Field for Service Route Discovery During Registration
- RFC 3611—RTP Control Protocol Extended Reports (RTCP XR)
- 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 3863—Presence Information Data Format

- 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—IANA Registry for SIP Header Field
- RFC 3969—IANA Registry for SIP URI
- RFC 4028—Session Timers in the Session Initiation Protocol (SIP)
- RFC 4083—3GPP Release 5 Requirements on 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 4458—SIP URIs for Applications such as Voicemail and Interactive Voice Response (IVR)
- 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 4583—Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams
- RFC 4662—A SIP Event Notification Extension for Resource Lists
- RFC 4730—Event Package for KPML
- 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
- RFC 5630—The Use of the SIPS URI Scheme in SIP
- RFC 5806—Diversion Indication in SIP
- RFC 5954—Essential Correction for IPv6 ABNF and URI Comparison in RFC 3261
- RFC 6026—Correct Transaction Handling for 2xx Responses to SIP INVITE Requests
- RFC 6141—Re-INVITE and Target-Refresh Request Handling 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-anil-sipping-bla-03.txt—Implementing Bridged Line Appearances (BLA) Using Session Initiation Protocol (SIP)
- draft-ietf-sip-privacy-00.txt—SIP Extensions for Caller Identity and Privacy, November
- draft-ietf-sip-privacy-04.txt—SIP Extensions for Network-Asserted Caller Identity and Privacy within Trusted Networks
- draft-levy-sip-diversion-08.txt—Diversion Indication in SIP
- draft-ietf-sipping-cc-conferencing-03.txt—SIP Call Control - Conferencing for User Agents
- draft-ietf-sipping-cc-conferencing-05.txt—Connection Reuse in the Session Initiation Protocol (SIP)
- draft-ietf-sipping-rtc-summary-02.txt—Session Initiation Protocol Package for Voice Quality Reporting Event
- draft-ietf-sip-connect-reuse-06.txt—Connection Reuse in the Session Initiation Protocol (SIP)
- draft-ietf-bliss-shared-appearances-15.txt—Shared Appearances of a Session Initiation Protocol (SIP) Address of Record (AOR)

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 IP DECT phones support mid-call changes such as placing a call on hold as signaled by a new INVITE that contains an existing Call-ID.
ACK	Yes	
CANCEL	Yes	
BYE	Yes	
OPTIONS	Yes	

Method	Supported	Notes
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:

### Note

In the following table, a "Yes" in the Supported column means the header is sent and properly parsed.

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	
History-Info	Yes	
Event	Yes	
Expires	Yes	

Method	Supported	Notes
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	
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:

**Note**

In the following table, a “Yes” in the Supported column means the header is sent and properly parsed. The phone may not actually generate the response.

### 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	
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	



4xx Response	Supported	Notes
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	
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 G: 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 DECT 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

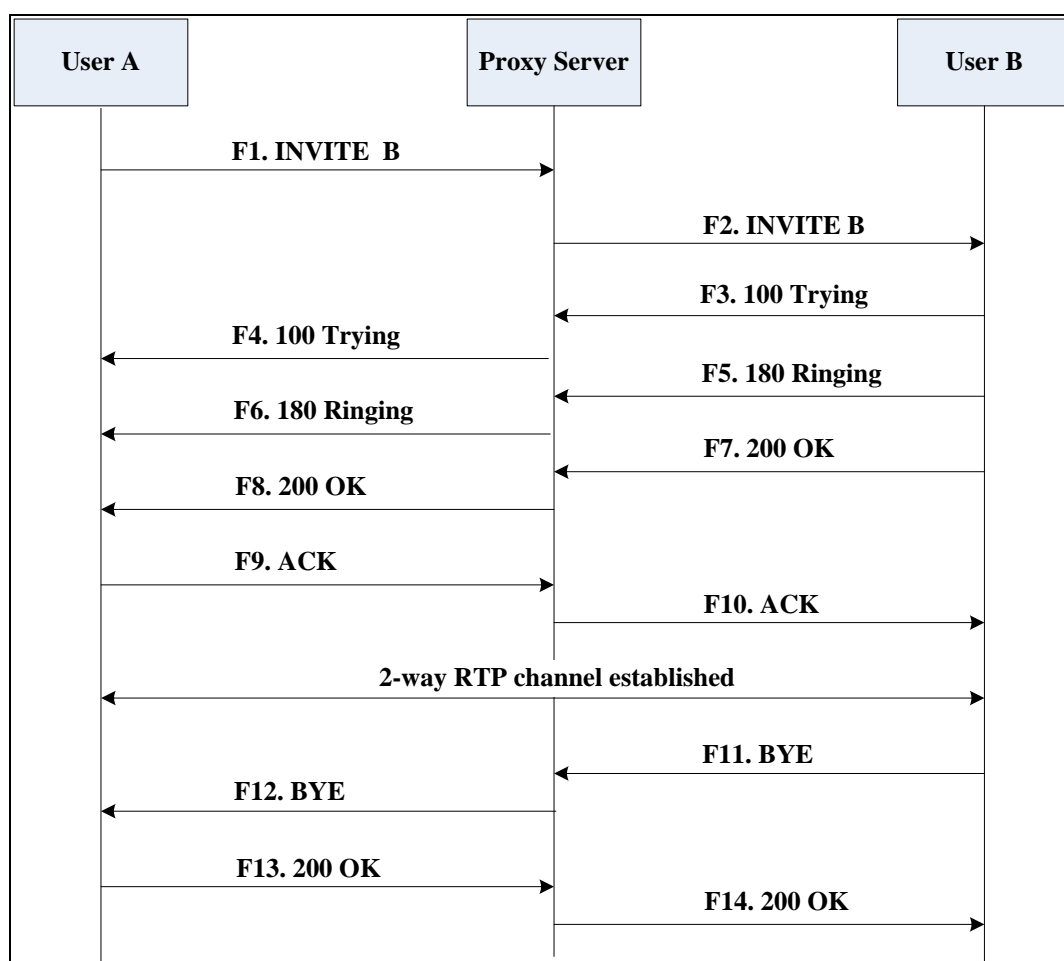
SIP 6xx—Global Failure Responses

## 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 DECT 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"> <li>• The IP address of User B is inserted in the Request-URI field.</li> <li>• User A is identified as the call session initiator in the From field.</li> <li>• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li> <li>• The transaction number within a single call leg is identified in the CSeq field.</li> <li>• The media capability User A is ready to receive is specified.</li> <li>• The port on which User B is prepared to receive the RTP data is specified.</li> </ul>
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.

