Yealink

Ultra-elegant Gigabit IP Phone SIP-T46G Administrator Guide

Version 71.60

Apr 2013

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 BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF PRODUCTS.

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

Declaration of Conformity

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

CE Mark Warning

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

Part 15 FCC Rules

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

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

Class B Digital Device or Peripheral

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

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

About This Guide

The guide is considered to be an administration-level version, which is intended for administrators who need to properly configure, customize, manage, and troubleshoot the IP phone systems rather than the end-users of IP phones. It provides details on the functionality and configuration of the IP phones.

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

Documentations

The following related documents for the SIP-T46G IP phones are available:

- Quick Installation Guide, which describes how to assemble IP phones.
- Quick Reference Guide, which describes the most basic features available on IP phones.
- User Guide, which describes the basic and advanced features available on IP phones.
- Auto Provisioning User Guide, which describes how to auto provision IP phones using the configuration files.
- Configuration Conversion Tool User Guide, which describes how to convert and encrypt the configuration files using the Configuration Conversion Tool.
- <y000000000028>.cfg and <MAC>.cfg template configuration files.
- IP Phones Deployment Guide for BroadWorks Environments, which describes how to configure the BroadSoft features on the BroadWorks web portal and IP phones.

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

In This Guide

The information detailed in this guide is applicable to the firmware version 71. The firmware format likes x.x.x.x.rom (e.g., 28.71.0.50.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 the 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, "Upgrading the Firmware" describes how to upgrade the firmware of the IP phones.
- Chapter 8, "Resource Files" describes the resource files that can be downloaded by the IP phones.
- Chapter 9, "Troubleshooting" describes how to troubleshoot the IP phones and provides some common troubleshooting solutions.
- Chapter 10, "Appendix" provides the glossary, reference information about the IP phones compliant with RFC 3261, SIP call flows and the sample configuration files.

Table of Contents

Product Overview

This chapter contains the following information about the SIP-T46G IP phones:

- VoIP Principle
- SIP Components
- Introducing the SIP-T46G IP Phones

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 implement.

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 worldwide by service providers and enterprises for both voice and video services over IP networks.

SIP

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

SIP provides the capabilities to:

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

SIP Components

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

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

User Agent Client (UAC)

The UAC is an application that initiates up to six feasible SIP requests to the UAS. The six requests issued by the UAC are: INVITE, ACK, OPTIONS, BYE, CANCEL and REGISTER. When the SIP session is being initiated by the UAC SIP component, the UAC determines the information essential for the request, which is the protocol, the port and the IP address of the UAS to which the request is being sent. This information can be dynamic and this 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. Using this method may be the preferred measure when not using an application layer firewall, application layer firewalls like to know what applications are flowing though which ports and it is possible using content types of other applications other than the one you are trying to let through which has been denied.

User agent server (UAS)

UAS is the server that hosts the application responsible for receiving the SIP requests from a UAC, and on reception 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.

Introducing the SIP-T46G IP Phones

The SIP-T46G IP phones are the 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. The SIP-T46G 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.

The SIP-T46G 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 history and directory access. The SIP-T46G IP phones also support advanced functionalities, including LDAP, Busy Lamp Field, Sever Redundancy and Network Conference.

The SIP-T46G IP phones comply with the SIP standard (RFC 3261), and they can only be used within a network that supports this type of phone.

For successfully operating as SIP endpoints in your network, the SIP-T46G IP phones must meet the following requirements:

- A working IP network is established.
- Routers are configured for VoIP.
- VoIP gateways are configured for SIP.
- The latest (or compatible) firmware of the SIP-T46G IP phones is available.
- A call server is active and configured to receive and send SIP messages.

Physical Features of the SIP-T46G IP Phones

This section lists the available physical features of the SIP-T46G IP phones.

