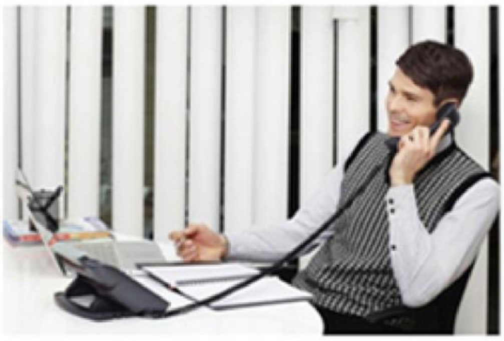
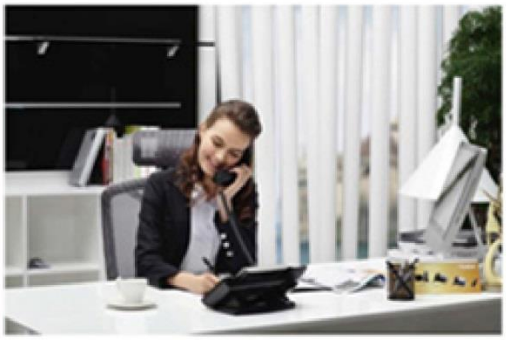
Yealink





Yealink SIP-T2xP IP Phones Administrator Guide

Version 73.40
Dec. 2014

Copyright

Warranty

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

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

Declaration of Conformity

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

CE Mark Warning

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

Part 15 FCC Rules

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

1. This device may not cause harmful interference.
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.

GNU GPL INFORMATION

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

The original GPL license, source code of components licensed under GPL and used in Yealink products can be downloaded from Yealink web site:
http://www.yealink.com/GPLOpenSource.aspx?BaseInfoCateId=293&NewsCateId=293&CateId=293.

About This Guide

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

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

Documentations

This guide covers SIP-T28P, SIP-T26P, SIP-T22P and SIP-T20P IP phones. The following related documents are available:

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

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

In This Guide

The information detailed in this guide is applicable to firmware version 73 or higher. The firmware format is like x.x.x.x.rom. The second x from left must be greater than or equal to 73 (e.g., the firmware version of SIP-T28P IP phone: 2.73.0.40.rom). This administrator guide includes the following chapters:

- Chapter 1, "Product Overview" describes the SIP components and SIP IP phones.
- Chapter 2, "Getting Started" describes how to install and connect IP phones and the configuration methods.
- Chapter 3, "Configuring Basic Features" describes how to configure the basic features on IP phones.
- Chapter 4, "Configuring Advanced Features" describes how to configure the

advanced features on IP phones.

- Chapter 5, "Configuring Audio Features" describes how to configure the audio features on IP phones.
- Chapter 6, "Configuring Security Features" describes how to configure the security features on IP phones.
- Chapter 7, "Resource Files" describes the resource files that can be downloaded by IP phones.
- Chapter 9, "Troubleshooting" describes how to troubleshoot IP phones and provides some common troubleshooting solutions.
- Chapter 10, "Appendix" provides the glossary, reference information about IP phones compliant with RFC 3261, SIP call flows and the sample configuration files.

Summary of Changes

This section describes the changes to this guide for each release and guide version. For more information on changes, refer to version-specific release notes of Yealink IP phones online:
http://www.yealink.com/DocumentDownload.aspx?CateId=142&flag=142.

Changes for Release 73, Guide Version 73.40

This version is updated to remove SIP-T21P and SIP-T19P IP phones. The following section is new for this version:

- Hide Features Access Code on page 309

Major updates have occurred to the following sections:

- Physical Features of IP Phones on page 4
- Configuration Files on page 18
- ReCall on page 236
- Distinctive Ring Tones on page 264
- BLF List on page 303
- Static DNS Cache on page 368
- Voice Quality Monitoring on page 391
- Appendix D: Configuring DSS Key on page 513
- Appendix B: Time Zones on page 509

Changes for Release 73, Guide Version 73.16

The following sections are new for this version:

- Notification Popups on page 54
- Call Display on page 62
- Input Method Customization on page 99
- Off Hook Hot Line Dialing on page 131
- Feature Key Synchronization on page 215
- BLF List on page 303
- Capturing the Current Screen of the Phone on page 355
- Voice Quality Monitoring on page 391

Major updates have occurred to the following sections:

- Configuration Files on page 18
- DHCP on page 22
- Configuring Basic Network Parameterson page 22
- Upgrading Firmware on page 41
- Backlight on page 59
- Phone Lock on page 71
- Time and Date on page 77
- Language on page 89
- Anonymous Call Rejection on page 161
- DTMF on page 246
- Distinctive Ring Tones on page 264
- Remote Phone Book on page 277
- LDAP on page 281
- Message Waiting Indicator on page 310
- Multicast Paging on page 316
- VLAN on page 380
- 802.1X Authentication on page 416
- Transport Layer Security on page 457
- Secure Real-Time Transport Protocol on page 467
- Encrypting Configuration Files on page 470
- Analyzing Configuration File on page 497

Changes for Release 72, Guide Version 72.26

The following sections are new for this version:

- Provisioning Server on page 20

- Static DNS Cache on page 368
- Background Noise Suppression on page 451
- Automatic Gain Control on page 451

Major updates have occurred to the following section:

- Configuration Files on page 18
- Audio Codecs on page 442
- Acoustic Clarity Technology on page 450

Changes for Release 72, Guide Version 72.25

The following sections are new for this version:

- Directory on page 133
- Search Source in Dialing on page 135

Major updates have occurred to the following section:

- Transport Layer Security on page 457

Changes for Release 72, Guide Version 72.1

The following section is new for this version:

- Power Indicator LED on page 50

Major updates have occurred to the following sections:

- DHCP on page 22
- Replace Rule on page 117
- Dial-now on page 120
- Contrast on page 57
- Backlight on page 59
- Time and Date on page 77
- Key as Send on page 113
- Anonymous Call on page 157
- LDAP on page 281
- Busy Lamp Field on page 293
- Action URL on page 335
- IPv6 Support on page 430
- Transport Layer Security on page 457
- Upgrading Firmware on page 41

- Resource Files on page 477

Changes for Release 71, Guide Version 71.165

Documentations of the newly released SIP-T19P and SIP-T21P IP phones have also been added.

Changes for Release 71, Guide Version 71.141

Major updates have occurred to the following sections:

- Action URL on page 335
- Action URI on page 351

Changes for Release 71, Guide Version 71.140

Major updates have occurred to the following sections:

- Logo Customization on page 103
- Anonymous Call on page 157
- Distinctive Ring Tones on page 264
- Server Redundancy on page 356
- Transport Layer Security on page 457
- Secure Real-Time Transport Protocol on page 467
- Encrypting Configuration Files on page 470
- Local Contact File on page 484
- Viewing Log Files on page 489
- Capturing Packets on page 494

Changes for Release 71, Guide Version 71.125

Major updates have occurred to the following section:

- Appendix B: Time Zones on page 509

Changes for Release 71, Guide Version 71.120

Major updates have occurred to the following section:

- Appendix D: Configuring DSS Key on page 513

Changes for Release 71, Guide Version 71.110

The following sections are new for this version:

- Hot Desking on page 332
- TR-069 Device Management on page 424
- IPv6 Support on page 430

Major updates have occurred to the following sections:

- Configuring Network Parameters Manually on page 28
- Softkey Layout on page 107
- Directed Call Pickup on page 219
- Distinctive Ring Tones on page 264
- Action URL on page 351
- Server Redundancy on page 355
- VLAN on page 380
- Transport Layer Security on page 457
- Local Contact File on page 484

Changes for Release 70, Guide Version 70

The following sections are new for this version:

- Configuring Network Parameters Manually on page 28
- Contrast on page 57
- Backlight on page 59
- Logo Customization on page 103
- Softkey Layout on page 107
- Key as Send on page 113
- Call Log on page 137
- Live Dialpad on page 145
- Auto Answer on page 152
- Call Completion on page 155
- Anonymous Call on page 157
- Anonymous Call Rejection on page 161
- Busy Tone Delay on page 175
- Return Code When Refuse on page 176
- Early Media on page 178

Major updates have occurred to the following sections:

Changes for Release 70, Guide Version 2.0

The following sections are new for this version:

Major updates have occurred to the following sections:

- Dial Plan on page 116
- Phone Lock on page 71
- Time and Date on page 77
- Busy Lamp Field on page 293

Table of Contents

Product Overview

This chapter contains the following information about IP phones:

- VoIP Principle
- SIP Components
- SIP IP Phone Models

VoIP Principle

VoIP

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

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

H.323

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

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

SIP

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

SIP provides capabilities to:

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

SIP Components

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

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

User Agent Client (UAC)

The UAC is an application that initiates up to six feasible SIP requests to the UAS. The six requests issued by the UAC are: INVITE, ACK, OPTIONS, BYE, CANCEL and REGISTER. When the SIP session is being initiated by the UAC SIP component, the UAC determines the information essential for the request, which is the protocol, the port and the IP address of the UAS to which the request is being sent. This information can be dynamic and will make it challenging to put through a firewall. For this reason, it may be recommended to open the specific application type on the firewall. The UAC is also capable of using the information in the request URI to establish the course of the SIP request to its destination, as the request URI always specifies the host which is essential. The port and protocol are not always specified by the request URI. Thus if the request does not specify a port or protocol, a default port or protocol is contacted. It may be preferential to use this method when not using an application layer firewall. Application layer firewalls like to know what applications are flowing though which ports and it is possible to use content types of other applications other than the one you are trying to let through what has been denied.

User agent server (UAS)

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

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

SIP IP Phone Models

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

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

The following IP phone models are described:

- SIP-T28P
- SIP-T26P
- SIP-T22P
- SIP-T20P

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

For a list of key features available on Yealink IP phones running the latest firmware, refer to Key Features of IP Phones on page 8.

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

- A working IP network is established.
- VoIP gateways are configured for SIP.
- The latest (or compatible) firmware of IP phones is available.
- A call server is active and configured to receive and send SIP messages.

Physical Features of IP Phones

This section lists the available physical features of IP phones.

SIP-T28P

Physical Features:

- TI TITAN chipset and TI voice engine
- 320x160 graphic LCD with 4-level grayscales
- 6 VoIP accounts, Broadsoft Validated/Asterisk® Compatible
- HD Voice: HD Codec, HD Handset, HD Speaker
- 47 keys including 16 DSS keys
- 1*RJ9 (4P4C) handset port
- 1*RJ9 (4P4C) headset port
- 2*RJ45 10/100Mbps Ethernet ports
- 1*RJ12 (6P6C) expansion module port
- 19 LEDs: 1*power, 6*line, 1*message, 1*headset, 10*memory
- Power adapter: AC 100~240V input and DC 5V/1.2A output
- Power over Ethernet (IEEE 802.3af)

SIP-T26P

Physical Features:

- TI TITAN chipset and TI voice engine
- 132x64 graphic LCD
- 3 VoIP accounts, Broadsoft Validated/Asterisk® Compatible
- HD Voice: HD Codec, HD Handset, HD Speaker
- 44 keys including 13 DSS keys
- 1*RJ9 (4P4C) handset port
- 1*RJ9 (4P4C) headset port
- 2*RJ45 10/100Mbps Ethernet ports
- 1*RJ12 (6P6C) expansion module port
- 16 LEDs: 1*power, 3*line, 1*message, 1*headset, 10*memory
- Power adapter: AC 100~240V input and DC 5V/1.2A output
- Power over Ethernet (IEEE 802.3af)

SIP-T22P

Physical Features:

- TI TITAN chipset and TI voice engine
- 132x64 graphic LCD
- 3 VoIP accounts, Broadsoft Validated/Asterisk® Compatible
- HD Voice: HD Codec, HD Handset, HD Speaker
- 31 keys including 3 line keys
- 1*RJ9 (4P4C) handset port
- 1*RJ9 (4P4C) headset port
- 2*RJ45 10/100Mbps Ethernet ports
- 5 LEDs: 1*power, 3*line, 1*message
- Power adapter: AC 100~240V input and DC 5V/1.2A output
- Power over Ethernet (IEEE 802.3af)
- Wall Mount

SIP-T20P

Physical Features:

- TI TITAN chipset and TI voice engine
- 3-line LCD consists of an icon line and two 15-character lines
- 2 VoIP accounts, Broadsoft Validated/Asterisk® Compatible
- HD Voice: HD Codec, HD Handset, HD Speaker
- 30 keys including 2 line keys
- 1*RJ9 (4P4C) handset port
- 1*RJ9 (4P4C) headset port
- 2*RJ45 10/100Mbps Ethernet ports
- 4 LEDs: 1*power, 2*line, 1*message
- Power adapter: AC 100~240V input and DC 5V/1.2A output
- Power over Ethernet (IEEE 802.3af)
- Wall Mount

Key Features of IP Phones

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

- Phone Features
  - **Call Options**: emergency call, call waiting, call hold, call mute, call forward, call transfer, call pickup, conference.
  - **Basic Features:** DND, phone lock, auto redial, live dialpad, dial plan, hotline, caller identity, auto answer.
  - **Advanced Features:** BLF, server redundancy, distinctive ring tones, remote phone book (not applicable to SIP-T20P IP phones), LDAP, 802.1X authentication.
- Codecs and Voice Features
  - Wideband codec: G.722
  - Narrowband codec: G.711 (A/μ), G.723, G.726, G.729, iLBC.
  - VAD, CNG, AEC, PLC, AJB, AGC
  - Full-duplex speakerphone with AEC
- Network Features
  - SIP v1 (RFC2543), v2 (RFC3261)
  - NAT Traversal: STUN mode
  - DTMF: INBAND, RFC2833, SIP INFO
  - Proxy mode and peer-to-peer SIP link mode
  - IP assignment: Static/DHCP/PPPoE
  - VLAN assignment: LLDP/Static/DHCP
  - Bridge mode for PC port
  - TFTP/DHCP/PPPoE client
  - HTTP/HTTPS server
  - DNS client
  - NAT/DHCP server
  - IPv6 support
- Management
  - FTP/TFTP/HTTP/PnP auto-provision
  - Configuration: browser/phone/auto-provision
  - Direct IP call without SIP proxy
  - Dial number via SIP server
  - Dial URL via SIP server
  - TR-069

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

Getting Started

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

This chapter provides the following sections:

- Connecting the IP Phones
- Initialization Process Overview
- Verifying Startup
- Reading Icons
- Configuration Methods
- Provisioning Server
- Configuring Basic Network Parameters
- Upgrading Firmware

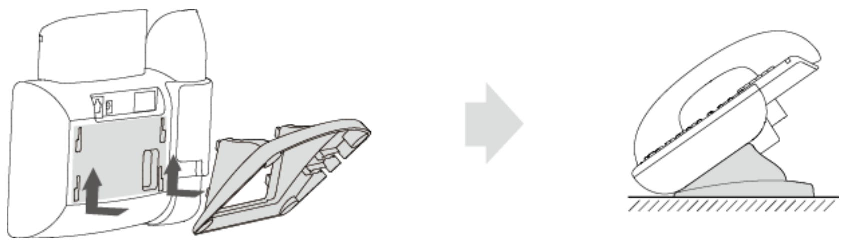
Connecting the IP Phones

This section introduces how to install IP phones with components in packaging contents.

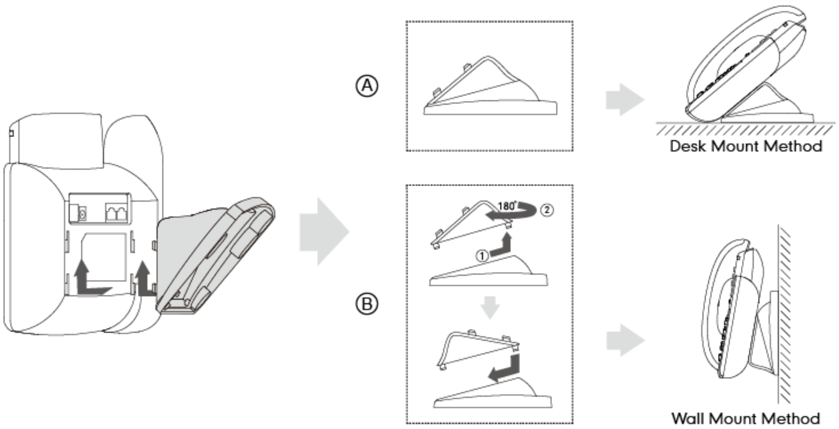
1. Attach the stand and optional wall mount bracket
2. Connect the handset and optional headset
3. Connect the network and power

Note A headset is not included in packaging contents.

1) **Attach the stand:**

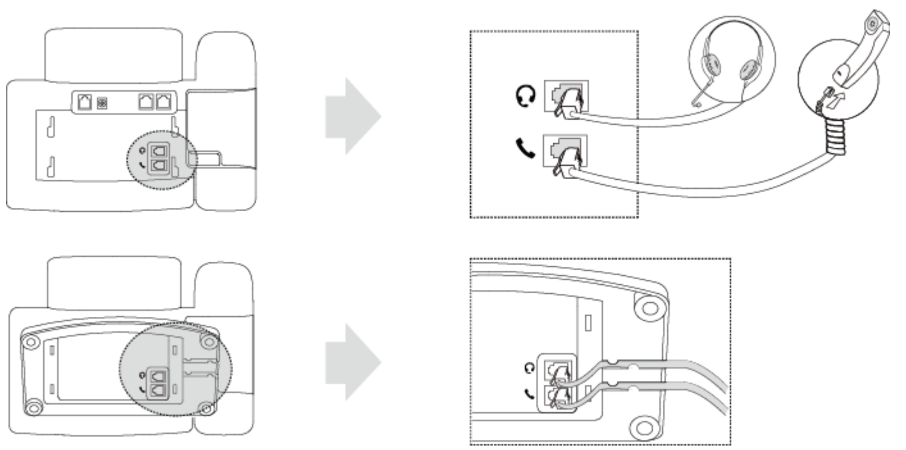


SIP-T28P/T26P

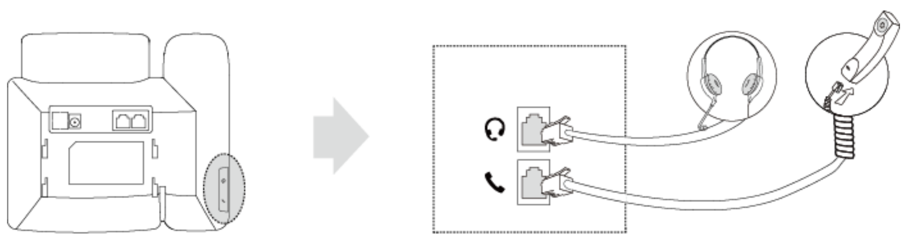


SIP-T22P/T20P

2) **Connect the handset and optional headset:**



SIP-T28P/T26P



SIP-T22P/T20P

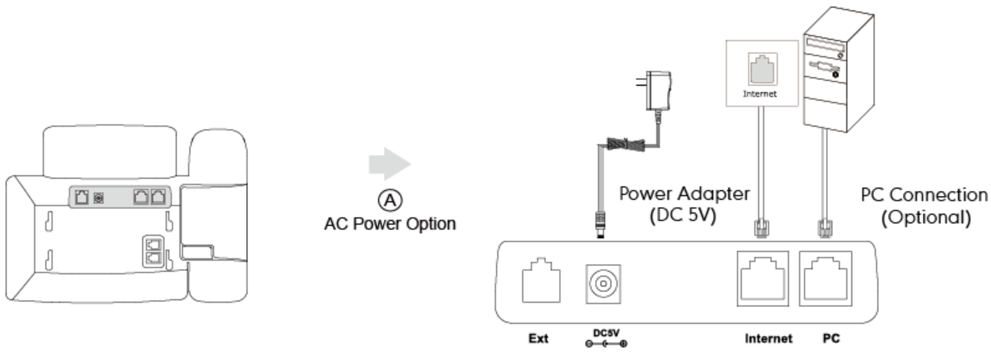
3) **Connect the network and power:**

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

AC Power (Optional)

To connect the AC power and network:

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

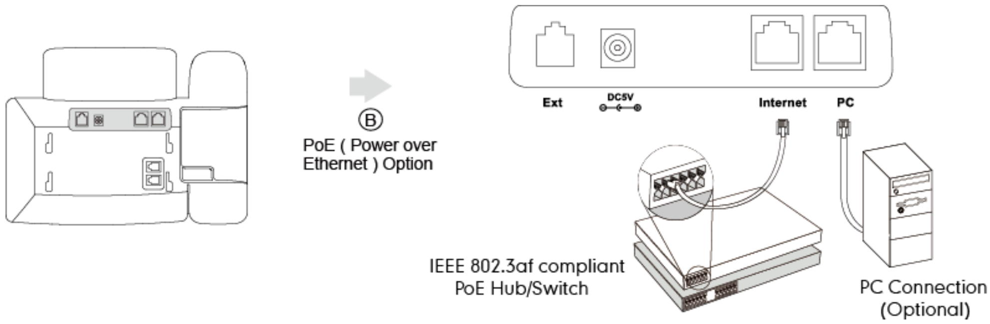


Power over Ethernet

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

To connect the PoE:

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



Note	If in-line power switch/hub is provided, you don't need to connect the phone to the power adapter. Make sure the switch/hub is PoE-compliant. The IP phone can also share the network with another network device such as a PC (personal computer). It is an optional connection. **Important!** Do not unplug or remove the power while the IP phone is updating firmware and configurations.

Initialization Process Overview

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

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

During the initialization process, the following events take place:

Loading the ROM file

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

Configuring the VLAN

If the IP phone is connected to a switch, the switch notifies the IP phone of the VLAN information defined on the switch (if using LLDP). The IP 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 phone is capable of querying a DHCP server. DHCP is enabled on the IP 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 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 28.

Contacting the provisioning server

If the IP 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 phone will be able to resolve and update configurations written in the configuration file(s). If the IP phone does not obtain configurations from the provisioning server, the IP 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 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 phone will perform a firmware update.

Downloading the resource files

In addition to configuration file(s), the IP 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
- Ring tones
- Contact files

Verifying Startup

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

1. The power indicator LED illuminates green.

2. The message "Initializing… Please Wait" appears on the LCD screen when the IP phone starts up.
3. The main LCD screen displays the following:
   - Time and date
   - Soft key labels (not applicable to SIP-T20P IP phones)
4. Press the OK key to check the IP phone status, the LCD screen displays the valid IP address, MAC address, firmware version, etc.

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

Reading Icons

Icons associated with different features may appear on the LCD screen. The following table provides a description for each icon on IP phones.

SIP-T28P	SIP-T26P	SIP-T22P	SIP-T20P	Description
				Network is unavailable
			/	Registered successfully
			/	Registration failed
			/	Registering
				Hands-free speakerphone mode
				Handset mode
				Headset mode
				Voice Mail
			/	Text Message
AA	AA	AA	AA	Auto Answer
DND	DND	DND	DND	Do Not Disturb

SIP-T28P	SIP-T26P	SIP-T22P	SIP-T20P	Description
				Call Forward/Forwarded Calls
			/	Call Hold
				Call Mute
			/	Ringer volume is 0
				Phone Lock
				Received Calls
				Placed Calls
				Missed Calls
			/	Recording box is full
			/	A call cannot be recorded
			/	Recording starts successfully
			/	Recording cannot be started
			/	Recording cannot be stopped

Configuration Methods

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

The recommended method for configuring IP 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 phones using each method.

- Phone User Interface
- Web User Interface
- Configuration Files

Phone User Interface

An administrator or a user can configure and use IP phones via phone user interface. Access to specific features is restricted to the administrator. The default password is "admin"(case-sensitive). Not all features are available on phone user interface. For more information, refer to Yealink phone-specific user guide, available online: http://www.yealink.com/DocumentDownload.aspx?CateId=142&flag=142.

Web User Interface

An administrator or a user can configure IP phones via web user interface. The default user name and password for the administrator to log into the web user interface are both "admin" (case-sensitive). Most features are available for configuring via web user interface. IP phones support both HTTP and HTTPS protocols for accessing the web user interface. For more information, refer to Web Server Type on page 64.

Configuration Files

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

- Common CFG file
- MAC-Oriented CFG file
- MAC-local CFG file (Only for IP phones running firmware version 73 or later)

Common CFG file

A Common CFG file contains parameters that affect the basic operation of the IP phone, such as language and volume. It will be effectual for all IP phones of the same model.

The common CFG file has a fixed name for each IP phone model. The name of the Common CFG file for each IP phone model is:

- SIP-T28P: y000000000000.cfg
- SIP-T26P: y000000000004.cfg
- SIP-T22P: y000000000005.cfg
- SIP-T20P: y000000000007.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 phone. The MAC-Oriented CFG file is named after the MAC address of the IP phone. For example, if the MAC address of an IP phone is 001565113af8, the name of the MAC-Oriented CFG file must be 001565113af8.cfg.

MAC-local CFG file

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

The MAC-local CFG file enables the phone to protect personalized settings. For more information on how to protect personalized settings, refer to the section *Specific Scenarios-Protect Personalized Settings* in *Yealink_SIP-T2_Series_T4_Series_IP_Phones_Auto_Provisioning_Guide*, available online: http://www.yealink.com/DocumentDownload.aspx?CateId=142&flag=142.

Central Provisioning

IP phones can be centrally provisioned from a provisioning server using the configuration files (<y0000000000xx>.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 20.

IP phones can obtain the provisioning server address during startup. Then IP 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_T4_Series_IP_Phones_Auto_Provisioning_Guide*, available online: http://www.yealink.com/DocumentDownload.aspx?CateId=142&flag=142.

When modifying parameters, learn the following:

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

following rules:

```
variable-name = value
```

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

Provisioning Server

Supported Provisioning Protocols

IP 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. IP 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. IP 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_T4_Series_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 phones using configuration files, refer to Deploying Phones from the Provisioning Server on page 21.

Note

Typically all 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-account 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, IP 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.

Yealink supplies configuration files for each phone model, which is delivered with the phone firmware. The configuration files, supplied with each firmware release, must be used with that release. Otherwise, configurations may not take effect, and the IP phone will behave without exception. 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 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 bar code label on the back of the IP phone 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 <y0000000000xx>.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 phones to trigger the auto provisioning process.

IP 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 18. For more information on encrypting configuration files, refer to Encrypting Configuration Files on page 470.

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

- **Zero Touch:** Zero Touch feature guides you to configure network settings and the provisioning server address via phone user interface after startup.
- **PnP**: PnP feature allows IP 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 IP phones. When the IP 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 phone user interface or web user interface.

For more information on the above methods, refer to *Yealink_SIP-T2_Series_T4_Series_IP_Phones_Auto_Provisioning_Guide*, available online: http://www.yealink.com/DocumentDownload.aspx?CateId=142&flag=142.

Configuring Basic Network Parameters

In order to get your IP phones running, you must perform basic network setup, such as IP address and subnet mask configuration. This section describes how to configure basic network parameters for IP phones.

Note

This section mainly introduces IPv4 network parameters. IP phones also support IPv6. For more information on IPv6, refer to IPv6 Support on page 430.

DHCP

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

DHCP Option

DHCP provides a framework for passing information to TCP/IP network devices. Network and other control information are carried in tagged data items that are stored in the options field of the DHCP message. The data items themselves are also called options.

DHCP can be initiated by simply connecting the IP phone with the network. IP phones broadcast DISCOVER messages to request the network information carried in DHCP options, and the DHCP server responds with specific values in corresponding options.

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

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

Parameter	DHCP Option	Description
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.

Procedure

DHCP can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure DHCP on the IP phone. **Parameter:** network.internet_port.type Configure static DNS address when DHCP is used. **Parameters:** network.primary_dns network.secondary_dns
	<y0000000000xx>.cfg	Configure the IP phone to use manually configured static IPv4 DNS. **Parameters:** network.static_dns_enable
Local	Web User Interface	Configure DHCP on the IP phone. Configure static DNS address when DHCP is used. **Navigate to:** http://<phoneIPAddress>/servlet?p=network&q=load
	Phone User Interface	Configure DHCP on the IP phone.

Details of Configuration Parameters:

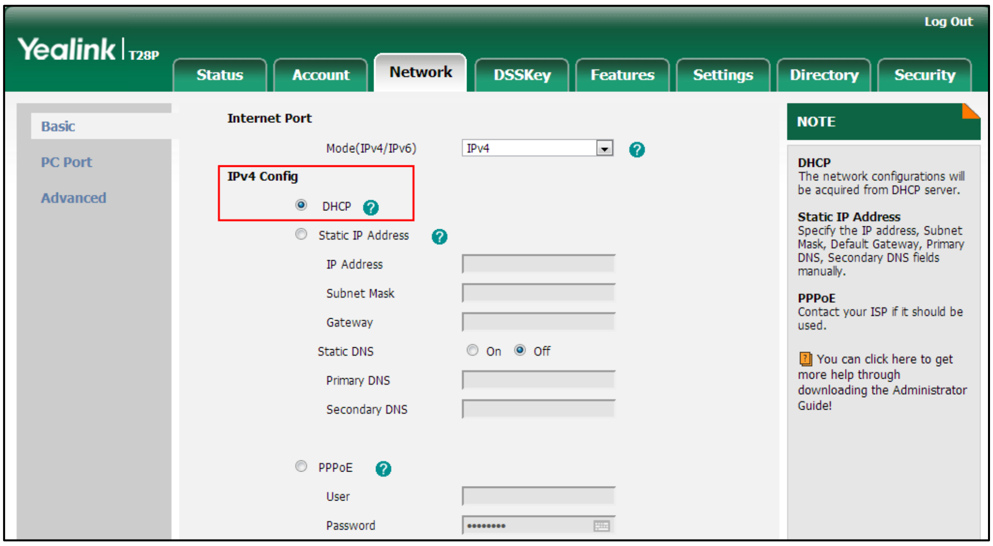
Parameters	Permitted Values	Default
network.internet_port.type	0, 1 or 2	0
Description: Configures the Internet (WAN) port type for IPv4 when the IP address mode is configured as IPv4 or IPv4&IPv6. **0**-DHCP **1**-PPPoE **2**-Static IP Address **Note**: If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv4 Config **Phone User Interface:** Menu->Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv4		
network.static_dns_enable	0 or1	0
Description: Enables or disables the IP phone to use manually configured static IPv4 DNS when the Internet (WAN) port type for IPv4 is configured as DHCP. **0**-Disabled **1**-Enabled **Note**: If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv4 Config->Static DNS **Phone User Interface:** Menu->Settings->Advanced Settings (default password: admin)->Network->WAN Port->IPv4->DHCP IPv4 Client->Static DNS		
network.primary_dns	IPv4 Address	Blank
Description: Configures the primary IPv4 DNS server when the static IPv4 DNS is enabled.		

Parameters	Permitted Values	Default
Example: network.primary_dns = 202.101.103.55 **Note**: If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv4 Config->Static IP Address->Primary DNS **Phone User Interface:** Menu->Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv4->DHCP IPv4 Client->Static DNS (Enabled) ->IPv4 Pri.DNS		
network.secondary_dns	**IPv4 Address**	**Blank**
Description: Configures the secondary IPv4 DNS server when the static IPv4 DNS is enabled. **Example:** network.secondary_dns = 202.101.103.54 **Note**: If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv4 Config->Static IP Address->Secondary DNS **Phone User Interface:** Menu->Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv4->DHCP IPv4 Client->Static DNS (Enabled) ->IPv4 Sec.DNS		

To configure DHCP via web user interface:

1. Click on **Network**->**Basic**.

2. In the **IPv4 Config** block, mark the **DHCP** radio box.



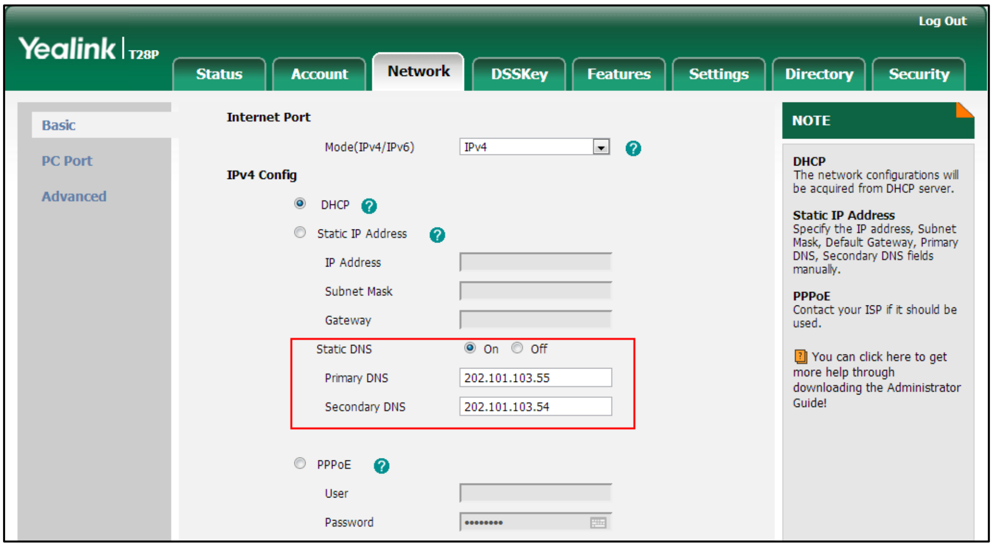
3. Click **Confirm** to accept the change.

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

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

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

1. Click on **Network**->**Basic**.
2. In the **IPv4 Config** block, mark the **DHCP** radio box.
3. Mark the **Static DNS** radio box.
4. Enter the desired values in the **Primary DNS** and **Secondary DNS** fields.



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

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

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

To configure DHCP via phone user interface:

1. Press **Menu**->**Settings**->**Advanced Settings** (default password: admin) ->**Network**->**WAN Port**->**IPv4**.
2. Press ▲ or ▼ to highlight the **DHCP IPv4 Client** field.

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

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

1. Press **Menu**-> **Settings**->**Advanced Settings** (default password: admin) ->**Network**->**WAN Port**->**IPv4**->**DHCP IP Client**.
2. Press ◄ or ► , or the **Switch** soft key to select **Enabled** from the **Static DNS** field.
3. Enter the desired values in the **IPv4 Pri.DNS** and **IPv4 Sec.DNS** fields respectively.
4. Press the **Save** soft key to accept the change.

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

Configuring Network Parameters Manually

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

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

Procedure

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

Configuration File	<y0000000000xx>.cfg	Configure network parameters of the IP phone manually. **Parameters:** network.internet_port.type network.ip_address_mode network.internet_port.ip network.internet_port.mask network.internet_port.gateway network.primary_dns network.secondary_dns

Local	Web User Interface	Configure network parameters of the IP phone manually. **Navigate to**: http://<phoneIPAddress>/servlet?p=network&q=load
	Phone User Interface	Configure network parameters of the IP phone manually.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
network.internet_port.type	**0, 1 or 2**	**0**
Description: Configures the Internet (WAN) port type for IPv4 when the IP address mode is configured as IPv4 or IPv4&IPv6. **0**-DHCP **1**-PPPoE **2**-Static IP Address **Note**: If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv4 Config **Phone User Interface:** Menu->Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv4		
network.ip_address_mode	**0, 1 or 2**	**0**
Description: Configures the IP address mode. **0**-IPv4 **1**-IPv6 **2**-IPv4&IPv6 **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->Internet Port->Mode (IPv4/IPv6) **Phone User Interface:** Menu->Settings->Advanced Settings (default password: admin) ->Network->WAN		

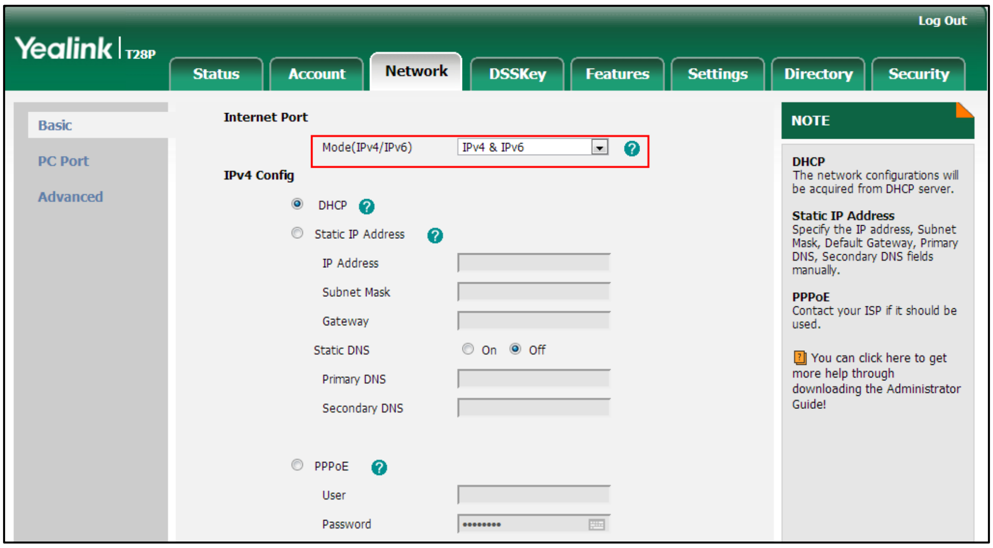
Parameters	Permitted Values	Default
Port->IP Mode		
network.internet_port.ip	**IPv4 Address**	**Blank**
Description: Configures the IPv4 address when the IP address mode is configured as IPv4 or IPv4&IPv6, and the Internet (WAN) port type for IPv4 is configured as Static IP Address. **Example:** network.internet_port.ip = 192.168.1.20 **Note**: If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv4 Config->Static IP Address->IP Address **Phone User Interface:** Menu->Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv4->Static IP Client->IP Address		
network.internet_port.mask	**Subnet Mask**	**Blank**
Description: Configures the IPv4 subnet mask when the IP address mode is configured as IPv4 or IPv4&IPv6, and the Internet (WAN) port type for IPv4 is configured as Static IP Address. **Example:** network.internet_port.mask = 255.255.255.0 **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv4 Config->Static IP Address->Subnet Mask **Phone User Interface:** Menu->Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv4->Static IP Client->Subnet Mask		
network.internet_port.gateway	**IPv4 Address**	**Blank**

Parameters	Permitted Values	Default
Description: Configures the IPv4 default gateway when the IP address mode is configured as IPv4 or IPv4&IPv6, and the Internet (WAN) port type for IPv4 is configured as Static IP Address. **Example:** network.internet_port.gateway = 192.168.1.254 **Note**: If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv4 Config->Static IP Address->Gateway **Phone User Interface:** Menu->Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv4->Static IP Client->Default Gateway		
network.primary_dns	**IPv4 Address**	**Blank**
Description: Configures the primary IPv4 DNS server when the IP address mode is configured as IPv4 or IPv4&IPv6, and the Internet (WAN) port type for IPv4 is configured as Static IP Address. **Example:** network.primary_dns = 202.101.103.55 **Note**: If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv4 Config->Static IP Address->Primary DNS **Phone User Interface:** Menu->Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv4->Static IP Client->IPv4 Pri.DNS		
network.secondary_dns	**IPv4 Address**	**Blank**

Parameters	Permitted Values	Default
Description: Configures the secondary IPv4 DNS server when the IP address mode is configured as IPv4 or IPv4&IPv6, and the Internet (WAN) port type for IPv4 is configured as Static IP Address. **Example:** network.secondary_dns = 202.101.103.54 **Note**: If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv4 Config->Static IP Address->Secondary DNS **Phone User Interface:** Menu->Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv4->Static IP Client->IPv4 Sec.DNS		

To configure the IP address mode via web user interface:

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



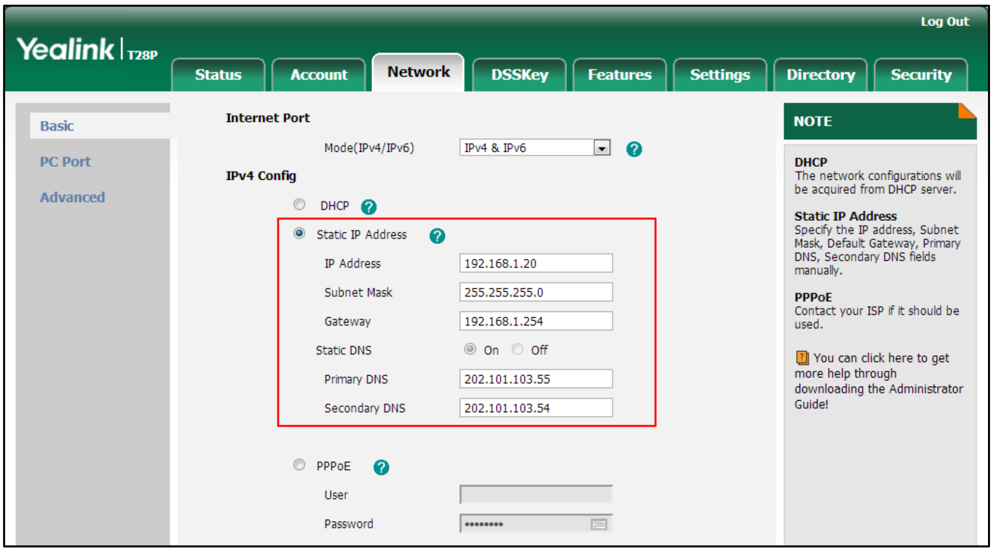
3. Click **Confirm** to accept the change.

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

To configure a static IPv4 address via web user interface:

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

3. Enter the desired values in the **IP Address**, **Subnet Mask**, **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 the IP address mode via phone user interface:

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

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

To configure a static IPv4 address via phone user interface:

1. Press **Menu**->**Settings**->**Advanced Settings** (default password: admin) ->**Network**->**WAN Port**->**IPv4**->**Static IP Client**.
2. Enter the desired values in the **IP Address**, **Subnet Mask**, **Default Gateway**, **IPv4 Pri.DNS** and **IPv4 Sec.DNS** fields respectively.
3. Press the **Save** soft key to accept the change.

   The IP phone 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 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 phone. **Parameters:** network.internet_port.type
	<y0000000000xx>.cfg	Configure the user name and password for PPPoE on the IP phone. **Parameters:** network.pppoe.user network.pppoe.password
Local	Web User Interface	Configure PPPoE on the IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?p=network&q=load
	Phone User Interface	Configure PPPoE on the IP phone.

Details of Configuration Parameters:

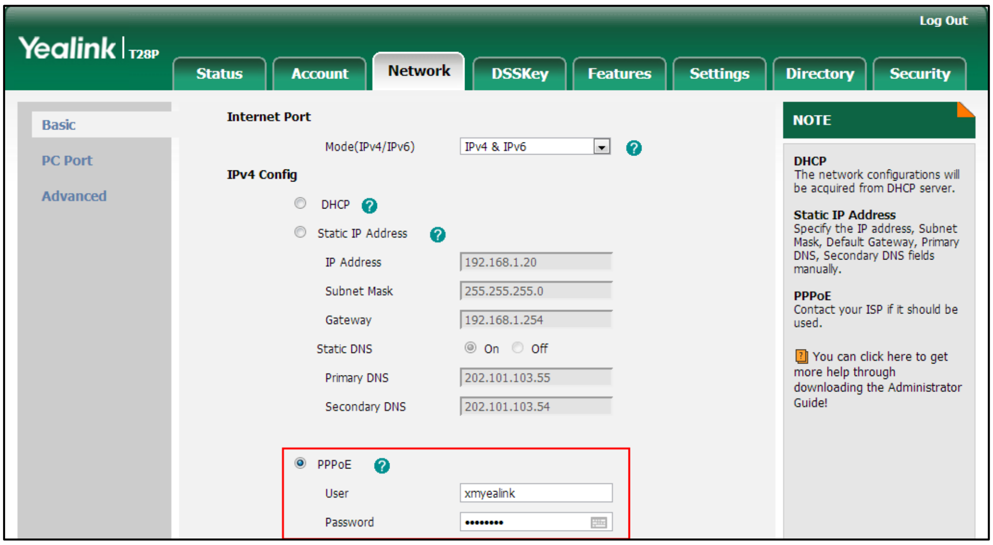
Parameters	Permitted Values	Default
network.internet_port.type	**0, 1 or 2**	**0**
Description: Configures the Internet (WAN) port type for IPv4 when the IP address mode is configured as IPv4 or IPv4&IPv6. **0**-DHCP **1**-PPPoE **2**-Static IP Address **Note**: If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv4 Config **Phone User Interface:** Menu->Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv4		

Parameters	Permitted Values	Default
network.pppoe.user	**String within 32 characters**	**Blank**
Description: Configures the user name for PPPoE connection when the IP address mode is configured as IPv4 or IPv4&IPv6, and the Internet port type is configured as PPPoE. **Example:** network.pppoe.user = xmyealink **Note**: If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv4 Config->PPPoE->User **Phone User Interface:** Menu->Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv4->PPPoE IP Client->PPPoE User		
network.pppoe.password	**String within 99 characters**	**Blank**
Description: Configures the password for PPPoE connection when the IP address mode is configured as IPv4 or IPv4&IPv6, and the Internet port type is configured as PPPoE. **Example:** network.pppoe.password = yealink123 **Note**: If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv4 Config->PPPoE->Password **Phone User Interface:** Menu->Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv4->PPPoE IP Client->PPPoE PWD		

To configure PPPoE via web user interface:

1. Click on **Network**->**Basic**.
2. In the **IPv4 Config** 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 phone user interface:

1. Press **Menu**->**Settings**->**Advanced Settings** (default password: admin) ->**Network**->**WAN Port**->**IPv4**->**PPPoE IP Client**.
2. Enter the user name and password in corresponding fields.
3. Press the **Save** soft key to accept the change.

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

Configuring Transmission Methods of the Internet Port and PC Port

Two Ethernet ports on the back of the IP phone: Internet port and PC port. Three optional methods of transmission configuration for IP phone Internet or PC Ethernet ports:

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

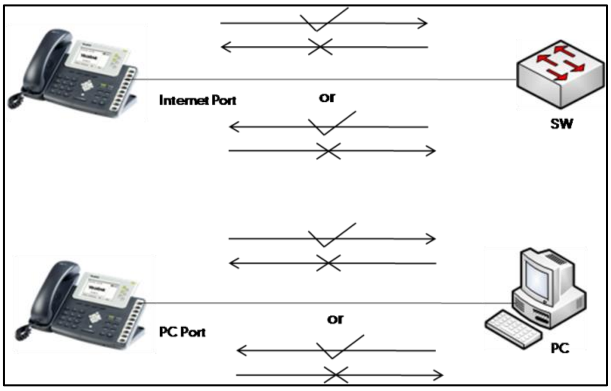
Auto-negotiation is configured for both Internet and PC ports on the IP phone by default.

Auto-negotiation

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

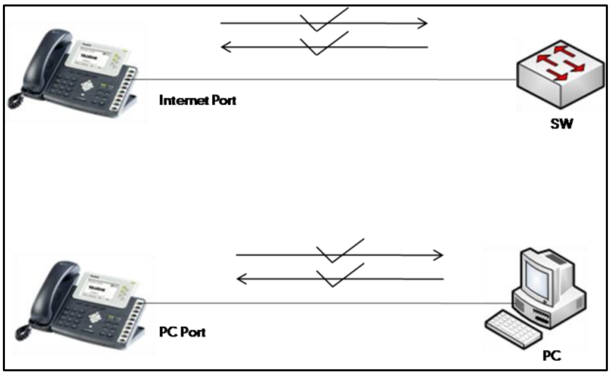
Half-duplex

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



Full-duplex

Full-duplex transmission refers to transmitting voice or data in both directions at the same time; this means one device can send data on the line while receiving data. You can configure the full-duplex transmission on both Internet port and PC port for the IP phone to transmit in 10Mbps or 100Mbps.



Procedure

The transmission methods of Ethernet ports can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure the transmission methods of Ethernet ports. **Parameters:** network.internet_port.speed_duplex network.pc_port.speed_duplex

Local	Web User Interface	Configure the transmission methods of Ethernet ports. **Navigate to**: http://<phoneIPAddress>/servlet?p=network-adv&q=load

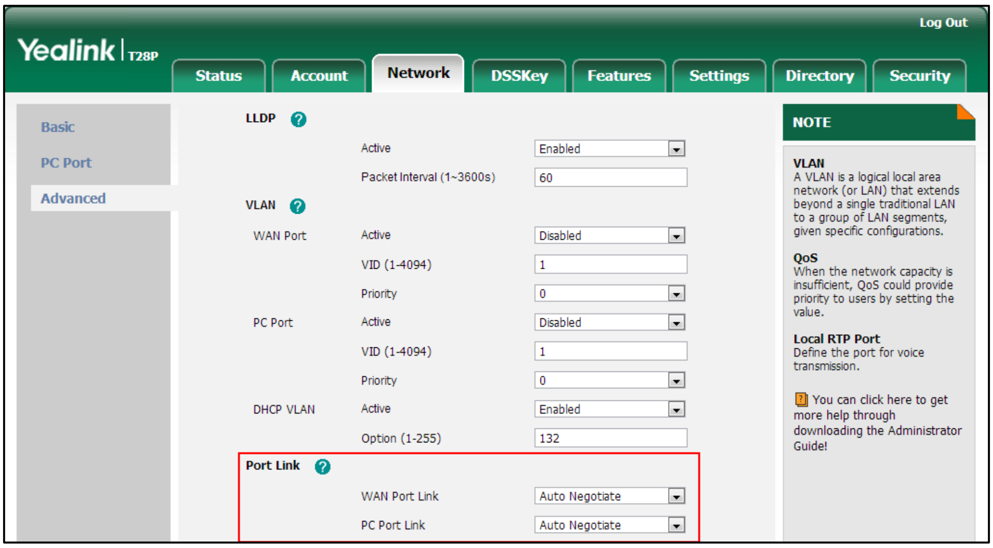
Details of Configuration Parameters:

Parameters	Permitted Values	Default
network.internet_port.speed_duplex	**0, 1, 2, 3 or 4**	**0**
Description: Configures the transmission method and speed of the Internet (WAN) port. **0**-Auto negotiate **1**-Full duplex, 10Mbps **2**-Full duplex, 100Mbps **3**-Half duplex, 10Mbps **4**-Half duplex, 100Mbps **Note**: We recommend that you do not change this parameter. If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->Port Link->WAN Port Link **Phone User Interface:** None		
network.pc_port.speed_duplex	**0, 1, 2, 3 or 4**	**0**
Description: Configures the transmission method and speed of the PC (LAN) port. **0**-Auto negotiate **1**-Full duplex, 10Mbps **2**-Full duplex, 100Mbps **3**-Half duplex, 10Mbps **4**-Half duplex, 100Mbps **Note**: We recommend that you do not change this parameter. If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->Port Link->PC Port Link		

Parameters	Permitted Values	Default
Phone User Interface: None		

To configure the transmission methods of Ethernet ports via web user interface:

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



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

Configuring PC Port Mode

The PC port on the back of the IP phone is used to connect a PC. You can enable or disable the PC (LAN) port on SIP-T2X IP phones via web user interface or using configuration files.

Procedure

PC port mode can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure the PC port. **Parameter:** network.PC_port.enable
Local	Web User Interface	Configure the PC port mode. **Navigate to**: http://<phoneIPAddress>/servlet

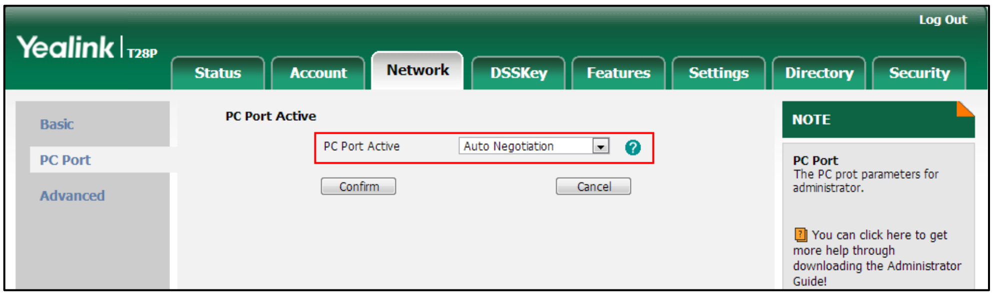
		?p=network-pcport&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
network.PC_port.enable	0 or 1	1
Description: Enables or disables the PC (LAN) port. **0**-Disabled **1**-Auto Negotiation **Note**: If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->PC Port ->PC Port Active **Phone User Interface:** None		

To enable the PC port via web user interface:

1. Click on **Network**->**PC Port**.
2. Select **Auto Negotiation** from the pull-down list of **PC Port Active**.



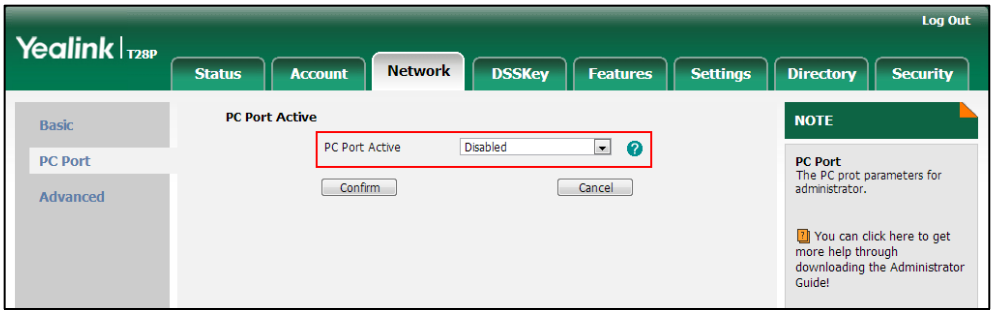
3. Click **Confirm** to accept the change.

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

To disable the PC port via web user interface:

1. Click on **Network**->**PC Port**.

2. Select **Disabled** from the pull-down list of **PC Port Active**.



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 phone firmware. Two methods of firmware upgrade:

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

The following table lists the associated and latest firmware name for each IP phone model (X is replaced by the actual firmware version).

IP Phone Model	Associated Firmware Name	Firmware Name Example
SIP-T28P	2.x.x.x.rom	2.73.0.40.rom
SIP-T26P	6.x.x.x.rom	6.73.0.40.rom
SIP-T22P	7.x.x.x.rom	7.73.0.40.rom
SIP-T20P	9.x.x.x.rom	9.73.0.40.rom

Note

You can download the latest firmware online: http://www.yealink.com/DocumentDownload.aspx?CateId=142&flag=142.

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

Upgrade 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 firmware manually via web user interface:

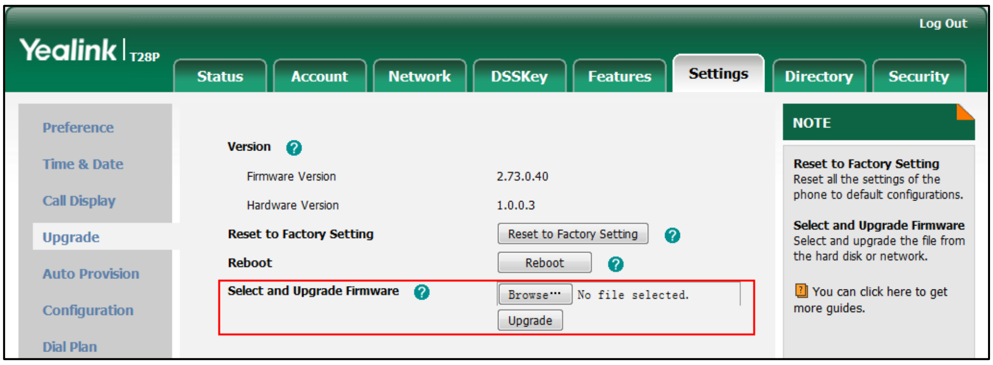
1. Click on **Settings**->**Upgrade**.

2. Click **Browse**.

3. Select firmware from the local system.

4. Click **Upgrade**.

   A dialog box pops up to prompt "Firmware of the SIP Phone will be updated. It will take 5 minutes to complete. Please don't power off!".



5. Click **OK** to confirm the upgrade.

Note

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

Upgrade Firmware from the Provisioning Server

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

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

- Check for 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.

Configuration File	<y0000000000xx>.cfg	Configure the way for the IP phone to check for configuration files. **Parameters:** 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. **Parameter:** firmware.url
Local	Web User Interface	Configure the way for the IP phone to check for configuration files. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-autop&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
auto_provision.power_on	**0 or 1**	**1**
Description: Enables or disables the IP phone to perform an auto provisioning process when powered on. **0**-Disabled **1**-Enabled **Web User Interface:** Settings->Auto Provision->Power On **Phone User Interface:** None		
auto_provision.repeat.enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to perform an auto provisioning process repeatedly. **0**-Disabled **1**-Enabled **Web User Interface:** Settings->Auto provision->Repeatedly **Phone User Interface:**		

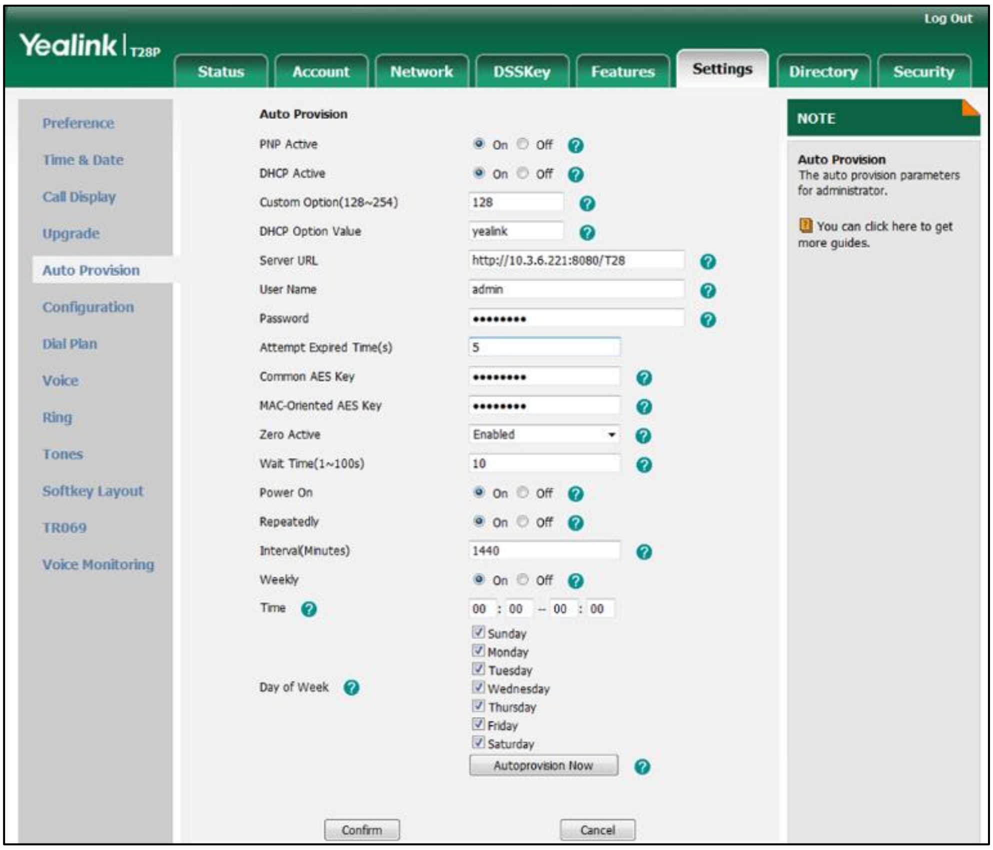
Parameters	Permitted Values	Default
None		
auto_provision.repeat.minutes	**Integer from 1 to 43200**	**1440**
Description: Configures the interval (in minutes) for the IP phone to perform an auto provisioning process repeatedly. **Note**: It works only if the parameter "auto_provision.repeat.enable" is set to 1(Enabled). **Web User Interface:** Settings->Auto provision->Interval (Minutes) **Phone User Interface:** None		
auto_provision.weekly.enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to perform an auto provisioning process weekly. **0**-Disabled **1**-Enabled **Web User Interface:** Settings->Auto provision->Weekly **Phone User Interface:** None		
auto_provision.weekly.begin_time	**Time from 00:00 to 23:59**	**00:00**
Description: Configures the begin time of the day for the IP phone to perform an auto provisioning process weekly. **Note**: It works only if the parameter "auto_provision.weekly.enable" is set to 1(Enabled). **Web User Interface:** Settings->Auto provision->Time **Phone User Interface:** None		
auto_provision.weekly.end_time	**Time from 00:00 to 23:59**	**00:00**

Parameters	Permitted Values	Default
Description: Configures the end time of the day for the IP phone to perform an auto provisioning process weekly. **Note**: It works only if the parameter "auto_provision.weekly.enable" is set to 1(Enabled). **Web User Interface:** Settings->Auto provision->Time **Phone User Interface:** None		
auto_provision.weekly.dayofweek	**0,1,2,3,4,5,6 or a combination of these digits**	**0123456**
Description: Configures the days of the week for the IP phone to perform an auto provisioning process weekly. **0**-Sunday **1**-Monday **2**-Tuesday **3**-Wednesday **4**-Thursday **5**-Friday **6**-Saturday **Example**: auto_provision.weekly.dayofweek = 01 means the IP phone will perform an auto provisioning process every Sunday and Monday. **Note**: It works only if the parameter "auto_provision.weekly.enable" is set to 1(Enabled). The old parameters "auto_provision.schedule.dayofweek" is also applicable to SIP-T28P/T26P/T22P/T20P IP phones. **Web User Interface:** Settings->Auto provision->Day of Week **Phone User Interface:** None		
firmware.url	**URL within 511 characters**	**Blank**

Parameters	Permitted Values	Default
Description: Configures the access URL of the firmware file. **Example:** firmware.url = http://192.168.1.20/2.73.0.40.rom **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Settings->Upgrade->Select and Upgrade Firmware **Phone User Interface:** None		

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

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



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

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

Configuring Basic Features

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

- Power Indicator LED
- Notification Popups
- Contrast
- Backlight
- Call Display
- Web Server Type
- User Password
- Administrator Password
- Phone Lock
- Time and Date
- Language
- Input Method Customization
- Logo Customization
- Softkey Layout
- Key as Send
- Dial Plan
- Hotline
- Off Hook Hot Line Dialing
- Directory
- Search Source in Dialing
- Missed Call Log
- Local Directory
- Live Dialpad
- Call Waiting
- Auto Redial
- Auto Answer
- Call Completion
- Anonymous Call
- Anonymous Call Rejection

- Do Not Disturb
- Busy Tone Delay
- Return Code When Refuse
- Early Media
- 180 Ring Workaround
- Use Outbound Proxy in Dialog
- SIP Session Timer
- Session Timer
- Call Hold
- Call Forward
- Call Transfer
- Network Conference
- Feature Key Synchronization
- Transfer on Conference Hang Up
- Directed Call Pickup
- Group Call Pickup
- Dialog Info Call Pickup
- ReCall
- Call Park
- Calling Line Identification Presentation
- Connected Line Identification Presentation
- DTMF
- Suppress DTMF Display
- Transfer via DTMF
- Intercom

Power Indicator LED

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

Common Power Light On

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

Ringing Power Light Flash

Ringing Power Light Flash allows the power indicator LED to flash when the IP phone receives an incoming call.

Voice/Text Mail Power Light Flash

Voice/Text Mail Power Light Flash allows the power indicator LED to flash when the IP phone receives a voice mail or a text message.

Mute Power Light Flash

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

Hold/Held Power Light Flash

Hold/Held Power Light Flash allows the power indicator LED to flash when a call is placed on hold or is held.

Talk/Dial Power Light On

Talk/Dial Power Light On allows the power indicator LED to be turned on when the IP phone is busy.

Note

For SIP-T28P IP phones, the hardware version must be 1.0.0.2 or higher. For SIP-T26P IP Phones, the hardware version must be 4.0.0.2 or later.

Procedure

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

Configuration File	<y0000000000xx>.cfg	Configure the power indicator LED. **Parameters:** phone_setting.common_power_led_enable phone_setting.ring_power_led_flash_enable phone_setting.mail_power_led_flash_enable phone_setting.mute_power_led_flash_enable phone_setting.hold_and_held_power_led_flash_enable phone_setting.talk_and_dial_power_led_enable
Local	Web User Interface	Configure the power indicator LED. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-powerled&q=load

Details of Configuration Parameters:

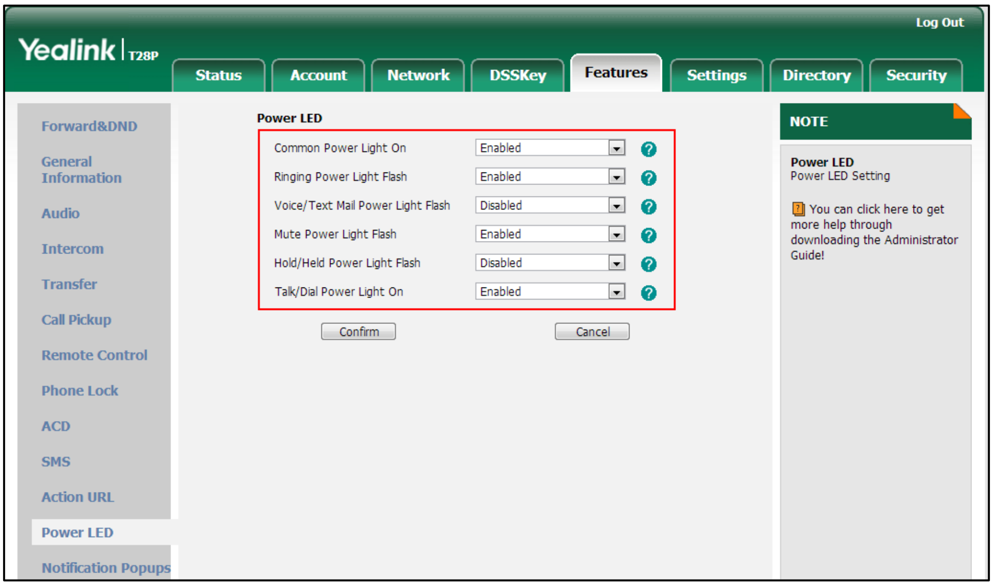
Parameters	Permitted Values	Default
phone_setting.common_power_led_enable	**0 or 1**	**1**
Description: Enables or disables the power indicator LED to be turned on. **0**-Disabled (power indicator LED is off) **1**-Enabled (power indicator LED is solid green) **Note**: The old parameter "features.power_led_on" is also applicable to IP phones. **Web User Interface:** Features->Power LED->Common Power Light On **Phone User Interface:** None		
phone_setting.ring_power_led_flash_enable	**0 or 1**	**1**
Description: Enables or disables the power indicator LED to flash when the IP phone receives an incoming call. **0**-Disabled (power indicator LED does not flash) **1**-Enabled (power indicator LED fast flashes (300ms) green) **Web User Interface:** Features->Power LED->Ring Power Light Flash **Phone User Interface:** None		
phone_setting.mail_power_led_flash_enable	**0 or 1**	**0**
Description: Enables or disables the power indicator LED to flash when the IP phone receives a voice mail or a text message. **0**-Disabled (power indicator LED does not flash) **1**-Enabled (power indicator LED slow flashes (1000ms) green) **Web User Interface:** Features->Power LED->Voice/Text Mail Power Light Flash **Phone User Interface:** None		

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>phone_setting.mute_power_led_flash_enable</td><td>0 or 1</td><td>1</td></tr>
<tr><td colspan="3">Description:
Enables or disables the power indicator LED to flash when a call is mute.
0-Disabled (power indicator LED does not flash)
1-Enabled (power indicator LED fast flashes (300ms) green)
Web User Interface:
Features->Power LED->Mute Power Light Flash
Phone User Interface:
None</td></tr>
<tr><td>phone_setting.hold_and_held_power_led_flash_enable</td><td>0 or 1</td><td>0</td></tr>
<tr><td colspan="3">Description:
Enables or disables the power indicator LED to flash when a call is placed on hold or is held.
0-Disabled (power indicator LED does not flash)
1-Enabled (power indicator LED fast flashes (500ms) green)
Web User Interface:
Features->Power LED->Hold/Held Power Light Flash
Phone User Interface:
None</td></tr>
<tr><td>phone_setting.talk_and_dial_power_led_enable</td><td>0 or 1</td><td>1</td></tr>
<tr><td colspan="3">Description:
Enables or disables the power indicator LED to be turned on when the IP phone is busy.
0-Disabled (power indicator LED is off)
1-Enabled (power indicator LED is solid green)
Web User Interface:
Features->Power LED->Talk/Dial Power Light On
Phone User Interface:
None</td></tr>
</table>

To configure the power Indicator LED via web user interface:

1. Click on **Features**->**Power LED**.
2. Select the desired value from the pull-down list of **Common Power Light On**.

3. Select the desired value from the pull-down list of **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 **Mute Power Light Flash**.
6. Select the desired value from the pull-down list of **Hold/Held Power Light Flash**.
7. Select the desired value from the pull-down list of **Talk/Dial Power Light On**.



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

Notification Popups

Notification popups feature allows the IP phone to display the pop-up message when it misses a call, forwards an incoming call to other party or receives a new voice mail or a new text message.

Note

Notification popups feature is applicable to IP phones running firmware version 73 or later.

Procedure

Notification popups can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure notification popups. **Parameters:** features.voice_mail_popup.enable features.missed_call_popup.enable features.forward_call_popup.enable features.text_message_popup.enable
Local	Web User Interface	Configure notification popups.

		Navigate to: http://<phoneIPAddress>/servlet?p=features-notifypop&q=load

Details of Configuration Parameters:

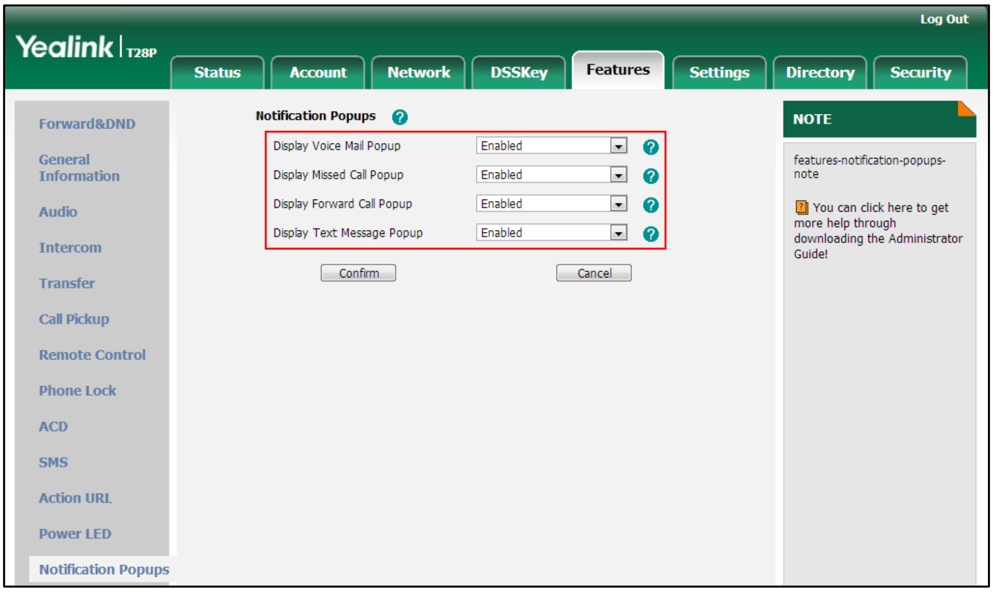
Parameters	Permitted Values	Default
features.voice_mail_popup.enable	**0 or 1**	**1**
Description: Enables or disables the IP phone to display the pop-up message box when it receives a new voice mail. **0**-Disabled **1**-Enabled **Note**: If the voice mail pop-up message box disappears, it won't pop up again unless the user receives a new voice mail or the user re-registers the account that has unread voice mail(s). It is only applicable to IP phones running firmware version 73 or later. **Web User Interface:** Features->Notification Popups->Display Voice Mail Popup **Phone User Interface:** None		
features.missed_call_popup.enable	**0 or 1**	**1**
Description: Enables or disables the IP phone to display the pop-up message box when it misses a call. **0**-Disabled **1**-Enabled **Note**: It is only applicable to IP phones running firmware version 73 or later. **Web User Interface:** Features->Notification Popups->Display Missed Call Popup **Phone User Interface:** None		
features.forward_call_popup.enable	**0 or 1**	**1**
Description: Enables or disables the IP phone to display the pop-up message box when it forwards an incoming call to other party.		

Parameters	Permitted Values	Default
0-Disabled **1**-Enabled **Note**: It is only applicable to IP phones running firmware version 73 or later. **Web User Interface:** Features->Notification Popups->Display Forward Call Popup **Phone User Interface:** None		
features.text_message_popup.enable	**0 or 1**	**1**
Description: Enables or disables the IP phone to display the pop-up message box when it receives a new text message. **0**-Disabled **1**-Enabled **Note**: It is only applicable to IP phones running firmware version 73 or later. **Web User Interface:** Features->Notification Popups->Display Text Message Popup **Phone User Interface:** None		

To configure the notification popups via web user interface:

1. Click on **Features**->**Notification Popups**.
2. Select the desired value from the pull-down list of **Display Voice Mail Popup**.
3. Select the desired value from the pull-down list of **Display Missed Call Popup.**
4. Select the desired value from the pull-down list of **Display Forward Call Popup**.

5. Select the desired value from the pull-down list of **Display Text Message Popup**.



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

Contrast

Contrast determines the readability of the texts displayed on the LCD screen. Adjusting the contrast to a comfortable level can optimize the screen viewing experience. When configured properly, contrast allows users to read the LCD's display with minimal eyestrain. The contrast of the LCD screen is only applicable to SIP-T28P IP phones, and EXP39 connected to SIP-T26P and SIP-T28P IP phones.

Procedure

Contrast can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure the contrast of the LCD screen. **Parameter:** phone_setting.contrast
Local	Web User Interface	Configure the contrast of the LCD screen. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-preference&q=load
	Phone User Interface	Configure the contrast of the LCD screen.

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
phone_setting.contrast	Integer from 1 to 10	6

Description:

Configures the contrast of the LCD screen.

For SIP-T28P IP phones, it configures the LCD's contrast of the IP phone and the connected EXP39.

For SIP-T26P IP phones, it configures the LCD's contrast of the connected EXP39 only.

Note: We recommend that you set the contrast of the LCD screen to 6 as a more comfortable level. It is only applicable to SIP-T28P IP phones, and EXP39 connected to SIP-T26P and SIP-T28P IP phones.

Web User Interface:

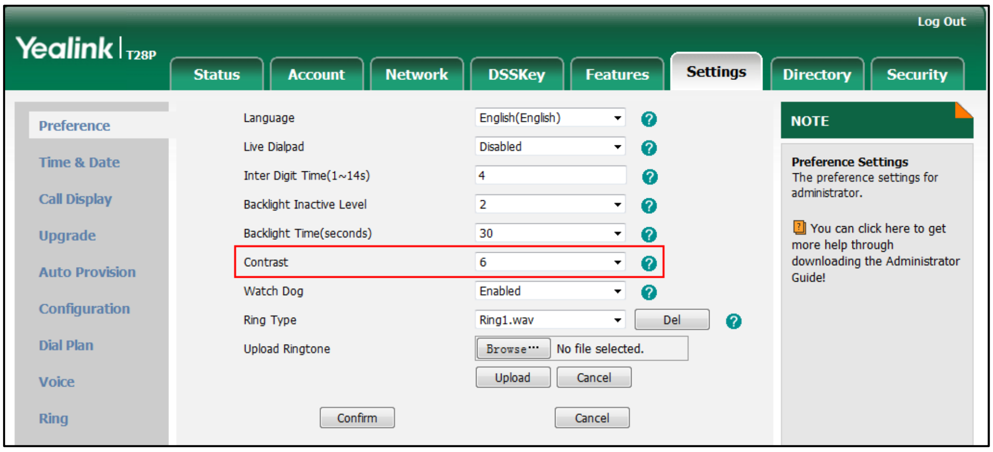
Settings->Preference->Contrast

Phone User Interface:

Menu->Settings->Basic Settings->Display->Contrast

To configure contrast via web user interface:

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



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

To configure contrast via phone user interface (applicable to SIP-T28P IP phones and EXP39 connected to SIP-T26P and SIP-T28P IP phones):

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

   The default contrast level is 6.

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

Note

Before you adjust the LCD's contrast of the expansion module, make sure the expansion module has been connected to the IP phone.

Backlight

Backlight determines the brightness of the LCD screen display, allowing users to read easily in dark environments. Backlight time specifies the delay time to turn off the backlight when the IP phone is inactive. Backlight time is only applicable to SIP-T22P, SIP-T26P and SIP-T28P IP phones, and EXP39 connected to SIP-T26P and SIP-T28P IP phones. Backlight turns off quickly if a short backlight time is configured, this may not give users enough time to read messages. Backlight active level is used to adjust the backlight intensity of the LCD screen. Backlight active level is only applicable to SIP-T28P IP phones and the connected EXP39.

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

- **Always Off:** Backlight is turned off permanently.
- **Always On:** Backlight is turned on permanently.
- **15s**, **30s**, **60s**, **120s**, **300s**, **600s** or **1800s:** Backlight is turned off when the IP phone is inactive after a preset period of time (in seconds), but it is automatically turned on if the status of the IP phone changes or any key is pressed.

The following table lists available methods and configuration options to configure the backlight of each phone model.

Note

Before you adjust the LCD's backlight of expansion module, make sure the expansion module has been connected to the IP phone.

Phone Model	Configuration Methods	Configuration Options
SIP-T28P	Configuration Files Web User Interface Phone User Interface	Backlight Active Level Backlight Time
SIP-T26P	Configuration Files Web User Interface Phone User Interface	Backlight Active Level (only applicable to the connected EXP39) Backlight Time
SIP-T22P	Configuration Files	Backlight Time

Phone Model	Configuration Methods	Configuration Options
	Web User Interface Phone User Interface	

Procedure

Backlight can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure the backlight of the LCD screen. **Parameters:** phone_setting.active_backlight_level phone_setting.backlight_time
Local	Web User Interface	Configure the backlight of the LCD screen. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-preference&q=load
	Phone User Interface	Configure the backlight of the LCD screen.

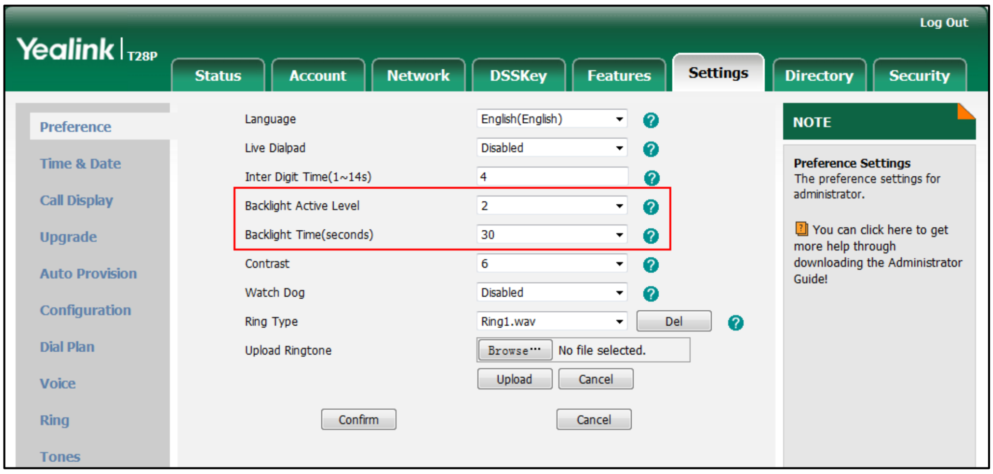
Details of Configuration Parameters:

Parameters	Permitted Values	Default
phone_setting.active_backlight_level	**Integer from 1 to 3**	**2**
Description: Configures the intensity of the LCD screen when the phone is active. Level 3 is the brightest. **Note**: It is only applicable to SIP-T28P IP phones and the connected EXP39. **Web User Interface:** Settings->Preference->Backlight Active Level **Phone User Interface:** Menu->Settings->Basic Settings->Display->Backlight->Backlight Level		
phone_setting.backlight_time	**0, 1, 15, 30, 60, 120, 300, 600 or 1800**	**30**
Description: Configures the delay time (in seconds) to change the intensity of the LCD screen		

Parameters	Permitted Values	Default
when the IP phone is inactive. **0**-Always on **1**-Always off **15**-15s **30**-30s **60**-60s **120**-120s **300**-300s **600**-600s **1800**-1800s If it is set to 60 (60s), the intensity of the LCD screen will be changed when the IP phone is inactive for 60 seconds. **Note**: It is not applicable to SIP-T20P IP phones. **Web User Interface:** Settings->Preference->Backlight Time (seconds) **Phone User Interface:** Menu->Settings->Basic Settings->Display->Backlight->Backlight Time		

To configure backlight via web user interface:

1. Click on **Settings**->**Preference**.
2. Select the desired value from the pull-down list of **Backlight Active Level** (only applicable to SIP-T28P IP phones and the connected EXP39).
3. Select the desired value from the pull-down list of **Backlight Time (seconds)**.



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

To configure backlight via phone user interface (only applicable to SIP-T28P IP phones and EXP39 connected to SIP-T26P and SIP-T28P IP phones):

1. Press **Menu**->**Settings**->**Basic Settings**->**Display**->**Backlight**.
2. Press or , or the **Switch** soft key to select the desired level from the **Backlight Level** field.
3. Press or , or the **Switch** soft key to select the desired type from the **Backlight Time** field.
4. Press the **Save** soft key to accept the change.

To configure backlight via phone user interface (only applicable to SIP-T26P/T22P IP phones):

1. Press **Menu**->**Settings**->**Basic Settings**->**Display**->**Backlight**.
2. Press or , or the **Switch** soft key to select the desired type from the **Backlight Time** field.
3. Press the **Save** soft key to accept the change.

Call Display

Display called party information allows the IP phone to present the callee identity in addition to the presentation of caller identity when it recevices an incoming call, dials an outgoing call or engages in a call.

The following figure shows an example of screen display when Display Called Party Information feature is enabled on the phone.

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

Note

Call Display feature is not applicable to SIP-T20 IP phones and applicable to IP phones running firmware version 73 or later.

Procedure

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

Configuration File	<y0000000000xx>.cfg	Enable or disable display called party information feature. **Parameter:** phone_setting.called_party_info_display.enable Sepecify the type of caller information display. **Parameter:** phone_setting.call_info_display_method
Local	Web User Interface	Configure call display features. **Navigate to:** 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**	**0**
Description: Enables or disables the IP phone to display the called account information when receiving an incoming call. **Web User Interface:** Settings->Call Display->Display Called Party Information **Phone User Interface:** None		
phone_setting.call_info_display_method	**Integer from 0 to 4**	**0**

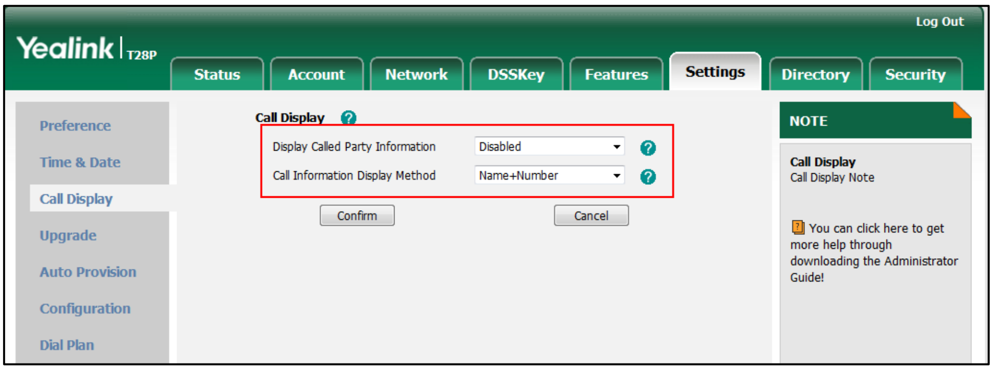
<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td colspan="3">Description:
Specifies the caller and callee information display method when the IP phone receives an incoming call, dials an outgoing call or is during an active call.
0-Name+Number
1-Number+Name
2-Name
3-Number
4-Full Contact Info (display name<sip:xxx@domain.com>)
Note: The selected display method will also apply to the called account information display.
Web User Interface:
Settings->Call Display->Call Information Display Method
Phone User Interface:
None</td></tr>
</table>

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**.

   The default value is Disabled.
3. Select the desired value from the pull-down list of **Call Information Display Method**..

   The default value is Name+Number.



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

Web Server Type

Web server type determines access protocol of the IP phone’s web user interface. IP phones support both HTTP and HTTPS protocols for accessing the web user interface. HTTP is an application protocol that runs on top of the TCP/IP suite of protocols. HTTPS is a web protocol that encrypts and decrypts user page requests as well as 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.

Configuration File	<y0000000000xx>.cfg	Configure the web access type, HTTP port and HTTPS port. **Parameters:** wui.http_enable network.port.http wui.https_enable network.port.https
Local	Web User Interface	Configure the web access type, HTTP port and HTTPS port. **Navigate to**: http://<phoneIPAddress>/servlet?p=network-adv&q=load
	Phone User Interface	Configure the web access type, HTTP port and HTTPS port.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
wui.http_enable	**0 or 1**	**1**
Description: Enables or disables the user to access web user interface of the IP phone using HTTP protocol. **0**-Disabled **1**-Enabled **Note**: If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->Web Server->HTTP **Phone User Interface:** Menu->Settings->Advanced Settings (default password: admin) ->Network->Webserver Type->HTTP Status		

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>network.port.http</td><td>Integer from 1 to 65535</td><td>80</td></tr>
<tr><td colspan="3">Description:
Configures the HTTP port for the user to access web user interface of the IP phone using the HTTP protocol.
The default HTTP port is 80.
Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Web User Interface:
Network->Advanced->Web Server->HTTP Port (1~65535)
Phone User Interface:
Menu->Settings->Advanced Settings (default password: admin)
->Network->Webserver Type->HTTP Port</td></tr>
<tr><td>wui.https_enable</td><td>0 or 1</td><td>1</td></tr>
<tr><td colspan="3">Description:
Enables or disables the user to access web user interface of the IP phone using HTTPS protocol.
0-Disabled
1-Enabled
Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Web User Interface:
Network->Advanced->Web Server->HTTPS
Phone User Interface:
Menu->Settings->Advanced Settings (default password: admin)
->Network->Webserver Type->HTTPS Status</td></tr>
<tr><td>network.port.https</td><td>Integer from 1 to 65535</td><td>443</td></tr>
</table>

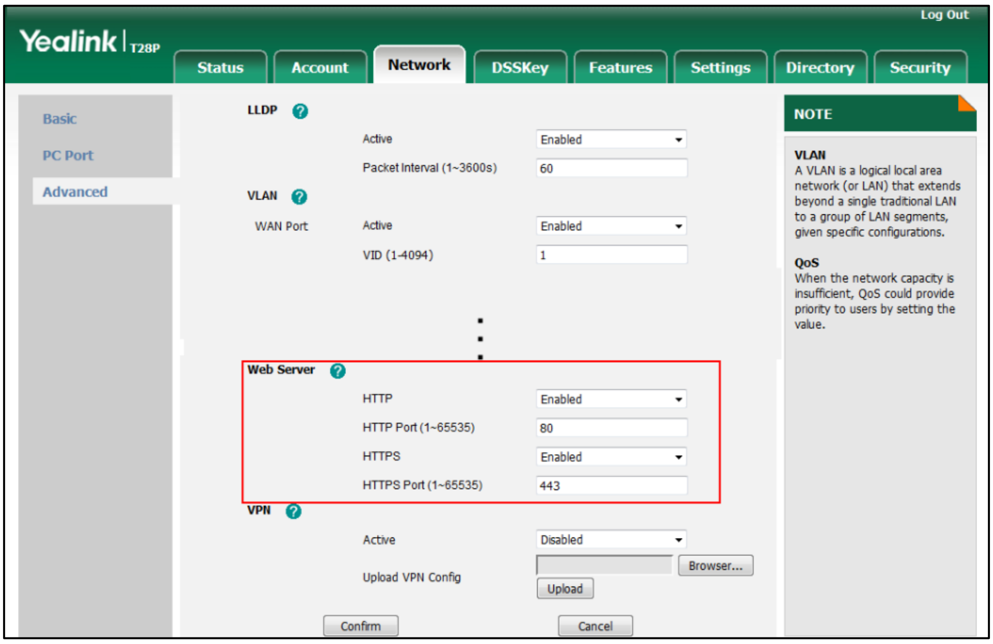
Parameters	Permitted Values	Default
Description: Configures the HTTPS port for the user to access web user interface of the IP phone using the HTTPS protocol. The default HTTPS port is 443. **Note**: If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->Web Server->HTTPS Port (1~65535) **Phone User Interface:** Menu->Settings->Advanced Settings (default password: admin) ->Network->Webserver Type->HTTP Port		

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 HTTP port number in the **HTTP Port (1~65535)** field.

   The default HTTP port number is 80.
4. Select the desired value from the pull-down list of **HTTPS**.
5. Enter the HTTPS port number in the **HTTPS Port (1~65535)** field.

   The default HTTPS port number is 443.



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.

To configure web server type via phone user interface:

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

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

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.

Configuration File	<y0000000000xx>.cfg	Change the user password of the IP phone. **Parameter:** security.user_password
Local	Web User Interface	Change the user password of the IP phone. **Navigate to:** http://<phoneIPAddress>/servlet?p=security&q=load

Details of the Configuration Parameter:

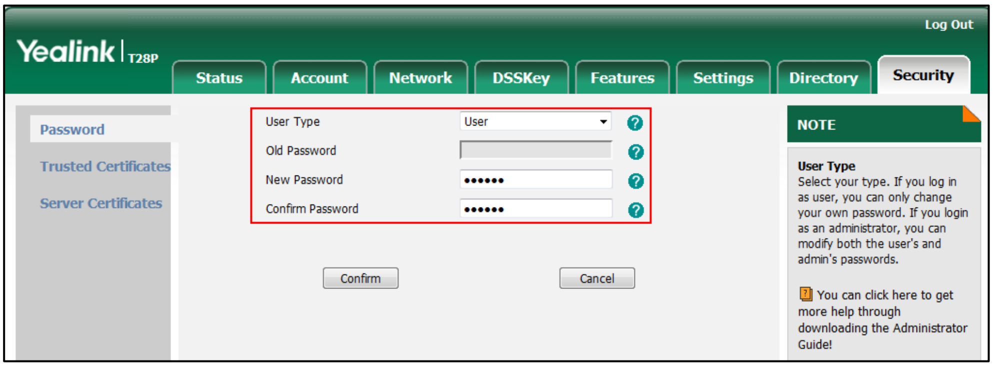
Parameter	Permitted Values	Default
security.user_password	String within 32 characters	user

Parameter	Permitted Values	Default
Description: Configures the password of the user for web server access. The IP phone uses "user" as the default user password. The valid value format is username:new password. **Example:** security.user_password = user:password123 means setting the password of user (current user name is "user") to password123. **Note**: IP 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 **Phone 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.

Configuration File	<y0000000000xx>.cfg	Change the administrator password. **Parameter**: security.user_password
Local	Web User Interface	Change the administrator password. **Navigate to**: http://<phoneIPAddress>/servlet?p=security&q=load
	Phone User Interface	Change the administrator password.

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
security.user_password	**String within 32 characters**	**admin**
Description: Configures the password of the administrator for web server access. The IP phone uses "admin" as the default administrator password. **Example**: security.user_password = admin:password123 means setting the password of administrator (current user name is "admin") to password123. **Note**: IP 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 **Phone User Interface:** None		

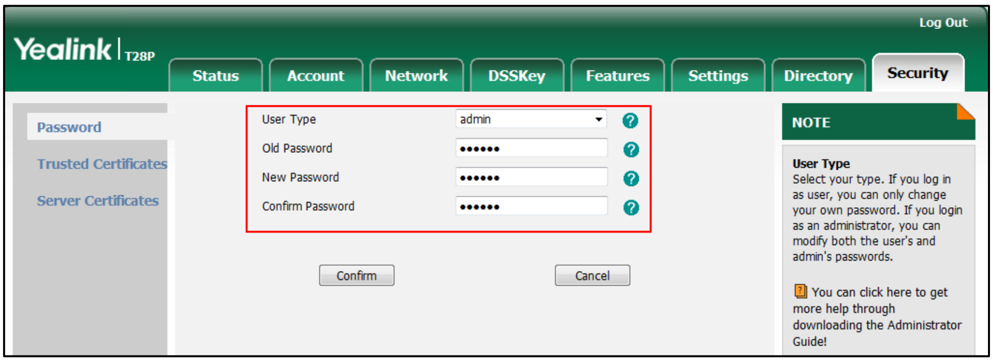
To change the administrator password via web user interface:

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.

To change the administrator password via phone user interface:

1. Press **Menu**->**Settings**->**Advanced Settings** (default password: admin) ->**Set Password**.

2. Enter the current administrator password in the **Current PWD** field.

3. Enter new password in the **New PWD** field and **Confirm PWD** field.

   Valid characters are ASCII characters 32-126(0x20-0x7E).

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

Phone Lock

Phone lock is used to lock the IP phone to prevent it from unauthorized use. Once the IP phone is locked, a user must enter the password to unlock it. IP phones offer three types of phone lock: Menu Key, Function Keys and All Keys. The IP phone will not be locked immediately after the phone lock type is configured. One of the following steps is also needed:

- Long press the pound key when the IP phone is idle.

- Press the phone lock key (if configured) when the IP phone is idle.

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

Procedure

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

Configuration File	<y0000000000xx>.cfg	Configure the type of phone lock. **Parameter:** phone_setting.lock

		Change the unlock PIN. **Parameter:** phone_setting.phone_lock.unlock_pin Configure the IP phone to automatically lock the keypad after a time interval. **Parameter:** phone_setting.phone_lock.lock_time_out Assign a phone lock key. **Parameter:** memorykey.X.type/linekey.X.type/ programablekey.X.type
Local	Web User Interface	Configure the type of phone lock. Change the unlock PIN. Configure the IP phone to automatically lock the keypad after a time interval. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-phonelock&q=load Assign a phone lock key. **Navigate to**: http://<phoneIPAddress>/servlet?p=dsskey&q=load&model=0
	Phone User Interface	Change the unlock PIN. Configure the type of phone lock. Assign a phone lock key.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
phone_setting.lock	**0, 1, 2 or 3**	**0**
Description: Configures the type of phone lock. **0**-Disabled **1**-Menu Key **2**-Function Keys **3**-All Keys **Menu Key**: The Menu soft key and MESSAGE key are locked (For SIP-T20P, the MENU		

Parameters	Permitted Values	Default
key is locked). **Function Keys**: MESSAGE, RD, CONF, HOLD, MUTE, TRAN, OK, X, navigation keys, soft keys, line keys and memory keys are locked (For SIP-T22P, CONF, HOLD, MUTE and memory keys do not exist; For SIP-T20P, the MUTE key, soft keys and memory keys do not exist, but the additional MENU and Directory keys are locked). **All Keys**: All keys are locked except the volume key. You are only allowed to dial emergency numbers, reject incoming calls by pressing the X key, answer incoming calls by lifting the handset, pressing the Speakerphone key, the HEADSET key or the OK key, place an active call on hold by pressing the Hold soft key or the HOLD key, resume the held call by pressing the Resume soft key or the HOLD key, and end the call by hanging up the handset, pressing the Speakerphone key or pressing the X key (pressing the X key to end the call is not applicable to SIP-T22P/T20P). For SIP-T22P, HOLD key does not exist; For SIP-T20P, soft keys do not exist. If it is set to 0 (Disabled), IP phone lock feature is disabled. **Web User Interface:** Features->Phone Lock->Phone Lock Type **Phone User Interface:** Menu->Settings->Advanced Settings(default password: admin)->Phone Lock		
phone_setting.phone_lock.unlock_pin	**characters within 15 digits**	**123**
Description: Configures the password for unlocking the keypad. **Web User Interface:** Features->Phone Lock->Phone Unlock PIN (0~15 Digit) **Phone User Interface:** Menu->Settings->Basic Settings->Change PIN		
phone_setting.phone_lock.lock_time_out	**Integer from 0 to 3600**	**0**
Description: Configures the interval (in seconds) to automatically lock the keypad. The default value is 0 (the keypad is locked only by long pressing the pound key or pressing the phone lock key). **Note**: It works only if the type of phone lock is preset. **Web User Interface:** Features->Phone Lock->Phone Lock Time Out (0~3600s) **Phone User Interface:**		

Parameters	Permitted Values	Default
None		

Phone Lock Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 513.

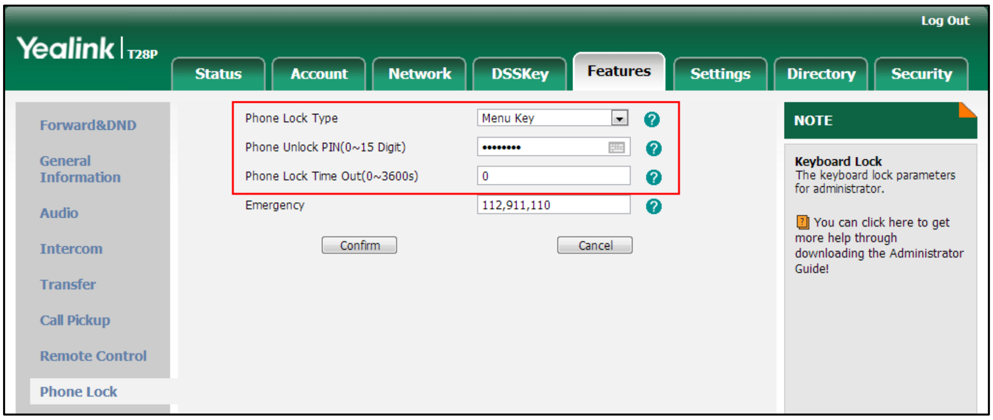
Parameter	Permitted Values	Default
memorykey.X.type/ linekey.X.type/ programablekey.X.type	**50**	**Refer to the following content**
Description: Configures a DSS key as a phone lock key on the IP phone. The digit **50** stands for the key type **Phone Lock**. For memory keys: X ranges from 1 to 10 (for SIP-T28/T26P). For line keys: X ranges from 1 to 6 (for SIP-T28P) X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). For programable keys: X ranges from 1 to 14 (for SIP-T28/T26P) X=1-10, 14 (for SIP-T22P) X=5-12, 14 (for SIP-T20P) **Example:** memorykey.1.type = 50 **Default:** For memory keys: The default value is 0. For line keys: The default value is 15. For programable keys: **For SIP-T28P/T26P IP phones:** When X=1, the default value is 28 (History). When X=2, the default value is 61 (Directory). When X=3, the default value is 5 (DND).		

Parameter	Permitted Values	Default
When X=4, the default value is 30 (Menu). When X=5, the default value is 28 (History). When X=6, the default value is 61 (Directory). When X=7, the default value is 31 (Switch Account). When X=8, the default value is 31 (Switch Account). When X=9, the default value is 33 (Status). When X=10, the default value is 0 (NA). When X=11, the default value is 0 (NA). When X=12, the default value is 0 (NA). When X=13, the default value is 0 (NA). When X=14, the default value is 2 (Forward). **For SIP-T22P IP phones:** When X=1, the default value is 28 (History). When X=2, the default value is 61 (Directory). When X=3, the default value is 5 (DND). When X=4, the default value is 30 (Menu). When X=5, the default value is 28 (History). When X=6, the default value is 61 (Directory). When X=7, the default value is 31 (Switch Account). When X=8, the default value is 31 (Switch Account). When X=9, the default value is 33 (Status). When X=10, the default value is 0 (NA). When X=14, the default value is 2 (Forward). **For SIP-T20P IP phones:** When X=5, the default value is 28 (History). When X=6, the default value is 61 (Directory). When X=7, the default value is 31 (Switch Account). When X=8, the default value is 31 (Switch Account). When X=9, the default value is 33 (Status). When X=10, the default value is 0 (NA). When X=11, the default value is 0 (NA). When X=12, the default value is 0 (NA). When X=14, the default value is 2 (Forward). **Web User Interface:** DSSKey->Memory Key/ Line Key / Programable Key ->Type		

Parameter	Permitted Values	Default
Phone User Interface: Menu->Features->DSS Keys->Memory Keys (or Line Keys)->DSS Key X (or Line Key X)->Type		

To configure phone lock via web user interface:

1. Click on **Features**->**Phone Lock**.
2. Select the desired type from the pull-down list of **Phone Lock Type**.
3. Enter the unlock PIN in the **Phone Unlock PIN (0~15 Digit)** field.
4. Enter the desired time in the **Phone Lock Time Out (0~3600s)** field.



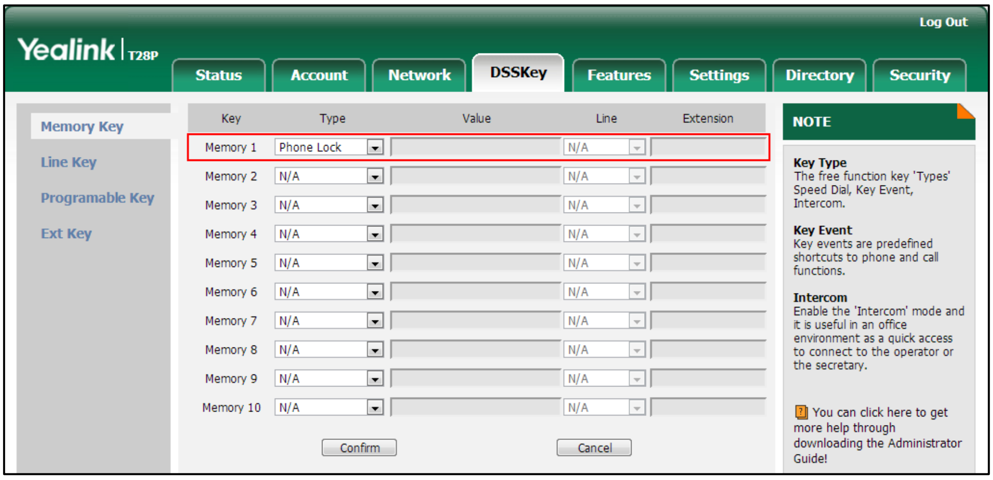
5. Click **Confirm** to accept the change.