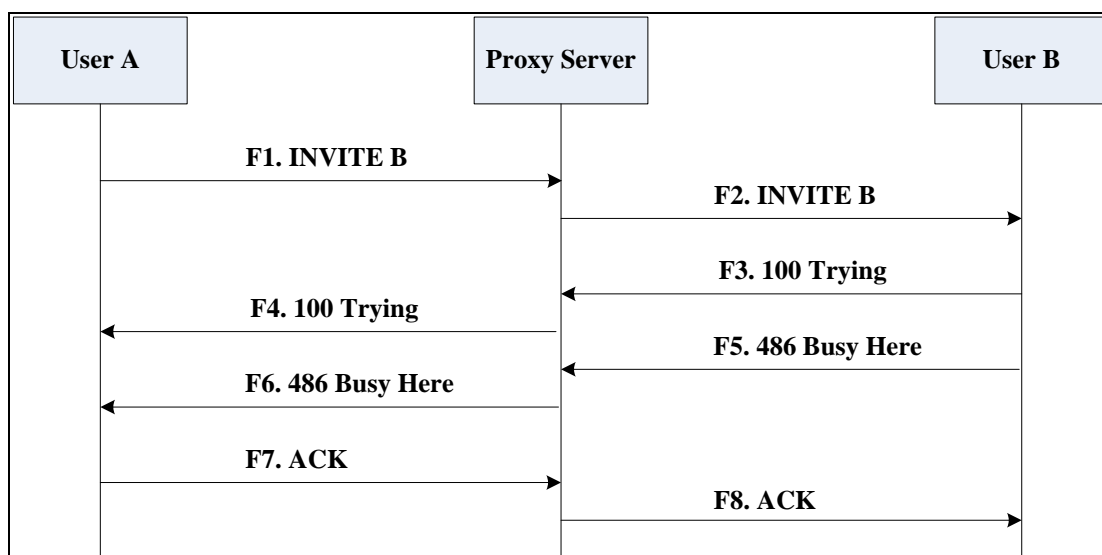
Step	Action	Description
F7	200 OK— User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F8	200OK—Proxy Server to User A	The proxy server forwards the 200 OK message to User A. The 200 OK response notifies 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 IP DECT phones.

The call flow scenario is as follows:

1. User A calls User B.
2. User B is busy on the IP DECT 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"> <li>• The IP address of User B is inserted in the Request-URI field.</li> <li>• User A is identified as the call session initiator in the From field.</li> <li>• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li> <li>• The transaction number within a single call leg is identified in the CSeq field.</li> <li>• The media capability User A is ready to receive is specified.</li> <li>• The port on which User B is prepared to receive the RTP data is</li> </ul>

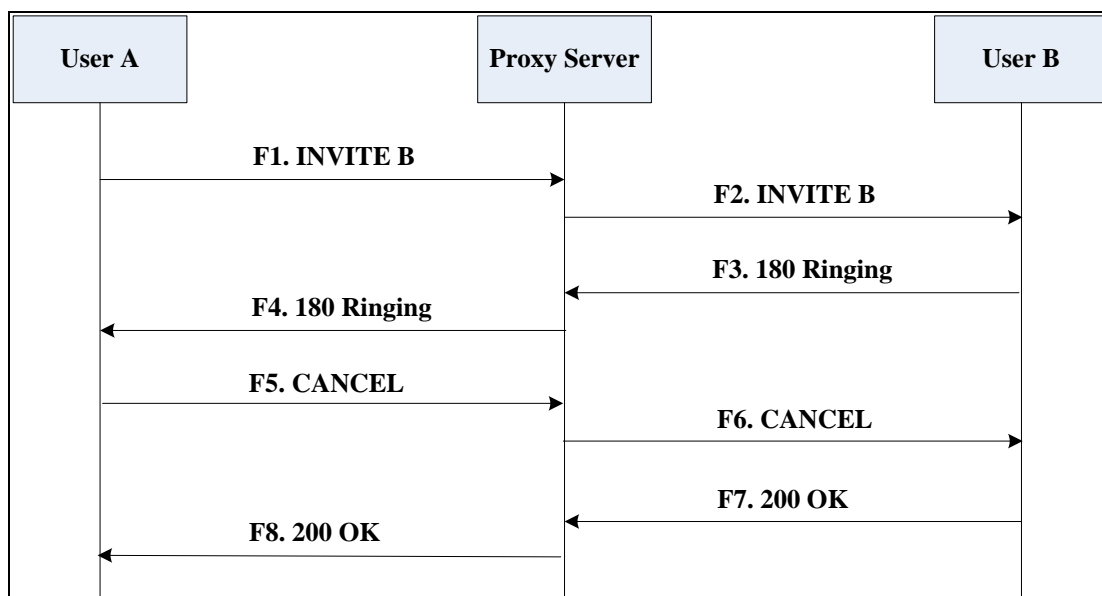
Step	Action	Description
		specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. Proxy server forwards the INVITE message to User B.
F3	100 Trying—User B to Proxy Server	User B sends a SIP 100 Trying response to the proxy server. The 100 Trying response 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 DECT 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 IP DECT 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"> <li>• The IP address of User B is inserted in the Request-URI field.</li> <li>• User A is identified as the call session initiator in the From field.</li> <li>• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li> <li>• The transaction number within a single call leg is identified in the CSeq field.</li> <li>• The media capability User A is ready to receive is specified.</li> </ul>