SIP-T46G

Physical Features:

- 4.3" TFT-LCD, 480 x 272 pixel, 16.7M colors
- 6 VoIP accounts
- HD Voice: HD Codec, HD Handset, HD Speaker
- 40 keys including 13 programmable keys
- 1xRJ9 (4P4C) handset port
- 1xRJ9 (4P4C) headset port
- 2xRJ45 10/100/1000M Ethernet ports
- 1XRJ12 (6P6C) expansion module port
- 14 LEDs: 1xpower, 10xline, 1xmute, 1xheadset, 1xspeakerphone
- Power adapter: AC 100~240V input and DC 5V/2A output
- Power over Ethernet (IEEE 802.3af)
- A USB port
- Bluetooth

Key Features of the SIP-T46G IP Phones

In addition to the physical features introduced above, the SIP-T46G 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, 3-way 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 phonebook, SNMP, LDAP, 802.1x authentication.
- Codecs and Voice Features
  - Wideband codec: G.722
  - Narrowband codec: G.711, G.723.1, G.726, G.729AB, GSM
  - VAD, CNG, AEC, PLC, AJB, AGC
  - Full-duplex speakerphone with AEC
- Network Features
  - SIP v1 (RFC2543), v2 (RFC3261)
  - Supports IPv4/IPv6
  - NAT Traversal: STUN mode
  - DTMF: INBAND, RFC2833, SIP INFO
  - Proxy mode and peer-to-peer SIP link mode
  - IP assignment: Static/DHCP/PPPoE
  - TFTP/DHCP/PPPoE client
  - HTTP/HTTPS server
  - DNS client
  - NAT/DHCP server
- Management
  - FTP/TFTP/HTTP/PnP auto-provision
  - Configuration: browser/phone/auto-provision
  - Direct IP call without SIP proxy
  - Dial number via SIP server
  - Dial URL via SIP server
- Security
  - HTTPS (server/client)

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

Getting Started

This chapter introduces the initialization of the SIP-T46G IP phones, the installing and connecting process of the IP phones which you need to follow.

This chapter provides the following major sections:

- Connecting the IP Phones
- Initialization Process Overview
- Verifying Startup
- Configuration Methods
- Reading Icons
- Configuring Basic Network Parameters
- Creating Dial Plan

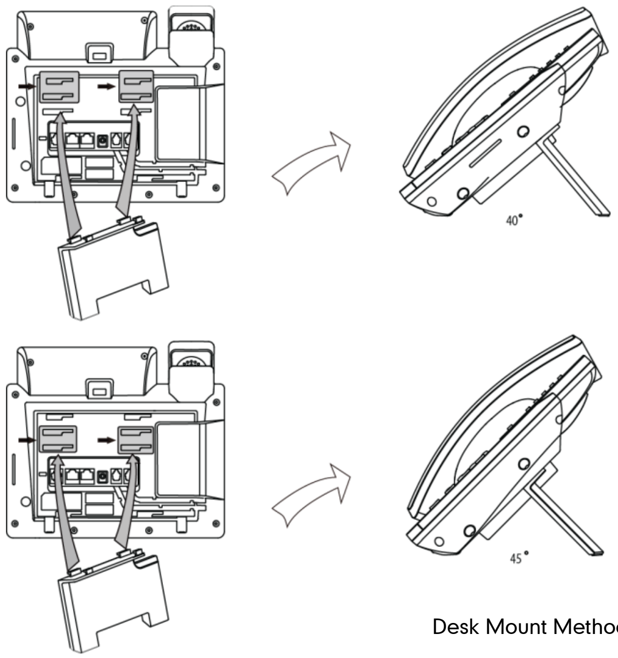
Connecting the IP Phones

This section introduces how to install SIP-T46G IP phones with the components in the packaging contents.

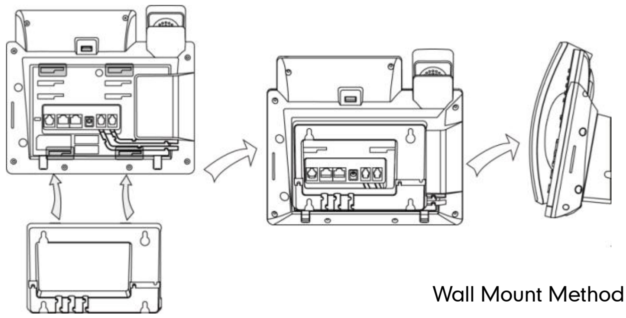
1. Attach the stand
2. Connect the handset and optional headset
3. Connect the network and power

Note The headset is not provided in the packaging contents.