To configure a phone lock key via web user interface:

1. Click on **DSSKey**->**Memory Key** (**Line Key** or **Programable Key**).

   SIP-T22P/T20P IP phones only support line keys and programable keys.

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



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

To configure the type of phone lock via phone user interface:

1. Press **Menu**->**Settings**->**Advanced Settings** (default password: admin) ->**Phone Lock**.
2. Press or , or the **Switch** soft key to select the desired type from the **Phone Lock** field.
3. Press the **Save** soft key to accept the change.

To change the unlock PIN via phone user interface:

1. Press **Menu**->**Settings**->**Basic Settings**->**Change PIN**.
2. Enter the current unlock PIN in the **Current PIN** field.
3. Enter the new unlock PIN in the **New PIN** field.
4. Enter the new unlock PIN again in the **Confirm PIN** field.
5. Press the **Save** soft key to accept the change.

To configure a phone lock key via phone user interface:

1. Press **Menu**->**Features**->**DSS Keys**->**Memory Keys** (or **Line Keys**).
2. Select the desired DSS key.
3. Press or , or the **Switch** soft key to select **Phone Lock** from the **Type** field.
4. Press the **Save** soft key to accept the change.

Time and Date

IP phones maintain a local clock and calendar. Time and date are displayed on the idle screen of IP phones. Time and date are synced automatically from the NTP server by default. The NTP server can be obtained by DHCP or configured manually. If IP phones cannot obtain the time and date from the NTP server, you need to manually configure them. The time and date display can use one of several different formats. SIP-T20P IP phones have a limited selection of date format due to a smaller display size.

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

Daylight Saving Time

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

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

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

Procedure

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

Configuration File	<MAC>.cfg	Configure NTP by DHCP priority feature and DHCP time features. **Parameters:** local_time.manual_ntp_srv_prior local_time.dhcp_time Configure the NTP server, time zone and DST. **Parameters:** local_time.ntp_server1 local_time.ntp_server2 local_time.interval local_time.time_zone

		local_time.time_zone_name local_time.summer_time local_time.dst_time_type local_time.start_time local_time.end_time local_time.offset_time Configure the time and date manually. **Parameter:** local_time.manual_time_enable Configure the time and date formats. **Parameters:** local_time.time_format local_time.date_format
Local	Web User Interface	Configure NTP by DHCP priority feature. Configure the NTP server, time zone and DST. Configure the time and date manually. Configure the time and date formats. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-datetime&q=load
	Phone User Interface	Configure the NTP server and time zone. Configure the time and date manually. Configure the time and date formats.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
local_time.manual_ntp_srv_prior	0 or 1	0

Parameters	Permitted Values	Default
Description: Enables or disables the IP phone to use manually configured NTP server preferentially. **0**-High (use the NTP server obtained by DHCP preferentially) **1**-Low (use the NTP server configured manually preferentially) **Web User Interface:** Settings->Time & Date->NTP By DHCP Priority **Phone User Interface:** None		
local_time.dhcp_time	**0 or 1**	**0**
Description: Enables or disables the IP phone to update time with the offset time obtained from the DHCP server. **0**-Disabled **1**-Enabled **Note**: It is only available to offset from GMT 0. **Web User Interface:** Settings->Time & Date->DHCP Time **Phone User Interface:** Menu->Settings->Basic Settings->Time & Date->DHCP Time Zone		
local_time.ntp_server1	**IP Address or Domain Name**	**cn.pool.ntp.org**
Description: Configures the IP address or the domain name of the NTP server 1. **Example:** local_time.ntp_server1 = 192.168.0.5 **Web User Interface:** Settings->Time & Date->Primary Server **Phone User Interface:** Menu->Settings->Basic Settings->Time & Date->SNTP Settings->NTP Server 1		
local_time.ntp_server2	**IP Address or Domain Name**	**cn.pool.ntp.org**
Description:		

Parameters	Permitted Values	Default
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 phone will request the time and date from the NTP server 2. **Example:** local_time.ntp_server2 = 192.168.0.6 **Web User Interface:** Settings->Time & Date->Secondary Server **Phone User Interface:** Menu->Settings->Basic Settings->Time & Date->SNTP Settings->NTP Server 2		
local_time.interval	**Integer from 15 to 86400**	**1000**
Description: Configures the interval (in seconds) to update time and date from the NTP server. **Example:** local_time.interval = 1000 **Web User Interface:** Settings->Time & Date->Synchronism (15~86400s) **Phone User Interface:** None		
local_time.time_zone	**-11 to +14**	**+8**
Description: Configures the time zone. For more available time zones, refer to Appendix B: Time Zones on page 509. **Example:** local_time.time_zone = +8 **Web User Interface:** Settings->Time & Date->Time Zone **Phone User Interface:** Menu->Settings->Basic Settings->Time & Date->SNTP Settings->Time Zone		
local_time.time_zone_name	**String within 32 characters**	**China(Beijing)**
Description: Configures the time zone name. The available time zone names depend on the time zone configured by the		

Parameters	Permitted Values	Default
parameter "local_time.time_zone". For more information on the available time zone names for each time zone, refer to Appendix B: Time Zones on page 509. **Note**: It works only if the value of the parameter "local_time.summer_time" is set to 2 (Automatic). **Example:** local_time.time_zone_name = China(Beijing) **Web User Interface:** Settings->Time & Date->Time Zone **Phone User Interface:** Menu->Settings->Basic Settings->Time & Date->SNTP Settings->Time Zone		
local_time.summer_time	**0, 1 or 2**	**2**
Description: Configures Daylight Saving Time (DST) feature. **0**-Disabled **1**-Enabled **2**-Automatic **Web User Interface:** Settings->Time & Date->Daylight Saving Time **Phone User Interface:** Menu->Settings->Basic Settings->Time & Date->SNTP Settings->DST		
local_time.dst_time_type	**0 or 1**	**0**
Description: Configures the DST time type. **0**-By Date **1**-By Week **Note**: It works only if the parameter "local_time.summer_time" is set to 1 (Enabled). **Web User Interface:** Settings->Time & Date->Fixed Type **Phone User Interface:** None		
local_time.start_time	**Time**	**1/1/0**
Description:		

Parameters	Permitted Values	Default
Configures the start time of the DST. **Value formats are:** • Month/Day/Hour (for By Date) • Month/ Day of Week Last in Month/ Day of Week/ Hour of Day (for By Week) If "local_time.dst_time_type" is set to 0 (By Date), use the mapping: Month: 1=Jan, 2=Feb,..., 12=Dec Day:1=the first day in a month,..., 31= the last day in a month Hour:0=0am, 1=1am,..., 23=11pm If "local_time.dst_time_type" is set to 1 (By Week), use the mapping: Month: 1=Jan, 2=Feb,..., 12=Dec Day of Week Last in Month: 1=the first week in a month,..., 5=the last week in a month Day of Week: 1=Mon, 2=Tues,..., 7=Sun Hour of Day: 0=0am, 1=1am,..., 23=11pm **Note**: It works only if the parameter "local_time.summer_time" is set to 1 (Enabled). **Web User Interface:** **For DST By Date:** Settings->Time & Date->Start Date **For DST By Week:** Settings->Time & Date->DST Start Month/ DST Start Day of Week/ DST Start Day of Week Last in Month/ Start Hour of Day **Phone User Interface:** None		
local_time.end_time	**Time**	**12/31/23**
Description: Configures the end time of the DST. **Value formats are:** • Month/Day/Hour (for By Date) • Month/ Day of Week Last in Month/ Day of Week/ Hour of Day (for By Week) If "local_time.dst_time_type" is set to 0 (By Date), use the mapping: Month: 1=Jan, 2=Feb,..., 12=Dec Day:1=the first day in a month,..., 31= the last day in a month Hour:0=0am, 1=1am,..., 23=11pm		

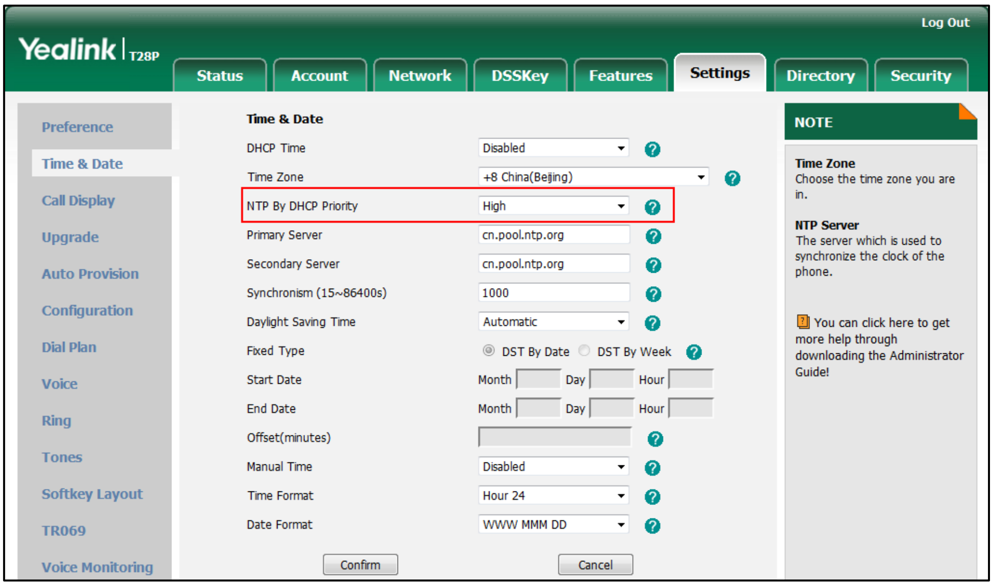
Parameters	Permitted Values	Default
If "local_time.dst_time_type" is set to 1 (By Week), use the mapping: Month: 1=Jan, 2=Feb,…, 12=Dec Day of Week Last in Month: 1=the first week in a month,…, 5=the last week in a month Day of Week: 1=Mon, 2=Tues,…, 7=Sun Hour of Day: 0=0am, 1=1am,…, 23=11pm **Note**: It works only if the parameter "local_time.summer_time" is set to 1 (Enabled). **Web User Interface:** **For DST By Date:** Settings->Time & Date->End Date **For DST By Week:** Settings ->Time & Date->DST Stop Month/ DST Stop Day of Week/ DST Stop Day of Week Last in Month/ Stop Hour of Day **Phone User Interface:** None		
local_time.offset_time	**Integer from -300 to 300**	**Blank**
Description: Configures the offset time (in minutes) of DST. **Note**: It works only if the parameter "local_time.summer_time" is set to 1 (Enabled). **Web User Interface:** Settings->Time & Date->Offset (minutes) **Phone User Interface:** None		
local_time.manual_time_enable	**0 or 1**	**0**
Description: Configures the IP phone to obtain time from the NTP server or manual settings. **0**-NTP **1**-Manual **Web User Interface:** Settings->Time & Date->Manual Time **Phone User Interface:** None		

Parameters	Permitted Values	Default
local_time.time_format	0 or 1	1
Description: Configures the time format. **0**-12 Hour **1**-24 Hour If it is set to 0 (12 Hour), the time will be displayed in 12-hour format with AM or PM specified. If it is set to 1 (24 Hour), the time will be displayed in 24-hour format (eg., 2:00 PM displays as 14:00). **Web User Interface:** Settings->Time & Date->Time Format **Phone User Interface:** Menu->Settings->Basic Settings->Time & Date->Time & Date Format->Clock		
local_time.date_format	Refer to the following content	Refer to the following content
Description: Configures the date format. **For SIP-T28P/T26P/T22P IP phones:** **Valid values are:** **0**-WWW MMM DD **1**-DD-MMM-YY **2**-YYYY-MM-DD **3**-DD/MM/YYYY **4**-MM/DD/YY **5**-DD MMM YYYY **6**-WWW DD MMM **For SIP-T20P IP phones:** **7**-MM DD YY **8**-DD MM YY **9**-YY MM DD **Permitted Values:** 0, 1, 2, 3, 4, 5 or 6 (for SIP-T22P/T26P/T28P) 7, 8 or 9 (for SIP-T20P) **Default Value:**		

Parameters	Permitted Values	Default
For SIP-T22P/T26P/T28P IP phones, the default value is 0. For SIP-T20P IP phones, the default value is 7. **Note**: "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 which is not displayed on the LCD screen of SIP-T20P IP phones. **Web User Interface:** Settings->Time & Date->Date Format **Phone User Interface:** Menu->Settings->Basic Settings->Time & Date->Time & Date Format->Date Format		

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

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



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

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

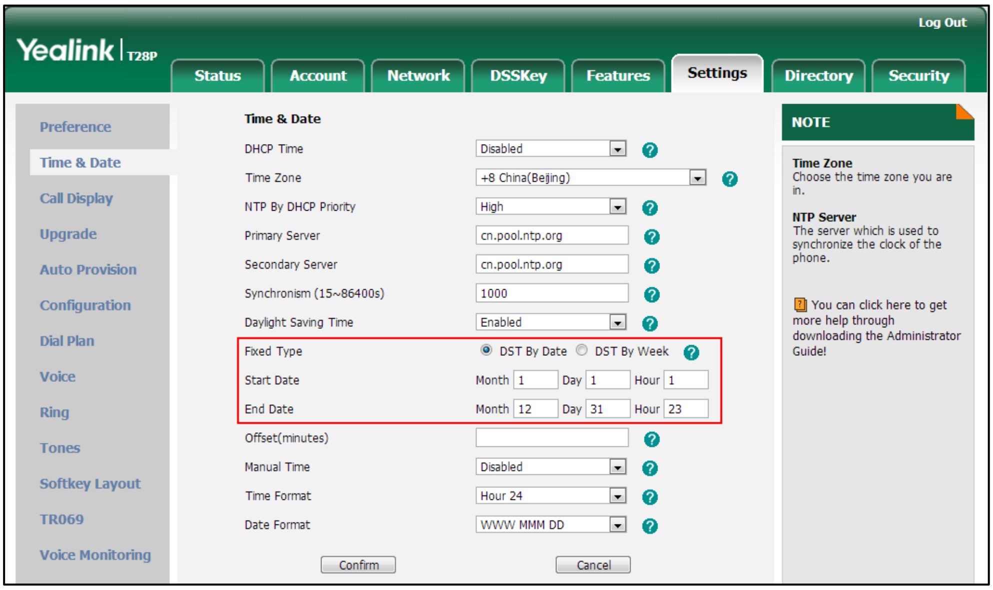
1. Click on **Settings**->**Time & Date**.
2. Select **Disabled** from the pull-down list of **Manual Time**.
3. Select the desired time zone from the pull-down list of **Time Zone**.
4. Enter the domain names or IP addresses in the **Primary Server** and **Secondary Server** fields respectively.
5.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

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

- Mark the **DST By Date** radio box in the **Fixed Type** field.

  Enter the start time in the **Start Date** field.

  Enter the end time in the **End Date** field.

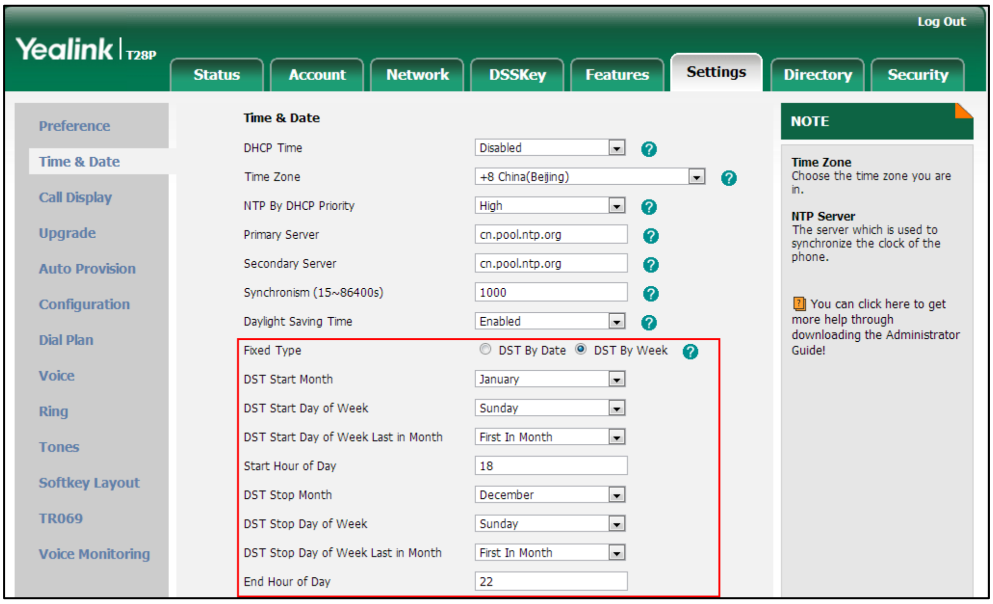


- Mark the **DST By Week** radio box in the **Fixed Type** field.

  Select the desired values from the pull-down lists of **DST Start Month, DST Start Day of Week**, **DST Start Day of Week Last in Month**, **DST Stop Month**, **DST Stop Day of Week** and **DST Stop Day of Week Last in Month**.

  Enter the desired time in the **Start Hour of Day** field.

  Enter the desired time in the **End Hour of Day** field.

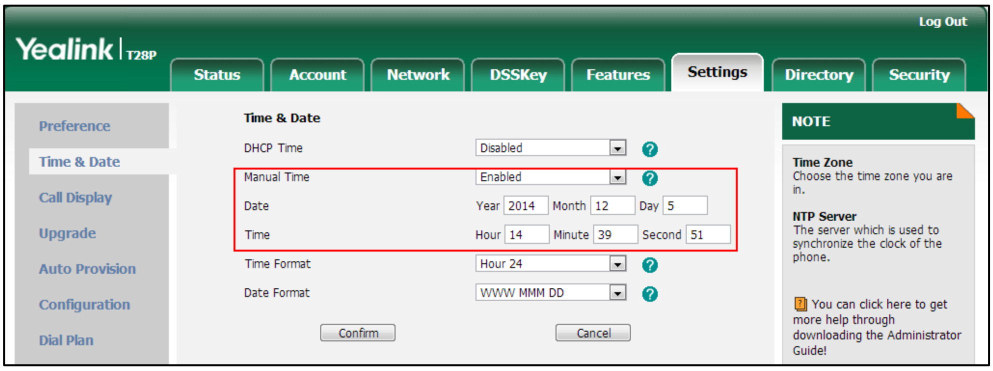


7. Enter the desired offset time in the **Offset (minutes)** field.

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

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

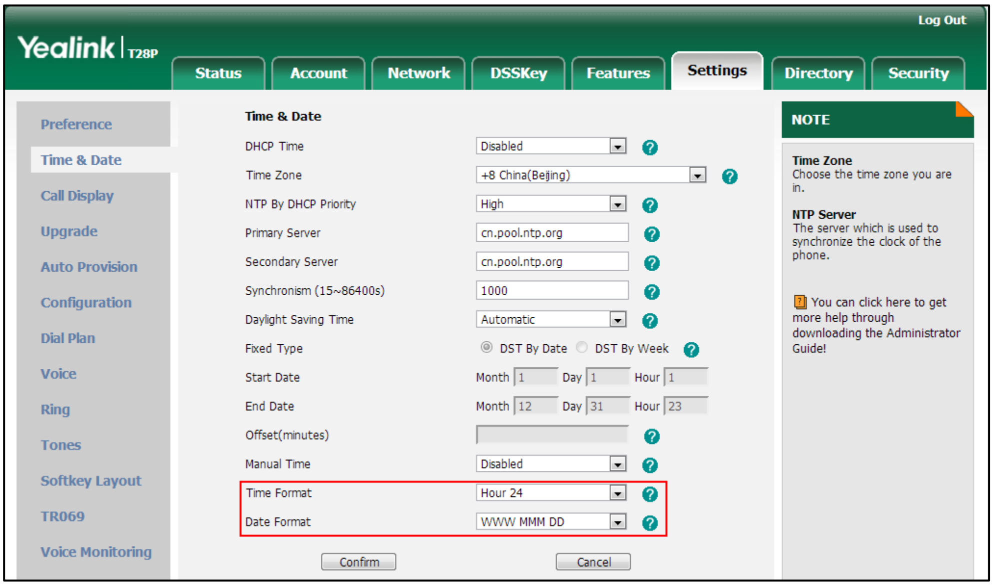
1. Click on **Settings**->**Time & Date**.
2. Select **Enabled** from the pull-down list of **Manual Time**.
3. Enter the time and date in the corresponding fields.



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

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

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



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

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

1. Press **Menu**->**Settings**->**Basic Settings**->**Time & Date**->**SNTP Settings**.
2. Press or , or the **Switch** soft key to select the time zone that applies to your area from the **Time Zone** field.

The default time zone is "+8 China(Beijing)".

3. Enter the domain names or IP addresses in the **NTP Server1** and **NTP Server2** fields respectively.

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

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

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

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

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

Language

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

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

Phone User Interface	Web User Interface
English	English
French	Chinese Simplified
German	Chinese Traditional
Italian	French
Polish	German
Portuguese	Italian
Spanish	Polish
Turkish	Portuguese
Russian (not applicable to SIP-T20P IP phones)	Spanish
	Turkish

Phone User Interface	Web User Interface
	Russian

Loading Language Packs

Languages available for selection depend on language packs currently loaded to the IP phone. You can customize the translation of the existing language on the phone user interface or web user interface. You can also make new languages available for use on the phone user interface and web user interface by loading language packs to the IP phone. Language packs can only be loaded using configuration files.

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

Available Language	Associated Language Pack For SIP-T20P/T22P/T26P/T28P
English	000.GUI.English.lang
Chinese Simplified	/
Chinese Traditional	/
French	001.GUI.French.lang
German	002.GUI.German.lang
Italian	003.GUI.Italian.lang
Polish	004.GUI.Polish.lang
Portuguese	005.GUI.Portuguese.lang
Spanish	006.GUI.Spanish.lang
Turkish	007.GUI.Turkish.lang
Russian	008.GUI.Russian.lang

When adding a new language pack for the phone user interface of SIP-T20/T22/T26/T28 IP Phones, the language pack must be formatted as "X.GUI.name.lang" (X starts from 009, "name" is replaced with the language name). If the language name is the same as the existing one, the existing language pack will be overridden by the new uploaded one. We recommend that the filename of the new language pack should not be the same as the existing one.

To customize a language file:

1. Open the desired language template file (e.g., 000.GUI.English.lang) using an ASCII editor.
2. Modify the characters within the double quotation marks on the right of the equal sign.

   Don't modify the translation item on the left of the equal sign.

The following shows a portion of the language pack "000.GUI.English.lang" for the phone user interface.

000.GUI.English.lang

```
[ lang ]
"(Empty)"="(Empty)"
"12 Hour"="12 Hour"
"120s"="120s"
"15s"="15s"
"1800s"="1800s"
"24 Hour"="24 Hour"
"300s"="300s"
"30s"="30s"
"600s"="600s"
"60s"="60s"
"802.1x Mode"="802.1x Mode"
"802.1x Settings"="802.1x Settings"
"ACD Login"="ACD Login"
"ACD State"="ACD State"
"ACD Status"="ACD Status"
"ACD Trace"="Trace"
"ACD"="ACD"
"ALERT"="ALERT"
"AM"="AM"
"Account Not Usable!"="Account Not Usable!"
"Account Status"="Account Status"
"Account"="Account"
"AccountID"="Account ID"
"Accounts"="Accounts"
"Activation"="Activation"
"Add Blacklist"="Add Blacklist"
"Add Contact"="Add Contact"
```

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

Available Language	Associated Language Pack	Associated Note Language Pack
English	1.English.js	1.English_note.xml
Chinese Simplified	2.Chinese_S.js	2.Chinese_S_note.xml
Chinese Traditional	3.Chinese_T.js	3.Chinest_T_note.xml
French	4.French.js	4.French_note.xml
German	5.German.js	5.German_note.xml

Available Language	Associated Language Pack	Associated Note Language Pack
Italian	6.Italian.js	6.Italian_note.xml
Polish	7.Polish.js	7.Polish_note.xml
Portuguese	8.Portuguese.js	8.Portuguese_note.xml
Spanish	9.Spanish.js	9.Spanish_note.xml
Turkish	10.Turkish.js	10.Turkish_note.xml
Russian	11.Russian.js	11.Russian_note.xml

When adding a new language pack for the web user interface, the language pack must be formatted as "Y.name.js" (Y starts from 12, "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:

```
var _objTrans =
{

" Call Number Filter":"Call Number Filter",
" Distinctive Ring Tones":"Distinctive Ring Tones",
" Do you want to reboot ?":"Do you want to reboot?",
"(800*480)":"(800*480)",
"0":"0",
"1":"1",
"10min":"10min",
"1min":"1min",
"2":"2",
"2min":"2min",
"3":"3",
"30min":"30min",
"4":"4",
"404 (Not found)":"404 (Not Found)",
"480 (Temporarily not available)":"480 (Temporarily Not Available)",
"486 (Busy here)":"486 (Busy Here)",
"5":"5",
"5min":"5min",
"6":"6",
"603 (Decline)":"603 (Decline)",
"ACD Auto Available Timer(0~120s)":"ACD Auto Available Timer(0~120s)",
"ACD Auto Available":"ACD Auto Available",
"ACD Trace":"ACD Trace",
"ACD":"ACD",
"ACD:":"ACD",
"ACD_SubscripPeriod(120~3600s)":"ACD Subscrip Period(120~3600s)",
"ACS Password":"ACS Password",
```

You can also customize the translation of the note language pack. The note information is integrated in the icon of the web user interface. The note language pack must be formatted as "Y.name_note.xml" ("Y" and "name" are associated with web language pack).

To customize a note language file:

1. Open the desired note language template file (e.g., 1.English_note.xml) using an ASCII editor.
2. Modify the text of the note field.

   Don't modify the name of the note field.

The following shows a portion of the note language pack “1.English_note.xml” for the web user interface:

```
1.English_note.xml

<?xml version="1.0" encoding="utf-8"?>
<notedata>

<status>
  <note name = "version">
    Displays current firmware version and hardware version of the device
  </note>
    <note name = "network">
    Shows details of the phone network configuration
  </note>
  <note name = "network-ipv4">
    Shows details of the phone network configuration
  </note>
  <note name = "network-ipv6">
    Shows details of the phone network configuration
  </note>
  <note name = "network-common">
    Shows details of the phone network configuration
  </note>
      <note name = "AccountStatus">
      According to current state of each account
  </note>
  <note name = "Ext">
    Shows software version and hardware version details of the Expansion LCD Modules
  </note>
</status>
```

Note

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

The total file sizes of the custom language files must be within 100k (for SIP-T28P/T26P/T22P/T20P).

Procedure

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

Configuration File	<y0000000000xx>.cfg	Specify the access URL of the phone user interface language pack. **Parameter:** gui_lang.url Specify the access URL of the note language pack of the web user interface **Parameter:**

		wui_lang.url Specify the access URL of the note language pack of the web user interface **Parameter:** wui_lang_note.url Delete customized language packs of the phone user interface **Parameter:** gui_lang.delete Delete customized language packs and note language packs of the web user interface. **Parameter:** wui_lang.delete

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
gui_lang.url	URL within 511 characters	Blank

Description:

Configures the access URL of the language pack for the phone user interface.

Example:

The following example uses HTTP to download the language pack "000.GUI.English.lang" from the provisioning server 192.168.10.25 to the phone user interface.

gui_lang.url = http://192.168.10.25/000.GUI.English.lang

If you want to download multiple language packs to the phone simultaneously, you can configure as following:

gui_lang.url = http://192.168.10.25/000.GUI.English.lang

gui_lang.url = http://192.168.10.25/008.GUI.Russian.lang

Note: If you change this parameter, the IP phone will reboot to make the change take effect.

Web User Interface:

None

Phone User Interface:

Parameter	Permitted Values	Default
None		
gui_lang.delete	**http://localhost/all or http://localhost/*X.GUI.name.lang***	**Blank**
Description: Deletes the specified or all customized language packs of the phone user interface. **Example:** Delete all customized language packs of the phone user interface. gui_lang.delete = http://localhost/all Delete a customized language pack of the phone user interface (e.g., 008.GUI.Russian.lang) gui_lang.delete = http://localhost/008.GUI.Russian.lang **Note**: If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** None **Phone User Interface:** None		
wui_lang.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the language pack for the web user interface. **Example:** The following example uses HTTP to download the language pack "1.English.js" from the provisioning server 192.168.10.25 to the web user interface. wui_lang.url = http://192.168.10.25/1.English.js 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://192.168.10.25/11.Russian.js **Note**: If you change this parameter, the IP phone will reboot to make the change take effect. It is only applicable to IP phones running firmware version 73 or later. **Web User Interface:** None **Phone User Interface:**		

Parameter	Permitted Values	Default
None		
wui_lang_note.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the language pack for web note. **Example:** The following example uses HTTP to download the language pack "1.English_note.xml" from the provisioning server 192.168.10.25 to the web user interface. wui_lang_note.url = http://192.168.10.25/1.English_note.xml If you want to download multiple language packs to the phone simultaneously, you can configure as following: wui_lang.url = http://192.168.10.25/1.English_note.xml wui_lang.url = http://192.168.10.25/11.Russian_note.xml **Note**: If you change this parameter, the IP phone will reboot to make the change take effect. It is only applicable to IP phones running firmware version 73 or later. **Web User Interface:** None **Phone User Interface:** None		
wui_lang.delete	**http://localhost/all or http://localhost/*Y.name.js***	**Blank**
Description: Delete all customized language packs and note language packs of the web user interface. **Example:** Delete all customized language packs: wui_lang.delete = http://localhost/all Delete a customized language pack (e.g., 11.Russian.js) of the web user interface. wui_lang.delete = http://localhost/11.Russian.js The corresponding note language pack (e.g., 11.Russian_note.xml) will also be		

Parameter	Permitted Values	Default
deleted. **Note**: If you change this parameter, the IP phone will reboot to make the change take effect. It is only applicable to IP phones running firmware version 73 or later. **Web User Interface:** None **Phone User Interface:** None		

Specifying the Language to Use

The default language used on the phone user interface is English. You can specify the languages for the phone user interface and web user interface respectively.

Procedure

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

Configuration File	<y0000000000xx>.cfg	Specify the languages for the phone user interface and the web user interface. **Parameters:** lang.gui lang.wui
Local	Web User Interface	Specify the language for the web user interface. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-preference&q=load
	Phone User Interface	Specify the language for the phone user interface.

Details of Configuration Parameters:

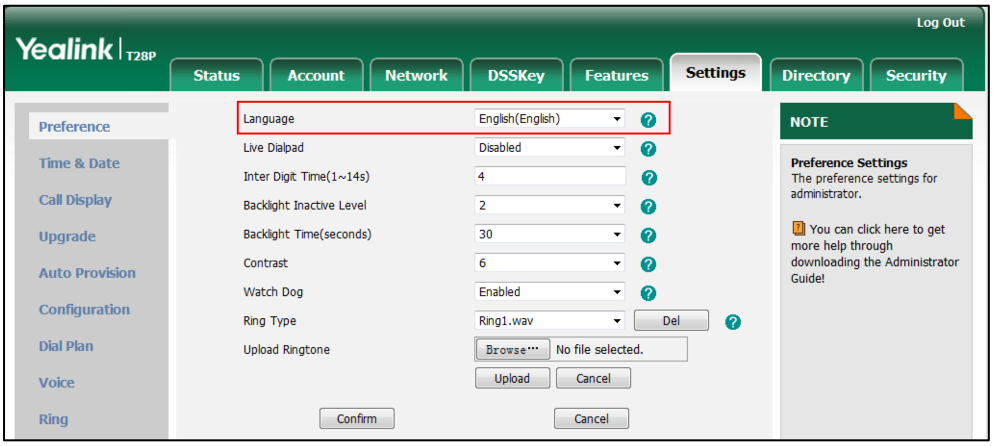
Parameters	Permitted Values	Default
lang.gui	Refer to the following content	English
Description:		

Parameters	Permitted Values	Default
Configures the language used on the phone user interface. **Permitted Values**: English, Chinese_S, Chinese_T, French, German, Italian, Portuguese, Polish, Spanish, Turkish, Russian or the custom language name. **Example:** lang.gui = English **Web User Interface:** None **Phone User Interface:** Menu->Settings->Basic Settings->Language		
lang.wui	**Refer to the following content**	**Blank**
Description: Configures the language used on the web user interface. **Permitted Values**: English, Chinese_S, Chinese_T, French, German, Italian, Polish, Spanish, Turkish, Russian, Portuguese or the custom language name. **Example:** lang.wui = English **Web User Interface:** Settings->Preference->Language **Phone User Interface:** None		

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

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

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



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

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

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

Input Method Customization

Input method customization allows users to customize the existing input method on IP phones. You can first customize the Yealink-supplied input method file “ime.txt”, and then download it to the IP phone. IP phones support 5 input methods: 2aB, abc, Abc, 123, ABC.

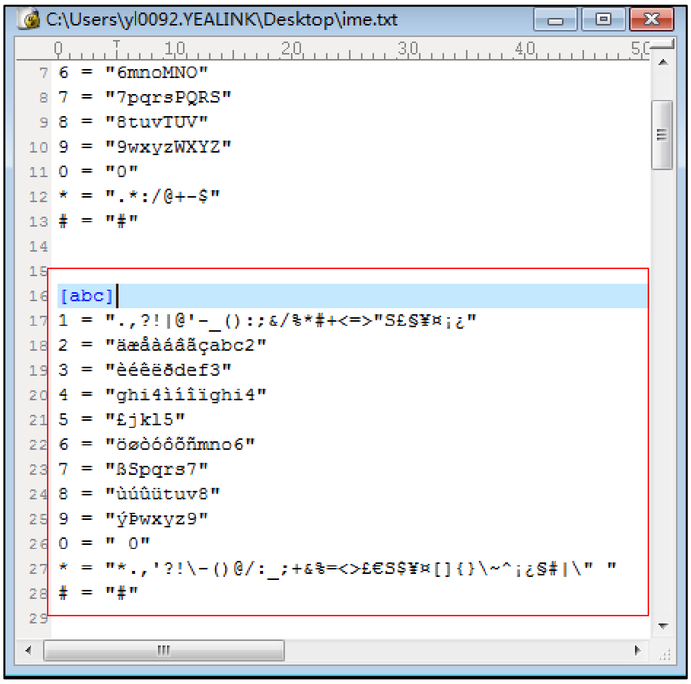
The following shows a portion of the input method file "ime.txt":

C:\Users\yl0092.YEALINK\Desktop\ime.txt

```
[2aB]
1 = "1"
2 = "2abcABC"
3 = "3defDEF"
4 = "4ghiGHI"
5 = "5jklJKL"
6 = "6mnoMNO"
7 = "7pqrsPQRS"
8 = "8tuvTUV"
9 = "9wxyzWXYZ"
0 = "0"
* = ".*:/@+-$"
# = "#"


[abc]
1 = ""
2 = "abc"
3 = "def"
4 = "ghi"
5 = "jkl"
6 = "mno"
7 = "pqrs"
8 = "tuv"
9 = "wxyz"
0 = " "
* = ".*:/@+-$"
# = "#"
```

You can add new characters or adjust the character order of the existing input method. The following show an example of adding the Russian characters for the input method “abc”.



Note

> When adding new characters for the existing input method, ensure that the added characters are supported by IP phones.
>
> The IP phones can only recognize the input method files uploaded using Unicode encoding.
>
> Do not rename the input mode filename.

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

Procedure

Specify the access URL of the custom input method file and the default input methods using the configuration files.

Configuration File	<y0000000000xx>.cfg	Specify the access URL of the custom input method file. **Parameter:** gui_input_method.url Specify the default input method when editing contacts. **Parameter:** directory.edit_default_input_method

		Specify the default input method when searching for contacts. **Parameter:** directory.search_default_input_method

Details of Configuration Parameters:

Parameters	Permitted Values	Default
gui_input_method.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the custom input method file. **Example:** The following example uses HTTP to download the custom input method file (ime.txt) from the provisioning server 192.168.10.25. gui_input_method.url = http://192.168.10.25/ime.txt **Web User Interface:** None **Phone User Interface:** None		
directory.edit_default_input_method	**Abc, 2aB, 123, abc or ABC**	**Abc**
Description: Specify the default input method when editing contacts. **Example:** directory.edit_default_input_method = abc **Web User Interface:** None **Phone User Interface:** None		
directory.search_default_input_method	**Abc, 2aB, 123, abc or ABC**	**Abc**
Description: Specify the default input method when searching for contacts. **Example:** directory.search_default_input_method = abc		

Parameters	Permitted Values	Default
Web User Interface: None **Phone User Interface:** None		

Logo Customization

Logo customization allows unifying the IP phone appearance or displaying a custom image on the idle screen such as a company logo, instead of the default system logo. SIP-T20P IP phones only support a text logo.

The following table lists the logo file format, resolution and total files size for each phone model.

Phone Model	Logo File Format	Resolution	Total Files Size
SIP-T28P	.dob	<=236*82 2 gray scale	<=100KB
SIP-T26P/T22P	.dob	<=132*64 2 gray scale	<=100KB

Note

Before uploading your custom logo to IP phones, ensure your logo file is correctly formatted. For more information on customizing a logo file, refer to *Yealink_SIP-T2_Series_T4_Series_IP_Phones_Auto_Provisioning_Guide*, available online: http://www.yealink.com/DocumentDownload.aspx?CateId=142&flag=142.

Procedure

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

Configuration File	<y0000000000xx>.cfg	Configure the logo shown on the idle screen and specify the access URL of the custom logo file. **Parameters:** phone_setting.lcd_logo.mode lcd_logo.url phone_setting.lcd_logo.text
Local	Web User Interface	Configure the logo shown on the idle screen. **Navigate to:** http://<phoneIPAddress>/servlet

		?p=features-general&q=load

Details of Configuration Parameters:

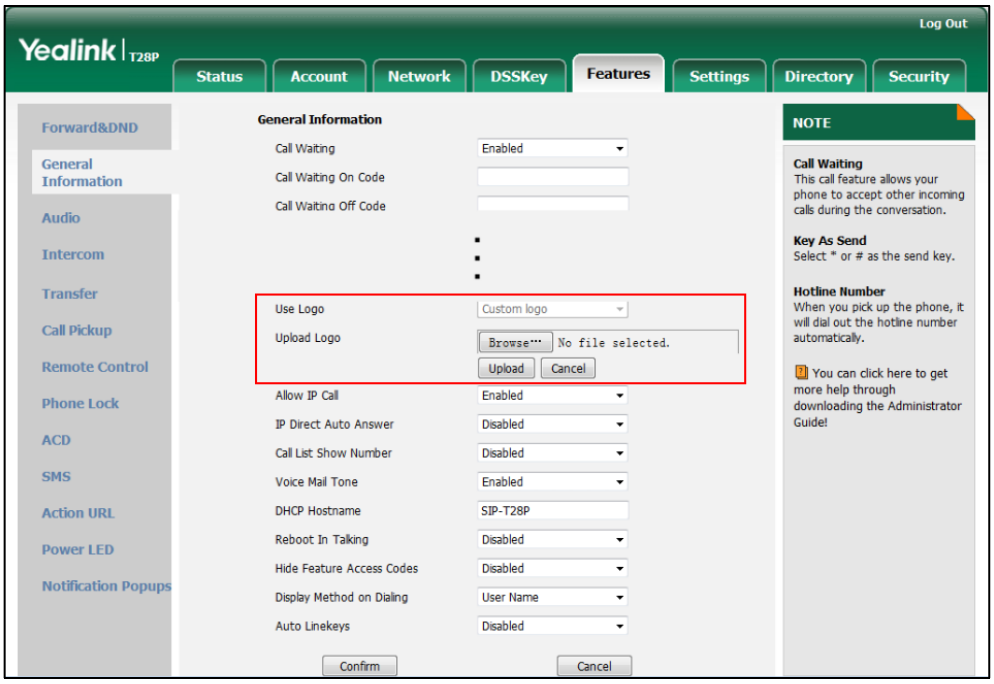
Parameters	Permitted Values	Default
phone_setting.lcd_logo.mode	0, 1 or 2	Refer to the following content
Description: Configures the logo mode of the LCD screen. **0**-Disabled **1**-System logo **2**-Custom logo If it is set to 0 (Disabled), the IP phone is not allowed to display a logo. If it is set to 1 (System logo), the LCD screen will display the system logo. If it is set to 2 (Custom logo), the LCD screen will display the custom logo (you need to upload a custom logo file to the IP phone). **Default Value:** For SIP-T26P/T22P/T20P IP phones, the default value is 0. For SIP-T28P IP phones, the default value is 1. **Note**: For SIP-T28P IP phones, valid values are 1(System logo) and 2(Custom logo). For SIP-T20P IP phones, valid values are 0(Disabled) and 1(Enabled). **For SIP-T20P IP phones:** Enables or disables a text logo. If it is set to 0 (Disabled), the IP phone is not allowed to display a text logo. If it is set to 1 (Enabled), the LCD screen will display the custom text logo. **Web User Interface:** Features->General Information->Use Logo **Phone User Interface:** None		
lcd_logo.url	URL within 511 characters	Blank

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td colspan="3">Description:
Configures the access URL of the custom logo file.
Example:
The following example uses HTTP to download the custom logo file (logo.dob) from the provisioning server 192.168.10.25.
lcd_logo.url = http://192.168.10.25/logo.dob
Note: It is not applicable to SIP-T20P IP phones.
Web User Interface:
Features->General Information->Upload Logo
Phone User Interface:
None</td></tr>
<tr><td>phone_setting.lcd_logo.text</td><td>String within 15 characters</td><td>Yealink</td></tr>
<tr><td colspan="3">Description:
Configures a text logo.
Example:
phone_setting.lcd_logo.text = Yealink
Note: It is only applicable to SIP-T20P IP phones.
Web User Interface:
Features->General Information->Text Logo
Phone User Interface:
None</td></tr>
</table>

To configure an image logo via web user interface (not applicable to SIP-T20P IP phones):

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

2. Select **Custom logo** from the pull-down list of **Use Logo**.



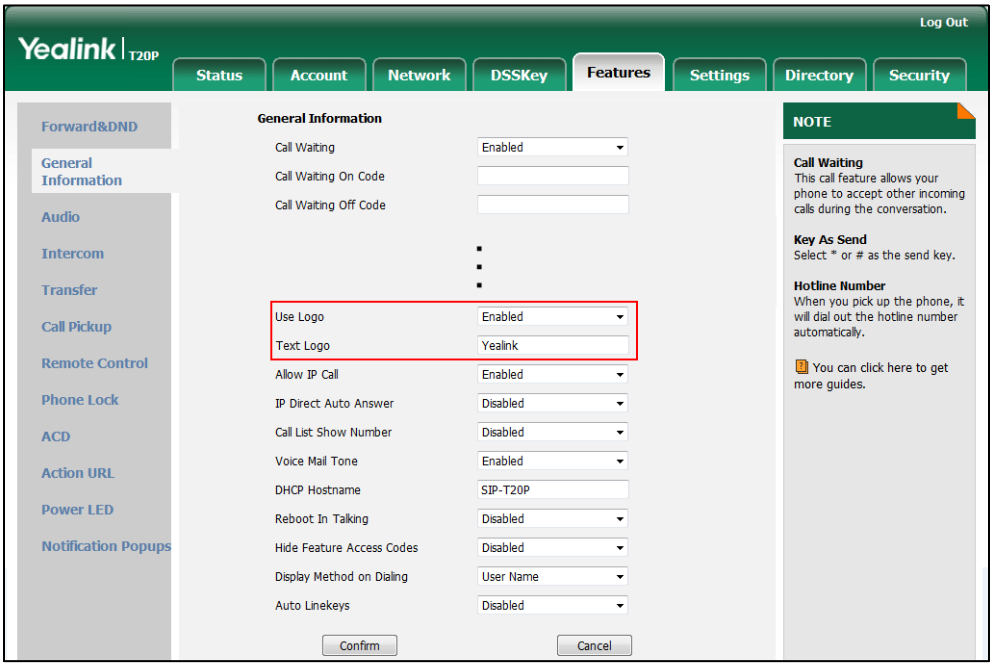
3. Click **Browse** to select the logo file from your local system.
4. Click **Upload** to upload the file.
5. Click **Confirm** to accept the change.

   For SIP-T28P IP phones, the image logo is displayed on the idle screen. For SIP-T26P/T22P IP phones, the image logo screen and the idle screen are displayed alternately.

To configure a text logo via web user interface (only applicable to SIP-T20P IP phones):

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

3. Enter the desired text (0~15 characters) in the **Text Logo** field.



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

   The registered account and the configured text logo are displayed alternately.

Softkey Layout

Softkey layout is used to customize the soft keys at the bottom of the LCD screen to best meet users' requirements. In addition to specifying which soft keys to display, you can determine their display order. It can be configured based on call states. Softkey layout is not applicable to SIP-T20P IP phones.

You can configure the softkey layout using the softkey layout templates for different call states. For more information on how to configure a softkey layout template, refer to Softkey Layout Template on page 480.

The following table lists soft keys available for IP phones in different call states.

Call State	Default Soft Keys	Optional Soft Keys
CallFailed	NewCall Empty Empty Empty	Empty Switch Cancel
CallIn	Answer Forward Silence Reject	Empty Switch

Call State		Default Soft Keys	Optional Soft Keys
Connecting	Connecting	Empty Empty Empty Cancel	Empty Switch
	SemiAttendTrans	Transfer Empty Empty Cancel	Empty Switch
Dialing		Send IME Delete Cancel	Empty History Switch Line Directory GPickup DPickup Retrieve
RingBack	RingBack	Empty Empty Empty Cancel	Empty Switch CC
	SemiAttendTransBack	Transfer Empty Empty Cancel	Empty Switch CC
Talking	Talk	Transfer Hold Conference Cancel	Empty Mute SWAP NewCall Switch Answer Reject PriHold Park GPark
	Hold	Transfer	Empty

<table>
<tr><th colspan="2">Call State</th><th>Default Soft Keys</th><th>Optional Soft Keys</th></tr>
<tr><td rowspan="4"></td><td></td><td>Resume
NewCall
Cancel</td><td>Switch
Answer
Reject</td></tr>
<tr><td>Held</td><td>Empty
Empty
Empty
Cancel</td><td>Empty
Switch
Answer
Reject
NewCall</td></tr>
<tr><td>PreTrans</td><td>Transfer
IME
Delete
Cancel</td><td>Empty
Directory
Switch
Send</td></tr>
<tr><td>Conferenced</td><td>Empty
Hold
Split
Cancel</td><td>Empty
Switch
Answer
Reject
Mute</td></tr>
</table>

Procedure

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

Configuration File	<y0000000000xx>.cfg	Specify the access URL of the softkey layout template. **Parameters:** phone_setting.custom_softkey_enable custom_softkey_call_failed.url custom_softkey_call_in.url custom_softkey_connecting.url custom_softkey_dialing.url custom_softkey_ring_back.url custom_softkey_talking.url
Local	Web User Interface	Configure the softkey layout. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-softkey&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
phone_setting.custom_softkey_enable	**0 or 1**	**0**
Description: Enables or disables custom soft keys layout feature. **0**-Disabled **1**-Enabled **Web User Interface:** Settings->Softkey Layout->Custom Softkey **Phone User Interface:** None		
custom_softkey_call_failed.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the custom file for the soft key presented on the LCD screen when in the Call Failed state. **Example:** The following example uses HTTP to download the CallFailed state file from the "XMLfiles" directory on provisioning server 10.2.8.16 using 8080 port. custom_softkey_call_failed.url = http://10.2.8.16:8080/XMLfiles/CallFailed.xml **Web User Interface:** None **Phone User Interface:** None		
custom_softkey_call_in.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the custom file for the soft key presented on the LCD screen when in the Call In state. **Example:** The following example uses HTTP to download the CallIn state file from the "XMLfiles" directory on provisioning server 10.2.8.16 using 8080 port. custom_softkey_call_in.url = http://10.2.8.16:8080/XMLfiles/CallIn.xml **Web User Interface:** None		

Parameters	Permitted Values	Default
Phone User Interface: None		
custom_softkey_connecting.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the custom file for the soft key presented on the LCD screen when in the Connecting state. **Example:** The following example uses HTTP to download the Connecting state file from the "XMLfiles" directory on provisioning server 10.2.8.16 using 8080 port. custom_softkey_connecting.url = http://10.2.8.16:8080/XMLfiles/Connecting.xml **Web User Interface:** None **Phone User Interface:** None		
custom_softkey_dialing.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the custom file for the soft key presented on the LCD screen when in the Dialing state. **Example:** The following example uses HTTP to download the Dialing state file from the "XMLfiles" directory on provisioning server 10.2.8.16 using 8080 port. custom_softkey_dialing.url = http://10.2.8.16:8080/XMLfiles/Dialing.xml **Web User Interface:** None **Phone User Interface:** None		
custom_softkey_ring_back.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the custom file for the soft key presented on the LCD screen when in the RingBack state. **Example:** The following example uses HTTP to download the RingBack state file from the		

Parameters	Permitted Values	Default
"XMLfiles" directory on provisioning server 10.2.8.16 using 8080 port. custom_softkey_ring_back.url = http://10.2.8.16:8080/XMLfiles/RingBack.xml **Web User Interface:** None **Phone User Interface:** None		
custom_softkey_talking.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the custom file for the soft key presented on the LCD screen when in the Talking state. **Example:** The following example uses HTTP to download the Talking state file from the "XMLfiles" directory on provisioning server 10.2.8.16 using 8080 port. custom_softkey_talking.url = http://10.2.8.16:8080/XMLfiles/Talking.xml **Web User Interface:** None **Phone User Interface:** None		

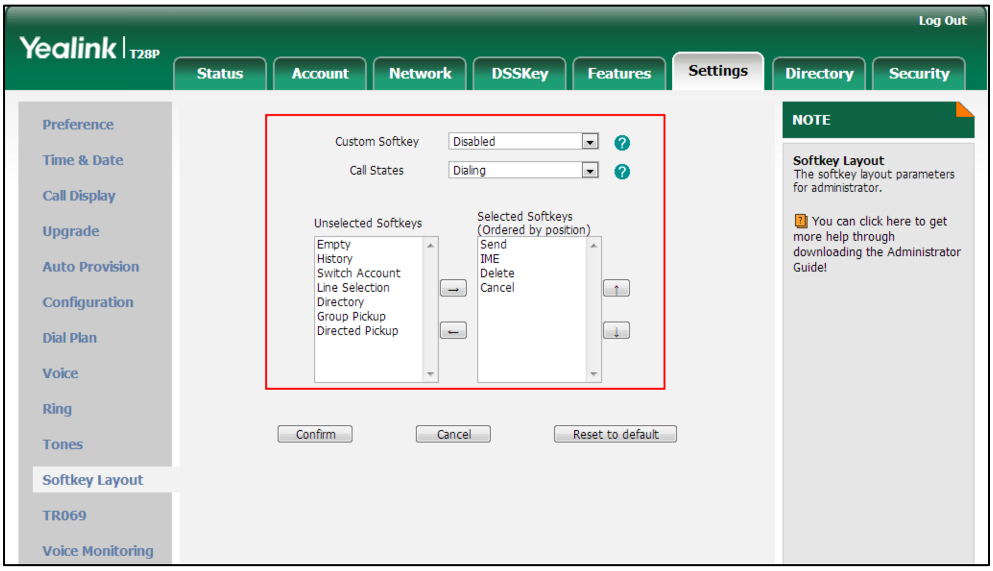
To configure softkey layout via web user interface:

1. Click on **Settings**->**Softkey Layout**.
2. Select the desired value from the pull-down list of **Custom Softkey**.
3. Select the desired state from the pull-down list of **Call States**.
4. Select the desired soft key from the **Unselected Softkeys** column and then click → .

   The selected soft key appears in the **Selected Softkeys** column. If more than four soft keys are selected, a **More** soft key will appear on the LCD screen, and the selected soft keys are displayed in two pages.
5. Repeat the step 4 to add more soft keys to the **Selected Softkeys** column.
6. To remove the soft key from the **Selected Softkeys** column, select the desired soft key and then click ← .

7. To adjust the display order of soft keys, select the desired soft key and then click ↑ or ↓.

   The LCD screen displays the soft keys in the adjusted order.



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

Key as Send

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

Procedure

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

Configuration File	<y0000000000xx>.cfg	Configure a send key. **Parameter:** features.key_as_send Configure a send sound. **Parameter:** features.send_key_tone Configure a key tone. **Parameter:** features.key_tone
Local	Web User Interface	Configure a send key. **Navigate to:** http://<phoneIPAddress>/servlet

		?p=features-general&q=load Configure a send sound and key tone. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-audio&q=load
	Phone User Interface	Configure the send key. Configure a key tone.

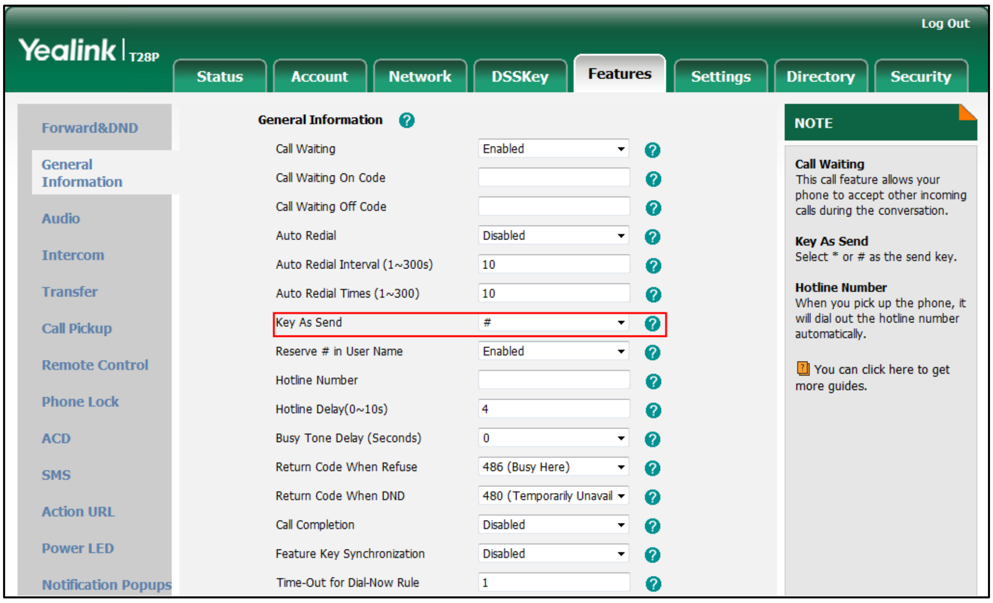
Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.key_as_send	**0, 1 or 2**	**1**
Description: Configures the "#" or "*" key as the send key. **0**-Disabled **1**-# key **2**-* key If it is set to 0 (Disabled), neither "#" nor "*" can be used as a send key. If it is set to 1 (# key), the pound key is used as the send key. If it is set to 2 (* key), the asterisk key is used as the send key. **Note**: The old parameter "features.pound_key.mode" is also applicable to IP phones. **Web User Interface:** Features->General Information->Key As Send **Phone User Interface:** Menu->Features->Key as Send		
features.key_tone	**0 or 1**	**1**
Description: Enables or disables the IP phone to play a tone when a user presses a key on your phone keypad. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the IP phone will play a tone when a user presses a key on your phone keypad. **Web User Interface:**		

Parameters	Permitted Values	Default
Features->Audio->Key Tone **Phone User Interface:** Menu->Settings->Basic Settings->Sound->Key Tone		
features.send_key_tone	**0 or 1**	**1**
Description: Enables or disables the IP phone to play a tone when a user presses a send key. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the IP phone will play a tone when a user presses a send key. **Note**: It works only if the parameter "features.key_tone" is set to 1 (Enabled). **Web User Interface:** Features->Audio->Send Sound **Phone User Interface:** None		

To configure a send key via web user interface:

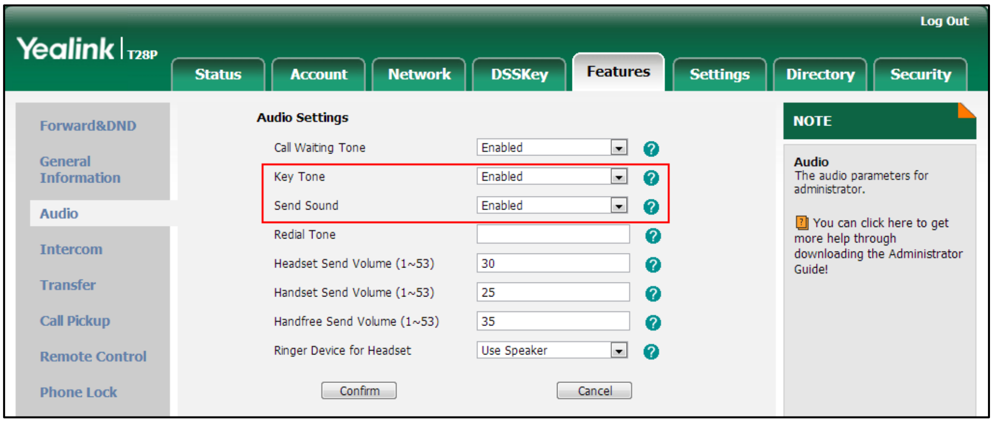
1. Click on **Features**->**General Information**.
2. Select the desired value from the pull-down list of **Key As Send**.



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

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

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



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

To configure a send key via phone user interface:

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

To configure a key tone via web user interface:

1. Press **Menu**->**Settings**->**Basic Settings**->**Sound**->**Key Tone**.
2. Press ◀ or ▶ , or the **Switch** soft key to select the desired type from the **Key Tone** field.
3. Press the **Save** soft key to accept the change.

Dial Plan

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

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

- Replace Rule

- Dial-now
- Area Code
- Block Out

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

.	The dot "." can be used as a placeholder or multiple placeholders for any string. Example: "12." would match "123", "1234", "12345", "12abc", etc.
x	The "x" can be used as a placeholder for any character. Example: "12x" would match "121", "122", "123", "12a", etc.
-	The dash "-" can be used to match a range of characters within the brackets. Example: "[5-7]" would match the number "5", "6" or "7".
,	The comma "," can be used as a separator within the bracket. Example: "[2,5,8]" would match the number "2", "5" or "8".
[]	The square bracket "[]" can be used as a placeholder for a single character which matches any of a set of characters. Example: "91[5-7]1234"would match "9151234", "9161234", "9171234".
()	The parenthesis "( )" can be used to group together patterns, for instance, to logically combine two or more patterns. Example: "([1-9])([2-7])3" would match "923", "153", "673", etc.
$	The "$" followed by the sequence number of a parenthesis means the characters placed in the parenthesis. The sequence number stands for the corresponding parenthesis. Example: A replace rule configuration, Prefix: "001(xxx)45(xx)", Replace: "9001$145$2". When you dial out "0012354599" on your phone, the IP phone will replace the number with "90012354599". "$1" means 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. IP phones support up to 100 replace rules, which can be created either one by one or in batch using a replace rule template. For more information on how to customize a replace rule template, refer to Replace Rule Template on page 478.

Procedure

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

Configuration File	<y0000000000xx>.cfg	Create the replace rule for the IP phone. **Parameters:** dialplan.replace.prefix.X dialplan.replace.replace.X dialplan.replace.line_id.X Configure the access URL of the replace rule template. **Parameter:** dialplan_replace_rule.url
Local	Web User Interface	Create the replace rule for the IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-dialplan&q=load

Details of Configuration Parameters:

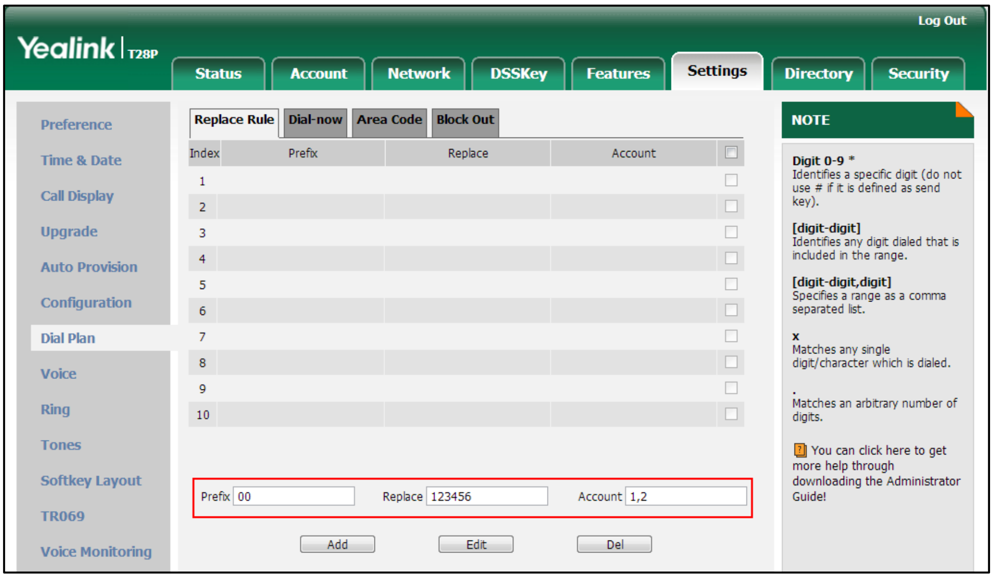
Parameters	Permitted Values	Default
dialplan.replace.prefix.X (X ranges from 1 to 100)	**String within 32 characters**	**Blank**
Description: Configures the entered number to be replaced. **Example:** dialplan.replace.prefix.1 = 00 **Web User Interface:** Settings->Dial Plan->Replace Rule->Prefix **Phone User Interface:** None		
dialplan.replace.replace.X (X ranges from 1 to 100)	**String within 32 characters**	**Blank**

Parameters	Permitted Values	Default
Description: Configures the alternate number to replace the entered number. **Example:** dialplan.replace.replace.1 = 123456 **Web User Interface:** Settings->Dial Plan->Replace Rule->Replace **Phone User Interface:** None		
dialplan.replace.line_id.X (X ranges from 1 to 100)	**Refer to the following content**	**Blank (for all lines)**
Description: 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 phone. **Permitted Values**: 0 to 6 (for SIP-T28P) 0 to 3 (for SIP-T26P/T22P) 0 to 2 (for SIP-T20P) **Example:** dialplan.replace.line_id.1 = 1,2 **Note:** Multiple line IDs are separated by commas. **Web User Interface:** Settings->Dial Plan->Replace Rule->Account **Phone User Interface:** None		
dialplan_replace_rule.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the replace rule template file. **Example:** dialplan_replace_rule.url = http://192.168.10.25/dialplan.xml **Web User Interface:** None **Phone User Interface:** None		

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 phone.



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

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 phone will automatically dial out the numbers without pressing the send key. IP phones support up to 100 dial-now rules, which can be created either one by one or in batch using a dial-now rule template. For more information on how to customize a dial-now template, refer to Dial-now Template on page 479.

Delay Time for Dial-now Rule

The IP 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.

Configuration File	<y0000000000xx>.cfg	Create the dial-now rule for the IP phone. **Parameters:** dialplan.dialnow.rule.X dialplan.dialnow.line_id.X Configure the delay time for the dial-now rule and the access URL of the dial-now template. **Parameters:** phone_setting.dialnow_delay dialplan_dialnow.url
Local	Web User Interface	Create the dial-now rule for the IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-dialnow&q=load Configure the delay time for the dial-now rule. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
dialplan.dialnow.rule.X (X ranges from 1 to 100)	**String within 511 characters**	**Blank**
Description: 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 phone will automatically dial out the numbers without pressing the send key. **Example:** dialplan.dialnow.rule.1 = 1234 **Web User Interface:**		

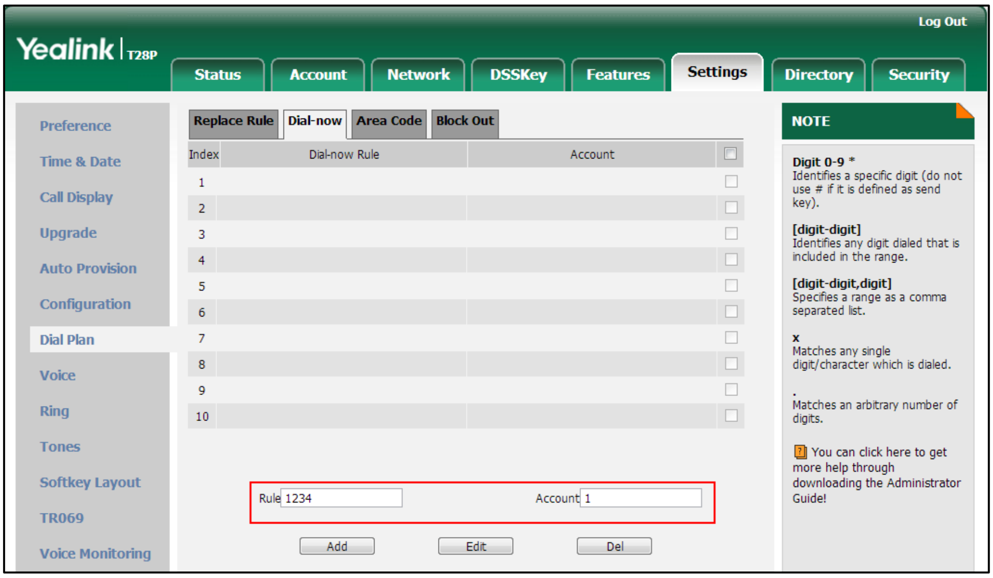
Parameters	Permitted Values	Default
Settings->Dial Plan->Dial-now->Rule **Phone User Interface:** None		
dialplan.dialnow.line_id.X (X ranges from 1 to 100)	**Refer to the following content**	**Blank (for all lines)**
Description: Configures the desired line to apply the dial-now rule. The digit 0 stands for all lines. If it is left blank, the dial-now rule will apply to all lines on the IP phone. **Permitted Values:** 0 to 6 (for SIP-T28P) 0 to 3 (for SIP-T26P/T22P) 0 to 2 (for SIP-T20P) **Example:** dialplan.dialnow.line_id.1 = 1 **Note:** Multiple line IDs are separated by commas. **Web User Interface:** Settings->Dial Plan->Dial-now->Account **Phone User Interface:** None		
phone_setting.dialnow_delay	**Integer from 1 to 14**	**1**
Description: Configures the delay time (in seconds) for the dial-now rule. When entered numbers match the predefined dial-now rule, the IP phone will automatically dial out the entered number after the specified delay time. **Web User Interface:** Features->General Information->Time-Out for Dial-Now Rule **Phone User Interface:** None		
dialplan_dialnow.url	**URL within 511 characters**	**Blank**

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td colspan="3">Description:
Configures the access URL of the dial-now rule template file.
Example:
dialplan_dialnow.url = http://192.168.10.25/dialnow.xml
Web User Interface:
None
Phone User Interface:
None</td></tr>
</table>

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 phone.

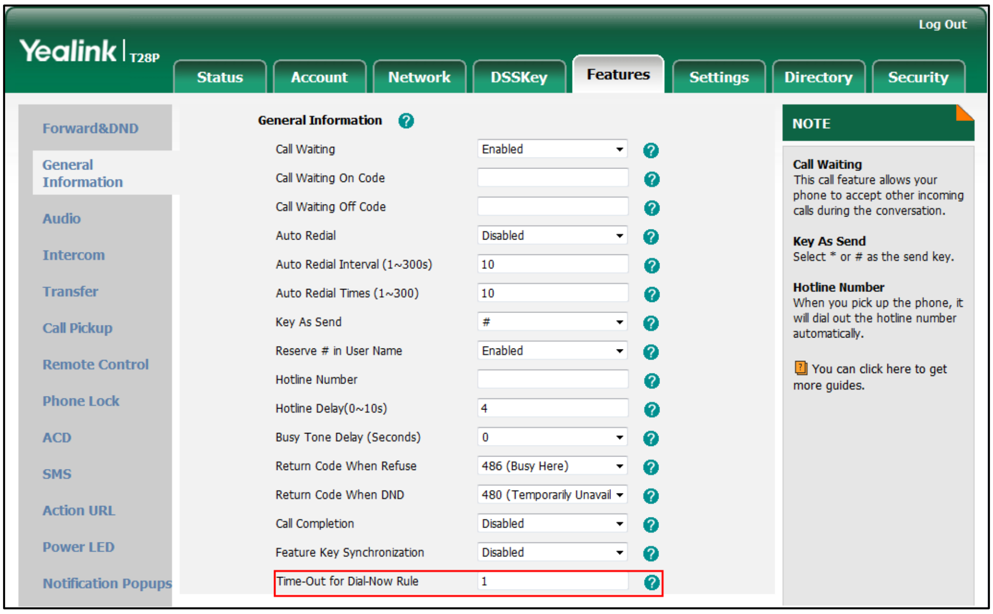


4. Click **Add** to add the dial-now rule.

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



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

Area Code

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

Procedure

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

Configuration File	<y0000000000xx>.cfg	Create the area code rule and specify the maximum and minimum lengths of entered numbers. **Parameters:** dialplan.area_code.code dialplan.area_code.min_len dialplan.area_code.max_len dialplan.area_code.line_id
Local	Web User Interface	Create the area code rule and specify the maximum and minimum lengths of entered

		numbers. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-areacode&q=load

Details of Configuration Parameters:

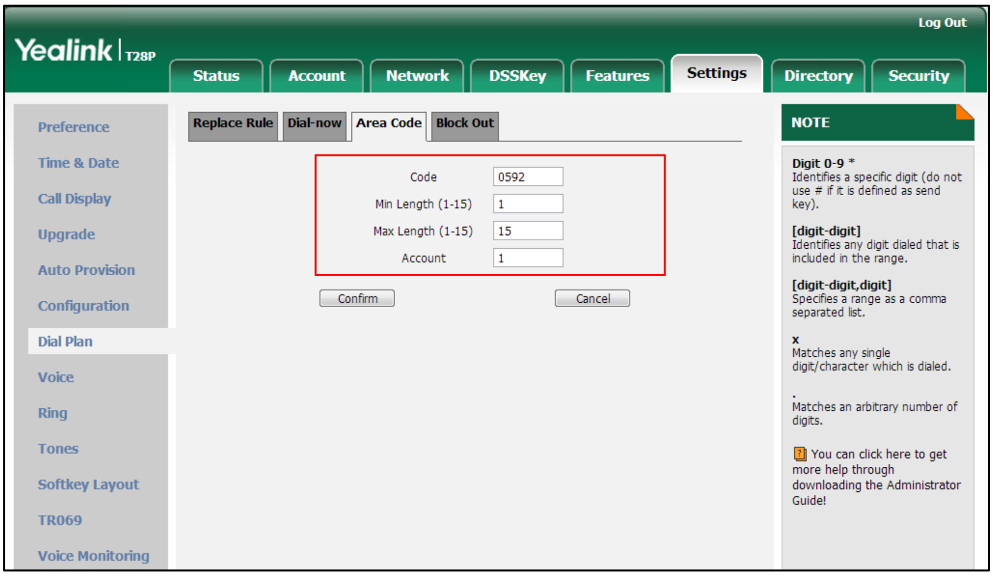
Parameters	Permitted Values	Default
dialplan.area_code.code	**String within 16 characters**	**Blank**
Description: Configures the area code to be added before the entered numbers when dialing out. **Note**: The length of the entered number must be between the minimum length configured by the parameter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

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td colspan="3">Phone User Interface:
None</td></tr>
<tr><td>dialplan.area_code.line_id</td><td>Refer to the following content</td><td>Blank (for all lines)</td></tr>
<tr><td colspan="3">Description:
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 phone.
Permitted Values:
0 to 6 (for SIP-T28P)
0 to 3 (for SIP-T26P/T22P)
0 to 2 (for SIP-T20P)
Example:
dialplan.area_code.line_id = 1
Note: Multiple line IDs are separated by commas.
Web User Interface:
Settings->Dial Plan->Area Code->Account
Phone User Interface:
None</td></tr>
</table>

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 phone.



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

Block Out

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

Procedure

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

Configuration File	<y0000000000xx>.cfg	Create the block out rule for the IP phone. **Parameters:** dialplan.block_out.number.X dialplan.block_out.line_id.X
Local	Web User Interface	Create the block out rule for the desired line. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-blackout&q=load

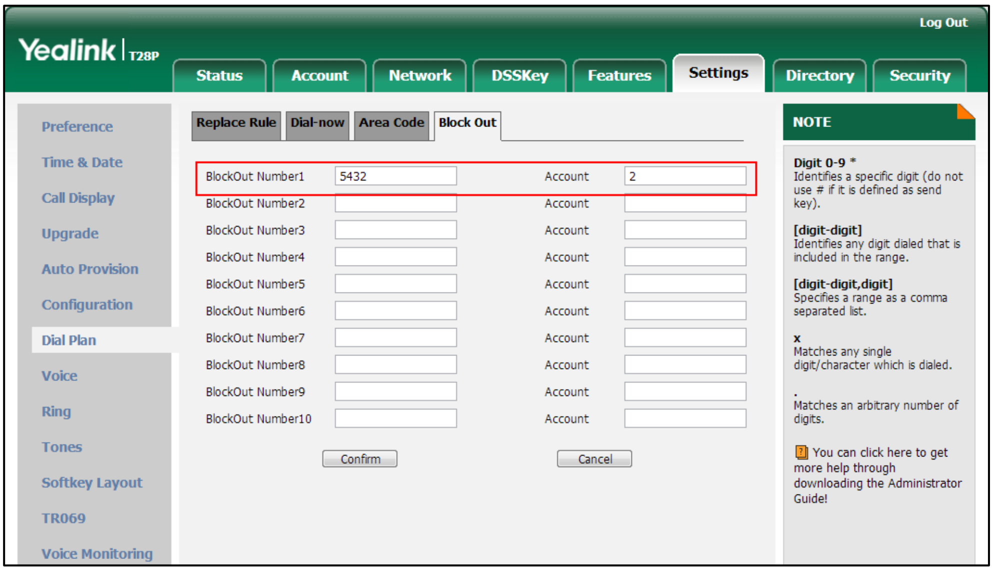
Details of Configuration Parameters:

Parameters	Permitted Values	Default
dialplan.block_out.number.X (X ranges from 1 to 10)	**String within 32 characters**	**Blank**
Description: Configures the block out numbers. **Example:** dialplan.block_out.number.1 = 5432 **Web User Interface:** Settings->Dial Plan->Block Out->BlockOut NumberX **Phone User Interface:** None		
dialplan.block_out.line_id.X (X ranges from 1 to 10)	**Refer to the following content**	**Blank (for all lines)**
Description: 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 phone. **Permitted Values:** 0 to 6 (for SIP-T28P) 0 to 3 (for SIP-T26P/T22P) 0 to 2 (for SIP-T20P) **Example:** dialplan.block_out.line_id.1 = 2 **Note**: Multiple line IDs are separated by commas. **Web User Interface:** Settings->Dial Plan->Block Out->Account **Phone User Interface:** 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 Number** 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 phone.



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

Hotline

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

Procedure

Hotline can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure the hotline number. **Parameter:** features.hotline_number Specify the time (in seconds) the IP phone waits before automatically dialing out the hotline number. **Parameter:** features.hotline_delay
Local	Web User Interface	Configure the hotline number. Specify the time (in seconds) the IP phone waits before automatically dial out the hotline

		number. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load
	Phone User Interface	Configure the hotline number. Specify the time (in seconds) the IP phone waits before automatically dialing out the hotline number.

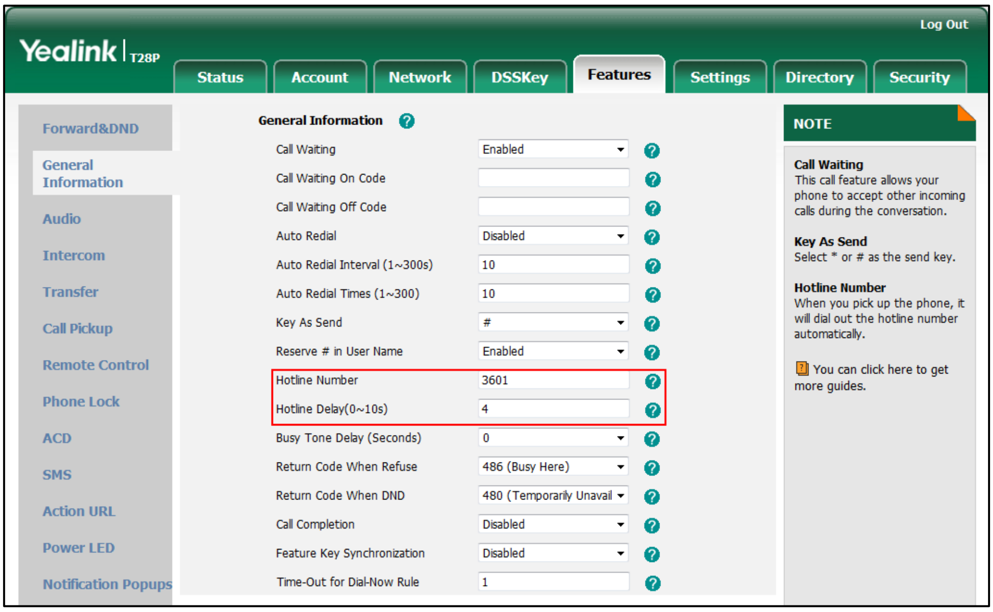
Details of Configuration Parameters:

Parameter	Permitted Values	Default
features.hotline_number	**String within 32 characters**	**Blank**
Description: Configures the hotline number that the IP phone automatically dials out when lifting the handset, pressing the speakerphone key or the line key. Leaving it blank disables hotline feature. **Example:** features.hotline_number = 3601 **Web User Interface:** Features->General Information->Hotline Number **Phone User Interface:** Menu->Features->Hotline->Hotline Number		
features.hotline_delay	**Integer from 0 to 10**	**4**
Description: Configures the waiting time (in seconds) for the IP phone to automatically dial out the hotline number. If it is set to 0 (0s), the IP phone will immediately dial out the preconfigured hotline number when you lift the handset, press the speakerphone key or press the line key. If it is set to a value greater than 0, the IP phone will wait the designated seconds before dialing out the predefined hotline number when you lift the handset, press the speakerphone key or press the line key. **Web User Interface:** Features->General Information->Hotline Delay (0~10s) **Phone User Interface:**		

Parameter	Permitted Values	Default
Menu->Features->Hotline->Hotline Delay		

To configure hotline via web user interface:

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



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

To configure hotline via phone user interface:

1. Press **Menu**->**Features**->**Hot Line**.
2. Enter the hotline number in the **Number** field.
3. Enter the waiting time (in seconds) in the **Hotline Delay** field.
4. Press the **Save** soft key to accept the change.

Off Hook Hot Line Dialing

For security reasons, IP phones support off hook hot line dialing feature, which allows the phone to first dial out the pre-configured number when the user presses the speakerphone key or desired line key, dials out a call or off hook the phone 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 phone will use this account to dial out a call successfully.

Off hook hot line dialing feature is configurable on a per-line basis and depends on support from a SIP server.

Note

Off hook hot line dialing feature limits the call-out permission of this account and disables the hotline feature. For example, when the phone goes off hook using the account with this feature enabled, the configured hotline number will not be dialed out automatically.

The server actions may vary from different servers.

This feature is also applicable to the IP call and intercom call.

Procedure

Off hook hot line dialing can be configured using the configuration files.

Configuration File	<y0000000000xx>.cfg	Configure off hook hot line dialing feature. **Parameter:** account.X.auto_dial_enable Specify the number that the phone first dials out. **Parameter:** account.X.auto_dial_num

Details of Configuration Parameters:

Parameter	Permitted Values	Default
account.X.auto_dial_enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to first dial out a pre-configured number when a user presses the speakerphone key or desired line key, dials out a call or off hook the phone using account X. **0**-Disabled **1**-Enabled If it is set to 1(Enabled), the phone will first dial out the pre-configured number (configured by the parameter "account.X.auto_dial_num") when a user presses the speakerphone key or desired line key, dials out a call or off hook the phone using account X. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Note**: It is only applicable to IP phones running firmware version 73 or later.		

Parameter	Permitted Values	Default
Web User Interface: None **Phone User Interface:** None		
account.X.auto_dial_num	String within 32 characters	Blank
Description: Configures the number that the IP phone first dials out when a user presses the speakerphone key or desired line key, dials out a call or off hook the phone using account X. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Note**: It works only if the value of the parameter "account.X.auto_dial_enable" is set to 1 (Enabled). And it is only applicable to IP phones running firmware version 73 or later. **Web User Interface:** None **Phone User Interface:** None		

Directory

Directory provides easy access to frequently used lists. The lists can be Local Directory, History, Remote Phone Book and LDAP. The desired lists can be added to Directory using a directory file. For more information on how to customize a directory file, refer to Directory Template on page 481.

Procedure

Directory can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Specify the access URL of the Directory file. **Parameter:** directory_setting.url
Local	Web User Interface	Configure the Directory. **Navigate to:**

		http://<phoneIPAddress>/servlet ?p=contacts-favorite&q=load

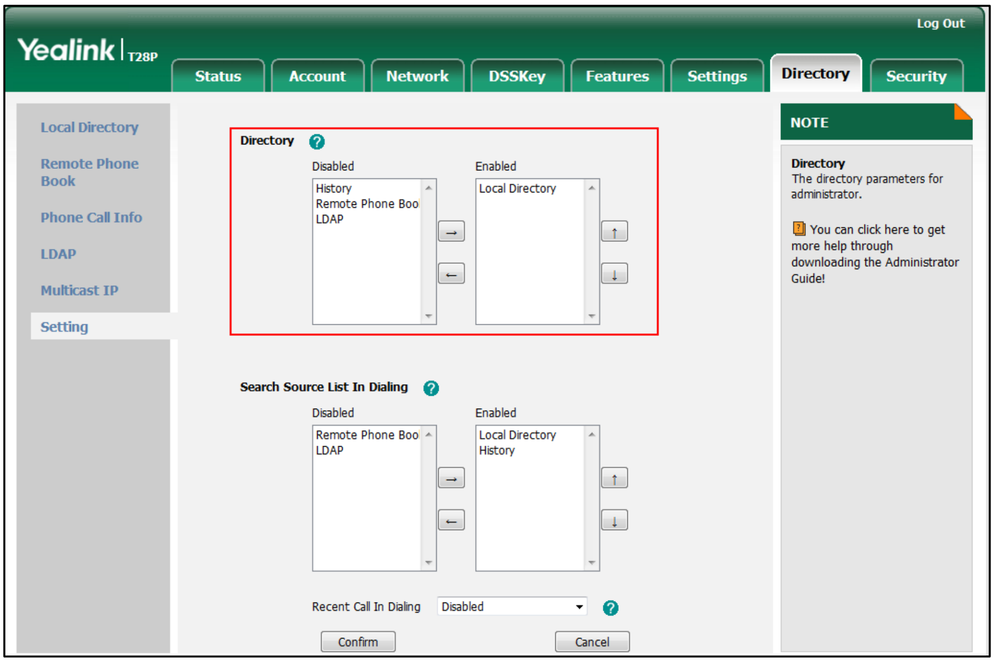
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
directory_setting.url	URL within 511 characters	Blank
Description: Configures the access URL of the directory template. **Example:** directory_setting.url = http://192.168.1.20/favorite_setting.xml **Web User Interface:** Directory->Setting->Directory **Phone User Interface:** None		

To configure the directory via web user interface:

1. Click on **Directory**->**Setting**.
2. In the **Directory** block, select the desired list from the **Disabled** column and then click → .

   The selected list appears in the **Enabled** column.
3. Repeat 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 list, select the desired list and then click ↑ or ↓ .



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

   The IP phone LCD screen will display the enabled list(s) in the adjusted order.

Search Source in Dialing

Search source list in dialing allows the IP phone to automatically search entries from the search source list based on the entered string, and display results on the pre-dialing screen. The search source list can be Local Directory, History, Remote Phone Book and LDAP. The search source list can be configured using a super search file. For more information on how to customize a super search template, refer to Super Search Template on page 482.

Procedure

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

Configuration File	<y0000000000xx>.cfg	Specify the access URL of the super search file. **Parameter:** super_search.url
Local	Web User Interface	Configure the search source list in dialing. **Navigate to:** http://<phoneIPAddress>/servlet?p=contacts-favorite&q=load

Details of the Configuration Parameter:

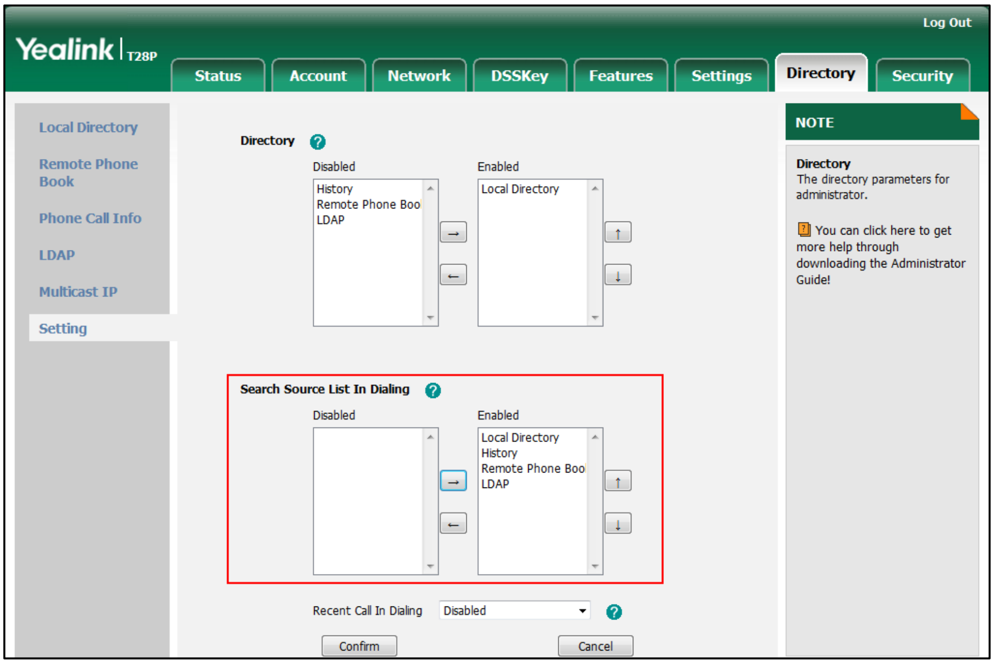
<table>
<tr><th>Parameter</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>super_search.url</td><td>URL within 511 characters</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the access URL of the super search template.
Web User Interface:
Directory->Setting->Search Source List In Dialing
Phone User Interface:
None</td></tr>
</table>

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 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.



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

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.

IP phones maintain a local call log. Call log consists of four lists: Placed Calls, Received Calls, Missed Calls and Forwarded Calls. Call log lists support 100 entries in all. 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.

Configuration File	<y0000000000xx>.cfg	Configure call log feature. **Parameter:** features.save_call_history
Local	Web User Interface	Configure call log feature. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-general&q=load
	Phone User Interface	Configure the call log.

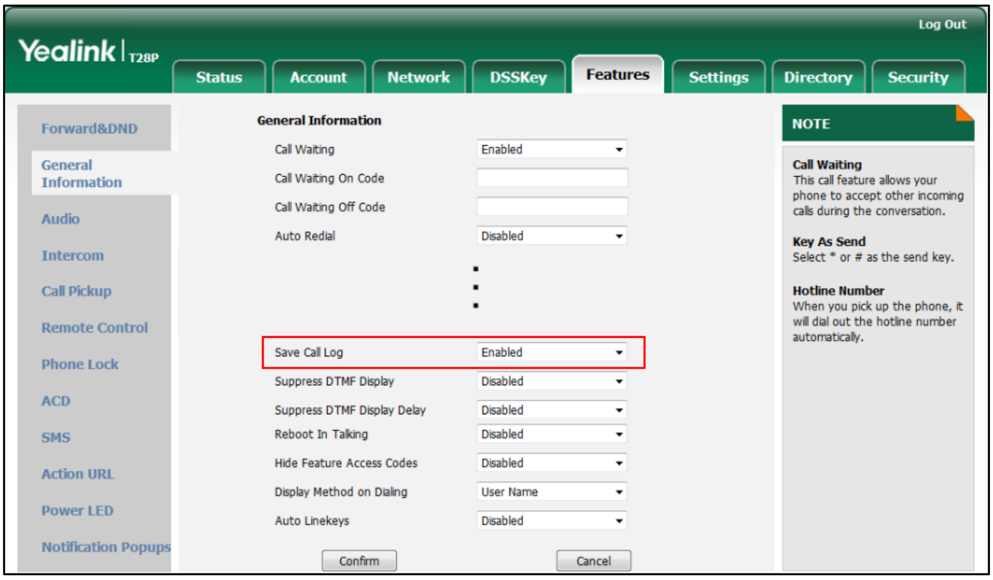
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
features.save_call_history	**0 or 1**	**1**
Description: Enables or disables the IP phone to save call log. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), the IP phone cannot log the placed calls, received calls, missed calls and the forwarded calls in the call log lists. **Web User Interface:** Features->General Information->Save Call Log **Phone User Interface:** Menu->Features->History Setting		

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.

To configure call log feature via phone user interface:

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

Missed Call Log

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

Procedure

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

Configuration File	<MAC>.cfg	Configure missed call log feature. **Parameter:** account.X.missed_calllog
Local	Web User Interface	Configure missed call log feature. **Navigate to:** http://<phoneIPAddress>/servlet?p=account-basic&q=load&acc

		=0

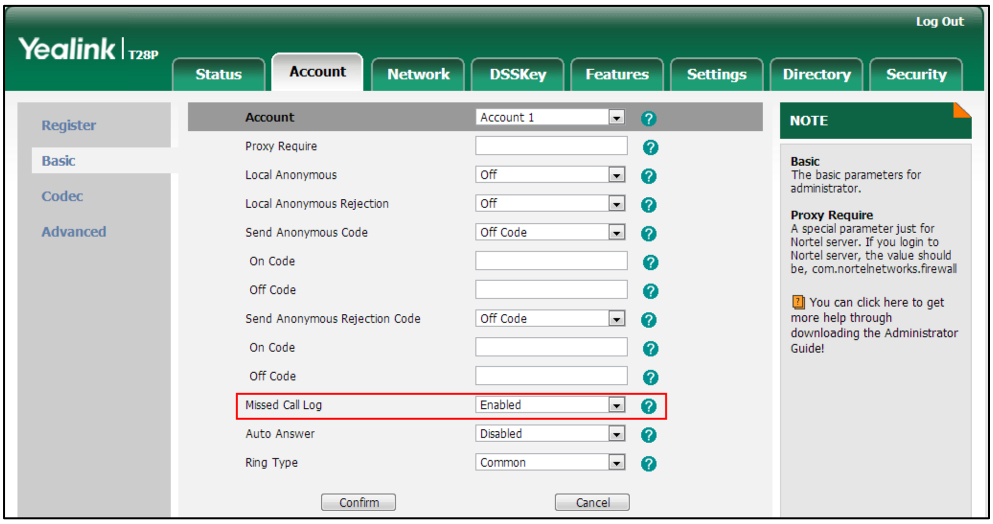
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
account.X.missed_calllog	**0 or 1**	**1**
Description: Enables or disables the IP phone to record missed calls for account X. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), there is no indicator displaying on the LCD screen, the IP phone does not log the missed call in the Missed Calls list. If it is set to 1 (Enabled), a prompt message "<number> New Missed Call(s)" along with an indicator icon is displayed on the IP phone idle screen when the IP phone misses calls. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Web User Interface:** Account->Basic->Missed Call Log **Phone User Interface:** None		

To configure missed call log via web user interface:

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

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



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

Local Directory

IP phones maintain a local directory. The local directory can store up to 1000 contacts and 5 groups. When adding a contact to the local directory, in addition to name and phone numbers, you can also specify the account, ring tone and group for the contact. Contacts and groups can be added either one by one or in batch using a local contact file. Yealink IP phones support both *.xml and *.csv format contact files. For more information on how to customize a contact file (*.xml), refer to Local Contact File on page 484.

Procedure

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

Configuration File	<y0000000000xx>.cfg	Specify the access URL of the local contact file (*.xml). **Parameter:** local_contact.data.url
Local	Web User Interface	Add a new group and a contact to the local directory. To import or export the local contact file. **Navigate to:** http://<phoneIPAddress>/servlet?p=contactsbasic&q=load&num=1&group=

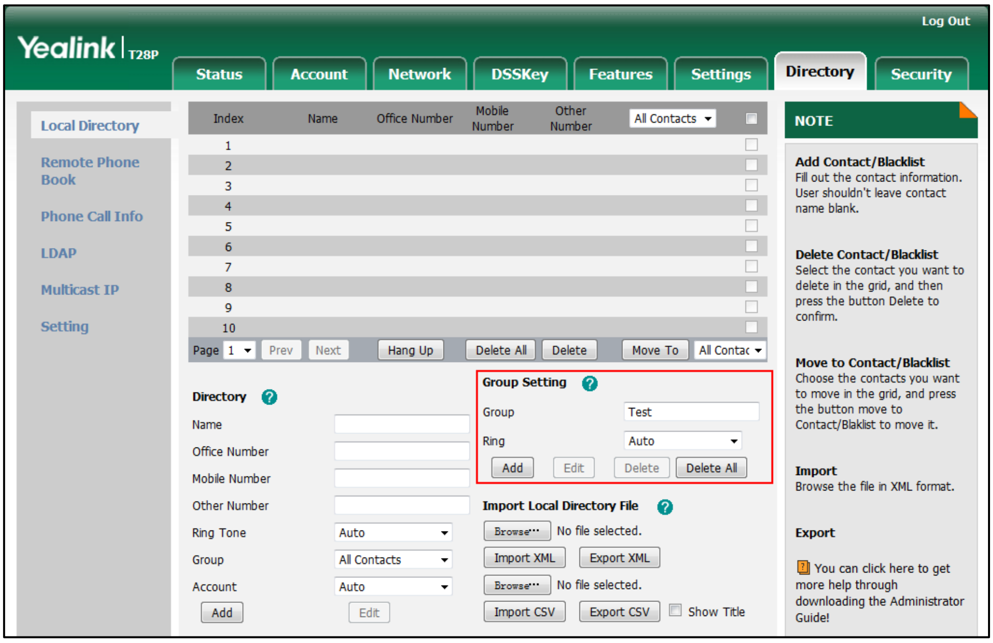
	Phone User Interface	Add a group and a contact to the local directory.

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
local_contact.data.url	URL within 511 characters	Blank
Description: Configures the access URL of the local contact file (*.xml). **Example:** local_contact.data.url = http://192.168.10.25/contact.xml **Web User Interface:** Directory->Local Directory->Import Local Directory File **Phone User Interface:** None		

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

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

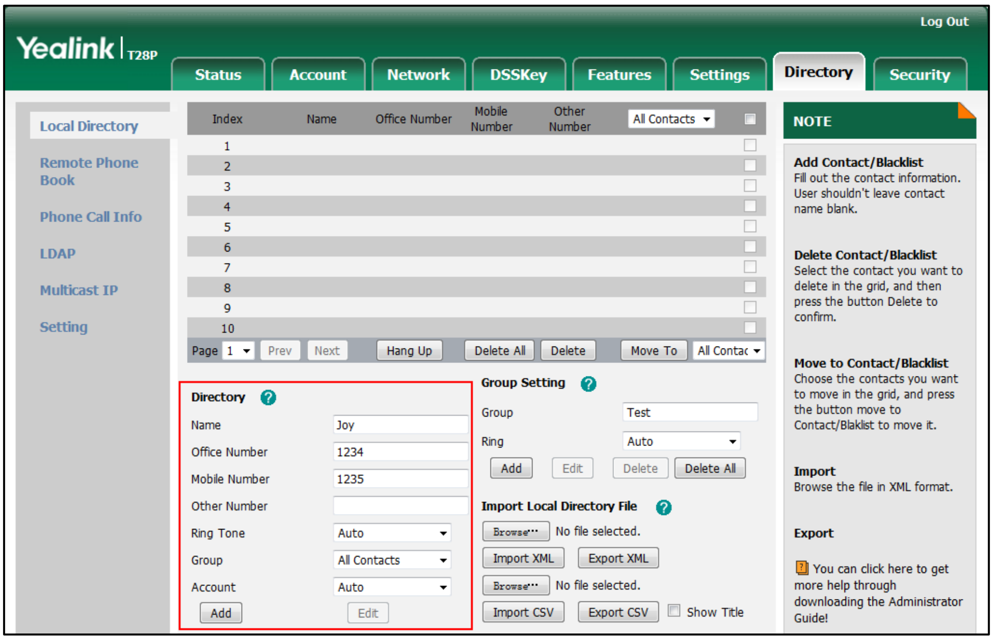


4. Click **Add** to add the group.

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

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

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



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

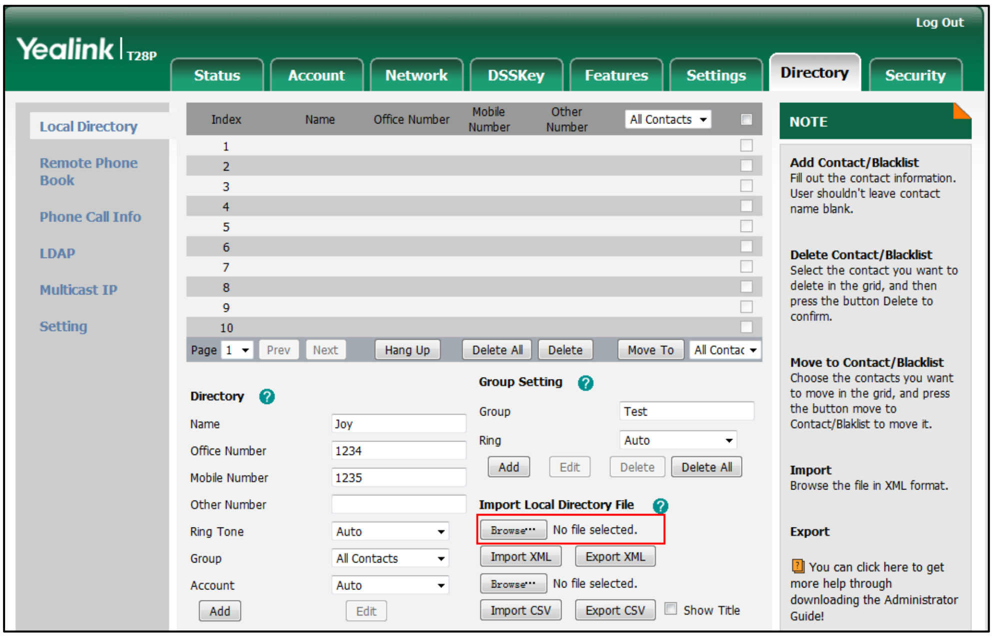
To add a group to the local directory via phone user interface:

1. Press **Menu**->**Directory**->**Local Directory**.
2. Press the **Add Group** soft key.
3. Enter the desired group name in the **Name** field.
4. Press ◀ or ▶ , or the **Switch** soft key to select the desired group ring tone from the **Ring** field.
5. Press the **Add** soft key to accept the change.

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

1. Click on **Directory**->**Local Directory**.

2. Click **Browse** to locate a contact list file (the file format must be *.xml) from your local system.



3. Click **Import XML** to import the contact list.

   The web user interface prompts "The original contact will be covered, Continue?".

4. 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. Click **Browse** to locate a contact list file (the file format must be *.csv) from your local system.
3. (Optional.) Check the **Show Title** checkbox.

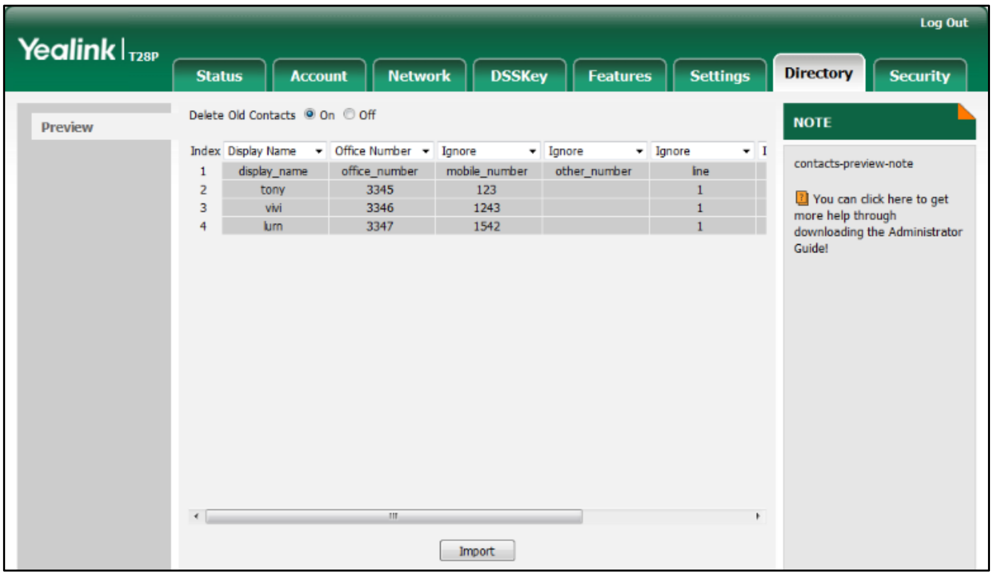
   It will prevent importing the title of the contact information which is located in the first line of the CSV file.

4. Click **Import CSV** 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 row information 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. Click **Export XML** (or **Export CSV**).
3. Click **Save** to save the contact list to your local system.