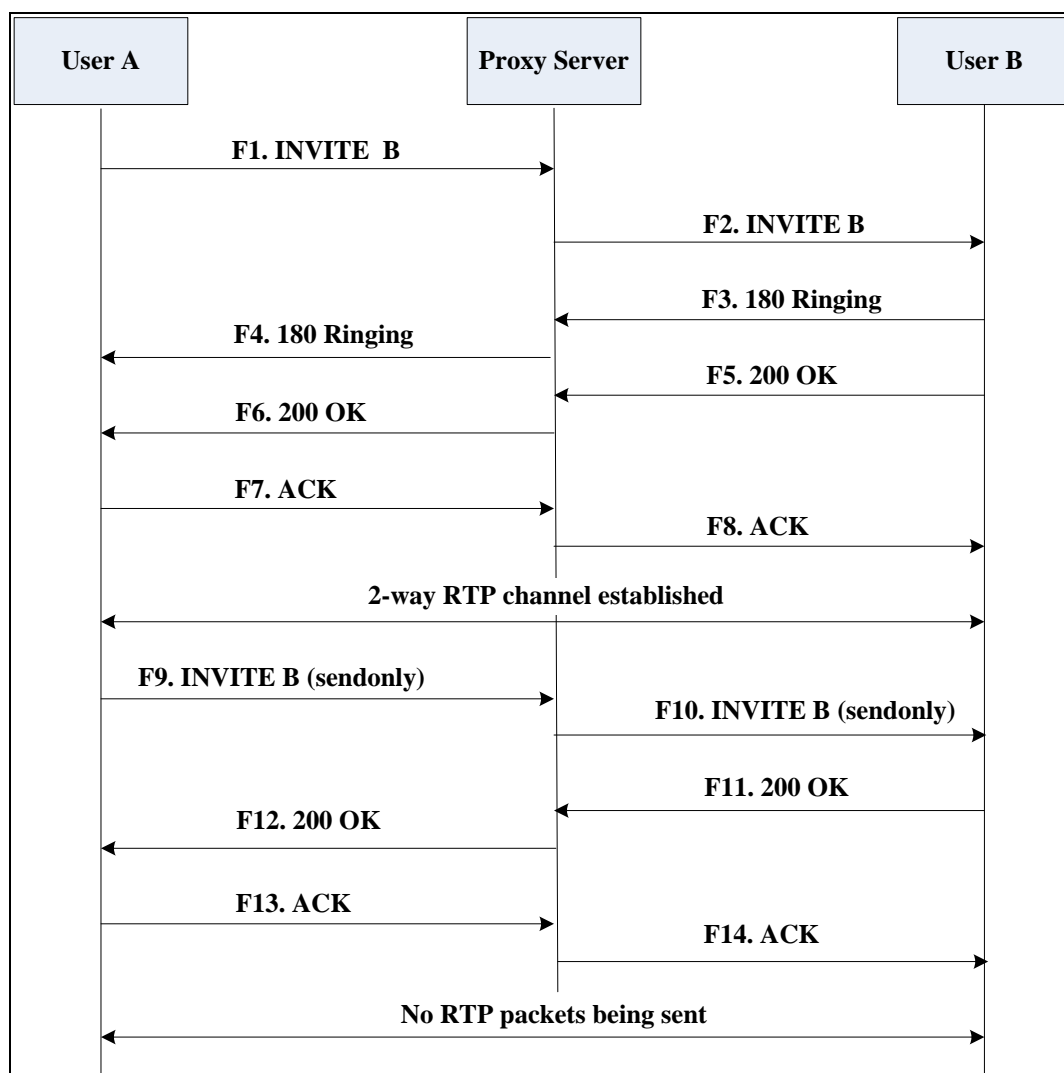
Step	Action	Description
		<ul style="list-style-type: none"> <li>The port on which User B is prepared to receive the RTP data is specified.</li> </ul>
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. Proxy server forwards the INVITE message to User B.
F3	180 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 IP DECT phones.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.
3. User A places 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"> <li>• The IP address of User B is inserted in the Request-URI field.</li> <li>• User A is identified as the call session initiator in the From field.</li> <li>• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li> <li>• The transaction number within a single call leg is identified in the CSeq field.</li> <li>• The media capability User A is ready to receive is specified.</li> <li>• The port on which User B is prepared to receive the RTP data is specified.</li> </ul>
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 placed 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.

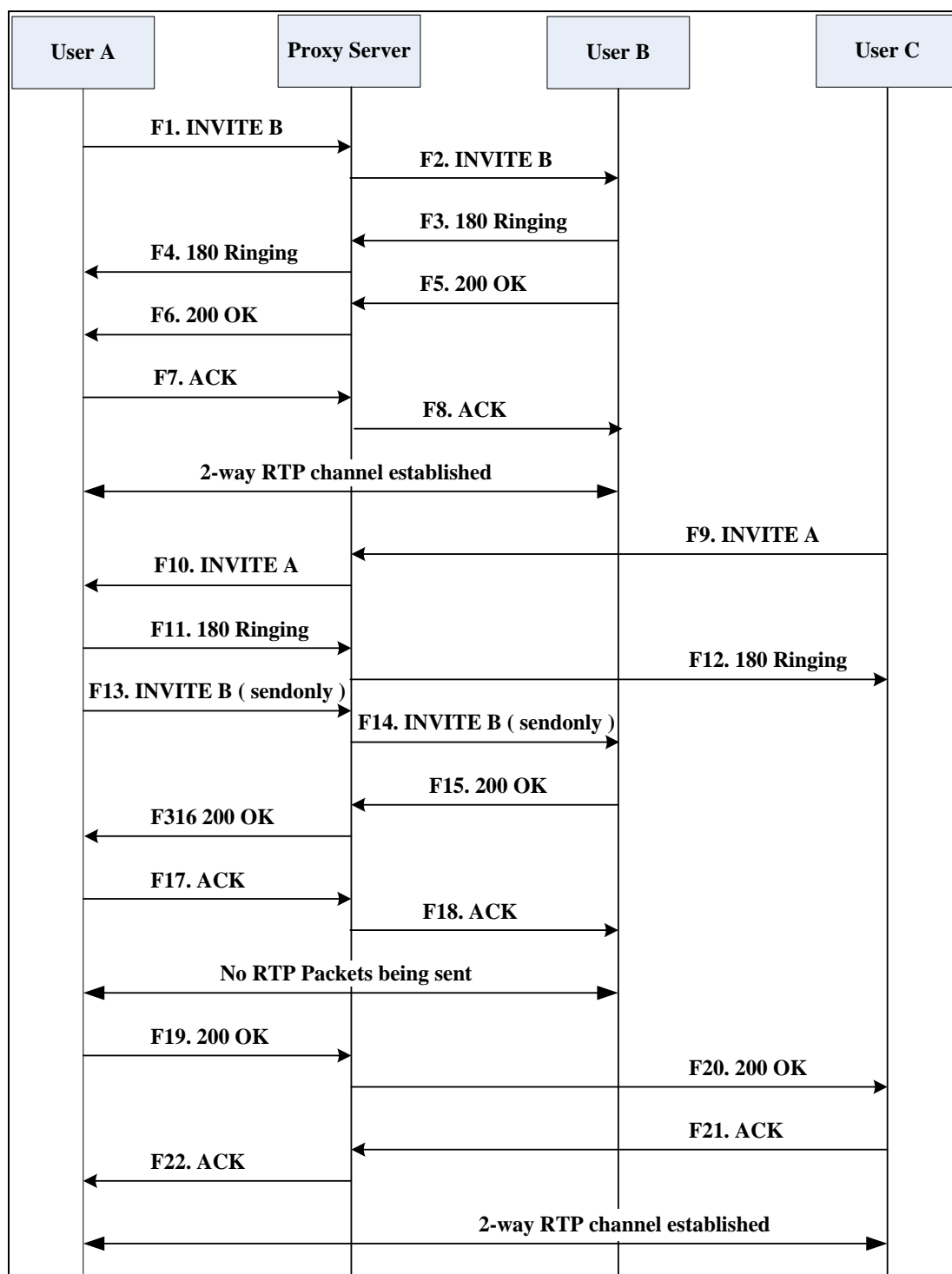
## Successful Call Setup and Call Waiting

The following figure illustrates a successful call between Yealink IP DECT 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 IP DECT 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"> <li>• The IP address of User B is inserted in the Request-URI field.</li> <li>• User A is identified as the call session initiator in the From field.</li> <li>• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li> <li>• The transaction number within a single call leg is identified in the CSeq field.</li> <li>• The media capability User A is ready to receive is specified.</li> <li>• The port on which User B is prepared to receive the RTP data is specified.</li> </ul>
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

Step	Action	Description
		connection has been made.
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"> <li>• The IP address of User A is inserted in the Request-URI field.</li> <li>• User C is identified as the call session initiator in the From field.</li> <li>• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li> <li>• The transaction number within a single call leg is identified in the CSeq field.</li> <li>• The media capability User C is ready to receive is specified.</li> <li>• The port on which User A is prepared to receive the RTP data is specified.</li> </ul>
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

Step	Action	Description
		User A is being alerted.
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 placed 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.