1) **Attach the stand:**

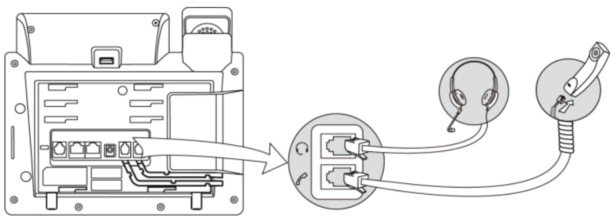


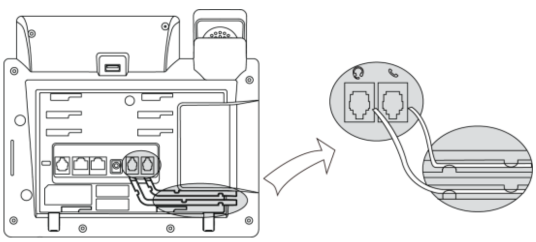
Desk Mount Method



Wall Mount Method

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





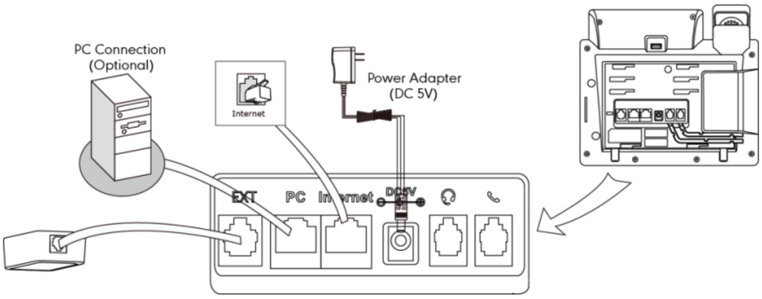
3) **Connect the network and power:**

- AC power
- Power over Ethernet (PoE)

AC Power

To connect the AC power and network:

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

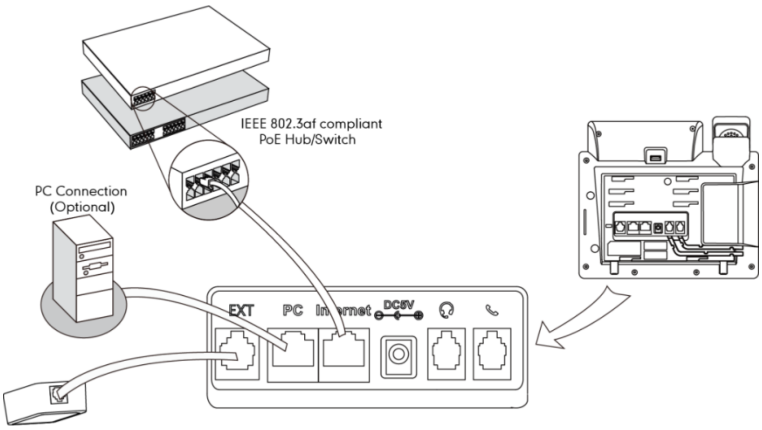


Power over Ethernet

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

To connect the PoE:

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



Note

If in-line power is provided, you do not need to connect the AC adapter. Make sure the Ethernet cable and switch/hub is PoE compliant.

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

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

Initialization Process Overview

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

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

During the initialization process, the following events proceed:

Loading the ROM file

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

Configuring the VLAN

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

Querying the DHCP (Dynamic Host Configuration Protocol) Server

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

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

You need to configure the network parameters of the IP phones manually if any of them is not supplied by the DHCP server. For more information on configuring network parameters manually, refer to Configuring Network Parameters Manually on page 17.