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

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

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

6. Press or , or the **Switch** soft key to select the desired ring tone from the **Ring** field.
7. Press the **Save** soft key to accept the change.

Live Dialpad

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

Procedure

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

Configuration File	<y0000000000xx>.cfg	Configure live dialpad. **Parameters:** phone_setting.predial_autodial phone_setting.inter_digit_time
Local	Web User Interface	Configure live dialpad. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-preference&q=load

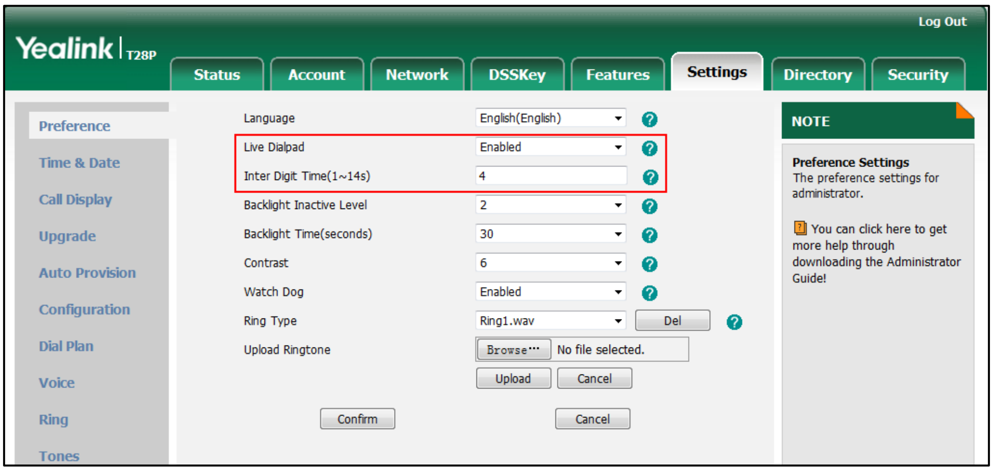
Details of Configuration Parameters:

Parameters	Permitted Values	Default
phone_setting.predial_autodial	**0 or 1**	**0**
Description: Enables or disables live dialpad feature. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the IP phone will automatically dial out the entered phone number in the pre-dialing screen without pressing a send key. **Web User Interface:** Settings->Preference->Live Dialpad **Phone User Interface:** None		
phone_setting.inter_digit_time	**Integer from 1 to 14**	**4**
Description: Configures the time (in seconds) for the IP phone to automatically dial out the entered digits without pressing a send key. **Note**: It works only if the parameter "phone_setting.predial_autodial" is set to 1		

Parameters	Permitted Values	Default
(Enabled). **Web User Interface:** Settings->Preference->Inter Digit Time (1~14s) **Phone User Interface:** None		

To configure live dialpad via web user interface:

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



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

Call Waiting

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

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

Procedure

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

<table>
<tr><td rowspan="1">Configuration File</td><td><y0000000000xx>.cfg</td><td>Configure call waiting and call waiting tone.
Parameters:
call_waiting.enable
call_waiting.tone
call_waiting.on_code
call_waiting.off_code</td></tr>
<tr><td rowspan="2">Local</td><td>Web User Interface</td><td>Configure call waiting.
Navigate to:
http://<phoneIPAddress>/servlet?p=features-general&q=load
Configure call waiting tone.
Navigate to:
http://<phoneIPAddress>/servlet?p=features-audio&q=load</td></tr>
<tr><td>Phone User Interface</td><td>Configure call waiting and call waiting tone.</td></tr>
</table>

Details of Configuration Parameters:

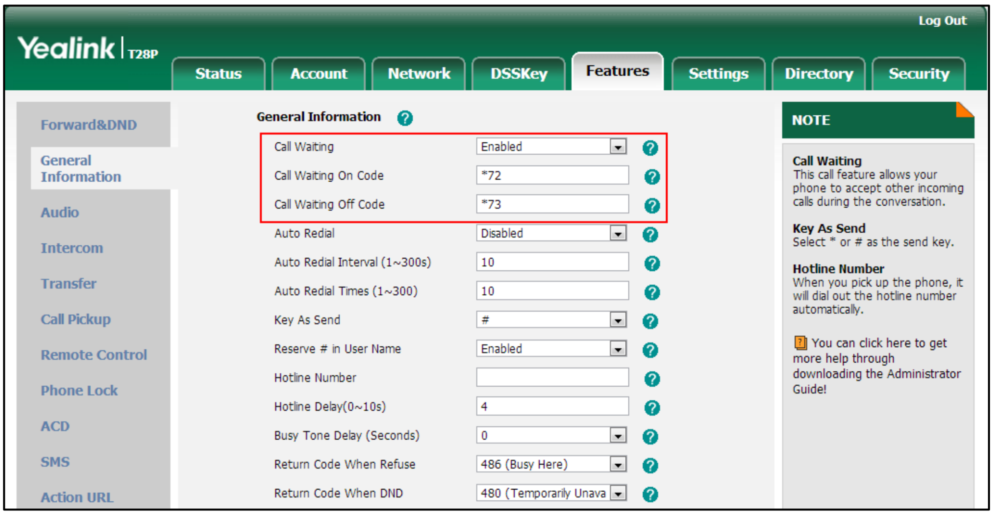
<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>call_waiting.enable</td><td>0 or 1</td><td>1</td></tr>
<tr><td colspan="3">Description:
Enables or disables call waiting feature.
0-Disabled
1-Enabled
If it is set to 0 (Disabled), a new incoming call is automatically rejected by the IP phone with a busy message while during a call.
If it is set to 1 (Enabled), the LCD screen will present a new incoming call while during a call.
Web User Interface:
Features->General Information->Call Waiting
Phone User Interface:</td></tr>
</table>

Parameters	Permitted Values	Default
Menu->Features->Call Waiting->Call Waiting		
call_waiting.tone	**0 or 1**	**1**
Description: Enables or disables the IP phone to play the call waiting tone when the IP phone receives an incoming call during a call. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the IP phone will perform an audible indicator when receiving a new incoming call during a call. **Note**: It works only if the parameter "call_waiting.enable" is set to 1 (Enabled). **Web User Interface:** Features->Audio->Call Waiting Tone **Phone User Interface:** Menu->Features->Call Waiting->Play Tone		
call_waiting.on_code	**String within 32 characters**	**Blank**
Description: Configures the call waiting on code to activate the server-side call waiting feature. The IP phone will send the call waiting on code to the server when you activate call waiting feature on the IP phone. **Example:** call_waiting.on_code = *72 **Web User Interface:** Features->General Information->Call Waiting On Code **Phone User Interface:** Menu->Features->Call Waiting->On Code		
call_waiting.off_code	**String within 32 characters**	**Blank**
Description: Configures the call waiting off code to deactivate the server-side call waiting feature. The IP phone will send the call waiting off code to the server when you deactivate call waiting feature on the IP phone. **Example:** call_waiting.off_code = *73		

Parameters	Permitted Values	Default
Web User Interface: Features->General Information->Call Waiting Off Code **Phone User Interface:** Menu->Features->Call Waiting->Off Code		

To configure call waiting via web user interface:

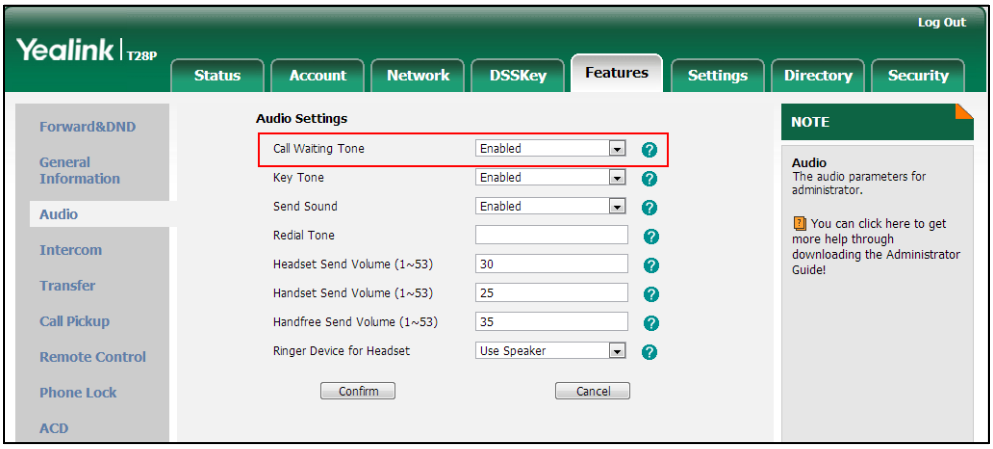
1. Click on **Features**->**General Information**.
2. Select the desired value from the pull-down list of **Call Waiting**.
3. (Optional.) Enter the call waiting on code in the **Call Waiting On Code** field.
4. (Optional.) Enter the call waiting off code in the **Call Waiting Off Code** field.



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

To configure call waiting tone via web user interface:

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



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

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

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

Auto Redial

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

Procedure

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

Configuration File	<y0000000000xx>.cfg	Configure auto redial feature. **Parameters:** auto_redial.enable auto_redial.interval auto_redial.times
Local	Web User Interface	Configure auto redial feature. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-general&q=load
	Phone User Interface	Configure auto redial feature.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
auto_redial.enable	**0 or 1**	**0**

Parameters	Permitted Values	Default
Description: Enables or disables the IP phone to automatically redial the dialed number when the callee is temporarily unavailable. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the IP phone will dial the previous dialed out number automatically when the dialed number is temporarily unavailable. **Web User Interface:** Features->General Information->Auto Redial **Phone User Interface:** Menu->Features->Auto Redial->Auto Redial		
auto_redial.interval	**Integer from 1 to 300**	**10**
Description: Configures the interval (in seconds) for the IP phone to wait between redials. The IP phone redials the dialed number at regular intervals till the callee answers the call. **Web User Interface:** Features->General Information->Auto Redial Interval (1~300s) **Phone User Interface:** Menu->Features->Auto Redial->Redial Interval		
auto_redial.times	**Integer from 1 to 300**	**10**
Description: Configures the auto redial times when the callee is temporarily unavailable. The IP phone tries to redial the dialed number as many times as configured till the callee answers the call. **Web User Interface:** Features->General Information->Auto Redial Times (1~300) **Phone User Interface:** Menu->Features->Auto Redial->Redial Times		

To configure auto redial via web user interface:

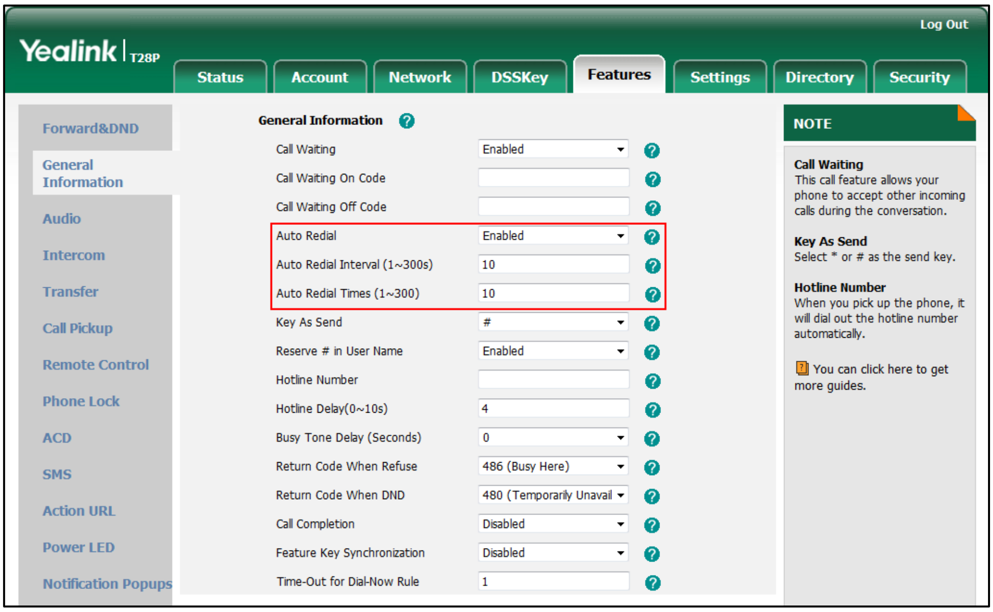
1. Click on **Features**->**General Information**.
2. Select the desired value from the pull-down list of **Auto Redial**.

3. Enter the waiting time in the **Auto Redial Interval (1~300s)** field.

   The default waiting time is 10s.

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

   The default value is 10.



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

To configure auto redial via phone user interface:

1. Press **Menu**->**Features**->**Auto Redial**.
2. Press or , or the **Switch** soft key to select the desired value from the **Auto Redial** field.
3. Enter the waiting time (in seconds) in the **Redial Interval** field.
4. Enter the desired times in the **Redial Times** field.
5. Press the **Save** soft key to accept the change.

Auto Answer

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

Procedure

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

Configuration File	<MAC>.cfg	Configure auto answer. **Parameter:** account.X.auto_answer
	<y0000000000xx>.cfg	Specify a period of delay time for auto answer. **Parameter:** features.auto_answer_delay
Local	Web User Interface	Configure auto answer. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-basic&q=load&acc=0 Specify a period of delay time for auto answer. **Navigate to**: http://<phoneIPAddress>servlet?p=features-general&q=load
	Phone User Interface	Configure auto answer.

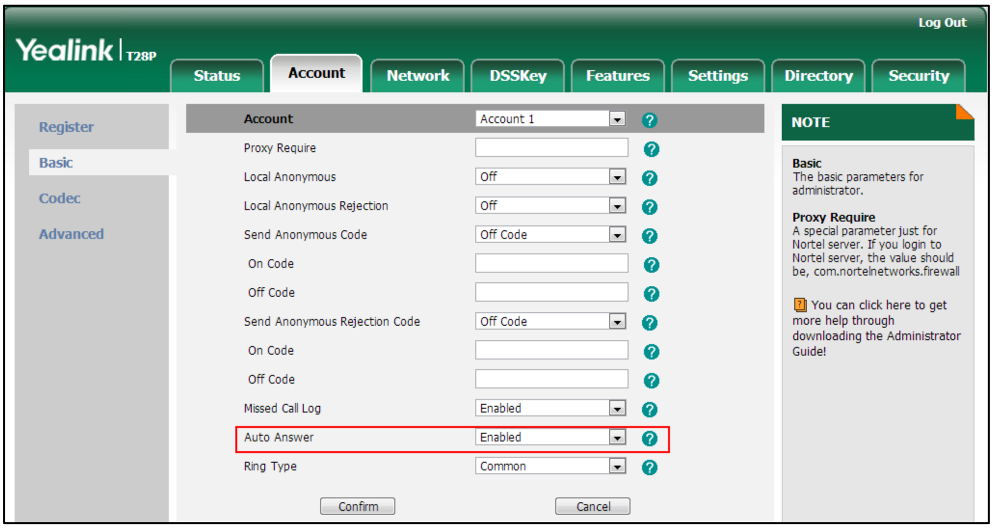
Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.auto_answer	**0 or 1**	**0**
Description: Enables or disables auto answer feature for account X. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the IP phone can automatically answer an incoming call. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Note**: The IP phone cannot automatically answer the incoming call during a call even if auto answer is enabled. **Web User Interface:**		

Parameters	Permitted Values	Default
Account->Basic->Auto Answer **Phone User Interface:** Menu->Settings->Advanced Settings (default password: admin)->Account->Account X->Auto Answer		
features.auto_answer_delay (X ranges from 1 to 6)	Integer from 1 to 4	1
Description: Configures the delay time (in seconds) before the IP phone automatically answers an incoming call. **Web User Interface:** Features->General Information->Auto-Answer Delay (1~4s) **Phone User Interface:** None		

To configure auto answer via web user interface:

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

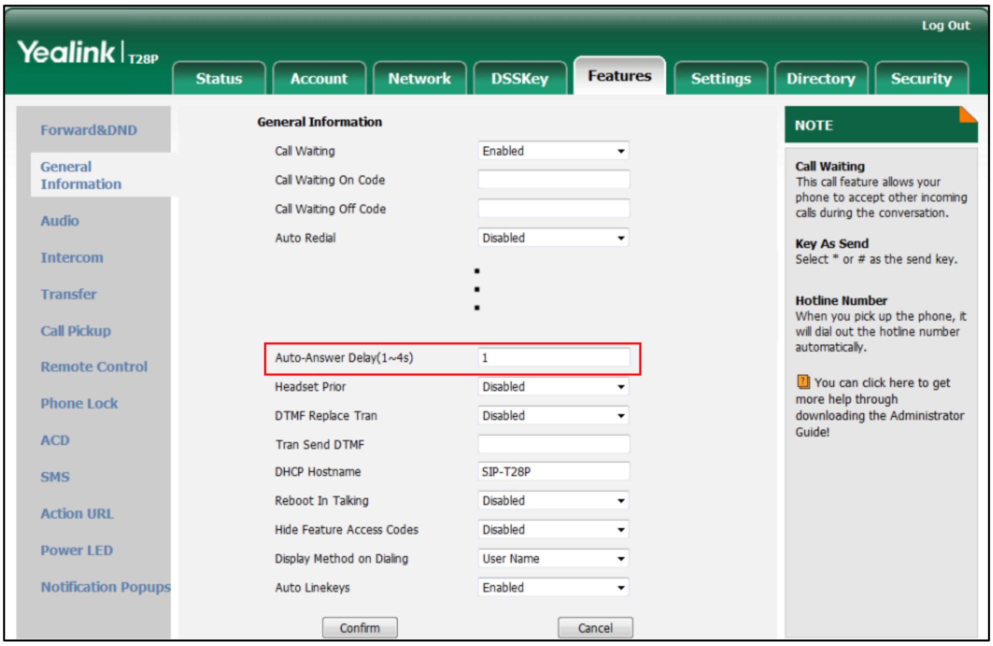


5. Click **Confirm** to accept the change.

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

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

2. Enter the desired time in the **Auto-Answer Delay (1~4s)** field.



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

To configure auto answer via phone user interface:

1. Press **Menu**->**Settings**->**Advanced Settings** (default password: admin) ->**Accounts**.
2. Select the desired account and then press the **Enter** soft key.
3. Press or , or the **Switch** soft key to select the desired value from the **Auto Answer** field.
4. Press the **Save** soft key to accept the change.

Call Completion

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

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

IP phones support call completion using the SUBSCRIBE/NOTIFY method, which is specified in draft-poetzl-sipping-call-completion-00, to subscribe to the busy party and receive notifications of their status changes.

Procedure

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

Configuration File	<y0000000000xx>.cfg	Configure call completion. **Parameter:** features.call_completion_enable
Local	Web User Interface	Configure call completion. **Navigate to**: http://<phoneIPAddress>/servlet ?p=features-general&q=load
	Phone User Interface	Configure call completion.

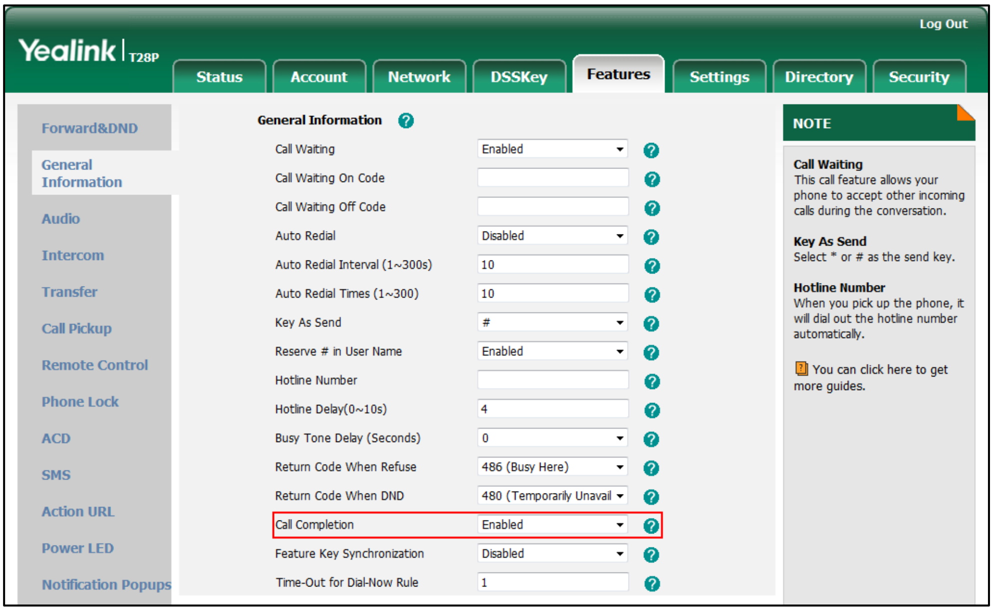
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
features.call_completion_enable	**0 or 1**	**0**
Description: Enables or disables call completion feature. If a user places a call and the callee is temporarily unavailable to answer the call, call completion feature allows notifying the user when the callee becomes available to receive a call. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the caller is notified when the callee becomes available to receive a call. **Web User Interface:** Features->General Information->Call Completion **Phone User Interface:** Menu->Features->Call Completion->Call Completion		

To configure call completion via web user interface:

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

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



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

To configure call completion via phone user interface:

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

Anonymous Call

Anonymous call allows the caller to conceal the identity information displayed on the callee's screen. The callee's phone LCD screen prompts an incoming call from anonymity. Anonymous call is configurable on a per-line basis.

Example of anonymous SIP header:

Via: SIP/2.0/UDP 10.2.8.183:5063;branch=z9hG4bK1535948896
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=128043702
To: <sip:1011@10.2.1.199>
Call-ID: 1773251036@10.2.8.183
CSeq: 1 INVITE
Contact: <sip:1012@10.2.8.183:5063>
Content-Type: application/sdp
Allow: INVITE, INFO, PRACK, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REGISTER, SUBSCRIBE, REFER, PUBLISH, UPDATE, MESSAGE
Max-Forwards: 70
User-Agent: Yealink SIP-T28P 2.72.0.1

Privacy: id
Supported: replaces
Allow-Events: talk,hold,conference,refer,check-sync
P-Preferred-Identity: <sip:1012@10.2.1.199>
Content-Length: 302

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

Procedure

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

Configuration File	<MAC>.cfg	Configure anonymous call. **Parameters:** account.X.anonymous_call account.X.send_anonymous_code account.X.anonymous_call_oncode account.X.anonymous_call_offcode
Local	Web User Interface	Configure anonymous call. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-basic&q=load&acc=0
	Phone User Interface	Configure anonymous call.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.anonymous_call	**0 or 1**	**0**
Description: Enables or disables anonymous call feature for account X. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the IP phone will block its identity from showing up to the callee when placing a call. The callee's phone LCD screen presents anonymous instead of the caller's identity. X ranges from 1 to 6 (for SIP-T28P).		

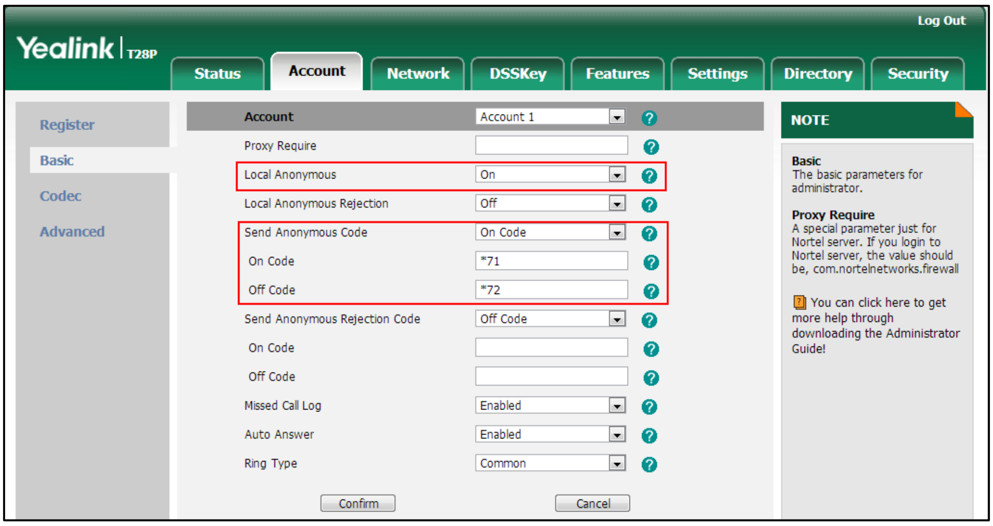
Parameters	Permitted Values	Default
X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Web User Interface:** Account->Basic->Local Anonymous **Phone User Interface:** Menu->Features->Anonymous Call->Local Anonymous		
account.X.send_anonymous_code	**0 or 1**	**0**
Description: Configures the IP phone to send anonymous on/off code to activate/deactivate the server-side anonymous call feature for account X. **0**-Off Code **1**-On Code If it is set to 0 (Off Code), the IP phone will send anonymous off code to deactivate the server-side anonymous call feature. If it is set to 1 (On Code), the IP phone will send anonymous on code to activate the server-side anonymous call feature. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Web User Interface:** Account->Basic->Send Anonymous Code **Phone User Interface:** Menu->Features->Anonymous Call->Send Anony Code		
account.X.anonymous_call_oncode	**String within 32 characters**	**Blank**
Description: Configures the anonymous call on code to activate the server-side anonymous call feature for account X. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Example:** account.1.anonymous_call_oncode = *71 **Note:** It works only if the parameter "account.X.send_anonymous_code" is set to 1		

Parameters	Permitted Values	Default
(On Code). **Web User Interface:** Account->Basic->Anonymous Call->On Code **Phone User Interface:** Menu->Features->Anonymous Call->Send Anony Code->On Code		
account.X.anonymous_call_offcode	**String within 32 characters**	**Blank**
Description: Configures the anonymous call off code to deactivate the server-side anonymous call feature for account X. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Example:** account.1.anonymous_call_offcode = *72 **Note:** It works only if the parameter "account.X.send_anonymous_code" is set to 0 (Off Code). **Web User Interface:** Account->Basic->Anonymous Call->Off Code **Phone User Interface:** Menu->Features->Anonymous Call->Send Anony Code->Off Code		

To configure anonymous call via web user interface:

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

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



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

To configure the anonymous call via phone user interface:

1. Press **Menu**->**Features**->**Anonymous Call**.
2. Press ◀ or ▶ , or the **Switch** soft key to select the desired line from the **Account ID** field.
3. Press ◀ or ▶ , or the **Switch** soft key to select the desired value from the **Local Anonymous** field.
4. (Optional.) Press ◀ or ▶ , or the **Switch** soft key to select the desired value from the **Send Anony Code** field.
5. (Optional.) Enter the anonymous call on code in the **On Code** field.
6. (Optional.) Enter the anonymous call off code in the **Off Code** field.

Anonymous Call Rejection

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

Configuration File	<MAC>.cfg	Configure anonymous call rejection. **Parameters:** account.X.reject_anonymous_call account.X.send_anonymous_rejection_code account.X.anonymous_reject_oncode account.X.anonymous_reject_offcode
Local	Web User Interface	Configure anonymous call rejection. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-basic&q=load&acc=0
	Phone User Interface	Configure anonymous call rejection.

Details of Configuration Parameters:

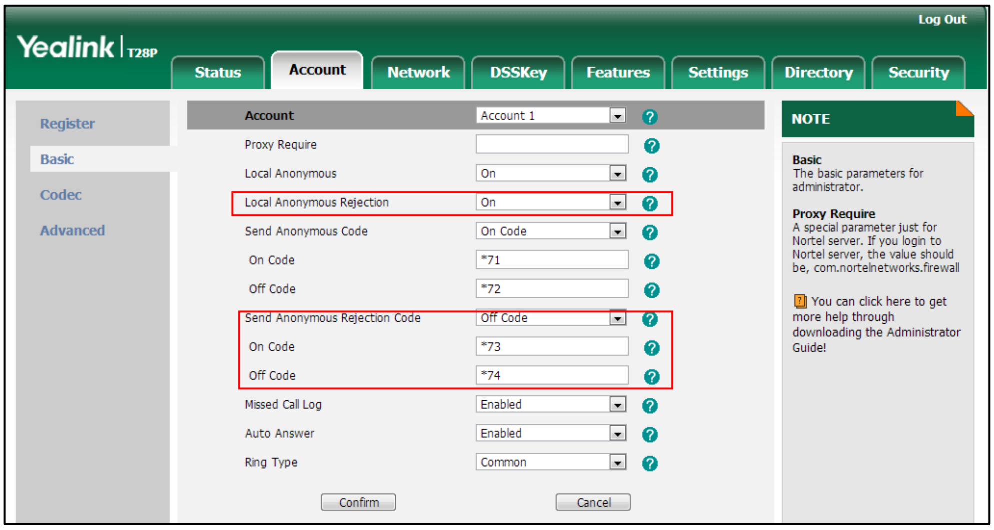
Parameters	Permitted Values	Default
account.X.reject_anonymous_call	**0 or 1**	**0**
Description: Enables or disables anonymous call rejection feature for account X. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the IP phone will automatically reject incoming calls from users enabled anonymous call feature. The anonymous user's phone LCD screen presents "Anonymity Disallowed". X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Web User Interface:** Account->Basic->Local Anonymous Rejection **Phone User Interface:** Menu->Features->Anonymous Call->Anon Reject		
account.X.anonymous_reject_oncode	**String within 32 characters**	**Blank**

Parameters	Permitted Values	Default
Description: Configures the anonymous call rejection on code to activate the server-side anonymous call rejection feature for account X. The IP phone will send the anonymous call rejection on code to the server when you activate anonymous call rejection feature for account X on the IP phone. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Example:** account.1.anonymous_reject_oncode = *73 **Web User Interface:** Account->Basic->Send Anonymous Rejection Code->On Code **Phone User Interface:** Menu->Features->Anonymous Call->Send rejection Code->On Code		
account.X.anonymous_reject_offcode	**String within 32 characters**	**Blank**
Description: Configures the anonymous call rejection off code to deactivate the server-side anonymous call rejection feature for account X. The IP phone will send the anonymous call rejection off code to the server when you deactivate anonymous call rejection feature for account X on the IP phone. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Example:** account.1.anonymous_reject_offcode = *74 **Web User Interface:** Account->Basic->Send Anonymous Rejection Code->Off Code **Phone User Interface:** Menu->Features->Anonymous Call->Send rejection Code->Off Code		
account.X.send_anonymous_rejection_code	**0 or 1**	**0**

Parameters	Permitted Values	Default
Configures what code sent to the server for account X. 0- off code 1- on code X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Web User Interface:** Account->Basic->Send Anonymous Rejection Code **Phone User Interface:** Menu->Features->Anonymous Call->Send rejection Code		

To configure anonymous call rejection via web user interface:

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



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

To configure anonymous call rejection via phone user interface:

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

2. Press or , or the **Switch** soft key to select the desired line from the **Account ID** field.
3. Press or to scroll to the **Anon Reject** field.
4. Press or to select **Enabled** from the **Anon Reject** field.
5. Press or to scroll to the **Send rejection Code** field.
6. (Optional.) Press or to select the desired value from the **Send rejection Code** field.
7. (Optional.) Enter the anonymous call rejection on code and off code respectively in the **On Code** and **Off Code** field.
8. Press the **Save** soft key to accept the change or the **Back** soft key to cancel.

Do Not Disturb

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

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

A user can activate or deactivate DND using the DND key or DND soft key (not applicable to SIP-T20P IP phones). The server-side DND feature disables the local DND and call forward settings. If the server-side DND feature is enabled on any of the IP phone's registrations, the other registrations are not affected. For more information on call forward, refer to Call Forward on page 191.

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

Return Message When DND

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

Procedure

DND can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure DND in the custom mode. **Parameters:** account.X.dnd.enable account.X.dnd.on_code account.X.dnd.off_code

	<y0000000000xx>.cfg	Assign a DND key. **Parameters:** memorykey.X.type/ linekey.X.type/ programablekey.X.type Configure the DND mode. **Parameter:** features.dnd_mode Configure DND in the IP phone mode. **Parameters:** features.dnd.enable features.dnd.on_code features.dnd.off_code Specify the return code and the reason of the SIP response message when DND is enabled. **Parameter:** features.dnd_refuse_code
Local	Web User Interface	Assign a DND key. **Navigate to**: http://<phoneIPAddress>/servlet?p=dsskey&q=load&model=0 Configure DND. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-forward&q=load Specify the return code and the reason of the SIP response message when DND is enabled. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load
	Phone User Interface	Assign a DND key. Configure DND.

Details of Configuration Parameters:

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>account.X.dnd.enable</td><td>0 or 1</td><td>0</td></tr>
<tr><td colspan="3">Description:
Enables or disables DND feature for account X when the DND mode is configured as Custom.
0-Disabled
1-Enabled
If it is set to 1 (Enabled), the IP phone will reject incoming calls on account X.
X ranges from 1 to 6 (for SIP-T28P).
X ranges from 1 to 3 (for SIP-T26P/T22P).
X ranges from 1 to 2 (for SIP-T20P).
Web User Interface:
Features->Forward& DND->DND->DND Status
Phone User Interface:
DND->Account X</td></tr>
<tr><td>account.X.dnd.on_code</td><td>String within 32 characters</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the DND on code to activate the server-side DND feature for account X when the DND mode is configured as Custom. The IP phone will send the DND on code to the server when you activate DND feature for account X on the IP phone.
X ranges from 1 to 6 (for SIP-T28P).
X ranges from 1 to 3 (for SIP-T26P/T22P).
X ranges from 1 to 2 (for SIP-T20P).
Example:
account.1.dnd.on_code = *73
Web User Interface:
Features->Forward& DND->DND On Code
Phone User Interface:
Menu->Features->DND Code->DND On Code</td></tr>
<tr><td>account.X.dnd.off_code</td><td>String within 32 characters</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the DND off code to deactivate the server-side DND feature for account X</td></tr>
</table>

Parameters	Permitted Values	Default
when the DND mode is configured as Custom. The IP phone will send the DND off code to the server when you deactivate DND feature for account X on the IP phone. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Example:** account.1.dnd.off_code = *74 **Web User Interface:** Features->Forward& DND->DND Off Code **Phone User Interface:** Menu->Features->DND Code->DND On Code		
features.dnd_mode	**0 or 1**	**0**
Description: Configures the DND mode for the IP phone. **0**-Phone **1**-Custom If it is set to 0 (Phone), DND feature is effective for the IP phone. If it is set to 1 (Custom), you can configure DND feature for each account. **Web User Interface:** Features->Forward& DND->DND->Mode **Phone User Interface:** None		
features.dnd.enable	**0 or 1**	**0**
Description: Enables or disables DND feature when the DND mode is configured as Phone. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the IP phone will reject incoming calls on all accounts. **Web User Interface:** Features->Forward& DND->DND->DND Status **Phone User Interface:** DND		

Parameters	Permitted Values	Default
features.dnd.on_code	**String within 32 characters**	**Blank**
Description: Configures the DND on code to activate the server-side DND feature when the DND mode is configured as Phone. The IP phone will send the DND on code to the server when you activate DND feature on the IP phone. **Example:** features.dnd.on_code = *71 **Web User Interface:** Features->Forward& DND->DND->DND On Code **Phone User Interface:** Menu->Features->DND Code->DND On Code		
features.dnd.off_code	**String within 32 characters**	**Blank**
Description: Configures the DND off code to deactivate the server-side DND feature when the DND mode is configured as Phone. The IP phone will send the DND off code to the server when you deactivate DND feature on the IP phone. **Example:** features.dnd.off_code = *72 **Web User Interface:** Features->Forward& DND->DND->DND Off Code **Phone User Interface:** Menu->Features->DND Code->DND Off Code		
features.dnd_refuse_code	**404, 480 or 486**	**480**
Description: Configures a return code and reason of SIP response messages when rejecting an incoming call by DND. A specific reason is displayed on the caller's phone LCD screen. **404**-No Found **480**-Temporarily Unavailable **486**-Busy Here If it is set to 486 (Busy Here), the caller's LCD screen will display the reason "Busy Here" when the callee enables DND.		

Parameters	Permitted Values	Default
Web User Interface: Features->General Information->Return Code When DND **Phone User Interface:** None		

DND Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 513.

Parameter	Permitted Values	Default
memorykey.X.type/ linekey.X.type/ programablekey.X.type	**5**	**Refer to the following content**
Description: Configures a DSS key as a DND key on the IP phone. The digit **5** stands for the key type **DND**. For memory keys: X ranges from 1 to 10. For line keys: X ranges from 1 to 6 (for SIP-T28P) X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). For programable keys: X ranges from 1 to 14 (for SIP-T28/T26P) X=1-10, 14 (for SIP-T22P) X=5-12, 14 (for SIP-T20P) **Example:** memorykey.1.type = 5 **Default:** For memory keys: The default value is 0. For line keys: The default value is 15. For programable keys: **For SIP-T28P/T26P IP phones:**		

Parameter	Permitted Values	Default
When X=1, the default value is 28 (History). When X=2, the default value is 61 (Directory). When X=3, the default value is 5 (DND). When X=4, the default value is 30 (Menu). When X=5, the default value is 28 (History). When X=6, the default value is 61 (Directory). When X=7, the default value is 31 (Switch Account). When X=8, the default value is 31 (Switch Account). When X=9, the default value is 33 (Status). When X=10, the default value is 0 (NA). When X=11, the default value is 0 (NA). When X=12, the default value is 0 (NA). When X=13, the default value is 0 (NA). When X=14, the default value is 2 (Forward). **For SIP-T22P IP phones:** When X=1, the default value is 28 (History). When X=2, the default value is 61 (Directory). When X=3, the default value is 5 (DND). When X=4, the default value is 30 (Menu). When X=5, the default value is 28 (History). When X=6, the default value is 61 (Directory). When X=7, the default value is 31 (Switch Account). When X=8, the default value is 31 (Switch Account). When X=9, the default value is 33 (Status). When X=10, the default value is 0 (NA). When X=14, the default value is 2 (Forward). **For SIP-T20P IP phones:** When X=5, the default value is 28 (History). When X=6, the default value is 61 (Directory). When X=7, the default value is 31 (Switch Account). When X=8, the default value is 31 (Switch Account). When X=9, the default value is 33 (Status). When X=10, the default value is 0 (NA). When X=11, the default value is 0 (NA). When X=12, the default value is 0 (NA).		

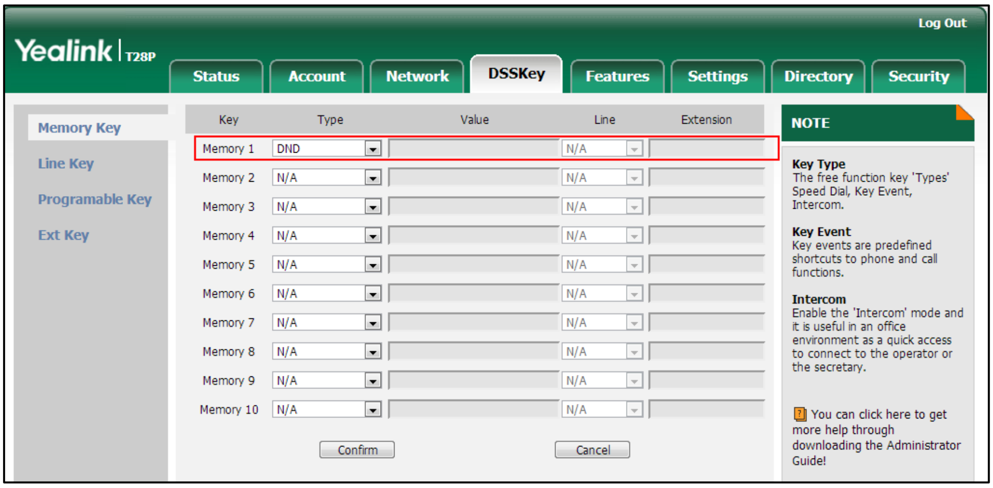
Parameter	Permitted Values	Default
When X=14, the default value is 2 (Forward). **Web User Interface:** DSSKey->Memory Key/Line Key/Programable Key->Type **Phone User Interface:** Menu->Features->DSS Keys->Memory Keys (or Line Keys)->DSS Key X (or Line Key X)->Type		

To configure a DND key via web user interface:

1. Click on **DSSKey**->**Memory Key** (**Line Key** or **Programable Key**).

   SIP-T22P/T20P IP phones only support line keys and programable keys.

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



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

To configure DND feature via web user interface:

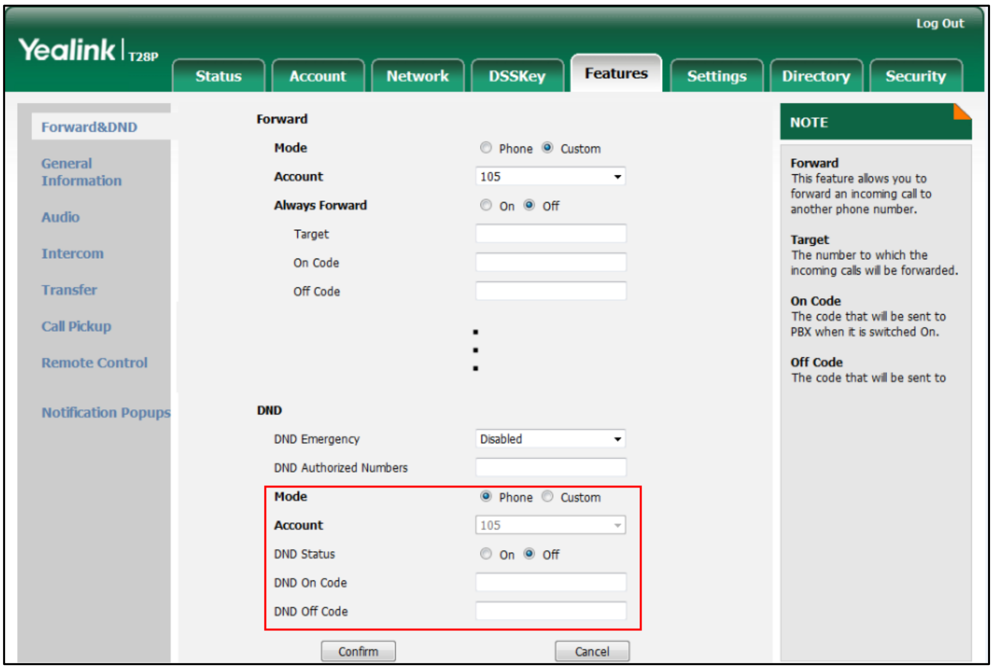
1. Click on **Features**->**Forward & DND**.
2. In the **DND** block, mark the desired radio box in the **Mode** field.

   a) If you mark the **Phone** radio box:

   1) Mark the desired radio box in the **DND Status** field.

   2) (Optional.) Enter the DND on code in the **DND On Code** field.

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



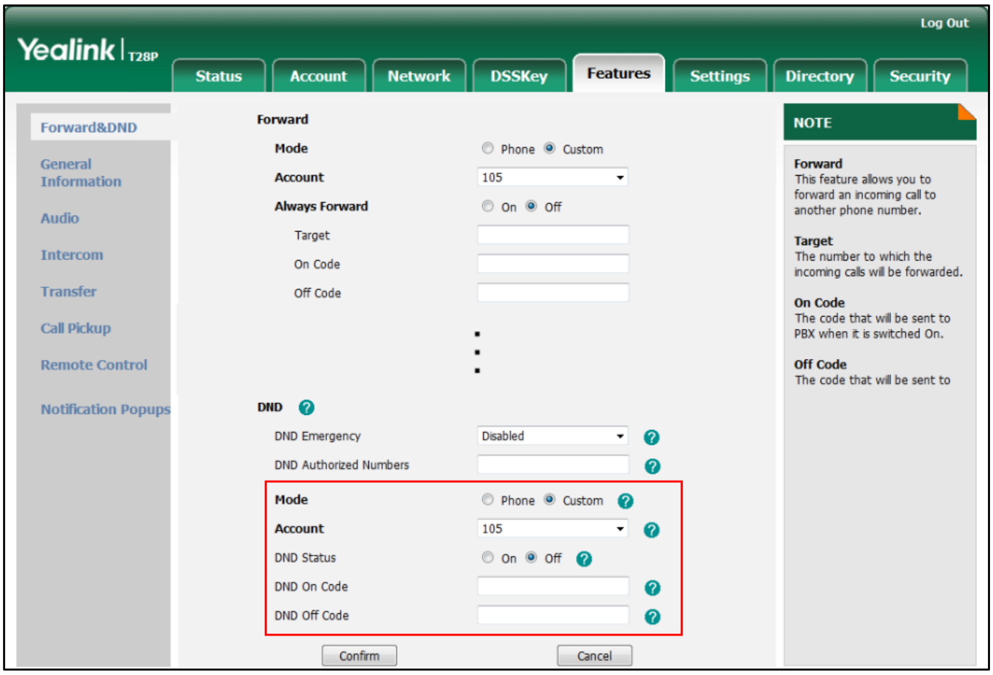
b) If you mark the **Custom** radio box:

1) Select the desired account from the pull-down list of **Account**.

2) Mark the desired radio box in the **DND Status** field.

3) (Optional.) Enter the DND on code in the **DND On Code** field.

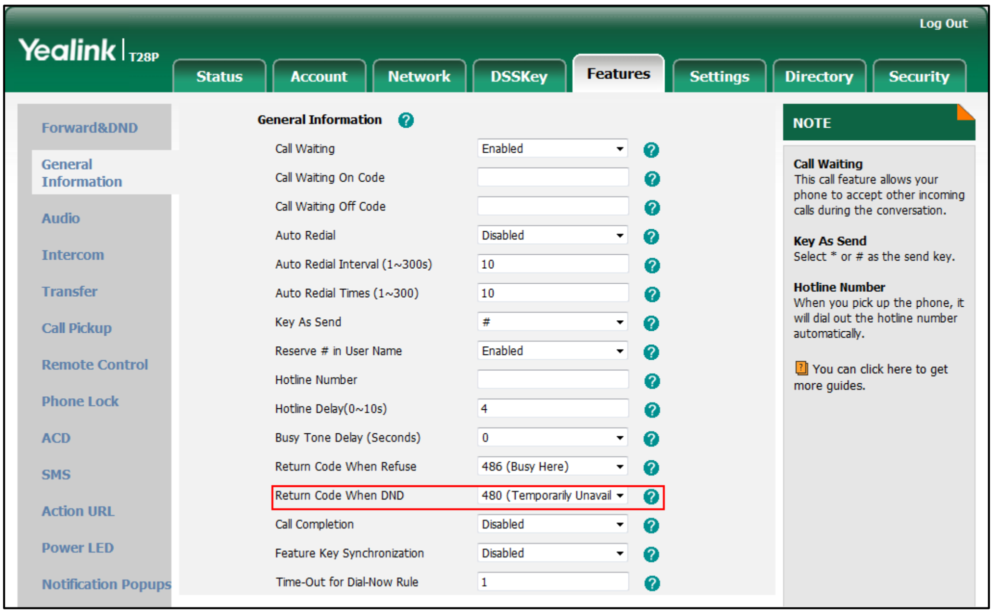
4) (Optional.) Enter the DND off code in the **DND Off Code** field.



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

To specify the return code and the reason when DND is enabled via web user interface:

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



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

To configure a DND key via phone user interface:

1. Press **Menu**->**Features**->**DSS Keys**->**Memory Keys** (or **Line Keys**).
2. Select the desired DSS key.
3. Press or , or the **Switch** soft key to select **Key Event** from the **Type** field.
4. Press or , or the **Switch** soft key to select **DND** from the **Key Type** field.
5. Press the **Save** soft key to accept the change.

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

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

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

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

   The LCD screen displays a list of accounts registered on the IP phone.
2. Press or to select the desired account.
3. Press or to select **On** to activate DND.

   You can configure DND in the custom mode for all accounts by pressing the **All On** soft key.
4. Press the **Save** soft key to accept the change.

Busy Tone Delay

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

Procedure

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

Configuration File	<y0000000000xx>.cfg	Configure busy tone delay. **Parameter:** features.busy_tone_delay
Local	Web User Interface	Configure busy tone delay. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-general&q=load

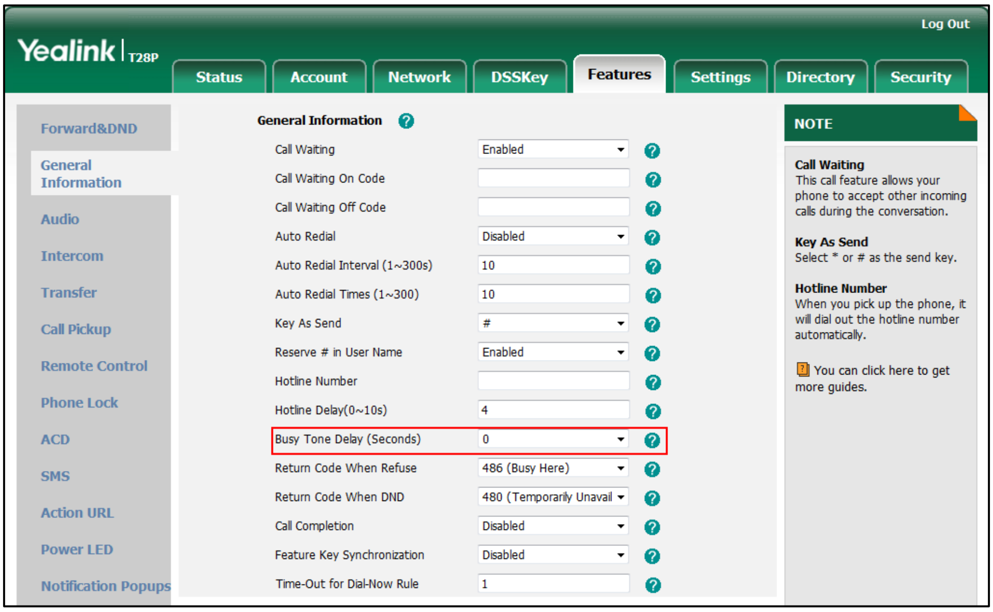
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
features.busy_tone_delay	**0, 3 or 5**	**0**
Description: 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. **0**-0s **3**-3s **5**-5s If it is set to 3 (3s), a busy tone is audible for 3 seconds on the IP phone. **Web User Interface:** Features->General Information->Busy Tone Delay (Seconds) **Phone User Interface:** None		

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)

Procedure

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

Configuration File	<y0000000000xx>.cfg	Specify the return code and the reason of the SIP response message when refusing a call. **Parameter:** features.normal_refuse_code
Local	Web User Interface	Specify the return code and the reason of the SIP response message when refusing a call. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-general&q=load

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
features.normal_refuse_code	404, 480 or 486	486

Description:

Configures a return code and reason of SIP response messages when the IP phone rejects an incoming call. A specific reason is displayed on the caller's phone LCD screen.

404-No Found

480-Temporarily Unavailable

486-Busy Here

If it is set to 486 (Busy Here), the caller's phone LCD screen will display the message "Busy Here" when the callee rejects the incoming call.

Web User Interface:

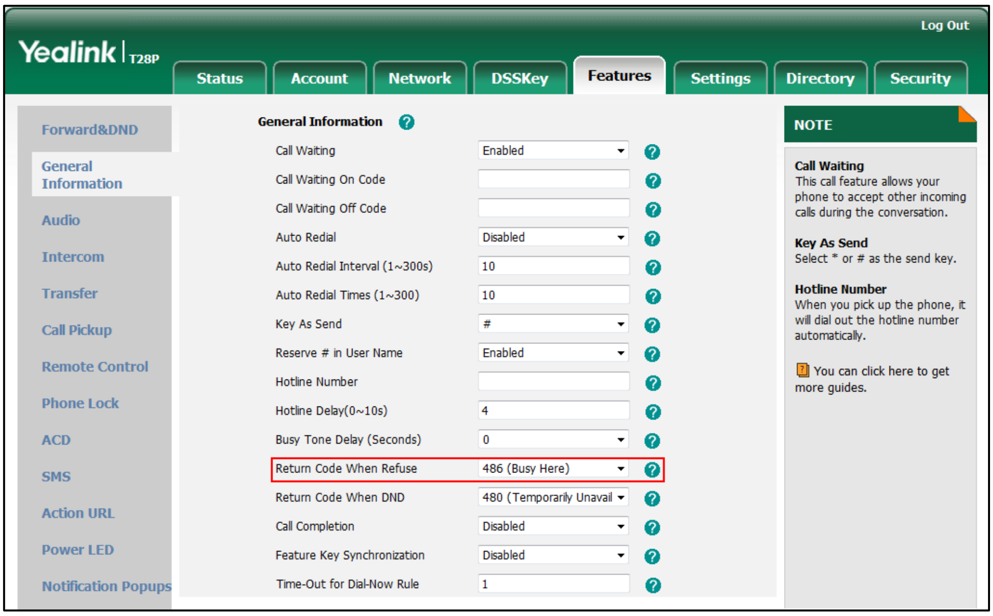
Features->General Information->Return Code When Refuse

Phone User Interface:

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 ringback tone and begins to play the media received. 180 ring workaround allows IP phones to resume and play the local ringback tone upon a subsequent 180 message received.

Procedure

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

Configuration File	<y0000000000xx>.cfg	Configure 180 ring workaround. **Parameter:** phone_setting.is_deal180
Local	Web User Interface	Configur 180 ring workaround. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-general&q=load

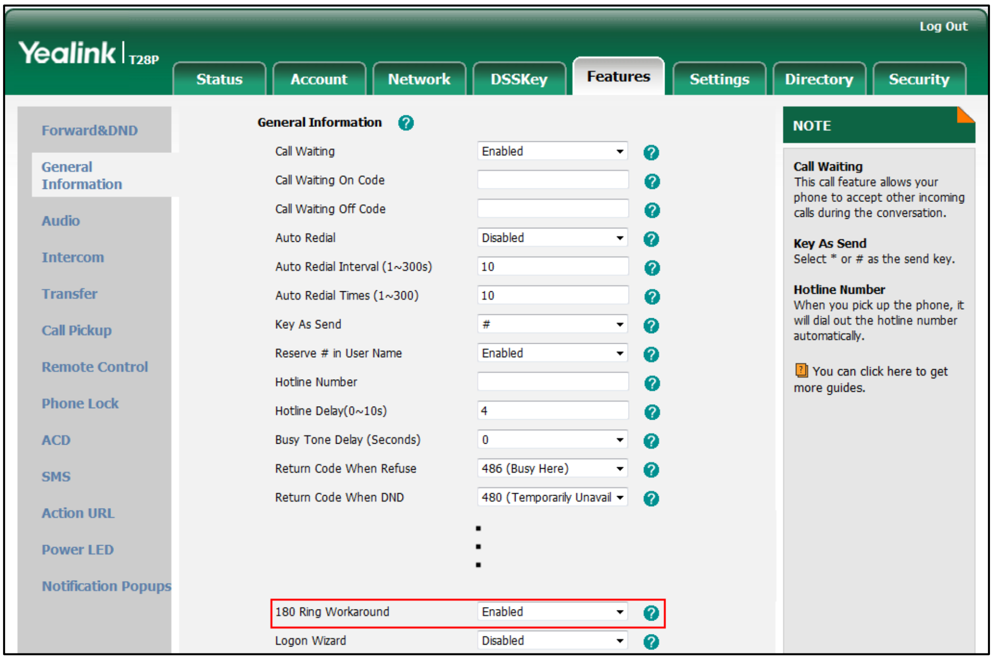
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
phone_setting.is_deal180	**0 or 1**	**1**
Description: Enables or disables the IP phone to deal with the 180 SIP message received after the 183 SIP message. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the IP phone will resume and play the local ringback tone upon a subsequent 180 message received. **Web User Interface:** Features->General Information->180 Ring Workaround		

Parameter	Permitted Values	Default
Phone User Interface: None		

To configure 180 ring workaround via web user interface:

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



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

Use Outbound Proxy in Dialog

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

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

Procedure

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

Configuration File	<y0000000000xx>.cfg	Specify whether to use outbound proxy in a dialog. **Parameter:**

		sip.use_out_bound_in_dialog
Local	Web User Interface	Specify whether to use outbound proxy in a dialog. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

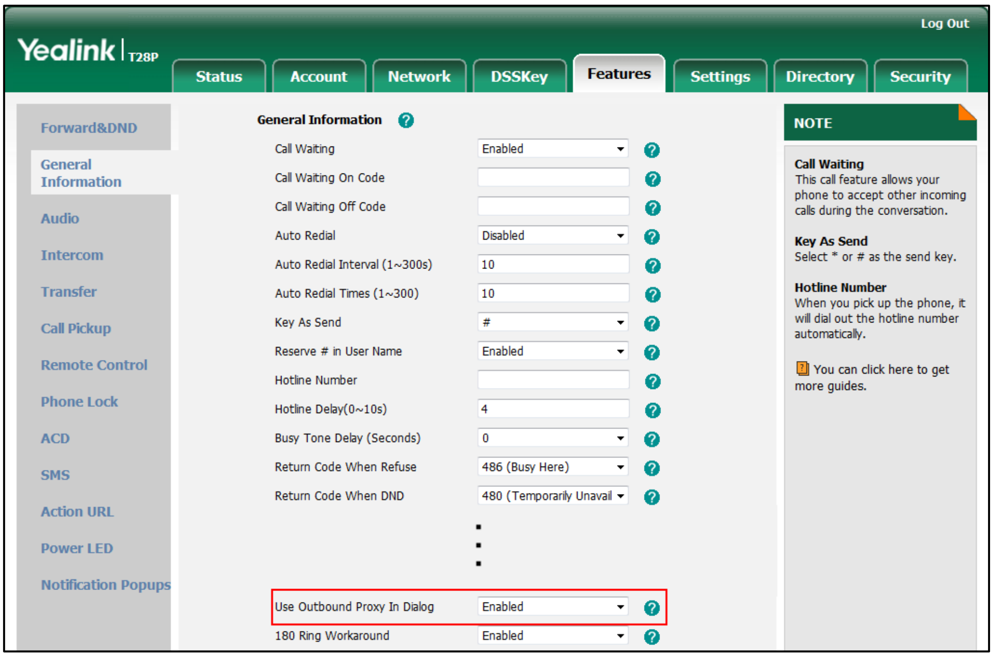
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
sip.use_out_bound_in_dialog	**0 or 1**	**1**
Description: Enables or disables the IP phone to keep sending SIP requests to the outbound proxy server in a dialog. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), all the SIP request messages from the IP phone will be forced to send to the outbound proxy server in a dialog. **Note**: If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Features->General Information->Use Outbound Proxy In Dialog **Phone User Interface:** None		

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

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

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



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

SIP Session Timer

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

Procedure

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

Configuration File	<MAC>.cfg	Configure SIP session timer. **Parameters:** account.X.advanced.timer_t1 account.X.advanced.timer_t2 account.X.advanced.timer_t4
Local	Web User Interface	Configure SIP session timer. **Navigate to:** http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=

		0

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.advanced.timer_t1	**Float from 0.5 to10**	**0.5**
Description: Configures the SIP session timer T1 (in seconds) for account X. T1 is an estimate of the Round Trip Time (RTT) of transactions between a SIP client and SIP server. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Web User Interface:** Account->Advanced->SIP Session Timer T1 (0.5~10s) **Phone User Interface:** None		
account.X.advanced.timer_t2	**Float from 2 to 40**	**4**
Description: Configures the session timer T2 (in seconds) for account X. T2 represents the maximum retransmit interval for non-INVITE requests and INVITE responses. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Web User Interface:** Account->Advanced->SIP Session Timer T2 (2~40s) **Phone User Interface:** None		
account.X.advanced.timer_t4	**Float from 2.5 to 60**	**5**

Parameters	Permitted Values	Default
Description: Configures the session timer of T4 (in seconds) for account X. T4 represents the maximum duration a message will remain in the network. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Web User Interface:** Account->Advanced->SIP Session Timer T4 (2.5~60s) **Phone User Interface:** None		

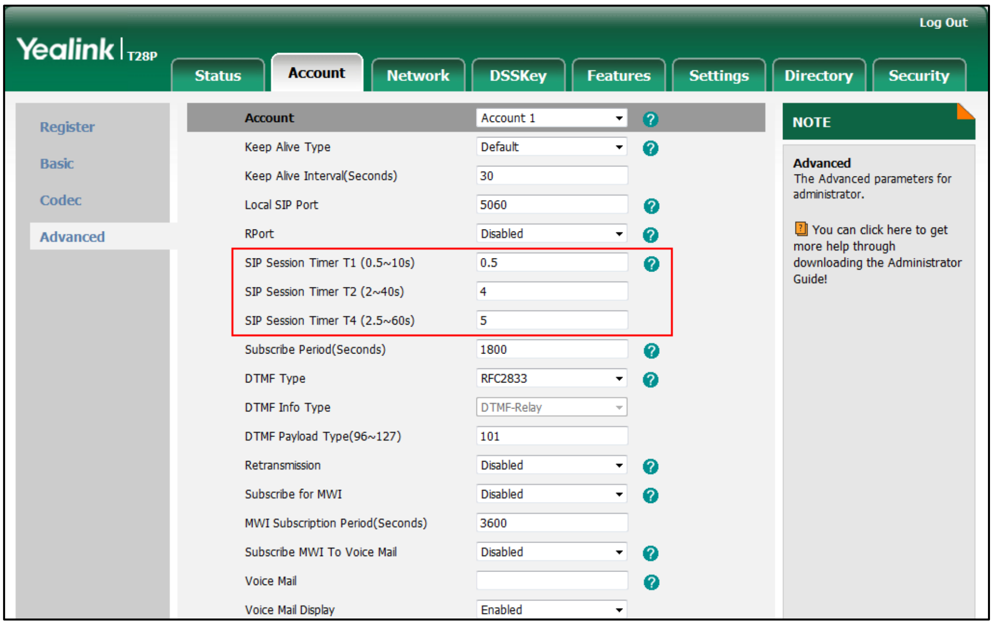
To configure session timer via web user interface:

1. Click on **Account**.
2. Select the desired account from the pull-down list of **Account**.
3. Click on **Advanced**.
4. Enter the desired value in the **SIP Session Timer T1 (0.5~10s)** field.

   The default value is 0.5s.
5. Enter the desired value in the **SIP Session Timer T2 (2~40s)** field.

   The default value is 4s.
6. Enter the desired value in the **SIP Session Timer T4 (2.5~60s)** field.

   The default value is 5s.



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

Session Timer

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

Procedure

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

Configuration File	<MAC>.cfg	Configure session timer. **Parameters:** account.X.session_timer.enable account.X.session_timer.expires account.X.session_timer.refresher
Local	Web User Interface	Configure session timer. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

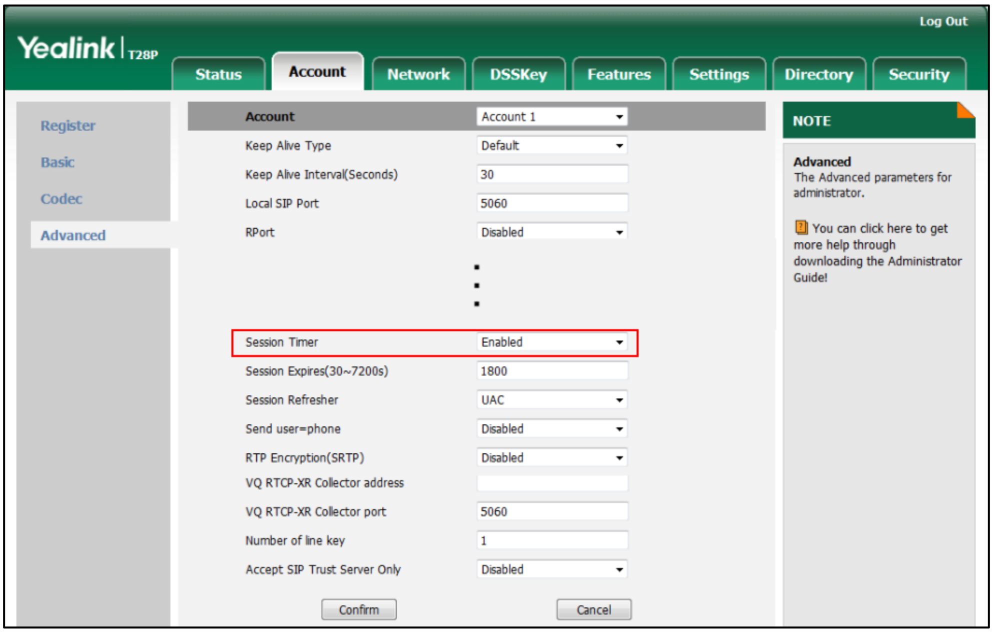
Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.session_timer.enable	**0 or 1**	**0**
Description: Enables or disables the session timer for account X. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), IP phone will send periodic re-INVITE requests to refresh the session during a call. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Web User Interface:**		

Parameters	Permitted Values	Default
Account->Advanced->Session Timer **Phone User Interface:** None		
account.X.session_timer.expires	**Integer from 30 to 7200**	**1800**
Description: Configures the IP phone to refresh the session during a call at regular intervals (in seconds) for account X. If it is set to 1800 (1800s), the IP phone will refresh the session during a call before 1800 seconds. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Example:** account.1.session_timer.expires = 1800 **Web User Interface:** Account->Advanced->Session Expires (30~7200s) **Phone User Interface:** None		
account.X.session_timer.refresher	**0 or 1**	**0**
Description: Configures the session timer refresher for account X. **0**-UAC **1**-UAS If it is set to 0 (UAC), refreshing the session is performed by the IP phone. If it is set to 1 (UAS), refreshing the session is performed by a SIP server. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Web User Interface:** Account->Advanced->Session Refresher **Phone User Interface:** None		

To configure session timer via web user interface:

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



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

Call Hold

Call hold provides a service of placing an active call on hold. When a call is placed on hold, the IP 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. IP phones support two call hold methods, one is RFC 3264, which sets the "a" (media attribute) in the SDP to sendonly, recvonly or inactive (e.g., a=sendonly). The other is RFC 2543, which sets the "c" (connection addresses for the media streams) in the SDP to zero (e.g., c=0.0.0.0). Call hold tone allows IP phones to play a warning tone at regular intervals when there is a call on hold. The warning tone is played through the speakerphone.

IP phones also support Music on Hold (MoH) feature. MoH is the business practice of playing recorded music to fill the silence that would be heard by the party who has been placed on hold. To use this feature, specify a SIP URI pointing to a MoH server account. When a call is placed on hold, the IP phone will send an INVITE message to the specified MoH server account according to the SIP URI. The MoH server account automatically responds to the INVITE message and immediately plays audio from some source located anywhere (LAN, Internet) to the held party.

Procedure

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

Configuration File	<y0000000000xx>.cfg	Configure the call hold tone and call hold tone delay. **Parameters:** features.play_hold_tone.enable features.play_hold_tone.delay Specify whether RFC 2543 (c=0.0.0.0) outgoing hold signaling is used. **Parameter:** sip.rfc2543_hold
	<MAC>.cfg	Configure MoH on a per-line basis. **Parameter:** account.X.music_server_uri
Local	Web User Interface	Configure the call hold tone and call hold tone delay. Specify whether RFC 2543 (c=0.0.0.0) outgoing hold signaling is used. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load Configure MoH on a per-line basis. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

Details of Configuration Parameters:

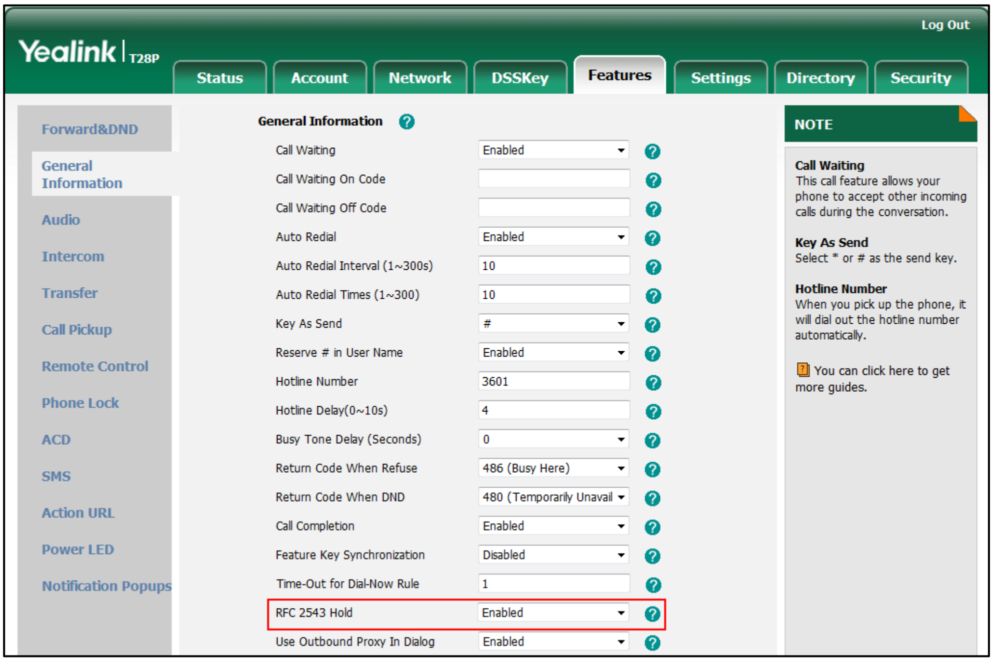
Parameters	Permitted Values	Default
features.play_hold_tone.enable	**0 or 1**	**1**

Parameters	Permitted Values	Default
Description: Enables or disables the IP phone to play a tone when there is a call on hold. **0**-Disabled **1**-Enabled **Web User Interface:** Features->General Information->Play Hold Tone **Phone User Interface:** None		
features.play_hold_tone.delay	**Integer from 3 to 3600**	**30**
Description: Configures the interval (in seconds) at which the IP phone plays a hold tone. If it is set to 30 (30s), the IP phone will play a hold tone every 30 seconds when there is a hold call on the IP phone. **Note:** It works only if the parameter "features.play_hold_tone.enable" is set to 1 (Enabled). **Web User Interface:** Features->General Information->Play Hold Tone Delay **Phone User Interface:** None		
sip.rfc2543_hold	**0 or 1**	**0**
Description: Enables or disables the IP phone to use RFC 2543 (c=0.0.0.0) outgoing hold signaling. **0**-Disabled **1**-Enabled 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. 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. **Web User Interface:** Features->General Information->RFC 2543 Hold **Phone User Interface:** None		

Parameters	Permitted Values	Default
account.X.music_server_uri	SIP URI within 256 characters	Blank
Description: Configures the address of the Music On Hold server for account X. Examples for valid values: <10.1.3.165>, 10.1.3.165, sip:moh@sip.com, <sip:moh@sip.com>, <yealink.com> or yealink.com. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Example:** account.1.music_server_uri = sip:moh@sip.com **Note**: The DNS query in this parameter only supports A query. **Web User Interface:** Account->Advanced->Music Server URI **Phone User Interface:** None		

To configure call hold method via web user interface:

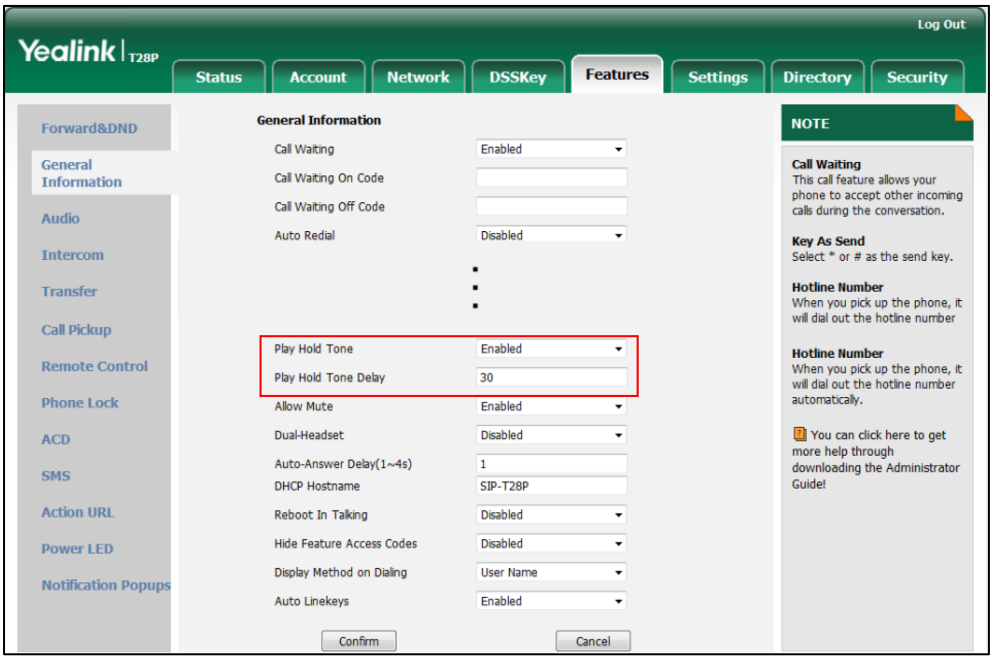
1. Click on **Features->General Information**.
2. Select the desired value from the pull-down list of **RFC 2543 Hold**.



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

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

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

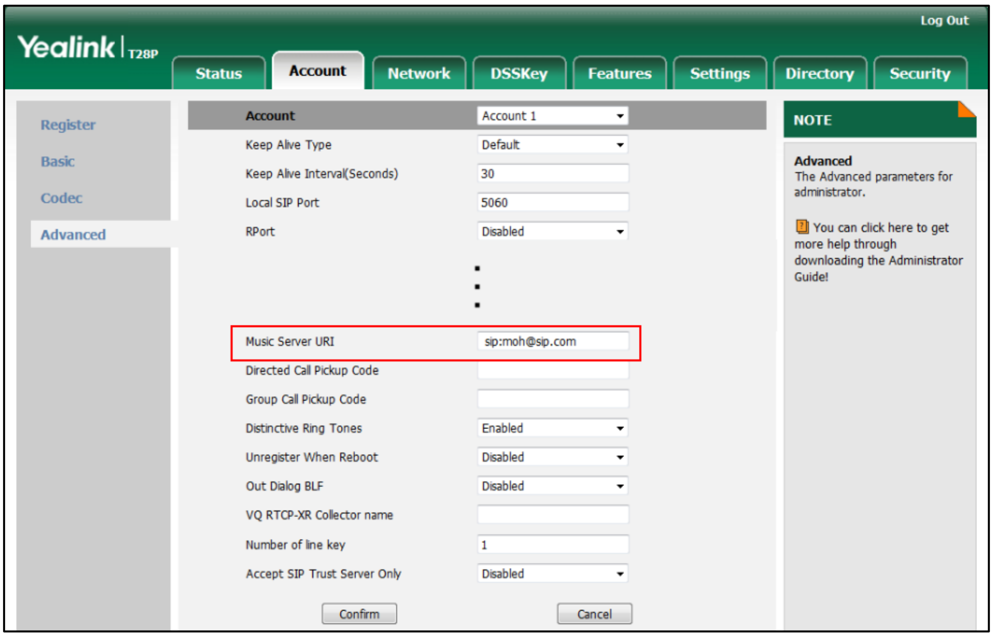


4. Click **Confirm** to accept the change.

To configure MoH via web user interface:

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

4. Enter the SIP URI (e.g., sip:moh@sip.com) in the **Music Server URI** field.



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

Call Forward

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

- **Always Forward** -- Forward the incoming call immediately.
- **Busy Forward** -- Forward the incoming call when the IP 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 following describes the call forward modes:

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

The server-side call forward settings disable the local call forward settings. If the server-side call forward feature is enabled on any of the IP phone's registrations, the other registrations are not affected. DND activated on the IP phone disables the local no answer forward settings.

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

IP phones support the redirected call information sent by the SIP server with Diversion header, per draft-levy-sip-diversion-08, or History-info header, per RFC 4244. The Diversion/History-info header is used to inform the IP phone of a call’s history. For example, when a phone has been set to enable call forward, the Diversion/History-info header allows the receiving phone to indicate who the call was from, and from which phone number it was forwarded.

Forward International

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

Procedure

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

Configuration File	<MAC>.cfg	Configure call forward in custom mode. **Parameters:** 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
	<y0000000000xx>.cfg	Configure the call forward mode. **Parameter:** features.fwd_mode Configure call forward in phone mode. **Parameters:** forward.always.enable forward.always.target forward.always.on_code

		forward.always.off_code forward.busy.enable forward.busy.target forward.busy.on_code forward.busy.off_code forward.no_answer.enable forward.no_answer.target forward.no_answer.timeout forward.no_answer.on_code forward.no_answer.off_code Configure diversion/history-info feature. **Parameter:** features.fwd_diversion_enable Configure forward international. **Parameter:** forward.international.enable
Local	Web User Interface	Configure call forward. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-forward&q=load Configure diversion/history-info feature. Configure forward international. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load
	Phone User Interface	Configure call forward. Configure forward international.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.always_fwd.enable	**0 or 1**	**0**
Description: Enables or disables always forward feature for account X when the call forward mode is configured as Custom. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), incoming calls to the account X are forwarded to the destination number immediately. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Web User Interface:** Features->Forward& DND->Forward->Always Forward->On/Off **Phone User Interface:** Menu->Features->Call Forward->Always Forward->Always Forward		
account.X.always_fwd.target	**String within 32 characters**	**Blank**
Description: Configures the destination number of the always forward for account X when the call forward mode is configured as Custom. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Example:** account.1.always_fwd.target = 3601 **Web User Interface:** Features->Forward& DND->Forward->Always Forward->Target **Phone User Interface:** Menu->Features->Call Forward->Always Forward->Forward to		
account.X.always_fwd.on_code	**String within 32 characters**	**Blank**
Description: Configures the always forward on code to activate the server-side always forward		

Parameters	Permitted Values	Default
feature for account X when the call forward mode is configured as Custom. The IP 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 phone. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Example:** account.1.always_fwd.on_code = *72 **Web User Interface:** Features->Forward& DND->Forward->Always Forward->On Code **Phone User Interface:** Menu->Features->Call Forward->Always Forward->On Code		
account.X.always_fwd.off_code	**String within 32 characters**	**Blank**
Description: Configures the always forward off code to deactivate the server-side always forward feature for account X when the call forward mode is configured as Custom. The IP phone will send the always forward off code to the server when you deactivate always forward feature for account X on the IP phone. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Example:** account.1.busy_fwd.off_code = *73 **Web User Interface:** Features->Forward& DND->Forward->Always Forward ->Off Code **Phone User Interface:** Menu->Features->Call Forward->Always Forward->Off Code		
account.X.busy_fwd.enable	**0 or 1**	**0**

Parameters	Permitted Values	Default
Description: Enables or disables busy forward feature for account X when the call forward mode is configured as Custom. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), incoming calls to the account X are forwarded to the destination number when the callee is busy. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Web User Interface:** Features->Forward& DND->Forward->Busy Forward->On/Off **Phone User Interface:** Menu->Features->Call Forward->Busy Forward->Busy Forward		
account.X.busy_fwd.target	**String within 32 characters**	**Blank**
Description: Configures the destination number of the busy forward for account X when the call forward mode is configured as Custom. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Example:** account.1.busy_fwd.target = 3602 **Web User Interface:** Features->Forward& DND->Forward->Busy Forward->Target **Phone User Interface:** Menu->Features->Call Forward->Busy Forward->Forward to		
account.X.busy_fwd.on_code	**String within 32 characters**	**Blank**

Parameters	Permitted Values	Default
Description: Configures the busy forward on code to activate the server-side busy forward feature for account X when the call forward mode is configured as Custom. The IP 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 phone. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Example:** account.1.busy_fwd.on_code = *74 **Web User Interface:** Features->Forward& DND->Forward->No Answer Forward->On Code **Phone User Interface:** Menu->Features->Call Forward->Busy Forward->On Code		
account.X.busy_fwd.off_code	**String within 32 characters**	**Blank**
Description: Configures the busy forward off code to deactivate the server-side busy forward feature for account X when the call forward mode is configured as Custom. The IP phone will send the busy forward off code to the server when you deactivate busy forward feature for account X on the IP phone. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Example:** account.1.busy_fwd.off_code = *75 **Web User Interface:** Features->Forward& DND->Forward->No Answer Forward ->Off Code **Phone User Interface:** Menu->Features->Call Forward->Busy Forward->Off Code		
account.X.timeout_fwd.enable	**0 or 1**	**0**

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td colspan="3">Description:
Enables or disables no answer forward feature for account X when the call forward mode is configured as Custom.
0-Disabled
1-Enabled
If it is set to 1 (Enabled), incoming calls to the account X are forwarded to the destination number after a period of ring time.
X ranges from 1 to 6 (for SIP-T28P).
X ranges from 1 to 3 (for SIP-T26P/T22P).
X ranges from 1 to 2 (for SIP-T20P).
Web User Interface:
Features->Forward& DND->Forward->No Answer Forward->On/Off
Phone User Interface:
Menu->Features->Call Forward->No Answer Forward->No Answer Forward</td></tr>
<tr><td>account.X.timeout_fwd.target</td><td>String within 32 characters</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the destination number of the no answer forward for account X when the call forward mode is configured as Custom.
X ranges from 1 to 6 (for SIP-T28P).
X ranges from 1 to 3 (for SIP-T26P/T22P).
X ranges from 1 to 2 (for SIP-T20P).
Example:
account.1.timeout_fwd.target = 3603
Web User Interface:
Features->Forward& DND->Forward->No Answer Forward->Target
Phone User Interface:
Menu->Features->Call Forward->No Answer Forward->Forward to</td></tr>
<tr><td>account.X.timeout_fwd.timeout</td><td>Integer from 0 to 20</td><td>2</td></tr>
</table>

Parameters	Permitted Values	Default
Description: Configures ring times (N) to wait before forwarding incoming calls for account X when the call forward mode is configured as Custom. Incoming calls will be forwarded when not answered after N*6 seconds. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Web User Interface:** Features->Forward& DND->Forward->No Answer Forward->After Ring Time **Phone User Interface:** Menu->Features->Call Forward->No Answer Forward->After Ring Time		
account.X.timeout_fwd.on_code	**String within 32 characters**	**Blank**
Description: Configures the no answer forward on code to activate the server-side no answer forward feature for account X when the call forward mode is configured as Custom. The IP 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 phone. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Example:** account.1.timeout_fwd.on_code = *76 **Web User Interface:** Features->Forward& DND->Forward->No Answer Forward ->On Code **Phone User Interface:** Menu->Features->Call Forward->No Answer Forward->On Code		
account.X.timeout_fwd.off_code	**String within 32 characters**	**Blank**

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td colspan="3">Description:
Configures the no answer forward off code to deactivate the server-side no answer forward feature for account X when the call forward mode is configured as Custom. The IP 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 phone.
X ranges from 1 to 6 (for SIP-T28P).
X ranges from 1 to 3 (for SIP-T26P/T22P).
X ranges from 1 to 2 (for SIP-T20P).
Example:
account.1.timeout_fwd.off_code = *77
Web User Interface:
Features->Forward& DND->Forward->No Answer Forward ->Off Code
Phone User Interface:
Menu->Features->Call Forward->No Answer Forward->Off Code</td></tr>
<tr><td>features.fwd_mode</td><td>0 or 1</td><td>0</td></tr>
<tr><td colspan="3">Description:
Configures the call forward mode for the IP phone.
0-Phone
1-Custom
If it is set to 0 (Phone), call forward feature is effective for the IP phone.
If it is set to 1 (Custom), you can configure call forward feature for each account.
Web User Interface:
Features->Forward&DND->Forward->Forward->Mode
Phone User Interface:
None</td></tr>
<tr><td>forward.always.enable</td><td>0 or 1</td><td>0</td></tr>
</table>

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td colspan="3">Description:
Enables or disables always forward feature.
0-Disabled
1-Enabled
If it is set to 1 (Enabled), incoming calls are forwarded to the destination number immediately.
Web User Interface:
Features->Forward &DND->Forward->Always Forward->On/Off
Phone User Interface:
Menu->Features->Call Forward->Always Forward->Always Forward</td></tr>
<tr><td>forward.always.target</td><td>String within 32 characters</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the destination number the IP phone forwards all incoming calls to.
Web User Interface:
Features->Forward &DND->Forward->Always Forward->Target
Phone User Interface:
Menu->Features->Call Forward->Always Forward->Forward to</td></tr>
<tr><td>forward.always.on_code</td><td>String within 32 characters</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the always forward on code to activate the server-side always forward feature. The IP phone will send the always forward on code and the pre-configured destination number to the server when you activate always forward feature on the IP phone.
Example:
forward.always.on_code = *72
Web User Interface:
Features->Forward &DND->Forward->Always Forward->On Code
Phone User Interface:
Menu->Features->Call Forward->Always Forward->On Code</td></tr>
<tr><td>forward.always.off_code</td><td>String within 32 characters</td><td>Blank</td></tr>
</table>

Parameters	Permitted Values	Default
Description: Configures the always forward off code to deactivate the server-side always forward feature. The IP phone will send the always forward off code to the server when you deactivate always forward feature on the IP phone. **Example:** forward.always.off_code = *73 **Web User Interface:** Features->Forward &DND->Always Forward->Off Code **Phone User Interface:** Menu->Features->Call Forward->Always Forward->Off Code		
forward.busy.enable	**0 or 1**	**0**
Description: Enables or disables busy forward feature. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), incoming calls are forwarded to the destination number when the callee is busy. **Web User Interface:** Features->Forward &DND->Forward->Busy Forward->On/Off **Phone User Interface:** Menu->Features->Call Forward->Busy Forward->Busy Forward		
forward.busy.target	**String within 32 characters**	**Blank**
Description: Configures the destination number the IP phone forwards incoming calls to when busy. **Example:** forward.busy.target = 3602 **Web User Interface:** Features->Forward &DND->Forward->Busy Forward->Target **Phone User Interface:** Menu->Features->Call Forward->Busy Forward->Forward to		
forward.busy.on_code	**String within 32 characters**	**Blank**

Parameters	Permitted Values	Default
Description: Configures the busy forward on code to activate the server-side busy forward feature. The IP phone will send the busy forward on code and the pre-configured destination number to the server when you activate busy forward feature on the IP phone. **Example:** forward.busy.on_code = *74 **Web User Interface:** Features->Forward &DND->Forward->Busy Forward->On Code **Phone User Interface:** Menu->Features->Call Forward->Busy Forward->On Code		
forward.busy.off_code	**String within 32 characters**	**Blank**
Description: Configures the busy forward off code to deactivate the server-side busy forward feature. The IP phone will send the busy forward off code to the server when you deactivate busy forward feature on the IP phone. **Example:** forward.busy.off_code = *75 **Web User Interface:** Features->Forward &DND->Forward->Busy Forward->Off Code **Phone User Interface:** Menu->Features->Call Forward->Busy Forward->Off Code		
forward.no_answer.enable	**0 or 1**	**0**
Description: Enables or disables no answer forward feature. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), incoming calls are forwarded to the destination number after a period of ring time. **Web User Interface:** Features->Forward &DND->Forward->No Answer Forward->On/Off **Phone User Interface:** Menu->Features->Call Forward->No Answer Forward->No Answer Forward		

Parameters	Permitted Values	Default
forward.no_answer.target	**String within 32 characters**	**Blank**
Description: Configures the destination number the IP phone forwards incoming calls to after a period of ring time. **Example:** forward.no_answer.target = 3603 **Web User Interface:** Features->Forward &DND->Forward->No Answer Forward->Target **Phone User Interface:** Menu->Features->Call Forward->No Answer Forward->Forward to		
forward.no_answer.timeout	**Integer from 0 to 20**	**2**
Description: Configures ring times (N) to wait before forwarding incoming calls. Incoming calls will be forwarded when not answered after N*6 seconds. **Web User Interface:** Features->Forward &DND->Forward->No Answer Forward->After Ring Time (0~120s) **Phone User Interface:** Menu->Features->Call Forward->No Answer Forward->After Ring Time		
forward.no_answer.on_code	**String within 32 characters**	**Blank**
Description: Configures the no answer forward on code to activate the server-side no answer forward feature. The IP 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 on the IP phone. **Example:** forward.no_answer.on_code = *76 **Web User Interface:** Features->Forward &DND->Forward->No Answer Forward->On Code **Phone User Interface:** Menu->Features->Call Forward->No Answer Forward->On Code		

Parameters	Permitted Values	Default
forward.no_answer.off_code	**String within 32 characters**	**Blank**
Description: Configures the no answer forward off code to deactivate the server-side no answer forward feature. The IP phone will send the no answer forward off code to the server when you deactivate no answer forward feature on the IP phone. **Example:** forward.no_answer.off_code = *77 **Web User Interface:** Features->Forward &DND->Forward->No Answer Forward->Off Code **Phone User Interface:** Menu->Features->Call Forward->No Answer Forward->Off Code		
features.fwd_diversion_enable	**0 or 1**	**1**
Description: Enables or disables the IP phone to present the diversion information when an incoming call is forwarded to your IP phone. **0**-Disabled **1**-Enabled **Web User Interface:** Features->General Information->Diversion/History-Info **Phone User Interface:** None		
forward.international.enable	**0 or 1**	**1**
Description: Enables or disables the IP phone to forward incoming calls to international numbers (the prefix is 00). **0**-Disabled **1**-Enabled **Web User Interface:** Features->General Information->Fwd International **Phone User Interface:** Menu->Settings->Advanced Settings (default password: admin)->Forward Intl		

To configure call forward via web user interface:

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

2. In the **Forward** block, mark the desired radio box in the **Mode** field.

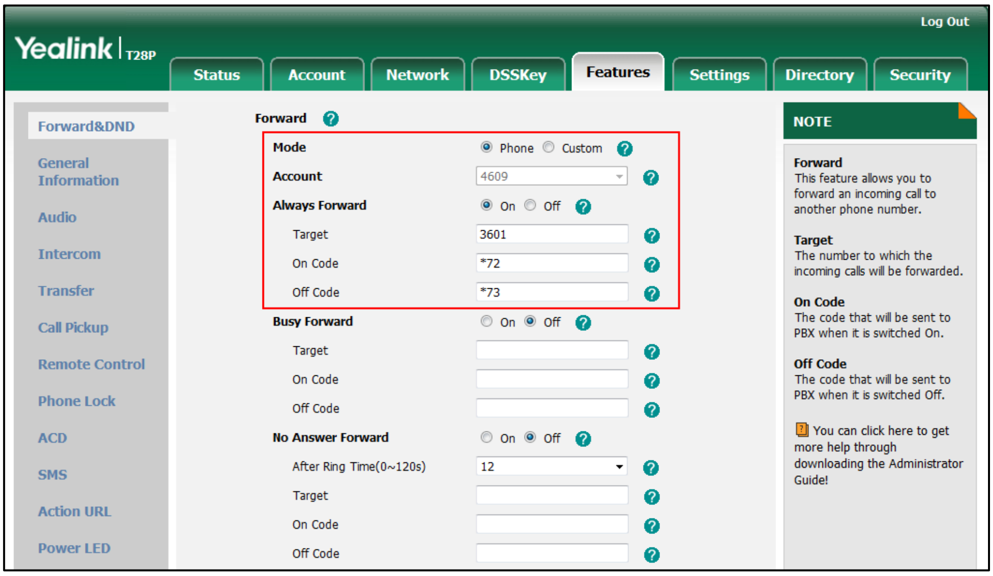
   a) If you mark the **Phone** radio box:

   1) Mark the desired radio box in the **Always/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).



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

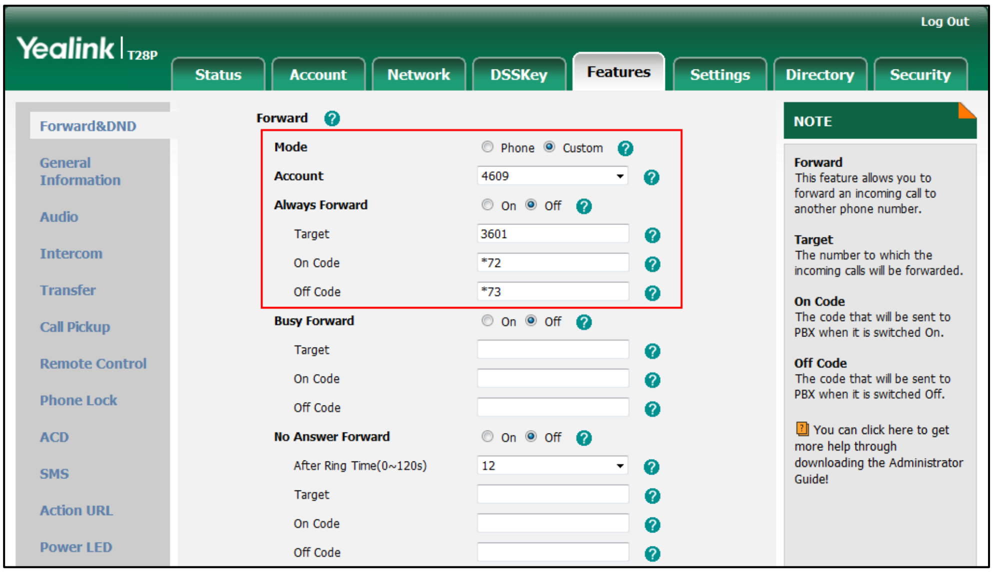
   1) Select the desired account from the pull-down list of **Account**.

   2) Mark the desired radio box in the **Always/Busy/No Answer Forward** field.

   3) Enter the destination number you want to forward in the **Target** field.

   4) Enter the on code and off code in the **On Code** and **Off Code** fields.

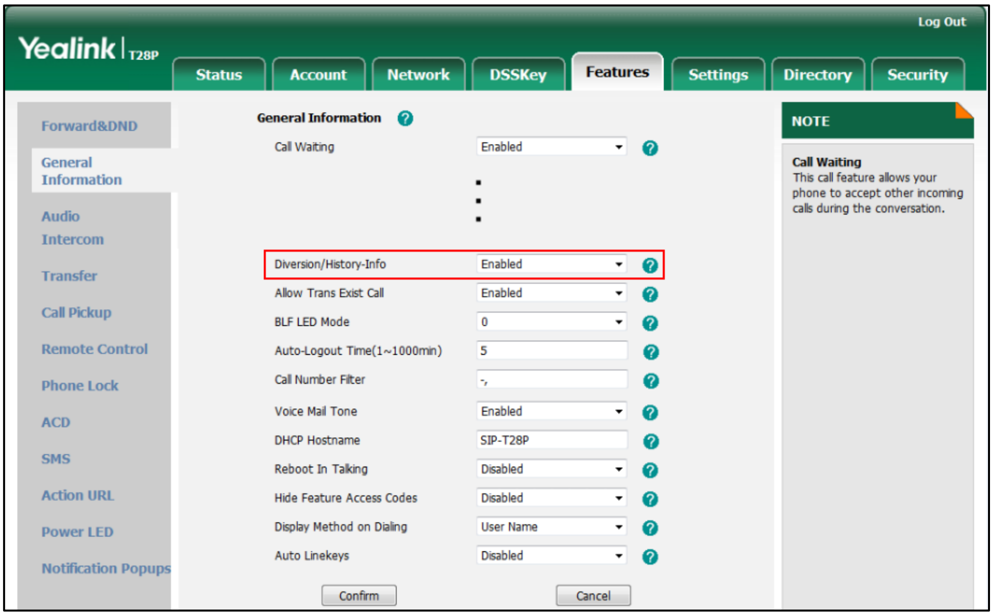
5) Select the ring time to wait before forwarding from the pull-down list of **After Ring Time (0~120s)** (only for the no answer forward).



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

To configure Diversion/History-Info feature via web user interface:

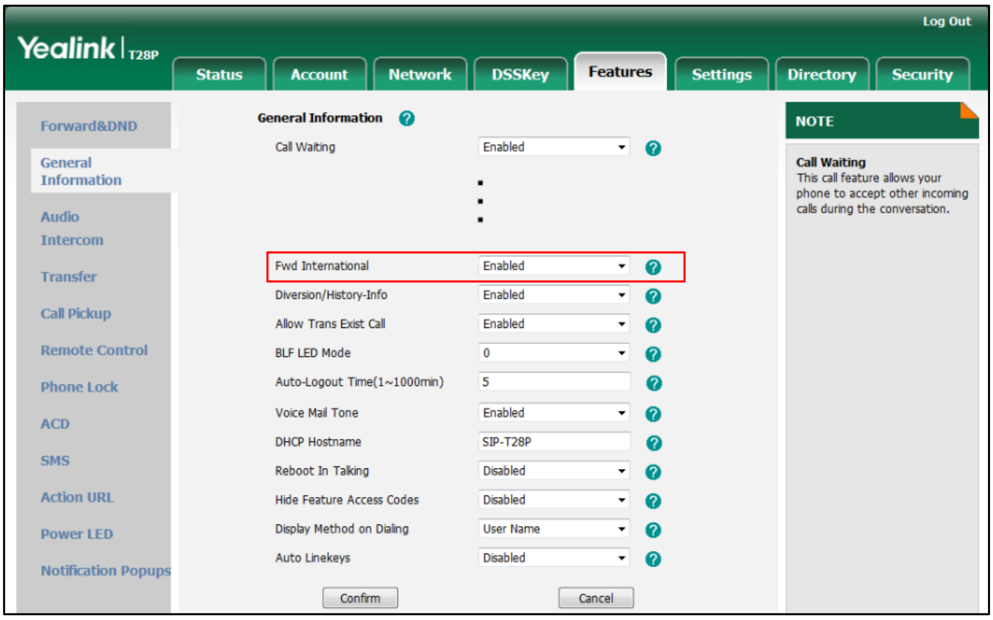
1. Click on **Features**->**General Information**.
2. Select the desired value from the pull-down list of **Diversion/History-Info**.



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 configure call forward in phone mode via phone user interface:

1. Press **Menu**->**Features**->**Call Forward**.
2. Press or to select the desired forwarding type, and then press the **Enter** soft key.
3. Depending on your selection:

   a) If you select **Always Forward**:

   1) Press or , or the **Switch** soft key to select the desired value from the **Always Forward** field.

   2) Enter the destination number you want to forward all incoming calls to in the **Forward to** field.

   3) (Optional.) Enter the always forward on code and off code respectively in the **On Code** and **Off Code** fields.

   b) If you select **Busy Forward**:

   1) Press or , or the **Switch** soft key to select the desired value from the **Busy Forward** field.

   2) Enter the destination number you want to forward all incoming calls to when the IP phone is busy in the **Forward to** field.

   3) (Optional.) Enter the busy forward on code and off code respectively in the **On Code** and **Off Code** fields.

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

1) Press or , or the **Switch** soft key to select the desired value from the **No Answer Forward** field.

2) Enter the destination number you want to forward all unanswered incoming calls to in the **Forward to** field.

3) Press or , or the **Switch** soft key to select the ring time to wait before forwarding from the **After Ring Time** field.

The default ring time is 12 seconds.

4) (Optional.) Enter the no answer forward on code and off code respectively in the **On Code** and **Off Code** fields.

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

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

1. Press **Menu**->**Features**->**Call Forward**.
2. Press or to select the desired account, and then press the **Enter** soft key.
3. Press or to select the desired forwarding type, and then press the **Enter** soft key.
4. Depending on your selection:

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

1) Press or , or the **Switch** soft key to select the desired value from the **Always Forward** field.

2) Enter the destination number you want to forward all incoming calls to in the **Forward to** field.

3) (Optional.) Enter the always forward on code and off code respectively in the **On Code** and **Off Code** fields.

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

1) Press or to highlight the **Always Forward** field.

2) Press the **All Lines** soft key.

The LCD screen prompts "Copy to All Lines?".

3) Press the **OK** soft key to accept the change.

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

1) Press or , or the **Switch** soft key to select the desired value from the **Busy Forward** field.

2) Enter the destination number you want to forward all incoming calls to when the IP phone is busy in the **Forward to** field.

3) (Optional.) Enter the busy forward on code and off code respectively in the **On Code** and **Off Code** fields.

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

1) Press or to highlight the **Busy Forward** field.

2) Press the **All Lines** soft key.

The LCD screen prompts "Copy to All Lines?".

3) Press the **OK** soft key to accept the change.

c) If you select **No Answer Forward**, you can configure it for a specific account.

1) Press or , or the **Switch** soft key to select the desired value from the **No Answer Forward** field.

2) Enter the destination number you want to forward all unanswered incoming calls to in the **Forward to** field.

3) Press or , or the **Switch** soft key to select the ring time to wait before forwarding from the **After Ring Time** field

The default ring time is 12 seconds.

4) (Optional.) Enter the no answer forward on code and off code respectively in the **On Code** and **Off Code** fields.

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

1) Press or to highlight the **No Answer Forward** field.

2) Press the **All Lines** soft key.

The LCD screen prompts "Copy to All Lines?".

3) Press the **OK** soft key to accept the change.

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

To configure forward international via phone user interface:

1. Press **Menu**->**Settings**->**Advanced Settings** (default password: admin) ->**FWD International.**
2. Press or , or the **Switch** soft key to select the desired type from the **FWD International** field.
3. Press the **Save** soft key to accept the change.

Call Transfer

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

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

Semi-attended transfer is implemented by a REFER method with Replaces in the Refer-To header.

- **Attended Transfer** -- Transfer a call with prior consulting. Attended transfer is implemented by a REFER method with Replaces in the Refer-To header.

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

When a user performs a semi-attended transfer, semi-attended transfer feature determines whether to display the prompt "**n New Missed Call(s)**" ("n" indicates the number of the missed calls) on the destination party's phone LCD screen.