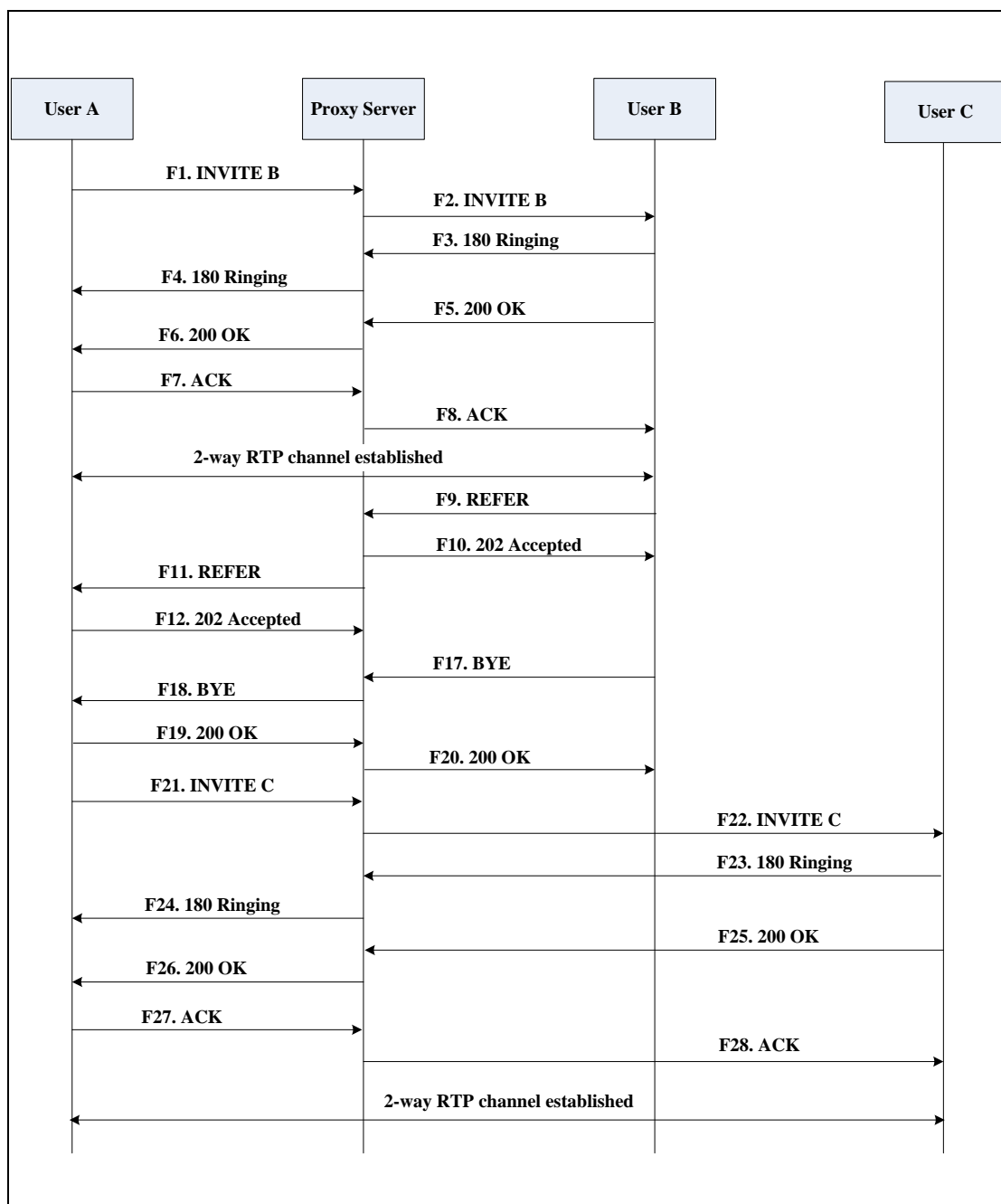
## Call Transfer without Consultation

The following figure illustrates a successful call between Yealink IP DECT phones in which two parties are in a call and then one of the parties transfer 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 IP DECT 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"> <li>• The IP address of User B is inserted in the Request-URI field.</li> <li>• User A is identified as the call session initiator in the From field.</li> <li>• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li> <li>• The transaction number within a single call leg is identified in the CSeq field.</li> <li>• The media capability User A is ready to receive is specified.</li> <li>• The port on which User B is prepared to receive the RTP data is specified.</li> </ul>
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.