Contacting the auto provisioning server

SIP-T46G IP phones support the FTP, TFTP, HTTP, and HTTPS protocols for auto provisioning and are configured by default to use TFTP protocol. If the IP phones are configured to obtain configurations from the TFTP server, they will connect to the TFTP server and download the configuration file(s) during booting up. The IP phones will be able to resolve and apply the configurations written in the configuration file(s). If the IP phones do not obtain the configurations from the TFTP server, the IP phones will use the configurations stored in the flash memory.

Updating the firmware

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

Downloading the resource files

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

The followings are examples of resource files:

- Language packs
- Ring tones
- Contact files

Verifying Startup

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

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

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

Configuration Methods

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

- Phone User Interface
- Web User Interface
- Configuration Files

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

Phone User Interface

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

Web User Interface

An administrator or a user can configure the IP phones via web user interface. The default user name and password for the administrator to log in the web user interface are both "admin" (case-sensitive). Almost all features are available for configuring via web user interface. The IP phones support both HTTP and HTTPS protocols for accessing the web user interface. For more information, refer to Web Server Type on page 101.

Configuration Files

You can batch configure the IP phones by using the configuration files. There are two configuration files both of which are CFG formatted. We call them Common CFG file and MAC-Oriented CFG file. A Common CFG file will be effectual for all IP phones of the same model. However, a MAC-Oriented CFG file will only be effectual for a specific IP phone. The Common CFG file has a fixed name for each IP phone model, while the MAC-Oriented CFG file is named as the MAC address of the IP phones. For example, if the MAC address of a SIP-T46G IP phone is 001565113af8, the file name of the MAC-Oriented CFG file is 001565113af8.cfg. The file name of the Common CFG file for SIP-T46G IP phone model is y000000000028.cfg.

In order to configure the IP phones using the configuration files (<y000000000028>.cfg and <MAC>.cfg), you need to use a text-based editing application to edit the configuration files, and store the configuration files to the root directory of a provisioning server. The IP phones support downloading the configuration files using any of the following protocols: FTP, TFTP, HTTP and HTTPS.

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

When modifying parameters, remember the following:

- Parameters in the configuration files override those stored in the IP phones' flash memory.
- The .cfg extension of the configuration files must be in lowercase.

- Each line in a configuration file must use the following format and adhere to the following rules:

  `variable-name = value`

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

The IP phones can accept two sources of configuration data:

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

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

Reading Icons

Icons associated with different features may appear on the phone LCD screen. The following table provides a description for each icon on SIP-T46G IP phone model.

Icons	Description
	Network is unavailable
	Registered successfully
	Registration failed
	Registering
	Hands-free speakerphone mode
	Handset mode
	Headset mode
abc	Multi-lingual lowercase letters input mode
ABC	Multi-lingual uppercase letters input mode
2aB	Alphanumeric input mode

Icons	Description
123	Numeric input mode
	Voice Mail
	Text Message
	Auto Answer
	Do Not Disturb
	Call Forward
	Call Hold
	Call Mute
	Ringer volume is 0
	Keypad Lock
	Received Calls
	Dialed Calls
	Missed Calls
	Forwarded Calls
	Recording box is full
	A call cannot be recorded
	Recording starts successfully
	Recording cannot be started
	Recording cannot be stopped
	Open VPN
	Bluetooth

Icons	Description
	Bluetooth headset is both paired and connected
	Conference
	The contact icon
	The default contact photo

Configuring Basic Network Parameters

This section describes how to configure the basic network parameters that are required for the IP phones to operate in the network.

DHCP

DHCP (Dynamic Host Configuration Protocol) is a network protocol used to dynamically allocate network parameters to hosts connected to a network. The automatic distribution of network parameters to hosts eases the administrative burden of maintaining IP networks. The IP phones comply with the DHCP specifications documented in RFC 2131. If using DHCP, the IP phones connected to the network become operational without having to be manually assigned IP addresses and additional network parameters. By default, DHCP is enabled on the IP phones.

DHCP Option

DHCP provides a framework for passing network information to devices on a TCP/IP network. 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.