Procedure

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

Configuration File	<y0000000000xx>.cfg	Specify whether to complete the transfer through on-hook. **Parameters:** transfer.blind_tran_on_hook_enable transfer.on_hook_trans_enable Configure semi-attended transfer feature. **Parameter:** transfer.semi_attend_tran_enable
Local	Web User Interface	Specify whether to complete the transfer through on-hook. Configure semi-attended transfer feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-transfer&q=load

Details of Configuration Parameters:

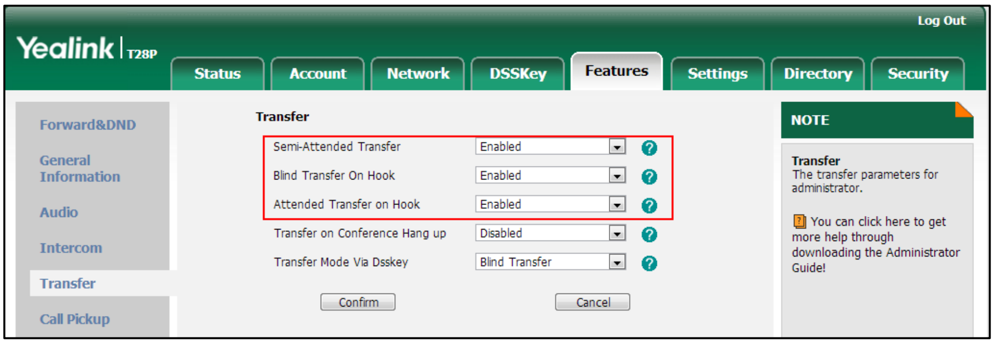
Parameters	Permitted Values	Default
transfer.blind_tran_on_hook_enable	**0 or 1**	**1**

Parameters	Permitted Values	Default
Description: Enables or disables the IP phone to complete the blind transfer through on-hook besides pressing the Transfer/Tran soft key or TRAN/TRANSFER key. **0**-Disabled **1**-Enabled **Web User Interface:** Features->Transfer->Blind Transfer On Hook **Phone User Interface:** None		
transfer.on_hook_trans_enable	**0 or 1**	**1**
Description: Enables or disables the IP phone to complete the semi-attended/attended transfer through on-hook besides pressing the Transfer/Tran soft key or TRAN/TRANSFER key. **0**-Disabled **1**-Enabled **Web User Interface:** Features->Transfer ->Attended Transfer On Hook **Phone User Interface:** None		
transfer.semi_attend_tran_enable	**0 or 1**	**1**
Description: Enables or disables the transferee party's phone to prompt a missed call on the LCD screen before displaying the caller ID when performing a semi-attended transfer. **0**-Disabled **1**-Enabled **Web User Interface:** Features->Transfer ->Semi-Attended Transfer **Phone User Interface:** 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). IP phones implement network conference using the REFER method specified in RFC 4579. This feature depends on support from a SIP server.

Procedure

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

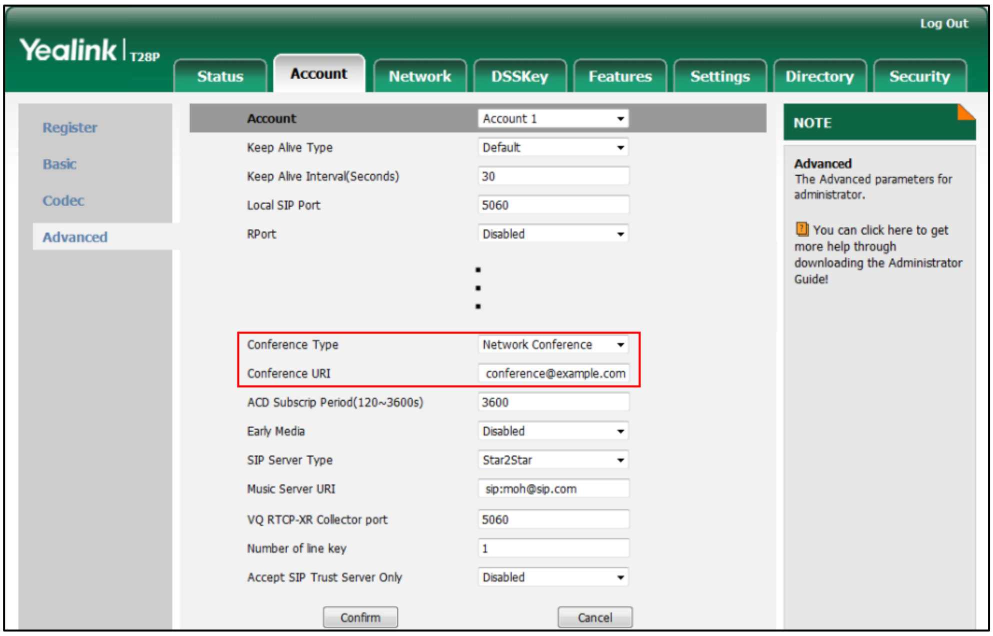
Configuration File	<MAC>.cfg	Configure network conference. **Parameters:** account.X.conf_type account.X.conf_uri
Local	Web User Interface	Configure network conference. **Navigate to:** http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.conf_type	0 or 2	0
Description: Configures the network conference type for account X. **0**-Local Conference **2**-Network Conference If it is set to 0 (Local Conference), conferences are set up on the IP phone locally. If it is set to 2 (Network Conference), conferences are set up by the server. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Web User Interface:** Account->Advanced->Conference Type **Phone User Interface:** None		
account.X.conf_uri	SIP URI within 511 characters	Blank
Description: Configures the network conference URI for account X. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Example:** account.1.conf_uri = conference@example.com **Note**: It works only if the parameter "account.X.conf_type" is set to 2 (Network Conference). **Web User Interface:** Account->Advanced->Conference URI **Phone User Interface:** None		

To configure the network conference via web user interface:

1. Click on **Account**.
2. Select the desired account from the pull-down list of **Account**.
3. Click on **Advanced**.
4. Select **Network Conference** from the pull-down list of **Conference Type**.
5. Enter the conference URI in the **Conference URI** field.



6. 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 phone and the server:

- Do Not Disturb (DND)
- Call Forwarding Always (CFA)
- Call Forwarding Busy (CFB)
- Call Forwarding No Answer (CFNA)

Note

Feature key synchronization is applicable to IP phones running firmware version 73 or later.

Procedure

Feature key synchronization can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure feature key synchronization. **Parameters:** bw.feature_key_sync
Local	Web User Interface	Configure network conference. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

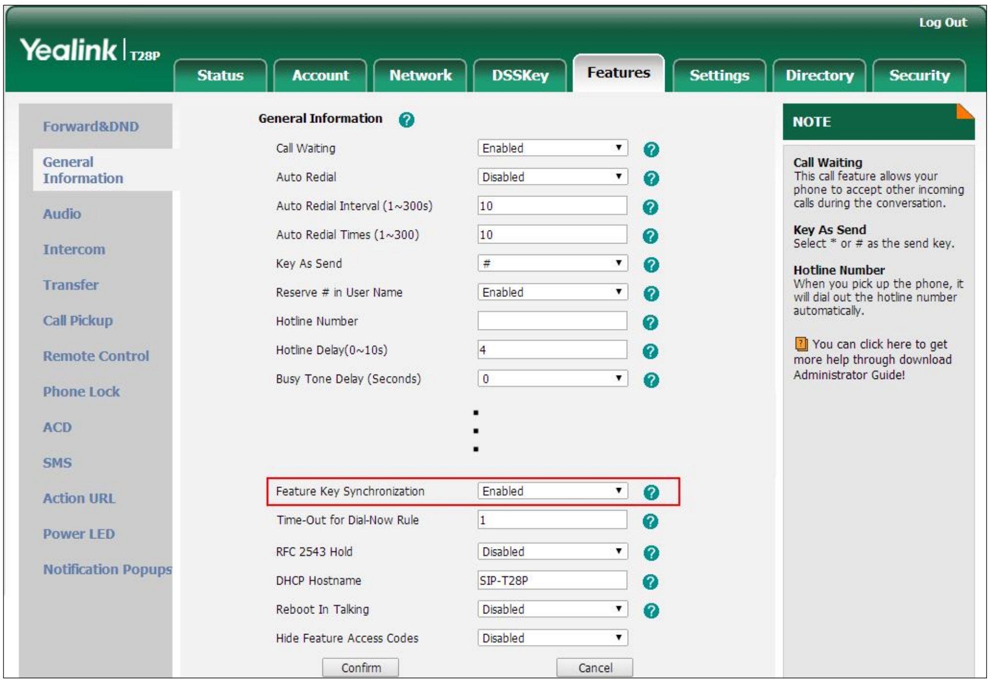
Details of Configuration Parameter:

Parameters	Permitted Values	Default
bw.feature_key_sync	**0 or 1**	**0**
Description: Enables or disables feature key synchronization. **0**-Disabled **1**-Enabled **Web User Interface:** Features->General Information->Feature Key Synchronization **Phone User Interface:** None		

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.

Transfer on Conference Hang Up

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

Procedure

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

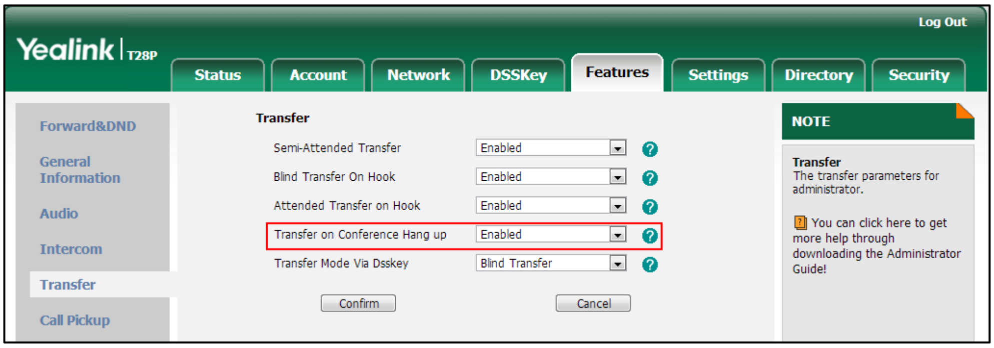
Configuration File	<y0000000000xx>.cfg	Configure the transfer on conference hang up. **Parameter:** transfer.tran_others_after_conf_enable
Local	Web User Interface	Configure the transfer on conference hang up. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-transfer&q=load

Details of the Configuration Parameter:

Parameter & Description	Permitted Values	Default
transfer.tran_others_after_conf_enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to transfer the local conference call to the two parties after the conference initiator drops the local conference call. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the other two parties remain connected when the conference initiator drops the conference call. **Note**: It is only applicable to the local conference. **Web User Interface:** Features->Transfer ->Transfer on Conference Hang up **Phone User Interface:** None		

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

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



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

Directed Call Pickup

Directed call pickup is used for picking up an incoming call on a specific extension. A user can pick up the incoming call using a directed pickup key or the DPickup soft key (not applicable to SIP-T20P IP phones). This feature depends on support from a SIP server. For many SIP servers, directed call pickup requires a directed pickup code, which can be configured on a phone or a per-line basis.

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

Procedure

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

Configuration File	<MAC>.cfg	Configure the directed call pickup code on a per-line basis. **Parameter:** account.X.direct_pickup_code
	<y0000000000xx>.cfg	Configure directed call pickup features on a phone basis. **Parameters:** features.pickup.direct_pickup_enable features.pickup.direct_pickup_code Assign a directed call pickup key. **Parameters:** memorykey.X.type/ linekey.X.type/ programablekey.X.type memorykey.X.line/ linekey.X.line/ programablekey.X.line memorykey.X.value/ linekey.X.value/ programablekey.X.value
Local	Web User Interface	Assign a directed call pickup key. **Navigate to:**

		http://<phoneIPAddress>/servlet?p=dsskey&q=load&model=0 Configure directed call pickup feature on a phone basis. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-callpickup&q=load Configure directed call pickup code on a per-line basis. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0
	Phone User Interface	Assign a directed call pickup key.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.direct_pickup_code	**String within 32 characters**	**Blank**
Description : Configures the directed call pickup code for account X. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Example:** account.1.direct_pickup_code = *68 **Note**: The directed call pickup code configured on a per-line basis takes precedence over that configured on a phone basis. **Web User Interface:** Account->Advanced->Directed Call Pickup Code **Phone User Interface:** None		
features.pickup.direct_pickup_enable	**0 or 1**	**0**

Parameters	Permitted Values	Default
Description: Enables or disables the IP phone to display the DPickup soft key when the IP phone is in the pre-dialing screen. **0**-Disabled **1**-Enabled **Note**: It is not applicable to SIP-T20P IP phones. **Web User Interface:** Features->Call Pickup->Directed Call Pickup **Phone User Interface:** None		
features.pickup.direct_pickup_code	**String within 32 characters**	**Blank**
Description: Configures the directed call pickup code on a phone basis. **Example:** features.pickup.direct_pickup_code = *97 **Note**: The directed call pickup code configured on a per-line basis takes precedence over that configured on a phone basis. **Web User Interface:** Features->Call Pickup->Directed Call Pickup Code **Phone User Interface:** None		

Directed Call Pickup Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 513.

Parameters	Permitted Values	Default
memorykey.X.type/ linekey.X.type/ programablekey.X.type	**9**	**Refer to the following content**
Description: Configures a DSS key as a directed call pickup key on the IP phone. The digit **9** stands for the key type **Directed Pickup**. For memory keys:		

Parameters	Permitted Values	Default
X ranges from 1 to 10 (for SIP-T28/T26P). For line keys: X ranges from 1 to 6 (for SIP-T28P) X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). For programable keys: X ranges from 1 to 14 (for SIP-T28/T26P) X=1-10, 14 (for SIP-T22P) X=5-12, 14 (for SIP-T20P) **Example:** memorykey.1.type = 9 **Default:** For memory keys: The default value is 0. For line keys: The default value is 15. For programable keys: **For SIP-T28P/T26P IP phones:** When X=1, the default value is 28 (History). When X=2, the default value is 61 (Directory). When X=3, the default value is 5 (DND). When X=4, the default value is 30 (Menu). When X=5, the default value is 28 (History). When X=6, the default value is 61 (Directory). When X=7, the default value is 31 (Switch Account). When X=8, the default value is 31 (Switch Account). When X=9, the default value is 33 (Status). When X=10, the default value is 0 (NA). When X=11, the default value is 0 (NA). When X=12, the default value is 0 (NA). When X=13, the default value is 0 (NA). When X=14, the default value is 2 (Forward). **For SIP-T22P IP phones:** When X=1, the default value is 28 (History). When X=2, the default value is 61 (Directory).		

Parameters	Permitted Values	Default
When X=3, the default value is 5 (DND). When X=4, the default value is 30 (Menu). When X=5, the default value is 28 (History). When X=6, the default value is 61 (Directory). When X=7, the default value is 31 (Switch Account). When X=8, the default value is 31 (Switch Account). When X=9, the default value is 33 (Status). When X=10, the default value is 0 (NA). When X=14, the default value is 2 (Forward). **For SIP-T20P IP phones:** When X=5, the default value is 28 (History). When X=6, the default value is 61 (Directory). When X=7, the default value is 31 (Switch Account). When X=8, the default value is 31 (Switch Account). When X=9, the default value is 33 (Status). When X=10, the default value is 0 (NA). When X=11, the default value is 0 (NA). When X=12, the default value is 0 (NA). When X=14, the default value is 2 (Forward). **Web User Interface:** DSSKey->Memory Key/ Line Key / Programable Key ->Type **Phone User Interface:** Menu->Features->DSS Keys->Memory Keys (or Line Keys)->DSS Key X (or Line Key X)->Type		
memorykey.X.line/ linekey.X.line/ programablekey.X.line	**Integer from 1 to 6**	**Blank for memory key, 1-6 for lines 1-6, 1 for programable key**
Description: Configures the desired line to apply the directed call pickup key. For memory keys: X ranges from 1 to 10 (for SIP-T28/T26P). For line keys: X ranges from 1 to 6 (for SIP-T28P) X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P).		

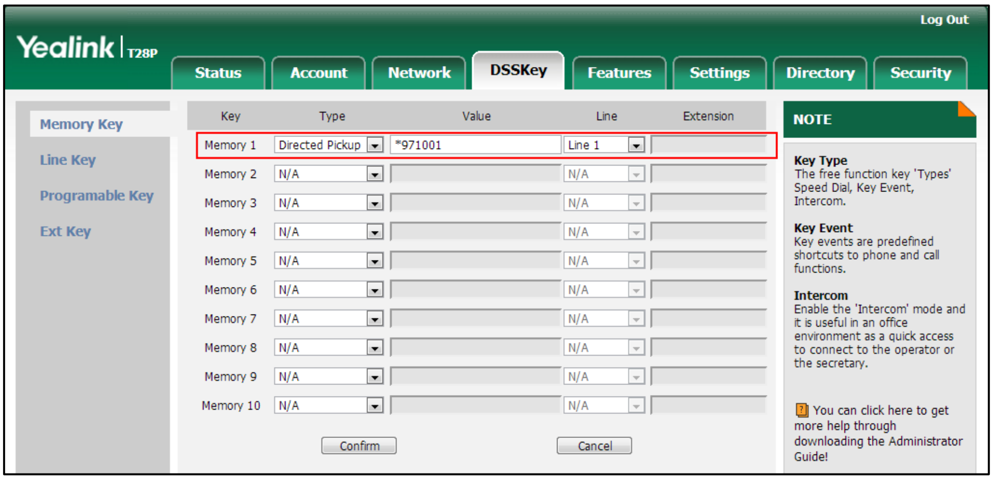
Parameters	Permitted Values	Default
For programable keys: X ranges from 1 to 14 (for SIP-T28/T26P) X=1-10, 14 (for SIP-T22P) X=5-12, 14 (for SIP-T20P) **Example:** memorykey.1.line = 1 **Web User Interface:** DSSKey->Memory Key/Line Key/Programable Key ->Line **Phone User Interface:** Menu->Features->DSS Keys->Memory Keys (or Line Keys)->DSS Key X (or Line Key X)->Account ID		
memorykey.X.value/ linekey.X.value/ programablekey.X.value	String within 99 characters	Blank
Description: Configures the directed call pickup feature code followed by the monitored extension. For memory keys: X ranges from 1 to 10 (for SIP-T28/T26P). For line keys: X ranges from 1 to 6 (for SIP-T28P) X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). For programable keys: X ranges from 1 to 14 (for SIP-T28/T26P) X=1-10, 14 (for SIP-T22P) X=5-12, 14 (for SIP-T20P) **Example:** memorykey.1.value = *971001 **Web User Interface:** DSSKey->Memory Key/ Line Key / Programable Key ->Value **Phone User Interface:** Menu->Features->DSS Keys->Memory Keys (or Line Keys)->DSS Key X (or Line Key X)->Value		

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

1. Click on **DSSKey**->**Memory Key** (**Line Key** or **Programable Key**).

   SIP-T22P/T20P IP phones only support line keys and programable keys.

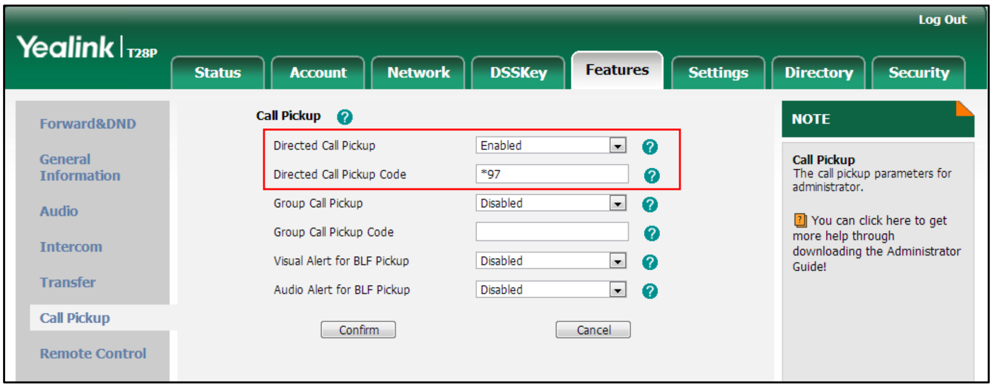
2. In the desired DSS key field, select **Directed Pickup** from the pull-down list of **Type**.
3. Enter the directed call pickup code followed by the specific extension in the **Value** field.
4. Select the desired line from the pull-down list of **Line**.



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

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

1. Click on **Features**->**Call Pickup**.
2. Select the desired value from the pull-down list of **Directed Call Pickup** (not applicable to SIP-T20P IP phones).
3. Enter the directed call pickup code in the **Directed Call Pickup Code** field.

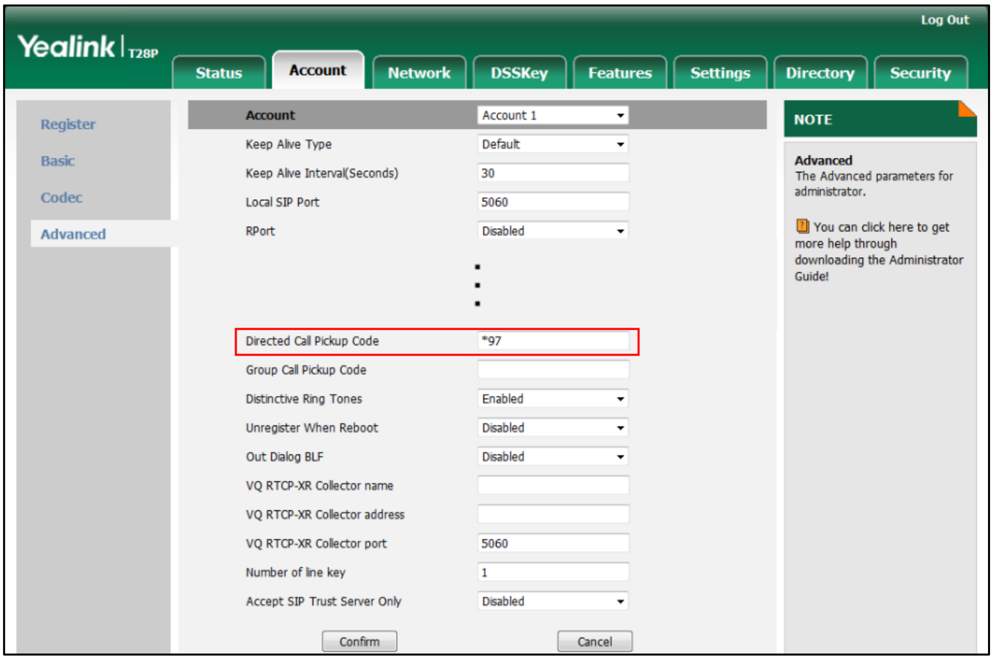


4. Click **Confirm** to accept the change.

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

1. Click on **Account**.

2. Select the desired account from the pull-down list of **Account**.
3. Click on **Advanced**.
4. Enter the directed call pickup code in the **Directed Call Pickup Code** field.



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

To configure a directed pickup key via phone user interface:

1. Press **Menu**->**Features**->**DSS Keys**->**Memory Keys** (or **Line Keys**).
2. Select the desired DSS key.
3. Press or , or the **Switch** soft key to select **Key Event** from the **Type** field.
4. Press or , or the **Switch** soft key to select **DPickup** from the **Key Type** field.
5. Press or , or the **Switch** soft key to select the desired line from the **Account ID** field.
6. Enter the directed call pickup code followed by the specific extension in the **Value** field.
7. Press the **Save** soft key to accept the change.

Group Call Pickup

Group call pickup is used for picking up incoming calls within a pre-defined group. If the group receives many incoming calls at once, the user will pick up the first incoming call, using a group pickup key or the GPickup soft key (not applicable to SIP-T20P IP phones). This feature depends on support from a SIP server. For many SIP servers, group call pickup requires a group pickup code, which can be configured on a phone or a per-line basis.

Procedure

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

Configuration File	<MAC>.cfg	Configure the group call pickup feature. **Parameters:** features.pickup.group_pickup_enable account.X.group_pickup_code features.pickup.group_pickup_code
	<y0000000000xx>.cfg	Assign a group call pickup key. **Parameters:** memorykey.X.type/ linekey.X.type/ programablekey.X.type memorykey.X.line/ linekey.X.line/ programablekey.X.line memorykey.X.value/ linekey.X.value/ programablekey.X.value
Local	Web User Interface	Assign a group call pickup key. **Navigate to**: http://<phoneIPAddress>/servlet?p=dsskey&q=load&model=0 Configure group call pickup feature on a phone basis. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-callpickup&q=load Configure the group call pickup code on a per-line basis. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0
	Phone User Interface	Assign a group call pickup key.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.pickup.group_pickup_enable	**0 or 1**	**0**

Parameters	Permitted Values	Default
Description: Enables or disables the IP phone to display the GPickup soft key when the IP phone is in the pre-dialing screen. **0**-Disabled **1**-Enabled **Note**: It is not applicable to SIP-T20P IP phones. **Web User Interface:** Features->Call Pickup->Group Call Pickup **Phone User Interface:** None		
account.X.group_pickup_code	**String within 32 characters**	**Blank**
Description: Configures the group pickup code for account X. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Example:** account.1.group_pickup_code = *69 **Note**: The group call pickup code configured on a per-line basis takes precedence over that configured on a phone basis. **Web User Interface:** Account->Advanced->Group Call Pickup Code **Phone User Interface:** None		
features.pickup.group_pickup_code	**String within 32 characters**	**Blank**
Description: Configures the group call pickup code on a phone basis. **Example:** features.pickup.group_pickup_code = *98 **Note**: The group call pickup code configured on a per-line basis takes precedence over that configured on a phone basis. **Web User Interface:** Features->Call Pickup->Group Call Pickup Code		

Parameters	Permitted Values	Default
Phone User Interface: None		

Group Call Pickup Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 513.

Parameters	Permitted Values	Default
memorykey.X.type/ linekey.X.type/ programablekey.X.type	**23**	**Refer to the following content**
Description: Configures a DSS key as a group call pickup key on the IP phone. The digit **23** stands for the key type **Group Pickup**. For memory keys: X ranges from 1 to 10 (for SIP-T28/T26P). For line keys: X ranges from 1 to 6 (for SIP-T28P) X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). For programable keys: X ranges from 1 to 14 (for SIP-T28/T26P) X=1-10, 14 (for SIP-T22P) X=5-12, 14 (for SIP-T20P) **Example:** memorykey.1.type = 23 **Default:** For memory keys: The default value is 0. For line keys: The default value is 15. For programable keys: **For SIP-T28P/T26P IP phones:** When X=1, the default value is 28 (History). When X=2, the default value is 61 (Directory).		

Parameters	Permitted Values	Default
When X=3, the default value is 5 (DND). When X=4, the default value is 30 (Menu). When X=5, the default value is 28 (History). When X=6, the default value is 61 (Directory). When X=7, the default value is 31 (Switch Account). When X=8, the default value is 31 (Switch Account). When X=9, the default value is 33 (Status). When X=10, the default value is 0 (NA). When X=11, the default value is 0 (NA). When X=12, the default value is 0 (NA). When X=13, the default value is 0 (NA). When X=14, the default value is 2 (Forward). **For SIP-T22P IP phones:** When X=1, the default value is 28 (History). When X=2, the default value is 61 (Directory). When X=3, the default value is 5 (DND). When X=4, the default value is 30 (Menu). When X=5, the default value is 28 (History). When X=6, the default value is 61 (Directory). When X=7, the default value is 31 (Switch Account). When X=8, the default value is 31 (Switch Account). When X=9, the default value is 33 (Status). When X=10, the default value is 0 (NA). When X=14, the default value is 2 (Forward). **For SIP-T20P IP phones:** When X=5, the default value is 28 (History). When X=6, the default value is 61 (Directory). When X=7, the default value is 31 (Switch Account). When X=8, the default value is 31 (Switch Account). When X=9, the default value is 33 (Status). When X=10, the default value is 0 (NA). When X=11, the default value is 0 (NA). When X=12, the default value is 0 (NA). When X=14, the default value is 2 (Forward). **Web User Interface:**		

Parameters	Permitted Values	Default
DSSKey->Memory Key/ Line Key / Programable Key ->Type **Phone User Interface:** Menu->Features->DSS Keys->Memory Keys (or Line Keys)->DSS Key X (or Line Key X)->Type		
memorykey.X.line/ linekey.X.line/ programablekey.X.line	**Integer from 1 to 6**	**Blank for memory key, 1-6 for lines 1-6, 1 for programable key**
Description: Configures the desired line to apply the group call pickup key. For memory keys: X ranges from 1 to 10 (for SIP-T28/T26P). For line keys: X ranges from 1 to 6 (for SIP-T28P) X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). For programable keys: X ranges from 1 to 14 (for SIP-T28/T26P) X=1-10, 14 (for SIP-T22P) X=5-12, 14 (for SIP-T20P) **Example:** memorykey.1.line = 1 **Web User Interface:** DSSKey->Memory Key/ Line Key / Programable Key ->Line **Phone User Interface:** Menu->Features->DSS Keys->Memory Keys (or Line Keys)->DSS Key X (or Line Key X)->Account ID		
memorykey.X.value/ linekey.X.value/ programablekey.X.value	**String within 99 characters**	**Blank**

Parameters	Permitted Values	Default
Description: Configures the group call pickup feature code. For memory keys: X ranges from 1 to 10 (for SIP-T28/T26P). For line keys: X ranges from 1 to 6 (for SIP-T28P) X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). For programable keys: X ranges from 1 to 14 (for SIP-T28/T26P) X=1-10, 14 (for SIP-T22P) X=5-12, 14 (for SIP-T20P) **Example:** memorykey.1.value = *98 **Web User Interface:** DSSKey->Memory Key/ Line Key / Programable Key ->Value **Phone User Interface:** Menu->Features->DSS Keys->Memory Keys (or Line Keys)->DSS Key X (or Line Key X)->Value		

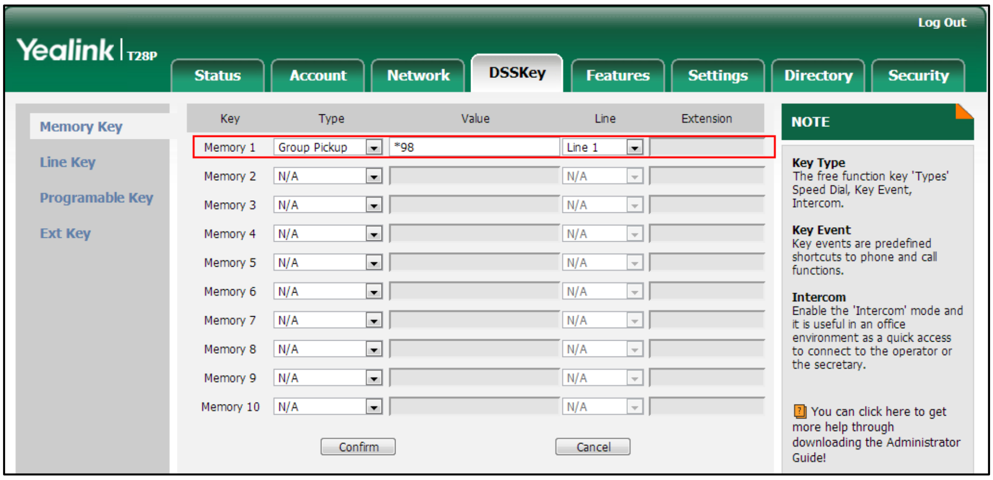
To configure a group call pickup key via web user interface:

1. Click on **DSSKey**->**Memory Key** (**Line Key** or **Programable Key**).

   SIP-T22P/T20P IP phones only support line keys and programable keys.

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

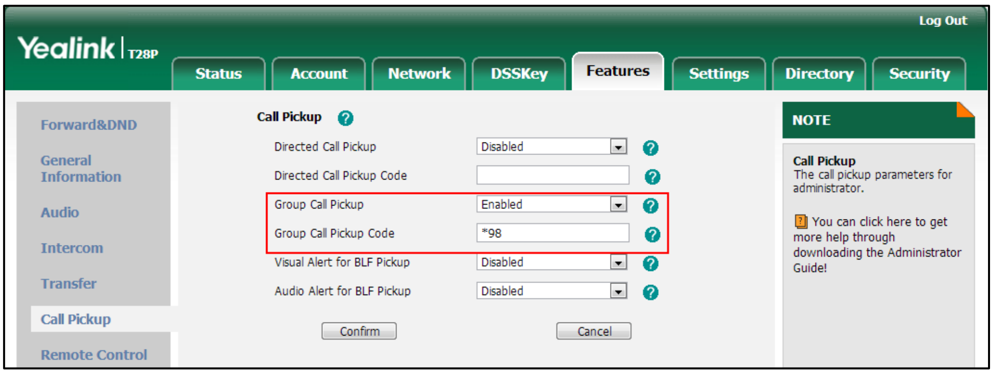
4. Select the desired line from the pull-down list of **Line**.



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

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

1. Click on **Features**->**Call Pickup**.
2. Select the desired value from the pull-down list of **Group Call Pickup** (not applicable to SIP-T20P IP phones).
3. Enter the group call pickup code in the **Group Call Pickup Code** field.

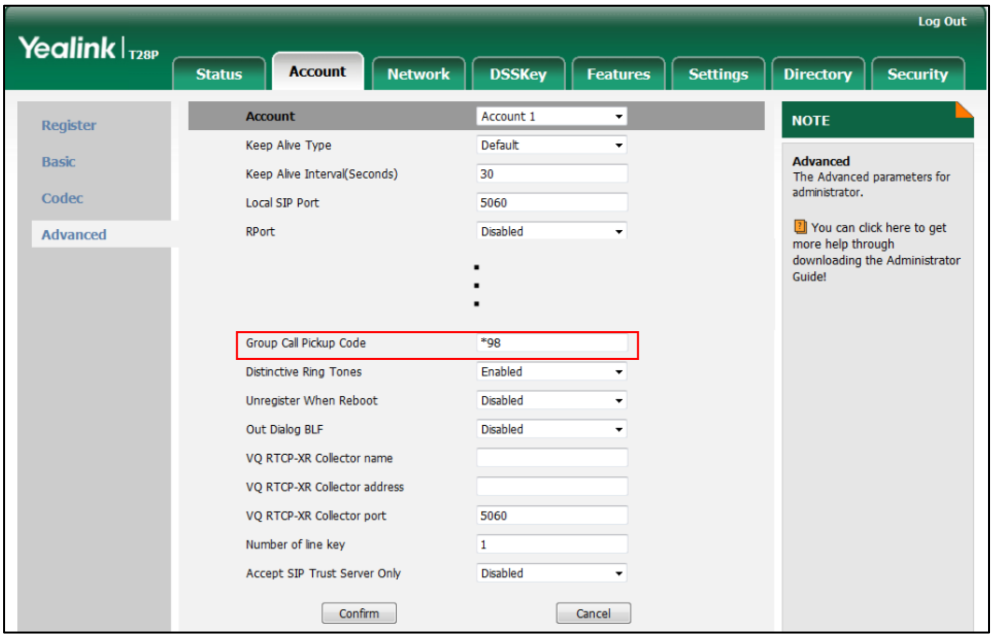


4. Click **Confirm** to accept the change.

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

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

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



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

To configure a group pickup key via phone user interface:

1. Press **Menu**->**Features**->**DSS Keys**->**Memory Keys** (or **Line Keys**).
2. Select the desired DSS key.
3. Press or , or the **Switch** soft key to select **Key Event** from the **Type** field.
4. Press or , or the **Switch** soft key to select **GPickup** from the **Key Type** field.
5. Press or , or the **Switch** soft key to select the desired line from the **Account ID** field.
6. Enter the group call pickup code in the **Value** field.
7. Press the **Save** soft key to accept the change.

Dialog Info Call Pickup

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

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

```
<?xml version="1.0"?>
<dialog-info xmlns="urn:ietf:params:xml:ns:dialog-info" version="6" state="full"
entity="sip:1013@10.2.1.199">
<dialog id="706655206@10.2.8.213" call-id="706655206@10.2.8.213" local-tag="827932784"
```

```
remote-tag="1887460740" direction="recipient">
<state>early</state>
<local>
<identity>sip:1013@10.2.1.199</identity>
<target uri="sip:1013@10.2.1.199">
</target>
</local>
<remote>
<identity>sip:1011@10.2.1.199</identity>
<target uri="sip:1011@10.2.8.213:5063">
</target>
</remote>
</dialog>
</dialog-info>
```


Procedure

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

Configuration File	<MAC>.cfg	Configure dialog info call pickup. **Parameter**: account.X.dialoginfo_callpickup
Local	Web User Interface	Configure dialog-info call pickup on the IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

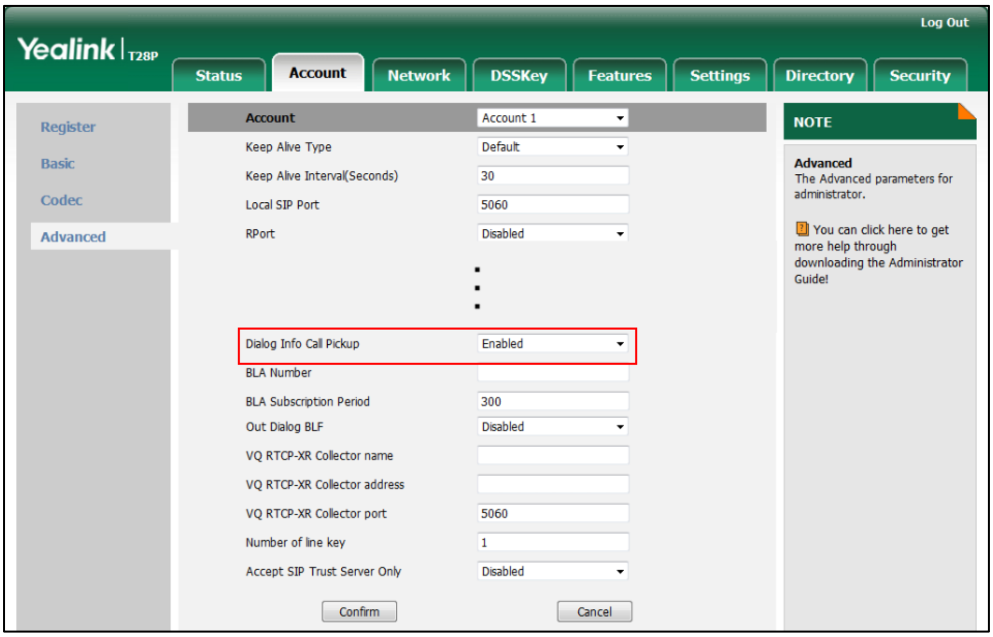
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
account.X.dialoginfo_callpickup	**0 or 1**	**0**
Description: Enables or disables the IP phone to pick up a call according to the SIP header of dialog-info for account X. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), call pickup is implemented through SIP signals. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P).		

Parameter	Permitted Values	Default
X ranges from 1 to 2 (for SIP-T20P). **Web User Interface:** Account->Advanced->Dialog Info Call Pickup **Phone User Interface:** None		

To configure dialog info call pickup via web user interface:

1. Click on **Account**.
2. Select the desired account from the pull-down list of **Account**.
3. Click on **Advanced**.
4. Select the desired value from the pull-down list of **Dialog Info Call Pickup**.



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

ReCall

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

Procedure

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

Configuration File	<y0000000000xx>.cfg	Assign a recall key.

		Parameters: memorykey.X.type/ linekey.X.type/ programablekey.X.type
Local	Web User Interface	Assign a recall key. **Navigate to:** http://<phoneIPAddress>/servlet?p=dsskey&q=load&model=0
	Phone User Interface	Assign a recall key.

Recall Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 513.

Parameter	Permitted Values	Default
memorykey.X.type/ linekey.X.type/ programablekey.X.type	**7**	**Refer to the following content**
Description: Configures a DSS key as a recall key on the IP phone. The digit **7** stands for the key type **ReCall**. For memory keys: X ranges from 1 to 10 (for SIP-T28/T26P). For line keys: X ranges from 1 to 6 (for SIP-T28P) X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). For programable keys: X ranges from 1 to 14 (for SIP-T28/T26P) X=1-10, 14 (for SIP-T22P) X=5-12, 14 (for SIP-T20P) **Example:** memorykey.1.type = 7 **Default:** For memory keys: The default value is 0. For line keys: The default value is 15.		

Parameter	Permitted Values	Default
For programable keys: **For SIP-T28P/T26P IP phones:** When X=1, the default value is 28 (History). When X=2, the default value is 61 (Directory). When X=3, the default value is 5 (DND). When X=4, the default value is 30 (Menu). When X=5, the default value is 28 (History). When X=6, the default value is 61 (Directory). When X=7, the default value is 31 (Switch Account). When X=8, the default value is 31 (Switch Account). When X=9, the default value is 33 (Status). When X=10, the default value is 0 (NA). When X=11, the default value is 0 (NA). When X=12, the default value is 0 (NA). When X=13, the default value is 0 (NA). When X=14, the default value is 2 (Forward). **For SIP-T22P IP phones:** When X=1, the default value is 28 (History). When X=2, the default value is 61 (Directory). When X=3, the default value is 5 (DND). When X=4, the default value is 30 (Menu). When X=5, the default value is 28 (History). When X=6, the default value is 61 (Directory). When X=7, the default value is 31 (Switch Account). When X=8, the default value is 31 (Switch Account). When X=9, the default value is 33 (Status). When X=10, the default value is 0 (NA). When X=14, the default value is 2 (Forward). **For SIP-T20P IP phones:** When X=5, the default value is 28 (History). When X=6, the default value is 61 (Directory). When X=7, the default value is 31 (Switch Account). When X=8, the default value is 31 (Switch Account). When X=9, the default value is 33 (Status). When X=10, the default value is 0 (NA).		

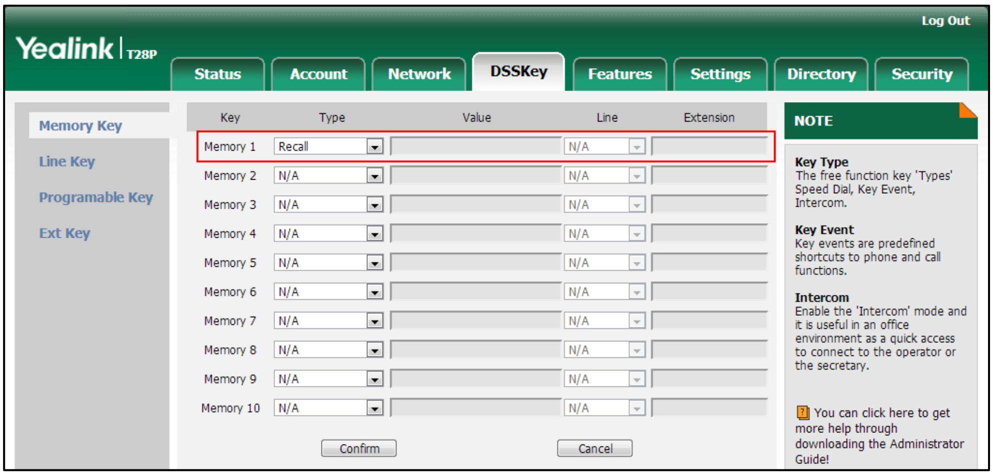
Parameter	Permitted Values	Default
When X=11, the default value is 0 (NA). When X=12, the default value is 0 (NA). When X=14, the default value is 2 (Forward). **Web User Interface:** DSSKey->Memory Key/ Line Key / Programable Key ->Type **Phone User Interface:** Menu->Features->DSS Keys->Memory Keys (or Line Keys)->DSS Key X (or Line Key X)->Type		

To configure a recall key via web user interface:

1. Click on **DSSKey**->**Memory Key** (**Line Key** or **Programable Key**).

   SIP-T22P/T20P IP phones only support line keys and programable keys.

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



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

To configure a recall key via phone user interface:

1. Press **Menu**->**Features**->**DSS Keys**->**Memory Keys** (or **Line Keys**).
2. Select the desired DSS key.
3. Press or , or the **Switch** soft key to select **Key Event** from the **Type** field.
4. Press or , or the **Switch** soft key to select **ReCall** from the **Key Type** field.
5. Press the **Save** soft key to accept the change.

Call Park

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

Procedure

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

Configuration File	<y0000000000xx>.cfg	Assign a call park key. **Parameters:** memorykey.X.type/ linekey.X.type/ memorykey.X.line/ linekey.X.line/ memorykey.X.value/ linekey.X.value/
Local	Web User Interface	Assign a call park key. **Navigate to:** http://<phoneIPAddress>/servlet?p=dsskey&q=load&model=0
	Phone User Interface	Assign a call park key.

Call Park Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 513.

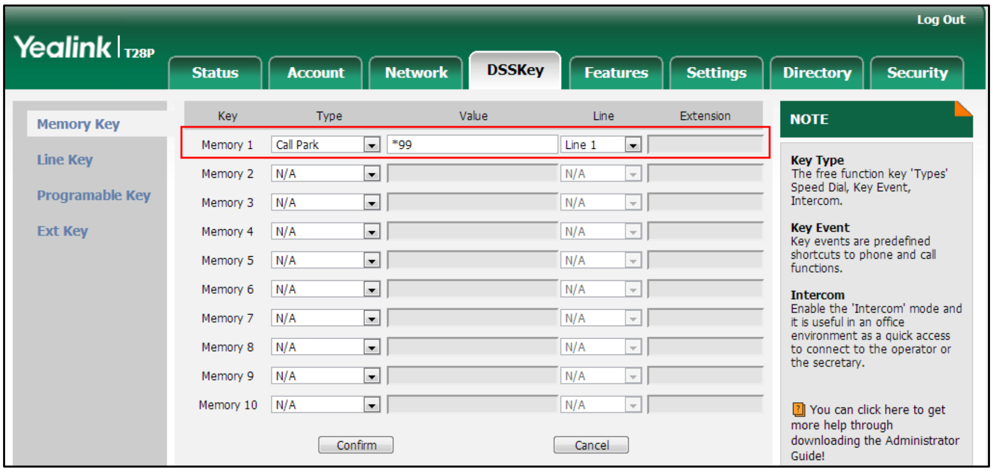
Parameters	Permitted Values	Default
memorykey.X.type/ linekey.X.type	**Integer**	**0 for memory key,15 for line key**
Description: Configures a DSS key as a call park key on the IP phone. The digit **10** stands for the key type **Call Park**. For the memory key, x ranges from 1 to 10. For the line key, x ranges from 1 to 6. **Example:** memorykey.1.type = 10 **Web User Interface:** DSSKey->Memory Key(or Line key)->Type **Phone User Interface:**		

Parameters	Permitted Values	Default
Menu->Features->DSS Keys->Memory Keys (or Line Keys)->DSS Key X (or Line Key X)->Type		
memorykey.X.line/ linekey.X.line	**Integer from 1 to 6**	**Blank for memory key,1-6 for lines 1-6**
Description: Configures the desired line to apply the call park key. For the memory key, x ranges from 1 to 10. For the line key, x ranges from 1 to 6. **Example:** memorykey.1.line = 1 **Web User Interface:** DSSKey->Memory Key(or Line key)->Line **Phone User Interface:** Menu->Features->DSS Keys->Memory Keys (or Line Keys)->DSS Key X (or Line Key X)->Account ID		
memorykey.X.value/ linekey.X.value	**String within 99 characters**	**blank**
Description: Configures the call park feature code. For the memory key, x ranges from 1 to 10. For the line key, x ranges from 1 to 6. **Example:** memorykey.1.value = *99 **Web User Interface:** DSSKey->Memory Key(or Line key)->Value **Phone User Interface:** Menu->Features->DSS Keys->Memory Keys (or Line Keys)->DSS Key X (or Line Key X)->Value		

To configure a call park key via web user interface:

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

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



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

To configure a call park key via phone user interface:

1. Press **Menu**->**Features**->**DSS Keys**->**Memory Keys** (or **Line Keys**).
2. Select the desired DSS key.
3. Press or , or the **Switch** soft key to select **Key Event** from the **Type** field.
4. Press or , or the **Switch** soft key to select **Call Park** from the **Key Type** field.
5. Press or , or the **Switch** soft key to select the desired line from the **Account ID** field.
6. Enter the desired value (e.g., call park feature code) in the **Value** field.
7. Press the **Save** soft key to accept the change.

Calling Line Identification Presentation

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

If the caller already exists in the local directory, the local contact name assigned to the caller should be preferentially displayed and stored in the call log.

For more information on calling line identification presentation, refer to *Calling and Connected Line Identification Presentation on Yealink IP Phones*, available online: http://www.yealink.com/DocumentDownload.aspx?CateId=142&flag=142.

Procedure

CLIP can be configured using the configuration files or locally.

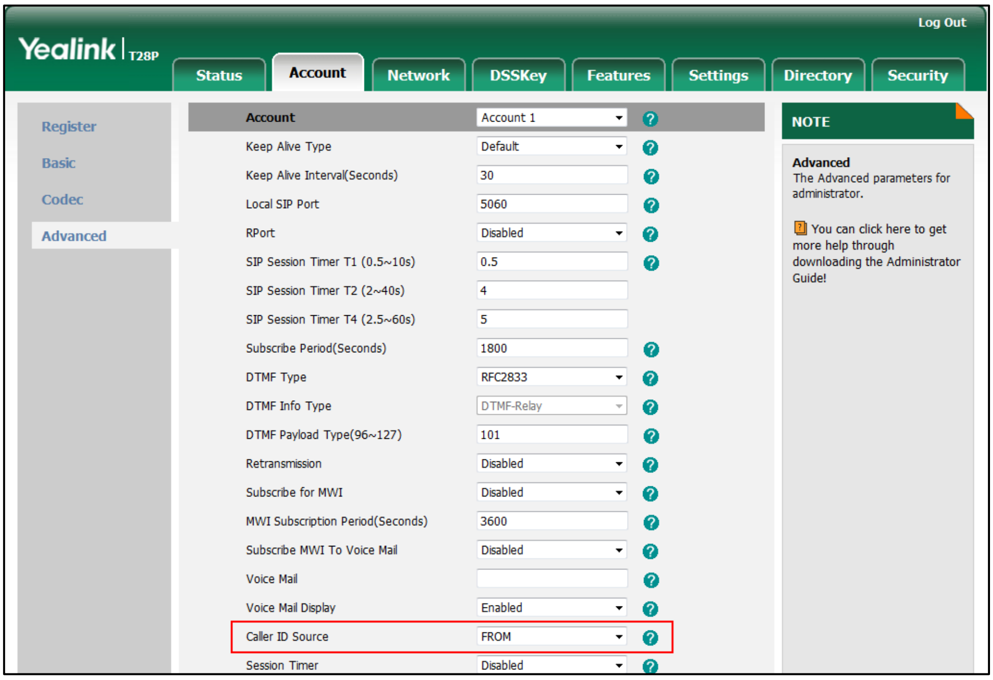
Configuration File	<MAC>.cfg	Configure the presentation of the caller identity. **Parameter:** account.X.cid_source
Local	Web User Interface	Configure the presentation of the caller identity. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
account.X.cid_source	**0, 1, 2, 3, 4 or 5**	**0**
Description: Configures the presentation of the caller identity when receiving an incoming call for account X. **0**-FROM (Derives the name and number of the caller from the "From" header). **1**-PAI (Derives the name and number of the caller from the "PAI" header. If the server does not send the "PAI" header, displays "anonymity" on the callee's phone). **2**-PAI-FROM (Derives the name and number of the caller from the "PAI" header preferentially. If the server does not send the "PAI" header, derives from the "From" header). **3**-RPID-PAI-FROM **4**-PAI-RPID-FROM **5**-RPID-FROM X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Web User Interface:** Account->Advanced->Caller ID Source **Phone User Interface:** None		

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

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



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

Connected Line Identification Presentation

Connected Line Identification Presentation (COLP) allows IP phones to display the identity of the connected party specified for outgoing calls. IP 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 RFC 4916. 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.

If the callee already exists in the local directory, the local contact name assigned to the callee should be preferentially displayed.

For more information on connected line identification presentation, refer to *Calling and Connected Line Identification Presentation on Yealink IP Phones*, available online: http://www.yealink.com/DocumentDownload.aspx?CateId=142&flag=142.

Procedure

COLP can be configured only using the configuration files.

Configuration File	<MAC>.cfg	Configure the presentation of the callee's identity. **Parameter:** account.X.cp_source

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
account.X.cp_source	**0, 1 or 2**	**0**
Description: Configures the presentation of the callee's identity for account X. **0**-PAI-RPID (Derives the name and number of the callee from the "PAI" header preferentially. If the server does not send the "PAI" header, derives from the "RPID" header). **1**-Dialed Digits (Preferentially displays the dialed digits on the caller's phone). **2**-RFC 4916 (Derives the name and number of the callee from "From" header in the Update message). When the RFC 4916 is enabled on the IP phone, the caller sends the SIP request message which contains the from-change tag in the Supported header. The caller then receives an UPDATE message from the callee, and displays the identity in the From header. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Web User Interface:** None **Phone User Interface:** None		

DTMF

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

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

DTMF Keypad Frequencies:

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

Three methods of transmitting DTMF digits on SIP calls:

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

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

RFC 2833

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

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

INBAND

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

Configuration File	<MAC>.cfg	Configure the method of transmitting DTMF digit and the payload type. **Parameters**: account.X.dtmf.type account.X.dtmf.dtmf_payload account.X.dtmf.info_type
	<y0000000000xx>.cfg	Configure the number of times for the IP phone to send the end RTP Event packet. **Parameter**: features.dtmf.repetition Configure the frequency level of DTMF digits. **Parameter**: features.dtmf.volume
Local	Web User Interface	Configure the method of transmitting DTMF digits and the payload type. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0 Configure the number of times for the IP phone to send the end RTP Event packet. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=loa

		d

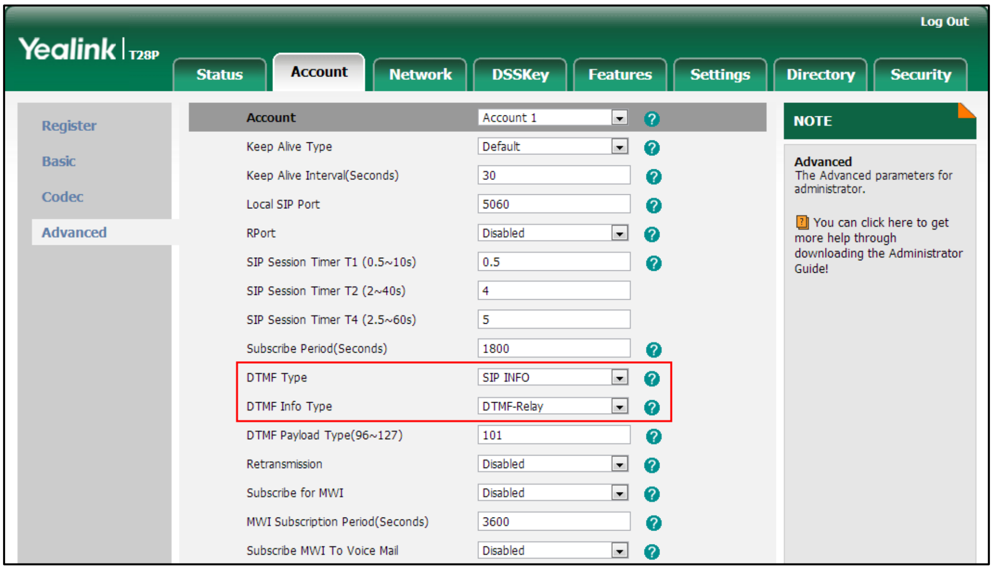
Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.dtmf.type	**0, 1, 2 or 3**	**1**
Description: Configures the DTMF type for account X. **0**-INBAND **1**-RFC 2833 **2**-SIP INFO **3**-RFC2833 + SIP INFO If it is set to 0 (INBAND), DTMF digits are transmitted in the voice band. If it is set to 1 (RFC 2833), DTMF digits are transmitted by RTP Events compliant to RFC 2833. If it is set to 2 (SIP INFO), DTMF digits are transmitted by the SIP INFO messages. If it is set to 3 (RFC2833 + SIP INFO), DTMF digits are transmitted by RTP Events compliant to RFC 2833 and the SIP INFO messages. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Web User Interface:** Account->Advanced->DTMF Type **Phone User Interface:** None		
account.X.dtmf.dtmf_payload	**Integer from 96 to 127**	**101**
Description: Configures the RFC 2833 payload type for account X. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Web User Interface:** Account->Advanced->DTMF Payload Type (96~127) **Phone User Interface:** None		

Parameters	Permitted Values	Default
account.X.dtmf.info_type	**1, 2 or 3**	**0**
Description: Configures the DTMF info type when the DTMF type is configured as "SIP INFO", "RFC2833 + SIP INFO" for account X. **0**-Disabled **1**-DTMF-Relay **2**-DTMF **3**-Telephone-Event X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Web User Interface:** Account->Advanced->DTMF Info Type **Phone User Interface:** None		
features.dtmf.repetition	**1, 2 or 3**	**3**
Description: Configures the repetition times for the IP phone to send the end RTP EVENT packet during an active call. **Web User Interface:** Features->General Information->DTMF Repetition **Phone User Interface:** None		
features.dtmf.volume	**Integer from -10~-2**	**-10**
Description: Configures the frequency level of DTMF digits (in db). **Web User Interface:** None **Phone User Interface:** None		

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

1. Click on **Account**.
2. Select the desired account from the pull-down list of **Account**.
3. Click on **Advanced**.
4. Select the desired value from the pull-down list of **DTMF Type**.
5. If **SIP INFO** or **RFC2833 + SIP INFO** is selected, select the desired value from the pull-down list of **DTMF Info Type**.
6. Enter the desired value in the **DTMF Payload Type** field.

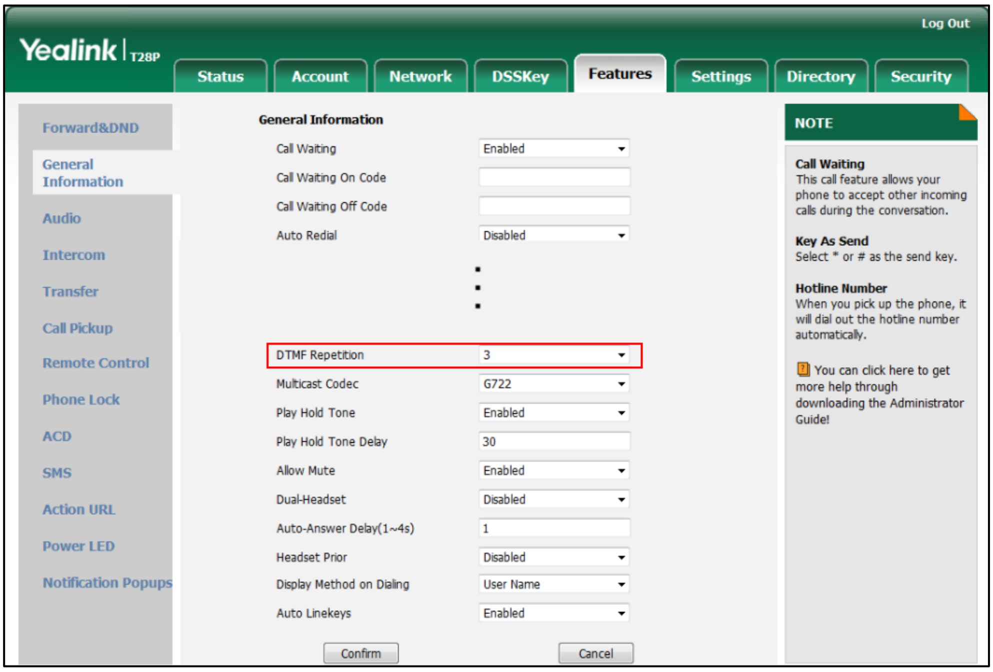


7. Click **Confirm** to accept the change.

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

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

2. Select the desired value (1-3) from the pull-down list of **DTMF Repetition**.



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

Suppress DTMF Display

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

Procedure

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

Configuration File	<y0000000000xx>.cfg	Configure suppress DTMF display and suppress DTMF display delay. **Parameters:** features.dtmf.hide features.dtmf.hide_delay
Local	Web User Interface	Configure suppress DTMF display and suppress DTMF display delay. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-general&q=load

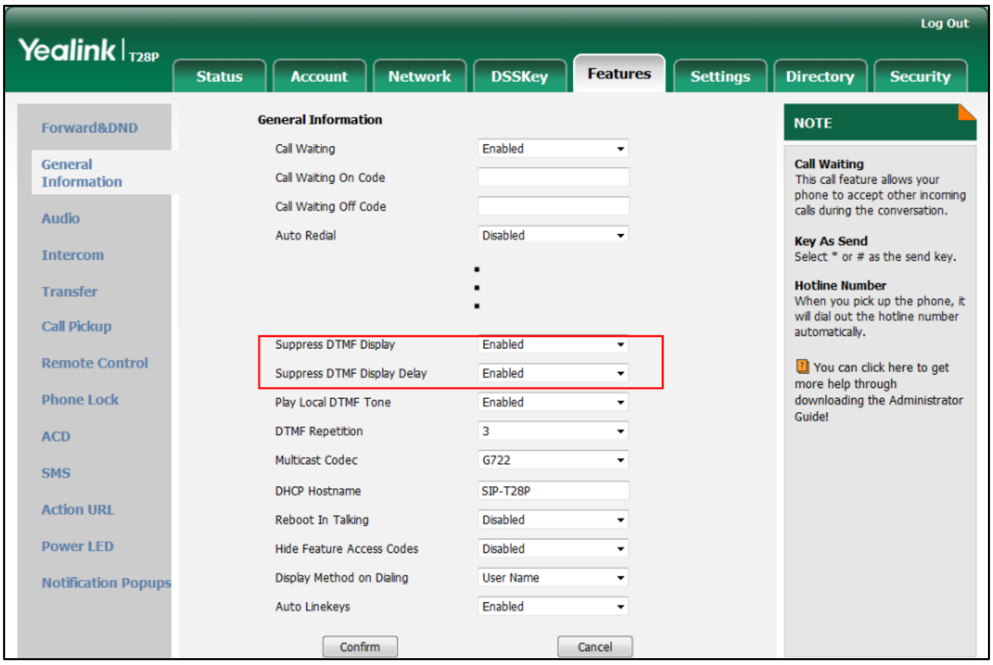
Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.dtmf.hide	**0 or 1**	**0**
Description: Enables or disables the IP phone to suppress the display of DTMF digits during an active call. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the DTMF digits are displayed as asterisks. **Web User Interface:** Features->General Information->Suppress DTMF Display **Phone User Interface:** None		
features.dtmf.hide_delay	**0 or 1**	**0**
Description: Enables or disables the IP phone to display the DTMF digits for a short period before displaying asterisks during an active call. **0**-Disabled **1**-Enabled **Note:** It works only if the parameter "features.dtmf.hide" is set to 1 (Enabled). It is not applicable to SIP-T20P IP phones. **Web User Interface:** Features->General Information->Suppress DTMF Display Delay **Phone User Interface:** None		

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** (not applicable to SIP-T20P IP phones).



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

Transfer via DTMF

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

Procedure

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

Configuration File	<y0000000000xx>.cfg	Configure transfer via DTMF. **Parameters:** features.dtmf.replace_tran features.dtmf.transfer
Local	Web User Interface	Configure transfer via DTMF. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-general&q=load

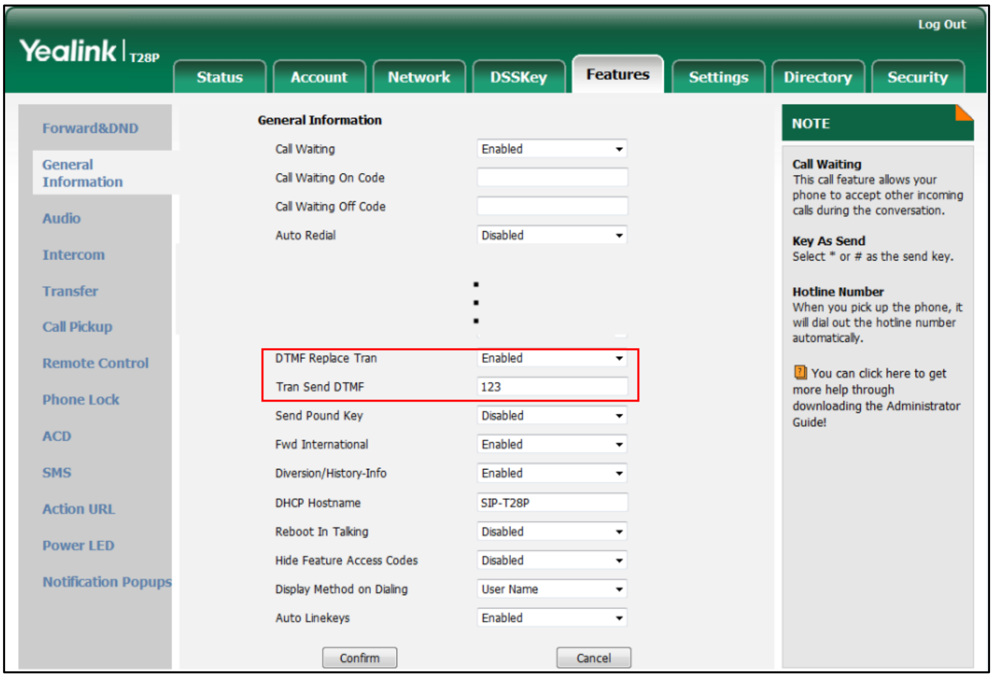
Details of Configuration Parameters:

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>features.dtmf.replace_tran</td><td>0 or 1</td><td>0</td></tr>
<tr><td colspan="3">Description:
Enables or disables the IP phone to send DTMF sequences for transfer function when pressing the transfer soft key or the TRAN key.
0-Disabled
1-Enabled
If it is set to 0 (Disabled), the IP phone will perform the transfer as normal when pressing the transfer key during a call.
If it is set to 1 (Enabled), the IP phone will transmit the designated DTMF digits to the server for completing call transfer when pressing the transfer key during a call.
Web User Interface:
Features->General Information->DTMF Replace Tran
Phone User Interface:
None</td></tr>
<tr><td>features.dtmf.transfer</td><td>String within 32 characters</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the DTMF digits to be transmitted to perform call transfer. Valid values are: 0-9, *, # and A-D.
Example:
features.dtmf.transfer = 123
Note: It works only if the parameter "features.dtmf.replace_tran" is set to 1 (Enabled).
Web User Interface:
Features->General Information->Tran Send DTMF
Phone User Interface:
None</td></tr>
</table>

To configure transfer via DTMF via web user interface:

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

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



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

Intercom

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

Outgoing Intercom Calls

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

Procedure

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

Configuration File	<y0000000000xx>.cfg	Assign an intercom key. **Parameters:** memorykey.X.type/ linekey.X.type memorykey.X.line/ linekey.X.line memorykey.X.value/ linekey.X.value
Local	Web User Interface	Assign an intercom key.

		Navigate to: http://<phoneIPAddress>/servlet?p=dsskey&q=load&model=0
	Phone User Interface	Assign an intercom key.

Intercom Key

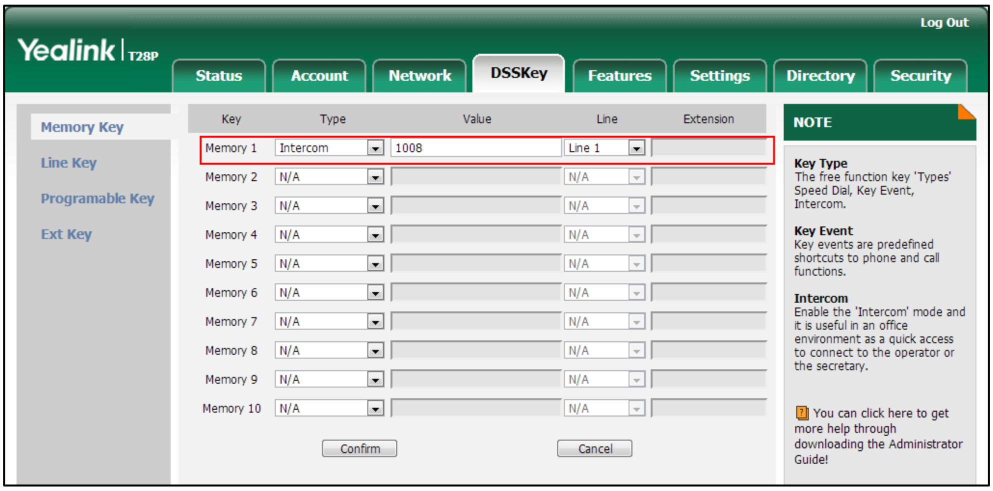
For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 513.

Parameters	Permitted Values	Default
memorykey.X.type/ linekey.X.type	**Integer**	**0 for memory key,15 for line key**
Description: Configures a DSS key as an intercom key. The digit **14** stands for the key type **Intercom**. For the memory key, x ranges from 1 to 10. For the line key, x ranges from 1 to 6. **Example:** memorykey.1.type = 14 **Web User Interface:** DSSKey->Memory Key(or Line key)->Type **Phone User Interface:** Menu->Features->DSS Keys->Memory Keys (or Line Keys)->DSS Key X (or Line Key X)->Type		
memorykey.X.line/ linekey.X.line	**Integer from 1 to 6**	**Blank for memory key, 1-6 for lines 1-6**
Description: Configures the desired line to apply the intercom key. For the memory key, x ranges from 1 to 10. For the line key, x ranges from 1 to 6. **Example:** memorykey.1.line = 1 **Web User Interface:** DSSKey->Memory Key(or Line key)->Line **Phone User Interface:** Menu->Features->DSS Keys->Memory Keys (or Line Keys)->DSS Key X (or Line Key		

Parameters	Permitted Values	Default
X)->Account ID		
memorykey.X.value/ linekey.X.value	String within 99 characters	blank
Description: Configures the intercom number. For the memory key, x ranges from 1 to 10. For the line key, x ranges from 1 to 6. **Example:** memorykey.1.value = 1008 **Web User Interface:** DSSKey->Memory Key(or Line key)->Value **Phone User Interface:** Menu->Features->DSS Keys->Memory Keys (or Line Keys)->DSS Key X (or Line Key X)->Value		

To configure an intercom key via web user interface:

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



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

To configure an intercom key via phone user interface:

1. Press **Menu**->**Features**->**DSS Keys**->**Memory Keys** (or **Line Keys**).
2. Select the desired DSS key.

3. Press or , or the **Switch** soft key to select **Intercom** from the **Type** field.
4. Select the desired line from the **Account ID** field.
5. Enter the remote extension number in the **Value** field.
6. Press the **Save** soft key to accept the change.

Incoming Intercom Calls

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

Accept Intercom

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

Intercom Mute

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

Intercom Tone

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

Intercom Barge

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

Procedure

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

Configuration File	<y0000000000xx>.cfg	Configure incoming intercom call feature. **Parameters:** features.intercom.allow features.intercom.mute features.intercom.tone features.intercom.barge
Local	Web User Interface	Configure incoming intercom call feature. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-intercom&q=load
	Phone User Interface	Configure incoming intercom call feature.

Details of Configuration Parameters:

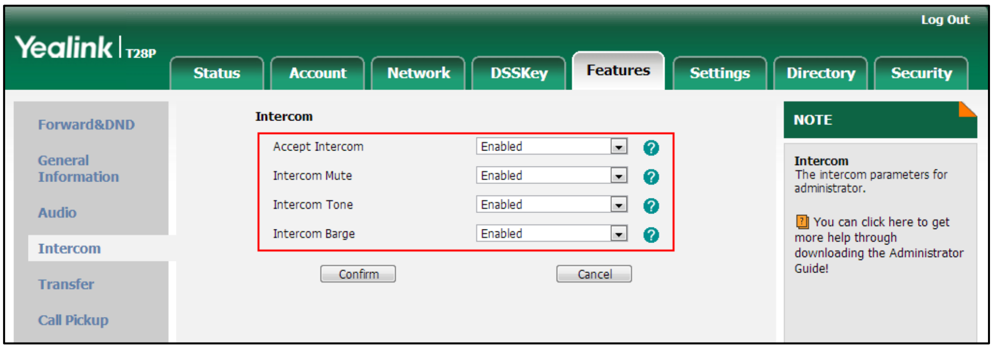
Parameters	Permitted Values	Default
features.intercom.allow	**0 or 1**	**1**
Description: Enables or disables the IP phone to automatically answer an incoming intercom call. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), the IP phone will reject incoming intercom calls and sends a busy signal to the caller. If it is set to 1 (Enabled), the IP phone will automatically answer an incoming intercom call. **Web User Interface:** Features->Intercom->Accept Intercom **Phone User Interface:** Menu->Features->Intercom->Acpt Intercom		
features.intercom.mute	**0 or 1**	**0**
Description: Enables or disables the IP phone to mute the microphone when answering an intercom call. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the microphone is muted for intercom calls, and then the other party cannot hear you. **Note:** It works only if the parameter "features.intercom.allow" is set to 1 (Enabled). **Web User Interface:** Features->Intercom ->Intercom Mute **Phone User Interface:** Menu->Features->Intercom->Intercom Mute		
features.intercom.tone	**0 or 1**	**1**

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td colspan="3">Description:
Enables or disables the IP phone to play a warning tone when receiving an intercom call.
0-Disabled
1-Enabled
Note: It works only if the parameter "features.intercom.allow" is set to 1 (Enabled).
Web User Interface:
Features->Intercom ->Intercom Tone
Phone User Interface:
Menu->Features->Intercom->Intercom Tone</td></tr>
<tr><td>features.intercom.barge</td><td>0 or 1</td><td>0</td></tr>
<tr><td colspan="3">Description:
Enables or disables the IP phone to automatically answer an incoming intercom call while there is already an active call on the IP phone.
0-Disabled
1-Enabled
If it is set to 0 (Disabled), the IP phone will handle an incoming intercom call like a waiting call while there is already an active call on the IP phone.
If it is set to 1 (Enabled), the IP phone will automatically answer the intercom call while there is already an active call on the IP phone and place the active call on hold.
Note: It works only if the parameter "features.intercom.allow" is set to 1 (Enabled).
Web User Interface:
Features->Intercom ->Intercom Barge
Phone User Interface:
Menu->Features->Intercom->Intercom Barge</td></tr>
</table>

To configure intercom via web user interface:

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

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



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

To configure intercom via phone user interface:

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

Configuring Advanced Features

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

- Distinctive Ring Tones
- Tones
- Remote Phone Book
- LDAP
- Busy Lamp Field
- BLF List
- Hide Features Access Code
- Message Waiting Indicator
- Multicast Paging
- Call Recording
- Hot Desking
- Action URL
- Action URI
- Server Redundancy
- Static DNS Cache
- LLDP
- VLAN
- VPN
- Voice Quality Monitoring
- Quality of Service
- Network Address Translation
- 802.1X Authentication
- TR-069 Device Management
- IPv6 Support

Distinctive Ring Tones

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

Note If the caller already exists in the local directory, the ring tone assigned to the caller should be preferentially played.

Alert-Info headers in the following four formats:

Alert-Info: 127.0.0.1/Bellcore-drN (or Alert-Info: Bellcore-drN)

Alert-Info: ringtone-N (or Alert-Info: MyMelodyN)

Alert-Info: <URL>

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

- When the Alter-Info header contains the keyword "Bellcore-drN", the IP phone will play the Bellcore-drN (N=1, 2, 3, 4 or 5) ring tone if the parameter "features.alert_info_tone" is set to 1, or play the corresponding local ring tone (RingN.wav) in about ten seconds if the parameter "features.alert_info_tone" is set to 0.

  Example:

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

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

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

Bellcore Tone	Pattern ID	Pattern	Cadence	Minimum Duration (ms)	Nominal Duration (ms)	Maximum Duration (ms)
		Silent		145	200	525
		Ringing	Long	630	800	1025
		Silent		2975	4000	4400
Bellcore-dr4	4	Ringing	Short	200	300	525
		Silent		145	200	525
		Ringing	Long	800	1000	1100
		Silent		145	200	525
		Ringing	Short	200	300	525
		Silent		2975	4000	4400
Bellcore-dr5	5	Ringing		450	500	550

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

- When the Alter-Info header contains the keyword "ringtone-N" or "MyMolodyN", the IP phone will play the corresponding local ring tone (RingN.wav), or play the first local ring tone (Ring1.wav) in about ten seconds if "N" is greater than 8 or less than 1.

  Example:

  Alert-Info: ringtone-2

  Alert-Info: MyMelody2

  The following table identifies the corresponding local ring tone:

Value of N	Ring Tone
1	Ring1.wav
2	Ring2.wav
3	Ring3.wav
4	Ring4.wav
5	Ring5.wav
6	Silent.wav

Value of N	Ring Tone
7	Splash.wav
N<1 or N>8	Ring1.wav

- When the Alert-Info header contains a remote URL, the IP phone will try to download the WAV ring tone file from the URL and then play the remote ring tone if the parameter “account.X.alert_info_url_enable” is set to 1 (or the item called “Distinctive Ring Tones” on the web user interface is Enabled), or play the preconfigured local ring tone in about ten seconds if the parameter “account.X.alert_info_url_enable” is set to 0 or if the IP phone fails to download the remote ring tone.

  Example:

  Alert-Info: http://192.168.0.12:8080/Custom.wav

- When the Alert-Info header contains an info text, the IP phone will map the text with the internal ringer text preconfigured on the IP phone, and then play the ring tone associated with the internal ringer text. If no internal ringer text maps, the IP phone will play the preconfigured local ring tone in about ten seconds.

  Example:

  Alert-Info: info=family;x-line-id=0

Auto Answer

If the Alert-Info header contains the following type of strings, the IP phone will answer incoming calls automatically without playing the ring tone:

- Alert-Info: Auto Answer
- Alert-Info: info = alert-autoanswer
- Alert-Info: answer-after = 0 (or Alert-Info: Answer-After = 0)

Note If the Alert-Info header contains multiple types of keywords, the IP phone will process the keywords in the following order:AutoAnswer>URL>“Bellcore-drN/ringtone-N/MyMelodyN”>info text.

Procedure

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

Configuration File	<MAC>.cfg	Configure distinctive ring tones. **Parameter:** account.X.alert_info_url_enable
	<y0000000000xx>.cfg	Configure the internal ringer text and internal ringer file.

		Parameters: features.alert_info_tone distinctive_ring_tones.alert_info.X.text distinctive_ring_tones.alert_info.X.ringer
Local	Web User Interface	Configure distinctive ring tones. **Navigate to:** http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0 Configure the internal ringer text and internal ringer file. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-ring&q=load

Details of Configuration Parameters:

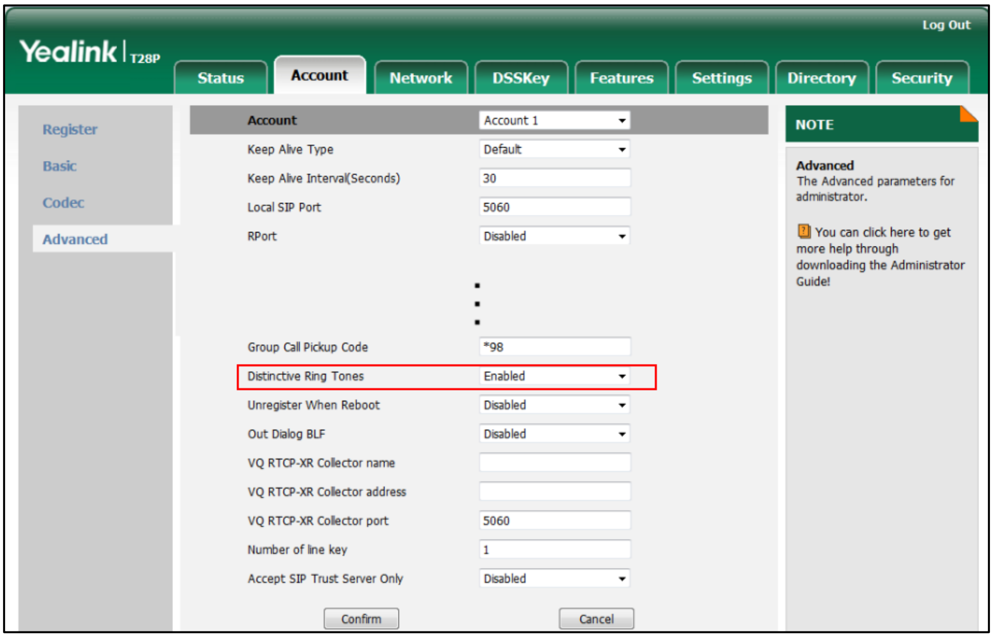
Parameters	Permitted Values	Default
account.X.alert_info_url_enable	**0 or 1**	**1**
Description: Enables or disables the IP phone to download the ring tone from the URL contained in the Alert-Info header for account X. **0**-Disabled **1**-Enabled X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Web User Interface:** Account->Advanced->Distinctive Ring Tones **Phone User Interface:** None		
features.alert_info_tone	**0 or 1**	**0**

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td colspan="3">Description:
Enables or disables the IP phone to map the keywords in the Alert-info header to the specified Bellcore ring tones.
0-Disabled
1-Enabled
Web User Interface:
None
Phone User Interface:
None</td></tr>
<tr><td>distinctive_ring_tones.alert_info.X.text</td><td>String within 32 characters</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the internal ringer text to map the keywords contained in the Alert-Info header.
X ranges from 1 to 10.
Example:
distinctive_ring_tones.alert_info.1.text = Family
Web User Interface:
Settings->Ring->Internal Ringer Text
Phone User Interface:
None</td></tr>
<tr><td>distinctive_ring_tones.alert_info.X.ringer
(X ranges from 1 to 10)</td><td>Integer from 1 to 7</td><td>1</td></tr>
<tr><td colspan="3">Description:
Configures the desired ring tones for each text.
The value ranges from 1 to 7, the digit stands for the appropriate ring tone.
1-Ring1.wav
2-Ring2.wav
3-Ring3.wav
4-Ring4.wav
5-Ring5.wav
6-Silent.wav
7-Splash.wav
Note: Silent.wav and Splash.wav only applicable to IP phones running firmware</td></tr>
</table>

Parameters	Permitted Values	Default
version 73 or later. **Web User Interface:** Settings->Ring->Internal Ringer File **Phone User Interface:** None		

To configure distinctive ring tones via web user interface:

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

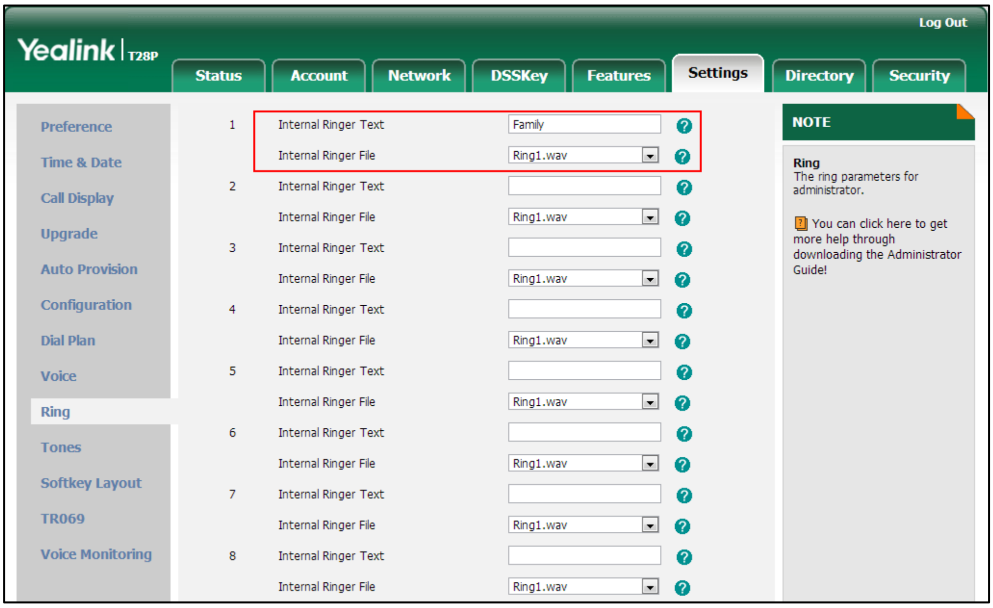


5. Click **Confirm** to accept the change.

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

1. Click on **Settings**->**Ring**.
2. Enter the keywords in the **Internal Ringer Text** fields.

3. Select the desired ring tones for each text from the pull-down lists of **Internal Ringer File**.



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

Tones

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

- Australia
- Austria
- Brazil
- Belgium
- China
- Czech
- Denmark
- Finland
- France
- Germany
- Great Britain
- Greece
- Hungary

- Lithuania
- India
- Italy
- Japan
- Mexico
- New Zealand
- Netherlands
- Norway
- Portugal
- Spain
- Switzerland
- Sweden
- Russia
- United States
- Chile
- Czech ETSI

Configured tones can be heard on IP 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
Congestion	When the network is congested
Call Waiting	Call waiting tone
Dial Recall	When receiving a call back
Info	When receiving a special message
Stutter	When receiving a voice mail
Message	When receiving a text message **Note**: It is not applicable to SIP-T20P IP phones.
Auto Answer	When automatically answering a call

Procedure

Tones can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure the tones for the IP phone. **Parameters:** voice.tone.country voice.tone.dial voice.tone.ring voice.tone.busy voice.tone.congestion voice.tone.callwaiting voice.tone.dialrecall voice.tone.info voice.tone.stutter voice.tone.message (not applicable to SIP-T20P IP phones) voice.tone.autoanswer
Local	Web User Interface	Configure the tones for the IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-tones&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
voice.tone.country	**Refer to the following content**	**Custom**
Description: Configures the country tone for the IP phone. **Permitted Values:** Custom, 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 **Example:**		

Parameters	Permitted Values	Default
voice.tone.country = Custom **Web User Interface:** Settings->Tones->Select Country **Phone User Interface:** None		
voice.tone.dial	**String**	**Blank**
Description: Customizes the dial tone. tonelist = element[,element] [,element]… Where **element** = [!]Freq1[+Freq2][+Freq3][+Freq4] /Duration **Freq**: the frequency of the tone (ranges from 200 to 7000 Hz). If it is set to 0Hz, it means the tone is not played. A tone is comprised of at most four different frequencies. **Duration**: the duration (in milliseconds) of the dial tone, ranges from 0 to 30000ms. 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). If you want the IP 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). **Note**: It works only if the parameter "voice.tone.country" is set to Custom. **Web User Interface:** Settings->Tones->Dial **Phone User Interface:** None		
voice.tone.ring	**String**	**Blank**
Description: Customizes the ringback tone. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **Note**: It works only if the parameter "voice.tone.country" is set to Custom. **Web User Interface:** Settings->Tones->Ring Back **Phone User Interface:**		

Parameters	Permitted Values	Default
None		
voice.tone.busy	String	Blank
Description: 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”. **Note**: It works only if the parameter “voice.tone.country” is set to Custom. **Web User Interface:** Settings->Tones->Busy **Phone User Interface:** None		
voice.tone.congestion	String	Blank
Description: Customizes the tone when the network is congested. The value format is Freq/Duration. For more information on the value format, refer to the parameter “voice.tone.dial”. The default value is blank. **Note**: It works only if the parameter “voice.tone.country” is set to Custom. **Web User Interface:** Settings->Tones->Congestion **Phone User Interface:** None		
voice.tone.callwaiting	String	Blank
Description: 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”. The default value is blank. **Note**: It works only if the parameter “voice.tone.country” is set to Custom. **Web User Interface:** Settings->Tones->Call Waiting **Phone User Interface:**		

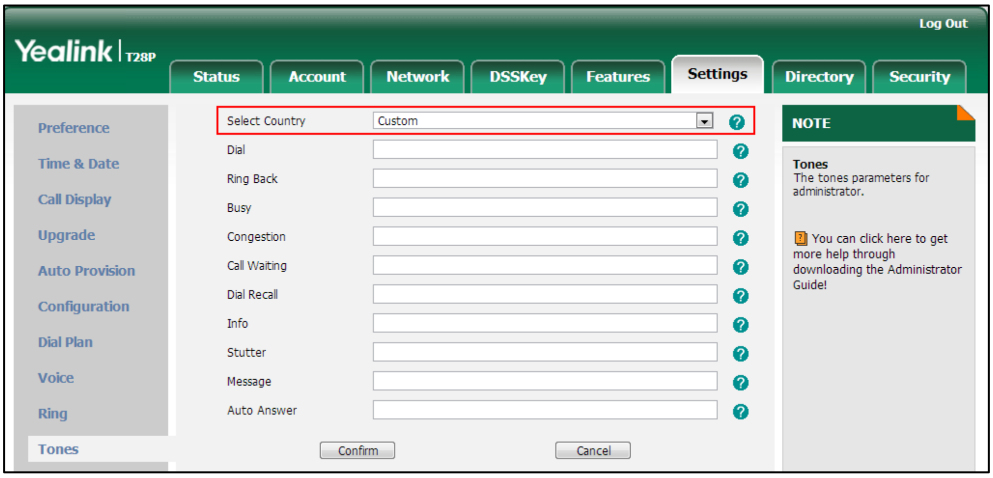
Parameters	Permitted Values	Default
None		
voice.tone.dialrecall	**String**	**Blank**
Description: Customizes the call back tone. The value format is Freq/Duration. For more information on the value format, refer to the parameter “voice.tone.dial”. **Note**: It works only if the parameter “voice.tone.country” is set to Custom. **Web User Interface:** Settings->Tones->Dial Recall **Phone User Interface:** None		
voice.tone.info	**String**	**Blank**
Description: Customizes the info tone. The phone will play the info tone with the special information, for example, the number you are calling is not in service. The value format is Freq/Duration. For more information on the value format, refer to the parameter “voice.tone.dial”. The default value is blank. **Note**: It works only if the parameter “voice.tone.country” is set to Custom. **Web User Interface:** Settings->Tones->Info **Phone User Interface:** None		
voice.tone.stutter	**String**	**Blank**
Description: Customizes the tone when the IP phone receives a voice mail. The value format is Freq/Duration. For more information on the value format, refer to the parameter “voice.tone.dial”. The default value is blank. **Note**: It works only if the parameter “voice.tone.country” is set to Custom. **Web User Interface:** Settings->Tones->Stutter		

Parameters	Permitted Values	Default
Phone User Interface: None		
voice.tone.message (not applicable to SIP-T20P IP phones)	String	Blank
Description: Customizes the tone when the IP phone receives a text message or voice message. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". The default value is blank. **Note**: It works only if the parameter "voice.tone.country" is set to Custom. **Web User Interface:** Settings->Tones->Message **Phone User Interface:** None		
voice.tone.autoanswer	String	Blank
Description: Customizes the warning tone for auto answer. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". The default value is blank. **Note**: It works only if the parameter "voice.tone.country" is set to Custom. **Web User Interface:** Settings->Tones->Auto Answer **Phone User Interface:** None		

To configure tones via web user interface:

1. Click on **Settings**->**Tones**.
2. Select the desired type from the pull-down list of **Select Country**.

If you select **Custom**, you can customize a tone for each condition of the IP phone.



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

Remote Phone Book

Remote phone book is a centrally maintained phone book, stored on the remote server. Users only need the access URL of the remote phone book. The IP phone can establish a connection with the remote server and download the phone book, and then display the remote phone book entries on the phone user interface. IP phones support up to 5 remote phone books. SIP-T28/T26P/T22P IP phones support up to 2500 remote phone book entries. Remote phone book is customizable. For more information how to customize a remote phone book, refer to Remote XML Phone Book on page 485.

Incoming/Outgoing Call lookup allows IP phones to search the entry names from the remote phone book for incoming/outgoing calls. Update Time Interval specifies how often IP phones refresh the local cache of the remote phone book.

Note Remote phone book is not applicable to SIP-T20P IP phones.

Procedure

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

Configuration File	<y0000000000xx>.cfg	Specify the access URL and the display name of the remote phone book. **Parameters:** remote_phonebook.data.X.url remote_phonebook.data.X.name remote_phonebook.display_name Specify whether to query the entry name from the remote phone book for

		outgoing/incoming calls. **Parameter:** features.remote_phonebook.enable Specify how often the IP phone refreshes the local cache of the remote phone book. **Parameter:** features.remote_phonebook.flash_time Specify whether to refresh the local cache of the remote phone book at a time when accessing the remote phone book. features.remote_phonebook.enter_update_enable
Local	Web User Interface	Specify the access URL of the remote phone book. **Navigate to**: http://<phoneIPAddress>/servlet?p=contacts-remote&q=load Specify whether to query the entry name from the remote phone book for outgoing/incoming calls. Specify how often the IP phone refreshes the local cache of the remote phone book. **Navigate to**: http://<phoneIPAddress>/servlet?p=contacts-remote&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
remote_phonebook.data.X.url (X ranges from 1 to 5)	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the remote phone book. **Example:** remote_phonebook.data.1.url = http://192.168.1.20/phonebook.xml **Note**: It is not applicable to SIP-T20P IP phones. **Web User Interface:** Directory->Remote Phone Book->Remote URL		

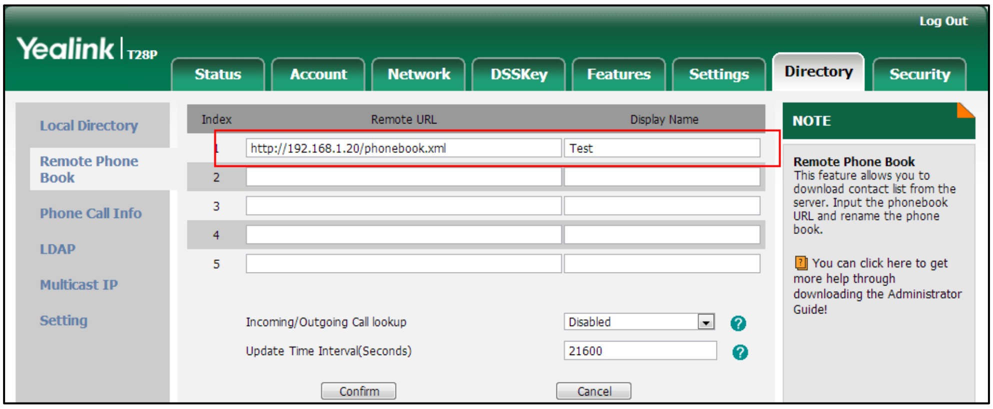
Parameters	Permitted Values	Default
Phone User Interface: None		
remote_phonebook.data.X.name (X ranges from 1 to 5)	String within 99 characters	Blank
Description: Configures the display name of the remote phone book item. **Example:** remote_phonebook.data.1.name = Test **Note**: It is not applicable to SIP-T20P IP phones. **Web User Interface:** Directory->Remote Phone Book->Display Name **Phone User Interface:** None		
remote_phonebook.display_name	String within 99 characters	Blank
Description: Configures the title of the remote phone book. If you leave it blank, Remote Phone Book is displayed on the LCD screen at the path Menu->Directory. **Example:** remote_phonebook.display_name = Remote Phone Book **Note**: It is not applicable to SIP-T20P IP phones. **Web User Interface:** None **Phone User Interface:** None		
features.remote_phonebook.enable	0 or 1	0
Description: Enables or disables the IP phone to perform a remote phone book search for an incoming or outgoing call and display the matched call on the LCD screen. **0**-Disabled **1**-Enabled **Note**: It is not applicable to SIP-T20P IP phones. **Web User Interface:**		

Parameters	Permitted Values	Default
Directory->Remote Phone Book->Incoming/Outgoing Call lookup **Phone User Interface:** None		
features.remote_phonebook.flash_time	**0, Integer from 3600 to 2592000**	**21600**
Description: Configures how often to refresh the local cache of the remote phone book. If it is set to 3600, the IP phone will refresh the local cache of the remote phone book every 3600 seconds. **Note**: If it is set to 0, the IP phone will refresh the local cache of the remote phone book aperiodically. It is not applicable to SIP-T20P IP phones. **Web User Interface:** Directory->Remote Phone Book->Update Time Interval(Seconds) **Phone User Interface:** None		
features.remote_phonebook.enter_update_enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to refresh the local cache of the remote phone book at a time when accessing the remote phone book.. **0**-Disabled **1**-Enabled **Web User Interface:** None **Phone User Interface:** None		

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

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

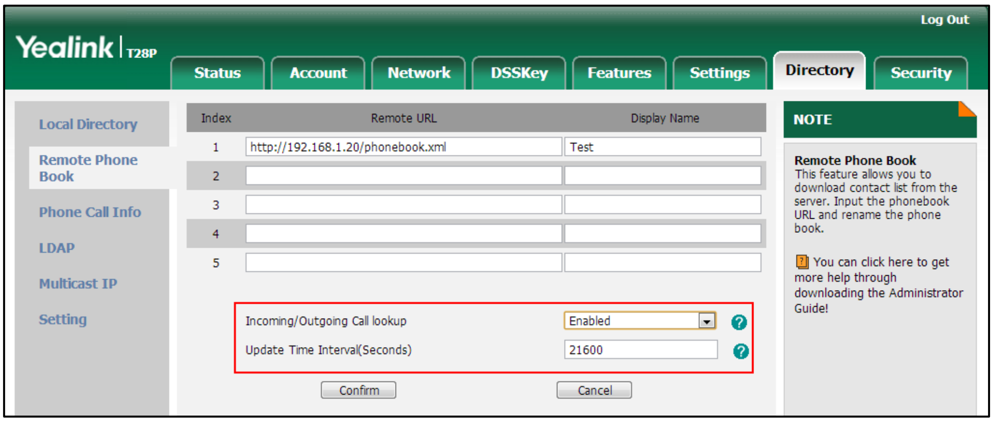
3. Enter the name in the **Display Name** field.



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

To configure 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.

LDAP

LDAP (Lightweight Directory Access Protocol) is an application protocol for accessing and maintaining information services for the distributed directory over an IP network. IP phones can be configured to interface with a corporate directory server that supports LDAP version 2 or 3. 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 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 phone are read only, which cannot be added, edited or deleted by users. When an LDAP server is properly configured, the IP phone can look up entries from the LDAP server in a wide variety of ways. The LDAP server indexes all the data in its entries, and "filters" can be used to select the desired entry or group, and return the desired information.

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

Note LDAP feature is not applicable to SIP-T20P IP phones.

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 phone is idle.

LDAP Attributes

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

Abbreviation	Name	Description
gn	givenName	First name
cn	commonName	LDAP attribute 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*, available online: http://www.yealink.com/DocumentDownload.aspx?CateId=142&flag=142.

Procedure

LDAP can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure LDAP. **Parameters:** 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 Assign an LDAP key. **Parameters:** memorykey.X.type/ linekey.X.type/ programablekey.X.type
Local	Web User Interface	Configure LDAP. **Navigate to**: http://<phoneIPAddress>/ servlet?p=contacts-LDAP &q=load Assign an LDAP key. **Navigate to**: http://<phoneIPAddress>/ servlet?p=dsskey&q=loa d&model=0
	Phone User Interface	Assign an LDAP key.