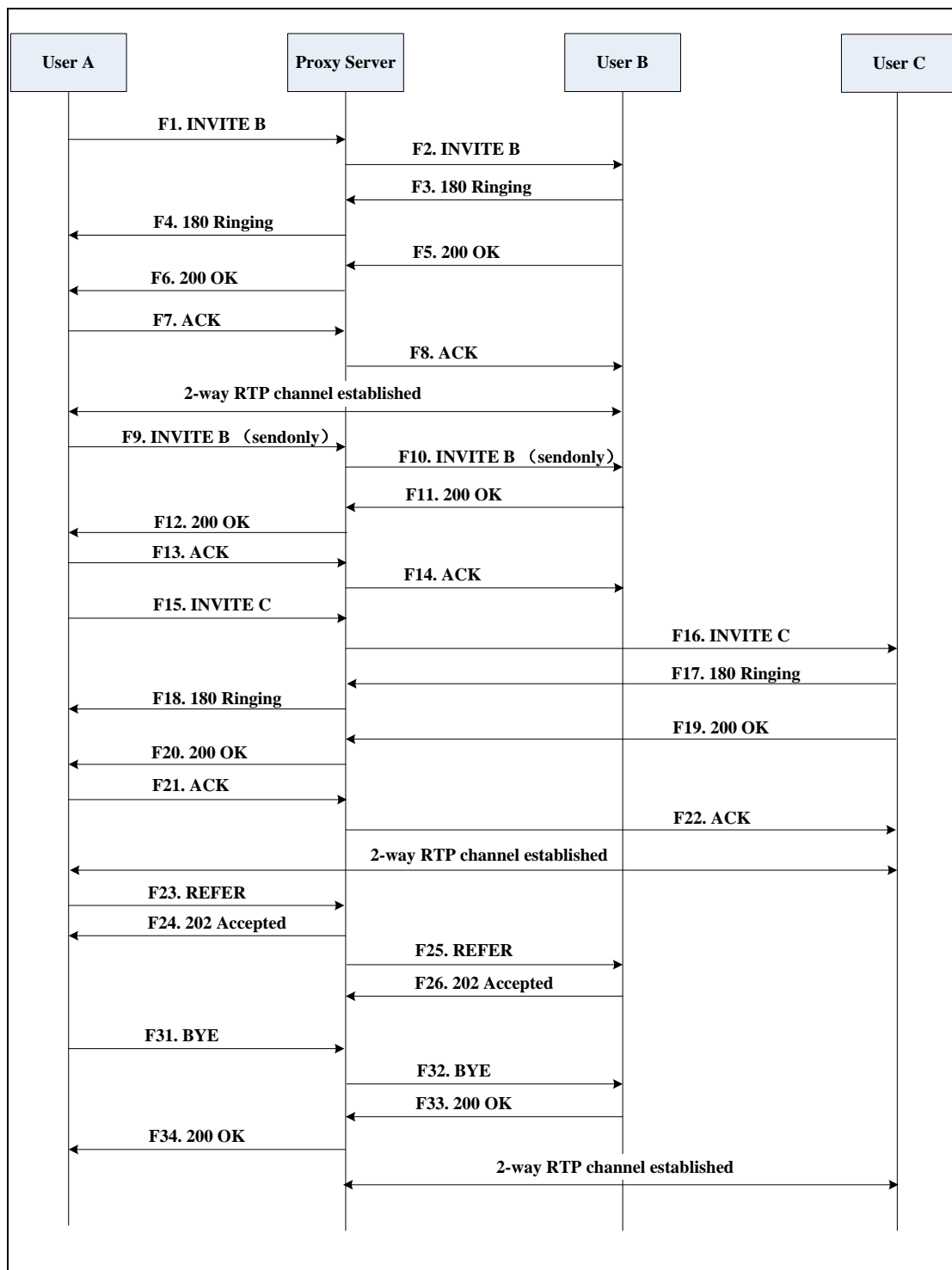
## Call Transfer with Consultation

The following figure illustrates a successful call between Yealink IP DECT 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 IP DECT 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"> <li>• The IP address of User B is inserted in the Request-URI field.</li> <li>• User A is identified as the call session initiator in the From field.</li> <li>• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li> <li>• The transaction number within a single call leg is identified in the CSeq field.</li> <li>• The media capability User A is ready to receive is specified.</li> <li>• The port on which User B is prepared to receive the RTP data is specified.</li> </ul>
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 placed 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 servers



Step	Action	Description
	C	ends 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.

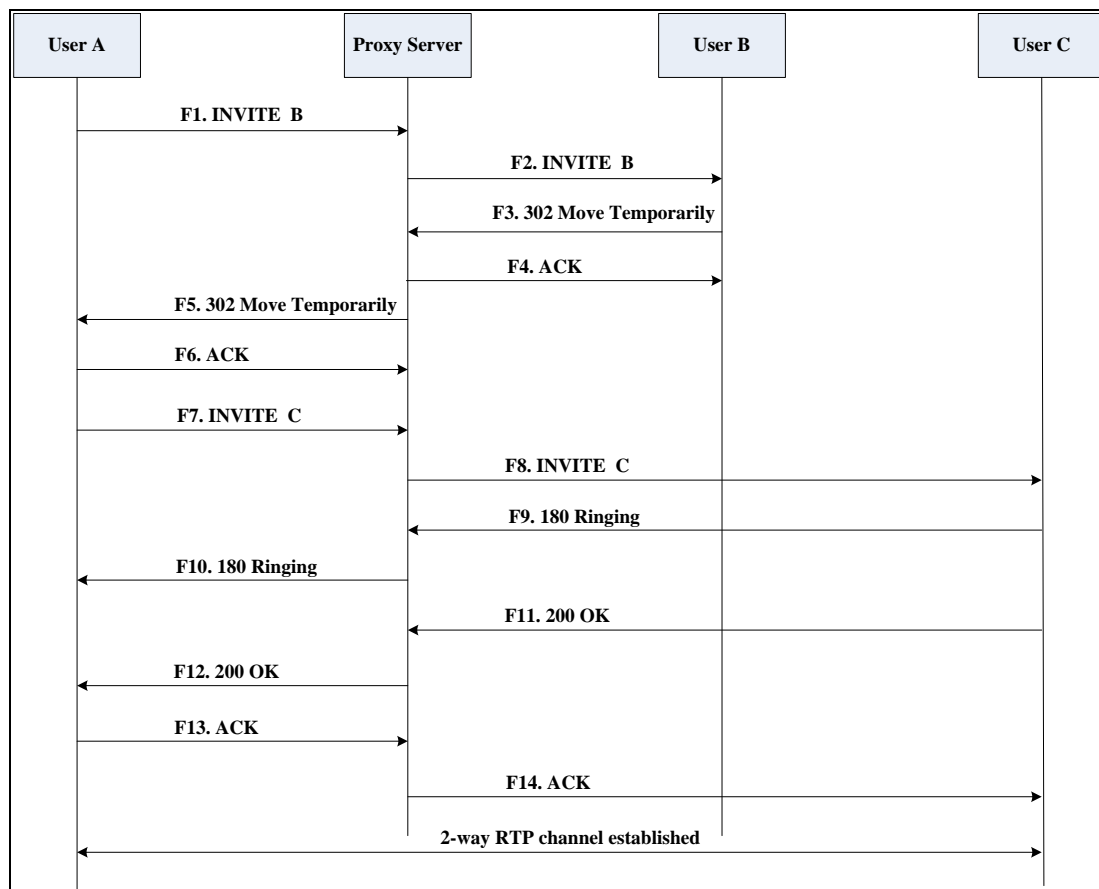
## Always Call Forward

The following figure illustrates successful call forwarding between Yealink IP DECT 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 IP DECT 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.
4. User C answers the call.

## 5. 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"> <li>• The IP address of the User B is inserted in the Request-URI field.</li> <li>• User A is identified as the call session initiator in the From field.</li> <li>• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li> <li>• The transaction number within a single call leg is identified in the CSeq field.</li> <li>• The media capability User A is ready to receive is specified.</li> <li>• The port on which User B is prepared to receive the RTP data is specified.</li> </ul>
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 IP DECT 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

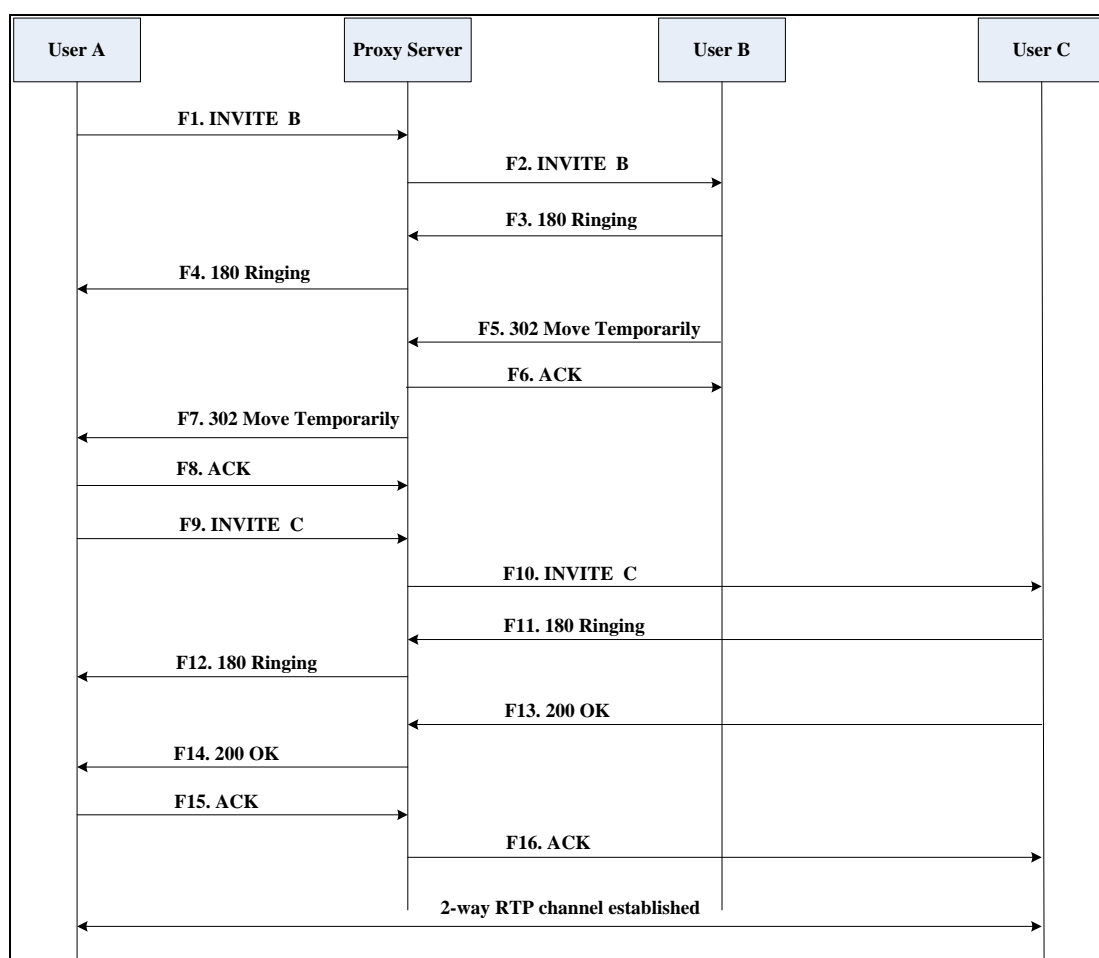
The following figure illustrates successful call forwarding between Yealink IP DECT phones in which User B has enabled busy call forward. The incoming call is forwarded to User C when User B is busy. In this call flow scenario, the end users are User A, User B,

and User C. They are all using Yealink IP DECT 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"> <li>• The IP address of User B is inserted in the Request-URI field.</li> <li>• User A is identified as the call session initiator in the From field.</li> <li>• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li> <li>• The transaction number within a single call leg is identified in the CSeq field.</li> <li>• The media capability User A is ready to receive is specified.</li> <li>• The port on which User B is prepared to receive the RTP data is specified.</li> </ul>
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 IP DECT 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 IP DECT

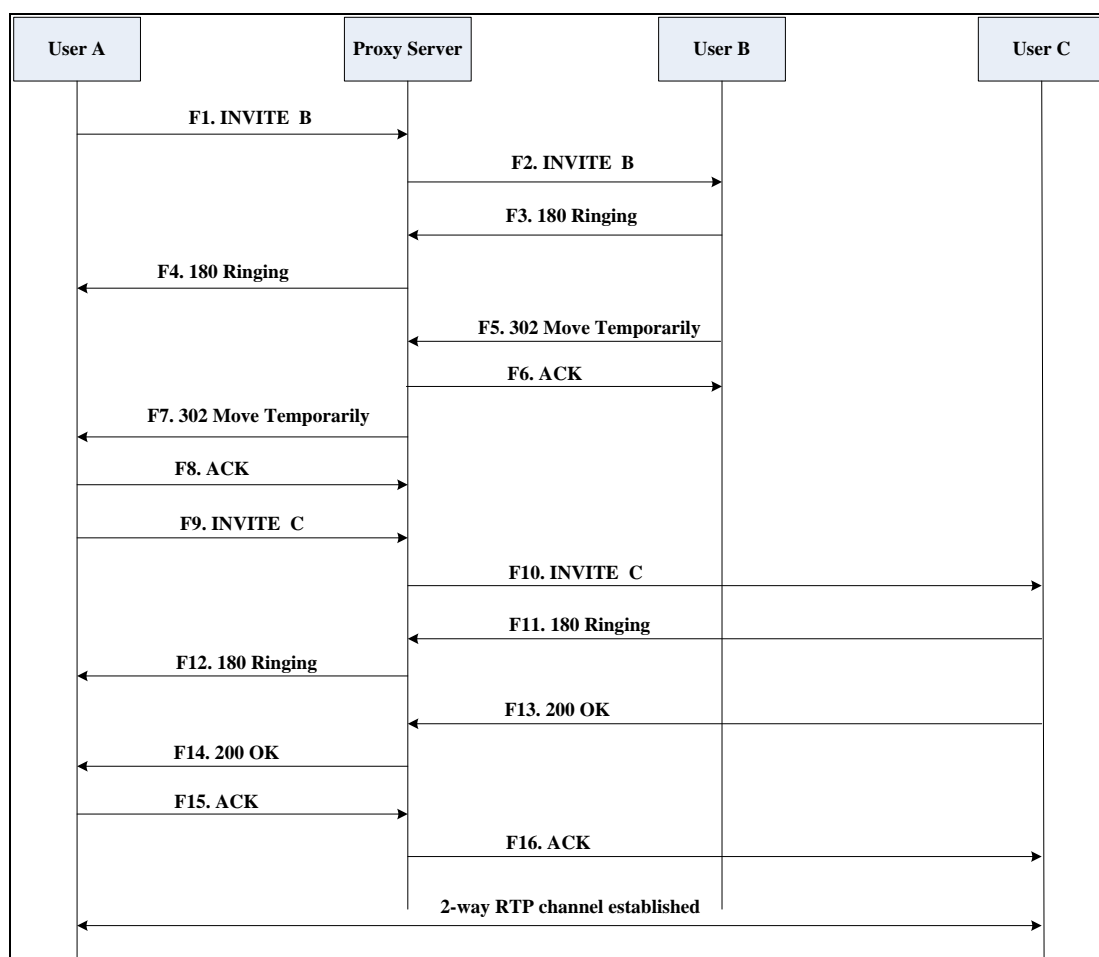


phones in which User B has enabled no answer call forward. The incoming call is forwarded to User C when User B does not answer the incoming call after a period of time. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink IP DECT phones, which are connected 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"> <li>• The IP address of User B is inserted in the Request-URI field.</li> <li>• User A is identified as the call session initiator in the From field.</li> <li>• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li> <li>• The transaction number within a single call leg is identified in the CSeq field.</li> <li>• The media capability User A is ready to receive is specified.</li> <li>• The port on which User B is prepared to receive the RTP data is specified.</li> </ul>
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 IP DECT 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.