Details of Configuration Parameters:

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>ldap.enable</td><td>0 or 1</td><td>0</td></tr>
<tr><td colspan="3">Description:
Enables or disables LDAP feature on the IP phone.
0-Disabled
1-Enabled
Note: It is not applicable to SIP-T20P IP phones.
Web User Interface:
Directory->LDAP->Enable LDAP
Phone User Interface:
None</td></tr>
<tr><td>ldap.name_filter</td><td>String within 99 characters</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the criteria for searching the LDAP contact name attributes. The "*" symbol in the filter stands for any character. The "%" symbol in the filter stands for the entering string used as the prefix of the filter condition.
Example:
ldap.name_filter = (|(cn=%)(sn=%))
When the name prefix of the cn or sn of the contact record matches the search criteria, the record will be displayed on the LCD screen.
Note: It is not applicable to SIP-T20P IP phones.
Web User Interface:
Directory->LDAP->LDAP Name Filter
Phone User Interface:
None</td></tr>
<tr><td>ldap.number_filter</td><td>String within 99 characters</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the criteria for searching the LDAP contact number attributes. The "*" symbol in the filter stands for any character. The "%" symbol in the filter stands for the entering string used as the prefix of the filter condition.
Example:</td></tr>
</table>

Parameters	Permitted Values	Default
ldap.number_filter = (|(telephoneNumber=%)(Mobile=%)(ipPhone=%)) When the number prefix of the telephoneNumber, Mobile or ipPhone of the contact record matches the search criteria, the record will be displayed on the LCD screen. **Note**: It is not applicable to SIP-T20P IP phones. **Web User Interface:** Directory->LDAP->LDAP Number Filter **Phone User Interface:** None		
ldap.tls_mode	**Integer from 0 to 2**	**0**
Description: Configures the connection mode between the LDAP server and the IP phone. **0**-LDAP—Unencrypted connection between LDAP server and the IP phone. (port 389 is used by default). **1**-LDAP TLS Start—TLS/SSL connection between LDAP server and the IP phone (port 389 is used by default). **2**-LDAPs—TLS/SSL connection between LDAP server and the IP phone (port 636 is used by default). **Web User Interface:** Directory->LDAP->LDAP TLS Mode **Phone User Interface:** None		
ldap.host	**String within 99 characters**	**Blank**
Description: Configures the IP address or domain name of the LDAP server. **Example:** ldap.host = 192.168.1.20 **Note**: It is not applicable to SIP-T20P IP phones. **Web User Interface:** Directory->LDAP->Server Address **Phone User Interface:** None		

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>ldap.port</td><td>Integer from 1 to 65535</td><td>389</td></tr>
<tr><td colspan="3">Description:
Configures the port of the LDAP server.
Example:
ldap.port = 389
Note: It is not applicable to SIP-T20P IP phones.
Web User Interface:
Directory->LDAP->Port
Phone User Interface:
None</td></tr>
<tr><td>ldap.base</td><td>String within 99 characters</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the LDAP search base which corresponds to the location of the LDAP phone book from which the LDAP search request begins. The search base narrows the search scope and decreases directory search time.
Example:
ldap.base = dc=yealink,dc=cn
Note: It is not applicable to SIP-T20P IP phones.
Web User Interface:
Directory->LDAP->Base</td></tr>
<tr><td>ldap.user</td><td>String within 99 characters</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the user name used to login the LDAP server.
This parameter can be left blank in case the server allows anonymous to login. Otherwise you will need to provide the user name to login the LDAP server.
Example:
ldap.user = cn=manager,dc=yealink,dc=cn
Note: It is not applicable to SIP-T20P IP phones.
Web User Interface:
Directory->LDAP->Username
Phone User Interface:</td></tr>
</table>

Parameters	Permitted Values	Default
None		
ldap.password	**String within 99 characters**	**Blank**
Description: Configures the password to login the LDAP server. This parameter can be left blank in case the server allows anonymous to login. Otherwise you will need to provide the password to login the LDAP server. **Example:** ldap.password = secret **Note**: It is not applicable to SIP-T20P IP phones. **Web User Interface:** Directory->LDAP->Password **Phone User Interface:** None		
ldap.max_hits	**Integer from 1 to 32000**	**50**
Description: Configures the maximum number of search results to be returned by the LDAP server. If the value of the "Max.Hits" is blank, the LDAP server will return all searched results. Please note that a very large value of the "Max. Hits" will slow down the LDAP search speed, therefore it should be configured according to the available bandwidth. **Example:** ldap.max_hits = 50 **Note**: It is not applicable to SIP-T20P IP phones. **Web User Interface:** Directory->LDAP->Max. Hits (1~32000) **Phone User Interface:** None		
ldap.name_attr	**String within 99 characters**	**Blank**

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td colspan="3">Description:
Configures the name attributes of each record to be returned by the LDAP server. It compresses the search results. You can configure multiple name attributes separated by spaces.
Example:
ldap.name_attr = cn sn
Note: It is not applicable to SIP-T20P IP phones.
Web User Interface:
Directory->LDAP->LDAP Name Attributes
Phone User Interface:
None</td></tr>
<tr><td>ldap.numb_attr</td><td>String within 99 characters</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the number attributes of each record to be returned by the LDAP server. You can configure multiple number attributes separated by spaces.
Example:
ldap.numb_attr = telephoneNumber
Note: It is not applicable to SIP-T20P IP phones.
Web User Interface:
Directory->LDAP->LDAP Number Attributes
Phone User Interface:
None</td></tr>
<tr><td>ldap.display_name</td><td>String within 99 characters</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the display name of the contact record displayed on the LCD screen. The value must start with "%" symbol.
Example:
ldap.display_name = %cn
The cn of the contact record is displayed on the LCD screen.
Note: It is not applicable to SIP-T20P IP phones.
Web User Interface:
Directory->LDAP->LDAP Display Name</td></tr>
</table>

Parameters	Permitted Values	Default
Phone User Interface: None		
ldap.version	**2 or 3**	**3**
Description: Configures the LDAP protocol version supported by the IP phone. Make sure the protocol value corresponds with the version assigned on the LDAP server. **Note**: It is not applicable to SIP-T20P IP phones. **Web User Interface:** Directory->LDAP->Protocol **Phone User Interface:** None		
ldap.call_in_lookup	**0 or 1**	**0**
Description: Enables or disables the IP phone to perform an LDAP search when receiving an incoming call. **0**-Disabled **1**-Enabled **Note**: It is not applicable to SIP-T20P IP phones. **Web User Interface:** Directory->LDAP->LDAP Lookup For Incoming Call **Phone User Interface:** None		
ldap.call_out_lookup	**0 or 1**	**1**
Description: Enables or disables the IP phone to perform an LDAP search when placing a call. **0**-Disabled **1**-Enabled **Web User Interface:** Directory->LDAP->LDAP Lookup For Callout **Phone User Interface:** None		

Parameters	Permitted Values	Default
ldap.ldap_sort	0 or 1	0
Description: Enables or disables the IP phone to sort the search results in alphabetical order or numerical order. **0**-Disabled **1**-Enabled **Note**: It is not applicable to SIP-T20P IP phones. **Web User Interface:** Directory->LDAP->LDAP Sorting Results **Phone User Interface:** None		

LDAP Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 513.

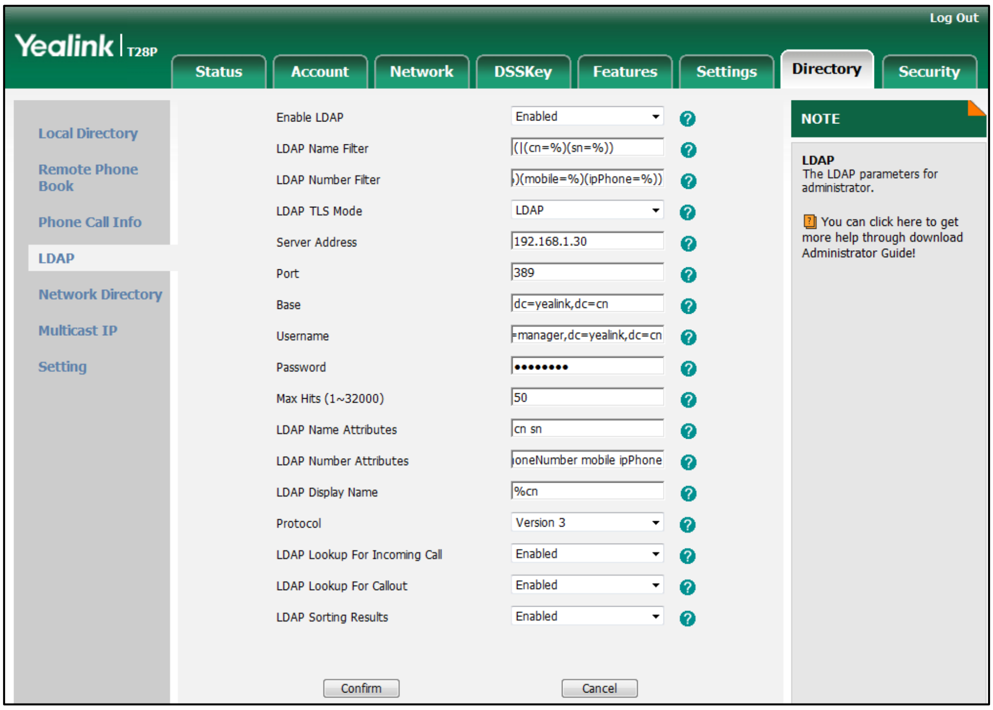
Parameters	Permitted Values	Default
memorykey.X.type/ linekey.X.type/ programablekey.X.type	38	Refer to the following content
Description: Configures a DSS key as an LDAP key on the IP phone. The digit **38** stands for the key type **LDAP**. For memory keys: X ranges from 1 to 10 (for SIP-T28/T26P). For line keys: X ranges from 1 to 6 (for SIP-T28P) X ranges from 1 to 3 (for SIP-T26P/T22P). For programable keys: X ranges from 1 to 14 (for SIP-T28/T26P) X=1-10, 14 (for SIP-T22P) **Example:** memorykey.1.type = 38 **Default:**		

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td colspan="3">For memory keys:
The default value is 0.
For line keys:
The default value is 15.
For programable keys:
For SIP-T28P/T26P IP phones:
When X=1, the default value is 28 (History).
When X=2, the default value is 61 (Directory).
When X=3, the default value is 5 (DND).
When X=4, the default value is 30 (Menu).
When X=5, the default value is 28 (History).
When X=6, the default value is 61 (Directory).
When X=7, the default value is 31 (Switch Account).
When X=8, the default value is 31 (Switch Account).
When X=9, the default value is 33 (Status).
When X=10, the default value is 0 (NA).
When X=11, the default value is 0 (NA).
When X=12, the default value is 0 (NA).
When X=13, the default value is 0 (NA).
When X=14, the default value is 2 (Forward).
For SIP-T22P IP phones:
When X=1, the default value is 28 (History).
When X=2, the default value is 61 (Directory).
When X=3, the default value is 5 (DND).
When X=4, the default value is 30 (Menu).
When X=5, the default value is 28 (History).
When X=6, the default value is 61 (Directory).
When X=7, the default value is 31 (Switch Account).
When X=8, the default value is 31 (Switch Account).
When X=9, the default value is 33 (Status).
When X=10, the default value is 0 (NA).
When X=14, the default value is 2 (Forward).
Note: It is not applicable to SIP-T20P IP phones.
Web User Interface:
DSSKey->Memory Key/ Line Key / Programable Key ->Type</td></tr>
</table>

Parameters	Permitted Values	Default
Phone User Interface: Menu->Features->DSS Keys->Memory Keys (or Line Keys)->DSS Key X (or Line Key X)->Type		

To configure LDAP via web user interface:

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



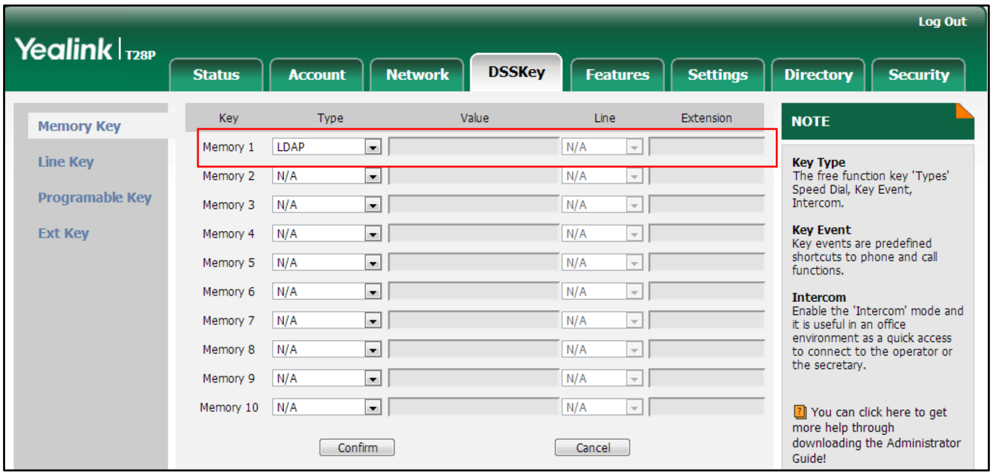
4. Click **Confirm** to accept the change.

To configure an LDAP key via web user interface:

1. Click on **DSSKey**->**Memory Key** (**Line Keys** or **Programable Key**).

   SIP-T22P/T20P IP phones only support line keys and programable keys.

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



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

To configure an LDAP key via phone user interface:

1. Press **Menu**->**Features**->**DSS Keys**->**Memory Keys** (or **Line Keys**).
2. Select the desired DSS key.
3. Press or , or the **Switch** soft key to select **Key Event** from the **Type** field.
4. Press or , or the **Switch** soft key to select **LDAP** from the **Key Type** field.
5. Press the **Save** soft key to accept the change.

Busy Lamp Field

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

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

Visual Alert and Audio Alert for BLF Pickup

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

Pickup on page 219.

Note Visual alert for BLF pickup feature is not applicable to SIP-T20P IP phones.

BLF LED Mode

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

BLF LED mode feature is also applicable to BLF list key. For more information on BLF List key, refer to BLF List on page 303.

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

LED Status	Description
Solid green	The monitored user is idle.
Fast flashing green (200ms)	The monitored user receives an incoming call.
Slow flashing green (500ms)	The monitored user is dialing. The monitored user is talking. The monitored user's conversation is placed on hold (This LED status requires server support).
Slow flashing green (1s)	The call is parked against the monitored user's phone number.
Off	The monitored user does not exist.

Memory key LED (configured as a BLF key or a BLF List key and BLF LED Mode is set to 0)

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

Line key LED (configured as a BLF key or a BLF List key and BLF LED Mode is set to 1)

LED Status	Description
Fast flashing green (200ms)	The monitored user receives an incoming call.

LED Status	Description
Solid green	The monitored user is dialing. The monitored user is talking. The monitored user's conversation is placed on hold (This LED status requires server support).
Slow flashing green (1s)	The call is parked against the monitored user's phone number.
Off	The monitored user is idle. The monitored user does not exist.

Memory key LED (configured as a BLF key or a BLF List key and BLF LED Mode is set to 1)

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

Line key LED (configured as a BLF key or a BLF List key and BLF LED Mode is set to 2)

LED Status	Description
Fast flashing green (200ms)	The monitored user receives an incoming call.
Slow flashing green (500ms)	The monitored user is dialing. The monitored user is talking. The monitored user's conversation is placed on hold (This LED status requires server support).
Slow flashing green (1s)	The call is parked against the monitored user's phone number.
Off	The monitored user is idle. The monitored user does not exist.

Memory key LED (configured as a BLF key or a BLF List key and BLF LED Mode is set to 2)

LED Status	Description
Fast flashing red (200ms)	The monitored user receives an incoming call.
Solid red	The monitored user is dialing. The monitored user is talking.

LED Status	Description
	The monitored user's conversation is placed on hold (This LED status requires server support).
Slow flashing red (1s)	The monitored user's conversation is placed on hold.
Off	The monitored user is idle. The monitored user does not exist.

Line key LED (configured as a BLF key or a BLF List key and BLF LED Mode is set to 3)

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

Memory key LED (configured as a BLF key or a BLF List key and BLF LED Mode is set to 3)

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

Procedure

BLF can be configured using the configuration files or locally.

Configuration File	y0000000000xx.cfg	Specify whether to use visual alert and audio alert for BLF pickup. **Parameters:** features.pickup.blf_visual_enable features.pickup.blf_audio_enable Assign a BLF key. **Parameters:** memorykey.X.type/ linekey.X.type memorykey.X.line/ linekey.X.line memorykey.X.value/ linekey.X.value memorykey.X.pickup_value/ linekey.X.pickup_value Configure BLF LED mode. **Parameter:** features.blf_led_mode
Local	Web User Interface	Assign a BLF key. **Navigate to**: http://<phoneIPAddress>/servlet?p=dskey&q=load&model=0 Specify whether to use visual alert and audio alert for BLF pickup. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-callpickup&q=load Configure BLF LED mode. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load
	Phone User Interface	Assign a BLF key.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.pickup.blf_visual_enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to display a visual alert when the monitored user receives an incoming call. **0**-Disabled **1**-Enabled **Note**: It is not applicable to SIP-T20P IP phones. **Web User Interface:** Features->Call Pickup->Visual Alert for BLF Pickup **Phone User Interface:** None		
features.pickup.blf_audio_enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to play an audio alert when the monitored user receives an incoming call. **0**-Disabled **1**-Enabled **Web User Interface:** Features->Call Pickup->Audio Alert for BLF Pickup **Phone User Interface:** None		
features.blf_led_mode	**0, 1, 2 or 3**	**0**
Description: Configures BLF LED mode and provides four kinds of definition for the BLF key LED status. **Web User Interface:** Features->General Information->BLF LED Mode **Phone User Interface:** None		

BLF Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 513.

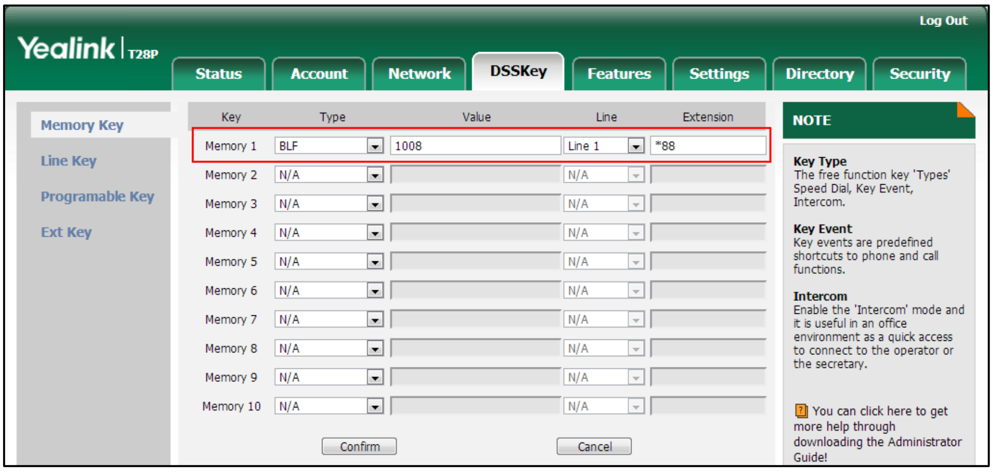
Parameters	Permitted Values	Default
memorykey.X.type/ linekey.X.type	**Integer**	**0 for memory key,** **15 for line key**
Description: Configures a DSS key as a BLF key on the IP phone. The digit **16** stands for the key type **BLF**. For the memory key, x ranges from 1 to 10. For the line key, x ranges from 1 to 6. **Example:** memorykey.1.type = 16 **Web User Interface:** DSSKey->Memory Key (or Line Key)->Type **Phone User Interface:** Menu->Features->DSS Keys->Memory Keys (or Line Keys)->DSS Key X (or Line Key X)->Type		
memorykey.X.line/ linekey.X.line	**Integer**	**Blank for memory key,** **1-6 for lines 1-6**
Description: Configures the desired line to apply the BLF key. For the memory key, x ranges from 1 to 10. For the line key, x ranges from 1 to 6. **Example:** memorykey.1.line = 1 **Web User Interface:** DSSKey->Memory Key(or Line Key)->Line **Phone User Interface:** Menu->Features->DSS Keys->Memory Keys (or Line Keys)->DSS Key X (or Line Key X)->Account ID		
memorykey.X.value/ linekey.X.value	**String within 99 characters**	**blank**

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td colspan="3">Description:
Configures the number of the monitored user.
For the memory key, x ranges from 1 to 10.
For the line key, x ranges from 1 to 6.
Example:
memorykey.1.value = 1008
Web User Interface:
DSSKey->Memory Key (or Line Key)->Value</td></tr>
<tr><td>memorykey.X.pickup_value/
linekey.X.pickup_value</td><td>String within 256 characters</td><td>blank</td></tr>
<tr><td colspan="3">Description:
Configures the pickup code for BLF feature.
This parameter only applies to BLF feature.
For the memory key, x ranges from 1 to 10.
For the line key, x ranges from 1 to 6.
Example:
memorykey.1.pickup_value = *88
Web User Interface:
DSSKey->Memory Key (or Line Key) ->Extension
Phone User Interface:
Menu->Features->DSS Keys->Memory Keys (or Line Keys)->DSS Key X (or Line Key X)->Value</td></tr>
</table>

To configure a BLF key via web user interface:

1. Click on **DSSKey**->**Memory Key** (or **Line Key**).
2. In the desired DSS key field, select **BLF** from the pull-down list of **Type**.
3. Enter the phone number or extension you want to monitor in the **Value** field.
4. Select the desired line from the pull-down list of **Line**.

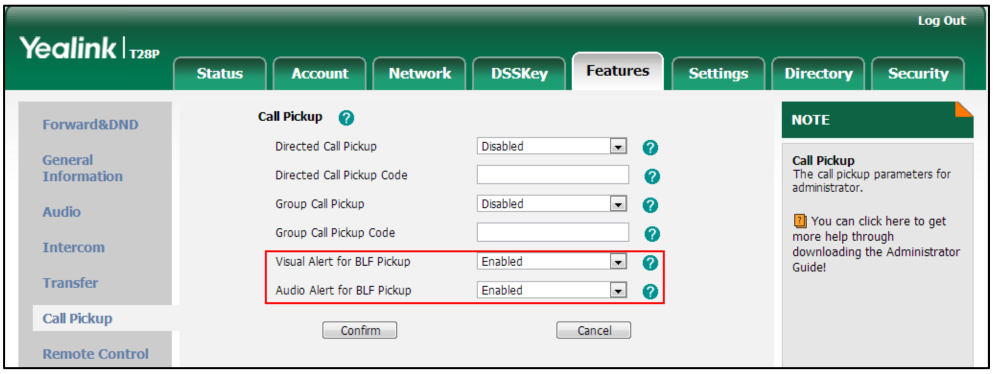
5. (Optional.) Enter the directed call pickup code in the **Extension** field.



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

To configure visual alert and audio alert for BLF pickup via web user interface:

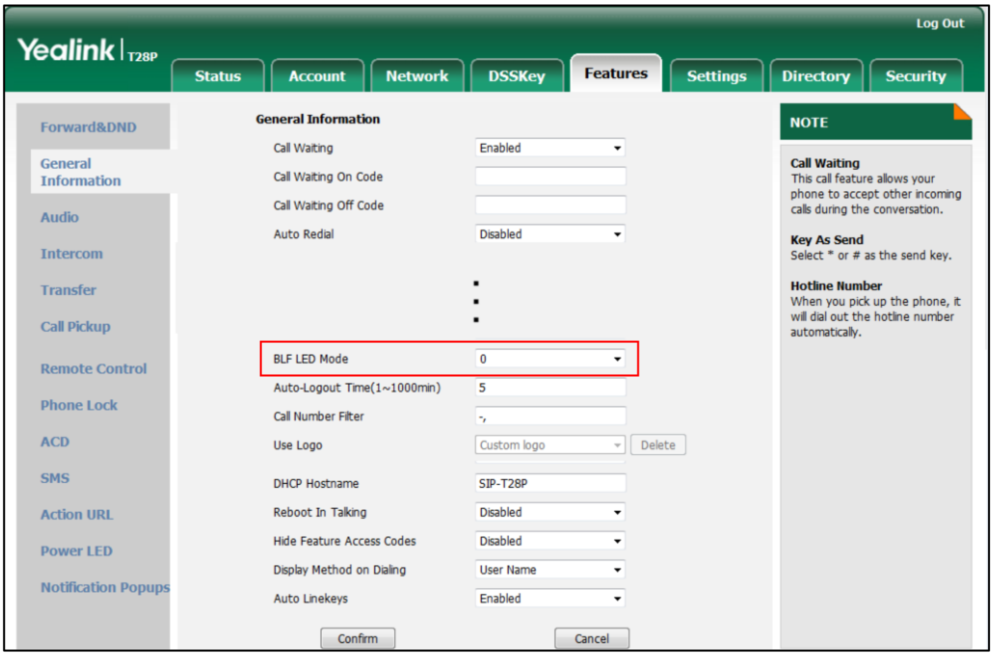
1. Click on **Features**->**Call Pickup**.
2. Select the desired value from the pull-down list of **Visual Alert for BLF Pickup**.
3. Select the desired value from the pull-down list of **Audio Alert for BLF Pickup**.



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

To configure BLF LED mode via web user interface:

1. Click on **Features**->**General Information**.
2. Select the desired value from the pull-down list of **BLF LED Mode**.



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

To configure a BLF key via phone user interface:

1. Press **Menu**->**Features**->**DSS Keys**->**Memory Keys** (or **Line Keys**).
2. Select the desired DSS key.
3. Press or , or the **Switch** soft key to select **BLF** from the **Type** field.
4. Press or , or the **Switch** soft key to select the desired line from the **Account ID** field.
5. Enter the phone number or extension you want to monitor in the **Value** field.
6. (Optional.) Enter the directed call pickup code in the **Extension** field.
7. Press the **Save** soft key to accept the change.

BLF List

Busy Lamp Field (BLF) List allows a list of specific extensions to be monitored for status changes. It enables the monitoring phone to subscribe to a list of users, and receive notifications of the status of monitored users. Different indicators on the monitoring phone show the status of monitored users. The monitoring user can also be notified about calls being parked/no longer parked against any monitored user. IP phones support BLF list using a SUBSCRIBE/NOTIFY mechanism as specified in RFC 3265. This feature depends on support from a SIP server.

Note BLF list feature is applicable to IP phones running firmware version 73 or later in the neutral version.

Procedure

BLF List can be configured using the configuration files or locally.

Configuration File	y0000000000xx.cfg	Configure BLF List. **Parameters:** account.X.blf.blf_list_uri account.X.blf_list_code account.X.blf_list_barge_in_code account.X.blf_list_retrieve_call_parked_code Specify whether to automatically configure the BLF list keys. **Parameter:** phone_setting.auto_blf_list_enable Configure the order of BLF list keys assigned automatically. **Parameter:** phone_setting.blf_list_sequence_type Assign a BLF List key. **Parameters:** memorykey.X.type/linekey.X.type memorykey.X.line/linekey.X.line
Local	Web User Interface	Configure BLF List. http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0 Assign a BLF List key.

		Navigate to: http://<phoneIPAddress>/servlet?p=dskey&q=load&model=0
	Phone User Interface	Assign a BLF List key.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.blf.blf_list_uri	**String within 256 characters**	**Blank**
Description: Configures the BLF List URI to monitor a list of users for account X. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Example:** account.1.blf.blf_list_uri = 4609@pbx.yealink.com **Web User Interface:** Account->Advanced->BLF List URI **Phone User Interface:** None		
account.X.blf_list_code	**String within 32 characters**	**Blank**
Description: Configures the directed pickup code for account X. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Example:** account.1.blf_list_code = *97 **Web User Interface:** Account->Advanced->BLF List Code **Phone User Interface:** None		

Parameters	Permitted Values	Default
account.X.blf_list_barge_in_code	String within 32 characters	Blank
Description: Configures the barge-in code for account X. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Example:** account.1.blf_list_barge_in_code = *33 **Web User Interface:** Account->Advanced->BLF List Barge In Code **Phone User Interface:** None		
account.X.blf_list_retrieve_call_parked_code	String within 32 characters	Blank
Description: Configures the call park retrieve code for account X. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Example:** account.1.blf_list_retrieve_call_parked_code = *88 **Web User Interface:** Account->Advanced->BLF List Retrieve Call Parked Code **Phone User Interface:** None		
phone_setting.auto_blf_list_enable	0 or 1	1
Description: Enables or disables the IP phone to automatically configure the BLF list keys. **0**-Disabled **1**-Enabled **Web User Interface:**		

Parameters	Permitted Values	Default
None **Phone User Interface:** None		
phone_setting.blf_list_sequence_type	**0 or 1**	**0**
Description: Configures the order of BLF list keys assigned automatically. **0**-Line Key->Memory Key->Ext Key **1**-Ext Key->Memory Key->Line Key **Note**: It is only applicable to SIP-T28P, SIP-T26P IP phones. **Web User Interface:** None **Phone User Interface:** None		

BLF List Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 513.

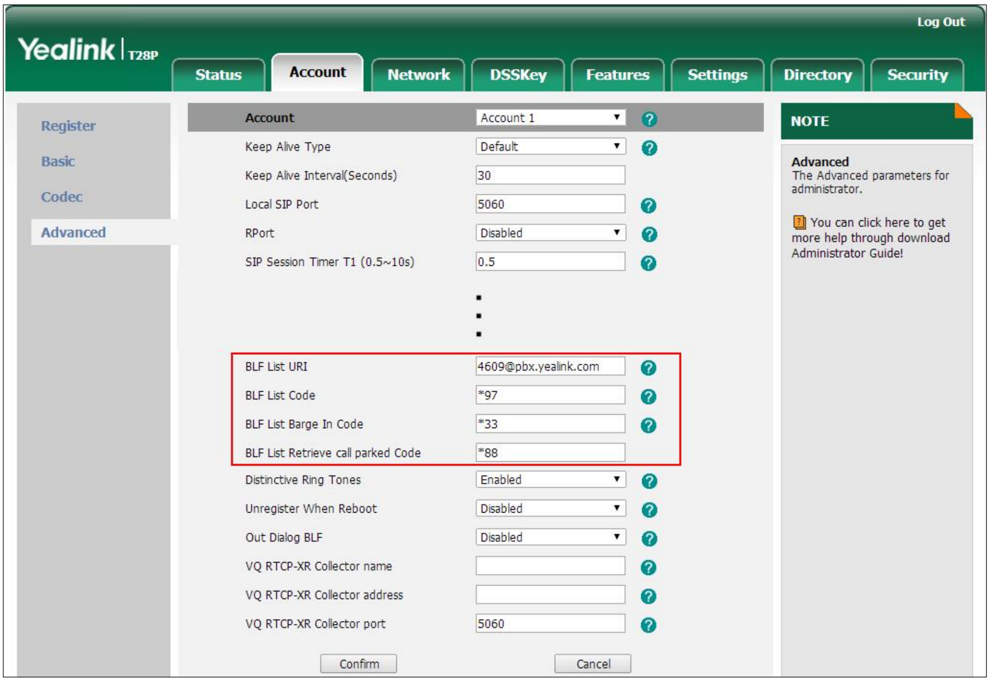
Parameters	Permitted Values	Default
memorykey.X.type/linekey.X.type	**Integer**	**0 for memory key, 15 for line key**
Description: Configures a DSS key as a BLF List key on the IP phone. The digit **39** stands for the key type **BLF List**. For the memory key, x ranges from 1 to 10. For the line key, x ranges from 1 to 6. **Example:** memorykey.1.type = 39 **Note**: It is only for SIP-T28P/T26P IP phones. **Web User Interface:** DSSKey->Memory Key (or Line Key)->Type **Phone User Interface:**		

Parameters	Permitted Values	Default
Menu->Features->DSS Keys->Memory Keys (or Line Keys)->DSS Key X (or Line Key X)->Type		
memorykey.X.line/linekey.X.line	Integer	blank for memory key, 1-6 for lines 1-6
Description: Configures the desired line to apply the BLF List key. For the memory key, x ranges from 1 to 10. For the line key, x ranges from 1 to 6. **Example:** memorykey.1.line = 1 **Note**: It is only for SIP-T28P/T26P IP phones. **Web User Interface:** DSSKey->Memory Key (or Line Key)->Line **Phone User Interface:** Menu->Features->DSS Keys->Memory Keys (or Line Keys)->DSS Key X (or Line Key X)->Account ID		

To configure the BLF List settings via web user interface:

1. Click on **Account**.
2. Select the desired account from the pull-down list of **Account**.
3. Click on **Advanced**.
4. Enter the BLF List URI in the **BLF List URL** field.
5. (Optional.) Enter the directed pickup code in the **BLF List Code** field.
6. (Optional.) Enter the barge-in code in the **BLF List Barge In Code** field.

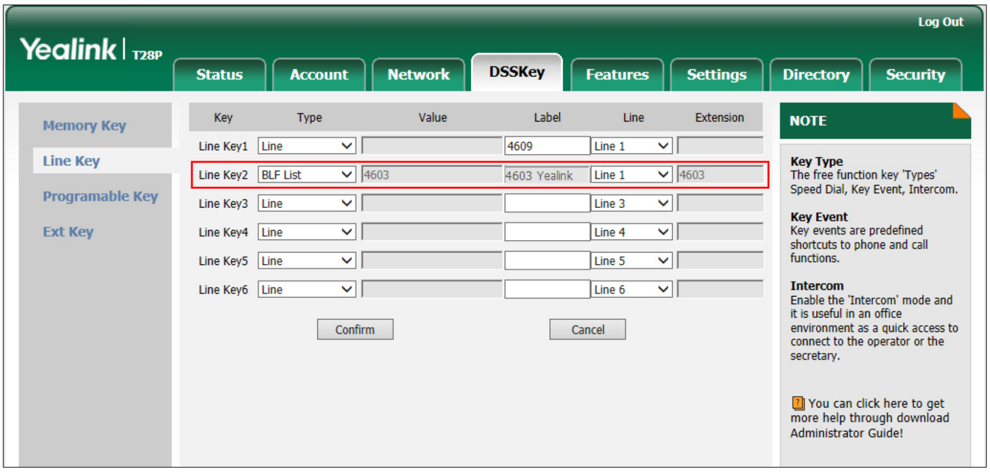
7. (Optional.) Enter the retrieve call parked code in the **BLF List Retrieve call parked Code** field.



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

To configure BLF List keys manually via web user interface:

1. Click on **DSSKey**->**Memory Key** (**Line Key** or **Programable Key**).
2. In the desired DSS key field, select **BLF List** from the pull-down list of **Type**.
3. Select the desired line from the pull-down list of **Line**.



4. Repeat step 2-3, configure more BLF list keys.
5. Click **Confirm** to accept the change.

Hide Features Access Code

Hide Features Access Code feature enables the IP phone to display the feature identifier instead of the dialed feature access code automatically. For example, the dialed call park code will be replaced by the identifier “Call Park” when you park an active call.

The hide feature access codes feature is applicable to the following features:

- Voice Mail
- Pick up
- Group Pick up
- Barge In
- Retrieve
- Call Park
- Group Park

Procedure

The hide feature access codes feature can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure the hide feature access codes feature: **Parameters:** features.hide_feature_access_codes.enable
Local	Web User Interface	Configure the hide feature access codes feature. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-general&q=load

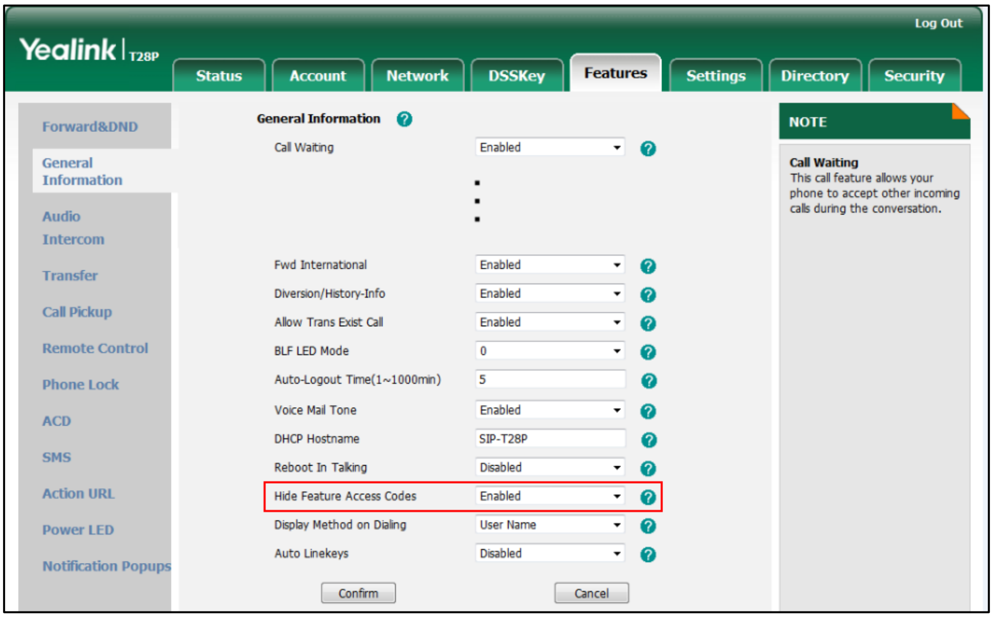
Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.hide_feature_access_codes.enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to display feature name instead of the feature access code when dialing and in talk.		

Parameters	Permitted Values	Default
0-Disabled **1**-Enabled **Web User Interface:** Features->General Information->Hide Feature Access Codes **Phone User Interface:** None		

To enable hide feature access codes feature via web user interface:

1. Click on **Features->General Information**.
2. Select **Enabled** from the pull-down list of **Hide Feature Access Codes.**



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. IP phones support both audio and visual MWI when receiving new voice messages.

IP phones support both solicited and unsolicited MWI. Unsolicited MWI is a server related feature.

The IP phone sends a SUBSCRIBE message to the server for message-summary updates. The server sends a message-summary NOTIFY within the subscription dialog each time the MWI status changes. For solicited MWI, you must enable MWI subscription feature on IP phones. IP phones support subscribing the MWI messages to the account or the voice mail number.

IP phones do not need to subscribe for message-summary updates. The server automatically sends a message-summary NOTIFY in a new dialog each time the MWI status changes.

Procedure

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

Configuration File	<MAC>.cfg	Configure subscribe for MWI. **Parameters:** account.X.subscribe_mwi account.X.subscribe_mwi_expires account.X.subscribe_mwi_to_vm Configure subscribe MWI to voice mail. **Parameter:** voice_mail.number.X Configure the presentation of audio and visual MWI. **Parameter:** account.X.display_mwi.enable
Local	Web User Interface	Configure subscribe for MWI. Configure subscribe MWI to voice mail. Configure the presentation of audio and visual MWI. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.subscribe_mwi	**0 or 1**	**0**
Description: Enables or disables the IP phone to subscribe the message waiting indicator for account X. **0**-Disabled		

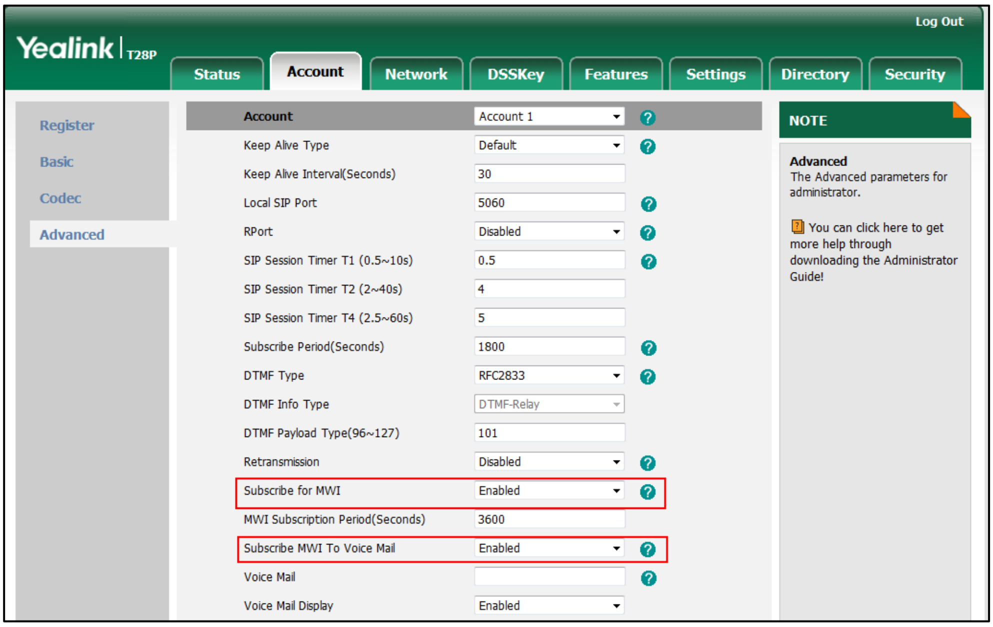
Parameters	Permitted Values	Default
1-Enabled If it is set to 1 (Enabled), the IP phone will send a SUBSCRIBE message to the server for message-summary updates. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Web User Interface:** Account->Advanced->Subscribe for MWI **Phone User Interface:** None		
account.X.subscribe_mwi_expires	**Integer from 0 to 84600**	**3600**
Description: Configures MWI subscribe expiry time (in seconds) for account X. The IP phone is able to successfully refresh the SUBSCRIBE for message-summary events before expiration of the SUBSCRIBE dialog. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Note**: It works only if the parameter "account.X.subscribe_mwi" is set to 1 (Enabled). **Web User Interface:** Account->Advanced->MWI Subscription Period (Seconds) **Phone User Interface:** None		
account.X.subscribe_mwi_to_vm	**0 or 1**	**0**
Description: Enables or disables the IP phone to subscribe the message waiting indicator to the voice mail number for account X. **0**-Disabled **1**-Enabled X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P).		

Parameters	Permitted Values	Default
Note: It works only if the parameters "account.X.subscribe_mwi" is set to 1 (Enabled) and "voice_mail.number.X" is configured. **Web User Interface:** Account->Advanced->Subscribe MWI To Voice Mail **Phone User Interface:** None		
voice_mail.number.X	**String within 99 characters**	**Blank**
Description: Configures the voice mail number for account X. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Example:** voice_mail.number.1 = 1234 **Note**: It works only if the parameter "account.X.subscribe_mwi_to_vm" is set to 1 (Enabled). **Web User Interface:** Account->Advanced->Voice Mail **Phone User Interface:** None		
account.X.display_mwi.enable	**0 or 1**	**1**
Description: Enables or disables the IP phone to support audio and visual MWI when receiving new voice messages. **0**-Disabled **1**-Enabled X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Note**: It always works at the time of Unsolicited MWI; but it works only if the parameters "account.X.subscribe_mwi_to_vm" and "account.X.subscribe_mwi" are set to 1 (Enabled) and "voice_mail.number.X" is configured at the time of solicited MWI.		

Parameters	Permitted Values	Default
Web User Interface: Account->Advanced->Voice Mail Display **Phone User Interface:** None		

To configure subscribe for MWI via web user interface:

1. Click on **Account**.
2. Select the desired account from the pull-down list of **Account**.
3. Click on **Advanced**.
4. Select the desired value from the pull-down list of **Subscribe for MWI**.
5. Enter the period time in the **MWI Subscription Period (Seconds)** field.

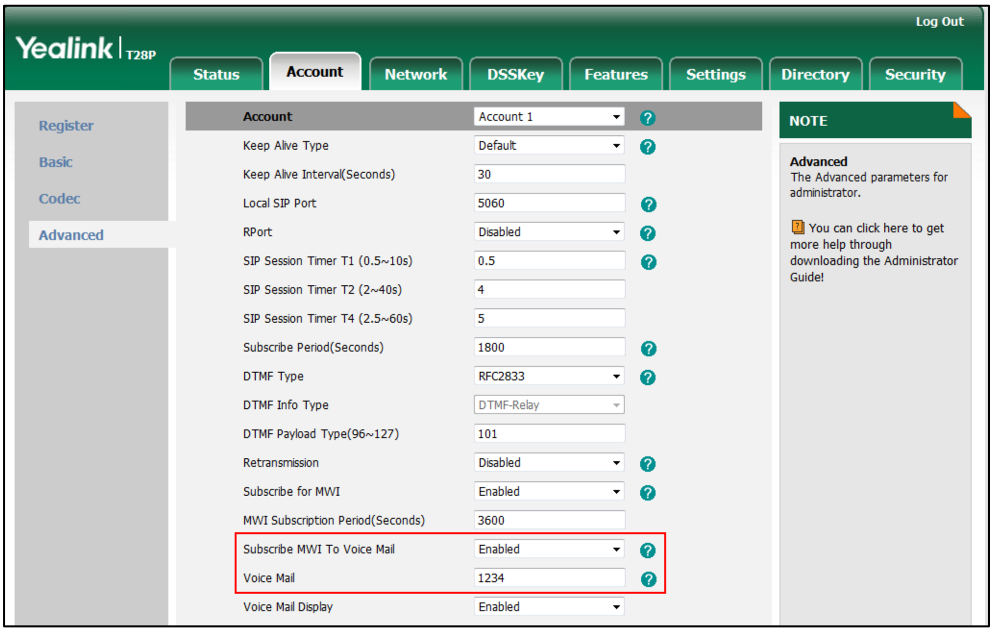


6. Click **Confirm** to accept the change.

To configure subscribe MWI to voice mail via web user interface:

1. Click on **Account**.
2. Select the desired account from the pull-down list of **Account**.
3. Click on **Advanced**.
4. Select the desired value from the pull-down list of **Subscribe MWI To Voice Mail**.

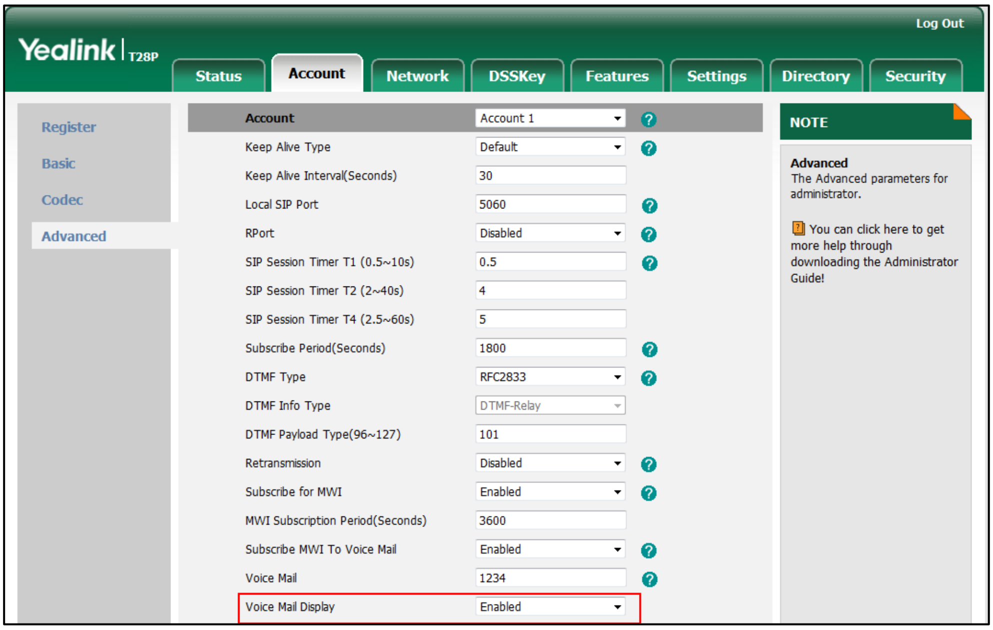
5. Enter the desired voice number in the **Voice Mail** field.



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

To configure the presentation of audio and visual MWI via web user interface:

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



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

Multicast Paging

Multicast paging allows IP phones to send/receive Real-time Transport Protocol (RTP) streams to/from the pre-configured multicast address(es) without involving SIP signaling. Up to 10 listening multicast addresses can be specified on the IP phone.

Sending RTP Stream

Users can send an RTP stream without involving SIP signaling by pressing a configured multicast paging key or a paging list key. A multicast address (IP: Port) should be assigned to the multicast paging key, which is defined to transmit RTP stream to a group of designated IP phones. When the IP phone sends the RTP stream to a pre-configured multicast address, each IP phone preconfigured to listen to the multicast address can receive the RTP stream. When the originator stops sending the RTP stream, the subscribers stop receiving it.

Procedure

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

Configuration File	<y0000000000xx>.cfg	Specify a multicast codec for the IP phone to use for multicast RTP. **Parameter:** multicast.codec Assign a multicast paging key. **Parameters:** memorykey.X.type/ linekey.X.type memorykey.X.value/ linekey.X.value Assign a paging list key. **Parameters:** memorykey.X.type/ linekey.X.type memorykey.X.value/ linekey.X.value Configure the multicast IP address and port number for a paging list key. **Parameter:** multicast.paging_address.X.ip_address Configure the multicast paging

		group name for a paging list key. **Parameter:** multicast.paging_address.X.label
Local	Web User Interface	Assign a multicast paging key or a paging list key. **Navigate to**: http://<phoneIPAddress>/servlet?p=dsskey&q=load&model=0 Specify a multicast codec for the IP phone to send the RTP stream. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load Configure the multicast IP address and port number for a paging list key. Configure the multicast paging group name for a paging list key. **Navigate to**: http://<phoneIPAddress>/servlet?p=contacts-multicastIP&q=load
	Phone User Interface	Assign a multicast paging key or a paging list key.

Details of the Configuration Parameter:

Parameters	Permitted Values	Default
multicast.codec	**Refer to the following content**	**G722**
Description: Configures the codec of multicast paging. **Permitted Values:** PCMU, PCMA, G729, G722 **Example:** multicast.codec = G722 **Web User Interface:** Features->General Information->Multicast Codec **Phone User Interface:**		

Parameters	Permitted Values	Default
None		
multicast.paging_address.X.ip_address	String within 99 characters	Blank
Description: Configures the multicast IP address and port number. **Example:** multicast.paging_address.1.ip_address = 224.5.6.20:10008 multicast.paging_address.2.ip_address = 224.0.0.1:1001 **Note**: The valid multicast IP addresses range from 224.0.0.0 to 239.255.255.255. **Web User Interface:** Directory->Multicast IP->Paging Address **Phone User Interface:** Menu->Features->Paging List->Option->Edit->Address		
multicast.paging_address.X.label	String	Blank
Description: Configures the multicast paging group name. **Example:** multicast.paging_address.1.label = Product multicast.paging_address.2.label = Sales **Web User Interface:** Directory->Multicast IP->Label(Paging List) **Phone User Interface:** Menu->Features->Paging List->Option->Edit->Label		

Multicast Paging Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 513.

Parameters	Permitted Values	Default
memorykey.X.type/ linekey.X.type	Integer	0 for memory key, 15 for line key
Description:		

Parameters	Permitted Values	Default
Configures a DSS key as a multicast paging key on the IP phone. The digit **24** stands for the key type **Multicast Paging**. For the memory key, x ranges from 1 to 10. For the line key, x ranges from 1 to 6. **Example:** memorykey.1.type = 24 **Web User Interface:** DSSKey->Memory Key(or Line Key)>Type **Phone User Interface:** Menu->Features->DSS Keys->Memory Keys (or Line Keys)->DSS Key X (or Line Key X)->Type		
memorykey.X.value/ linekey.X.value	**String within 99 characters**	**Blank**
Description: Configures the multicast IP address and port number. For the memory key, x ranges from 1 to 10. For the line key, x ranges from 1 to 6. **Example:** memorykey.1.value = 224.5.5.6:10008 **Note**: The valid multicast IP addresses range from 224.0.0.0 to 239.255.255.255. **Web User Interface:** DSSKey->Memory Key(or Line Key)->Value **Phone User Interface:** Menu->Features->DSS Keys->Memory Keys (or Line Keys)->DSS Key X (or Line Key X)->Value		

Paging List key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 513.

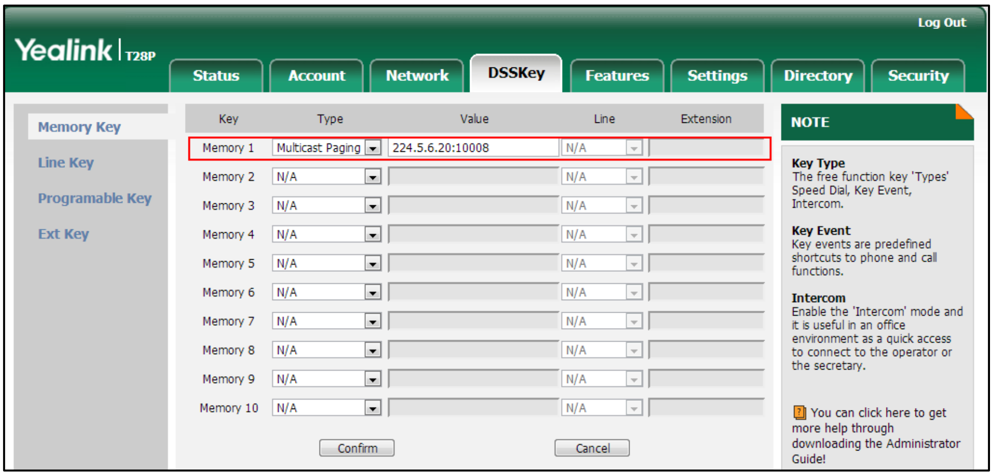
Parameters	Permitted Values	Default
memorykey.X.type/ linekey.X.type	**Integer**	**0 for memory key, 15 for line key**
Description:		

Parameters	Permitted Values	Default
Configures a DSS key as a paging list key on the IP phone. The digit **66** stands for the key type **Paging List**. For the memory key, x ranges from 1 to 10. For the line key, x ranges from 1 to 6. **Example:** memorykey.1.type = 66 **Web User Interface:** DSSKey->Memory Key(or Line Key)>Type **Phone User Interface:** Menu->Features->DSS Keys->Memory Keys (or Line Keys)->DSS Key X (or Line Key X)->Type		

To configure a multicast paging key via web user interface:

1. Click on **DSSKey**->**Memory Key** (or **Line Key**).
2. In the desired DSS key field, select **Multicast Paging** from the pull-down list of **Type**.
3. Enter the multicast IP address and port number in the **Value** field.

   The valid multicast IP addresses range from 224.0.0.0 to 239.255.255.255.

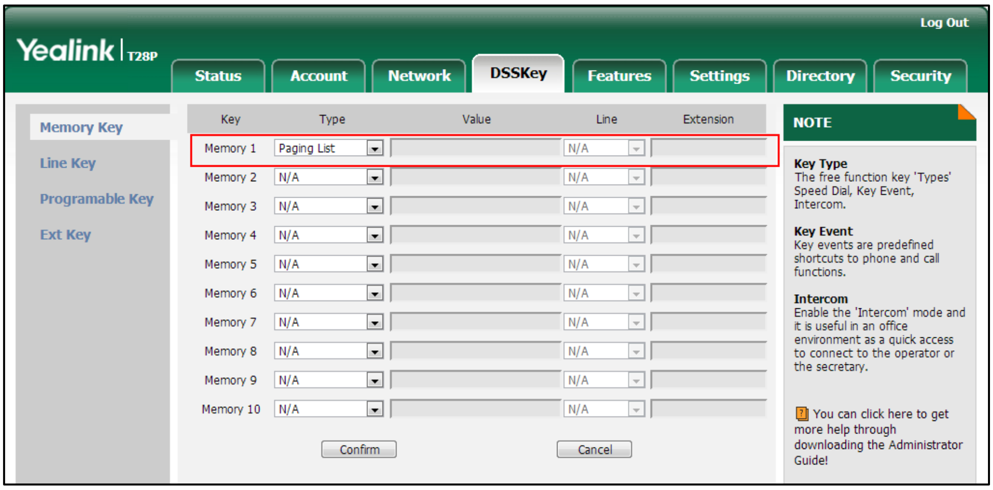


4. Click **Confirm** to accept the change.

To configure a paging list key via web user interface:

1. Click on **DSSKey**->**Memory Key** (or **Line Key**).

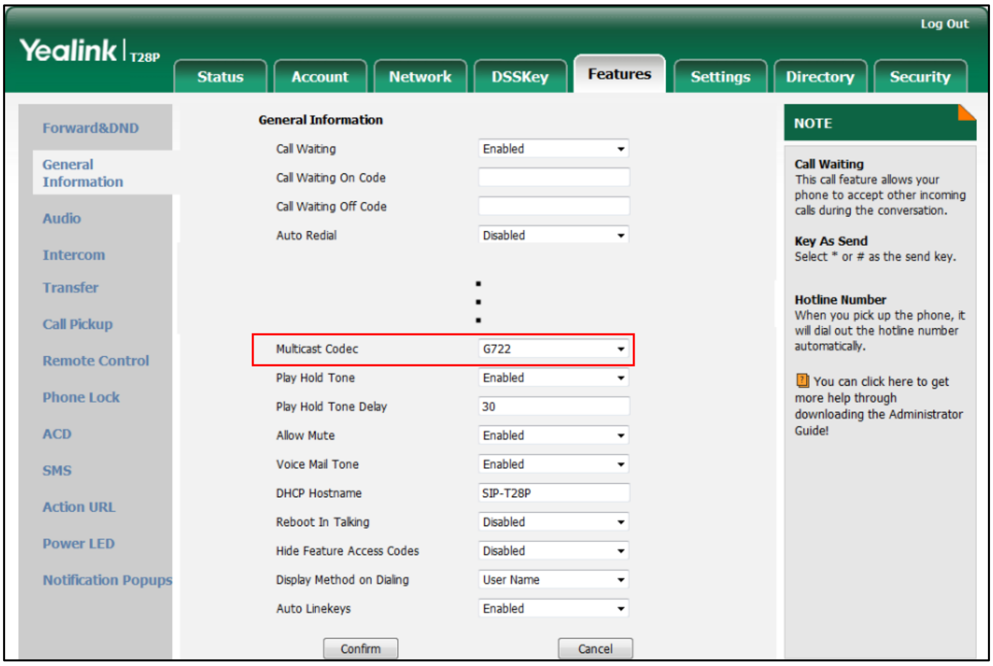
2. In the desired DSS key field, select **Paging List** from the pull-down list of **Type**.



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

To configure a codec for multicast paging via web user interface:

1. Click on **Features**->**General Information**.
2. Select the desired codec from the pull-down list of **Multicast Codec**.

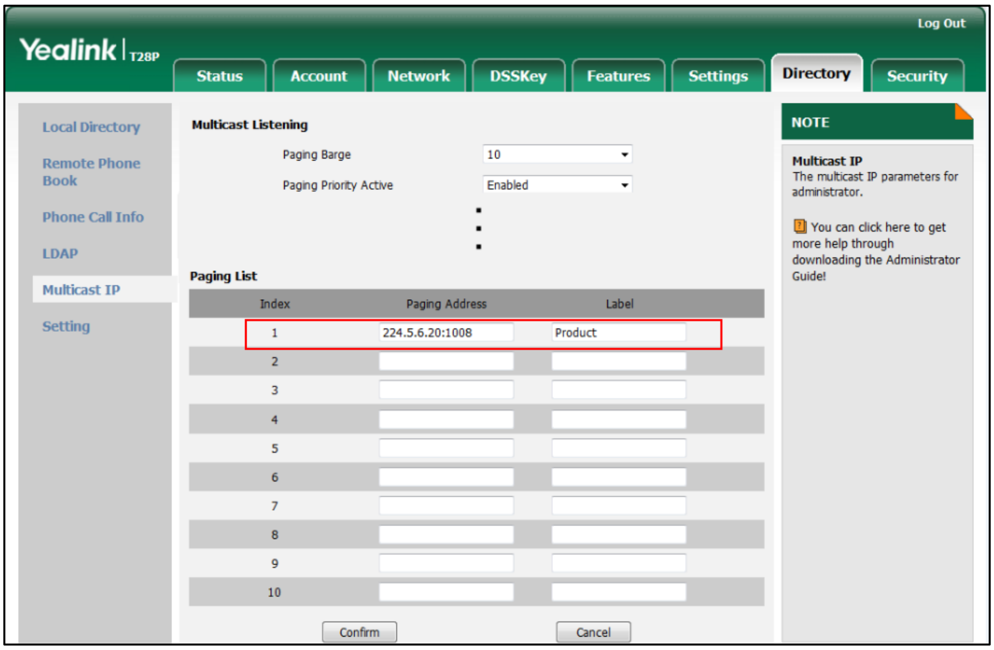


3. Click **Confirm** to accept the change.

To configure two sending multicast addresses via web user interface:

1. Click on **Directory**->**Multicast IP**.
2. Enter the sending multicast address and port number in the **Paging Address** field.
3. Enter the label in the **Label** field.

The label will appear on the LCD screen when sending the RTP multicast.



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

To configure a multicast paging key via phone user interface:

1. Press **Menu**->**Features**->**DSS Keys**->**Memory Keys** (or **Line Keys**).
2. Select the desired DSS key.
3. Press or , or the **Switch** soft key to select **Key Event** from the **Type** field.
4. Press or , or the **Switch** soft key to select **Multicast Paging** from the **Key Type** field.
5. Enter the multicast IP address and port number in the **Value** field.
6. Press the **Save** soft key to accept the change.

To configure a paging list key via phone user interface:

1. Press **Menu**->**Features**->**DSS Keys**->**Memory Keys** (or **Line Keys**).
2. Select the desired DSS key.
3. Press or , or the **Switch** soft key to select **Key Event** from the **Type** field.
4. Press or , or the **Switch** soft key to select **Paging List** from the **Key Type** field.
5. Press the **Save** soft key to accept the change.

To configure paging list via phone user interface:

1. Press **Menu->Features**->**Paging List**.
2. Press the **Option** soft key.
3. Press the **Edit** soft key.
4. Enter the multicast IP address and port number (e.g., 224.5.6.20:10008) in the **Address** field.

The valid multicast IP addresses range from 224.0.0.0 to 239.255.255.255.

5. Enter the group name in the **Label** field.
6. Press the **Save** soft key to accept the change.

   Repeat the step 2-6, you can add more paging groups.

Receiving RTP Stream

IP phones can receive an RTP stream from the pre-configured multicast address(es) without involving SIP signaling, and can handle the incoming multicast paging calls differently depending on the configurations of Paging Barge and Paging Priority Active.

Paging Barge

This parameter defines the priority of the voice call in progress, and decides how the IP phone handles the incoming multicast paging calls when there is already a voice call in progress. If the parameter is configured as disabled, all incoming multicast paging calls will be automatically ignored. If the parameter is the priority value, the incoming multicast paging calls with higher priority are automatically answered and the ones with lower priority are ignored.

Paging Priority Active

This parameter decides how the IP phone handles the incoming multicast paging calls when there is already a multicast paging call in progress. If the parameter is configured as disabled, the IP phone will automatically ignore all incoming multicast paging calls. If the parameter is configured as enabled, an incoming multicast paging call with higher priority is automatically answered, and the one with lower priority is ignored.

Procedure

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

Configuration File	<y0000000000xx>.cfg	Configure the listening multicast address. **Parameters:** multicast.listen_address.X.ip_address multicast.listen_address.X.label Configure Paging Barge and Paging Priority Active features. **Parameters:** multicast.receive_priority.enable multicast.receive_priority.priority
Local	Web User Interface	Configure the listening multicast address.

		Configure Paging Barge and Paging Priority Active features. **Navigate to**: http://<phoneIPAddress>/servlet?p=contacts-multicastIP&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
multicast.listen_address.X.ip_address (X ranges from 1 to 10)	**IP address: port**	**Blank**
Description: Configures the multicast address and port number that the IP phone listens to. **Example:** multicast.listen_address.1.ip_address = 224.5.6.20:10008 **Note**: The valid multicast IP addresses range from 224.0.0.0 to 239.255.255.255. **Web User Interface:** Directory->Multicast IP->Listening Address **Phone User Interface:** None		
multicast.listen_address.X.label (X ranges from 1 to 10)	**String within 99 characters**	**Blank**
Description: Configures the label to be displayed on the LCD screen when receiving the RTP multicast. **Example:** multicast.listen_address.1.label = Paging1 **Web User Interface:** Directory->Multicast IP->Label **Phone User Interface:** None		
multicast.receive_priority.enable	**0 or 1**	**1**
Description: Enables or disables the IP phone to handle the incoming multicast paging calls when there is an active multicast paging call on the IP phone. **0**-Disabled		

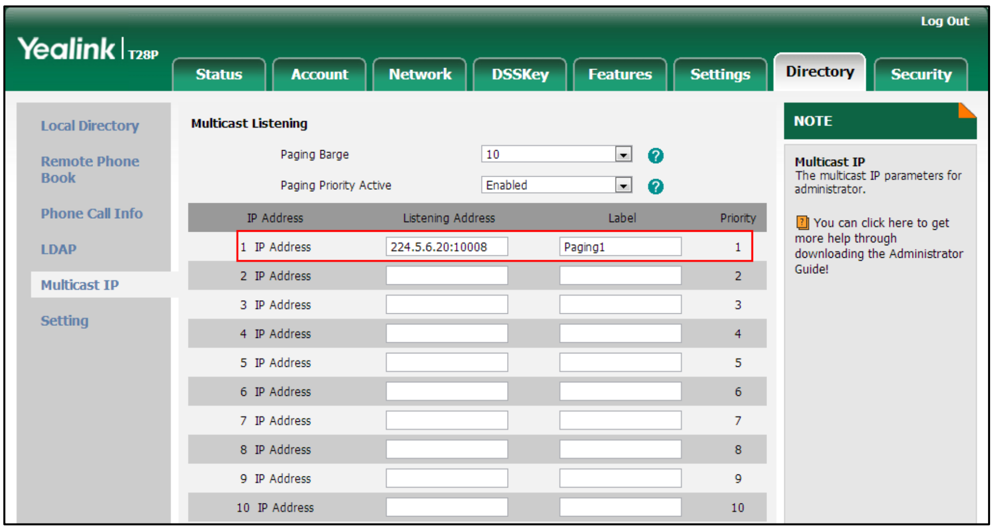
Parameters	Permitted Values	Default
1-Enabled If it is set to 1 (Enabled), the IP phone will answer the incoming multicast paging call with a higher priority and ignore that with a lower priority. **Web User Interface:** Directory->Multicast IP->Paging Priority Active **Phone User Interface:** None		
multicast.receive_priority.priority	**Integer from 0 to 10**	**10**
Description: Configures the priority of multicast paging calls. 1 is the highest priority, 10 is the lowest priority. If it is set to 0, all incoming multicast paging calls will be automatically ignored. **Web User Interface:** Directory->Multicast IP->Paging Barge **Phone User Interface:** None		

To configure a listening multicast address via web user interface:

1. Click on **Directory**->**Multicast IP**.
2. Enter the listening multicast address and port number in the **Listening Address** field.

   1 is the highest priority and 10 is the lowest priority.
3. Enter the label in the **Label** field.

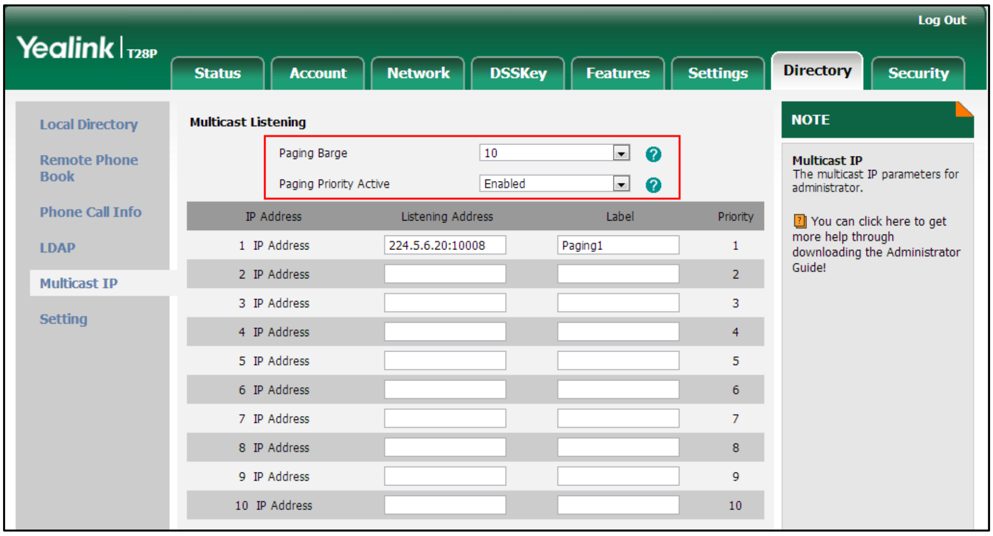
   The label will appear on the LCD screen when receiving the RTP multicast.



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

To configure paging barge and paging priority active features via web user interface:

1. Click on **Directory**->**Multicast IP**.
2. Select the desired value from the pull-down list of **Paging Barge**.
3. Select the desired value from the pull-down list of **Paging Priority Active**.



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

Call Recording

Call recording enables users to record calls. It depends on support from a SIP server. When the user presses the call record key, the IP phone sends a record request to the server. IP phones themselves do not have memory to store the recording, what they can do is to trigger the recording and indicate the recording status.

Normally, there are 2 main methods to trigger a recording on a certain server. We call them record and URL record. Record is for the IP phone to send the server a SIP INFO message containing a specific header. URL record is for the IP phone to send the server an HTTP GET message containing a specific URL. The server processes these messages and decides to start or stop a recording.

Record

When a user presses a record key for the first time during a call, the IP phone sends a SIP INFO message to the server with the specific header "Record: on", and then the recording starts.

Example of a SIP INFO message:

```
Via: SIP/2.0/UDP 10.1.4.148:5063;branch=z9hG4bK1139980711
From: "827" <sip:827@192.168.1.199>;tag=2066430997
To:<sip:614@192.168.1.199>;tag=371745247
```

```
Call-ID: 1895019940@10.1.4.148
CSeq: 2 INFO
Contact: <sip:827@10.1.4.148:5063>
Max-Forwards: 70
User-Agent: Yealink SIP-T28P 2.72.0.1
Record: on
Content-Length: 0
```

When the user presses the record key for the second time, the IP phone sends a SIP INFO message to the server with the specific header "Record: off", and then the recording stops.

Example of a SIP INFO message:

```
Via: SIP/2.0/UDP 10.1.4.148:5063;branch=z9hG4bK1619489730
From: "827" <sip:827@192.168.1.199>;tag=1831694891
To:<sip:614@192.168.1.199>;tag=2228378244
Call-ID: 1051886688@10.1.4.148
CSeq: 3 INFO
Contact: <sip:827@10.1.4.148:5063>
Max-Forwards: 70
User-Agent: Yealink SIP-T28P 2.72.0.1
Record: off
Content-Length: 0
```

URL Record

When a user presses a URL record key for the first time during a call, the IP phone sends an HTTP GET message to the server.

Example of an HTTP GET message:

```
Get /phonerecording.cgi?model=yealink HTTP/1.0\r\n
Request Method: GET
Request URI: /phonerecording.cgi?model=yealink
Request version: HTTP/1.0
Host: 10.1.2.224\r\n
User-agent: yealink SIP-T28P 2.72.0.1 00:16:65:11:30:68\r\n
```

If the recording is successfully started, the server will respond with a 200 OK message.

Example of a 200 OK message:

```
<YealinkIPPhoneText>
 <Title>
    </Title>
 <Text>
    The recording session is successfully started.
```

```
    </Text>
<YealinkIPPhoneText>
```

If the recording fails for some reasons, for example, the recording box is full, the server will respond with a 200 OK message.

Example of a 200 OK message:

```
<YealinkIPPhoneText>
 <Title>
    </Title>
 <Text>
    Probably the recording box is full.
    </Text>
<YealinkIPPhoneText>
```

When the user presses the URL record key for the second time, the IP phone sends an HTTP GET message to the server, and then the server will respond with a 200 OK message.

Example of a 200 OK message:

```
<YealinkIPPhoneText>
 <Title>
    </Title>
 <Text>
    The recording session is successfully stopped.
    </Text>
<YealinkIPPhoneText>
```

Procedure

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

Configuration File	<y0000000000xx>.cfg	Assign a record key. **Parameters:** memorykey.X.type/ linekey.X.type Assign a URL record key. **Parameters:** memorykey.X.type/ linekey.X.type memorykey.X.value/ linekey.X.value
Local	Web User Interface	Assign a record key and URL record key.

		Navigate to: http://<phoneIPAddress>/servlet?p=dsskey&q=load&model=0
	Phone User Interface	Assign a record key and URL record key.

Record Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 513.

Parameters	Permitted Values	Default
memorykey.X.type/ linekey.X.type	**Integer**	**0 for memory key,15 for Line key**
Description: Configures a DSS key as a record key on the IP phone. The digit **25** stands for the key type **Record**. For the memory key, x ranges from 1 to 10. For the line key, x ranges from 1 to 6. **Example:** memorykey.1.type = 25 **Web User Interface:** DSSKey->Memory Key(or Line Key)->Type **Phone User Interface:** Menu->Features->DSS Keys->Memory Keys (or Line Keys)->DSS Key X (or Line Key X)->Type		

URL Record Key

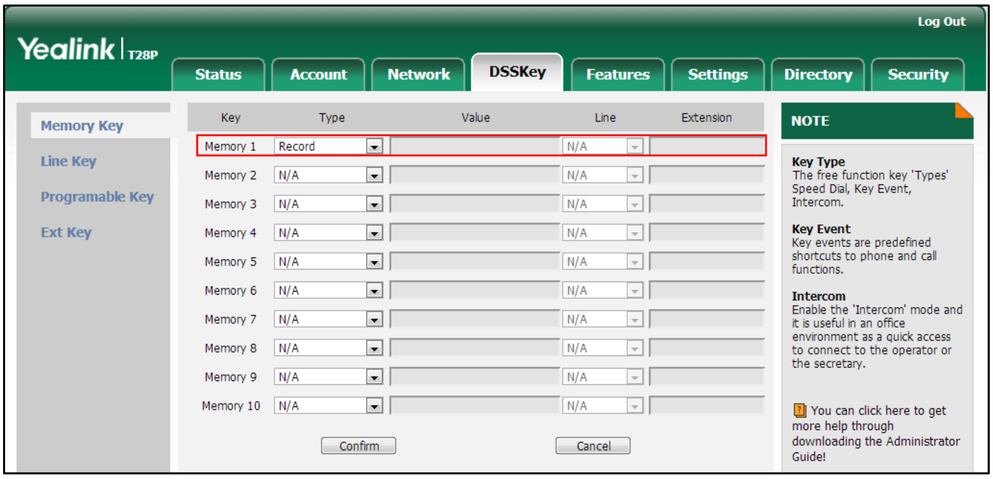
Parameters	Permitted Values	Default
memorykey.X.type/ linekey.X.type	**Integer**	**0 for memory key,15 for Line key**
Description: Configures a DSS key as a URL record key on the IP phone. The digit **35** stands for the key type **URL Record**.		

Parameters	Permitted Values	Default
For the memory key, x ranges from 1 to 10. For the line key, x ranges from 1 to 6. **Example:** memorykey.1.type = 35 **Web User Interface:** DSSKey->Memory Key(or Line Key)->Type **Phone User Interface:** Menu->Features->DSS Keys->Memory Keys (or Line Keys)->DSS Key X (or Line Key X)->Type		
memorykey.X.value/linekey.X.value	**String within 99 characters**	**blank**
Description: Configures the URL to record a call. For the memory key, x ranges from 1 to 10. For the line key, x ranges from 1 to 6. **Example:** memorykey.1.value = http://10.1.2.224/phonerecording.cgi **Web User Interface:** DSSKey->Memory Key->(or Line Key)->Value **Phone User Interface:** Menu->Features->DSS Keys->Memory Keys (or Line Keys)->DSS Key X (or Line Key X)->Value		

To configure a record key via web user interface:

1. Click on **DSSKey**->**Memory Key** (or **Line Key**).

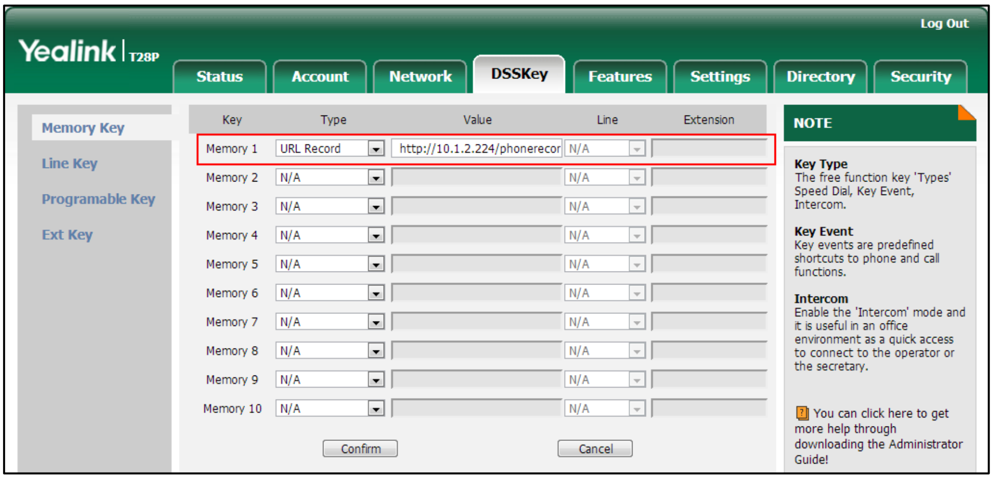
2. In the desired DSS key field, select **Record** from the pull-down list of **Type**.



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

To configure a URL record key via web user interface:

1. Click on **DSSKey**->**Memory Key** (or **Line Key**).
2. In the desired DSS key field, select **URL Record** from the pull-down list of **Type**.
3. Enter the URL in the **Value** field.



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

To configure a record key via phone user interface:

1. Press **Menu**->**Features**->**DSS Keys**->**Memory Keys** (or **Line Keys**).
2. Select the desired DSS key.
3. Press or , or the **Switch** soft key to select **Key Event** from the **Type** field.
4. Press or , or the **Switch** soft key to select **Record** from the **Key Type** field.
5. Press the **Save** soft key to accept the change.

To configure a URL record key via phone user interface:

1. Press **Menu**->**Features**->**DSS Keys**->**Memory Keys** (or **Line Keys**).
2. Select the desired DSS key.
3. Press or , or the **Switch** soft key to select **URL Record** from the **Type** field.
4. Enter the URL in the **Value** field.
5. Press the **Save** soft key to accept the change.

Hot Desking

Hot desking originates from the definition of being the temporary physical occupant of a work station or surface by a particular employee. A primary motivation for hot desking is cost reduction. Hot desking is regularly used in places where not all employees are in the office at the same time, or not in the office for a long time, which means actual personal offices would often be vacant, consuming valuable space and resources.

Hot desking allows a user to clear registration configurations of all accounts on the IP phone, and then register his account on line 1. To use this feature, you need to assign a hot desking key.

Procedure

Hot desking key can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Assign a hot desking key. **Parameters:** memorykey.X.type/ linekey.X.type/ programablekey.X.type
Local	Web User Interface	Assign a hot desking key. **Navigate to:** http://<phoneIPAddress>/servlet?p=dsskey&q=load&model=0
	Phone User Interface	Assign a hot desking key.

Hot Desking Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 513.

Parameters	Permitted Values	Default
memorykey.X.type/ linekey.X.type/ programablekey.X.type	**34**	**Refer to the following content**

Description:

Configures a DSS key as a hot desking key on the IP phone.

The digit **34** stands for the key type **Hot Desking**.

For memory keys:

X ranges from 1 to 10 (for SIP-T28/T26P).

For line keys:

X ranges from 1 to 6 (for SIP-T28P)

X ranges from 1 to 3 (for SIP-T26P/T22P).

X ranges from 1 to 2 (for SIP-T20P).

For programable keys:

X ranges from 1 to 14 (for SIP-T28/T26P)

X=1-10, 14 (for SIP-T22P)

X=5-12, 14 (for SIP-T20P)

Example:

memorykey.1.type = 34

Default:

For memory keys:

The default value is 0.

For line keys:

The default value is 15.

For programable keys:

For SIP-T28P/T26P IP phones:

When X=1, the default value is 28 (History).

When X=2, the default value is 61 (Directory).

When X=3, the default value is 5 (DND).

When X=4, the default value is 30 (Menu).

When X=5, the default value is 28 (History).

When X=6, the default value is 61 (Directory).

When X=7, the default value is 31 (Switch Account).

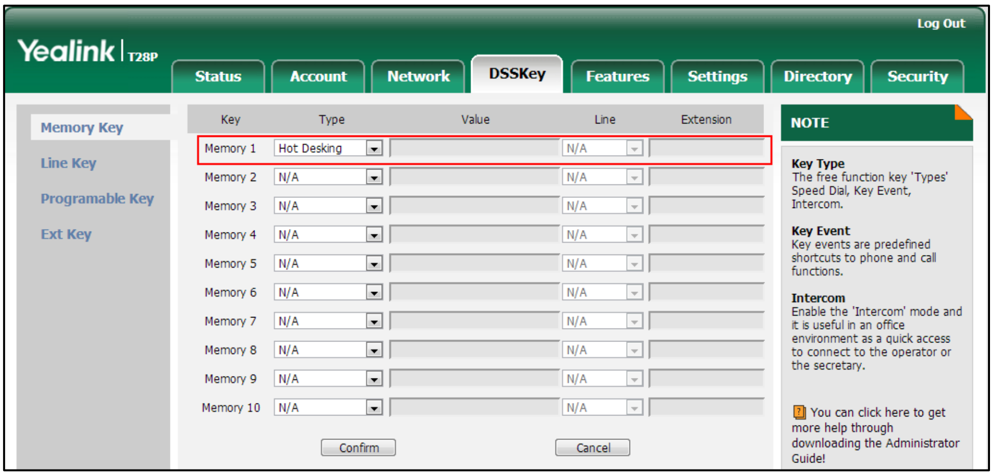
Parameters	Permitted Values	Default
When X=8, the default value is 31 (Switch Account). When X=9, the default value is 33 (Status). When X=10, the default value is 0 (NA). When X=11, the default value is 0 (NA). When X=12, the default value is 0 (NA). When X=13, the default value is 0 (NA). When X=14, the default value is 2 (Forward). **For SIP-T22P IP phones:** When X=1, the default value is 28 (History). When X=2, the default value is 61 (Directory). When X=3, the default value is 5 (DND). When X=4, the default value is 30 (Menu). When X=5, the default value is 28 (History). When X=6, the default value is 61 (Directory). When X=7, the default value is 31 (Switch Account). When X=8, the default value is 31 (Switch Account). When X=9, the default value is 33 (Status). When X=10, the default value is 0 (NA). When X=14, the default value is 2 (Forward). **For SIP-T20P IP phones:** When X=5, the default value is 28 (History). When X=6, the default value is 61 (Directory). When X=7, the default value is 31 (Switch Account). When X=8, the default value is 31 (Switch Account). When X=9, the default value is 33 (Status). When X=10, the default value is 0 (NA). When X=11, the default value is 0 (NA). When X=12, the default value is 0 (NA). When X=14, the default value is 2 (Forward). **Web User Interface:** DSSKey->Memory Key/ Line Key / Programmable Key ->Type **Phone User Interface:** Menu->Features->DSS Keys->Memory Keys (or Line Keys)->DSS Key X (or Line Key X)->Type		

To configure a hot desking key via web user interface:

1. Click on **DSSKey**->**Memory Keys** (**Line Key**).

   SIP-T22P/T20P IP phones only support line keys.

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



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

To configure a hot desking key via phone user interface:

1. Press **Menu**->**Features**->**DSS Keys**->**Memory Keys** (or **Line Keys**).
2. Select the desired DSS key.
3. Press or , or the **Switch** soft key to select **Key Event** from the **Type** field.
4. Press or , or the **Switch** soft key to select **Hot Desking** from the **Key Type** field.
5. Press the **Save** soft key to accept the change.

Action URL

Action URL allows IP phones to interact with web server applications by sending an HTTP or HTTPS GET request. You can specify a URL that triggers a GET request when a specified event occurs. Action URL can only be triggered by the pre-defined events (e.g., log on). The valid URL format is: http(s)://IP address of the server/help.xml?.

The following table lists the pre-defined events for action URL.

Event	Description
Setup Completed	When the IP phone completes startup.
Registered	When the IP phone successfully registers an account.
Unregistered	When the IP phone logs off the registered account.
Register Failed	When the IP phone fails to register an account.

Event	Description
Off Hook	When the IP phone is off hook.
On Hook	When the IP phone is on hook.
Incoming Call	When the IP phone receives an incoming call.
Outgoing Call	When the IP phone places a call.
Established	When the IP phone establishes a call.
Terminated	When the IP phone terminates a call.
Open DND	When the IP phone enables the DND mode.
Close DND	When the IP phone disables the DND mode.
Open Always Forward	When the IP phone enables the always forward.
Close Always Forward	When the IP phone disables the always forward.
Open Busy Forward	When the IP phone enables the busy forward.
Close Busy Forward	When the IP phone disables the busy forward.
Open No Answer Forward	When the IP phone enables the no answer forward.
Close No Answer Forward	When the IP phone disables the no answer forward
Transfer Call	When the IP phone transfers a call.
Blind Transfer	When the IP phone blind transfers a call.
Attended Transfer	When the IP phone performs the semi-attended/attended transfer.
Hold	When the IP phone places a call on hold.
UnHold	When the IP phone retrieves a hold call.
Mute	When the IP phone mutes a call.
UnMute	When the IP phone un-mutes a call.
Missed Call	When the IP phone misses a call.
IP Changed	When the IP address of the IP phone changes.
Forward Incoming Call	When the IP phone forwards an incoming call.
Reject Incoming Call	When the IP phone rejects an incoming call.
Answer New-In Call	When the IP phone answers a new call.
Transfer Finished	When the IP phone completes to transfer a call.
Transfer Failed	When the IP phone fails to transfer a call.
Idle To Busy	When the state of the IP phone changes from idle to busy.
Busy To Idle	When the state of phone changes from busy to idle.

Event	Description
Autop Finish	When the IP phone completes auto provisioning via power on.

An HTTP or HTTPS GET request may contain variable name and variable value, separated by "=". Each variable value starts with $ in the query part of the URL. The valid URL format is: http(s)://IP address of server/help.xml?variable name=$variable value. Variable name can be customized by users, while the variable value is pre-defined. For example, a URL "*http://192.168.1.10/help.xml?mac=$mac*" is specified for the event Mute, $mac will be dynamically replaced with the MAC address of the IP phone when the IP phone mutes a call.

The following table lists pre-defined variable values.

Variable Value	Description
$mac	The MAC address of the IP phone
$ip	The IP address of the IP phone
$model	The IP phone model
$firmware	The firmware version of the IP phone
$active_url	The SIP URI of the current account when the IP phone places a call, receives an incoming call or establishes a call.
$active_user	The user part of the SIP URI for the current account when the IP phone places a call, receives an incoming call or establishes a call.
$active_host	The host part of the SIP URI for the current account when the IP phone places a call, receives an incoming call or establishes a call.
$local	The SIP URI of the caller when the IP phone places a call. The SIP URI of the callee when the IP phone receives an incoming call.
$remote	The SIP URI of the callee when the IP phone places a call. The SIP URI of the caller when the IP phone receives an incoming call.
$display_local	The display name of the caller when the IP phone places a call. The display name of the callee when the IP phone receives an incoming call.

Variable Value	Description
$display_remote	The display name of the callee when the IP phone places a call. The display name of the caller when the IP phone receives an incoming call.
$call_id	The call-id of the active call.

Procedure

Action URL can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure action URL. **Parameters:** action_url.setup_completed action_url.registered action_url.unregistered action_url.register_failed action_url.off_hook action_url.on_hook action_url.incoming_call action_url.outgoing_call action_url.call_established action_url.dnd_on action_url.dnd_off action_url.always_fwd_on action_url.always_fwd_off action_url.busy_fwd_on action_url.busy_fwd_off action_url.no_answer_fwd_on action_url.no_answer_fwd_off action_url.transfer_call action_url.blind_transfer_call action_url.attended_transfer_call action_url.hold action_url.unhold action_url.mute action_url.unmute action_url.missed_call

		action_url.call_terminated action_url.busy_to_idle action_url.idle_to_busy action_url.ip_change action_url.forward_incoming_call action_url.reject_incoming_call action_url.answer_new_incoming_call action_url.transfer_finished action_url.transfer_failed action_url.setup_autop_finish
Local	Web User Interface	Configure action URL. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-actionurl&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
action_url.setup_completed	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends after startup. The value format is: http(s)://IP address of server/help.xml? variable name=variable value. **Valid variable values are:** • $mac • $ip • $model • $firmware • $active_url • $active_user • $active_host • $local • $remote • $display_local		

Parameters	Permitted Values	Default
• $display_remote • $call_id **Example:** action_url. setup_completed = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Setup Completed **Phone User Interface:** None		
action_url.registered	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends after an account is registered. **Example:** action_url.registered = http://192.168.0.20/help.xml?IP=$ip **Note:** The old parameter "action_url.log_on" is also applicable to IP phones. **Web User Interface:** Features->Action URL->Registered **Phone User Interface:** None		
action_url.unregistered	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends after an account is unregistered. **Example:** action_url.unregistered = http://192.168.0.20/help.xml?IP=$ip **Note**: The old parameter "action_url.log_off" is also applicable to IP phones. **Web User Interface:** Features->Action URL->Unregistered **Phone User Interface:** None		
action_url.register_failed	**URL within 511 characters**	**Blank**

Parameters	Permitted Values	Default
Description: Configures the action URL the IP phone sends after a register failed. **Example**: action_url.register_failed = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Register Failed **Phone User Interface:** None		
action_url.off_hook	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when off hook. **Example**: action_url.off_hook = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Off Hook **Phone User Interface:** None		
action_url.on_hook	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when on hook. **Example**: action_url.on_hook = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->On Hook **Phone User Interface:** None		
action_url.incoming_call	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when receiving an incoming call.		

Parameters	Permitted Values	Default
Example: action_url.incoming_call = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Incoming Call **Phone User Interface:** None		
action_url.outgoing_call	URL within 511 characters	Blank
Description: Configures the action URL the IP phone sends when placing a call. **Example**: action_url.outgoing_call = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Outgoing Call **Phone User Interface:** None		
action_url.call_established	URL within 511 characters	Blank
Description: Configures the action URL the IP phone sends when establishing a call. **Example**: action_url.call_established = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Established **Phone User Interface:** None		
action_url.dnd_on	URL within 511 characters	Blank
Description: Configures the action URL the IP phone sends when DND feature is enabled. **Example**: action_url.dnd_on = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:**		

Parameters	Permitted Values	Default
Features->Action URL->Open DND **Phone User Interface:** None		
action_url.dnd_off	URL within 511 characters	Blank
Description: Configures the action URL the IP phone sends when DND feature is disabled. **Example**: action_url.dnd_off = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Close DND **Phone User Interface:** None		
action_url.always_fwd_on	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when always forward feature is enabled. **Example**: action_url.always_fwd_on = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Open Always Forward **Phone User Interface:** None		
action_url.always_fwd_off	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when always forward feature is disabled. **Example**: action_url.always_fwd_off = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Close Always Forward **Phone User Interface:**		

Parameters	Permitted Values	Default
None		
action_url.busy_fwd_on	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when busy forward feature is enabled. **Example**: action_url.busy_fwd_on = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Open Busy Forward **Phone User Interface:** None		
action_url.busy_fwd_off	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when busy forward feature is disabled. **Example**: action_url.busy_fwd_off = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Close Busy Forward **Phone User Interface:** None		
action_url.no_answer_fwd_on	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when no answer forward feature is enabled. **Example**: action_url.no_answer_fwd_on = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Open No Answer Forward **Phone User Interface:**		

Parameters	Permitted Values	Default
None		
action_url.no_answer_fwd_off	URL within 511 characters	Blank
Description: Configures the action URL the IP phone sends when no answer forward feature is disabled. **Example**: action_url.no_answer_fwd_off = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Close No Answer Forward **Phone User Interface:** None		
action_url.transfer_call	URL within 511 characters	Blank
Description: Configures the action URL the IP phone sends when performing a transfer. **Example**: action_url.transfer_call = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Transfer Call **Phone User Interface:** None		
action_url.blind_transfer_call	URL within 511 characters	Blank
Description: Configures the action URL the IP phone sends when performing a blind transfer. **Example**: action_url.blind_transfer_call = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Blind Transfer **Phone User Interface:** None		

Parameters	Permitted Values	Default
action_url.attended_transfer_call	URL within 511 characters	Blank
Description: Configures the action URL the IP phone sends when performing an attended/semi-attended transfer. **Example**: action_url.attended_transfer_call = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Attended Transfer **Phone User Interface:** None		
action_url.hold	URL within 511 characters	Blank
Description: Configures the action URL the IP phone sends when placing a call on hold. **Example**: action_url.hold = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Hold **Phone User Interface:** None		
action_url.unhold	URL within 511 characters	Blank
Description: Configures the action URL the IP phone sends when resuming a held call. **Example**: action_url.unhold = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->UnHold **Phone User Interface:** None		
action_url.mute	URL within 511 characters	Blank

Parameters	Permitted Values	Default
Description: Configures the action URL the IP phone sends when muting a call. **Example**: action_url.mute = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Mute **Phone User Interface:** None		
action_url.unmute	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when un-muting a call. **Example**: action_url.unmute = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->UnMute **Phone User Interface:** None		
action_url.missed_call	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when missing a call. **Example**: action_url.missed_call = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Missed Call **Phone User Interface:** None		
action_url.call_terminated	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when terminating a call. **Example**:		

Parameters	Permitted Values	Default
action_url.call_terminated = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Terminated **Phone User Interface:** None		
action_url.busy_to_idle	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when changing the state of the IP phone from busy to idle. **Example:** action_url.busy_to_idle = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Busy To Idle **Phone User Interface:** None		
action_url.idle_to_busy	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when changing the state of the IP phone from idle to busy. **Example**: action_url.idle_to_busy = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Idle To Busy **Phone User Interface:** None		
action_url.ip_change	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when changing the IP address of the IP phone. **Example**:		

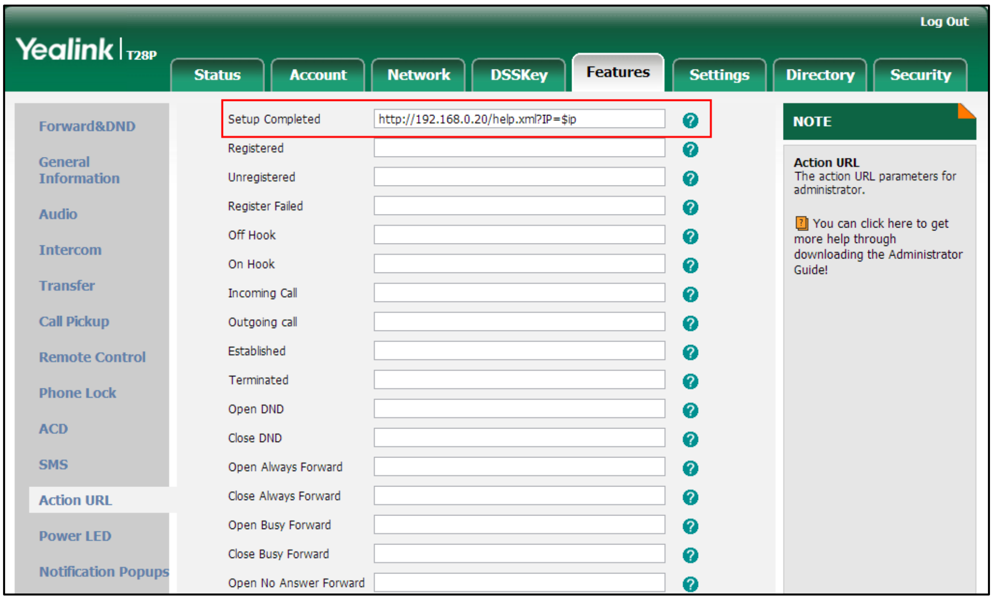
Parameters	Permitted Values	Default
action_url.ip_change = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->IP Changed **Phone User Interface:** None		
action_url.forward_incoming_call	URL within 511 characters	Blank
Description: Configures the action URL the IP phone sends when forwarding an incoming call. **Example**: action_url.forward_incoming_call = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Forward Incoming Call **Phone User Interface:** None		
action_url.reject_incoming_call	URL within 511 characters	Blank
Description: Configures the action URL the IP phone sends when rejecting an incoming call. **Example**: action_url.reject_incoming_call = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Reject Incoming Call **Phone User Interface:** None		
action_url.answer_new_incoming_call	URL within 511 characters	Blank
Description: Configures the action URL the IP phone sends when answering a new incoming call. **Example**: action_url.answer_new_incoming_call = http://192.168.0.20/help.xml?IP=$ip		

Parameters	Permitted Values	Default
Web User Interface: Features->Action URL->Answer New-In Call **Phone User Interface:** None		
action_url.transfer_finished	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when completing a call transfer. **Example**: action_url.transfer_finished = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Transfer Finished **Phone User Interface:** None		
action_url.transfer_failed	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when failing to transfer a call. **Example**: action_url.transfer_failed = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Transfer Failed **Phone User Interface:** None		
action_url.setup_autop_finish	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when completing auto provisioning via power on. **Example**: action_url.setup_autop_finish = http://192.168.0.20/help.xml?IP=$ip		

Parameters	Permitted Values	Default
Web User Interface: Features->Action URL->Autop Finish **Phone User Interface:** None		

To configure action URL via web user interface:

1. Click on **Features**->**Action URL**.
2. Enter the action URLs in the corresponding fields.



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

Action URI

Opposite to action URL, action URI allows IP phones to interact with web server application by receiving and handling an HTTP or HTTPS GET request. When receiving a GET request, the IP phone will perform the specified action and respond with a 200 OK message. A GET request may contain variable named as “key” and variable value, which are separated by “=”. The valid URI format is: http(s)://phone IP address/servlet?key=variable value.

The following table lists pre-defined variable values:

Variable Value	Phone Action
OK	Press the OK key.

Variable Value	Phone Action
ENTER	Press the Enter soft key (Except for SIP-T20P).
SPEAKER	Press the Speakerphone key.
F_TRANSFER	Transfers a call to another party.
VOLUME_UP	Increase the volume.
VOLUME_DOWN	Decrease the volume.
MUTE	Mute a call.
F_HOLD	Place an active call on hold.
X	Cancel actions or reject incoming calls (For SIP-T22P/T20P, also mute or un-mute calls).
0-9/*/POUND	Press the keypad (0-9, * or #).
L1-LX	Press the line keys (for SIP-T28P, X=6, for SIP-T26/22P, X=3, for SIP-T20P, X=2).
D1-D10	Press the memory keys (Only for SIP-T28/T26P).
F_CONFERENCE	Press the CONF key (Except for SIP-T22P) or the Conference soft key (Except for SIP-T20P).
F1-F4	Press the soft keys (Except for SIP-T20P).
MSG	Press the MESSAGE key.
HEADSET	Press the HEADSET key.
RD	Press the RD key.
UP/DOWN/LEFT/RIGHT	Press the navigation keys.
Reboot	Reboot the phone.
AutoP	Perform auto provisioning.
DNDOn	Activate the DND mode.
DNDOff	Deactivate the DND mode.
number=xxx&outgoing_uri=y	Place a call to xxx from SIP URI y.
OFFHOOK	Pick up the handset.
ONHOOK	Hang up the handset.
ANSWER	Answer a call.
Reset	Reset a phone.

Variable Value	Phone Action
ATrans=xxx	Perform a semi-attended/attended transfer to xxx.
BTrans=xxx	Perform a blind transfer to xxx.
CALLEND	End a call.
phonecfg=get[&accounts=x][&dnd=x][&fw=x]	Get firmware version, registration, DND or forward configuration information. The valid value of “x” is 0 or 1, 0 means you do not need to get configuration information. 1 means you want to get configuration information. **Note**: The valid URI is: http(s)://phone IP address/servlet?phonecfg=get[&accounts=x][&dnd=x][&fw=x] **Example**: http://10.3.20.10/servlet?phonecfg=get[&accounts=1][&dnd=0][&fw=1]

Note

The variable value is not applicable to all events. For example, the variable value “MUTE” is only applicable when the IP phone is during a call.

When authentication is required, you must enter “p=login&q=login&username=xxx&pwd=yyy&jumpto=URI&” before the variable “key”. xxx refers to the login user name and yyy refers to the login password.

For security reasons, IP phones do not receive and handle HTTP/HTTPS GET requests by default. You need to specify the trusted IP address for action URI. When the IP phone receives a GET request from the trusted IP address for the first time, the LCD screen prompts the message “Allow Remote Control?”. You can specify one or more trusted IP addresses on the IP phone, or configure the IP phone to receive and handle the URI from any IP address. You can use action URI feature to capture the phone’s current screen.

Procedure

Specify the trusted IP address for action URI using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Specify the trusted IP address(es) for sending the action URI to the IP phone. **Parameter:** features.action_uri_limit_ip

Local	Web User Interface	Specify the trusted IP address(es) for sending the action URI to the IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-remotecontrl&q=load

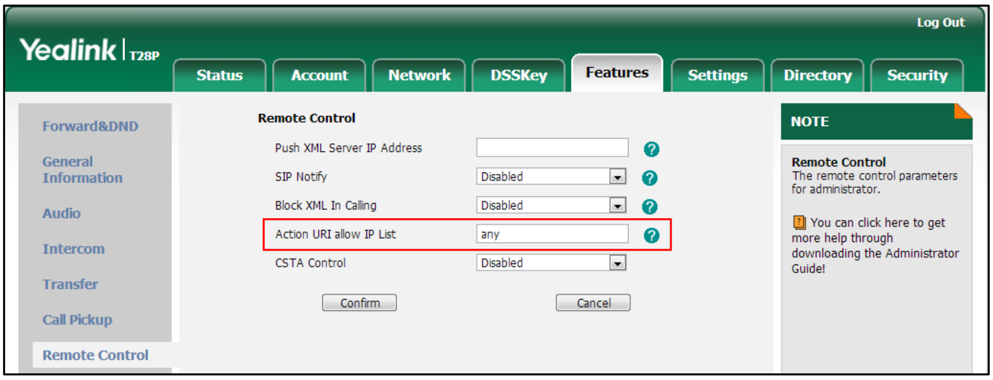
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
features.action_uri_limit_ip	**IP address or any**	**Blank**
Description: Configures the address(es) from which Action URI will be accepted. For discontinuous IP addresses, multiple IP addresses are separated by commas. For continuous IP addresses, the format likes *.*.*.* and the "*" stands for the values 0~255. For example: 10.10.*.* stands for the IP addresses that range from 10.10.0.0 to 10.10.255.255. If left blank, the IP phone will reject any HTTP GET request. If it is set to "any", the IP phone will accept and handle HTTP GET requests from any IP address. **Example:** features.action_uri_limit_ip = any **Web User Interface:** Features->Remote Control->Action URI allow IP List **Phone User Interface:** None		

To configure the trusted IP address(es) for action URI via web user interface:

1. Click on **Features**->**Remote Control**.
2. Enter the IP address or any in the **Action URI allow IP List** field.

Multiple IP addresses are separated by commas. If you enter "any" in this field, the IP phone can receive and handle GET requests from any IP address. If you leave the field blank, the IP phone cannot receive or handle any HTTP GET request.



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

Capturing the Current Screen of the Phone

You can capture the screen display of the IP phone using the action URI. IP phones support handling an HTTP or HTTPS GET request. The URI format is http(s)://<phoneIPAddress>/screencapture. The captured picture can be saved as a BMP or JPEG file.

You can also use the URI "http(s)://<phoneIPAddress>/screencapture/download" to capture the screen display first, and then download the image (which is saved as a JPG file and named with the phone model and the capture time) to the local system. Before capturing the phone's current screen, ensure that the IP address of the computer is included in the trusted IP address for Action URI on the phone.

When you capture the screen display, the IP phone may prompt you to enter the user name and password of the administrator if web browser does not remember the user name and password for web user interface login.

Note

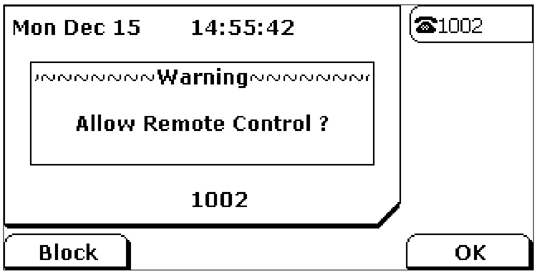
IP phones also support capturing the screen display using the old URI "http://<phoneIPAddress>/servlet?command=screenshot".

To capture the current screen of the phone:

1. Enter request URI (e.g., http://10.3.20.8/screencapture) in the browser's address bar and press the Enter key on the keyboard.