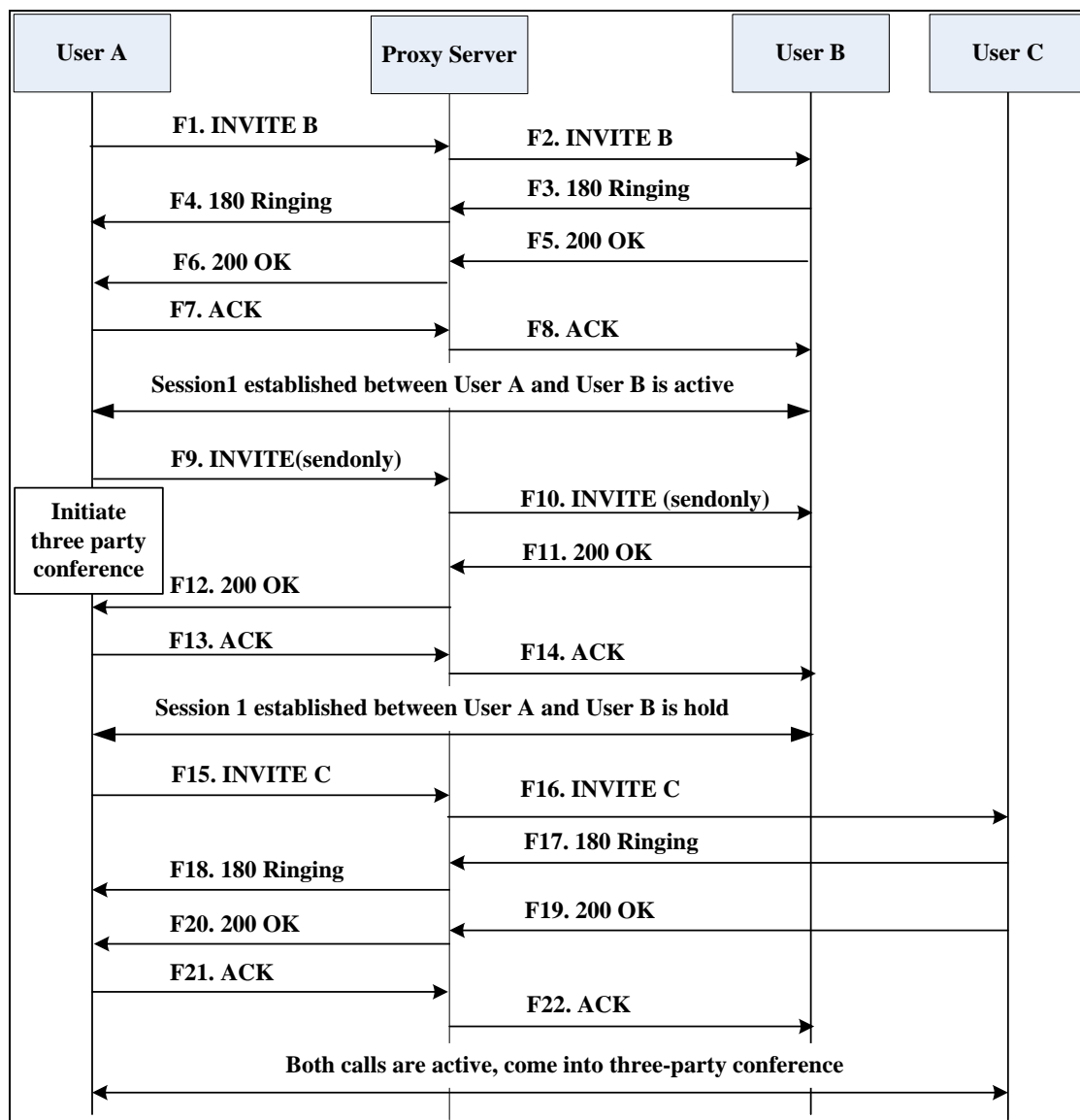
## Call Conference

The following figure illustrates successful 3-way calling between Yealink IP DECT 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 IP DECT 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 places 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"> <li>• The IP address of User B is inserted in the Request-URI field.</li> <li>• User A is identified as the call</li> </ul>

Step	Action	Description
		<p>session initiator in the From field.</p> <ul style="list-style-type: none"> <li>• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li> <li>• The transaction number within a single call leg is identified in the CSeq field.</li> <li>• The media capability User A is ready to receive is specified.</li> <li>• The port on which User B is prepared to receive the RTP data is specified.</li> </ul>
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.
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.

Step	Action	Description
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 placed 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 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.
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

Step	Action	Description
		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.



# Index

## Numeric

- 100 Reliable Retransmission [240](#)
- 180 Ring Workaround [193](#)
- 802.1X Authentication [71](#)

## A

- About This Guide [i](#)
- Accept SIP Trust Server Only [177](#)
- Account Registration [112](#)
- Acoustic Clarity Technology [319](#)
- Administrator Password [345](#)
- Advisory Tone [97](#)
- Allow IP Call [176](#)
- Always Forward [203](#)
- Analyzing Configuration Files [385](#)
- Anonymous Call [179](#)
- Anonymous Call Rejection [183](#)
- Appendix [403](#)
- Appendix A: Glossary [403](#)
- Appendix B: Time Zones [405](#)
- Appendix C: Trusted Certificates [406](#)
- Appendix D: Auto Provisioning Flowchart  
(Keep user personalized configuration settings) [408](#)
- Appendix E Configuration Defined Never be Saved to <MAC>-local.cfg [409](#)
- Appendix F SIP (Session Initiation Protocol) [414](#)
- Appendix G SIP Call Flows [422](#)
- Area Code [153](#)
- Audio Codecs [312](#)
- Audio Issue [392](#)
- Auto Answer [175](#)
- Auto Dial [162](#)
- Auto-Logout Time [346](#)
- Automatic Gain Control [319](#)