2. Do one of the following:

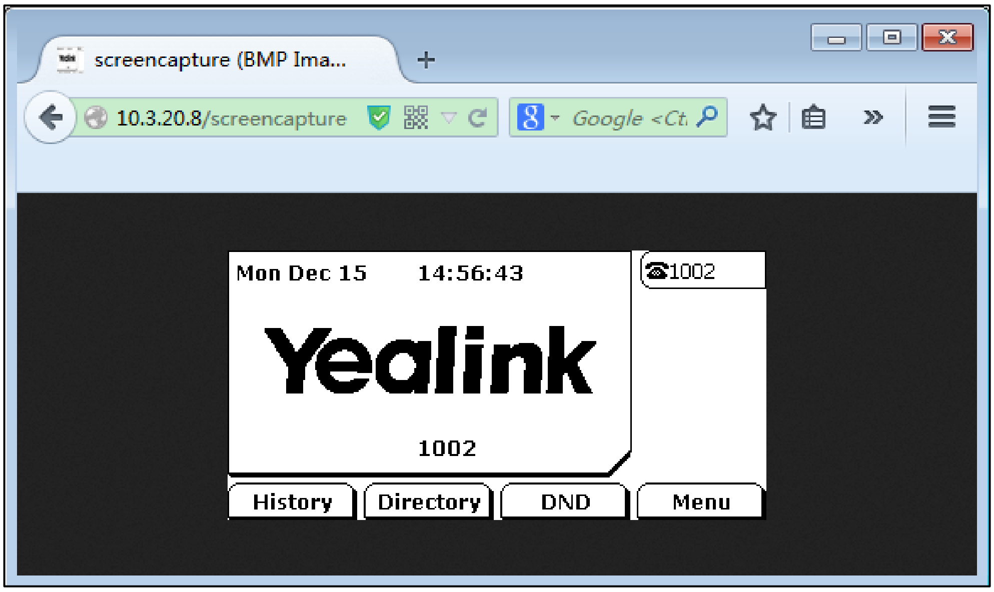
   - If it is the first time you capture the phone's current screen using the computer, the browser will display "remote control forbidden", and the LCD screen will prompt the message "Allow Remote Control?".



Press **OK** soft key on the phone to allow remote control. The phone will return to the previous screen.

Refresh the web page.

The browser will display an image showing the phone's current screen. You can save the image to your local system.



   - Else, the browser will display an image showing the phone's current screen directly. You can save the image to your local system.

Note Frequent capture may affect the phone performance. Yealink recommend you to capture the phone screen display within a minimum interval of 4 seconds.

Server Redundancy

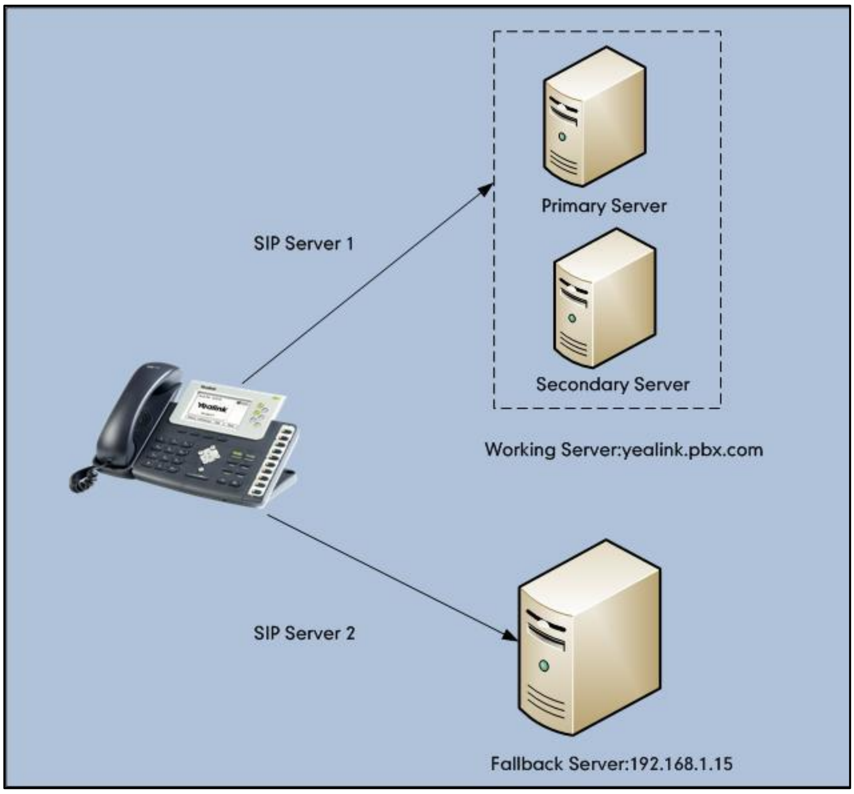
Server redundancy is often required in VoIP deployments to ensure continuity of phone service, for events where the server needs to be taken offline for maintenance, the server fails, or the connection between the IP phone and the server fails.

Two types of redundancy are possible. In some cases, a combination of the two may be deployed:

- **Failover:** In this mode, the full phone system functionality is preserved by having a second equivalent capability call server take over from the one that has gone down/off-line. This mode of operation should be done using the DNS 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. IP phones support configuration of two SIP servers per SIP registration for fallback purpose.

Phone Configuration for Redundancy Implementation

To assist in explaining the redundancy behavior, an illustrative example of how an IP phone may be configured is shown as below. In the example, server redundancy for fallback and failover purposes is deployed. Two separate SIP servers (a working server and a fallback server) are configured for per line registration.



Working Server: Server 1 is configured with the domain name of the working server. For example, yealink.pbx.com. DNS mechanism is used such that the working server is resolved to multiple SIP 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 methods of the fallback mode:

- **Concurrent registration**: The IP phone registers to two SIP servers (working server and fallback server) at the same time. In a failure situation, a fallback server can take over the basic calling capability, but without some of the advanced features offered by the working server (default registration method).
- **Successive registration**: The IP phone only registers to one server at a time. The IP phone first registers to the working server. In a failure situation, the IP phone registers to the fallback server.

When registering to the working server, the IP phone must always register to the primary server first except in failover conditions. When the primary server registration is unavailable, the secondary server will serve as the working server.

For more information on server redundancy, refer to *Server Redundancy on Yealink IP Phones*, available online:
http://www.yealink.com/DocumentDownload.aspx?CateId=142&flag=142.

Procedure

Server redundancy can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure the server redundancy on the IP phone. **Parameters:** account.X.sip_server.Y.address account.X.sip_server.Y.port account.X.sip_server.Y.expires account.X.sip_server.Y.retry_counts **Fallback Mode:** account.X.fallback.redundancy_type account.X.fallback.timeout **Failover Mode:** account.X.sip_server.Y.failback_mode account.X.sip_server.Y.failback_timeout account.X.sip_server.Y.register_on_enable
Local	Web User	Configure the server redundancy on the IP

	Interface	phone. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-register&q=load&acc=0

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.sip_server.Y.address (Y ranges from 1 to 2)	**String within 256 characters**	**Blank**
Description: Configures the IP address or domain name of the SIP server Y for account X. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Example:** account.1.sip_server.1.address = yealink.pbx.com **Web User Interface:** Account->Register ->SIP Server Y->Server Host **Phone User Interface:** None		
account.X.sip_server.Y.port (Y ranges from 1 to 2)	**Integer from 0 to 65535**	**5060**
Description: Configures the port of the SIP server Y for account X. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Example:** account.1.sip_server.1.port = 5060 **Web User Interface:** Account->Register ->SIP Server Y->Port **Phone User Interface:** None		
account.X.sip_server.Y.expires (Y ranges from 1 to 2)	**Integer from 30 to 2147483647**	**3600**

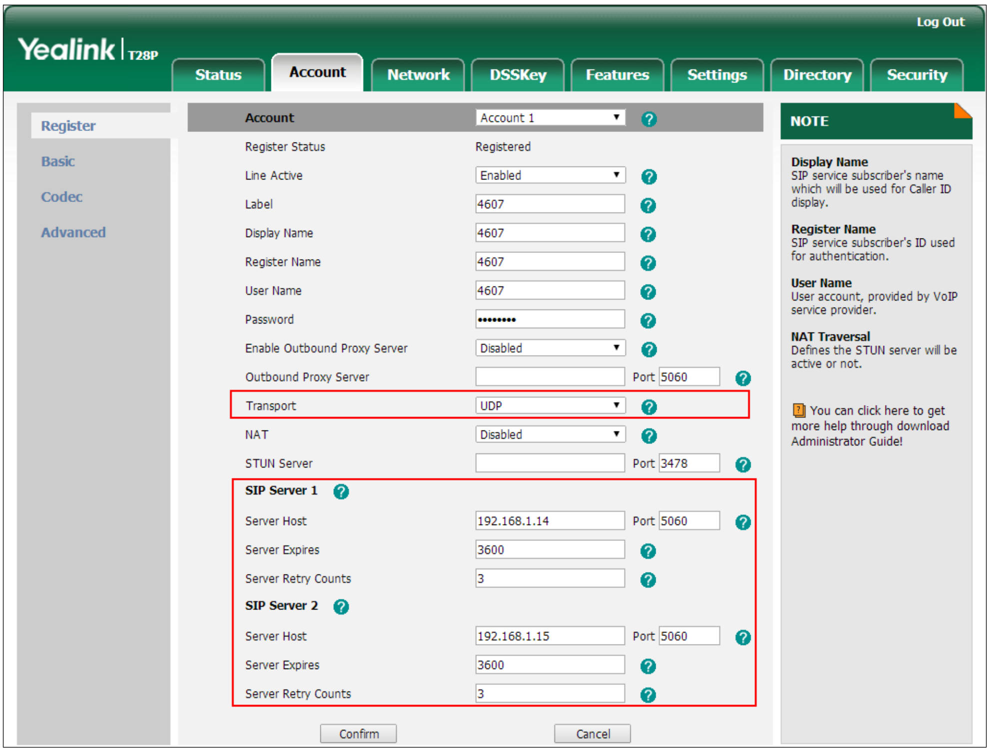
Parameters	Permitted Values	Default
Description: Configures the registration expiration time (in seconds) of the SIP server Y for account X. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Example:** account.1.sip_server.1.expires = 3600 **Web User Interface:** Account->Register ->SIP Server Y->Server Expires **Phone User Interface:** None		
account.X.sip_server.Y.retry_counts (Y ranges from 1 to 2)	**Integer from 0 to 20**	**3**
Description: Configures the retry times for the IP phone to resend requests when the SIP server Y is unavailable or there is no response from the SIP server Y for account X. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Web User Interface:** Account->Register ->SIP Server Y ->Server Retry Counts **Phone User Interface:** None		
account.X.fallback.redundancy_type	**0 or 1**	**0**
Description: Configures the registration mode for the IP phone in fallback mode. **0**-Concurrent Registration **1**-Successive Registration X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Web User Interface:**		

Parameters		Permitted Values	Default
None **Phone User Interface:** None			
account.X.fallback.timeout		**Integer from 10 to 2147483647**	**120**
Description: Configures the time interval (in seconds) for the IP phone to detect whether the working server is available by sending the registration request after the fallback server takes over call control. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). It is only applicable to the Successive Registration mode. **Web User Interface:** None **Phone User Interface:** None			
account.X.sip_server.Y.failback_mode (Y ranges from 1 to 2)		**0, 1, 2 or 3**	**0**
Description: Configures the way in which the phone fails back to the primary server for call control in the failover mode. **0**-newRequests: all requests are sent to the primary server first, regardless of the last server that was used. **1**-DNSTTL: the IP 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. **2**-registration: the IP 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. **3**-duration: the IP phone will send requests to the last registered server first. If the time defined by the account.X.sip_server.Y.failback_timeout parameter expires, the phone will retry to send requests to the primary server. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P).			

Parameters	Permitted Values	Default
Web User Interface: None **Phone User Interface:** None		
account.X.sip_server.Y.failback_timeout (Y ranges from 1 to 2)	**0, 60 to 65535**	**3600**
Description: 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 when the parameter account.X.sip_server.Y.failback_mode is set to duration. If you set the parameter to 0, the IP phone will not send requests to the primary server until a failover event occurs with the current working server. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Web User Interface:** None **Phone User Interface:** None		
account.X.sip_server.Y.register_on_enable (Y ranges from 1 to 2)	**0 or 1**	**0**
Description: Enables or disables the IP phone to register to the secondary server when sending requests to the secondary server in the failover mode. **0**-Disabled **1**-Enabled X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Web User Interface:** None **Phone User Interface:** None		

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. Select the desired value from the pull-down list of **Transport**.
5. Configure parameters of SIP server 1 and SIP server 2 in the corresponding fields.



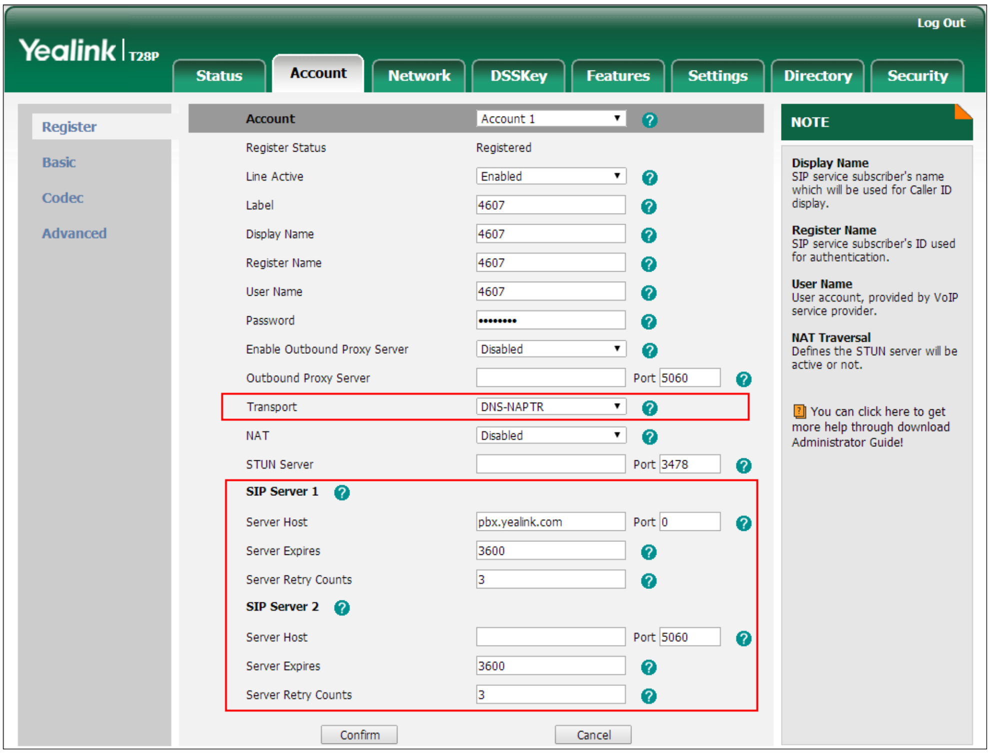
6. Click **Confirm** to accept the change.

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. Select **DNS-NAPTR** from the pull-down list of **Transport**.

5. 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.



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

Note If the outbound proxy server is required and the transport is set to DNS-NAPTR, you must set the port of outbound proxy server to 0 for NAPTR, SRV and A queries.

SIP Server Domain Name Resolution

If a domain name is configured for a SIP server, the IP address(es) associated with that domain name will be resolved through DNS as specified by RFC 3263. The DNS query involves NAPTR, SRV and A queries, which allows the IP phone to adapt to various deployment environments. The IP phone performs 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 SIP 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 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 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 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 phone will perform NAPTR query again according to the previous NAPTR query result.

SRV (Service Location Record)

The IP 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 phone uses this port. If the Target is not a numeric IP address, the IP phone performs an A query. So in this case, the IP phone uses "server1.yealink.pbx.com" and "server2.yealink.pbx.com" for the A query.

A (Host IP Address)

The IP 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 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 phone will go through the following steps to connect the call:

1. Sends the INVITE request to the primary server.
2. If the primary server does not respond correctly to the INVITE, then tries to make the call using the secondary server.
3. If the secondary server is also unavailable, the IP phone will try the fallback server until it either succeeds in making a call or exhausts all servers at which point the call will fail.

At the start of a call, server availability is determined by SIP signaling failure. SIP signaling failure depends on the SIP protocol being used as described below:

- If TCP is used, then the signaling fails if the connection or the send fails.
- If UDP is used, then the signaling fails if ICMP is detected or if the signal times out. If the signaling has been attempted through all servers in the list and this is the last server, then the signaling fails after the complete UDP timeout defined in RFC 3261. If it is not the last server in the list, the maximum number of retries depends on the

configured retry count.

Procedure

SIP Server Domain Name Resolution can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure the transport type on the IP phone. **Parameters:** account.X.transport account.X.naptr_build
Local	Web User Interface	Configure the transport type on the IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-register&q=load&acc=0

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.transport	**0, 1, 2 or 3**	**0**
Description: Configures the type of transport protocol for account X. **0**-UDP **1**-TCP **2**-TLS **3**-DNS-NAPTR If the parameter is set to 3 (DNS-NAPTR) and no server port is given, the IP phone performs the DNS NAPTR and SRV queries for the service type and port. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Web User Interface:** Account->Register ->Transport **Phone User Interface:** None		

Parameters	Permitted Values	Default
account.X.naptr_build	0 or 1	0
Description: Configures the way of SRV query for the IP phone to be performed when no result is returned from NAPTR query for account X. **0**-SRV query using UDP only **1**-SRV query using UDP, TCP and TLS X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Web User Interface:** None **Phone User Interface:** None		

Static DNS Cache

Failover redundancy can only be utilized when the configured domain name of the SIP server is resolved to multiple IP addresses. If the IP 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 phone. The IP phone will attempt to resolve the domain name of the SIP server with static DNS cache.

When the IP phone is configured with a DNS server, the IP phone will behave as follows to resolve domain name of the SIP server:

- The IP 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 phone will attempt to perform a DNS query again.
- If the DNS query returns a result, the IP phone will use the returned record and ignore the statically configured cache values.

When the IP phone is not configured with a DNS server, it will behave as follow:

- The IP phone attempts to resolve the domain name within the static DNS cache.

- The IP phone will always use the results returned from the static DNS cache.

IP 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.

Configuration File	<y0000000000xx>.cfg	Configure NAPTR/SRV/A records. **Parameters:** 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
	<MAC>.cfg	Configure the IP phone whether to cache the additional DNS records. **Parameter:** account.X.dns_cache_type Configure the IP phone whether to use static DNS cache preferentially. **Parameter:** account.X.static_cache_pri

Details of Configuration Parameters:

Parameters	Permitted Values	Default
dns_cache_naptr.X.name (X ranges from 1 to 12)	**String within 256 characters**	**Blank**
Description: Configures the domain name to which NAPTR record X refers. **Example:** dns_cache_naptr.1.name = yealink.pbx.com **Web User Interface:** None **Phone User Interface:** None		
dns_cache_naptr.X.flags (X ranges from 1 to 12)	**S, A, U or P**	**Blank**
Description: 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). **S**-Do an SRV lookup next. **A**-Do an A lookup next. **U**-No need to do a DNS query next. **P**-Service customized by the user **Example:** dns_cache_naptr.1.flags = S **Web User Interface:** None **Phone User Interface:** None		
dns_cache_naptr.X.order (X ranges from 1 to 12)	**Integer from 0 to 65535**	**0**
Description: Configures the order of NAPTR record X. NAPTR record with lower order is more preferred. **Example:**		

Parameters	Permitted Values	Default
dns_cache_naptr.1.order = 90 **Web User Interface:** None **Phone User Interface:** None		
dns_cache_naptr.X.preference (X ranges from 1 to 12)	**Integer from 0 to 65535**	**0**
Description: Configures the preference of NAPTR record X. NAPTR record with lower preference is more preferred. **Example:** dns_cache_naptr.1.preference = 50 **Web User Interface:** None **Phone User Interface:** None		
dns_cache_naptr.X.replace (X ranges from 1 to 12)	**Domain name**	**Blank**
Description: Configures a domain name to be used for the next SRV query in NAPTR record X. **Example:** dns_cache_naptr.1.replace = _sip._tcp.yealink.pbx.com **Web User Interface:** None **Phone User Interface:** None		
dns_cache_naptr.X.service (X ranges from 1 to 12)	**String within 32 characters**	**Blank**
Description: Configures the transport protocol available for the SIP server in NAPTR record X. **SIP+D2U**: SIP over UDP **SIP+D2T**: SIP over TCP		

Parameters	Permitted Values	Default
SIP+D2S: SIP over SCTP **SIPS+D2T**: SIPS over TCP **Example:** dns_cache_naptr.1.service = SIP+D2T **Web User Interface:** None **Phone User Interface:** None		
dns_cache_naptr.X.ttl (X ranges from 1 to 12)	Integer from 30 to 2147483647	300
Description: Configures the time interval (in seconds) that NAPTR record X may be cached before the record should be consulted again. **Example:** dns_cache_naptr.1.ttl = 3600 **Web User Interface:** None **Phone User Interface:** None		
dns_cache_srv.X.name (X ranges from 1 to 12)	Domain name	Blank
Description: Configures the domain name in SRV record X. **Example:** dns_cache_srv.1.name = _sip._tcp.yealink.pbx.com **Web User Interface:** None **Phone User Interface:** None		
dns_cache_srv.X.port (X ranges from 1 to 12)	Integer from 0 to 65535	0
Description:		

Parameters	Permitted Values	Default
Configures the port to be used in SRV record X. **Example;** dns_cache_srv.1.port = 5060 **Web User Interface:** None **Phone User Interface:** None		
dns_cache_srv.X.priority (X ranges from 1 to 12)	**Integer from 0 to 65535**	**0**
Description: Configures the priority for the target host in SRV record X. Lower priority is more preferred. **Web User Interface:** None **Phone User Interface:** None		
dns_cache_srv.X.target (X ranges from 1 to 12)	**Domain name**	**Blank**
Description: Configures the domain name of the target host for an A query in SRV record X. **Example:** dns_cache_srv.1.target = server1.yealink.pbx.com **Web User Interface:** None **Phone User Interface:** None		
dns_cache_srv.X.weight (X ranges from 1 to 12)	**Domain name**	**0**
Description: 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.		

Parameters	Permitted Values	Default
Example: dns_cache_srv.1.weight = 1 **Web User Interface:** None **Phone User Interface:** None		
dns_cache_srv.X.ttl (X ranges from 1 to 12)	**Integer from 30 to 2147483647**	**300**
Description: Configures the time interval (in seconds) that SRV record X may be cached before the record should be consulted again. **Example:** dns_cache_srv.1.ttl = 3600 **Web User Interface:** None **Phone User Interface:** None		
dns_cache_a.X.name (X ranges from 1 to 12)	**Domain name**	**Blank**
Description: Configures the domain name in A record X. **Example:** dns_cache_a.1.name = yealink.pbx.com **Web User Interface:** None **Phone User Interface:** None		
dns_cache_a.X.ip (X ranges from 1 to 12)	**IP address**	**Blank**
Description: Configures the IP address that the domain name in A record X maps to. **Example:** dns_cache_a.1.ip = 192.168.1.13		

Parameters	Permitted Values	Default
Web User Interface: None **Phone User Interface:** None		
dns_cache_a.X.ttl (X ranges from 1 to 12)	**Integer from 30 to 2147483647**	**300**
Description: Configures the time interval (in seconds) that A record X may be cached before the record should be consulted again. **Example:** dns_cache_a.1.ttl = 3600 **Web User Interface:** None **Phone User Interface:** None		
account.X.dns_cache_type	**0, 1 or 2**	**1**
Description: Configures whether the IP phone uses the DNS cache for domain name resolution of the SIP server and caches the additional DNS records for account X. **0**-Perform real-time DNS query rather than using DNS cache. **1**-Use DNS cache, but do not cache the additional DNS records. **2**-Use DNS cache and cache the additional DNS records. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Example:** account.1.dns_cache_type = 1 **Web User Interface:** None **Phone User Interface:** None		
account.X.static_cache_pri	**0 or 1**	**0**

Parameters	Permitted Values	Default
Description: Configures whether preferentially to use the static DNS cache for domain name resolution of the SIP server for account X. **0**-Use domain name resolution from the DNS server preferentially **1**-Use static DNS cache preferentially X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Example:** account.1.static_cache_pri = 1 **Web User Interface:** None **Phone User Interface:** None		

LLDP

LLDP (Linker Layer Discovery Protocol) is a vendor-neutral Link Layer protocol, which allows IP phones to receive and/or transmit device-related information from/to directly connected devices on the network that are also using the protocol, and store the information about other devices. LLDP transmits information as packets called LLDP Data Units (LLDPDUs). An LLDPDU consists of a set of Type-Length-Value (TLV) elements, each of which contains a particular type of information about the device or the port transmitting it.

LLDP-MED (Media Endpoint Discovery)

LLDP-MED is published by the Telecommunications Industry Association (TIA). It is an extension to LLDP that operates between endpoint devices and network connectivity devices. LLDP-MED specifically provides support for voice over IP (VoIP) applications and provides the following capabilities:

- Capabilities Discovery -- allows IP phones to determine the capabilities that the connected switch supports and has enabled.
- Network Policy -- provides voice VLAN configuration to notify IP phones which VLAN to use and QoS-related configuration for voice data. It provides a “plug and play” network environment.
- Power Management -- provides information related to how IP phones are powered, power priority, and how much power IP phones need.

- Inventory Management -- provides a means to effectively manage IP phones and their attributes such as model number, serial number and software revision.

TLVs supported by IP phones are summarized in the following table:

TLV Type	TLV Name	Description
Mandatory TLVs	Chassis ID	The network address of the IP phone.
	Port ID	The MAC address of the IP phone.
	Time To Live	Seconds until data unit expires.
	End of LLDPDU	Marks end of LLDPDU.
Optional TLVs	System Name	Name assigned to the IP phone. The default value is “yealink”.
	System Description	Description of the IP phone. The default value is “yealink”.
	System Capabilities	The supported and enabled capabilities of the IP phone. The supported capabilities are Bridge, Telephone and Router. The enabled capabilities are Bridge and Telephone by default.
	Port Description	Description of port that sends data unit. The default value is “WAN PORT”.
IEEE Std 802.3 Organizationally Specific TLV	MAC/PHY Configuration/Status	Duplex and bit rate settings of the IP phone. The Auto Negotiation is supported and enabled by default. The advertised capabilities of PMD. Auto-Negotiation is: 100BASE-TX (full duplex mode), 100BASE-TX (half duplex mode), 10BASE-T (full duplex mode), or 10BASE-T (half duplex mode).
TIA Organizationally Specific TLVs	Media Capabilities	The MED device type of the IP phone and the supported LLDP-MED TLV type can be encapsulated in LLDPDU. The supported LLDP-MED TLV types are: LLDP-MED Capabilities, Network Policy, Extended Power via MDI-PD and Inventory.

TLV Type	TLV Name	Description
	Network Policy	Port VLAN ID, application type, L2 priority and DSCP value.
	Extended Power-via-MDI	Power type, source, priority and value.
	Inventory – Hardware Revision	Hardware revision of the IP phone.
	Inventory – Firmware Revision	Firmware revision of the IP phone.
	Inventory – Software Revision	Software revision of the IP phone.
	Inventory – Serial Number	Serial number of the IP phone.
	Inventory – Manufacturer Name	Manufacturer name of the IP phone. The default value is "yealink".
	Inventory – Model Name	Model name of the IP phone.
	Asset ID	Assertion identifier of the IP phone. The default value is "asset".

Procedure

LLDP can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure LLDP. **Parameters:** network.lldp.enable network.lldp.packet_interval
Local	Web User Interface	Configure LLDP. **Navigate to**: http://<phoneIPAddress>/servlet?p=network-adv&q=load
	Phone User Interface	Configure LLDP feature.

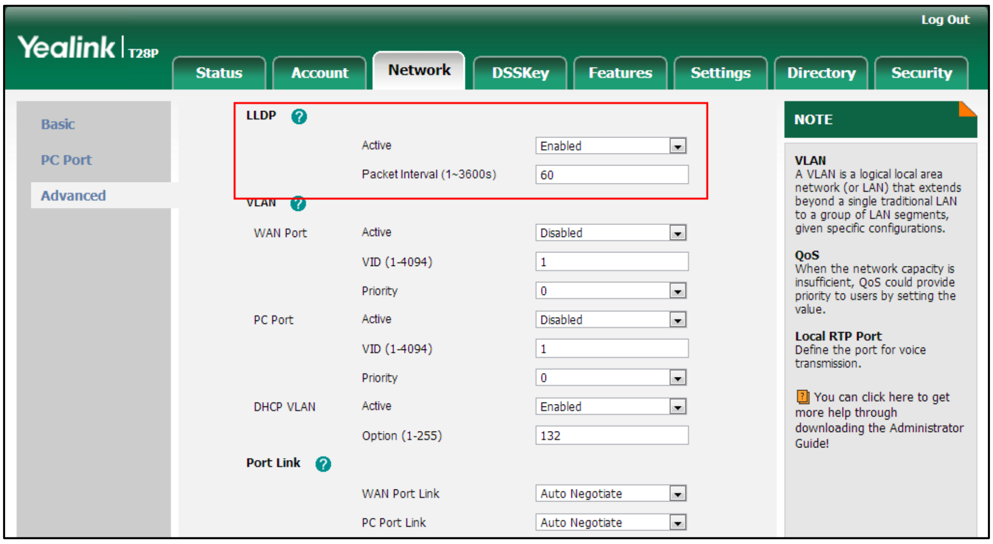
Details of Configuration Parameters:

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>network.lldp.enable</td><td>0 or 1</td><td>1</td></tr>
<tr><td colspan="3">Description:
Enables or disables LLDP feature on the IP phone.
0-Disabled
1-Enabled
Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Web User Interface:
Network->Advanced->LLDP->Active
Phone User Interface:
Menu->Settings->Advanced Settings (default password: admin) ->Network->LLDP->LLDP Status</td></tr>
<tr><td>network.lldp.packet_interval</td><td>Integer from 1 to 3600</td><td>60</td></tr>
<tr><td colspan="3">Description:
Configures the interval (in seconds) for the IP phone to send the LLDP request.
Note: If you change this parameter, the IP phone will reboot to make the change take effect. It works only if the parameter “network.lldp.enable” is set to 1 (Enabled).
Web User Interface:
Network->Advanced->LLDP->Packet Interval (1~3600s)
Phone User Interface:
Menu->Settings->Advanced Settings (default password: admin) ->Network->LLDP->Packet Interval</td></tr>
</table>

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.

To configure LLDP feature via phone user interface:

1. Press **Menu**->**Settings**->**Advanced Settings** (default password: admin) ->**Network**->**LLDP**->**LLDP Status.**
2. Press ◀ or ▶ , or the **Switch** soft key to select the desired value from the **LLDP Status** field.
3. Enter the priority value (1-3600s) in the **Packet Interval** field.
4. Press the **Save** soft key to accept the change.

VLAN

VLAN (Virtual Local Area Network) is used to logically divide a physical network into several broadcast domains. VLAN membership can be configured through software instead of physically relocating devices or connections. Grouping devices with a common set of requirements regardless of their physical location can greatly simplify network design. VLANs can address issues such as scalability, security and network management.

The purpose of VLAN configurations on the IP phone is to insert tag with VLAN information to the packets generated by the IP phone. When VLAN is properly configured for the ports (Internet port and PC port) on the IP phone, the IP phone will tag all packets from these ports with the VLAN ID. The switch receives and forwards the tagged packets to the corresponding VLAN according to the VLAN ID in the tag as described in IEEE Std 802.3.

VLAN on IP phones allows simultaneous access for a regular PC. This feature allows a PC to be daisy chained to an IP phone and the connection for both PC and IP phone to be trunked through the same physical Ethernet cable.

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

VLAN Discovery via DHCP

IP phones support VLAN discovery via DHCP. When the VLAN Discovery method is set to DHCP, the IP phone will examine DHCP option for a valid VLAN ID. The predefined option 132 is used to supply the VLAN ID by default. You can customize the DHCP option used to request the VLAN ID.

For more information on VLAN, refer to *VLAN Feature on Yealink IP Phones*, available online: http://www.yealink.com/DocumentDownload.aspx?CateId=142&flag=142.

Procedure

VLAN can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure VLAN for the Internet port and PC port manually. **Parameters:** network.vlan.internet_port_enable network.vlan.internet_port_vid network.vlan.internet_port_priority network.vlan.pc_port_enable network.vlan.pc_port_vid network.vlan.pc_port_priority Configure DHCP VLAN discovery feature. **Parameters:** network.vlan.dhcp_enable network.vlan.dhcp_option Configure the VLAN assignment method. **Parameter:** network.vlan.vlan_change.enable
Local	Web User Interface	Configure VLAN for the Internet port and PC port. Configure DHCP VLAN discovery feature.

		Navigate to: http://<phoneIPAddress>/servlet?p=network-adv&q=load
	Phone User Interface	Configure VLAN for the Internet port and PC port. Configure DHCP VLAN discovery feature.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
network.vlan.internet_port_enable	**0 or 1**	**0**
Description: Enables or disables VLAN for the Internet (WAN) port. **0**-Disabled **1**-Enabled **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->VLAN ->WAN Port->Active **Phone User Interface:** Menu->Settings->Advanced Settings (default password: admin) ->Network->VLAN->WAN Port->VLAN Status		
network.vlan.internet_port_vid	**Integer from 1 to 4094**	**1**
Description: Configures VLAN ID for the Internet (WAN) port. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->VLAN ->WAN Port->VID (1-4094) **Phone User Interface:** Menu->Settings->Advanced Settings (default password: admin) ->Network->VLAN->WAN Port->VID Number		
network.vlan.internet_port_priority	**Integer from 0 to 7**	**0**

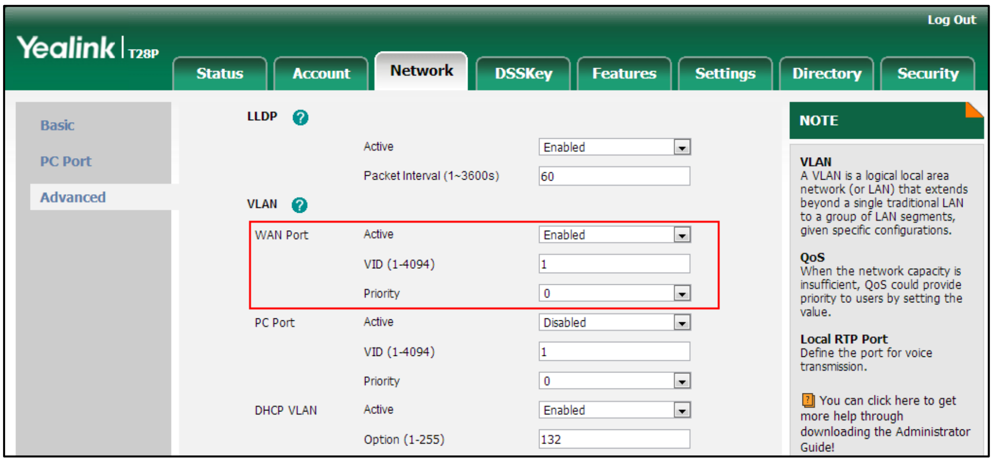
<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td colspan="3">Description:
Configures VLAN priority for the Internet (WAN) port.
7 is the highest priority, 0 is the lowest priority.
Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Web User Interface:
Network->Advanced->VLAN ->WAN Port->Priority
Phone User Interface:
Menu->Settings->Advanced Settings (default password: admin) ->Network->VLAN->WAN Port->Priority</td></tr>
<tr><td>network.vlan.pc_port_enable</td><td>0 or 1</td><td>0</td></tr>
<tr><td colspan="3">Description:
Enables or disables VLAN for the PC (LAN) port.
0-Disabled
1-Enabled
Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Web User Interface:
Network->Advanced->VLAN >PC Port->Active
Phone User Interface:
Menu->Settings->Advanced Settings (default password: admin) ->Network->VLAN->WAN Port->PC Port->VLAN Status</td></tr>
<tr><td>network.vlan.pc_port_vid</td><td>Integer from 1 to 4094</td><td>1</td></tr>
<tr><td colspan="3">Description:
Configures VLAN ID for the PC (LAN) port.
Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Web User Interface:
Network->Advanced->VLAN >PC Port->VID (1-4094)
Phone User Interface:
Menu->Settings->Advanced Settings (default password: admin) ->Network->VLAN->WAN Port->PC Port->VID</td></tr>
</table>

Parameters	Permitted Values	Default
network.vlan.pc_port_priority	**Integer from 0 to 7**	**0**
Description: Configures VLAN priority for the PC (LAN) port. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->VLAN >PC Port->Priority **Phone User Interface:** Menu->Settings->Advanced Settings (default password: admin) ->Network->VLAN->WAN Port->PC Port->Priority		
network.vlan.dhcp_enable	**0 or 1**	**1**
Description: Enables or disables DHCP VLAN discovery feature on the IP phone. **0**-Disabled **1**-Enabled **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->VLAN >DHCP VLAN->Active **Phone User Interface:** Menu->Settings->Advanced Settings (default password: admin) ->Network->VLAN->DHCP VLAN->DHCP VLAN		
network.vlan.dhcp_option	**Integer from 128 to 254**	**132**
Description: Configures the DHCP option from which the IP phone will obtain the VLAN settings. You can configure at most five DHCP options and separate them by commas. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->VLAN->DHCP VLAN->Option(1-255) **Phone User Interface:**		

Parameters	Permitted Values	Default
Menu->Settings->Advanced Settings (default password: admin) ->Network->VLAN->DHCP VLAN->Option		
network.vlan.vlan_change.enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to obtain IP address with lower preference of VLAN assignment method or disable VLAN feature when the IP phone cannot obtain IP address with the current VLAN assignment method. **0**-Disabled **1**-Enabled The priority of each method is: LLDP>Manual>DHCP VLAN. If it is set to 1 (Enabled), when the phone cannot obtain IP address using the VLAN ID obtained by LLDP during 2 minutes, the phone will use the manually configured VLAN ID to obtain IP address; when the phone cannot obtain IP address after using all the method, the phone will disable VLAN feature. **Web User Interface:** None **Phone User Interface:** None		

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**.



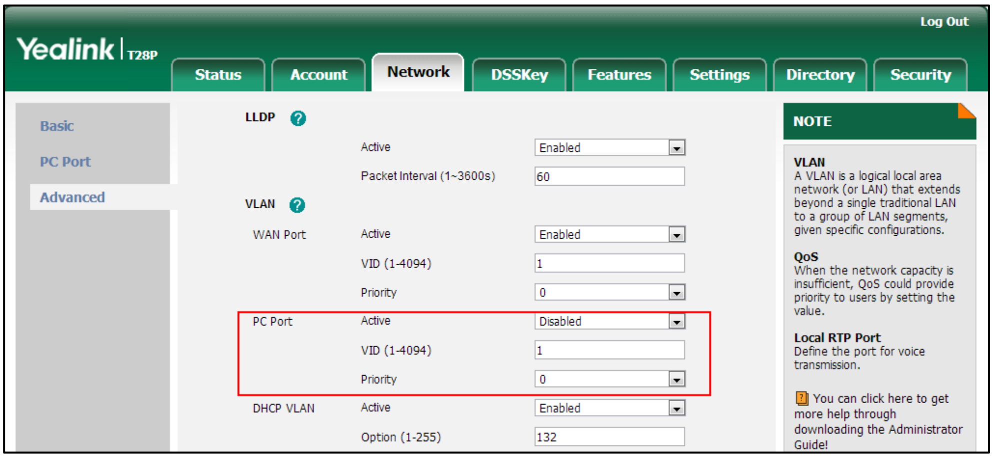
5. Click **Confirm** to accept the change.

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

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

To configure VLAN for PC port via web user interface:

1. Click on **Network**->**Advanced**.
2. In the **VLAN** block, select the desired value from the pull-down list of **PC Port Active**.
3. Enter the VLAN ID in the **VID (1-4094)** field.
4. Select the desired value (0-7) from the pull-down list of **Priority**.



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

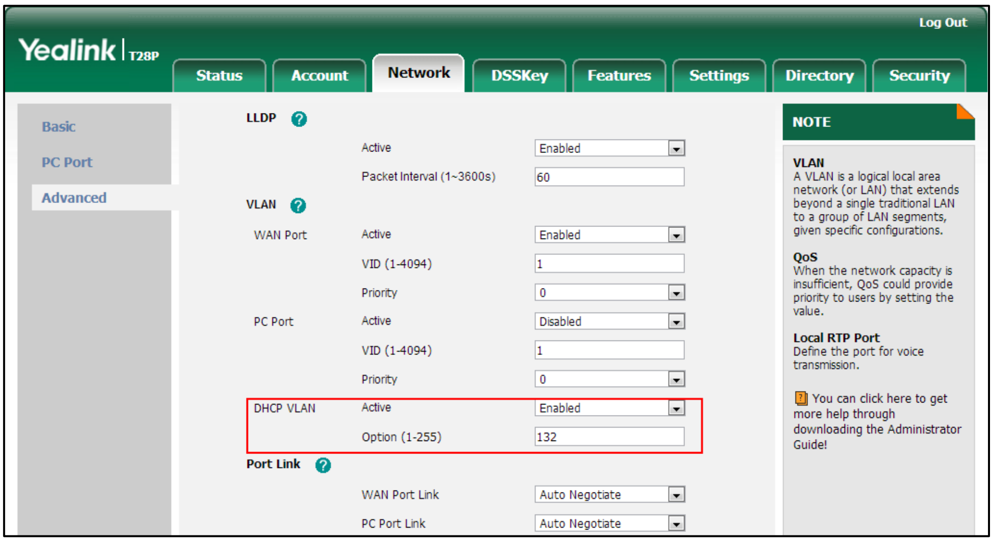
   A dialog box pops up to prompt that the settings will take effect after a reboot.

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

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.

To configure VLAN for Internet port (or PC port) via phone user interface:

1. Press **Menu**->**Settings**->**Advanced Settings** (default password: admin) ->**Network**->**VLAN**->**WAN Port** (or **PC Port**).
2. Press or , or the **Switch** soft key to select the desired value from the **VLAN Status** field.
3. Enter the VLAN ID (1-4094) in the **VID** field.
4. Enter the priority value (0-7) in the **Priority** field.
5. Press the **Save** soft key to accept the change

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

To configure DHCP VLAN discovery via phone user interface:

1. Press **Menu**->**Settings**->**Advanced Settings** (default password: admin) ->**Network**->**VLAN**->**DHCP VLAN**.
2. Press or , or the **Switch** soft key to select the desired value from the **DHCP VLAN** field.
3. Enter the desired option in the **Option** field.
4. Press the **Save** soft key to accept the change.

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

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. There are two types of VPN access: remote-access VPN (connecting an individual device to a network) and site-to-site VPN (connecting two networks together). Remote-access VPN allows employees to access their company's intranet from home or outside the office, and site-to-site VPN allows employees in geographically separated offices to share one cohesive virtual network. VPN can be also classified by the protocols used to tunnel the traffic. It provides security through tunneling protocols: IPSec, SSL, L2TP and PPTP.

IP phones support SSL VPN, which provides remote-access VPN capabilities through SSL. OpenVPN is a full featured SSL VPN software solution that creates secure connections in remote access facilities, designed to work with the TUN/TAP virtual 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. IP 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 phone, the IP 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 phone in advance. The file format of the compressed package must be *.tar. For SIP-T28/T26P/T22P IP phones, the maximum file size is 100KB. The related VPN files are: certificates (ca.crt and client.crt), key (client.key) and the configuration file (vpn.cnf) of the VPN client. For more information on how to package a TAR file, refer to *OpenVPN Feature on Yealink IP Phones*, available online: http://www.yealink.com/DocumentDownload.aspx?CateId=142&flag=142.

Procedure

VPN can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure VPN feature and upload a TAR file to the IP phone. **Parameters:** network.vpn_enable openvpn.url
Local	Web User Interface	Configure VPN feature and upload a TAR package to the IP phone. **Navigate to:**

		http://<phoneIPAddress>/servlet?p=network-adv&q=load
	Phone User Interface	Configure VPN feature.

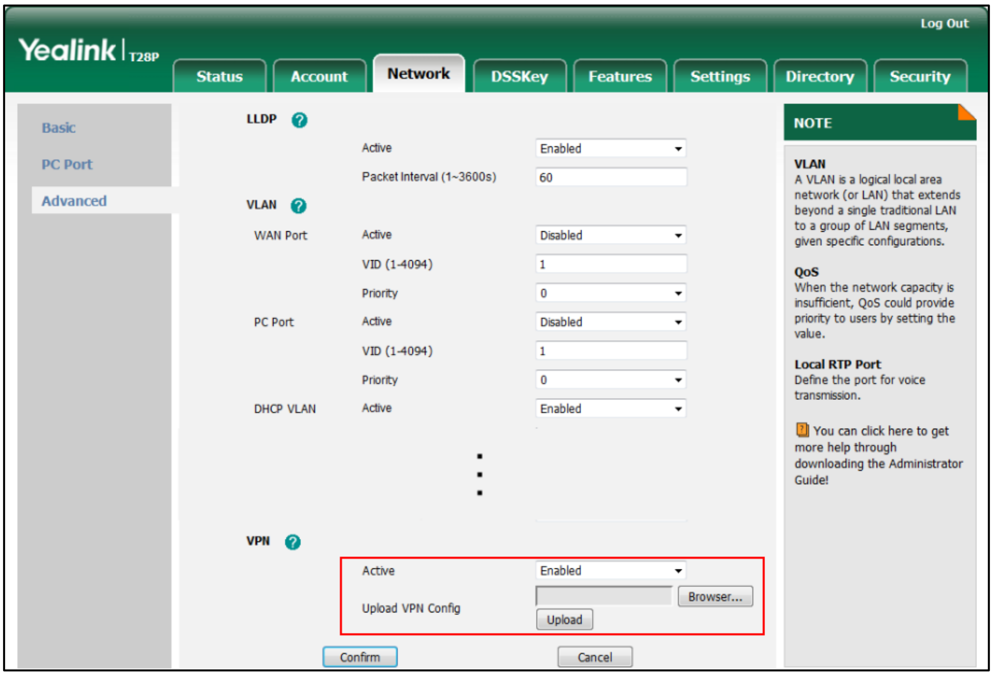
Details of Configuration Parameters:

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

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.

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



The web user interface prompts the message "Import config…".

4. In the **VPN** block, select the desired value from the pull-down list of **Active**.
5. Click **Confirm** to accept the change.

   A dialog box pops up to prompt that settings will take effect after a reboot.
6. Click **OK** to reboot the phone.

To configure VPN via phone user interface after uploading a TAR file:

1. Press **Menu**->**Settings**->**Advanced Settings** (default password: admin) ->**Network**->**VPN**.
2. Press or , or the **Switch** soft key to select the desired value from the **VPN Active** field.

   You must upload the OpenVPN TAR file using configuration files or via web user interface in advance.
3. Press the **Save** soft key to accept the change.

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

Voice Quality Monitoring

Voice quality monitoring feature allows the IP 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 phones:

- RTCP-XR
- VQ-RTCPXR

Note Voice quality monitoring feature is applicable to IP phones running firmware version 73 or later.

RTCP-XR

The RTCP-XR mechanism, complaint 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 configuration files.

Configuration File	<y0000000000xx>.cfg	Configure RTCP-XR. **Parameters:** phone_setting.rtcp_xr_report.enable

Details of Configuration Parameters:

Parameters	Permitted Values	Default
phone_setting.rtcp_xr_report.enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to periodically (every 5 seconds) send RTCP-XR packets to another participating phone during a call for call quality monitoring and diagnosing. **Note**: It is only applicable to IP phones running firmware version 73 or later. **Web User Interface:** None		

Parameters	Permitted Values	Default
Phone User Interface: None		

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 two ways:

- Based on current values, such as jitter, jitter buffer max and round trip delay.
- 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 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 phone user interface. Users can also specify the options of the RTP status to be displayed on the phone user interface. Options of the RTP status to be displayed on the web user interface cannot be specified.

Note

When using voice quality monitoring feature, some problems will occur:
1. GapDuration always equals to 0 while no burst duration.
2. JitterBufferAdaptive always equals to 2 (non-adaptive/fixed), even if it's configured adaptive.
3. MOSLQ/MOSCQ may be lower or higher than what VQMon calculates sometimes (error of [1, +0.5]).

The problems will be fixed in firmware version 80.

Procedure

RTCP-XR can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure the generation of session packets. **Parameter:** phone_setting.vq_rtcpxr.session_report.enable

		Configure the generation of interval packets. **Parameters:** phone_setting.vq_rtcpxr.interval_report.enable phone_setting.vq_rtcpxr_interval_period Configure the generation of alert packets. **Parameters:** 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 Configure the phone to display RTP status showing the voice quality report of the last call on the web user interface. **Parameter:** phone_setting.vq_rtcpxr.states_show_on_web.enable Configure the phone to display RTP status showing the voice quality report of the last call or the current call on the phone user interface. **Parameter:** phone_setting.vq_rtcpxr.states_show_on_gui.enable Configure the options of the RTP status displayed on the phone user interface. **Parameters:** phone_setting.vq_rtcpxr_display_start_time.enable phone_setting.vq_rtcpxr_display_stop_time.enable phone_setting.vq_rtcpxr_display_local_call_id.enable phone_setting.vq_rtcpxr_display_remote_call_id.enable phone_setting.vq_rtcpxr_display_local_codec.enable

		phone_setting.vq_rtcpxr_display_remote_codec.enable phone_setting.vq_rtcpxr_display_jitter.enable phone_setting.vq_rtcpxr_display_jitter_buffer_max.enable phone_setting.vq_rtcpxr_display_packets_lost.enable phone_setting.vq_rtcpxr_display_symm_oneway_delay.enable phone_setting.vq_rtcpxr_display_round_trip_delay.enable phone_setting.vq_rtcpxr_display_moslq.enable phone_setting.vq_rtcpxr_display_moscq.enable
	<MAC>.cfg	Configure the central report collector. **Parameters:** account.X.vq_rtcpxr.collector_name account.X.vq_rtcpxr.collector_server_host account.X.vq_rtcpxr.collector_server_port
Local	Web User Interface	Configure VQ-RTCPXR. Configure the phone to display RTP status showing the voice quality report of the last call on the web user interface. Configure the phone to display RTP status showing the voice quality report of the last call or the current call on the phone user interface. Configure the options of the RTP status displayed on the phone user interface. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-voicemonitoring&q=load Configure the central report collector. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

Details of Configuration Parameters:

Parameters	Permitted Values	Default
phone_setting.vq_rtcpxr.session_report.enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to send a session quality report to the central report collector at the end of each call. **0**-Disabled **1**-Enabled **Note**: It is only applicable to IP phones running firmware version 73 or later. **Web User Interface:** Settings->Voice Monitoring->VQ RTCP-XR Session Report **Phone User Interface:** None		
phone_setting.vq_rtcpxr.interval_report.enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to send an interval quality report to the central report collector periodically throughout a call. **0**-Disabled **1**-Enabled **Note**: It is only applicable to IP phones running firmware version 73 or later. **Web User Interface:** Settings->Voice Monitoring->VQ RTCP-XR Interval Report **Phone User Interface:** None		
phone_setting.vq_rtcpxr_interval_period	**Integer from 5 to 20**	**20**
Description: Configures the interval (in seconds) for the IP phone to send an interval quality report to the central report collector periodically throughout a call. **Note**: It is only applicable to IP phones running firmware version 73 or later. **Web User Interface:** Settings->Voice Monitoring->Period for Interval Report		

Parameters	Permitted Values	Default
Phone User Interface: None		
phone_setting.vq_rtcpxr_moslq_threshold_warning	**15 to 40**	**Blank**
Description: 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. 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. If it is set to blank, warning alerts are not generated due to MOS-LQ. **Note**: It is only applicable to IP phones running firmware version 73 or later. **Web User Interface:** Settings->Voice Monitoring->Warning threshold for Moslq **Phone User Interface:** None		
phone_setting.vq_rtcpxr_moslq_threshold_critical	**15 to 40**	**Blank**
Description: Configures the desired 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. 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. If it is set to blank, critical alerts are not generated due to MOS-LQ. **Note**: It is only applicable to IP phones running firmware version 73 or later. **Web User Interface:** Settings->Voice Monitoring->Critical threshold for Moslq **Phone User Interface:** None		

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>phone_setting.vq_rtcpxr_delay_threshold_warning</td><td>10 to 2000</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the threshold value of one way delay (in ms) that causes the phone to send a warning 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 less than or equal to 500, the phone will send a waring alert quality report to the central report collector; when the value of one way delay computed by the phone is greater than 500, the phone will not send a warning alert quality report to the central report collector.
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.
Note: It is only applicable to IP phones running firmware version 73 or later.
Web User Interface:
Settings->Voice Monitoring->Warning threshold for Delay
Phone User Interface:
None</td></tr>
<tr><td>phone_setting.vq_rtcpxr_delay_threshold_critical</td><td>10 to 2000</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the threshold value of one way delay (in ms) 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 less 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 greater 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.
Note: It is only applicable to IP phones running firmware version 73 or later.
Web User Interface:
Settings->Voice Monitoring->Critical threshold for Delay
Phone User Interface:
None</td></tr>
<tr><td>phone_setting.vq_rtcpxr.states_show_on_web.enable</td><td>0 or 1</td><td>0</td></tr>
</table>

Parameters		Permitted Values	Default
Description: Enables or disables the voice quality data of the last call to be displayed on web interface at path **Status->RTP Status**. **0**-Disabled **1**-Enabled **Note**: It is only applicable to IP phones running firmware version 73 or later. **Web User Interface:** Settings->Voice Monitoring->Display Report options on Web **Phone User Interface:** None			
phone_setting.vq_rtcpxr.states_show_on_gui.enable		**0 or 1**	**0**
Description: Enables or disables the voice quality data of the last call or current call to be displayed on the LCD screen. You can view the voice quality data of the last call by pressing Menu->Status->RTP Status. You can view the voice quality data of the current call by pressing RTP Status soft key during a call. **0**-Disabled **1**-Enabled **Note**: It is only applicable to IP phones running firmware version 73 or later. **Web User Interface:** Settings->Voice Monitoring->Display Report options on phone **Phone User Interface:** None			
phone_setting.vq_rtcpxr_display_start_time.enable		**0 or 1**	**1**
Description: Enables or disables the phone to display Start Time on the LCD screen. **0**-Disabled **1**-Enabled **Note:** It works only if the parameter "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to "1". **Note**: It is only applicable to IP phones running firmware version 73 or later. **Web User Interface:** Settings->Voice Monitoring->Report options on phone UI->Start Time			

Parameters	Permitted Values	Default
Phone User Interface: None		
phone_setting.vq_rtcpxr_display_stop_time.enable	**0 or 1**	**1**
Description: Enables or disables the phone to display Current Time or Stop Time on the LCD screen. **0**-Disabled **1**-Enabled **Note:** It works only if the parameter "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to "1" and it is only applicable to IP phones running firmware version 73 or later. **Web User Interface:** Settings->Voice Monitoring->Report options on phone UI->Current Time **Phone User Interface:** None		
phone_setting.vq_rtcpxr_display_local_call_id.enable	**0 or 1**	**1**
Description: Enables or disables the phone to display Local User on the LCD screen. **0**-Disabled **1**-Enabled **Note:** It works only if the parameter "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to "1" and it is only applicable to IP phones running firmware version 73 or later. **Web User Interface:** Settings->Voice Monitoring->Report options on phone UI->Local User **Phone User Interface:** None		
phone_setting.vq_rtcpxr_display_remote_call_id.enable	**0 or 1**	**1**

Parameters	Permitted Values	Default
Description: Enables or disables the phone to display Remote User on the LCD screen. **0**-Disabled **1**-Enabled **Note:** It works only if the parameter "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to "1" and it is only applicable to IP phones running firmware version 73 or later. **Web User Interface:** Settings->Voice Monitoring->Report options on phone UI->Remote User **Phone User Interface:** None		
phone_setting.vq_rtcpxr_display_local_codec.enable	**0 or 1**	**1**
Description: Enables or disables the phone to display Local Codec on the LCD screen. **0**-Disabled **1**-Enabled **Note:** It works only if the parameter "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to "1" and it is only applicable to IP phones running firmware version 73 or later. **Web User Interface:** Settings->Voice Monitoring->Report options on phone UI->Local Codec **Phone User Interface:** None		
phone_setting.vq_rtcpxr_display_remote_codec.enable	**0 or 1**	**1**
Description: Enables or disables the phone to display Remote Codec on the LCD screen. **0**-Disabled **1**-Enabled **Note:** It works only if the parameter "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to "1" and it is only applicable to IP phones running firmware version 73 or later. **Web User Interface:** Settings->Voice Monitoring->Report options on phone UI->Remote Codec		

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td colspan="3">Phone User Interface:
None</td></tr>
<tr><td>phone_setting.vq_rtcpxr_display_jitter.enable</td><td>0 or 1</td><td>1</td></tr>
<tr><td colspan="3">Description:
Enables or disables the phone to display Jitter on the LCD screen.
0-Disabled
1-Enabled
Note: It works only if the parameter "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to "1" and it is only applicable to IP phones running firmware version 73 or later.
Web User Interface:
Settings->Voice Monitoring->Report options on phone UI->Jitter
Phone User Interface:
None</td></tr>
<tr><td>phone_setting.vq_rtcpxr_display_jitter_buffer_max.enable</td><td>0 or 1</td><td>1</td></tr>
<tr><td colspan="3">Description:
Enables or disables the phone to display JitteBufferMax on the LCD screen.
0-Disabled
1-Enabled
Note: It works only if the parameter "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to "1" and it is only applicable to IP phones running firmware version 73 or later.
Web User Interface:
Settings->Voice Monitoring->Report options on phone UI->JitteBufferMax
Phone User Interface:
None</td></tr>
<tr><td>phone_setting.vq_rtcpxr_display_packets_lost.enable</td><td>0 or 1</td><td>1</td></tr>
</table>

Parameters	Permitted Values	Default
Description: Enables or disables the phone to display Packet lost on the LCD screen. **0**-Disabled **1**-Enabled **Note:** It works only if the parameter "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to "1" and it is only applicable to IP phones running firmware version 73 or later. **Web User Interface:** Settings->Voice Monitoring->Report options on phone UI->Packet lost **Phone User Interface:** None		
phone_setting.vq_rtcpxr_display_symm_oneway_delay.enable	**0 or 1**	**0**
Description: Enables or disables the phone to display SymmOneWayDelay on the LCD screen. **0**-Disabled **1**-Enabled **Note:** It works only if the parameter "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to "1" and it is only applicable to IP phones running firmware version 73 or later. **Web User Interface:** Settings->Voice Monitoring->Report options on phone UI->SymmOneWayDelay **Phone User Interface:** None		
phone_setting.vq_rtcpxr_display_round_trip_delay.enable	**0 or 1**	**0**
Description: Enables or disables the phone to display RoundTripDelay on the LCD screen. **0**-Disabled **1**-Enabled **Note:** It works only if the parameter "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to "1" and it is only applicable to IP phones running firmware version 73 or later. **Web User Interface:** Settings->Voice Monitoring->Report options on phone UI->RoundTripDelay		

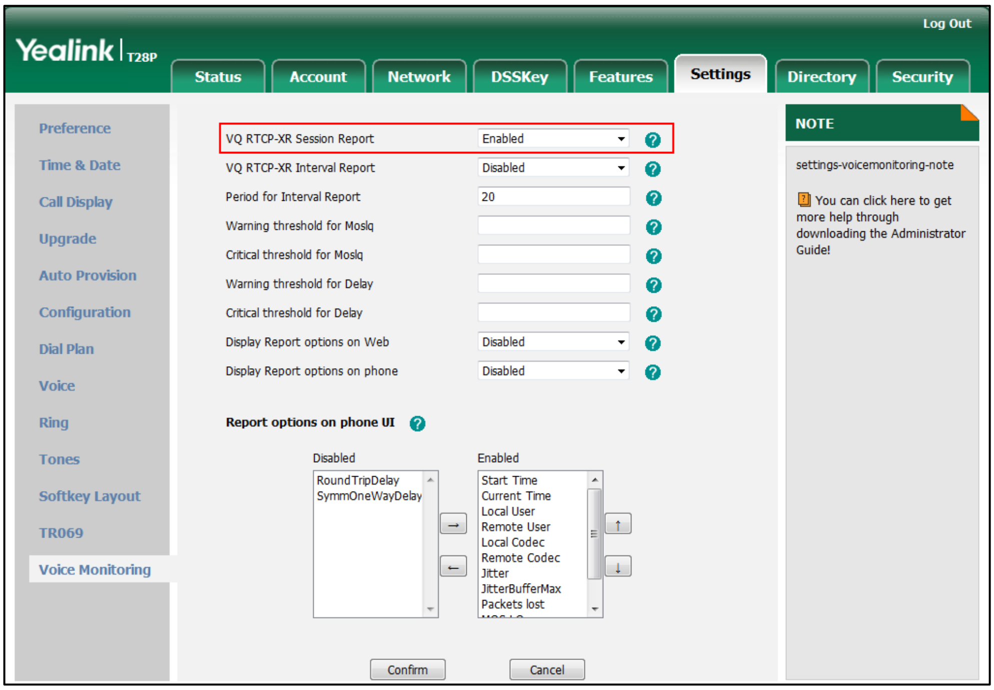
Parameters	Permitted Values	Default
Phone User Interface: None		
phone_setting.vq_rtcpxr_display_moslq.enable	**0 or 1**	**1**
Description: Enables or disables the phone to display MOS-LQ on the LCD screen. **0**-Disabled **1**-Enabled **Note:** It works only if the parameter "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to "1" and it is only applicable to IP phones running firmware version 73 or later. **Web User Interface:** Settings->Voice Monitoring->Report options on phone UI->MOS-LQ **Phone User Interface:** None		
phone_setting.vq_rtcpxr_display_moscq.enable	**0 or 1**	**1**
Description: Enables or disables the phone to display MOS-CQ on the LCD screen. **0**-Disabled **1**-Enabled **Note:** It works only if the parameter "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to "1" and it is only applicable to IP phones running firmware version 73 or later. **Web User Interface:** Settings->Voice Monitoring->Report options on phone UI->MOS-CQ **Phone User Interface:** None		
account.X.vq_rtcpxr.collector_name	**String within 32 characters**	**Blank**

Parameters	Permitted Values	Default
Description: Configures the host name of the central report collector that accepts voice quality reports contained in SIP PUBLISH messages for account X. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Note:** It is only applicable to IP phones running firmware version 73 or later. **Web User Interface:** Account->Advanced->VQ RTCP-XR Collector name **Phone User Interface:** None		
account.X.vq_rtcpxr.collector_server_host	IPv4 Address	Blank
Description: Configures the IP address of the central report collector that accepts voice quality reports contained in SIP PUBLISH messages for account X. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Note:** It is only applicable to IP phones running firmware version 73 or later. **Web User Interface:** Account->Advanced->VQ RTCP-XR Collector address **Phone User Interface:** None		
account.X.vq_rtcpxr.collector_server_port	Integer from 1 to 65535	5060
Description: Configures the port of the central report collector that accepts voice quality reports contained in SIP PUBLISH messages for account X. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Note:** It is only applicable to IP phones running firmware version 73 or later.		

Parameters	Permitted Values	Default
Web User Interface: Account->Advanced->VQ RTCP-XR Collector port **Phone User Interface:** None		

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.**

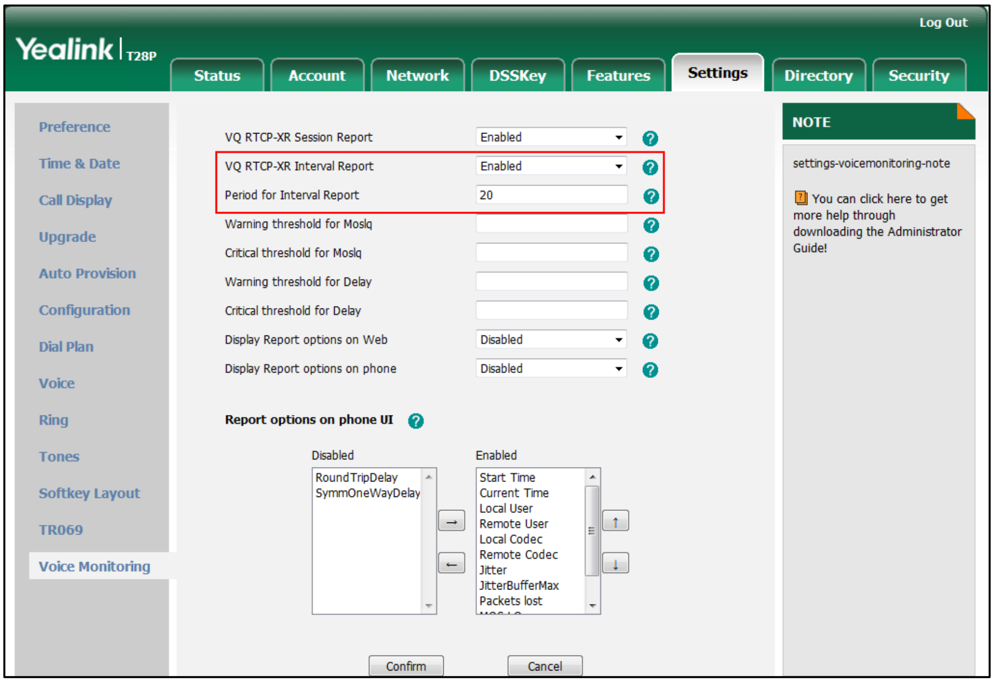


3. Click **Confirm** to accept the change.

To configure interval report for VQ RTCP-XR 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.

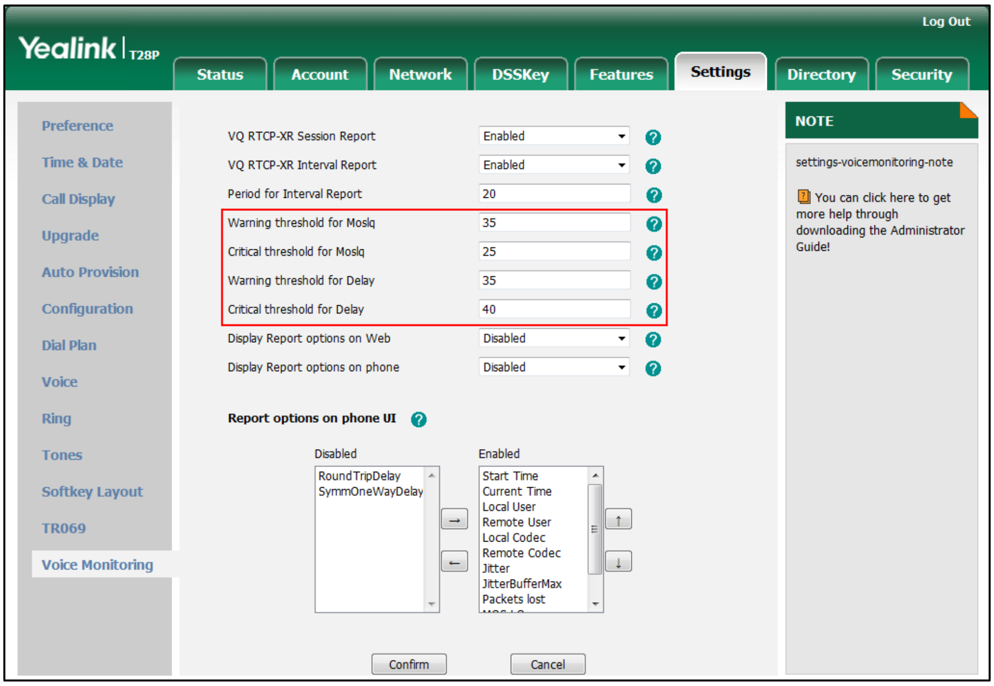


4. Click **Confirm** to accept the change.

To configure alert report for VQ RTCP-XR 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.

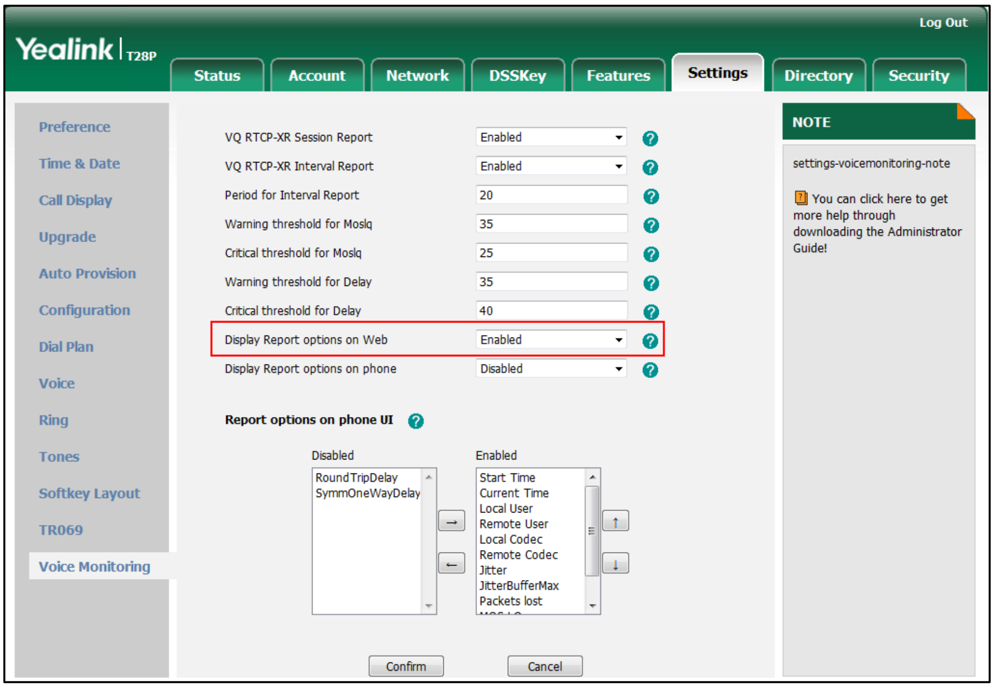
5. Enter the desired value in the **Critical threshold for Delay** field.



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

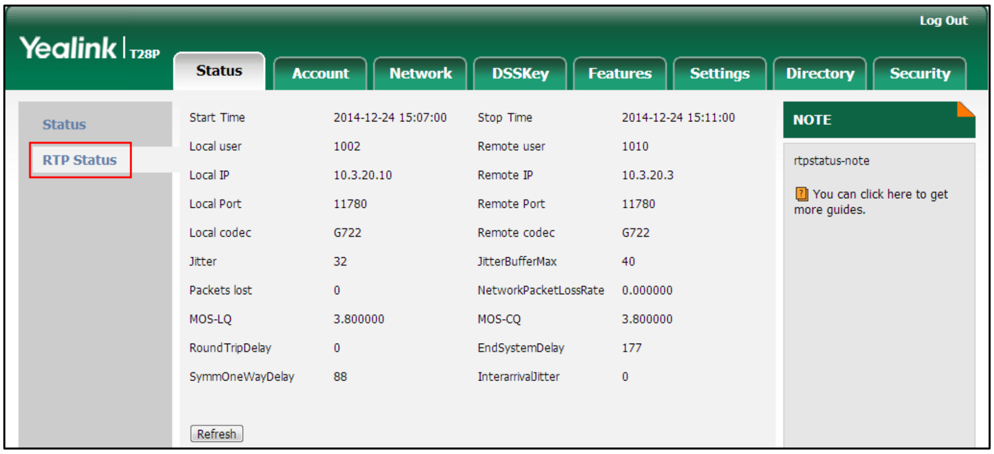
To configure RTP status displayed on the web page via web user interface:

1. Click on **Settings**->**Voice Monitoring.**
2. Select the desired value from the pull-down list of **Display Report options on Web**.



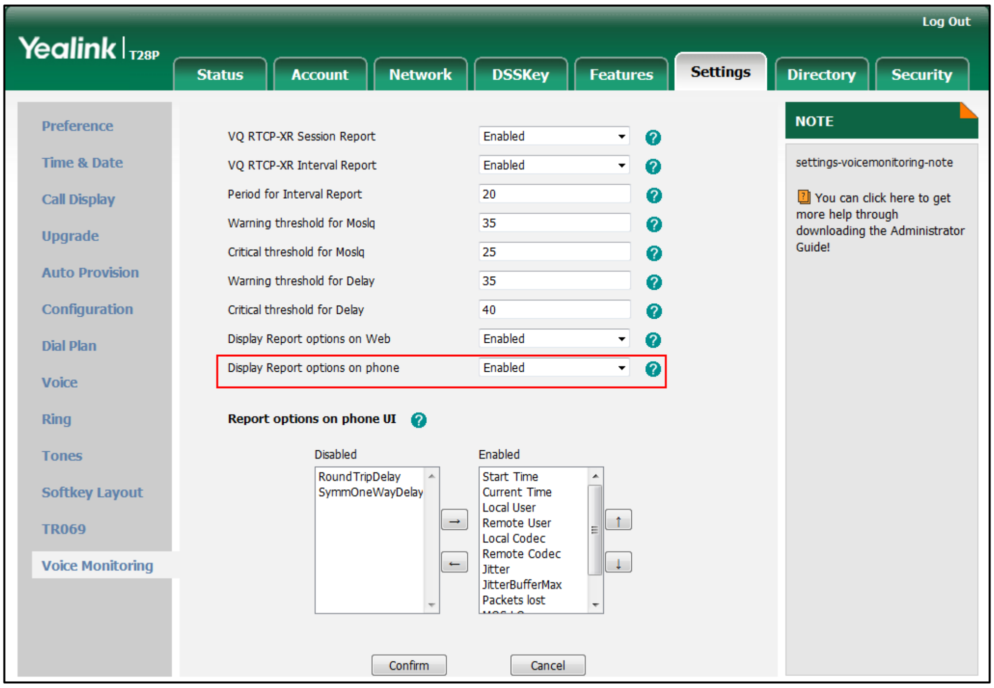
3. Click **Confirm** to accept the change.

The RTP status will appear on the web user interface at the path: **Status**.



To configure RTP status displayed on the LCD screen 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 phone**.



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

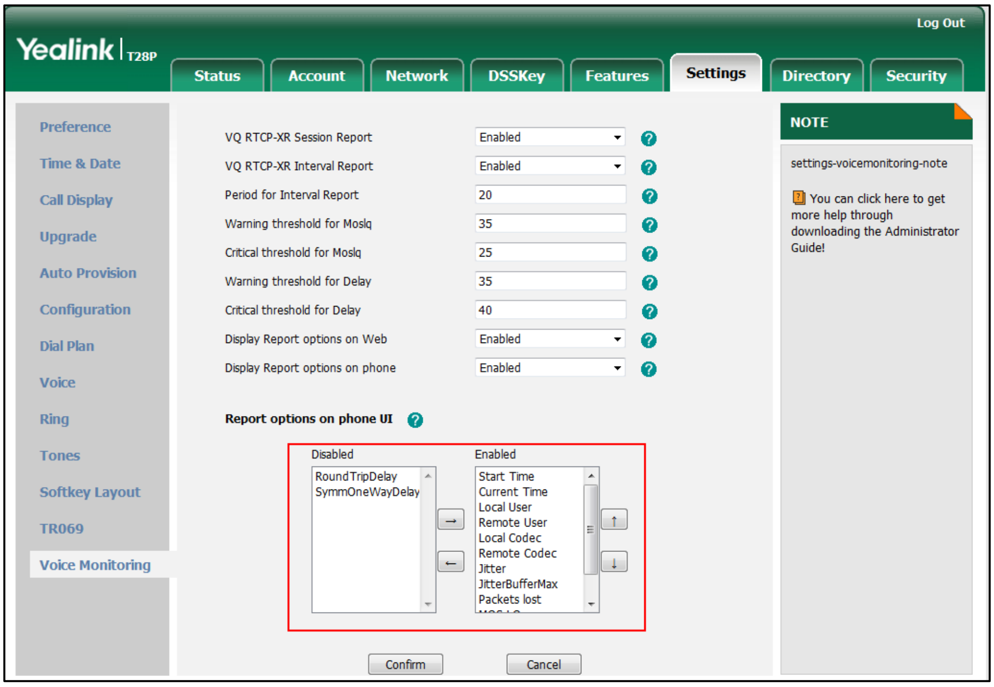
The RTP status will appear on the phone user interface at the path: **Menu**->**Status**->**More**….

To configure the options of the RTP status displayed on the LCD screen via web user interface:

1. Click on **Settings**->**Voice Monitoring.**
2. In the **Report options on phone UI** block, select the desired list from the **Disabled**

column and then click [→].

The selected list appears in the **Enabled** column.



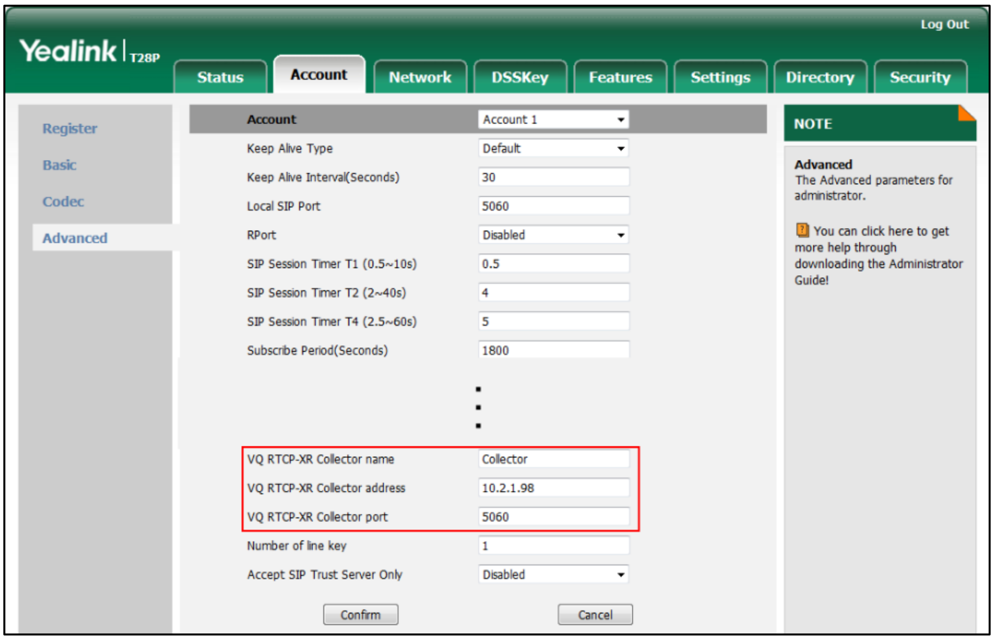
3. Repeat step 2 to add more items to the **Enabled** column.
4. To remove an item from the **Enabled** column, select the desired item and then click [←].
5. To adjust the display order of enabled items, select the desired item and then click [↑] or [↓].

   The LCD screen will display the item(s) in the adjusted order.
6. Click **Confirm** to accept the change.

To configure the central report collector via web user interface:

1. Click on **Account->Advanced.**
2. Enter the host name of the central report collector in the **VQ RTCP-XR Collector name** field.
3. Enter the IP address of the central report collector in the **VQ RTCP-XR Collector address** field.

4. Enter the port of the central report collector in the **VQ RTCP-XR Collector port** field.



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

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:

- **Class Selector PHB** -- backwards compatible with IP precedence. Class Selector code points are of the form “xxx000”. The first three bits are the IP precedence bits. These class selector PHBs retain almost the same forwarding behavior as nodes that implement IP precedence-based classification and forwarding.
- **Expedited Forwarding PHB** -- the key ingredient in DiffServ model for providing a low-loss, low-latency, low-jitter and assured bandwidth service.
- **Assured Forwarding PHB** -- defines a method by which BAs (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. IP phones support the DiffServ model of QoS.

Voice QoS

In order to make VoIP transmissions intelligible to receivers, voice packets should not be dropped, excessively delayed, 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 phones should be configured with a high transmission priority.

DSCPs for voice and SIP packets can be specified respectively.

Procedure

QoS can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure the DSCPs for voice packets and SIP packets. **Parameters:** network.qos.rtptos network.qos.signaltos
Local	Web User Interface	Configure the DSCPs for voice packets and SIP packets. **Navigate to**: http://<phoneIPAddress>/servlet?p=network-adv&q=load

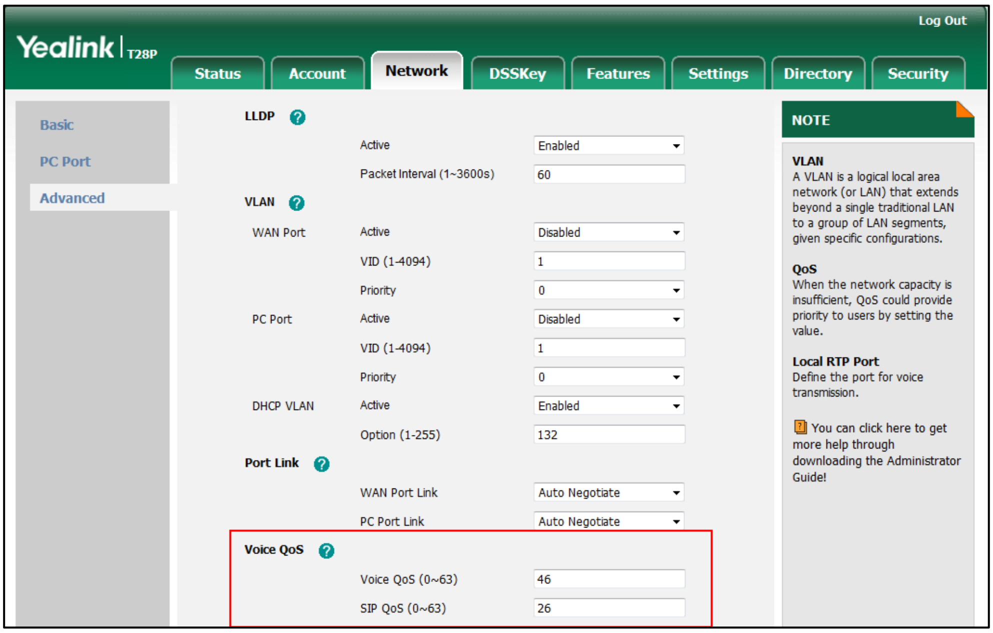
Details of Configuration Parameters:

Parameters	Permitted Values	Default
network.qos.rtptos	**Integer from 0 to 63**	**46**
Description: Configures the DSCP for voice packets. The default DSCP value for RTP packets is 46 (Expedited Forwarding). **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->Voice QoS (0~63) **Phone User Interface:** None		
network.qos.signaltos	**Integer from 0 to 63**	**26**
Description: Configures the DSCP for SIP packets. The default DSCP value for SIP packets is 26 (Assured Forwarding). **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.		

Parameters	Permitted Values	Default
Web User Interface: Network->Advanced->SIP QoS (0~63) **Phone User Interface:** 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.

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. But in the VoIP environment, NAT breaks end-to-end connectivity.

NAT Traversal

NAT traversal is a general term for techniques that establish and maintain IP connections traversing NAT gateways, typically required for client-to-client networking applications, especially for VoIP deployments. STUN is one of the NAT traversal techniques supported by IP phones.

STUN (Simple Traversal of UDP over NATs)

STUN is a network protocol, used in NAT traversal for applications of real-time voice, video, messaging, and other interactive IP communications. The STUN protocol allows applications to operate behind a NAT to discover the presence of the network address translator, and to obtain the mapped (public) IP address and port number that the NAT has allocated for the UDP connections to remote parties. The protocol requires assistance from a third-party network server (STUN server) usually located on public Internet. The IP phone can be configured to act as a STUN client, 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.

The NAT traversal and STUN server are configurable on a per-line basis.

Procedure

NAT traversal and STUN server can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure NAT traversal and STUN server on the IP phone. **Parameters:** account.X.nat.nat_traversal account.X.nat.stun_server account.X.nat.stun_port
Local	Web User Interface	Configure NAT traversal and STUN server on the IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-register&q=load&acc=0

Details of Configuration Parameters:

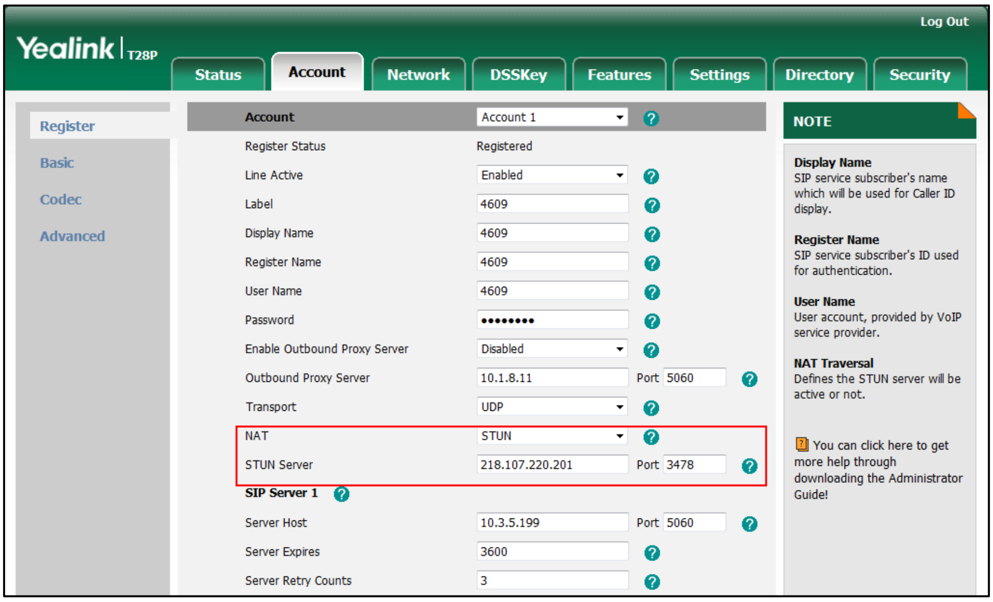
Parameters	Permitted Values	Default
account.X.nat.nat_traversal	**0 or 1**	**0**
Description: Enables or disables the NAT traversal for account X. **0**-Disabled		

Parameters	Permitted Values	Default
1-Enabled X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Web User Interface:** Account->Register->NAT **Phone User Interface:** None		
account.X.nat.stun_server	**IP address or domain name**	**Blank**
Description: Configures the IP address or the domain name of the STUN server for account X. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Example:** account.1.nat.stun_server = 218.107.220.201 **Web User Interface:** Account->Register->STUN Server **Phone User Interface:** None		
account.X.nat.stun_port	**Integer from 1024 to 65000**	**3478**
Description: Configures the port of the STUN server for account X. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Example:** account.1.nat.stun_port = 3478 **Web User Interface:** Account->Register->STUN Server->Port **Phone User Interface:**		

Parameters	Permitted Values	Default
None		

To configure NAT traversal and STUN server via web user interface:

1. Click on **Account**->**Register**.
2. Select the desired account from the pull-down list of **Account**.
3. Select **STUN** from the pull-down list of **NAT**.
4. Enter the IP address or the domain name of the STUN server in the **STUN Server** field.



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

802.1X Authentication

IEEE 802.1X authentication is an IEEE standard for Port-based Network Access Control (PNAC), part of the IEEE 802.1 group of networking protocols. It offers an authentication mechanism for devices to connect/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 phone that wishes to attach to the LAN or WLAN. With 802.1X port-based authentication, the IP phone provides credentials, such as user name and password, for the authenticator, and then the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the IP phone is allowed to access resources located on the protected side of the network.

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

For more information on 802.1X authentication, refer to *Yealink 802.1X Authentication*, available online:

http://www.yealink.com/DocumentDownload.aspx?CateId=142&flag=142.

Procedure

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

Configuration File	<y0000000000xx>.cfg	Configure the 802.1X authentication. **Parameters:** network.802_1x.mode network.802_1x.identity network.802_1x.md5_password network.802_1x.root_cert_url network.802_1x.client_cert_url
Local	Web User Interface	Configure the 802.1X authentication. **Navigate to:** http://<phoneIPAddress>/servlet?p=network-adv&q=load
	Phone User Interface	Configure the 802.1X authentication.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
network.802_1x.mode	**0, 1, 2, 3, 4, 5 or 6**	**0**
Description: Configures the 802.1x authentication method. **0**-Disabled **1**-EAP-MD5 **2**-EAP-TLS **3**-EAP-PEAP/MSCHAPv2 **4**-EAP-TTLS/EAP-MSCHAPv2 **5**-EAP-PEAP/GTC **6**-EAP-TTLS/EAP-GTC **Note:** If you change this parameter, the IP phone will reboot to make the change		

Parameters	Permitted Values	Default
take effect. **Web User Interface:** Network->Advanced->802.1x->802.1x Mode **Phone User Interface:** Menu->Settings->Advanced Settings (default password: admin) ->Network->802.1x Settings->802.1x Mode		
network.802_1x.identity	**String within 32 characters**	**Blank**
Description: Configures the user name for 802.1x authentication. **Example:** network.802_1x.identity = admin **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->802.1x->Identity **Phone User Interface:** Menu->Settings->Advanced Settings (default password: admin) ->Network->802.1x Settings->Identity		
network.802_1x.md5_password	**String within 32 characters**	**Blank**
Description: Configures the password for 802.1x authentication. **Example:** network.802_1x.md5_password = admin123 **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. It is required for all 802.1x authentication methods except EAP-TLS. **Web User Interface:** Network->Advanced->802.1x->MD5 Password **Phone User Interface:** Menu->Settings->Advanced Settings (default password: admin) ->Network->802.1x Settings->MD5 Password		
network.802_1x.root_cert_url	**URL within 511 characters**	**Blank**

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td colspan="3">Description:
Configures the access URL of the CA certificate when the 802.1x authentication method is configured as EAP-TLS, EAP-PEAP/MSCHAPv2, EAP-TTLS/EAP-MSCHAPV2, EAP-PEAP/GTC or EAP-TTLS/EAP-GTC.
Example :
network.802_1x.root_cert_url = http://192.168.1.10/ca.pem
Note: If you change this parameter, the IP phone will reboot to make the change take effect. It is only applicable to EAP-TLS, EAP-PEAP/MSCHAPv2, EAP-TTLS/EAP-MSCHAPV2, EAP-PEAP/GTC and EAP-TTLS/EAP-GTC protocols. The format of the certificate must be *.pem, *.crt, *.cer or *.der.
Web User Interface:
Network->Advanced->802.1x->CA Certificates
Phone User Interface:
None</td></tr>
<tr><td>network.802_1x.client_cert_url</td><td>URL within 511 characters</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the access URL of the device certificate when the 802.1x authentication method is configured as EAP-TLS.
Example:
network.802_1x.client_cert_url = http://192.168.1.10/client.pem
Note: If you change this parameter, the IP phone will reboot to make the change take effect. It is only applicable to the EAP-TLS protocol. The format of the certificate must be *.pem or *.cer.
Web User Interface:
Network->Advanced->802.1x->Device Certificates
Phone User Interface:
None</td></tr>
</table>

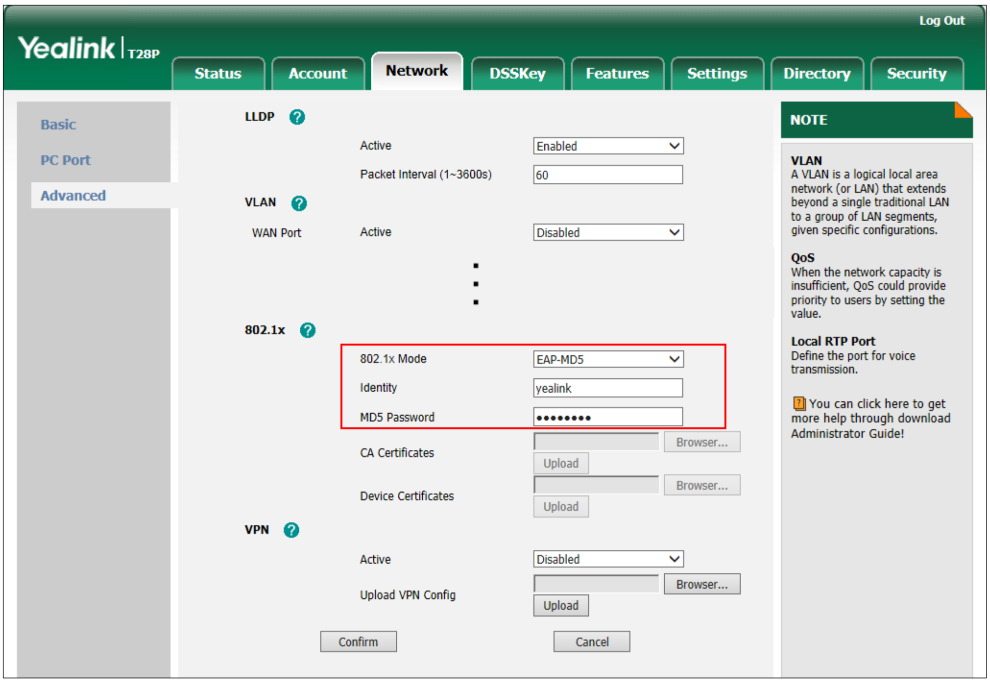
To configure the 802.1X authentication via web user interface:

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 user name for authentication in the **Identity** field.

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



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

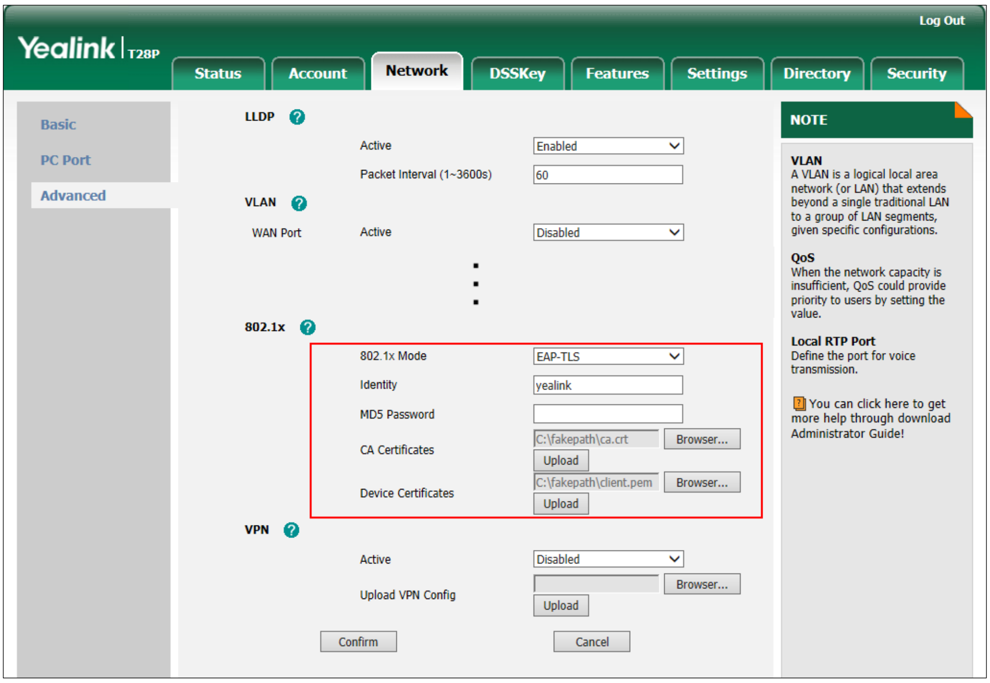
1) Enter the user name for authentication in the **Identity** field.

2) Leave the **MD5 Password** field blank.

3) In the **CA Certificates** field, click **Browse** to 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.



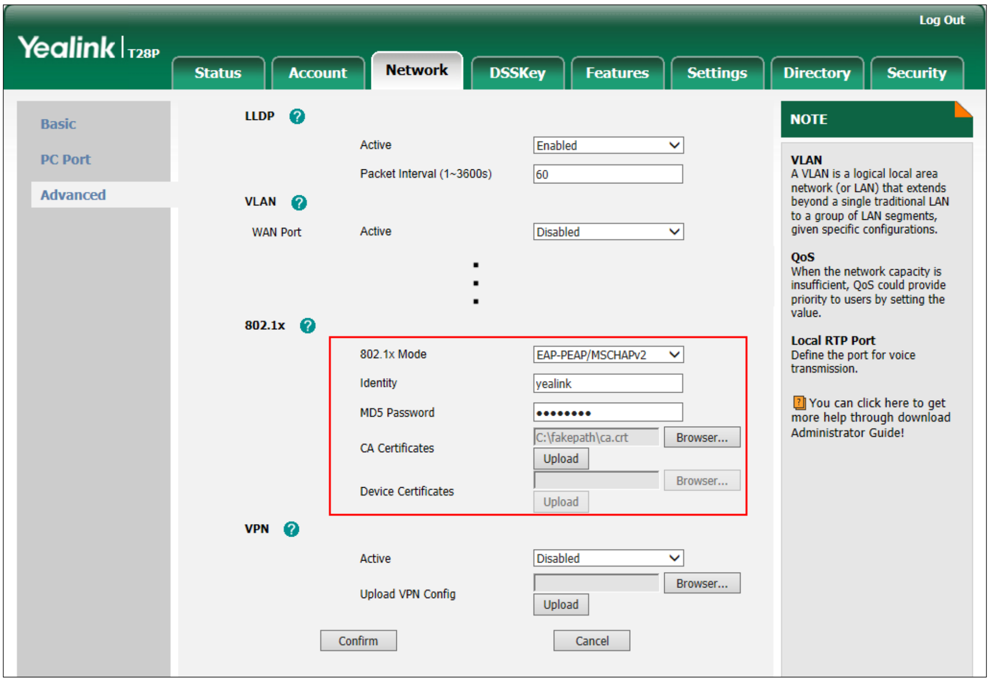
c) If you select **EAP-PEAP/MSCHAPv2**:

1) Enter the user name for authentication in the **Identity** field.

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

3) In the **CA Certificates** field, click **Browse** to select the desired CA certificate (*.pem, *.crt, *.cer or *.der) from your local system.

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



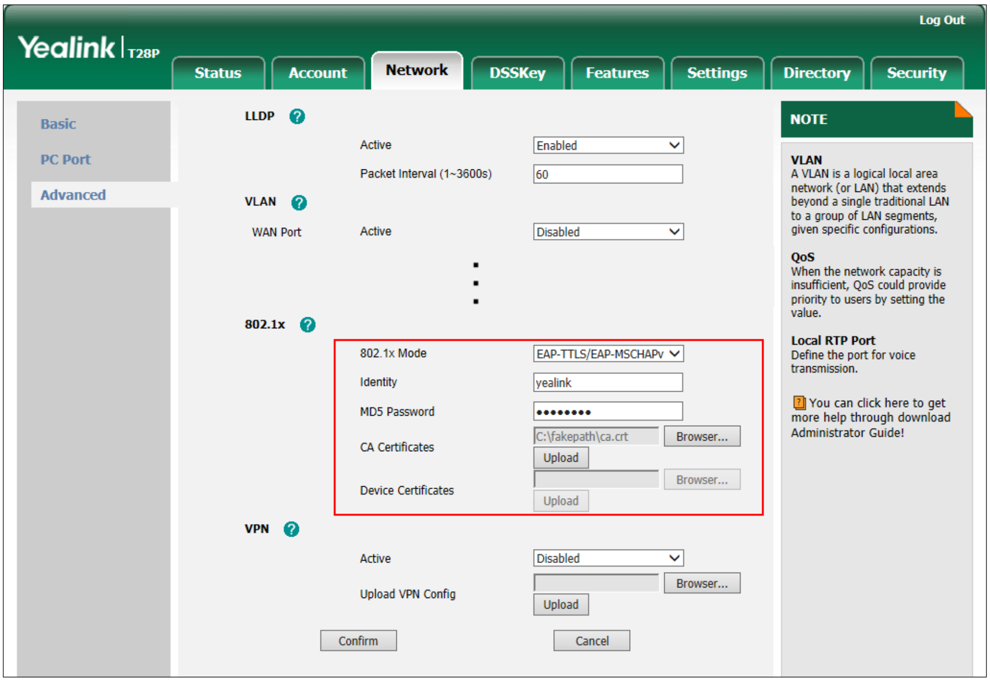
d) If you select **EAP-TTLS/EAP-MSCHAPv2**:

1) Enter the user name for authentication in the **Identity** field.

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

3) In the **CA Certificates** field, click **Browse** to select the desired CA certificate (*.pem, *.crt, *.cer or *.der) from your local system.

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

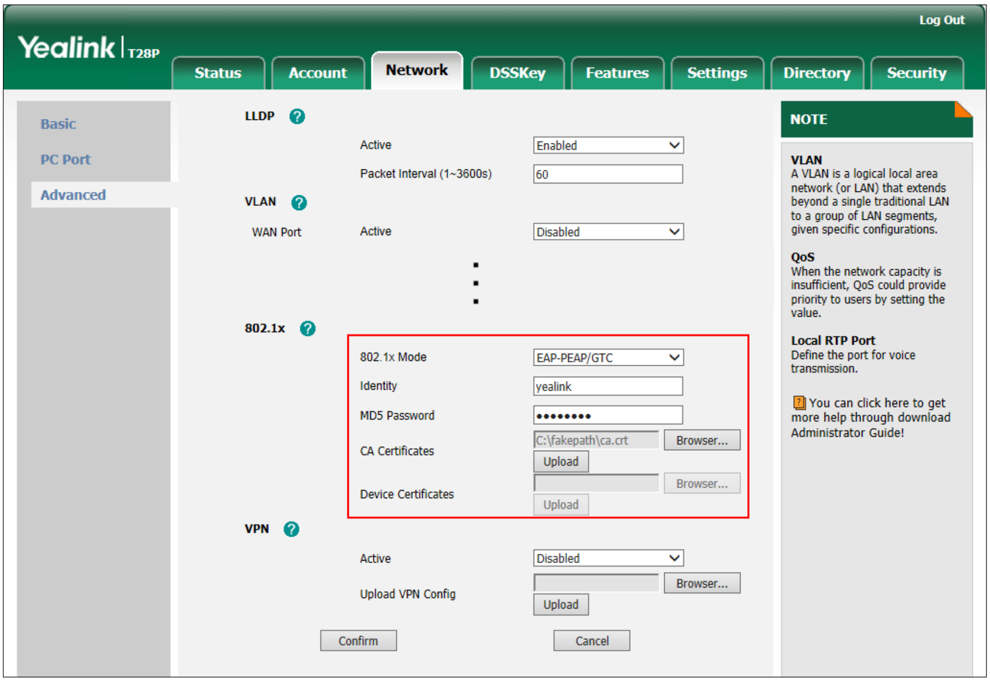


e) If you select **EAP-PEAP/GTC**:

1) Enter the user name for authentication in the **Identity** field.