## B

- Backlight [99](#)
  - Background Noise Suppression [319](#)
  - Base Issue [389](#)
  - Base PIN [348](#)
  - Base Station [2](#)
  - Battery Information [3](#)
  - Block Out [160](#)
  - Busy Forward [203](#)
  - Busy Tone Delay [190](#)
- ## C
- Call Display [120](#)
  - Call Forward [203](#)
  - Call Hold [201](#)
  - Call Number Filter [220](#)
  - Call Timeout [230](#)
  - Call Transfer
  - Call Waiting [167](#)
  - Calling Line Identification Presentation (CLIP) [219](#)
  - Capturing Packets [383](#)
  - Central Provisioning
  - Characters Supported [17](#)
  - Charging the Handset [8](#)
  - Clearing Personalized Settings of the Base station [25](#)
  - Clearing Personalized Settings of the Handset [25](#)
  - Comfort Noise Generation [321](#)
  - Configuration Files [14](#)
  - Configuration File Parameters Description [17](#)
  - Configuration Parameters [18](#)
  - Configuring Audio Features [307](#)
  - Configuring Advanced features [247](#)
  - Configuring Basic Features [103](#)
  - Configuring Network Parameters Manually [42](#)
  - Configuring Methods [12](#)

Configuring Security Features [343](#)  
 Connected Line Identification Presentation  
[226](#)  
 Connecting the Base Station [5](#)  
 Connecting the Handset [93](#)  
 Connecting the IP DECT phones [5](#)  
 Conventions Used in Yealink Documentations  
[i](#)  
 Customizing a Directory Template File [166](#)  
 Customizing a Super Search Template File  
[167](#)

## D

Daylight Saving Time [138](#)  
 Deploying Phones from the Provisioning  
 Server [30](#)  
 DHCP [32](#)  
 DHCP Option [37](#)  
 DHCP Option 66 and Option 43 [39](#)  
 DHCP Option 42 and Option 2 [40](#)  
 DHCP Option 12 and Hostname on the IP  
 DECT phone [41](#)  
 DHCP VLAN [66](#)  
 Dial Plan [145](#)  
 Dial-now [153](#)  
 Dial-now Template File [156](#)  
 Directory List [162](#)  
 Display Issue [391](#)  
 Display Method on Dialing [122](#)  
 Do Not Disturb (DND) [186](#)  
 Documentations [i](#)  
 DTMF [325](#)

## E

Early Media [193](#)  
 Emergency Number [349](#)  
 Encrypting Configuration Files [363](#)  
 Enabling the Watch Dog Feature [370](#)  
 End Call on Hook [244](#)

## F

Feature Key Synchronization [217](#)

## G

Getting Started [v](#)

## H

Handset Name [103](#)  
 Handset Model [3](#)  
 Handset Power Indicator LED [93](#)  
 Handset User Interface [13](#)  
 Hardware Issue [399](#)

## I

Icon Instructions [11](#)  
 In This Guide [ii](#)  
 Index [461](#)  
 Initialization Process Overview [10](#)  
 Intercom [228](#)  
 Input Method [145](#)  
 IPv6 Support [49](#)

## J

Jitter Buffer [323](#)

## K

Keep Alive [296](#)  
 Keep User Personalized Settings [17](#)  
 Keyboard Input Method Customization [145](#)  
 Keypad Light [95](#)  
 Key As Send [145](#)

## L

Language [143](#)  
 Lightweight Directory Access Protocol (LDAP)  
[251](#)  
 LLDP [62](#)  
 Local Directory [164](#)  
 Loading Language Packs [105](#)

## M

Manual Configuration for VLAN [64](#)  
 Message Waiting Indicator [262](#)  
 Method of Transmitting DTMF Digit [326](#)

**N**

- NAT Types [289](#)
- NAT Traversal [290](#)
- Network Address Translation (NAT) [289](#)
- Network Conference [215](#)
- No Answer Forward [203](#)
- Number Assignment [124](#)

**O**

- Obtaining Configuration Files and Resource Files [15](#)
- Off Hook Hot Line Dialing [162](#)
- Other Issues [400](#)

**P**

- Password Issues [398](#)
- Phone Lock [348](#)
- Phone Book Issues [393](#)
- Power Indicator LED [112](#)
- PPPoE [46](#)
- Product Overview [1](#)
- Protecting Personalized Settings of the Base Station [21](#)
- Protecting Personalized Settings of the Handset [23](#)
- Provisioning Issues [394](#)
- Provisioning Server [29](#)

**Q**

- Quality of Service [71](#)

**R**

- Real-Time Transport Protocol (RTP) Ports [299](#)
- Reboot in Talking [242](#)
- Recent Call in Dialing [219](#)
- Register Issue [390](#)
- Register Power Light Flash [112](#)
- Registering the Handset [9](#)
- Remote Phone Book [247](#)
- Replace Rule [149](#)
- Replace Rule Template File [151](#)

- Report [297](#)
- Reserve # in User Name [237](#)
- Resetting Issues [394](#)
- Return Code When Refuse [192](#)
- RFC and Internet Draft Support [414](#)
- Ringling Timeout [231](#)
- RTCP-XR [331](#)

**S**

- Save Call Log [167](#)
- Setting up DECT Phone Network [31](#)
- Setting up the Provisioning Server [30](#)
- Search Source in Dialing [167](#)
- Scenario A Protect Personalized Settings [21](#)
- Scenario B Clear Personalized Settings [25](#)
- Scenario C Protecting Personalized Settings after Reset [26](#)
- Scenario D Importing or exporting the local configuration File [28](#)
- Screen Saver [102](#)
- Search Source List in Dialing [167](#)
- Secure Real-Time Transport Protocol (SRTP) [360](#)
- Send user=phone [230](#)
- Server Domain Name Resolution [277](#)
- Server Redundancy [266](#)
- Session Timer [199](#)
- Setting Up Your Phone Network [31](#)
- Setting up the Charger Cradle [7](#)
- Setting up the Handset [7](#)
- Shared Call Appearance (SCA) [251](#)
- SIP Header [418](#)
- SIP Request [417](#)
- SIP Responses [419](#)
- SIP Send Line [235](#)
- SIP Send MAC [234](#)
- SIP Session Description Protocol Usage [422](#)
- SIP Session Timer [197](#)
- Specifying the Default Input Method [145](#)
- Specifying the Language to Use [108](#)
- Static DNS [34](#)
- STUN [290](#)
- Summary of Changes [iii](#)

Supported Provisioning Protocols	29
Suppress DTMF Display	329
System Log Issue	399

## T

Table of Contents	v
Time and Date	129
Time and Date Issue	392
Time and Date Settings	135
Tones	307
Transport Layer Security (TLS)	348
Troubleshooting	369
Troubleshooting Methods	369
Troubleshooting Solutions	389
TR-069 Device Management	301

## U

Unregister When Reboot	239
Upgrade Issue	392
Upgrading Firmware	49
Upgrading Firmware from the Provisioning Server	85
Upgrading Firmware via Web User Interface	83
Use Outbound Proxy in Dialog	195
User Agent Client (UAC)	458
User Agent Server (UAS)	248
User Password	343

## V

Verifying Startup	11
Viewing Log Files	369
VLAN	61
Voice Activity Detection	319
Voice Mail Tone	311
VPN	68
VQ-RTCPXR	333

## W

Wallpaper	101
Web Server Type	120
Web User Interface	13