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

3) In the **CA Certificates** field, click **Browse** to select the desired CA certificate (*.pem, *.crt, *.cer or *.der) from your local system.



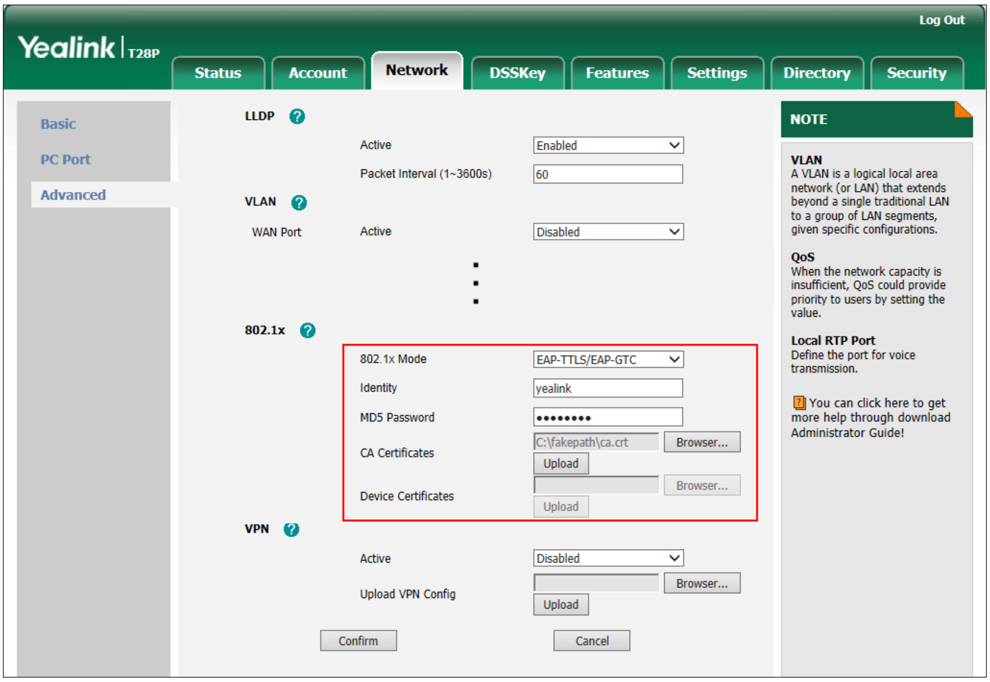
4) Click **Upload** to upload the certificate.

f) If you select **EAP-TTLS/EAP-GTC**:

1) Enter the user name for authentication in the **Identity** field.

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

3) In the **CA Certificates** field, click **Browse** to select the desired CA certificate (*.pem, *.crt, *.cer or *.der) from your local system.



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

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

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

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

To configure the 802.1X authentication via phone user interface after:

1. Press **Menu**->**Settings**->**Advanced Settings** (default password: admin) ->**Network**->**802.1x Settings**.

2. Press or , or the **Switch** soft key to select the desired value from the **802.1x Mode** field.

   a) If you select **EAP-MD5**:

   1) Enter the user name for authentication in the **Identity** field.

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

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

   1) Enter the user name for authentication in the **Identity** field.

   2) Leave the **MD5 Password** field blank.

   c) If you select **EAP-PEAP/MSCHAPv2**:

   1) Enter the user name for authentication in the **Identity** field.

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

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

   1) Enter the user name for authentication in the **Identity** field.

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

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

   1) Enter the user name for authentication in the **Identity** field.

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

   f) If you select **EAP-TTLS/EAP-GTC**:

   1) Enter the user name for authentication in the **Identity** field.

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

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

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

TR-069 Device Management

TR-069 is a technical specification defined by the Broadband Forum, which defines a mechanism that encompasses secure auto-configuration of a CPE (Customer-Premises Equipment), and incorporates other CPE management functions into a common framework. TR-069 uses common transport mechanisms (HTTP and HTTPS) for communication between CPE and ACS (Auto Configuration Servers). The HTTP(S) messages contain XML-RPC methods defined in the standard for configuration and management of the CPE.

TR-069 is intended to support a variety of functionalities to manage a collection of CPEs, including the following primary capabilities:

- Auto-configuration and dynamic service provisioning
- Software or firmware image management
- Status and performance monitoring
- Diagnostics

The following table provides a description of RPC methods supported by IP phones.

RPC Method	Description
GetRPCMethods	This method is used to discover the set of methods supported by the CPE.
SetParameterValues	This method is used to modify the value of one or more CPE parameters.
GetParameterValues	This method is used to obtain the value of one or more CPE parameters.
GetParameterNames	This method is used to discover the parameters accessible on a particular CPE.
GetParameterAttributes	This method is used to read the attributes associated with one or more CPE parameters.
SetParameterAttributes	This method is used to modify attributes associated with one or more CPE parameters.
Reboot	This method causes the CPE to reboot.
Download	This method is used to cause the CPE to download a specified file from the designated location. File types supported by IP phones are: • Firmware Image • Configuration File
Upload	This method is used to cause the CPE to upload a specified file to the designated location. File types supported by IP phones are: • Configuration File • Log File
ScheduleInform	This method is used to request the CPE to schedule a one-time Inform method call (separate from its periodic Inform method calls) sometime in the future.

RPC Method	Description
FactoryReset	This method resets the CPE to its factory default state.
TransferComplete	This method informs the ACS of the completion (either successful or unsuccessful) of a file transfer initiated by an earlier Download or Upload method call.
AddObject	This method is used to add a new instance of an object defined on the CPE.
DeleteObject	This method is used to remove a particular instance of an object.

For more information on TR-069, refer to *Yealink TR-069 Technote*, available online: http://www.yealink.com/DocumentDownload.aspx?CateId=142&flag=142.

Procedure

TR-069 can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure TR-069 feature. **Parameters:** managementserver.enable managementserver.username managementserver.password managementserver.url managementserver.connection_request_username managementserver.connection_request_password managementserver.periodic_inform_enable managementserver.periodic_inform_interval
Local	Web User Interface	Configure TR-069 feature. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-preference&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
managementserver.enable	**0 or 1**	**0**
Description: Enables or disables TR-069 feature.		

Parameters	Permitted Values	Default
0-Disabled **1**-Enabled **Web User Interface:** Settings->TR069->Enable TR069 **Phone User Interface:** None		
managementserver.username	String within 128 characters	Blank
Description: Configures the user name for the IP phone to authenticate with the ACS (Auto Configuration Servers). This string is set to the empty string if no authentication is required. **Example:** managementserver.username = user1 **Web User Interface:** Settings->TR069->ACS Username **Phone User Interface:** None		
managementserver.password	String within 64 characters	Blank
Description: Configures the password for the IP phone to authenticate with the ACS (Auto Configuration Servers). This string is set to the empty string if no authentication is required. **Example:** managementserver.password = pwd123 **Web User Interface:** Settings->TR069->ACS Password **Phone User Interface:** None		
managementserver.url	URL within 511 characters	Blank
Description:		

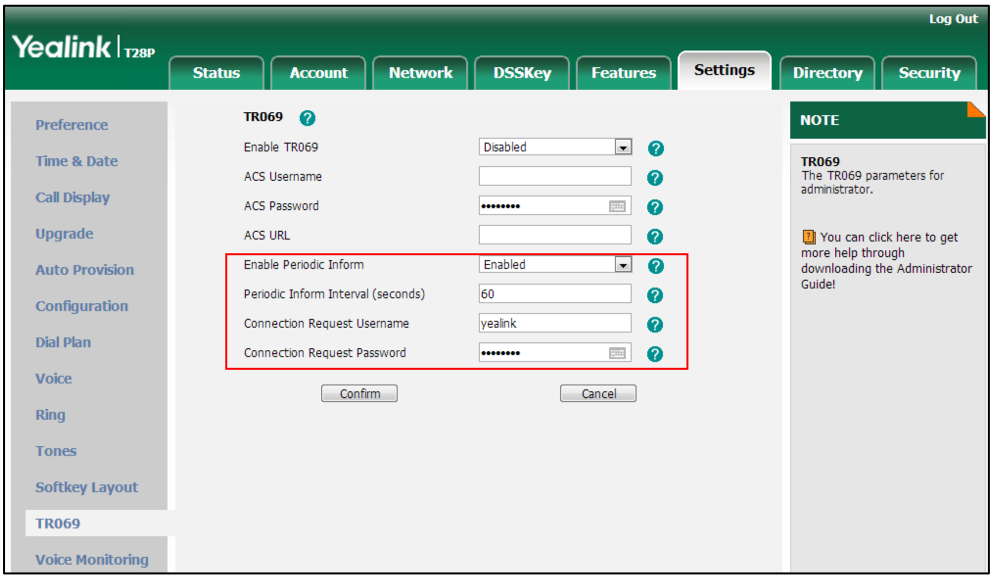
Parameters	Permitted Values	Default
Configures the access URL of the ACS (Auto Configuration Servers). **Example:** managementserver.url = http://192.168.1.20/acs/ **Web User Interface:** Settings->TR069->ACS URL **Phone User Interface:** None		
managementserver.connection_request_username	**String within 128 characters**	**Blank**
Description: Configures the user name for the IP phone to authenticate the incoming connection requests. **Example:** managementserver.connection_request_username = accuser **Web User Interface:** Settings->TR069->Connection Request Username **Phone User Interface:** None		
managementserver.connection_request_password	**String within 64 characters**	**Blank**
Description: Configures the password for the IP phone to authenticate the incoming connection requests. **Example:** managementserver.connection_request_password = acspwd **Web User Interface:** Settings->TR069->Connection Request Password **Phone User Interface:** None		
managementserver.periodic_inform_enable	**0 or 1**	**1**
Description: Enables or disables the IP phone to periodically report its configuration information		

Parameters	Permitted Values	Default
to the ACS (Auto Configuration Servers). **0**-Disabled **1**-Enabled **Web User Interface:** Settings->TR069->Enable Periodic Inform **Phone User Interface:** None		
managementserver.periodic_inform_interval	**Integer from 5 to 4294967295**	**60**
Description: Configures the interval (in seconds) for the IP phone to report its configuration to the ACS (Auto Configuration Servers). **Web User Interface:** Settings->TR069->Periodic Inform Interval (seconds) **Phone User Interface:** None		

To configure TR-069 via web user interface:

1. Click on **Settings**->**TR069**.
2. Select **Enabled** from the pull-down list of **Enable TR069**.
3. Enter the user name and password authenticated by the ACS in the **ACS Username** and **ACS Password** fields.
4. Enter the URL of the ACS in the **ACS URL** field.
5. Select the desired value from the pull-down list of **Enable Periodic Inform**.
6. Enter the desired time in the **Periodic Inform Interval (seconds)** field.

7. Enter the user name and password authenticated by the IP phone in the **Connection Request Username** and **Connection Request Password** fields.



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

IPv6 Support

IPv6 is the next generation network layer protocol, designed as a replacement for the current IPv4 protocol. IPv6 is developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. IPv6 uses a 128-bit address, consisting of eight groups of four hexadecimal digits separated by colons. VoIP network based on IPv6 can ensure QoS, a set of service requirements to deliver performance guarantee while transporting traffic over the network.

IPv6 Address Assignment Method

Supported IPv6 address assignment methods:

- **Manual Assignment:** An IPv6 address and other configuration parameters (e.g., DNS server) for the IP phone can be statically configured by an administrator.
- **Stateless Address Autoconfiguration (SLAAC):** SLAAC is one of the most convenient methods to assign IP addresses to IPv6 nodes. SLAAC requires no manual configuration of the IP phone, minimal (if any) configuration of routers, and no additional servers. To use IPv6 SLAAC, the IP phone must be connected to a network with at least one IPv6 router connected. This router is configured by the network administrator and sends out Router Advertisement announcements onto the link. These announcements can allow the on-link connected IP phone to configure itself with IPv6 address, as specified in RFC 4862.

Procedure

IPv6 can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure the IPv6 address parameters. **Parameters**: 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. **Parameters:** network.ipv6_primary_dns network.ipv6_secondary_dns
	<y0000000000xx>.cfg	Configure the IPv6 static DNS. **Parameter:** network.ipv6_static_dns_enable
Local	Web User Interface	Configure the IPv6 address parameters. Configure the IPv6 static DNS. **Navigate to**: http://<phoneIPAddress>/servlet?p=network&q=load
	Phone User Interface	Configure the IPv6 address parameters. Configure the IPv6 static DNS.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
network.ip_address_mode	**0, 1 or 2**	**0**
Description: Configures the IP address mode. **0**-IPv4		

Parameters	Permitted Values	Default
1-IPv6 **2**-IPv4&IPv6 **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->Internet Port->Mode (IPv4/IPv6) **Phone User Interface:** Menu->Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IP Mode		
network.ipv6_internet_port.type	**0 or 1**	**0**
Description: Configures the Internet (WAN) port type for IPv6 when the IP address mode is configured as IPv6 or IPv4&IPv6. **0**-DHCP **1**-Static IP Address **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv6 Config **Phone User Interface:** Menu->Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv6		
network.ipv6_static_dns_enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to use manually configured static IPv6 DNS when Internet (WAN) port type for IPv6 is configured as DHCP. **0**-Disabled **1**-Enabled **Note**: If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv6 Config->IPv6 Static DNS **Phone User Interface:**		

Parameters	Permitted Values	Default
None		
network.ipv6_internet_port.ip	**IPv6 address**	**Blank**
Description: Configures the IPv6 address when the IP address mode is configured as IPv6 or IPv4&IPv6, and the Internet (WAN) port type for IPv6 is configured as Static IP Address. **Example:** network.ipv6_internet_port.ip = 2026:1234:1:1:215:65ff:fe1f:caa **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv6 Config->Static IP Address->IP Address **Phone User Interface:** Menu->Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv6->Static IPv6 Client->IPv6		
network.ipv6_prefix	**Integer from 0 to 128**	**64**
Description: Configures the IPv6 prefix when the IP address mode is configured as IPv6 or IPv4&IPv6, and the Internet (WAN) port type for IPv6 is configured as Static IP Address. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv6 Config->Static IP Address->IPv6 Prefix (0~128) **Phone User Interface:** Menu->Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv6->Static IPv6 Client->IPv6 Prefix		
network.ipv6_internet_port.gateway	**IPv6 address**	**Blank**
Description: Configures the IPv6 default gateway when the IP address mode is configured as IPv6 or IPv4&IPv6, and the Internet (WAN) port type for IPv6 is configured as Static IP Address. **Example:**		

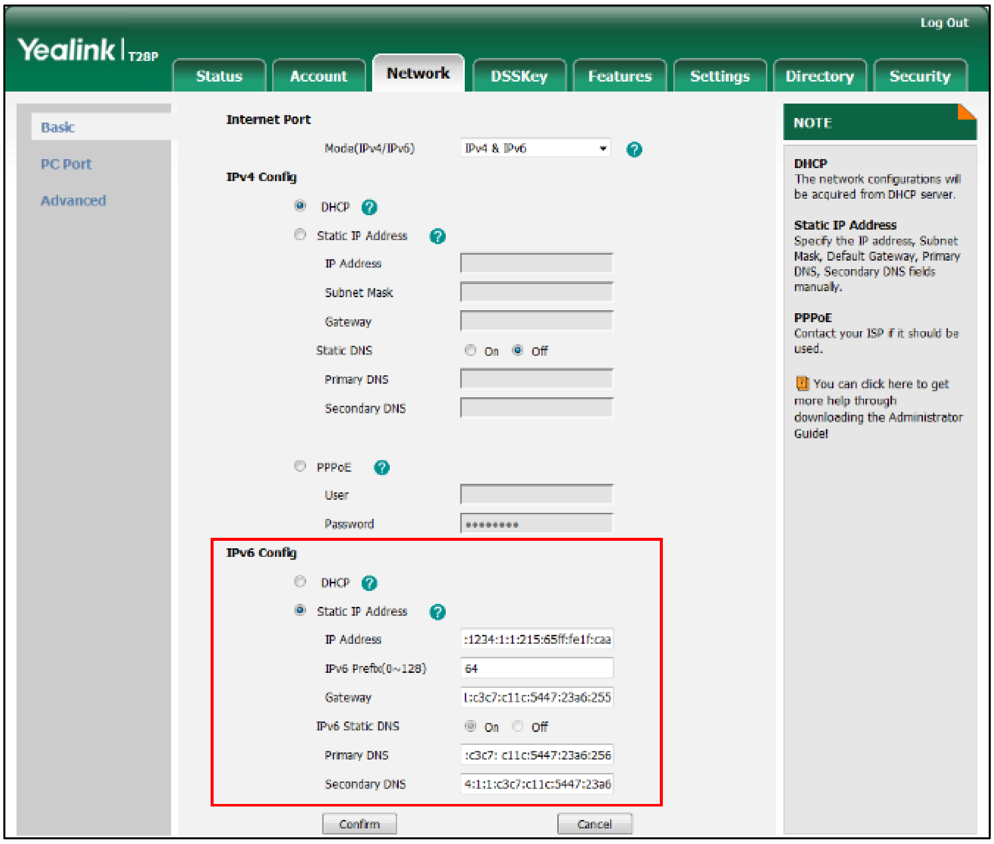
Parameters	Permitted Values	Default
network.ipv6_internet_port.gateway = 3036:1:1:c3c7:c11c:5447:23a6:255 **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv6 Config->Static IP Address->Gateway **Phone User Interface:** Menu->Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv6->Static IPv6 Client->IPv6 Gateway		
network.ipv6_primary_dns	**IPv6 address**	**Blank**
Description: Configures the primary IPv6 DNS server when the IP address mode is configured as IPv6 or IPv4&IPv6, and the Internet (WAN) port type for IPv6 is configured as Static IP Address, or and the Internet (WAN) port type for IPv6 is configured as DHCP and Staic DNS is configured as Enabled. **Example:** network.ipv6_primary_dns = 3036:1:1:c3c7: c11c:5447:23a6:256 **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv6 Config->Static IP Address->Primary DNS **Phone User Interface:** Menu->Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv6->Static IPv6 Client->IPv6 Pri.DNS **Or** Menu->Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv6->DHCP IPv6 Client->Staic DNS(Enabled) ->IPv6 Pri.DNS		
network.ipv6_secondary_dns	**IPv6 address**	**Blank**
Description: Configures the secondary IPv6 DNS server when the IP address mode is configured as IPv6 or IPv4&IPv6, and the Internet (WAN) port type for IPv6 is configured as Static IP Address, or and the Internet (WAN) port type for IPv6 is configured as DHCP and Staic DNS is configured as Enabled. **Example:** network.ipv6_secondary_dns = 2026:1234:1:1:c3c7:c11c:5447:23a6		

Parameters	Permitted Values	Default
Note: If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv6 Config->Static IP Address->Secondary DNS **Phone User Interface:** Menu->Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv6->Static IPv6 Client->IPv6 Sec.DNS **Or** Menu->Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv6->DHCP IPv6 Client->Staic DNS(Enabled) ->IPv6 Sec.DNS		

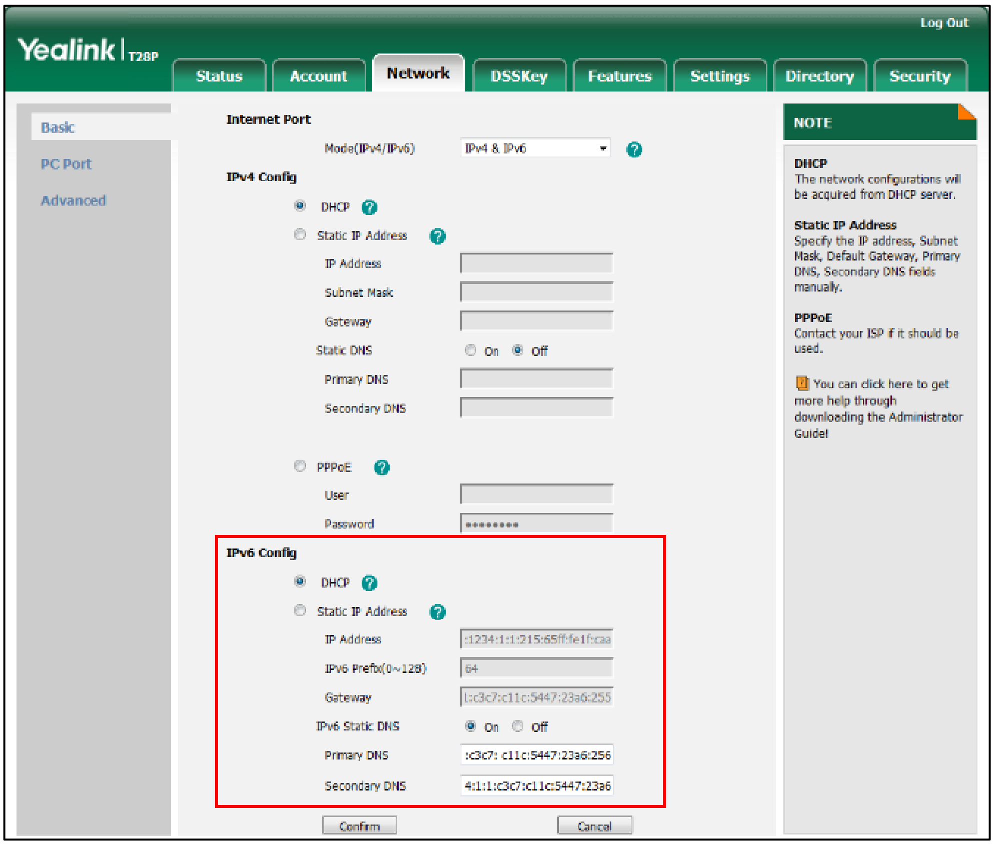
To configure IPv6 address assignment method via web user interface:

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, do one of the following.

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



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



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

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

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

To configure IPv6 address assignment method via phone user interface:

1. Press **Menu**->**Settings**->**Advanced Settings** (default password: admin) ->**Network**->**WAN Port**.
2. Press or to select **IPv4&IPv6** or **IPv6** from the **IP Mode** field.
3. Press or to highlight **IPv6** and press the **Enter** soft key.
4. Press or to select the desired IPv6 address assignment method.

   If you select the **Static IPv6 Client**, configure the IPv6 address and other network parameters in the corresponding fields.

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

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

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

1. Press **Menu**->**Settings**->**Advanced Settings** (default password: admin) ->**Network**->**WAN Port**->**IPv6**->**DHCPv6 IP Client**.

2. Press ◀ or ▶ , or the **Switch** soft key to select **Enabled** from the **Static DNS** field.
3. Enter the desired values in the **IPv6 Pri.DNS** and **IPv6 Sec.DNS** fields respectively.
4. Press the **Save** soft key to accept the change.

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

Configuring Audio Features

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

- Headset Prior
- Dual Headset
- Audio Codecs
- Acoustic Clarity Technology

Headset Prior

Headset prior allows users to use headset preferentially if a headset is physically connected to the IP phone. This feature is especially useful for permanent or full-time headset users.

Procedure

Headset prior can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure headset prior. **Parameter:** features.headset_prior
Local	Web User Interface	Configure headset prior. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-general&q=load

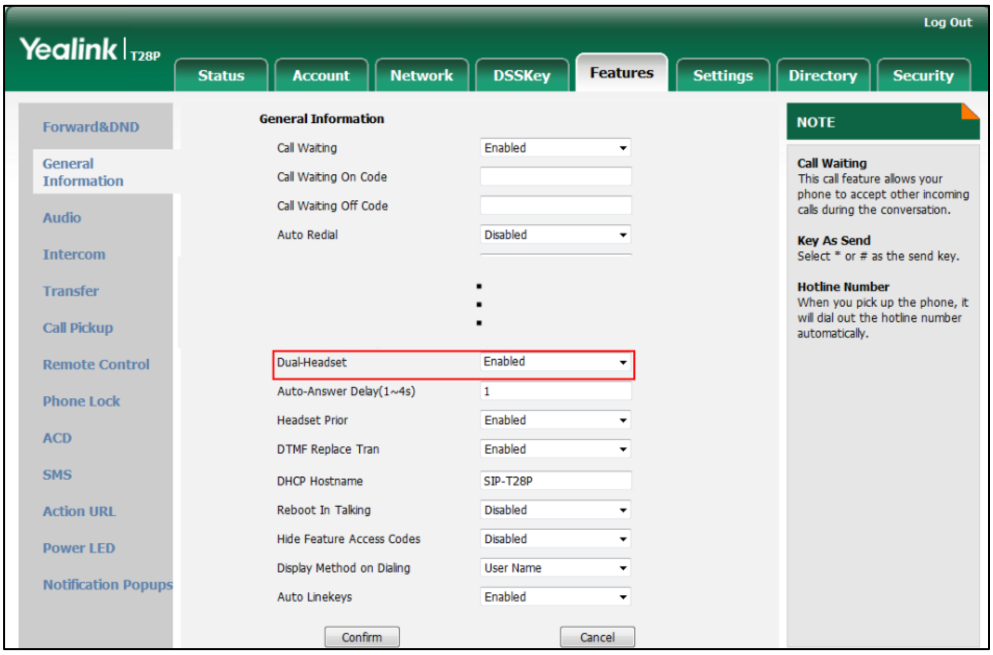
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
features.headset_prior	**0 or 1**	**0**
Description: Enables or disables headset prior feature. **0**-Disabled **1**-Enabled If it is set to 1 (enabled), a user needs to press the HEADSET key to activate the		

Parameter	Permitted Values	Default
headset mode. The headset mode will not be deactivated until the user presses the HEADSET key again. **Web User Interface:** Features->General Information->Headset Prior **Phone User Interface:** None		

To configure headset prior via web user interface:

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



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

Dual Headset

Dual headset allows users to use two headsets on one IP phone. To use this feature, users need to physically connect two headsets to the headset and handset jacks respectively. Once the IP phone connects to a call, the user with the headset connected to the headset jack has full-duplex capabilities, while the user with the headset connected to the handset jack is only able to listen.

Procedure

Dual headset can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure dual headset. **Parameter:** features.headset_training
Local	Web User Interface	Configure dual headset. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

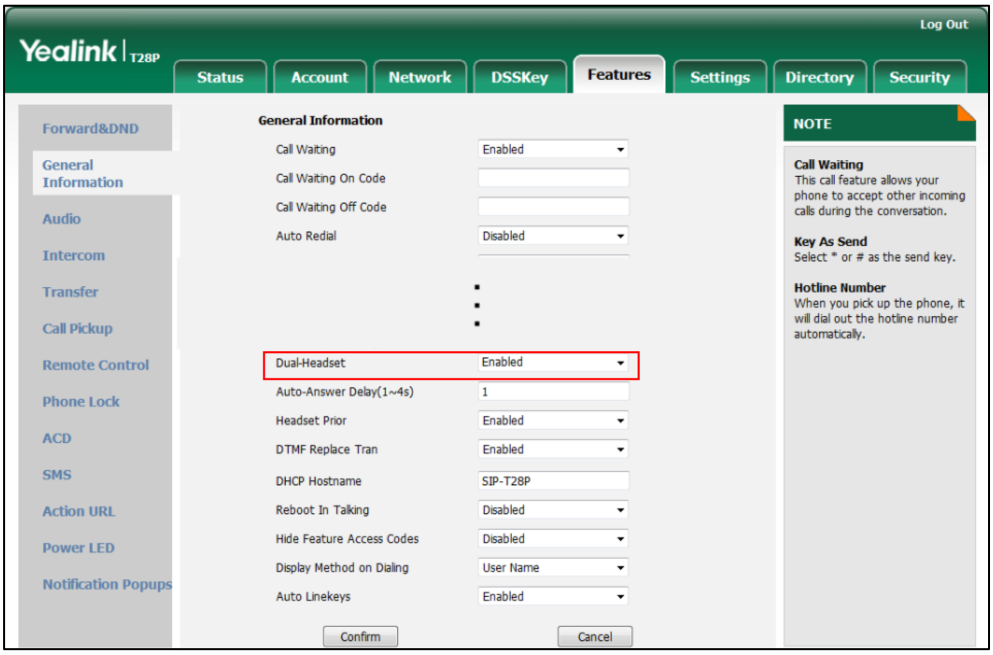
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
features.headset_training	**0 or 1**	**0**
Description: Enables or disables dual headset feature. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), users can use two headsets on one phone. When the IP phone joins in a call, the users with the headset connected to the headset jack have a full-duplex conversation, while the users with the headset connected to the handset jack are only allowed to listen to. **Web User Interface:** Features->General Information->Dual-Headset **Phone User Interface:** None		

To configure dual headset via web user interface:

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

2. Select the desired value from the pull-down list of **Dual-Headset**.



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

Audio Codecs

CODEC is an abbreviation of COmpress-DECompress, capable of coding or decoding a digital data stream or signal by implementing an algorithm. The object of the algorithm is to represent the high-fidelity audio signal with minimum number of bits while retaining the quality. This can effectively reduce the frame size and the bandwidth required for audio transmission.

The following table lists the audio codecs supported by each phone model:

Phone Model	Supported Audio Codecs	Default Audio Codecs
SIP-T28P/T26P/T22P/T20P	G722, PCMA, PCMU, G722, G723_53, G723_63, G726-16, G726-24, G726-32, G726-40, iLBC	G722, PCMA, PCMU, G729

The following table summarizes the supported audio codecs on IP phones:

Codec	Algorithm	Reference	Bit Rate	Sample	Packetization
G722	G.722	RFC 3551	64 Kbps	16 Ksps	20ms
PCMA	G.711	RFC 3551	64 Kbps	8 Ksps	20ms
PCMU	G.711	RFC 3551	64 Kbps	8 Ksps	20ms
G729	G.729	RFC 3551	8 Kbps	8 Ksps	20ms
G726-16	G.726	RFC 3551	16 Kbps	8 Ksps	20ms
G726-24	G.726	RFC 3551	24 Kbps	8 Ksps	20ms
G726-32	G.726	RFC 3551	32 Kbps	8 Ksps	20ms
G726-40	G.726	RFC 3551	40 Kbps	8 Ksps	20ms
G723_53/ G723_63	G.723.1	RFC 3951	5.3kbps 6.3kbps	8 Ksps	30ms
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 Web User Interface	3	8
G729	Configuration Files	4	18

Codec	Configuration Methods	Priority	RTPmap
	Web User Interface		
G723_53	Configuration Files Web User Interface	0	4
G723_63	Configuration Files Web User Interface	0	4
G726-16	Configuration Files Web User Interface	0	103
G726-24	Configuration Files Web User Interface	0	104
G726-32	Configuration Files Web User Interface	0	102
G726-40	Configuration Files Web User Interface	0	105
iLBC	Configuration Files Web User Interface	0	106

Procedure

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

Configuration File	<MAC>.cfg	Configure the codecs to use on a per-line basis. **Parameters:** account.X.codec.Y.enable account.X.codec.Y.payload_type Configure the priority and rtpmap for the enabled codec. **Parameters:** account.X.codec.Y.priority account.X.codec.Y.rtpmap Configure the ptime. **Parameter:** account.X.ptime
Local	Web User Interface	Configure the codecs to use and adjust the priority of the enabled codecs on a per-line basis. Configure the ptime.

		Navigate to: http://<phoneIPAddress>/servlet?p=account-codec&q=load&acc=0

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.codec.Y.enable (Y ranges from 1 to 11)	0 or 1	Refer to the following content
Description: Enables or disables the specified codec for account X. **0**-Disabled **1**-Enabled X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Default:** 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; When Y=9, the default value is 0; When Y=10, the default value is 0; When Y=11, the default value is 0. **Default:** 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.		

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td colspan="3">Web User Interface:
Account->Codec
Phone User Interface:
None</td></tr>
<tr><td>account.X.codec.Y.payload_type
(Y ranges from 1 to 11)</td><td>Refer to the following content</td><td>Refer to the following content</td></tr>
<tr><td colspan="3">Description:
Configures the codec for account X.
X ranges from 1 to 6 (for SIP-T28P).
X ranges from 1 to 3 (for SIP-T26P/T22P).
X ranges from 1 to 2 (for SIP-T20P).
Permitted Values:
PCMU, PCMA, G729, G722, G723_53, G723_63, G726-16, G726-24, G726-32, G726-40, iLBC
For SIP-T20P/T22P/T26P/T28P IP phones:
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 iLBC;
When Y=8, the default value is G726-16;
When Y=9, the default value is G726-24;
When Y=10, the default value is G726-32;
When Y=11, the default value is G726-40.
Example:
account.1.codec.1.payload_type = PCMU
Web User Interface:
Account->Codec
Phone User Interface:
None</td></tr>
<tr><td>account.X.codec.Y.priority
(Y ranges from 1 to 11)</td><td>Integer from 0 to 10</td><td>Refer to the following content</td></tr>
</table>

Parameters	Permitted Values	Default
Description: Configures the priority of the enabled codec for account X. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **For SIP-T20P/T22P/T26P/T28P IP phones:** When Y=1, the default value is 2; When Y=2, the default value is 3; When Y=3, the default value is 0; 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; When Y=9, the default value is 0; When Y=10, the default value is 0; When Y=11, the default value is 0. **Example:** account.1.codec.1.priority = 1 **Web User Interface:** Account->Codec **Phone User Interface:** None		
account.X.codec.Y.rtpmap (Y ranges from 1 to 11)	Integer from 0 to 127	Refer to the following content
Description: Configures the rtpmap of the audio codec for account X. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **For SIP-T20P/T22P/T26P/T28P IP phones:** When Y=1, the default value is 0; When Y=2, the default value is 8; When Y=3, the default value is 4;		

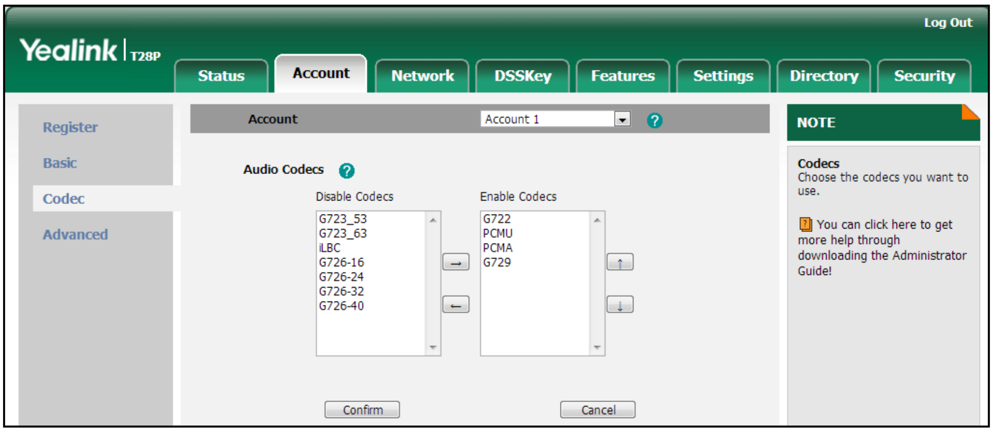
Parameters	Permitted Values	Default
When Y=4, the default value is 4; When Y=5, the default value is 18; When Y=6, the default value is 9; When Y=7, the default value is 106; When Y=8, the default value is 103; When Y=9, the default value is 104; When Y=10, the default value is 102; When Y=11, the default value is 105. **Example:** account.1.codec.1.rtpmap = 0 **Web User Interface:** None **Phone User Interface:** None		
account.X.ptime	**0 (Disabled), 10, 20, 30, 40, 50 or 60**	**20**
Description: Configures the ptime (in milliseconds) for the codec for account X. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Example:** account.1.ptime = 20 **Web User Interface:** Account->Advanced->PTime (ms) **Phone User Interface:** None		

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**.
2. Select the desired account from the pull-down list of **Account**.
3. Click on **Codec**.
4. Select the desired codec from the **Disable Codecs** column and then click → .

   The selected codec appears in the **Enable Codecs** column.

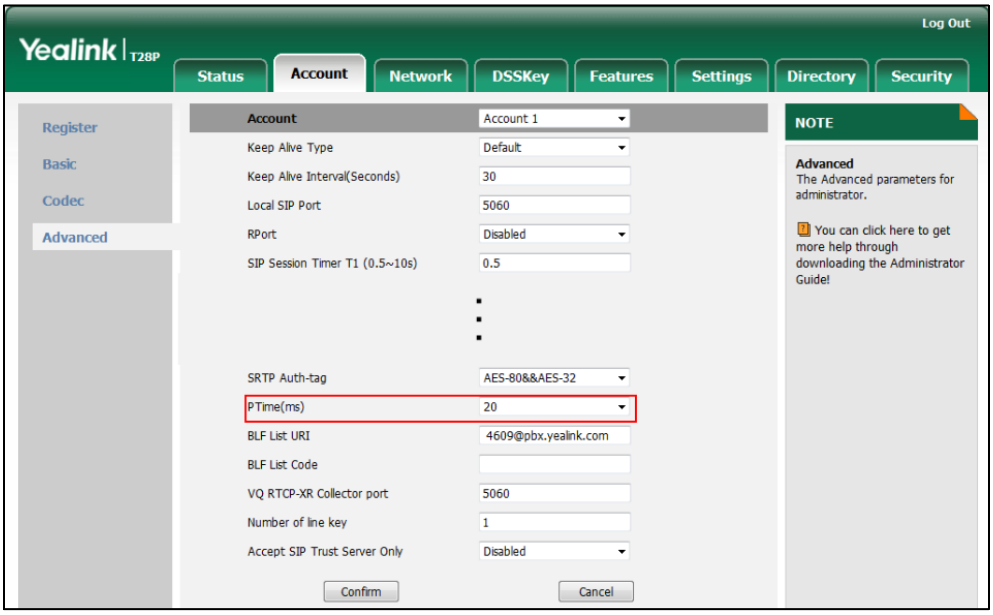
5. Repeat the step 4 to add more codecs to the **Enable Codecs** column.
6. To remove the codec from the **Enable Codecs** column, select the desired codec and then click ← .
7. To adjust the priority of codecs, select the desired codec and then click ↑ or ↓ .



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

To configure the ptime on a per-line basis via web user interface:

1. Click on **Account**.
2. Select the desired account from the pull-down list of **Account**.
3. Click on **Advanced**.
4. Select the desired value from the pull-down list of **PTime (ms)**.



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

Acoustic Clarity Technology

Acoustic Echo Cancellation

Acoustic Echo Cancellation (AEC) is used to reduce acoustic echo from a voice call to provide natural full-duplex communication patterns. It also increases the capacity achieved through silence suppression by preventing echo from traveling across a network. IP phones employ advanced AEC for hands-free operation. AEC is not normally required for calls via the handset. In certain situation, where echo is experienced by the remote party, AEC may be used to reduce/avoid echo when the user uses the handset.

Note: Utilizing acoustic echo cancellation will introduce a small delay increase into audio path which might cause a lower voice quality.

Procedure

AEC can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure AEC. **Parameter:** voice.echo_cancellation
Local	Web User Interface	Configure AEC. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-voice&q=load

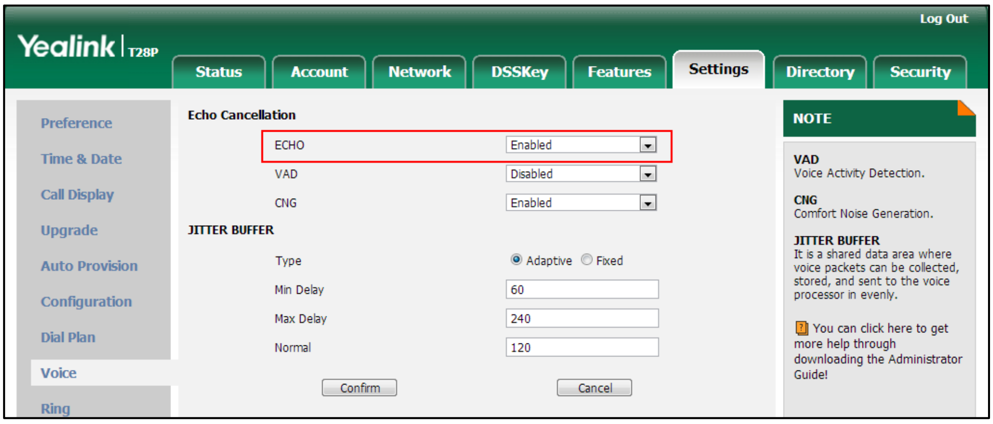
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
voice.echo_cancellation	0 or 1	1
Description: Enables or disables AEC (Acoustic Echo Canceller) feature on the IP phone. **0**-Disabled **1**-Enabled **Web User Interface:** Settings->Voice->Echo Cancellation->ECHO		

Parameter	Permitted Values	Default
Phone User Interface: None		

To configure AEC via web user interface:

1. Click on **Settings**->**Voice**.
2. Select the desired value from the pull-down list of **ECHO**.



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

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.

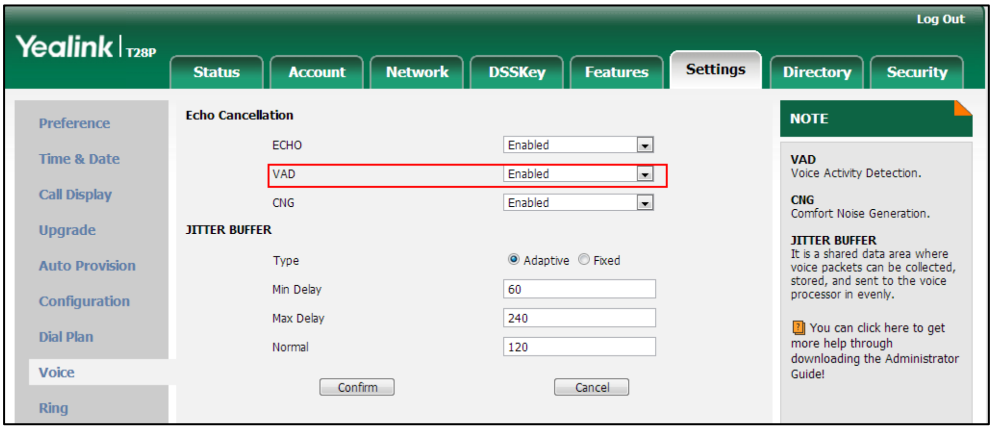
Configuration File	<y0000000000xx>.cfg	Configure VAD. **Parameter:** voice.vad
Local	Web User Interface	Configure VAD. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-voice&q=load

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
voice.vad	**0 or 1**	**0**
Description: Enables or disables VAD (Voice Activity Detection) feature on the IP phone. **0**-Disabled **1**-Enabled **Web User Interface:** Settings->Voice->Echo Cancellation ->VAD **Phone User Interface:** None		

To configure VAD via web user interface:

1. Click on **Settings**->**Voice**.
2. Select the desired value from the pull-down list of **VAD**.



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

Comfort Noise Generation

Comfort Noise Generation (CNG) is used to generate background noise for voice communications during periods of silence in a conversation. It is a part of the silence suppression or VAD handling for VoIP technology. CNG, in conjunction with VAD algorithms, quickly responds when periods of silence occur and inserts artificial noise until voice activity resumes. The insertion of artificial noise gives the illusion of a constant transmission stream, so that background sound is consistent throughout the call and the listener does not think the line has released. The purpose of VAD and CNG is to maintain an acceptable perceived QoS while simultaneously keeping transmission costs and bandwidth usage as low as possible.

Procedure

CNG can be configured using the configuration files or locally.

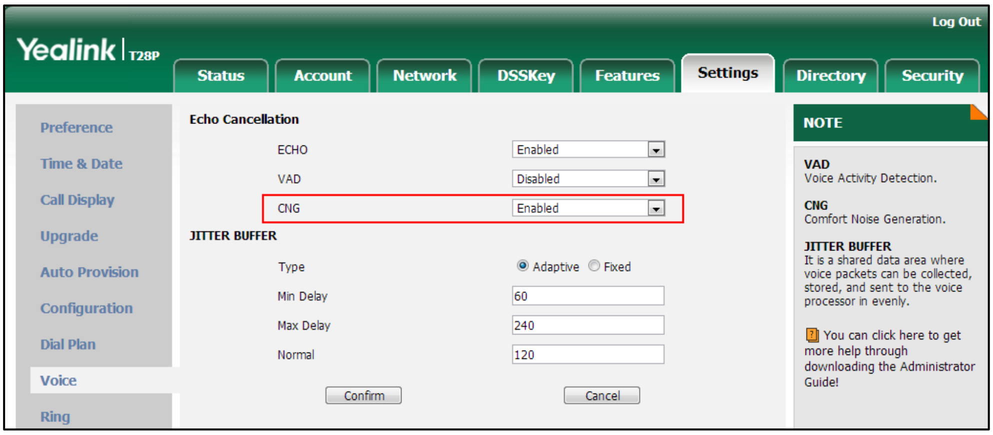
Configuration File	<y0000000000xx>.cfg	Configure CNG. **Parameter:** voice.cng
Local	Web User Interface	Configure CNG. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-voice&q=load

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
voice.cng	0 or 1	1
Description: Enables or disables CNG (Comfortable Noise Generator) feature on the IP phone. **0**-Disabled **1**-Enabled **Web User Interface:** Settings->Voice->Echo Cancellation ->CNG **Phone User Interface:** None		

To configure CNG via web user interface:

1. Click on **Settings**->**Voice**.
2. Select the desired value from the pull-down list of **CNG**.



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

Jitter Buffer

Jitter buffer is a shared data area where voice packets can be collected, stored, and sent to the voice processor in even intervals. Jitter is a term indicating variations in packet arrival time, which can occur because of network congestion, timing drift or route changes. The jitter buffer, located at the receiving end of the voice connection, intentionally delays the arriving packets so that the end user experiences a clear connection with very little sound distortion. IP phones support two types of jitter buffers: 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 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 phones.

Procedure

Jitter buffer can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure the mode of jitter buffer and the delay time for jitter buffer. **Parameters:** voice.jib.adaptive voice.jib.min voice.jib.max voice.jib.normal
Local	Web User Interface	Configure the mode of

		jitter buffer and the delay time for jitter buffer. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-voice&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
voice.jib.adaptive	0 or 1	1
Description: Configures the type of jitter buffer. **0**-Fixed **1**-Adaptive **Web User Interface:** Settings->Voice->JITTER BUFFER->Type **Phone User Interface:** None		
voice.jib.min	Integer from 0 to 400	60
Description: Configures the minimum delay time (in milliseconds) of jitter buffer. **Note**: It works only if the parameter “voice.jib.adaptive” is set to 1 (Adaptive). **Web User Interface:** Settings->Voice->JITTER BUFFER->Min Delay **Phone User Interface:** None		
voice.jib.max	Integer from 0 to 400	240
Description: Configures the maximum delay time (in milliseconds) of jitter buffer. **Note**: It works only if the parameter “voice.jib.adaptive” is set to 1 (Adaptive). **Web User Interface:** Settings->Voice->JITTER BUFFER->Max Delay **Phone User Interface:**		

Parameters	Permitted Values	Default
None		
voice.jib.normal	**Integer from 0 to 400**	**120**
Description: Configures the normal delay time (in milliseconds) of jitter buffer. **Note**: It works only if the parameter "voice.jib.adaptive" is set to 0 (Fixed). **Web User Interface:** Settings->Voice->JITTER BUFFER->Normal **Phone User Interface:** None		

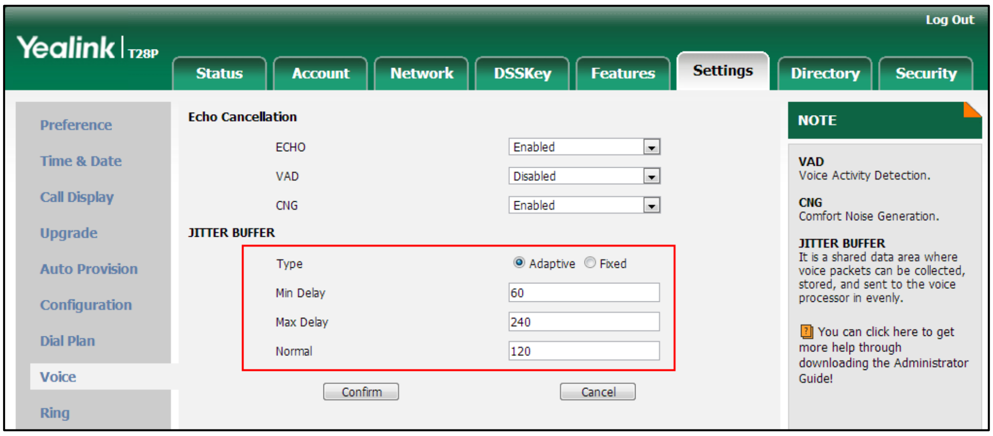
To configure Jitter Buffer via web user interface:

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 300.
4. Enter the maximum delay time for adaptive jitter buffer in the **Max Delay** field.

   The valid value ranges from 0 to 300.
5. Enter the fixed delay time for fixed jitter buffer in the **Normal** field.

   The valid value ranges from 0 to 300.



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

Configuring Security Features

This chapter provides information for making configuration changes for the following security-related features:

- Transport Layer Security
- Secure Real-Time Transport Protocol
- Encrypting Configuration Files

Transport Layer Security

TLS is a commonly-used protocol for providing communications privacy and managing the security of message transmission, allowing IP phones to communicate with other remote parties and connect to the HTTPS URL for provisioning in a way that is designed to prevent eavesdropping and tampering.

TLS protocol is composed of two layers: TLS Record Protocol and TLS Handshake Protocol. The TLS Record Protocol completes the actual data transmission and ensures the integrity and privacy of the data. The TLS Handshake Protocol allows the server and client to authenticate each other and negotiate an encryption algorithm and cryptographic keys before data is exchanged.

The TLS protocol uses asymmetric encryption for authentication of key exchange, symmetric encryption for confidentiality, and message authentication codes for integrity.

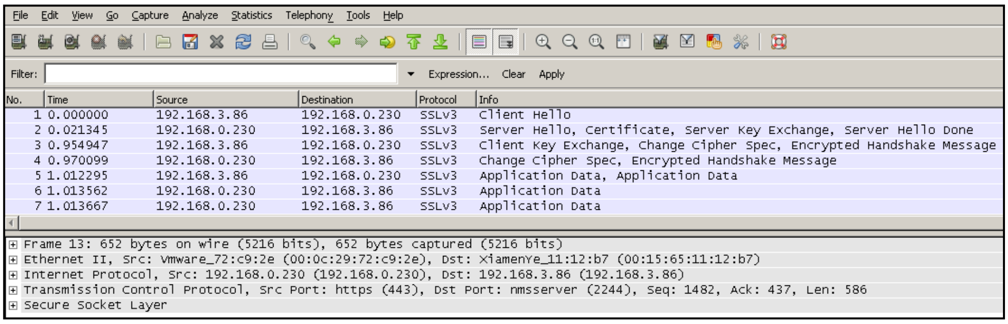
- **Symmetric encryption**: For symmetric encryption, the encryption key and the corresponding decryption key can be told by each other. In most cases, the encryption key is the same as the decryption key.
- **Asymmetric encryption**: For asymmetric encryption, each user has a pair of cryptographic keys – a public encryption key and a private decryption key. The information encrypted by the public key can only be decrypted by the corresponding private key and vice versa. Usually, the receiver keeps its private key. The public key is known by the sender, so the sender sends the information encrypted by the known public key, and then the receiver uses the private key to decrypt it.

IP 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. IP phones support the following cipher suites:

- DHE-RSA-AES256-SHA
- DHE-DSS-AES256-SHA

- AES256-SHA
- EDH-RSA-DES-CBC3-SHA
- EDH-DSS-DES-CBC3-SHA
- DES-CBC3-SHA
- DHE-RSA-AES128-SHA
- DHE-DSS-AES128-SHA
- AES128-SHA
- IDEA-CBC-SHA
- DHE-DSS-RC4-SHA
- RC4-SHA
- RC4-MD5
- EXP1024-DHE-DSS-DES-CBC-SHA
- EXP1024-DES-CBC-SHA
- EDH-RSA-DES-CBC-SHA
- EDH-DSS-DES-CBC-SHA
- DES-CBC-SHA
- EXP1024-DHE-DSS-RC4-SHA
- EXP1024-RC4-SHA
- EXP1024-RC4-MD5
- EXP-EDH-RSA-DES-CBC-SHA
- EXP-EDH-DSS-DES-CBC-SHA
- EXP-DES-CBC-SHA
- EXP-RC4-MD5

The following figure illustrates the TLS messages exchanged between the IP phone and TLS server to establish an encrypted communication channel:



Step1: IP phone sends "Client Hello" message proposing SSL options.

Step2: Server responds with "Server Hello" message selecting the SSL options, sends its public key information in "Server Key Exchange" message and concludes its part of the negotiation with “Server Hello Done” message.

Step3: IP phone sends session key information (encrypted by server’s public key) in the “Client Key Exchange” message.

Step4: Server sends “Change Cipher Spec” message to activate the negotiated options for all future messages it will send.

IP phones can encrypt SIP with TLS, which is called SIPS. When TLS is enabled for an account, the SIP message of this account will be encrypted, and a lock icon appears on the LCD screen after the successful TLS negotiation.

Certificates

The IP phone can serve as a TLS client or a TLS server. The TLS requires the following security certificates to perform the TLS handshake:

- **Trusted Certificate**: When the IP phone requests a TLS connection with a server, the IP phone should verify the certificate sent by the server to decide whether it is trusted based on the trusted certificates list. The IP phone has 30 built-in trusted certificates. You can upload 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 511.
- **Server Certificate**: When clients request a TLS connection with the IP phone, the IP phone sends the server certificate to the clients for authentication. The IP phone has two types of built-in server certificates: a unique server certificate and a generic server certificate. You can only upload one server certificate to the IP phone. The old server certificate will be overridden by the new one. The format of the server certificate files must be *.pem and *.cer and the maximum file size is 5MB.
  - **A unique server certificate**: It is unique to an IP 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 phone may send a generic certificate for authentication.

The IP phone can authenticate the server certificate based on the trusted certificates list. The trusted certificates list and the server certificates list contain the default and custom certificates. You can specify the type of certificates the IP phone accepts: default certificates, custom certificates or all certificates.

Common Name Validation feature enables the IP phone to mandatorily validate the common name of the certificate sent by the connecting server. 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.

Firmware upgrade from version 71 to 72 will result in update of the generic server certificates.

We strongly recommend that you do not downgrade the firmware. For SIP-T20P/T22P/T26P/T28P IP phones, firmware downgrade will result in damage to the unique server certificate.

Resetting the IP 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 457.

Procedure

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

Configuration File	<MAC>.cfg	Configure TLS on a per-line basis. **Parameter:** account.X.transport
	<y0000000000xx>.cfg	Configure trusted certificates feature. **Parameters:** security.trust_certificates security.ca_cert security.cn_validation Configure server certificates feature. **Parameters:** security.dev_cert Upload the trusted certificates. **Parameter:** trusted_certificates.url Upload the server certificates. **Parameter:** server_certificates.url Configure the custom certificates. **Parameter:** phone_setting.reserve_certs_enable
Local	Web User Interface	Configure TLS on a per-line basis.

		Navigate to: http://<phoneIPAddress>/servlet?p=account-register&q=load&acc=0 Configure trusted certificates feature. Upload the trusted certificates. **Navigate to**: http://<phoneIPAddress>/servlet?p=trusted-cert&q=load Configure server certificates feature. Upload the server certificates. **Navigate to**: http://<phoneIPAddress>/servlet?p=server-cert&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.transport	**Integer**	**0**
Description: Configures the type of transport protocol for account X. **0**-UDP **1**-TCP **2**-TLS **3**-DNS-NAPTR X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Web User Interface:** Account->Register ->Transport **Phone User Interface:** None		
security.trust_certificates	**0 or 1**	**1**
Description: Enables or disables the IP phone to only trust the server certificates in the Trusted Certificates list.		

Parameters	Permitted Values	Default
0-Disabled **1**-Enabled If it is set to 1 (Enabled), the IP phone will authenticate the server certificate based on the trusted certificates list. Only when the authentication succeeds, the IP phone will trust the server. If it is set to 0 (Disabled), the IP phone will trust the server no matter whether the certificate sent by the server is valid or not. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Security->Trusted Certificates->Only Accept Trusted Certificates **Phone User Interface:** None		
security.ca_cert	**0, 1 or 2**	**2**
Description: Configures the type of certificates in the Trusted Certificates list for the IP phone to authenticate for TLS connection. **0**-Default certificates **1**-Custom certificates **2**-All certificates **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Security->Trusted Certificates->CA Certificates **Phone User Interface:** None		
security.cn_validation	**0 or 1**	**0**
Description: Enables or disables the IP phone to mandatorily validate the CommonName or SubjectAltName of the certificate sent by the server. **0**-Disabled **1**-Enabled **Note:** If you change this parameter, the IP phone will reboot to make the change		

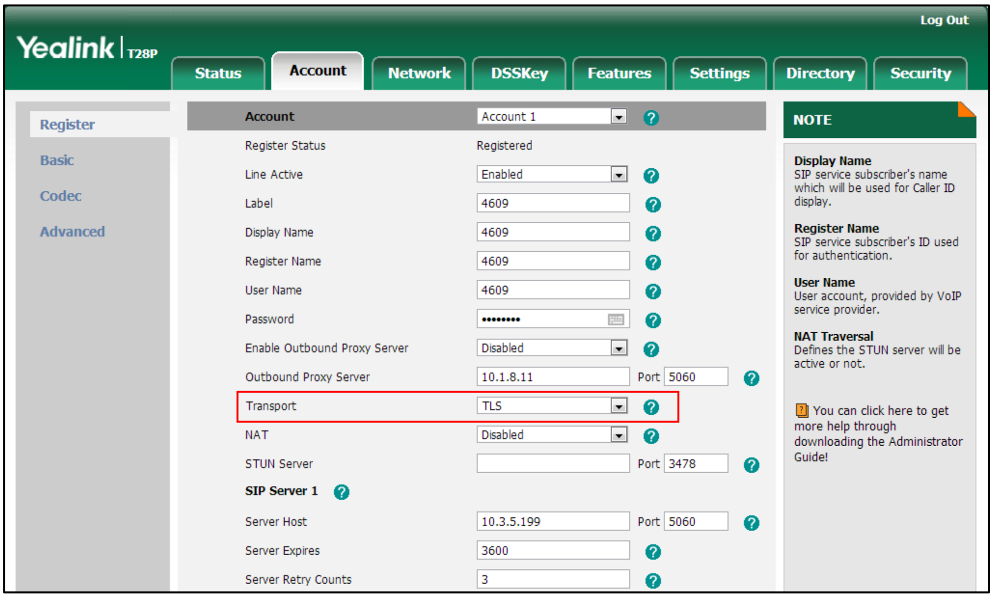
Parameters	Permitted Values	Default
take effect. **Web User Interface:** Security->Trusted Certificates->Common Name Validation **Phone User Interface:** None		
security.dev_cert	**0 or 1**	**0**
Description: Configures the type of the device certificates for the IP phone to send for TLS authentication. **0**-Default certificates **1**-Custom certificates **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Security->Server Certificates->Device Certificates **Phone User Interface:** None		
trusted_certificates.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the custom trusted certificate used to authenticate the connecting server. **Example:** trusted_certificates.url = http://192.168.1.20/tc.crt **Note**: The certificate you want to upload must be in *.pem, *.crt, *.cer or *.der format. **Web User Interface:** Security->Trusted Certificates->Load trusted certificates file **Phone User Interface:** None		
server_certificates.url	**URL within 511 characters**	**Blank**

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td colspan="3">Description:
Configures the access URL of the certificate the IP phone sends for authentication.
Example:
server_certificates.url = http://192.168.1.20/ca.pem
Note: The certificate you want to upload must be in *.pem or *.cer format.
Web User Interface:
Security->Server Certificates->Load server cer file
Phone User Interface:
None</td></tr>
<tr><td>phone_setting.reserve_certs_enable</td><td>0 or 1</td><td>0</td></tr>
<tr><td colspan="3">Description:
Enables or disables the IP phone to reserve custom certificates after it is reset to factory defaults.
0-Disabled
1-Enabled
Note: It is only applicable to SIP-T28P/T26P/T22P/T20P IP phones running firmware version X.72.0.25 or later.
Web User Interface:
None
Phone User Interface:
None</td></tr>
</table>

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**.

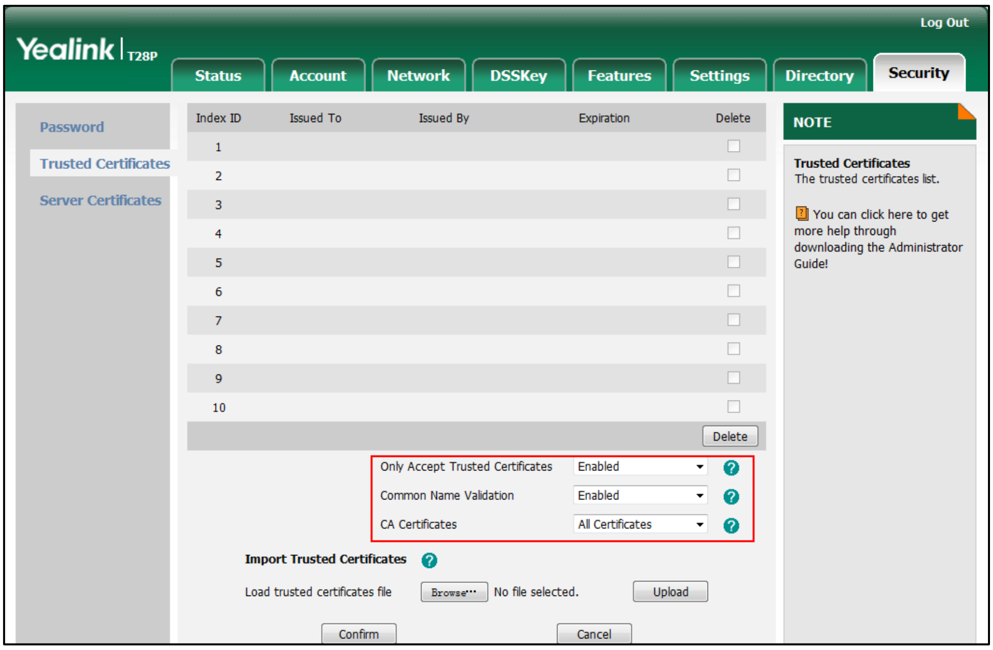
3. Select **TLS** from the pull-down list of **Transport**.



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**.

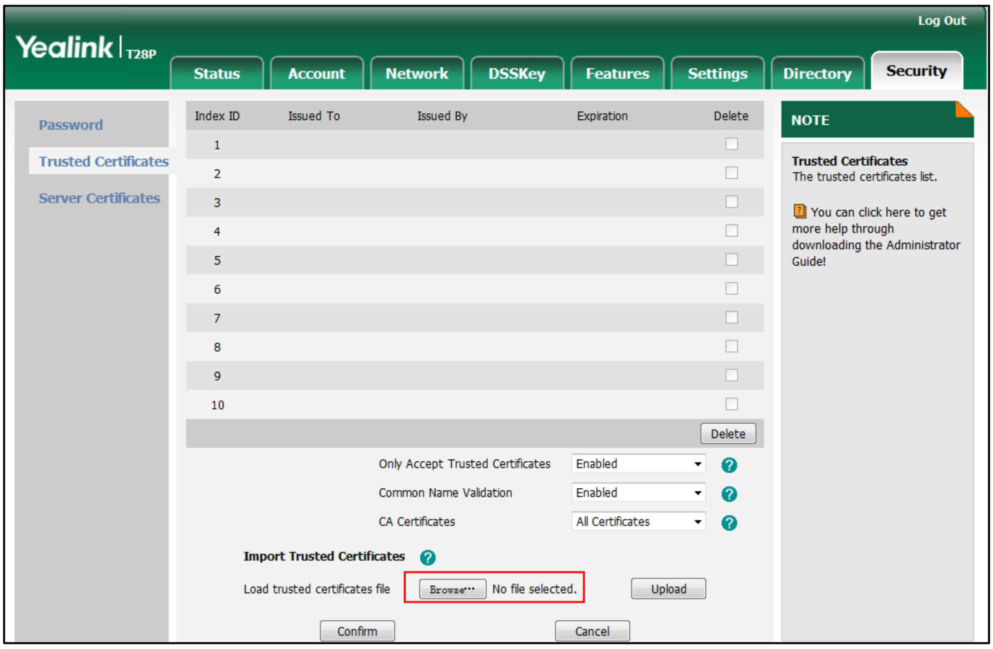


3. Click **Confirm** to accept the change.

To upload a trusted certificate via web user interface:

1. Click on **Security**->**Trusted Certificates**.

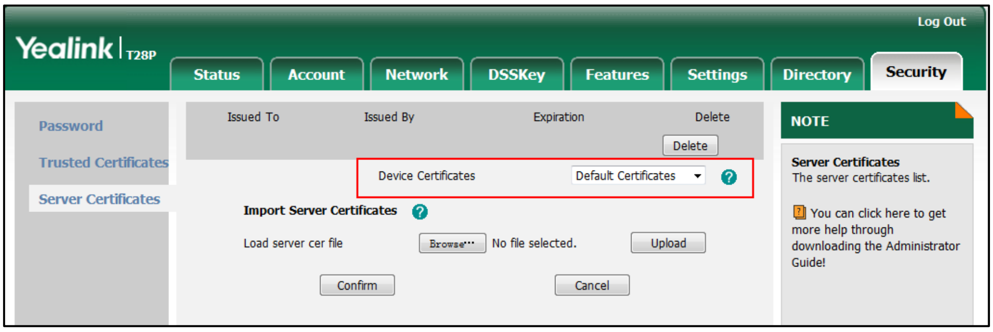
2. Click **Browse** to select the certificate (*.pem, *.crt, *.cer or *.der) from your local system.



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**.

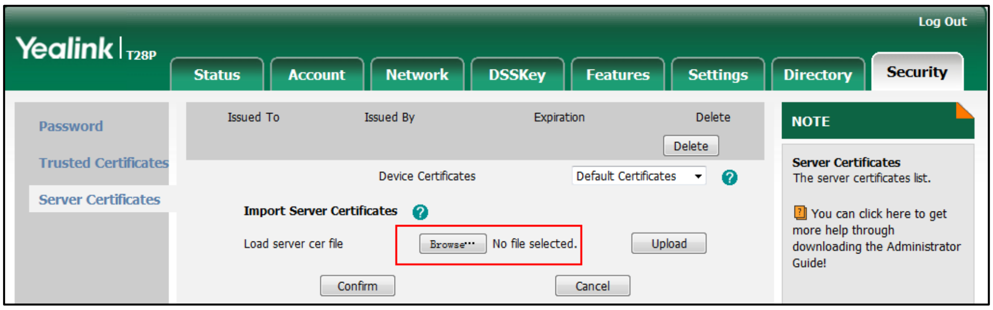


3. Click **Confirm** to accept the change.

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 streams during VoIP 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 phones. This negotiation process is compliant with RFC 4568.

When a user places a call on the enabled SRTP phone, the IP phone sends an INVITE message with the RTP encryption algorithm to the destination phone.

Example of the RTP encryption algorithm carried in the SDP of the INVITE message:

```
m=audio 11780 RTP/SAVP 0 8 18 9 101
a=crypto:1 AES_CM_128_HMAC_SHA1_80
inline:NzFlNTUwZDk2OGVlOTc3YzNkYTkwZWVkMTM1YWFj
a=crypto:2 AES_CM_128_HMAC_SHA1_32
inline:NzkyM2FjNzQ2ZDgxYjg0MzQwMGVmMGUxMzdmNWFm
a=crypto:3 F8_128_HMAC_SHA1_80 inline:NDliMWIzZGE1ZTAwZjA5ZGFhNjQ5YmEANTMzYzA0
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:NGY4OGViMDYzZjQzYTNiOTNkOWRiYzRlMjM0Yzcz
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 phones, RTP streams will be encrypted, and a lock icon appears on the LCD screen of each IP phone after successful negotiation.

Note

If you enable SRTP, then you should also enable TLS. This ensures the security of SRTP encryption. For more information on TLS, refer to Transport Layer Security on page 457.

Procedure

SRTP can be configured using the configuration files or locally.

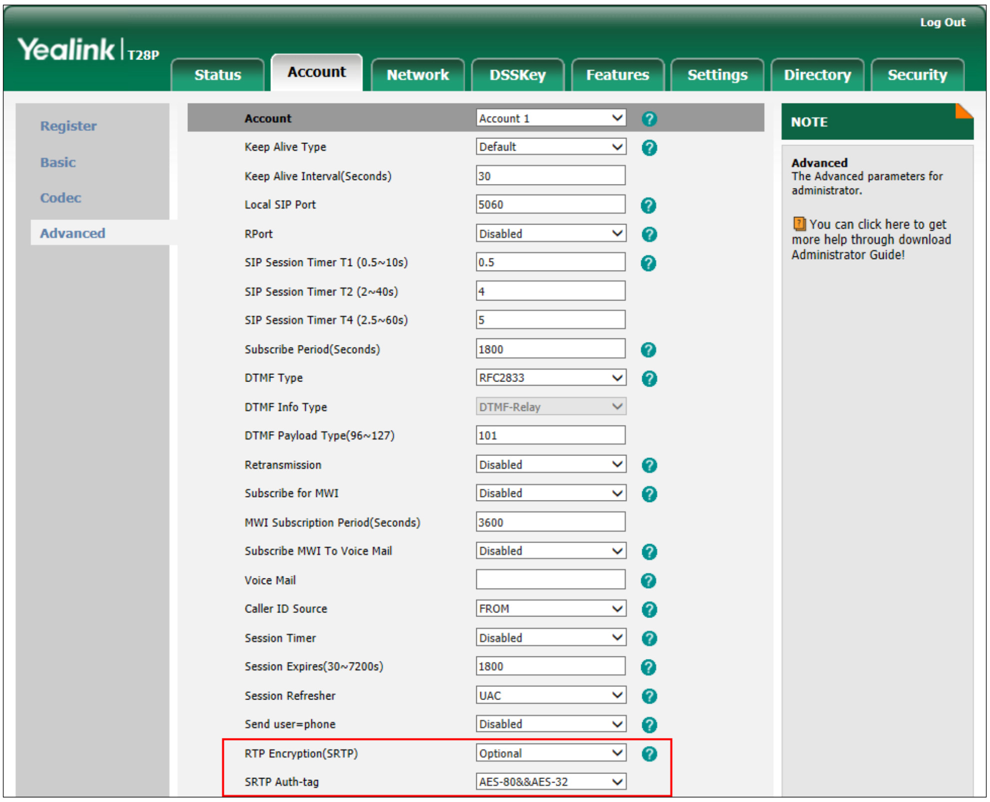
Configuration File	<MAC>.cfg	Configure SRTP feature on a per-line basis. **Parameter:** account.X.srtp_encryption account.X.srtp_auth_tag_mode
Local	Web User Interface	Configure SRTP feature on a per-line basis. **Navigate to:** http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

Details of the Configuration Parameter:

Parameters	Permitted Values	Default
account.X.srtp_encryption	**0, 1 or 2**	**0**
Description: Configures whether to use voice encryption service for account X. **0**-Disabled **1**-Optional **2**-Compulsory If it is set to 1 (Optional), the IP phone will negotiate with the other IP phone what type of encryption to utilize for the session. If it is set to 2 (Compulsory), the IP phone is forced to use SRTP during a call. X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Web User Interface:** Account->Advanced->RTP Encryption (SRTP) **Phone User Interface:** None		
account.X.srtp_auth_tag_mode	**0, 1 or 2**	**0**
Description: Configures the key type carried in the SRTP packet when using voice encryption service for account X. **0**-AES-80&&AES-32 **1**-AES-80 **2**-AES-32 X ranges from 1 to 6 (for SIP-T28P). X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). **Note**: It is only applicable to IP phones running firmware version 73 or later. **Web User Interface:** Account->Advanced->SRTP Auth-tag **Phone User Interface:** None		

To configure SRTP feature via web user interface:

1. Click on **Account**.
2. Select the desired account from the pull-down list of **Account**.
3. Click on **Advanced**.
4. Select the desired value from the pull-down list of **RTP Encryption (SRTP)**.
5. Select the desired key type from the pull-down list of **SRTP Auth-tag**.



6. 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 <y0000000000xx>.cfg and <MAC>.cfg files (one by one or in batch) using 16-character symmetric keys (the same or different keys for configuration files) and generates encrypted configuration files with the same file name as before. This tool also encrypts the plaintext 16-character symmetric keys using a fixed key, which is the same as the one built in the IP phone, and generates new files named as <xx_Security>.enc (xx indicates the name of the configuration file, for example, y000000000000_Security.enc for y000000000000.cfg file). This tool generates another new file named as Aeskey.txt to store the plaintext 16-character symmetric keys for each configuration file.

For a Microsoft Windows platform, you can use a Yealink-supplied encryption tool "Config_Encrypt_Tool.exe" to encrypt the <y0000000000xx>.cfg and <MAC>.cfg files respectively.

Note Yealink also supplies a configuration encryption tool (yealinkencrypt) for Linux platform if required. For more information, refer to *Yealink Configuration Encryption Tool User Guide*, available online: http://www.yealink.com/DocumentDownload.aspx?CateId=142&flag=142.

For security reasons, administrator should upload encrypted configuration files, <y0000000000xx_Security>.enc and/or <MAC_Security>.enc files to the root directory of the provisioning server. During auto provisioning, the IP phone requests to download <y0000000000xx>.cfg file first. If the downloaded configuration file is encrypted, the IP phone will request to download <y0000000000xx_Security>.enc file (if enabled) and decrypt it into the plaintext key (e.g., key2) using the built-in key (e.g., key1). Then the IP phone decrypts <y0000000000xx>.cfg file using key2. After decryption, the IP phone resolves configuration files and updates configuration settings onto the IP phone system.

The way the IP phone processes the <MAC>.cfg file is the same to that of the<y0000000000xx>.cfg file.

Procedure to Encrypt Configuration Files

To encrypt the <y0000000000xx>.cfg file:

1. Double click "Config_Encrypt_Tool.exe" to start the application tool.

   The screenshot of the main page is shown as below:

   When you start the application tool, a file folder named "Encrypted" is created automatically in the directory where the application tool is located.

2. Click **Browse** to locate configuration file(s) (e.g., y000000000000.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.

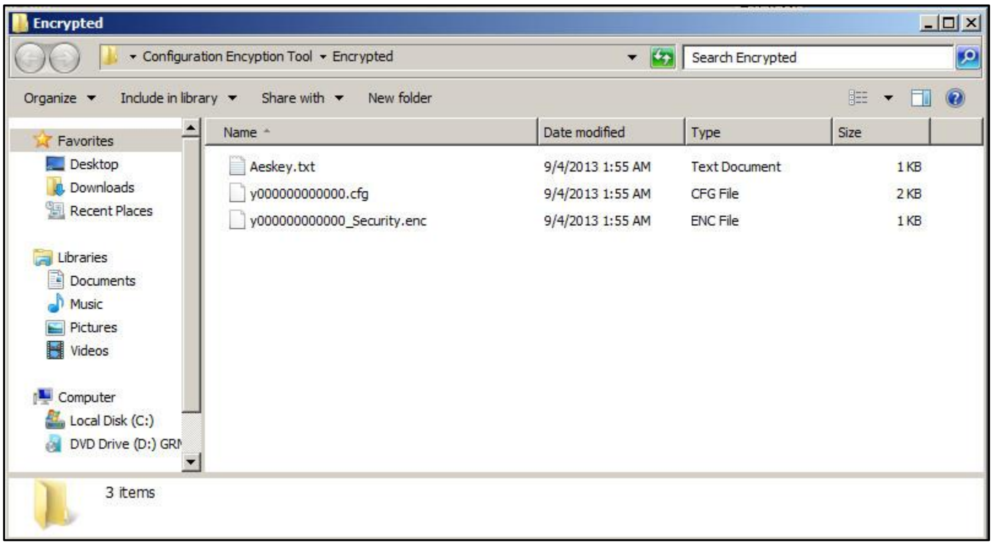
   If you mark the **Auto Generate** radio box, the configuration file(s) will be encrypted using random AES key. The AES keys of configuration files are different.

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.

Configuration File	<y0000000000xx>.cfg	Configure the decryption method. **Parameter:** auto_provision.aes_key_in_file Configure AES keys. **Parameters:** auto_provision.aes_key_16.com auto_provision.aes_key_16.mac auto_provision.update_file_mode
Local	Web User Interface	Configure AES keys. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-autop&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
auto_provision.aes_key_in_file	**0 or 1**	**0**
Description: Enables or disables the IP phone to decrypt configuration files using the encrypted AES keys. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the IP phone will download <y0000000000xx_Security>.enc and <MAC_Security>.enc files during auto provisioning, and then decrypts these files into the plaintext keys (e.g., key2, key3) respectively using the phone built-in key (e.g., key1). The IP phone then decrypts the encrypted configuration files using corresponding key (e.g., key2, key3). If it is set to 0 (Disabled), the IP phone will decrypt the encrypted configuration files using plaintext AES keys configured on the IP phone. **Web User Interface:** None **Phone User Interface:** None		

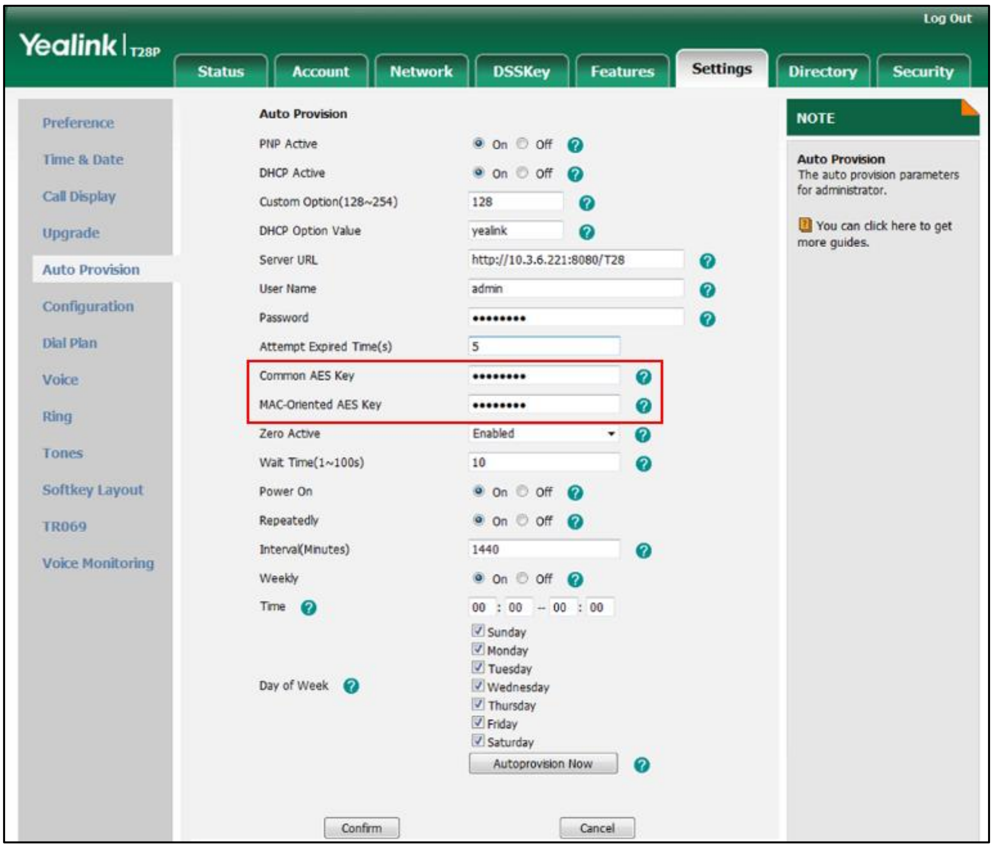
<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>auto_provision.aes_key_16.com</td><td>16 characters</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the plaintext AES key for decrypting the Common CFG file.
The valid characters contain: 0 ~ 9, A ~ Z, a ~ z and the following special characters are also supported: # $ % * + , - . : = ? @ [ ] ^ _ { } ~.
Example:
auto_provision.aes_key_16.com = 0123456789abcdef
Note: It works only if the parameter "auto_provision.aes_key_in_file" is set to 0 (Disabled).
Web User Interface:
Settings->Auto Provision->Common AES Key
Phone User Interface:
None</td></tr>
<tr><td>auto_provision.aes_key_16.mac</td><td>16 characters</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the plaintext AES key for decrypting the MAC-Oriented CFG file.
The valid characters contain: 0 ~ 9, A ~ Z, a ~ z and the following special characters are also supported: # $ % * + , - . : = ? @ [ ] ^ _ { } ~.
Example:
auto_provision.aes_key_16.mac = 0123456789abmins
Note: It works only if the parameter "auto_provision.aes_key_in_file" is set to 0 (Disabled).
Web User Interface:
Settings->Auto Provision->MAC-Oriented AES Key
Phone User Interface:
None</td></tr>
<tr><td>auto_provision.update_file_mode</td><td>0 or 1</td><td>0</td></tr>
<tr><td colspan="3">Description:
Enables or disables the IP phone to update encrypted configuration settings only during auto provisioning.
0-Disabled</td></tr>
</table>

Parameters	Permitted Values	Default
1-Enabled **Web User Interface:** None **Phone User Interface:** None		

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.

Resource Files

When configuring particular features, you may need to upload resource files (e.g., local contact directory, remote phone book) to IP phones. The resources files can be local contact directory, remote phone book and so on. Ask Yealink field application engineer for resource file templates. If the resource file is to be used for all IP phones of the same model, the resource file access URL is best specified in the <y0000000000xx>.cfg file. However, if you want to specify the desired phone to use the resource file, the resource file access URL should be specified in the <MAC>.cfg file.

The names of the Yealink-supplied template files are (You can rename the filename as required):

Template File	File Name
Replace Rule Template	dialplan.xml
Dial-now Template	dialnow.xml
Softkey Layout Template	CallFailed.xml CallIn.xml Connecting.xml Dialing.xml RingBack.xml Talking.xml
Directory Template	favorite_setting.xml
Super Search Template	super_search.xml
Local Contact File	contact.xml
Remote XML Phone Book	Department.xml Menu.xml

This chapter provides the detailed information on how to customize the following resource files:

- Replace Rule Template
- Dial-now Template
- Softkey Layout Template

- Directory Template
- Super Search Template
- Local Contact File
- Remote XML Phone Book

Replace Rule Template

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

When editing a replace rule template, learn the following:

- <DialRule> indicates the start of a template and </DialRule> indicates the end of a template.
- Create replace rules between <DialRule> and </DialRule>.
- When specifying the desired line(s) to apply the replace rule, the valid values are 0 and line ID. The digit 0 stands for all lines. Multiple line IDs are separated by commas.
- At most 100 replace rules can be added to the IP phone.
- The expression syntax in the replace rule template is the same as that introduced in the section Dial Plan on page 116.

Procedure

Use the following procedures to customize a replace rule template.

To customize a replace rule template:

1. Open the template file using an ASCII editor.
2. Add the following string to the template, each starting on a separate line:

   <Data Prefix="" Replace="" LineID=""/>

   Where:

   Prefix="" specifies the numbers to be replaced.

   Replace="" specifies the alternate string instead of what the user enters.

   LineID="" specifies the desired line(s) for this rule. When you leave it blank or enter 0, this replace rule will apply to all lines.
3. Specify the values within double quotes.
4. Place this file to the provisioning server.

The following shows an example of a replace rule template:

```
<DialRule>
```

```
  <Data Prefix="1" Replace="05928665234" LineID=""/>
  <Data Prefix="2(xx)" Replace="002$1" LineID="0"/>
  <Data Prefix="5([6-9])(.)" Replace="3$2" LineID="1,2,3"/>
  <Data Prefix="0(.)" Replace="9$1" LineID="2"/>
  <Data Prefix="1009" Replace="05921009" LineID="1"/>
</DialRule>
```

Dial-now Template

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

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

- <DialNow> indicates the start of a template and </DialNow> indicates the end of a template.
- Create dial-now rules between <DialNow> and </DialNow>.
- When specifying the desired line(s) for the dial-now rule, the valid values are 0 and line ID. 0 stands for all lines. Multiple line IDs are separated by commas.
- At most 100 rules can be added to the IP phone.
- The expression syntax in the dial-now rule template is the same as that introduced in the section Dial Plan on page 116.

Procedure

Use the following procedures to customize a dial-now template.

To customize a dial-now template:

1. Open the template file using an ASCII editor.
2. Add the following string to the template, each starting on a separate line:

   <Data DialNowRule="" LineID=""/>

   Where:

   DialNowRule="" specifies the dial-now rule.

   LineID="" specifies the desired line(s) for this rule. When you leave it blank or enter 0, this dial-now rule will apply to all lines.
3. Specify the values within double quotes.
4. Place this file to the provisioning server.

The following shows an example of a dial-now template:

```
<DialNow>
  <Data DialNowRule="1234" LineID="1"/>
```

```
    <Data DialNowRule="52[0-6]" LineID="1"/>
    <Data DialNowRule="xxxxxx" LineID=""/>
  </DialNow>
```

Softkey Layout Template

The softkey layout template allows you to customize soft key layout for different call states. The call states include CallFailed, CallIn, Connecting, Dialing, RingBack and Talking. After setup, place the templates to the provisioning server and specify the access URL in the configuration files.

When editing a softkey layout template, learn the following:

- <Call States> indicates the start of a template and </Call States> indicates the end of a template. For example, <CallFailed></CallFailed>.
- <Disable> indicates the start of the disabled soft key list and </Disable> indicates the end of the soft key list. The disabled soft keys are not displayed on the LCD screen.
- Create disabled soft keys between <Disable> and </Disable>.
- <Enable> indicates the start of the enabled soft key list and </Enable> indicates the end of the soft key list. The enabled soft keys are displayed on the LCD screen.
- Create enabled soft keys between <Enable> and </Enable>.
- <Default> indicates the start of the default soft key list and </Default> indicates the end of the default soft key list. The default soft keys are displayed on the LCD screen by default.

Procedure

Use the following procedures to customize a softkey layout template.

To customize a softkey layout template:

1. Open the template file using an ASCII editor.
2. For each soft key that you want to enable, add the following string between <Enable> and </Enable> in the file. Each starts on a separate line:

   <Key Type=""/>

   Where:

   Key Type="" specifies the enabled soft key (This value cannot be blank).

   For each disabled soft key and each default soft key that you want to add, add the same string introduced above.
3. Specify the values within double quotes.
4. Place this file to the provisioning server.

The following shows an example of the CallFailed template:

```
<CallFailed>
  <Disable>
    <Key Type="Empty"/>
    <Key Type="Switch"/>
    <Key Type="Cancel"/>
  </Disable>
  <Enable>
    <Key Type="NewCall"/>
    <Key Type="Empty"/>
    <Key Type="Empty"/>
    <Key Type="Empty"/>
  </Enable>
  <Default>
    <Key Type="NewCall"/>
    <Key Type="Empty"/>
    <Key Type="Empty"/>
    <Key Type="Empty"/>
  </Default>
</CallFailed>
```

Directory Template

Directory provides easy access to frequently used lists. Users can access lists by pressing the Directory soft key when the IP phone is idle. The lists may contain Local Directory, History, Remote Phone Book (not applicable to SIP-T20P IP phones) and LDAP. You can add the desired list(s) to Directory using the supplied directory template (favorite_setting.xml). After setup, place the directory template to the provisioning server and specify the access URL in the configuration files.

When editing a directory template, learn the following:

- <root_favorite_set> indicates the start of a template and </root_favorite_set> indicates the end of a template.
- The default display names of the directory lists are Local Directory, History, Remote Phone Book and LDAP.
- When specifying the display priority of the directory list, the valid values are 1, 2, 3 and 4. 1 is the highest priority, 4 is the lowest.
- When enabling or disabling the desired directory list, the valid values are 0 and 1. 0 stands for Disabled, 1 stands for Enabled.

Procedure

Use the following procedures to customize a directory template.

Customizing a directory template:

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

   <item id_name="localdirectory" display_name="Local Directory" priority="1" enable="1" />

   Where:

   id_name="" specifies the existing directory list ("localdirectory" for the local directory list). Do not edit this field.

   display_name="" specifies the display name of the directory list. We recommend you do not edit this field.

   priority="" specifies the display priority of the directory list.

   enable="" enables or disables the directory list.
3. Edit the values within double quotes.
4. Place this file to the provisioning server.

The following shows an example of a directory template:

```
<root_favorite_set>
  <item id_name="localdirectory" display_name="Local Directory"
  priority="1" enable="1" />
  <item id_name="history" display_name="History" priority="2"
  enable="0" />
  <item id_name="remotedirectory" display_name="Remote Phone Book"
  priority="3" enable="0" />
  <item id_name="ldap" display_name="LDAP" priority="4" enable="0" />
</root_favorite_set>
```

Super Search Template

Search source list in dialing allows the IP phone to search for entries from the desired lists based on the entered string when in the pre-dialing screen, and then the user can select the desired entry to dial out quickly. The lists may contain Local Directory, History, Remote Phone Book (not applicable to SIP-T20P IP phones) and LDAP. You can configure the search source list in dialing using the supplied super search template (super_search.xml). After setup, place the super search template to the provisioning server and specify the access URL in the configuration files.

When editing a super search template, learn the following:

- <root_super_search> indicates the start of a template and </root_super_search> indicates the end of a template.
- The default display names of the directory lists are Local Directory, History, Remote Phone Book and LDAP.
- When specifying the priority of search results, the valid values are 1, 2, 3 and 4. 1 is the highest priority, 4 is the lowest.
- When enabling or disabling the desired directory list, the valid values are 0 and 1. 0 stands for Disabled, 1 stands for Enabled.

Procedure

Use the following procedures to customize a super search template.

Customizing a super search template:

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

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

   Where:

   id_name="" specifies the directory list ("local_directory_search" for the local directory list). Do not edit this field.

   display_name="" specifies the display name of the directory list. We do not recommend editing this field.

   priority="" specifies the priority of search results.

   enable="" enables or disables the directory list.
3. Edit the values within double quotes.
4. Place this file to the provisioning server.

The following shows an example of a super search template:

```
<root_super_search>
  <item id_name="local_directory_search" display_name="Local
  Directory" priority="1" enable="1" />
  <item id_name="calllog_search" display_name="History" priority="2"
  enable="1" />
  <item id_name="remote_directory_search" display_name="Remote Phone
  Book" priority="3" enable="0" />
  <item id_name="ldap_search" display_name="LDAP" priority="4"
  enable="0" />
</root_super_search>
```

Local Contact File

You can add contacts one by one on the IP phone directly. You can also add multiple contacts at a time and/or share contacts between IP phones using the local contact template file. After setup, place the template file to the provisioning server and specify the access URL of the template file in the configuration files.

When editing a local contact template, learn the following:

- <root_contact> indicates the start of a contact list and </root_contact> indicates the end of a contact list.
- <root_group> indicates the start of a group list and </root_group> indicates the end of a group list.
- When specifying a ring tone for a contact or a group, the format of the value must be Auto (the first registered line), Resource: Silent.wav, Resource: Splash.wav or Resource: RingN.wav (system ring tone, integer N ranges from 1 to 5) or Custom: Name.wav (custom ring tone).
- When specifying a desired line for a contact, valid values are 0~6. Multiple line IDs are separated by commas.

  The following table lists valid values for each phone model.

Phone Model	Values	Description
SIP-T20P	0~2	0 stands for Auto (the first registered line) 1~2 stand for line1~line2
SIP-T22P/T26P	0~3	0 stands for Auto (the first registered line) 1~3 stand for line1~line3
SIP-T28P	0~6	0 stands for Auto (the first registered line) 1~6 stand for line1~line6

- At most 5 groups can be added to the IP phone.
- At most 1000 local contacts can be added to the IP phone.

Procedure

Use the following procedures to customize a local contact template file.

To customize a local contact file:

1. Open the template file using an ASCII editor.
2. For each group that you want to add, add the following string to the file. Each starts on a separate line:

   <group display_name="" ring=""/>

   Where:

   display_name="" specifies the name of the group.

   ring="" specifies the desired ring tone for this group.

3. For each contact that you want to add, add the following string to the file. Each starts on a separate line:

   <contact display_name="" office_number="" mobile_number="" other_number="" line="" ring="" group_id_name=""/>

   Where:

   display_name="" specifies the name of the contact (This value cannot be blank or duplicated).

   office_number="" specifies the office number of the contact.

   mobile_number="" specifies the mobile number of the contact.

   other_number="" specifies the other number of the contact.

   line="" specifies the line you want to add this contact to.

   ring="" specifies the ring tone for this contact.

   group_id_name="" specifies the existing group you want to add the contact to.

4. Specify the values within double quotes.
5. Place this file to the provisioning server.

The following shows an example of a local contact file:

```
<root_group>
  <group display_name="Friend" ring=""/>
  <group display_name="Family" ring="Resource:Ring1.wav"/>
</root_group>
<root_contact>
  <contact display_name="John" office_number="1001"
  mobile_number="12345678910" other_number="" line="0" ring="Auto"
  group_id_name="All Contacts"/>
  <contact display_name="Alice" office_number="1002" mobile_number=""
  other_number="" line="1,2" ring=”Resource:Ring2.wav”
  group_id_name="Friend"/>
</root_contact>
```

Remote XML Phone Book

IP phones can access 5 remote phone books. You can customize the remote XML phone book for IP phones as required. You can also add multiple remote contacts at a time and/or share remote contacts between IP phones using the supplied template files (Menu.xml and Department.xml). The Menu.xml file defines departments of a remote phone book. The Department.xml file defines contact lists for a department, which is nested in Menu.xml file. After setup, place the files (Menu.xml and Department.xml) to the provisioning server, and specify the access URL of the file (Menu.xml) in the configuration files.

When creating a Menu.xml file, learn the following:

- <YealinkIPPhoneMenu> indicates the start of a remote phone book file and </YealinkIPPhoneMenu> indicates the end of a remote phone book file.
- Create the title of a remote phone book between <Title> and </Title>.
- <MenuItem>indicates the start of specifying a department file and </MenuItem> indicates the end of specifying a department file.
- <SoftKeyItem> indicates the start of specifying a XML file and </SoftKeyItem> indicates the end of specifying a XML file.

Procedure

Use the following procedures to customize an XML phone book.

To customize a Menu.xml file:

1. Open the template file using an ASCII editor.
2. For each department that you want to add, add the following strings to the file. Each starts on a separate line:

   <MenuItem>

   <Name>*Department1*</Name>

   <URL>*http://10.3.6.117:8080/Department1.xml*</URL>

   </MenuItem>

   Where:

   Specify the name of a department between <Name> and </Name>.

   Specify the access URL of a department file between </URL> and </URL>.
3. For each XML file that you want to add, add the following strings to the file. Each starts on a separate line:

   <SoftKeyItem>

   <Name>*#*</Name>

   <URL>*http://10.3.6.128:8080/TextMenu.xml*</URL>

   </SoftKeyItem>

   Where:

   Specify the key between <Name> and </Name>.

   Specify the access URL of a XML file between </URL> and </URL>.
4. Save the file and place this file to the provisioning server.

The following shows an example of a Menu.xml file:

```
<YealinkIPPhoneMenu>
  <Title>XiaMen Yealink</Title>
    <MenuItem>
```

```
    <Name>Department1</Name>
    <URL>http://10.2.9.1:99/Department.xml</URL>
  </MenuItem>
  <MenuItem>
    <Name>Department2</Name>
    <URL>http://10.2.9.1:99/Department.xml</URL>
  </MenuItem>
  <SoftKeyItem>
    <Name>#</Name>
    <URL>http://10.2.9.1:99/Department.xml</URL>
  </SoftKeyItem>
  <SoftKeyItem>
    <Name>*</Name>
    <URL>http://10.2.9.1:99/Department.xml</URL>
  </SoftKeyItem>
  <SoftKeyItem>
    <Name>1</Name>
    <URL>http://10.2.9.1:99/Department.xml</URL>
  </SoftKeyItem>
</YealinkIPPhoneMenu>
```

When creating a Department.xml file, learn the following:

- <YealinkIPPhoneDirectory> indicates the start of a department file and </YealinkIPPhoneDirectory> indicates the end of a department file.
- Create contact lists for a department between <DirectoryEntry> and </DirectoryEntry>.

To customize a Department.xml file:

1. Open the template file using an ASCII editor.
2. For each contact that you want to add, add the following strings to the file. Each starts on a separate line:

   <Name>*Mary*</Name>

   <Telephone>*1001*</Telephone>

   Where:

   Specify the contact name between <Name> and </Name>.

   Specify the contact number between <Telephone> and </Telephone>.
3. Save the file and place this file to the provisioning server.

The following shows an example of a Department.xml file:

```
<YealinkIPPhoneDirectory>
  <DirectoryEntry>
    <Name>Test1</Name>
    <Telephone>23000</Telephone>
  </DirectoryEntry>
  <DirectoryEntry>
    <Name>Test2</Name>
    <Telephone>303</Telephone>
    <Telephone>915980830849</Telephone>
  </DirectoryEntry>
  <DirectoryEntry>
    <Name>Test3</Name>
    <Telephone>6650</Telephone>
    <Telephone>915980830849</Telephone>
  </DirectoryEntry>
</YealinkIPPhoneDirectory>
```

Note

Yealink supplies a phonebook generation tool to generate a remote XML phone book. For more information, refer to *Yealink Phonebook Generation Tool User Guide*, available online: http://www.yealink.com/DocumentDownload.aspx?CateId=142&flag=142.

Troubleshooting

This chapter provides an administrator with general information for troubleshooting some common problems that he (or she) may encounter while using IP phones.

Troubleshooting Methods

IP phones can provide feedback in a variety of forms such as log files, packets, status indicators and so on, which can help an administrator more easily find the system problem and fix it.

The following are helpful for better understanding and resolving the working status of the IP phone.

- Viewing Log Files
- Capturing Packets
- Enabling Watch Dog Feature
- Getting Information from Status Indicators
- Analyzing Configuration File

Viewing Log Files

If your IP phone encounters some problems, commonly the log files are needed. You can export the log files to a syslog server or the local system. You can also specify the severity level of the log to be reported to a log file. The default system log level is 3.

In the configuration files, you can use the following parameters to configure system log settings:

- **syslog.mode** – Specify the system log to be exported to a 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_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

Procedure

Log setting can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configures the syslog mode. **Parameters:** syslog.mode Configures the IP address or domain name of the syslog server where to export the log files. **Parameters:** syslog.server Configures the severity level of the logs to be reported to a log file. **Parameters:** syslog.log_level
Local	Web User Interface	Configures the syslog mode. Configures the IP address or domain name of the syslog server where to export the log files. Configures the severity level of the logs to be reported to a log file. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-config&q=load

Details of Configuration Parameters:

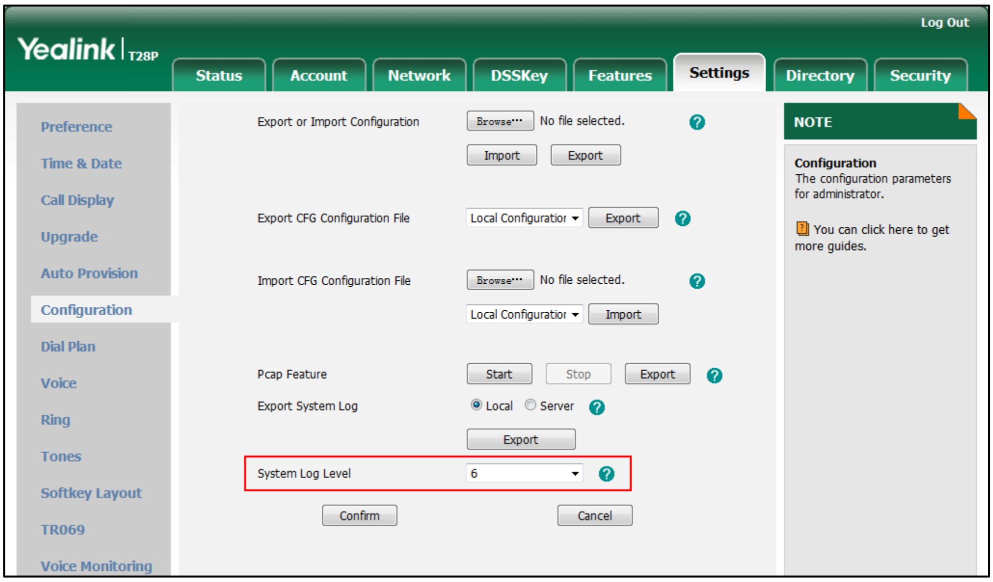
Parameters	Permitted Values	Default
syslog.mode	**0 or 1**	**0**
Description: Configures the IP phone to export log files to a syslog server or the local system. **0**-Local **1**-Server **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Settings->Configuration->Export System Log **Phone User Interface:**		

Parameters	Permitted Values	Default
None		
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 = 192.168.1.50 **Note:** It works only if the parameter "syslog.mode" is set to 1 (Server). If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Settings->Configuration->Server Name **Phone User Interface:** None		
syslog.log_level	**Integer from 0 to 6**	**3**
Description: Configures the detail level of syslog information to be exported. **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 **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Settings->Configuration->System Log Level **Phone User Interface:** None		

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.

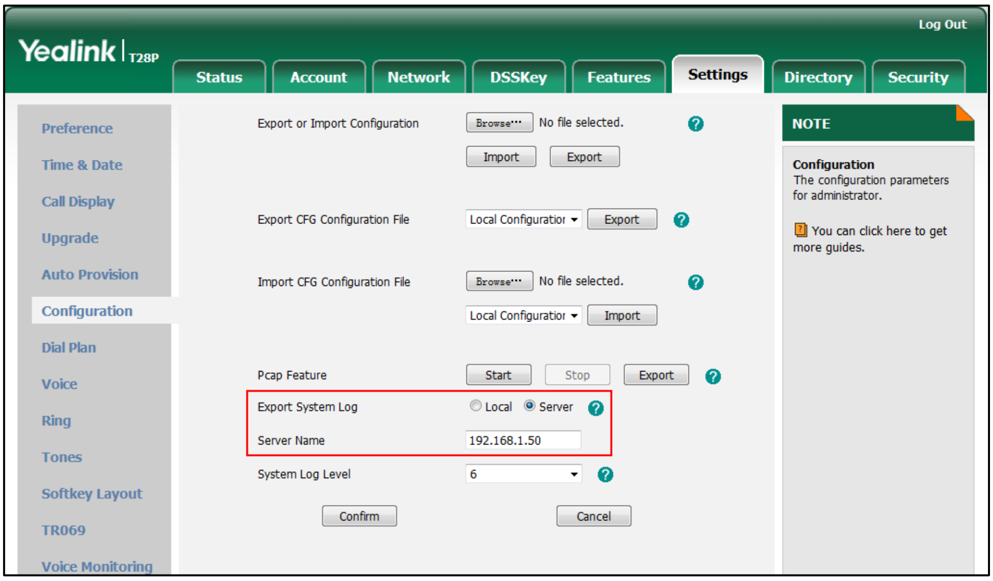
   The system log level is set as 6, the informational level.

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.

To configure the phone to export the system log to a syslog server via web user interface:

1. Click on **Settings**->**Configuration**.
2. Mark the **Server** radio box in the **Export System Log** field.

3. Enter the IP address or domain name of the syslog server in the **Server Name** field.



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

   A dialog box pops up to prompt “Do you want to restart your machine?”. The configuration will take effect after a reboot.

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

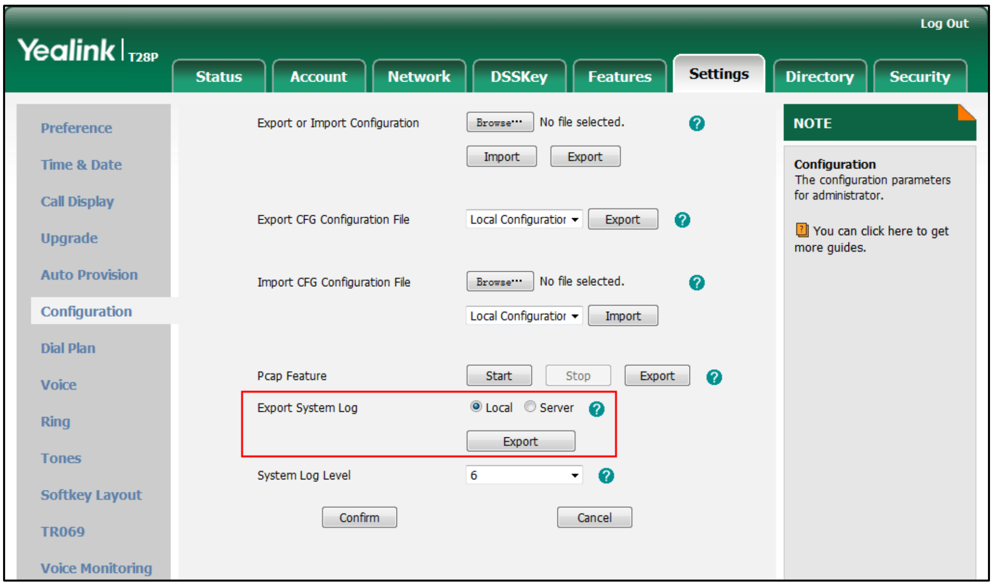
   The system log will be exported successfully to the desired syslog server after a reboot.

6. Reproduce the issue.

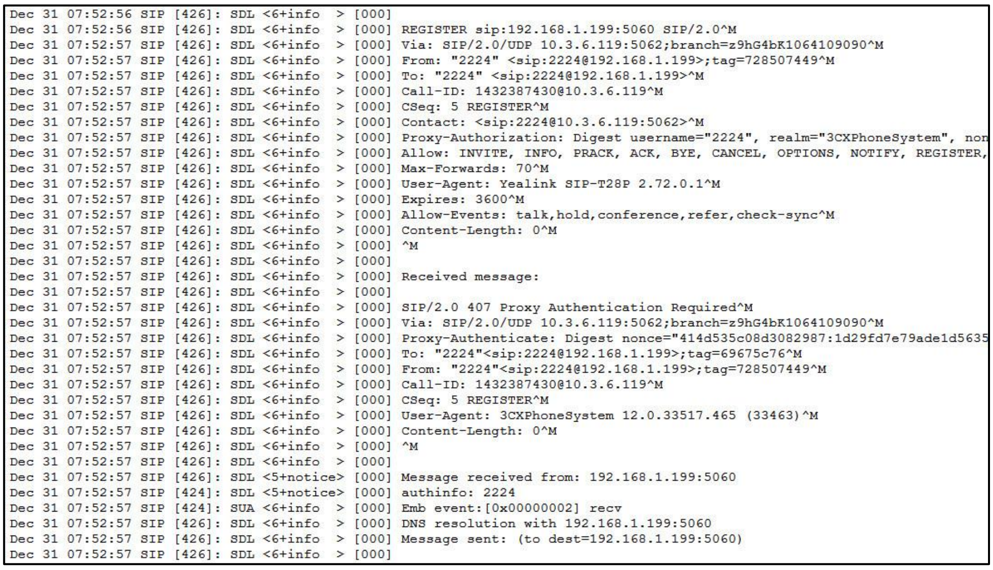
To export a log file to the local system via web user interface:

1. Click on **Settings**->**Configuration**.
2. Mark the **Local** radio box in the **Export System Log** field.
3. Reproduce the issue.

4. Click **Export** to open file download window, and then save the file to your local system.



The following figure shows a portion of a log file- an account registration:



```
Dec 31 07:52:56 SIP [426]: SDL <6+info  > [000]
Dec 31 07:52:56 SIP [426]: SDL <6+info  > [000] REGISTER sip:192.168.1.199:5060 SIP/2.0^M
Dec 31 07:52:57 SIP [426]: SDL <6+info  > [000] Via: SIP/2.0/UDP 10.3.6.119:5062;branch=z9hG4bK1064109090^M
Dec 31 07:52:57 SIP [426]: SDL <6+info  > [000] From: "2224" <sip:2224@192.168.1.199>;tag=728507449^M
Dec 31 07:52:57 SIP [426]: SDL <6+info  > [000] To: "2224" <sip:2224@192.168.1.199>^M
Dec 31 07:52:57 SIP [426]: SDL <6+info  > [000] Call-ID: 1432387430@10.3.6.119^M
Dec 31 07:52:57 SIP [426]: SDL <6+info  > [000] CSeq: 5 REGISTER^M
Dec 31 07:52:57 SIP [426]: SDL <6+info  > [000] Contact: <sip:2224@10.3.6.119:5062>^M
Dec 31 07:52:57 SIP [426]: SDL <6+info  > [000] Proxy-Authorization: Digest username="2224", realm="3CXPhoneSystem", non
Dec 31 07:52:57 SIP [426]: SDL <6+info  > [000] Allow: INVITE, INFO, PRACK, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REGISTER,
Dec 31 07:52:57 SIP [426]: SDL <6+info  > [000] Max-Forwards: 70^M
Dec 31 07:52:57 SIP [426]: SDL <6+info  > [000] User-Agent: Yealink SIP-T28P 2.72.0.1^M
Dec 31 07:52:57 SIP [426]: SDL <6+info  > [000] Expires: 3600^M
Dec 31 07:52:57 SIP [426]: SDL <6+info  > [000] Allow-Events: talk,hold,conference,refer,check-sync^M
Dec 31 07:52:57 SIP [426]: SDL <6+info  > [000] Content-Length: 0^M
Dec 31 07:52:57 SIP [426]: SDL <6+info  > [000] ^M
Dec 31 07:52:57 SIP [426]: SDL <6+info  > [000]
Dec 31 07:52:57 SIP [426]: SDL <6+info  > [000] Received message:
Dec 31 07:52:57 SIP [426]: SDL <6+info  > [000]
Dec 31 07:52:57 SIP [426]: SDL <6+info  > [000] SIP/2.0 407 Proxy Authentication Required^M
Dec 31 07:52:57 SIP [426]: SDL <6+info  > [000] Via: SIP/2.0/UDP 10.3.6.119:5062;branch=z9hG4bK1064109090^M
Dec 31 07:52:57 SIP [426]: SDL <6+info  > [000] Proxy-Authenticate: Digest nonce="414d535c08d3082987:1d29fd7e79ade1d5635
Dec 31 07:52:57 SIP [426]: SDL <6+info  > [000] To: "2224"<sip:2224@192.168.1.199>;tag=69675c76^M
Dec 31 07:52:57 SIP [426]: SDL <6+info  > [000] From: "2224"<sip:2224@192.168.1.199>;tag=728507449^M
Dec 31 07:52:57 SIP [426]: SDL <6+info  > [000] Call-ID: 1432387430@10.3.6.119^M
Dec 31 07:52:57 SIP [426]: SDL <6+info  > [000] CSeq: 5 REGISTER^M
Dec 31 07:52:57 SIP [426]: SDL <6+info  > [000] User-Agent: 3CXPhoneSystem 12.0.33517.465 (33463)^M
Dec 31 07:52:57 SIP [426]: SDL <6+info  > [000] Content-Length: 0^M
Dec 31 07:52:57 SIP [426]: SDL <6+info  > [000] ^M
Dec 31 07:52:57 SIP [426]: SDL <6+info  > [000]
Dec 31 07:52:57 SIP [426]: SDL <5+notice> [000] Message received from: 192.168.1.199:5060
Dec 31 07:52:57 SIP [424]: SDL <5+notice> [000] authinfo: 2224
Dec 31 07:52:57 SIP [424]: SUA <6+info  > [000] Emb event:[0x00000002] recv
Dec 31 07:52:57 SIP [426]: SDL <6+info  > [000] DNS resolution with 192.168.1.199:5060
Dec 31 07:52:57 SIP [426]: SDL <6+info  > [000] Message sent: (to dest=192.168.1.199:5060)
Dec 31 07:52:57 SIP [426]: SDL <6+info  > [000]
```

Capturing Packets

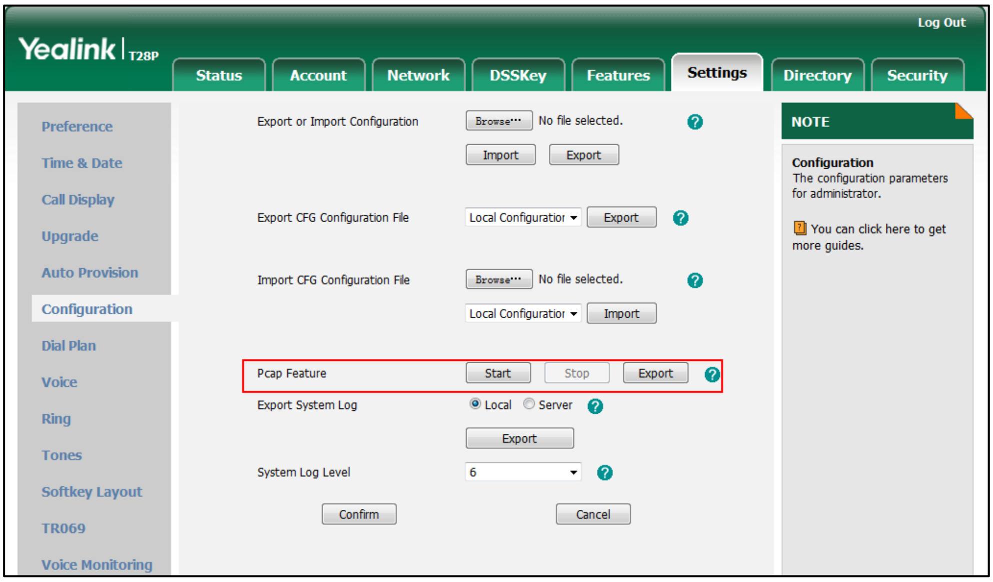
You can capture packet in two ways: capturing the packet via web user interface or using the Ethernet software. You can analyze the packet captured for troubleshooting purpose.

To capture packets via web user interface:

1. Click on **Settings**->**Configuration**.
2. Click **Start** to start capturing signal traffic.
3. Reproduce the issue to get stack traces.

4. Click **Stop** to stop capturing.

5. Click **Export** to open the file download window, and then save the file to your local system.



To capture packets using the Ethernet software:

Connect the Internet port of the IP phone and the PC to the same HUB, and then use Sniffer, Ethereal or Wireshark software to capture the signal traffic.

Enabling Watch Dog Feature

The IP phone provides a troubleshooting feature called "Watch Dog", which helps you monitor the IP phone status and provides the ability to get stack traces from the last time the IP phone failed. If Watch Dog feature is enabled, the IP phone will automatically reboot when it detects a fatal failure. This feature can be configured using the configuration files or via web user interface.

You can use the "watch_dog.enable" parameter to configure watch dog feature in the configuration files.

Procedure

Watch Dog can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure Watch Dog feature. **Parameter:** watch_dog.enable
Local	Web User Interface	Configure Watch Dog feature. Navigate to:

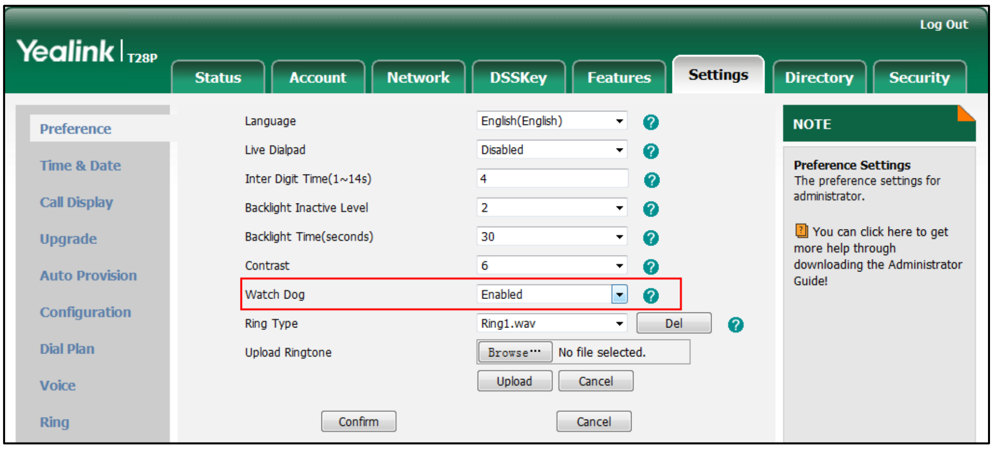
		http://<phoneIPAddress>/servlet?p=settings-preference&q=load

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
watch_dog.enable	0 or 1	1
Description : Enables or disables Watch Dog feature. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the IP phone will reboot automatically when the system is broken down. **Web User Interface:** Settings->Preference->Watch Dog **Phone User Interface:** None		

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 **Watch Dog**.



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

Getting Information from Status Indicators

Status indicators may consist of the power LED, MESSAGE key LED, line key indicator, headset key indicator and the on-screen icon.

The following shows two examples of obtaining the IP phone information from status indicators:

- If a LINK failure of the IP phone is detected, a prompting message "Network Unavailable" and the icon will appear on the LCD screen.
- If a voice mail is received, the MESSAGE key LED illuminates.

For more information on the icons, refer to Reading Icons on page 16.

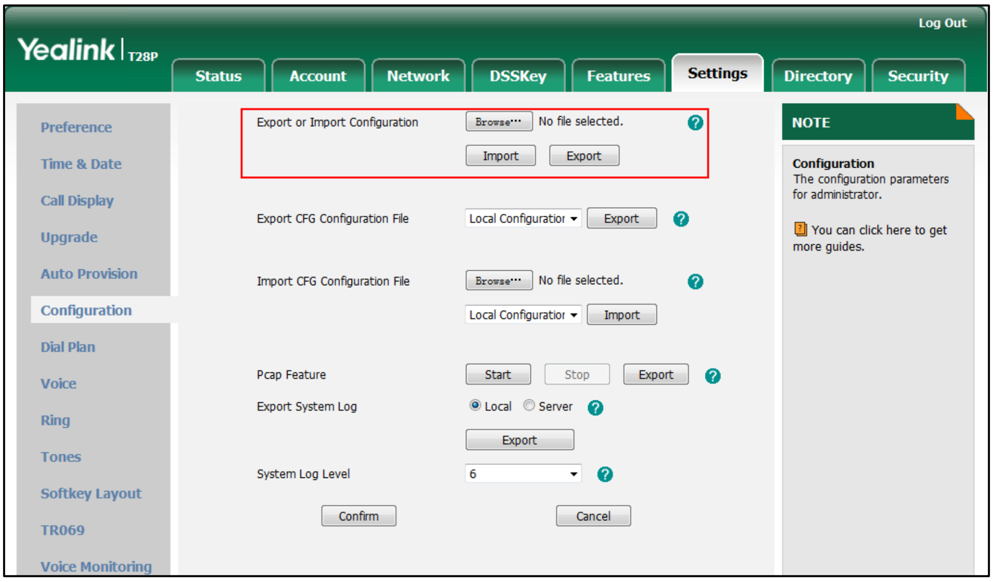
Analyzing Configuration File

Wrong configurations may have an impact on your phone use. You can export configuration file to check the current configuration of the IP 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 and <mac>-local.cfg. The <mac>-all.cfg configuration file contains all changes made via phone user interface, web user interface and using configuration files. The <mac>-local.cfg configuration file contains changes made via phone user interface and web user interface. The config.bin file is an encrypte file. For more information on config.bin file, contact your Yealink reseller.

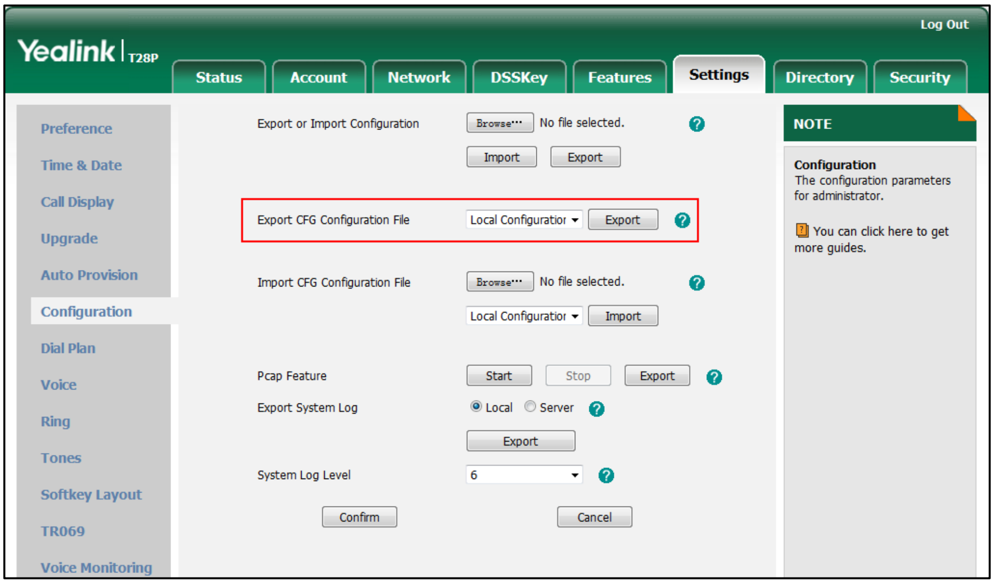
To export BIN configuration files via web user interface:

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.



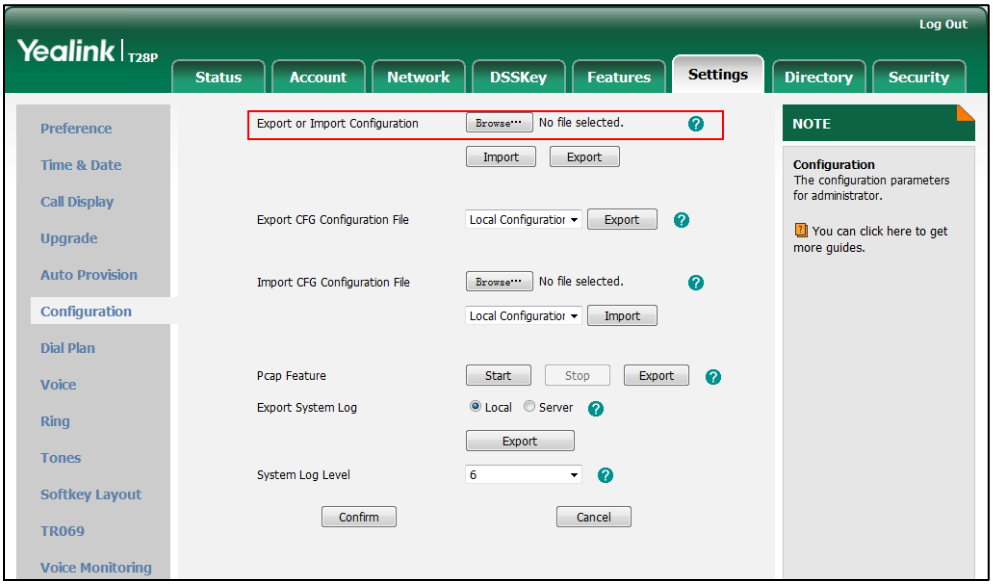
To export CFG configuration files via web user interface:

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 a BIN configuration file via web user interface:

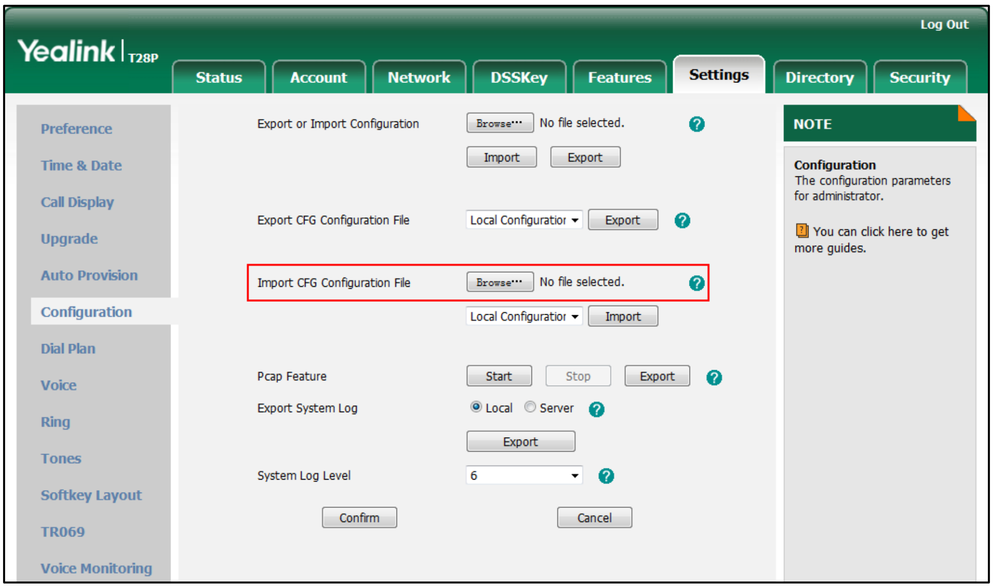
1. Click on **Settings**->**Configuration**.
2. In the **Export or Import Configuration** block, click **Browse** to locate a BIN configuration file from your local system.



3. Click **Import** to import the configuration file.

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 phone. Upon encountering a scenario not listed in this section, contact your Yealink reseller for further support.

Why is the LCD screen blank?

Do one of the following:

- Ensure that the IP phone is properly plugged into a functional AC outlet.
- Ensure that the IP phone is plugged into a socket controlled by a switch that is on.
- If the IP phone is plugged into a power strip, try plugging it directly into a wall outlet.
- If your phone is PoE powered, ensure that you are using a PoE-compliant switch or hub.

Why doesn't the IP phone get an IP address?

Do one of the following:

- Ensure that the Ethernet cable is plugged into the Internet port on the IP phone and the Ethernet cable is not loose.
- Ensure that the Ethernet cable is not damaged.
- Ensure that the IP address and related network parameters are set correctly.
- Ensure that your network switch or hub is operational.

Why does the IP phone display "No Service"?

The LCD screen prompts "No Service" message when there is no available SIP account on the IP phone.

Do one of the following:

- Ensure that an account is actively registered on the IP phone at the path **Menu**->**Status**->**More**->**Accounts**.
- Ensure that the SIP account parameters have been configured correctly.

How do I find the basic information of the IP phone?

Press the **OK** key when the IP phone is idle to check the basic information (e.g., IP address, MAC address and firmware version).

Why doesn't the IP phone upgrade firmware successfully?

Do one of the following:

- Ensure that the target firmware is not the same as the current firmware.
- Ensure that the target firmware is applicable to the IP phone model.
- Ensure that the current or the target firmware is not protected.
- Ensure that the power is on and the network is available in the process of upgrading.
- Ensure that the web browser is not closed or refreshed when upgrading firmware via web user interface.

Why doesn't the IP phone display time and date correctly?

Check if the IP phone is configured to obtain the time and date from the NTP server automatically. If your phone is unable to access the NTP server, configure the time and date manually.

Why do I get poor sound quality during a call?

If you have poor sound quality/acoustics like intermittent voice, low volume, echo or other 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.

What is the difference between a remote phone book and a local phone book?

A remote phone book is placed on a server, while a local phone book is placed on the IP phone flash. A remote phone book can be used by everyone that can access the server, while a local phone book can only be used by a specific phone. A remote phone book is always used as a central phone book for a company; each employee can load it to obtain the real-time data from the same server.

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.

How to reboot the IP phone remotely?

IP phones support remote reboot by a SIP NOTIFY message with "Event: check-sync" header. When receiving a NOTIFY message with the parameter "reboot=true", the IP phone reboots 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
```

Why does the IP phone use DOB format logo file instead of popular BMP, JPG and so on?

The IP phone only uses logo file in DOB format, as the DOB format file has a high compression ratio (the size of the uncompressed file compared to that of the compressed file) and can be stored in smaller space. Tools for converting BMP format to DOB format are available. For more information, refer to *Yealink_SIP-T2_Series_T4_Series_IP_Phones_Auto_Provisioning_Guide*, available online: http://www.yealink.com/DocumentDownload.aspx?CateId=142&flag=142.

How to increase or decrease the volume?

Press the volume key to increase or decrease the ringer volume when the IP phone is idle, or to adjust the volume of engaged audio device (handset, speakerphone or headset) when there is an active call in progress.

What will happen if I connect both PoE cable and power adapter? Which has the higher priority?

IP phones manufactured before February 2010 will use the power adapter preferentially, while those made later will use PoE preferentially.

What is auto provisioning?

Auto provisioning refers to the update of IP phones, including update on configuration parameters, local phone book, firmware and so on. You can use auto provisioning on a single phone, but it makes more sense in mass deployment.

What is PnP?

Plug and Play (PnP) is a method for IP phones to acquire the provisioning server address. With PnP enabled, the IP phone broadcasts the PnP SUBSCRIBE message to obtain a provisioning server address during startup. Any SIP server recognizing the message will respond with the preconfigured provisioning server address, so the IP phone will be able to download the CFG files from the provisioning server. PnP depends on support from a SIP server.

Why doesn't the IP phone update the configuration?

Do one of the following:

- Ensure that the configuration is set correctly.
- Reboot the phone. Some configurations require a reboot to take effect.
- Ensure that the configuration is applicable to the IP phone model.
- The configuration may depend on support from a server.

What do "on code" and "off code" mean?

They are codes that the IP phone sends to the server when a certain action takes place. On code is used to activate a feature on the server side, while off code is used to deactivate a feature on the server side.

For example, if you set the Always Forward on code to be *78 (may vary on different servers), and the target number to be 201. When you enable Always Forward on the IP phone, the IP phone sends *78201 to the server, and then the server will enable 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 157 and Anonymous Call Rejection on page 161.

How to solve the IP conflict problem?

Do one of the following:

- Reset another available IP address for the IP phone.
- Check network configuration via phone user interface at the path **Menu**->**Settings**->**Advanced Settings**->**Network**->**WAN Port**->**IPv4**. If Static IP Client is selected, select DHCP IP Client instead.

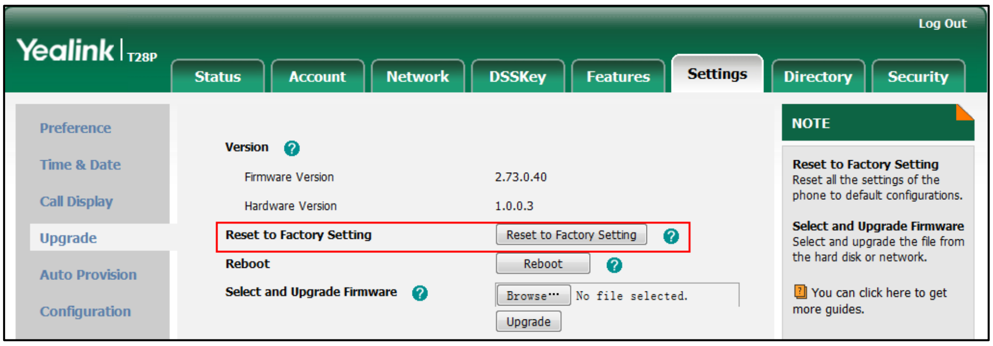
How to reset the IP phone to factory configurations?

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 phone via web user interface:

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

   The web user interface prompts the message "Do you want to reset to factory?".



3. Click **OK** to confirm the resetting.

   The IP phone will be reset to factory sucessfully after startup.

Note Reset of your phone may take a few minutes. Do not power off until the phone starts up successfully.

How to restore the administrator password?

Factory reset can restore the original password. All custom settings will be overwritten after reset.

What are the main differences among SIP-T28P, IP-T26P, SIP-T22P and SIP-T20P IP phones?

Phone Model	LCD	Logo Display	Line Key	Memory Key	SMS	XML Browser
SIP-T28P	320*160 pixel	236*82 pixel	6	10	Support	Support
SIP-T26P	132*64 pixel	132*64 pixel	3	10	Support	Support
SIP-T22P	132*64 pixel	132*64 pixel	3	/	Support	Support

Phone Model	LCD	Logo Display	Line Key	Memory Key	SMS	XML Browser
SIP-T20P	3-line (2*15 characters and an icon line)	Text log	2	/	/	Support (Non UI)

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 phone.

FAC (Feature Access Code)--special patterns of characters that are dialed from a phone keypad to invoke particular features.

HTTP (Hypertext Transfer Protocol)--used to request and transmit data on the World Wide Web.

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer)--a widely-used communications protocol for secure communication over a network.

IEEE (Institute of Electrical and Electronics Engineers)--a non-profit professional association headquartered in New York City that is dedicated to advancing technological innovation and excellence.

LAN (Local Area Network)--used to interconnects network devices in a limited area such as a home, school, computer laboratory, or office building.

MIB (Management Information Base)--a virtual database used for managing the entities in a communications network.

OID (Object Identifier)--assigned to an individual object within a MIB.

PnP (Plug and Play)--a term used to describe the characteristic of a computer bus, or device specification, which facilitates the discovery of a hardware component in a system, without the need for physical device configuration, or user intervention in resolving resource conflicts.

ROM (Read-only Memory)--a class of storage medium used in computers and other electronic devices.

RTP (Real-time Transport Protocol)--provides end-to-end service for real-time data.

TCP (Transmission Control Protocol)--a transport layer protocol used by applications that require guaranteed delivery.

UDP (User Datagram Protocol)--a protocol offers non-guaranteed datagram delivery.

URI (Uniform Resource Identifier)--a compact sequence of characters that identifies an abstract or physical resource.

URL (Uniform Resource Locator)--specifies the address of an Internet resource.

VLAN (Virtual LAN)-- a group of hosts with a common set of requirements, which communicate as if they were attached to the same broadcast domain, regardless of their physical location.

VoIP (Voice over Internet Protocol)--a family of technologies used for the delivery of voice communications and multimedia sessions over IP networks.

WLAN (Wireless Local Area Network)--a type of local area network that uses high-frequency radio waves rather than wires to communicate between nodes.

XML-RPC (Remote Procedure Call Protocol)--which uses XML to encode its calls and HTTP as a transport mechanism.

Appendix B: Time Zones

Time Zone	Time Zone Name
–11:00	Samoa
–10:00	United States-Hawaii-Aleutian
–09:30	French Polynesia
–09:00	United States-Alaska Time
–08:00	Canada(Vancouver, Whitehorse)
–08:00	Mexico(Tijuana, Mexicali)
–08:00	United States-Pacific Time
–07:00	Canada(Edmonton, Calgary)
–07:00	Mexico(Mazatlan, Chihuahua)
–07:00	United States-Mountain Time
–07:00	United States-MST no DST
–06:00	Canada-Manitoba(Winnipeg)
–06:00	Chile(Easter Islands)
–06:00	Mexico(Mexico City, Acapulco)
–06:00	United States-Central Time
–05:00	Bahamas(Nassau)
–05:00	Canada(Montreal, Ottawa, Quebec)
–05:00	Cuba(Havana)
–05:00	United States-Eastern Time
–04:30	Venezuela(Caracas)
–04:00	Canada(Halifax, Saint John)
–04:00	Chile(Santiago)
–04:00	Paraguay(Asuncion)
–04:00	United Kingdom-Bermuda(Bermuda)
–04:00	United Kingdom(Falkland Islands)
–04:00	Trinidad&Tobago
–03:30	Canada-New Foundland(St.Johns)
–03:00	Denmark-Greenland(Nuuk)
–03:00	Argentina(Buenos Aires)
–03:00	Brazil(no DST)
–03:00	Brazil(DST)
–02:30	Newfoundland and Labrador
–02:00	Brazil(no DST)
–01:00	Portugal(Azores)
0	GMT
0	Greenland
0	Denmark-Faroe Islands(Torshavn)
0	Ireland(Dublin)
0	Portugal(Lisboa, Porto, Funchal)

Time Zone	Time Zone Name
0	Spain-Canary Islands(Las Palmas)
0	United Kingdom(London)
0	Morocco
+01:00	Albania(Tirane)
+01:00	Austria(Vienna)
+01:00	Belgium(Brussels)
+01:00	Caicos
+01:00	Chad
+01:00	Spain(Madrid)
+01:00	Croatia(Zagreb)
+01:00	Czech Republic(Prague)
+01:00	Denmark(Kopenhagen)
+01:00	France(Paris)
+01:00	Germany(Berlin)
+01:00	Hungary(Budapest)
+01:00	Italy(Rome)
+01:00	Luxembourg(Luxembourg)
+01:00	Macedonia(Skopje)
+01:00	Netherlands(Amsterdam)
+01:00	Namibia(Windhoek)
+02:00	Estonia(Tallinn)
+02:00	Finland(Helsinki)
+02:00	Gaza Strip(Gaza)
+02:00	Greece(Athens)
+02:00	Israel(Tel Aviv)
+02:00	Jordan(Amman)
+02:00	Latvia(Riga)
+02:00	Lebanon(Beirut)
+02:00	Moldova(Kishinev)
+02:00	Russia(Kaliningrad)
+02:00	Romania(Bucharest)
+02:00	Syria(Damascus)
+02:00	Turkey(Ankara)
+02:00	Ukraine(Kyiv, Odessa)
+03:00	East Africa Time
+03:00	Iraq(Baghdad)
+03:00	Russia(Moscow)
+03:30	Iran(Teheran)
+04:00	Armenia(Yerevan)
+04:00	Azerbaijan(Baku)
+04:00	Georgia(Tbilisi)
+04:00	Kazakhstan(Aktau)

Time Zone	Time Zone Name
+04:00	Russia(Samara)
+04:30	Afghanistan(Kabul)
+05:00	Kazakhstan(Aqtobe)
+05:00	Kyrgyzstan(Bishkek)
+05:00	Pakistan(Islamabad)
+05:00	Russia(Chelyabinsk)
+05:30	India(Calcutta)
+05:45	Nepal(Katmandu)
+06:00	Kazakhstan(Astana, Almaty)
+06:00	Russia(Novosibirsk, Omsk)
+06:30	Myanmar(Naypyitaw)
+07:00	Russia(Krasnoyarsk)
+07:00	Thailand(Bangkok)
+08:00	China(Beijing)
+08:00	Singapore(Singapore)
+08:00	Australia(Perth)
+08:00	Russian(Irkutsk, Ulan-Ude)
+08:45	Eucla
+09:00	Korea(Seoul)
+09:00	Japan(Tokyo)
+09:00	Russian(Yakutsk, Chita)
+09:30	Australia(Adelaide)
+09:30	Australia(Darwin)
+10:00	Australia(Sydney, Melbourne, Canberra)
+10:00	Australia(Brisbane)
+10:00	Australia(Hobart)
+10:00	Russia(Vladivostok)
+10:30	Australia(Lord Howe Islands)
+11:00	New Caledonia(Noumea)
+11:00	Russia(Srednekolymsk Time)
+11:30	Norfolk Island
+12:00	New Zealand(Wellington, Auckland)
+12:00	Russian(Kamchatka Time)
+12:45	New Zealand(Chatham Islands)
+13:00	Tonga(Nukualofa)
+13:30	Chatham Islands
+14:00	Kiribati

Appendix C: Trusted Certificates

Yealink IP 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 457.

Appendix D: Configuring DSS Key

This section provides the DSS key parameters you can configure on IP phones. DSS key consists of memory key, line key and programable key. The following table lists the number of DSS keys you can configure for each phone model:

Phone Model	Line Key	Memory Key	Programable Key
SIP-T28P	6	10	14
SIP-T26P	3	10	14
SIP-T22P	3	/	13
SIP-T20P	2	/	9

Note The programable key takes effect only if the IP phone is idle.

DSS key can be assigned with various key features. The parameters of the DSS key are detailed in the following:

Parameter- memorykey.X.type	**Configuration File** <y0000000000xx>.cfg
Parameter- linekey.X.type	
Parameter- programablekey.X.type	
Description	Configures key feature for the DSS key. For memory keys: X ranges from 1 to 10 (for SIP-T28/T26P). For line keys: X ranges from 1 to 6 (for SIP-T28P) X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). For programable keys: X ranges from 1 to 14 (for SIP-T28/T26P) X=1-10, 14 (for SIP-T22P) X=5-12, 14 (for SIP-T20P) **For memory keys:** **Valid types are:** • N/A

	• Conference • Forward • Transfer • Hold • DND • ReCall • SMS • Directed Pickup • Call Park • DTMF • Voice Mail • Speed Dial • Intercom • Line • BLF • URL • Group Listening • XML Group • Group Pickup • Multicast Paging • Record • XML Browser • URL Record • LDAP • Prefix • Zero Touch • Local Group • Custom Button • Phone Lock • Directory **For line keys:** **Valid types are:** • Conference • Forward • Transfer • Hold • DND

	• ReCall • SMS (not applicable to SIP-T20P IP phones) • Directed Pickup • Call Park • DTMF • Voice Mail • Speed Dial • Intercom • Line • BLF • Group Listening • XML Group (not applicable to SIP-T20P IP phones) • Group Pickup • Multicast Paging • Record • XML Browser • Hot Desking • URL Record • LDAP (not applicable to SIP-T20P IP phones) • Prefix • Zero Touch • Local Group • Phone Lock • Directory **For programable keys:** **Valid types are:** • N/A • Forward • DND • ReCall • SMS (not applicable to SIP-T20P IP phones) • Directed Pickup • Spead Dial • XML Group • Group Pickup • XML Browser

	• History • Menu • Switch Account • New SMS (not applicable to SIP-T20P IP phones) • Status • LDAP • Prefix (not applicable to SIP-T20P IP phones) • Zero Touch • Local Directory • Local Group • XML Directory (not applicable to SIP-T20P IP phones) • Phone Lock • Directory
Format	Integer
Default Value	For the memory key, the default value is 0 (N/A). For the line key, the default value is 15 (Line). For programable keys: **For SIP-T28P/T26P IP phones:** When X=1, the default value is 28 (History). When X=2, the default value is 61 (Directory). When X=3, the default value is 5 (DND). When X=4, the default value is 30 (Menu). When X=5, the default value is 28 (History). When X=6, the default value is 61 (Directory). When X=7, the default value is 31 (Switch Account). When X=8, the default value is 31 (Switch Account). When X=9, the default value is 33 (Status). When X=10, the default value is 0 (NA). When X=11, the default value is 0 (NA). When X=12, the default value is 0 (NA). When X=13, the default value is 0 (NA). When X=14, the default value is 2 (Forward). **For SIP-T22P IP phones:**

	When X=1, the default value is 28 (History). When X=2, the default value is 61 (Directory). When X=3, the default value is 5 (DND). When X=4, the default value is 30 (Menu). When X=5, the default value is 28 (History). When X=6, the default value is 61 (Directory). When X=7, the default value is 31 (Switch Account). When X=8, the default value is 31 (Switch Account). When X=9, the default value is 33 (Status). When X=10, the default value is 0 (NA). When X=14, the default value is 2 (Forward). **For SIP-T20P IP phones:** When X=5, the default value is 28 (History). When X=6, the default value is 61 (Directory). When X=7, the default value is 31 (Switch Account). When X=8, the default value is 31 (Switch Account). When X=9, the default value is 33 (Status). When X=10, the default value is 0 (NA). When X=11, the default value is 0 (NA). When X=12, the default value is 0 (NA). When X=14, the default value is 2 (Forward).
Range	Valid values are: **0**-N/A **1**-Conference **2**-Forward **3**-Transfer **4**-Hold **5**-DND **7**-ReCall **8**-SMS **9**-Directed Pickup **10**-Call Park

	11-DTMF **12**-Voice Mail **13**-Speed Dial **14**-Intercom **15**-Line **16**-BLF **17**-URL **18**-Group Listening **22**-XML Group **23**-Group Pickup **24**-Multicast Paging **25**-Record **27**-XML Browser **28**-History **30**-Menu **31**-Switch Account **32**-New SMS (not applicable to SIP-T20P IP phones) **33**-Status **34**-Hot Desking **35**-URL Record **38**-LDAP **40**-Prefix **41**-Zero Touch **43**-Local Directory **45**-Local Group **47**-XML Directory **49**-Custom Button **50**-Phone Lock **61**-Directory
Example	memorykey.1.type = 8

Parameter- memorykey.X.line	**Configuration File** <y0000000000xx>.cfg

Parameter- linekey.X.line Parameter- programablekey.X.line	
Description	Configures the desired line to apply the key feature. For memory keys: X ranges from 1 to 10 (for SIP-T28/T26P). For line keys: X ranges from 1 to 6 (for SIP-T28P) X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). For programable keys: X ranges from 1 to 14 (for SIP-T28/T26P) X=1-10, 14 (for SIP-T22P) X=5-12, 14 (for SIP-T20P) **When assigning the following features, you do not need to configure this parameter:** • DTMF • Prefix • XML Browser • LDAP (not applicable to SIP-T20P) • Conference • Forward • Hold • DND • ReCall • SMS (not applicable to SIP-T20P) • Record • URL Record • Multicast Paging • Group Listening • Local Group • XML Group (not applicable to SIP-T20P) • Hot Desking • Zero Touch • URL (not applicable to SIP-T20P)

	• Phone Lock • Directory
Format	Integer
Default Value	For the memory key and programable key, the default value is not applicable. For the line key, when x=1, the default value is 1. When x=2, the default value is 2. … When x=6, the default value is 6.
Range	**Valid values are**: 1 to 6 (for SIP-T28P) 1 to 3 (for SIP-T26P/T22P) 1 to 2 (for SIP-T20P) 1-Line 1 2-Line 2 … 6-Line 6
Example	memorykey.1.line = 2

Parameter- memorykey.X.value	**Configuration File** <y0000000000xx>.cfg
Parameter- linekey.X.value	
Parameter- programablekey.X.value	
Description	Configures the value for some key features. For memory keys: X ranges from 1 to 10 (for SIP-T28/T26P). For line keys: X ranges from 1 to 6 (for SIP-T28P) X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). For programable keys: X ranges from 1 to 14 (for SIP-T28/T26P) X=1-10, 14 (for SIP-T22P)

	X=5-12, 14 (for SIP-T20P)
Format	String
Default Value	Blank
Range	String within 99 characters
Example	When you assign the Speed Dial to the memory key, this parameter is used to specify the number you want to dial out. memorykey.1.value = 1001

Parameter- linekey.X.label (only applicable to SIP-T28P)	**Configuration File** <y0000000000xx>.cfg
Parameter- programablekey.X.label (X ranges from 1 to 4)	
Description	Configures the label displaying on the LCD screen for each line key and each soft key. This is an optional configuration. For line keys: X ranges from 1 to 6 (for SIP-T28P) X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). For programable keys: X ranges from 1 to 4
Format	String
Default Value	Blank
Range	String within 99 characters
Example	linekey.1.label = Dir

Parameter- memorykey.X.pickup_value	**Configuration File** <y0000000000xx>.cfg
Parameter- linekey.X.pickup_value	
Description	Configures the pickup code for BLF feature.

	This parameter is only applicable to BLF feature. For the memory key, x ranges from 1 to 10. For the line key, x ranges from 1 to 6.
Format	String
Default Value	Blank
Range	String within 256 characters
Example	memorykey.1.pickup_value = *88

Parameter- memorykey.X.xml_phonebook	**Configuration File** <y0000000000xx>.cfg
Parameter- linekey.X.xml_phonebook	
Parameter- programablekey.X.xml_phonebook	
Description	Configures the desired group or remote phone book when multiple groups or remote phone books are configured on the IP phone. This parameter is only applicable to Local Group/XML Group features. For memory keys: X ranges from 1 to 10 (for SIP-T28/T26P). For line keys: X ranges from 1 to 6 (for SIP-T28P) X ranges from 1 to 3 (for SIP-T26P/T22P). X ranges from 1 to 2 (for SIP-T20P). For programable keys: X ranges from 1 to 14 (for SIP-T28/T26P) X=1-10, 14 (for SIP-T22P) X=5-12, 14 (for SIP-T20P) When the key feature is configured as Local Group, valid values are: **0**-All contacts **1**-First local group … **5**-Fifth local group

	When the key feature is configured as XML Group (remote phone book), valid values are: **0**-First XML group **1**-Second XML group … **4**-Fifth XML group
Format	Integer
Default Value	0
Range	0 to 5
Example	Configures the second remote phone book. memorykey.1.xml_phonebook = 1

Appendix E: SIP (Session Initiation Protocol)

This section describes how Yealink IP phones comply with the IETF definition of SIP as described in RFC 3261.

This section contains compliance information in the following:

- RFC and Internet Draft Support
- SIP Request
- SIP Header
- SIP Responses
- SIP Session Description Protocol (SDP) Usage

RFC and Internet Draft Support

The following RFC's and Internet drafts are supported:

- RFC 1321—The MD5 Message-Digest Algorithm
- RFC 1889—RTP Media control
- RFC 2112—Multipart MIME
- RFC 2246—The TLS Protocol Version 1.0
- RFC 2327—SDP: Session Description Protocol
- RFC 2543—SIP: Session Initiation Protocol
- RFC 2616—Hypertext Transfer Protocol -- HTTP/1.1
- RFC 2617—Http Authentication: Basic and Digest access authentication

- RFC 2782—A DNS RR for specifying the location of services (DNS SRV)
- RFC 2806—URLs for Telephone Calls
- RFC 2833—RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
- RFC 2915—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 3266—Support for IPv6 in Session Description Protocol (SDP)
- RFC 3310—HTTP Digest Authentication Using Authentication and Key Agreement (AKA)
- RFC 3311—The Session Initiation Protocol (SIP) UPDATE Method
- RFC 3312—Integration of Resource Management and SIP
- RFC 3313—Private SIP Extensions for Media Authorization
- RFC 3323—A Privacy Mechanism for the Session Initiation Protocol (SIP)
- RFC 3324—Requirements for Network Asserted Identity
- RFC 3325—SIP Asserted Identity
- RFC 3326—The Reason Header Field for the Session Initiation Protocol (SIP)
- RFC 3372—SIP for Telephones (SIP-T): Context and Architectures
- RFC 3420—Internet Media Type message/sipfrag
- RFC 3428—Session Initiation Protocol (SIP) Extension for Instant Messaging
- RFC 3455—Private Header (P-Header) Extensions to the SIP for the 3GPP
- RFC 3486—Compressing the Session Initiation Protocol (SIP)
- RFC 3489—STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)
- RFC 3515—The Session Initiation Protocol (SIP) Refer Method
- RFC 3550—RTP , RTCP, IETF RFC 3550
- RFC 3556—Session Description Protocol (SDP) Bandwidth Modifiers for RTCP Bandwidth
- RFC 3581—An Extension to the SIP for Symmetric Response Routing
- RFC 3608—SIP Extension Header Field for Service Route Discovery During Registration

- RFC 3665—Session Initiation Protocol (SIP) Basic Call Flow Examples
- RFC 3666—SIP Public Switched Telephone Network (PSTN) Call Flows.
- RFC 3680—SIP Event Package for Registrations
- RFC 3702—Authentication, Authorization, and Accounting Requirements for the SIP
- RFC 3711—The Secure Real-time Transport Protocol (SRTP)
- RFC 3725—Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)
- RFC 3842—A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)
- RFC 3856—A Presence Event Package for Session Initiation Protocol (SIP)
- RFC 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 4028—Session Timers in the Session Initiation Protocol (SIP)
- RFC 4235—An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP)
- RFC 4244—An Extension to the SIP for Request History Information
- RFC 4317—Session Description Protocol (SDP) Offer/Answer Examples
- RFC 4353—A Framework for Conferencing with the SIP
- RFC 4475—Session Initiation Protocol (SIP) Torture
- RFC 4485—Guidelines for Authors of Extensions to the SIP
- RFC 4504—SIP Telephony Device Requirements and Configuration
- RFC 4566—SDP: Session Description Protocol.
- RFC 4568—Session Description Protocol (SDP) Security Descriptions for Media Streams
- RFC 4575—A SIP Event Package for Conference State
- RFC 4579—SIP Call Control - Conferencing for User Agents
- RFC 4662—A SIP Event Notification Extension for Resource Lists
- RFC 5009—P-Early-Media Header
- RFC 5079—Rejecting Anonymous Requests in SIP
- RFC 5359—Session Initiation Protocol Service Examples

- RFC 5589—Session Initiation Protocol (SIP) Call Control - Transfer
- RFC 5763—Framework for Establishing a Secure Real-time Transport Protocol (SRTP)
- RFC 5806—Diversion Indication in SIP
- draft-levy-sip-diversion-04.txt—Diversion Indication in SIP
- draft-ietf-sip-cc-transfer-05.txt—SIP Call Control - Transfer
- draft-anil-sipping-bla-02.txt—Implementing Bridged Line Appearances (BLA) Using Session Initiation Protocol (SIP)
- draft-ietf-sip-privacy-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-ietf-sipping-cc-conferencing-03.txt—SIP Call Control - Conferencing for User Agents
- 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)
- draft-anil-sipping-bla-04.txt—Implementing Multiple Line Appearances using the Session Initiation Protocol (SIP)

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 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	

Method	Supported	Notes
OPTIONS	Yes	
SUBSCRIBE	Yes	
NOTIFY	Yes	
REFER	Yes	
PRACK	Yes	
INFO	Yes	
MESSAGE	Yes	
UPDATE	Yes	
PUBLISH	Yes	

SIP Header

The following SIP request headers are supported:

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	

Method	Supported	Notes
Expires	Yes	
From	Yes	
Max-Forwards	Yes	
Min-SE	Yes	
P-Asserted-Identity	Yes	
P-Preferred-Identity	Yes	
Proxy-Authenticate	Yes	
Proxy-Authorization	Yes	
RAck	Yes	
Record-Route	Yes	
Refer-To	Yes	
Referred-By	Yes	
Remote-Party-ID	Yes	
Replaces	Yes	
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 F: SIP Call Flows

SIP uses six request methods:

- INVITE—Indicates a user is being invited to participate in a call session.
- ACK—Confirms that the client has received a final response to an INVITE request.
- BYE—Terminates a call and can be sent by either the caller or the callee.
- CANCEL—Cancels any pending searches but does not terminate a call that has already been accepted.
- OPTIONS—Queries the capabilities of servers.
- REGISTER—Registers the address listed in the To header field with a SIP server.

The following types of responses are used by SIP and generated by the IP phone or the SIP server:

- SIP 1xx—Informational Responses

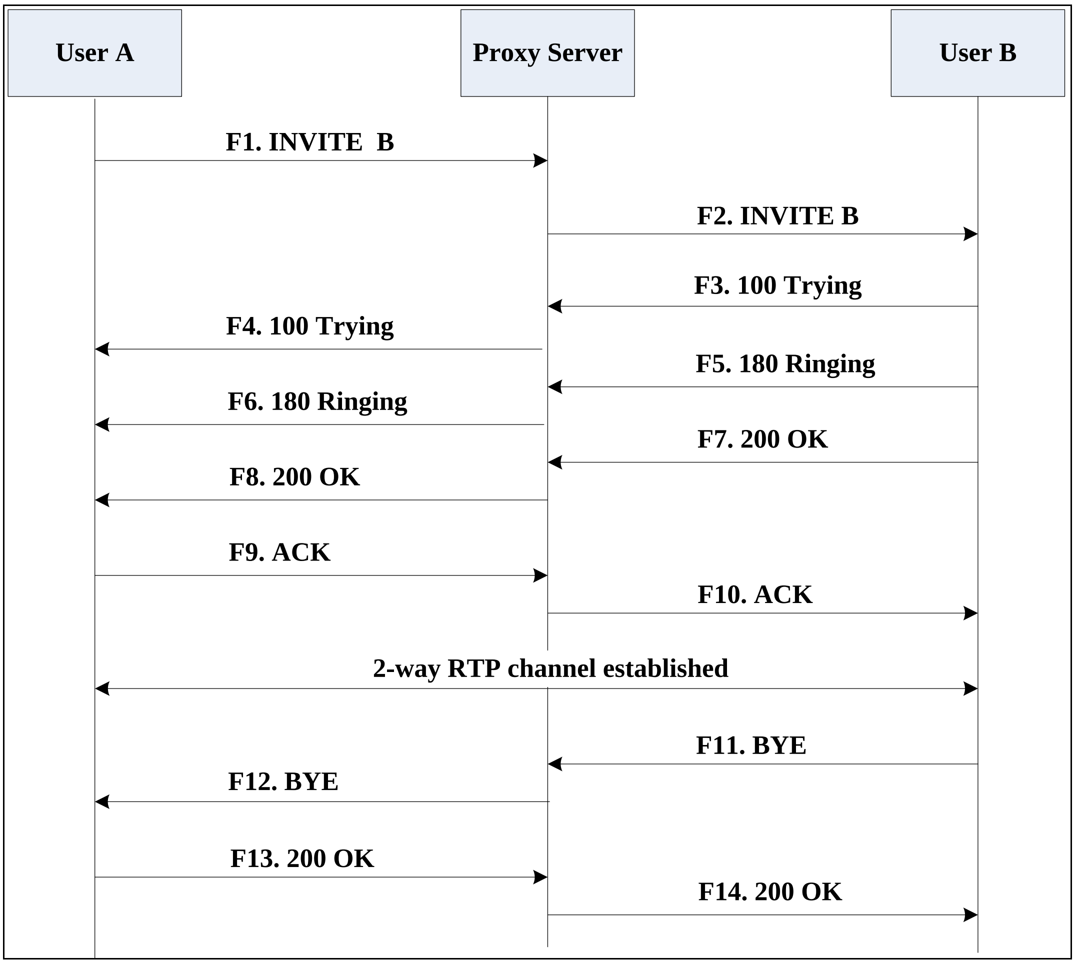
- SIP 2xx—Successful Responses
- SIP 3xx—Redirection Responses
- SIP 4xx—Client Failure Responses
- SIP 5xx—Server Failure Responses
- SIP 6xx—Global Failure Responses

Successful Call Setup and Disconnect

The following figure illustrates the scenario of a successful call. In this scenario, the two end users are User A and User B. User A and User B are located at Yealink SIP IP phones.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.
3. User B hangs up.



Step	Action	Description
F1	INVITE—User A to Proxy Server	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. In the INVITE request: • The IP address of User B is inserted in the Request-URI field. • User A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User A is ready to receive is specified. • The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	100 Trying—User B to Proxy Server	User B sends a SIP 100 Trying response to the proxy server. The 100 Trying response indicates that the INVITE request has been received by User B.
F4	100 Trying—Proxy Server to User A	The proxy server forwards the SIP 100 Trying to User A to indicate that the INVITE request has been received by User B.
F5	180 Ringing—User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the User B is being alerted.
F6	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.

Step	Action	Description
F7	200 OK— User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F8	200OK—Proxy Server to User A	The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the connection has been made.
F9	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F10	ACK—Proxy Server to User B	The proxy server sends the SIP ACK to User B. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.
F11	BYE—User B to Proxy Server	User B terminates the call session by sending a SIP BYE request to the proxy server. The BYE request indicates that User B wants to release the call.
F12	BYE—Proxy Server to User A	The proxy server forwards the SIP BYE request to User A to notify that User B wants to release the call.
F13	200 OK—User A to Proxy Server	User A sends a SIP 200 OK response to the proxy server. The 200 OK response indicates that User A has received the BYE request. The call session is now terminated.
F14	200 OK—Proxy Server to User B	The proxy server forwards the SIP 200 OK response to User B to indicate that User A has received the BYE request. The call session is now terminated.

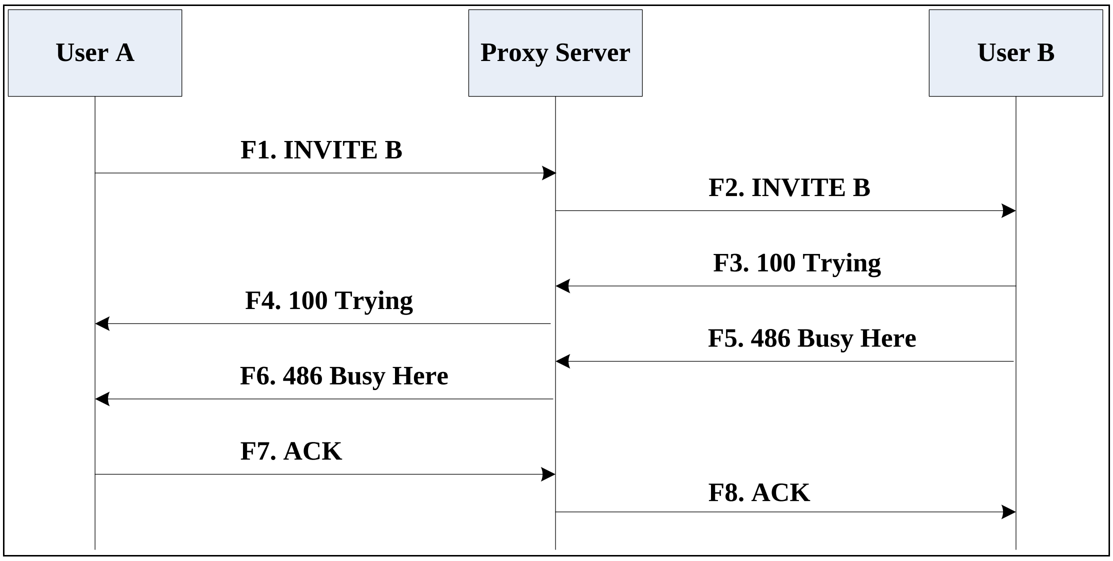
Unsuccessful Call Setup—Called User is Busy

The following figure illustrates the scenario of an unsuccessful call caused by the called user's being busy. In this scenario, the two end users are User A and User B. User A and User B are located at Yealink SIP IP phones.

The call flow scenario is as follows:

1. User A calls User B.
2. User B is busy on the IP phone and unable or unwilling to take another call.

   The call cannot be set up successfully.



Step	Action	Description
F1	INVITE—User A to Proxy Server	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. In the INVITE request: • The IP address of User B is inserted in the Request-URI field. • User A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User A is ready to receive is specified. • The port on which User B is prepared to receive the RTP data is specified.

Step	Action	Description
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. Proxy server forwards the INVITE message to User B.
F3	100 Trying—User B to Proxy Server	User B sends a SIP 100 Trying response to the proxy server. The 100 Trying response indicates that the INVITE request has been received by User B.
F4	100 Trying—Proxy Server to User A	The proxy server forwards the SIP 100 Trying to User A to indicate that the INVITE request has already been received.
F5	486 Busy Here—User B to Proxy Server	User B sends a SIP 486 Busy Here response to the proxy server. The 486 Busy Here response is a client error response indicating that User B is successfully connected but User B is busy on the IP phone and unable or unwilling to take the call.
F6	486 Busy Here—Proxy Server to User A	The proxy server forwards the 486 Busy Here response to notify User A that User B is busy.
F7	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The SIP ACK message indicates that User A has received the 486 Busy Here message.
F8	ACK—Proxy Server to User B	The proxy server forwards the SIP ACK to User B to indicate that the 486 Busy Here message has already been received.

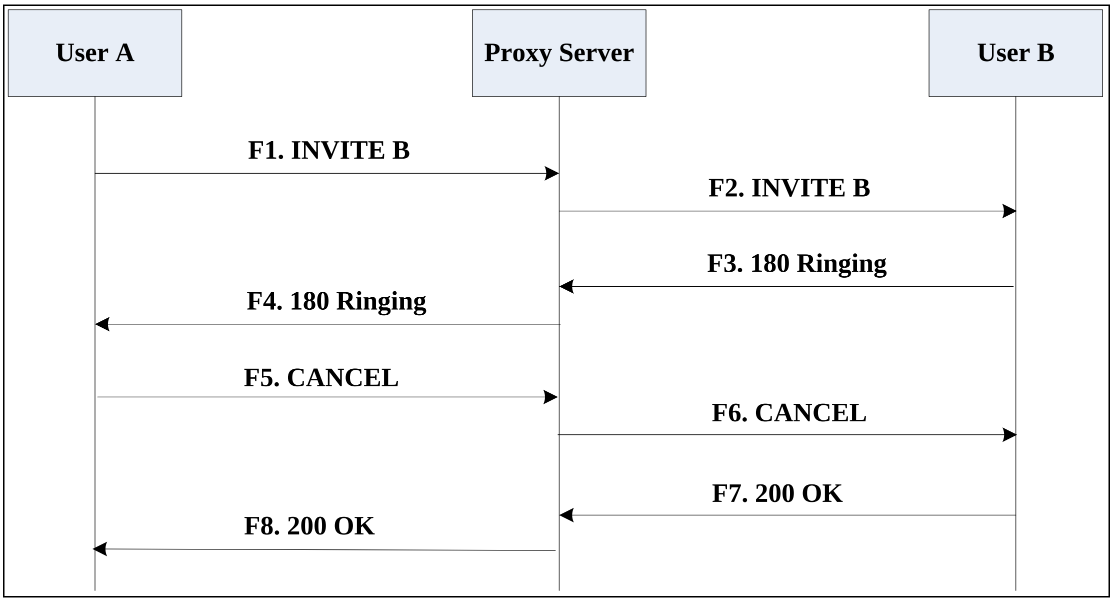
Unsuccessful Call Setup—Called User Does Not Answer

The following figure illustrates the scenario of an unsuccessful call caused by the called user's no answering. In this scenario, the two end users are User A and User B. User A and User B are located at Yealink SIP IP phones.

The call flow scenario is as follows:

1. User A calls User B.
2. User B does not answer the call.
3. User A hangs up.

   The call cannot be set up successfully.



Step	Action	Description
F1	INVITE—User A to Proxy Server	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. In the INVITE request: • The IP address of User B is inserted in the Request-URI field. • User A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User A is ready to receive is specified. • The port on which User B is

Step	Action	Description
		prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. Proxy server forwards the INVITE message to User B.
F3	180 Ringing—User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	CANCEL—User A to Proxy Server	User A sends a SIP CANCEL request to the proxy server after not receiving an appropriate response within the time allocated in the INVITE request. The SIP CANCEL request indicates that User A wants to disconnect the call.
F6	CANCEL—Proxy Server to User B	The proxy server forwards the SIP CANCEL request to notify User B that User A wants to disconnect the call.
F7	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The SIP 200 OK response indicates that User B has received the CANCEL request.
F8	200 OK—Proxy Server to User A	The proxy server forwards the SIP 200 OK response to notify User A that the CANCEL request has been processed successfully.

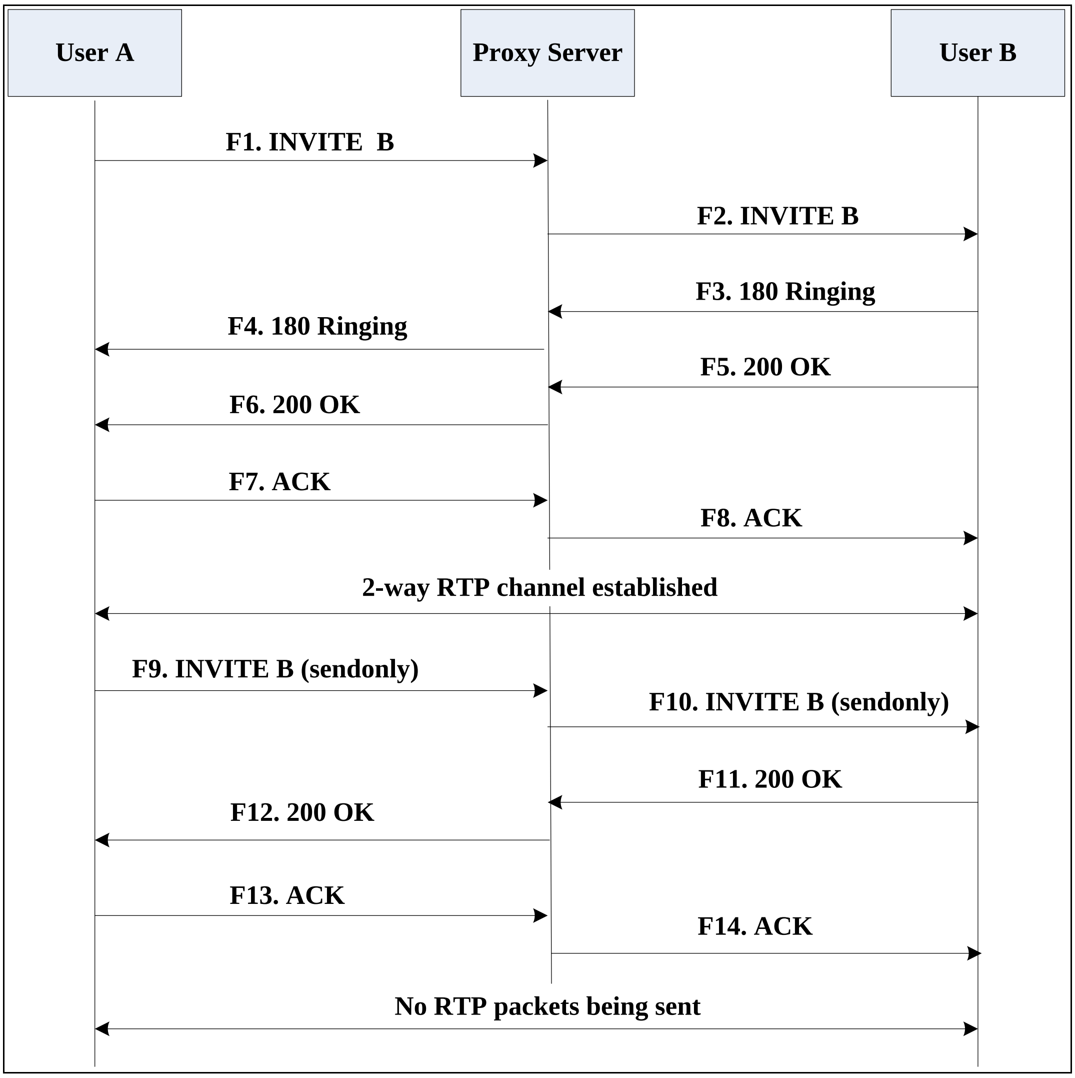
Successful Call Setup and Call Hold

The following figure illustrates a successful call setup and call hold. In this scenario, the two end users are User A and User B. User A and User B are located at Yealink SIP IP phones.

The call flow scenario is as follows:

1. User A calls User B.

2. User B answers the call.
3. User A places User B on hold.



Step	Action	Description
F1	INVITE—User A to Proxy Server	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. In the INVITE request: • The IP address of User B is inserted in the Request-URI field. • User A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted

Step	Action	Description
		in the Call-ID field. ● The transaction number within a single call leg is identified in the CSeq field. ● The media capability User A is ready to receive is specified. ● The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	180 Ringing—User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies the proxy server that the connection has been made.
F6	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the connection has been made.
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

Step	Action	Description
		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.

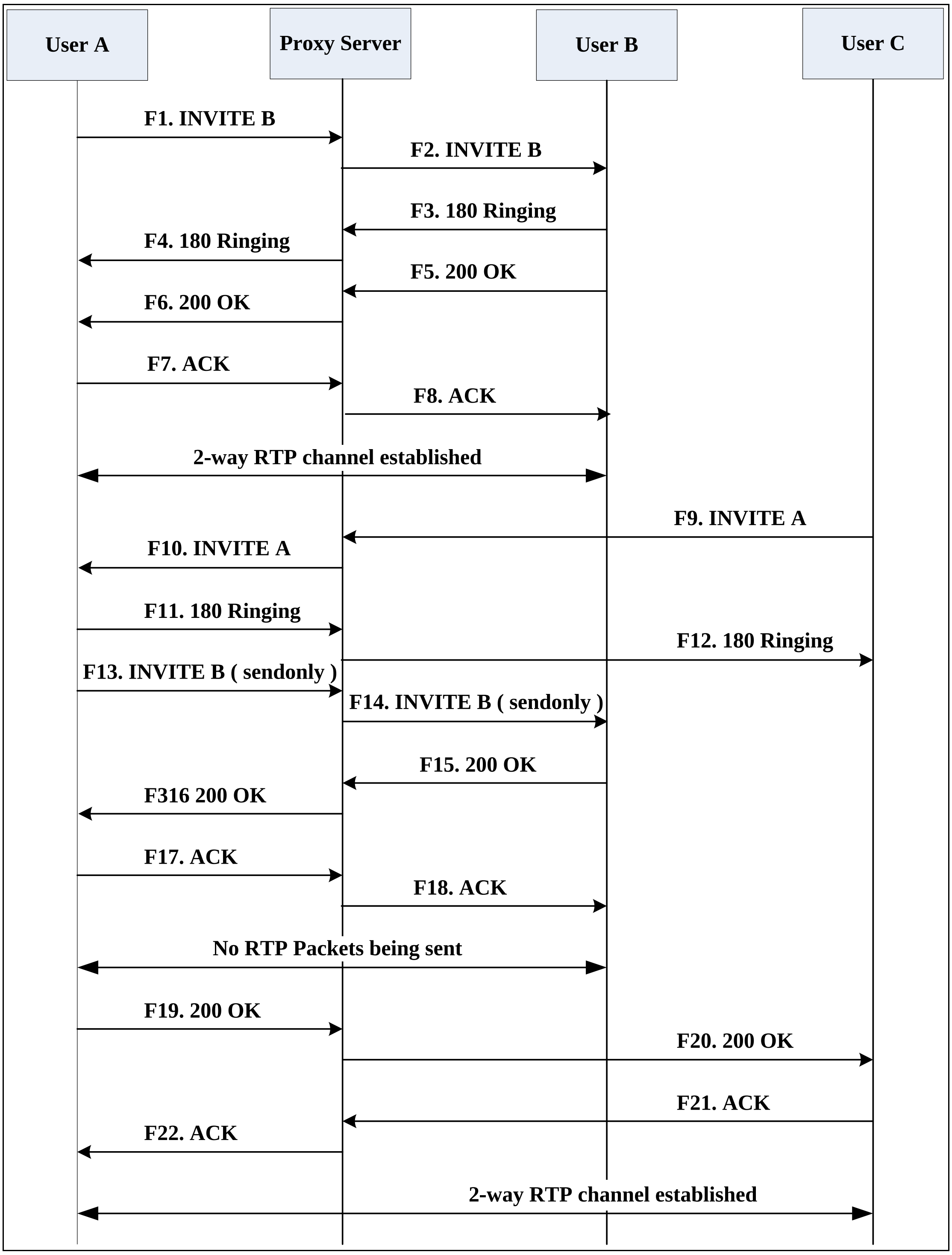
Successful Call Setup and Call Waiting

The following figure illustrates a successful call between Yealink SIP IP phones in which two parties are in a call, one of the participants receives and answers an incoming call from a third party. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.
3. User C calls User B.

4. User B accepts the call from User C.



Step	Action	Description
F1	INVITE—User A to Proxy Server	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.

Step	Action	Description
		In the INVITE request: • The IP address of User B is inserted in the Request-URI field. • User A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User A is ready to receive is specified. • The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	180 Ringing—User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies proxy server that the connection has been made.
F6	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the connection has been made.
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.

Step	Action	Description
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	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. In the INVITE request: • The IP address of User A is inserted in the Request-URI field. • User C is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User C is ready to receive is specified. • The port on which User A is prepared to receive the RTP data is specified.
F10	INVITE—Proxy Server to User A	The proxy server maps the SIP URI in the To field to User A. The proxy server sends the INVITE message to User A.
F11	180 Ringing—User A to Proxy Server	User A sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F12	180 Ringing—Proxy Server to User C	The proxy server forwards the 180 Ringing response to User C. User C hears the ring-back tone indicating that User A is being alerted.
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.

Step	Action	Description
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.

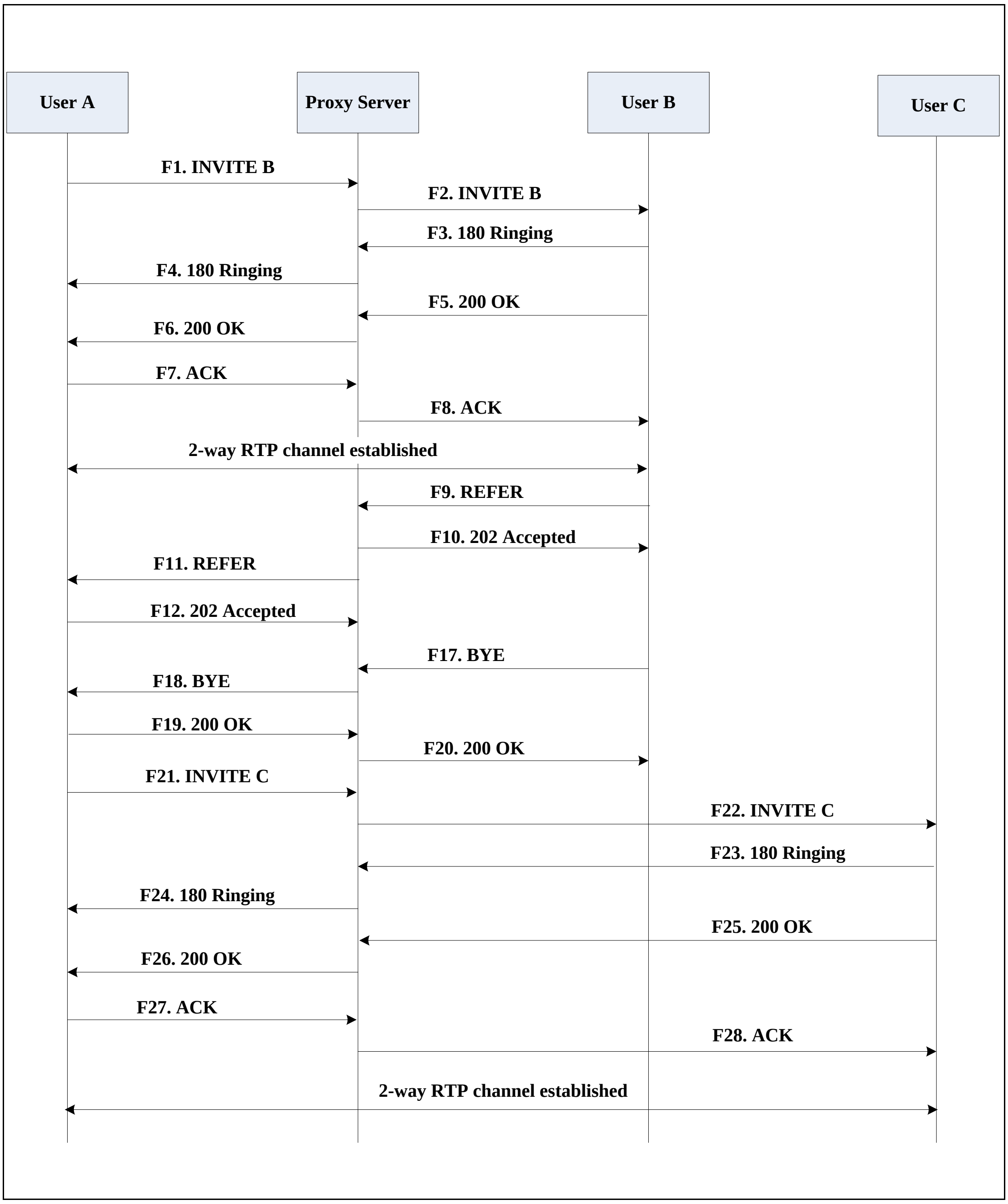
Call Transfer without Consultation

The following figure illustrates a successful call between Yealink SIP IP phones in which two parties are in a call and then one of the parties transfers the call to a third party without consultation. This is called a blind transfer. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.
3. User B transfers the call to User C.
4. User C answers the call.

Call is established between User A and User C.



Step	Action	Description
F1	INVITE—User A to Proxy Server	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. In the INVITE request: • The IP address of User B is inserted in the Request-URI field. • User A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User A is ready to receive is specified. • The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	180 Ringing—User B to Proxy server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F6	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the

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	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

Step	Action	Description
		Contact-URI field indicates that User A requests the call.
F18	INVITE—Proxy Server to User C	The proxy server maps the SIP URI in the To field to User C.
F19	180 Ringing—User C to Proxy Server	User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F20	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User C is being alerted
F21	200OK—User C to Proxy Server	User C sends a SIP 200 OK response to the proxy server. The 200 OK response notifies the proxy server that the connection has been made.
F22	200OK—Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A.
F23	ACK— User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F24	ACK—Proxy Server to User C	The proxy server forwards the ACK message to User C. The ACK confirms that User A has received the 200 OK response. The call session is now active.

Call Transfer with Consultation

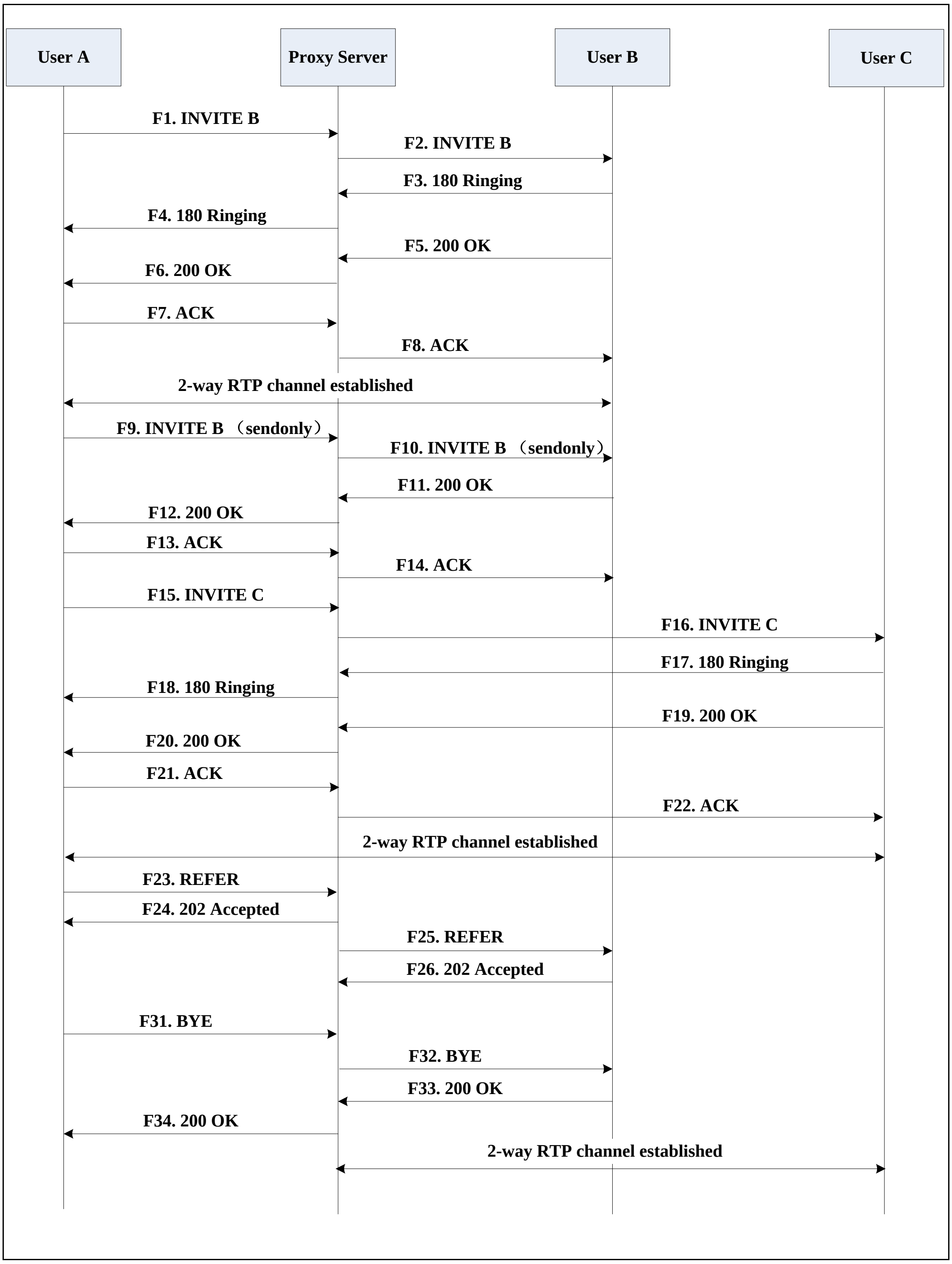
The following figure illustrates a successful call between Yealink SIP IP phones in which two parties are in a call and then one of the parties transfers the call to the third party with consultation. This is called attended transfer. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.
3. User A calls User C.

4. User C answers the call.
5. User A transfers the call to User C.

   Call is established between User B and User C.



Step	Action	Description
F1	INVITE—User A to Proxy Server	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. In the INVITE request: • The IP address of User B is inserted in the Request-URI field. • User A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User A is ready to receive is specified. • The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	180 Ringing—User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F6	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the

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 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.

Step	Action	Description
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 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.

Step	Action	Description
F26	202 Accepted—User B to Proxy Server	User B sends a SIP 202 Accept response to the proxy server. The 202 Accepted response indicates that User B accepts the transfer.
F27	BYE—User A to Proxy Server	User A terminates the call session by sending a SIP BYE request to the proxy server. The BYE request indicates that User A wants to release the call.
F28	BYE—Proxy Server to User B	The proxy server forwards the BYE request to User B.
F29	200OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that User B has received the BYE request.
F30	200OK—Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A.

Always Call Forward

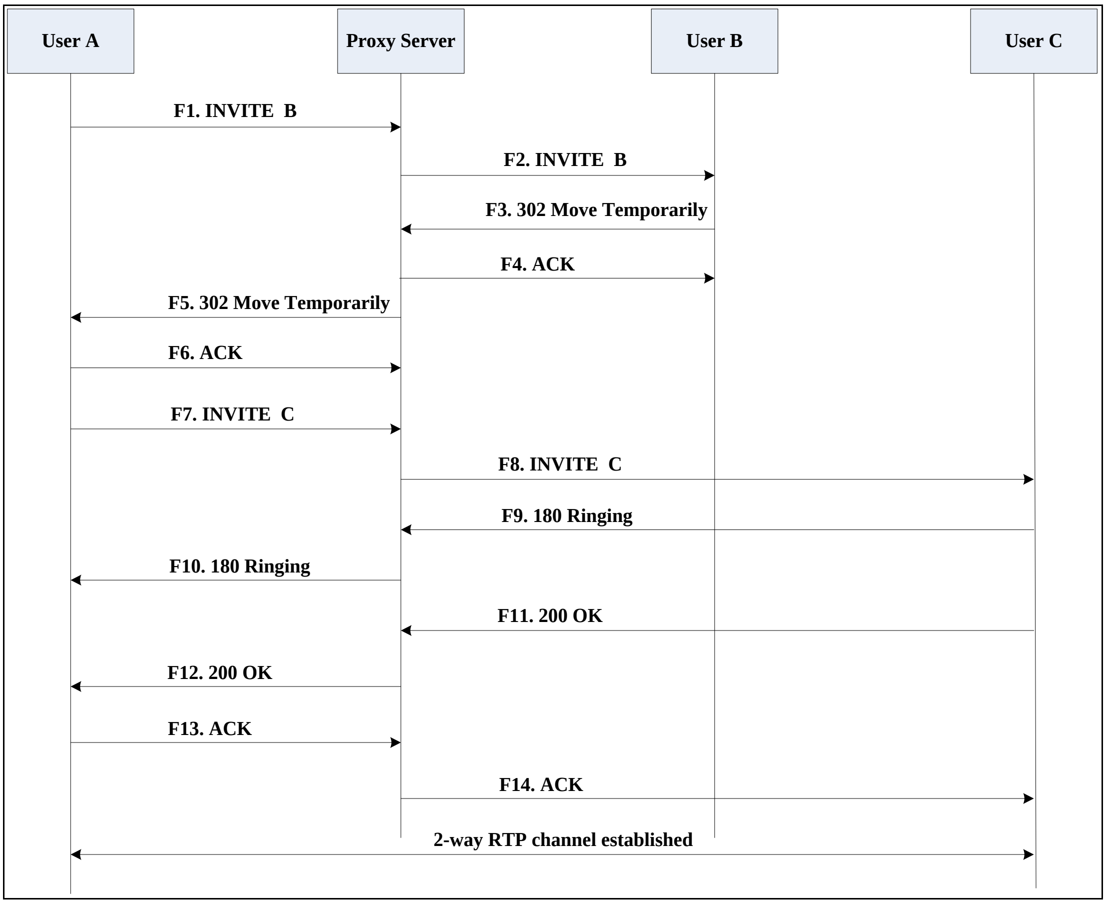
The following figure illustrates successful call forwarding between Yealink SIP IP phones in which User B has enabled always call forward. The incoming call is immediately forwarded to User C when User A calls User B. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User B enables always call forward, and the destination number is User C.
2. User A calls User B.
3. User B forwards the incoming call to User C.

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	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. In the INVITE request: • The IP address of the User B is inserted in the Request-URI field. • User A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field.

Step	Action	Description
		• The media capability User A is ready to receive is specified. • The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	302 Move Temporarily—User B to Proxy Server	User B sends a SIP 302 Moved Temporarily message to the proxy server. The message indicates that User B is not available at SIP phone B. User B rewrites the contact-URI.
F4	ACK—Proxy Server to User B	The proxy server sends a SIP ACK to User B, the ACK message notifies User B that the proxy server has received the 302 Move Temporarily message.
F5	302 Move Temporarily—Proxy Server to User A	The proxy server forwards the 302 Moved Temporarily message to User A.
F6	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK message notifies the proxy server that User A has received the 302 Move Temporarily message.
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

Step	Action	Description
		User C is being alerted.
F11	200OK—User C to Proxy Server	User C sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F12	200OK—Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A. The 200 OK response notifies User A that the connection has been made.
F13	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F14	ACK—Proxy Server to User C	The proxy server forwards the ACK message to User C. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.

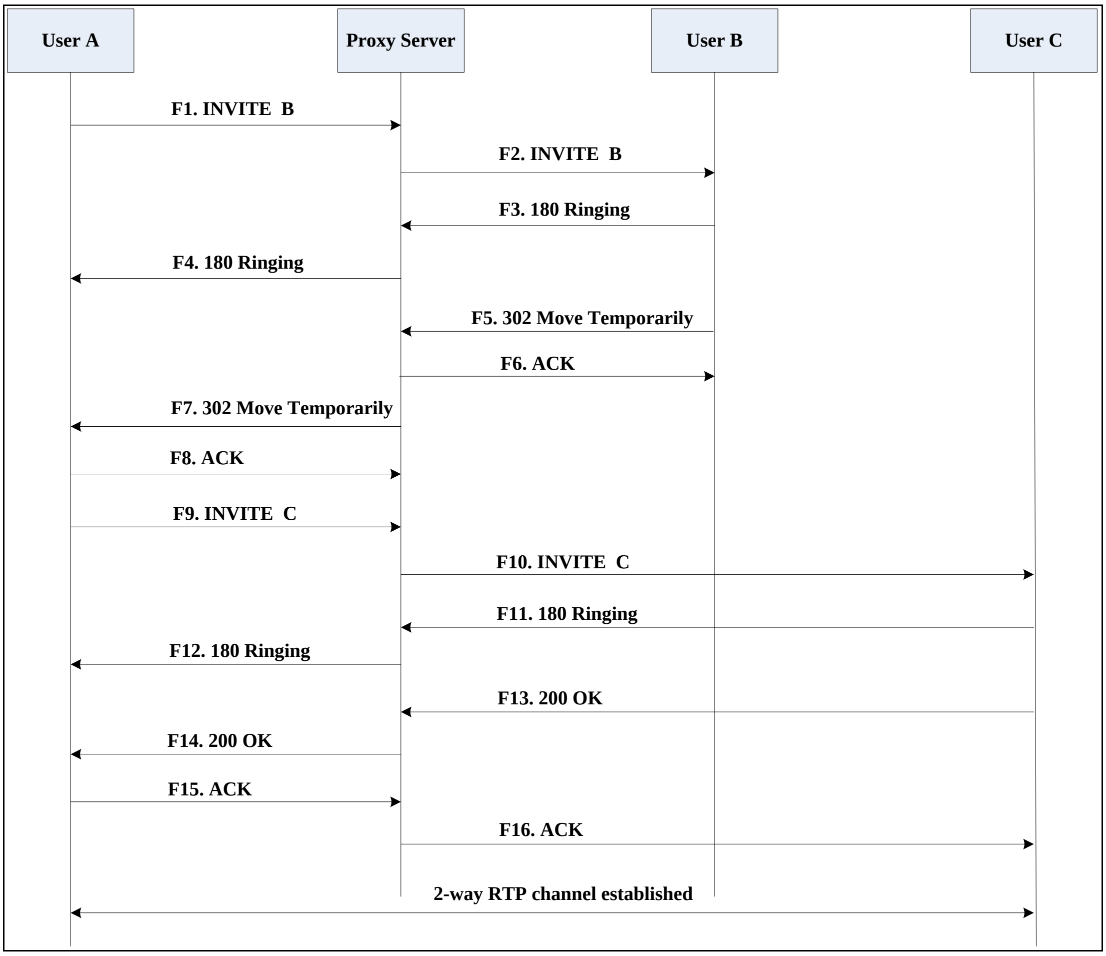
Busy Call Forward

The following figure illustrates successful call forwarding between Yealink SIP IP phones in which User B has enabled busy call forward. The incoming call is forwarded to User C when User B is busy. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User B enables busy call forward, and the destination number is User C.
2. User A calls User B.
3. User B is busy.
4. User B forwards the incoming call to User C.
5. User C answers the call.

Call is established between User A and User C.



Step	Action	Description
F1	INVITE—User A to Proxy Server	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. In the INVITE request: • The IP address of User B is inserted in the Request-URI field. • User A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field.

Step	Action	Description
		• The media capability User A is ready to receive is specified. • The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	180 Ringing—User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	302 Move Temporarily—User B to Proxy Server	User B sends a SIP 302 Moved Temporarily message to the proxy server. The message indicates that User B is not available at SIP phone B. User B rewrites the contact-URI.
F6	ACK—Proxy Server to User B	The proxy server sends a SIP ACK to User B, the ACK message notifies User B that the proxy server has received the 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.

Step	Action	Description
F11	180 Ringing—User C to Proxy Server	User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F12	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User C is being alerted.
F13	200OK—User C to Proxy Server	User C sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F14	200OK—Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A.
F15	ACK— User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F16	ACK—Proxy Server to User C	The proxy server sends the ACK message to User C.

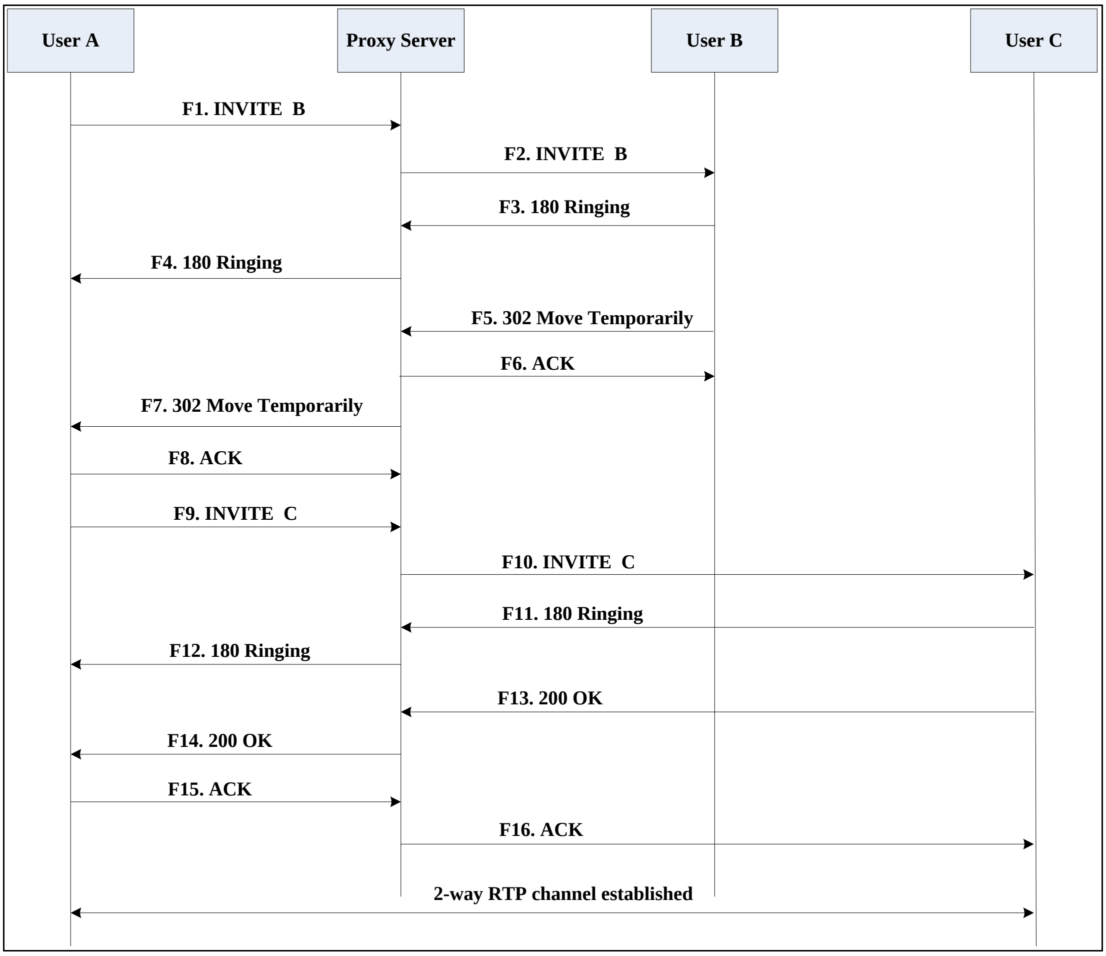
No Answer Call Forward

The following figure illustrates successful call forwarding between Yealink SIP IP phones in which User B has enabled no answer call forward. The incoming call is forwarded to User C when User B does not answer the incoming call after a period of time. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User B enables no answer call forward, and the destination number is User C.
2. User A calls User B.
3. User B does not answer the incoming call.
4. User B forwards the incoming call to User C.
5. User C answers the call.

Call is established between User A and User C.



Step	Action	Description
F1	INVITE—User A to Proxy Server	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. In the INVITE request: • The IP address of User B is inserted in the Request-URI field. • User A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field.

Step	Action	Description
		• The media capability User A is ready to receive is specified. • The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	180 Ringing—User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	302 Move Temporarily—User B to Proxy Server	User B sends a SIP 302 Moved Temporarily message to the proxy server. The message indicates that User B is not available at SIP phone B. User B rewrites the contact-URI.
F6	ACK—Proxy Server to User B	The proxy server sends a SIP ACK to User B, the ACK message notifies User B that the proxy server has received the 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.

Step	Action	Description
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.

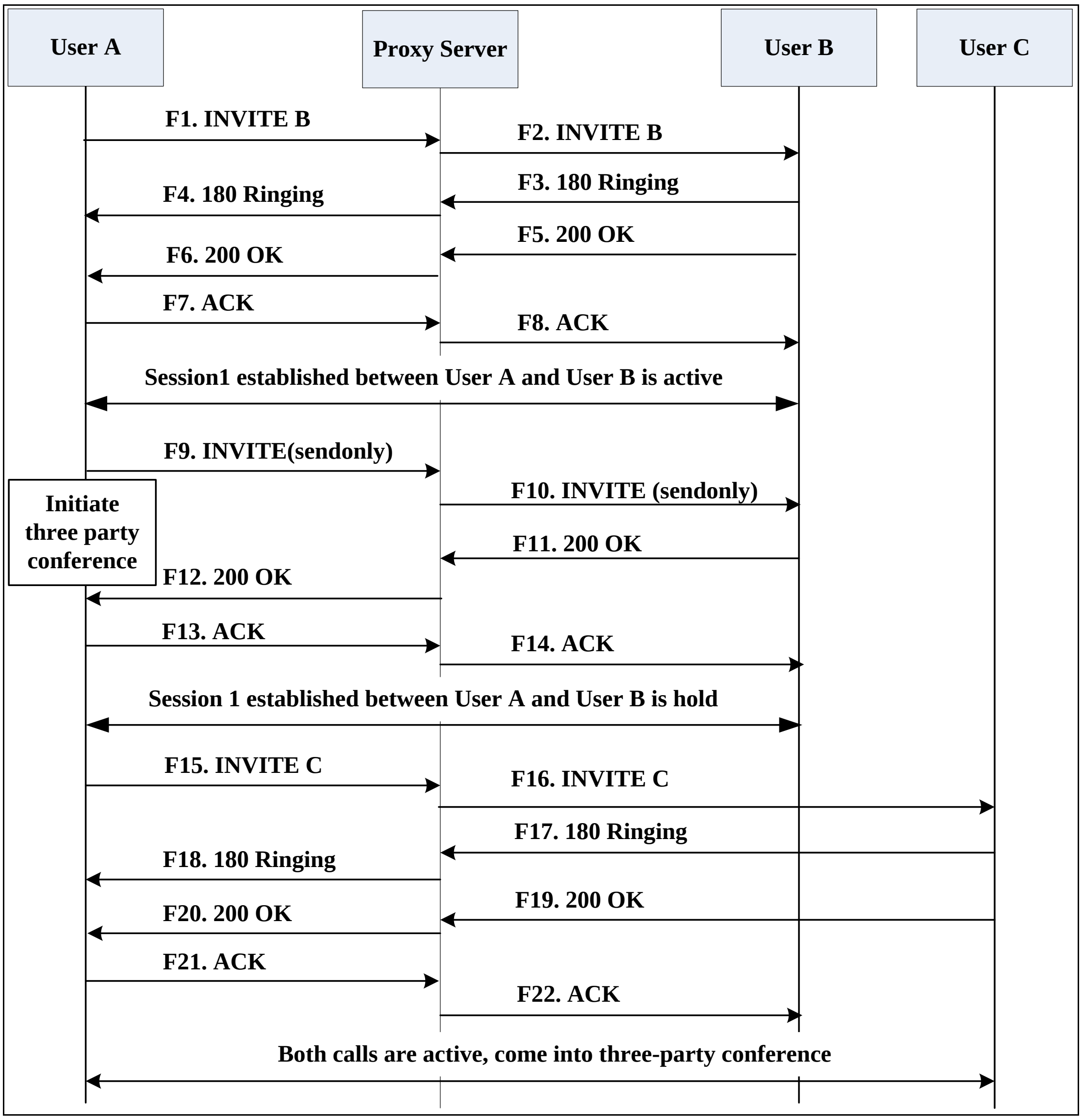
Call Conference

The following figure illustrates successful 3-way calling between Yealink IP phones in which User A mixes two RTP channels and therefore establishes a conference between User B and User C. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.
3. User A 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	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. In the INVITE request: • The IP address of User B is inserted in the Request-URI field. • User A is identified as the call session initiator in the From field.

Step	Action	Description
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User A is ready to receive is specified. • The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. Proxy server forwards the INVITE message to User B.
F3	180 Ringing—User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F6	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the connection has been made.
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	User A sends a mid-call INVITE request

Step	Action	Description
	Server	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 User C is being alerted.

Step	Action	Description
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