When the IP phones are simply plugged into the network, the DHCP process begins. The IP phones broadcast DISCOVER messages to request the network information carried in DHCP options and the DHCP server responds with the specific values in the corresponding options.

The following table lists the common DHCP options supported by the 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).

Parameter	DHCP Option	Description
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 the NTP servers available to the client by IP address.
Vendor-Specific Information	43	Identify the vendor-specific information.
Vendor Class Identifier	60	Identify the vendor type.
TFTP Server Name	66	Identify a TFTP server when the 'sname' field in the DHCP header has been used for DHCP options.
Bootfile Name	67	Identify a bootfile when the 'file' field in the DHCP header has been used for DHCP options.

Procedure

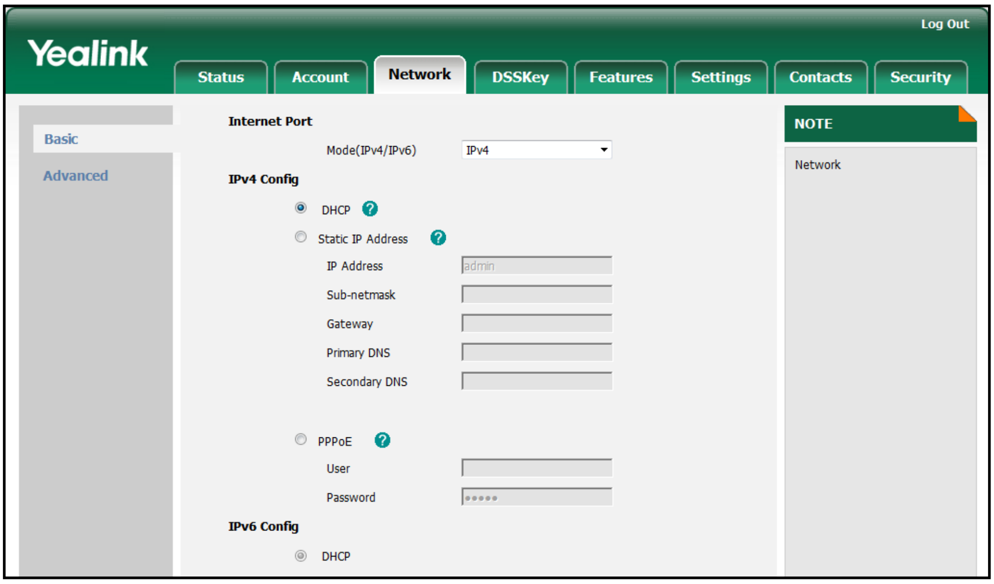
DHCP can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Configure DHCP on the IP phone. For more information, refer to DHCP on page 232.
Local	Web User Interface	Configure DHCP on the IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?p=network&q=load

	Phone User Interface	Configure DHCP on the IP phone.

To configure DHCP via web user interface:

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



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

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

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

To configure DHCP via phone user interface:

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

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

Configuring Network Parameters Manually

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

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

- Secondary DNS

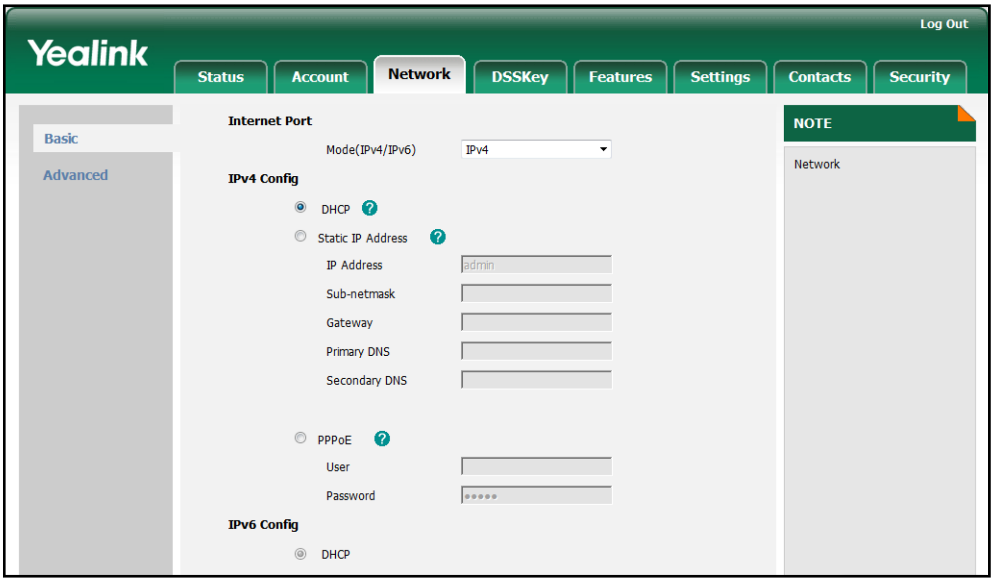
Procedure

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

Configuration File	<y000000000028>.cfg	Configure network parameters of the IP phone manually. For more information, refer to Static Network Settings on page 233.
Local	Web User Interface	Configure network parameters of the IP phone manually. **Navigate to:** http://<phoneIPAddress>/servlet?p=network&q=load
	Phone User Interface	Configure network parameters of the IP phone manually.

To configure the IP address mode via web user interface:

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

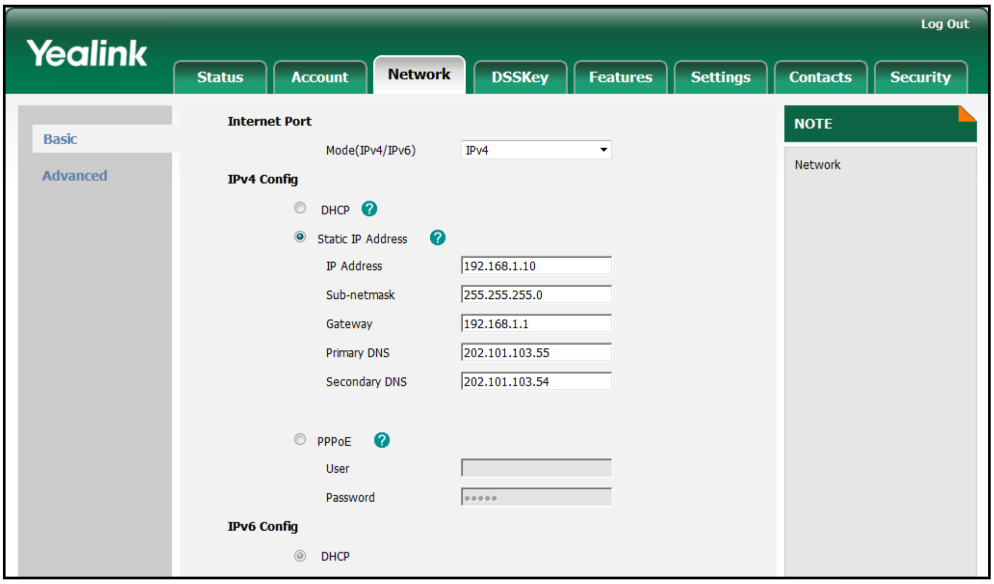


3. Click **Confirm** to accept the change.

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

To configure a static IPv4 address via web user interface:

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



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

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

To configure the IP address mode via phone user interface:

1. Press **Menu**->**Advanced** (password: admin) ->**Network**->**WAN Port**.
2. Press (▴) or (▾) to highlight the **IP Mode** field.
3. Press (◂) or (▸) to select **IPv4**, **IPv6** or **IPv4&IPv6** from the **IP Mode** field.
4. Press the **Save** soft key to accept the change.

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

To configure a static IPv4 address via phone user interface:

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

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

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

PPPoE

PPPoE (Point-to-Point Protocol over Ethernet) is a network protocol used by Internet Service Providers (ISPs) to provide Digital Subscriber Line (DSL) high speed Internet services. PPPoE allows an office or building-full of users to share a common DSL connection to the internet. The Internet port on the IP phones can be configured as a PPPoE port to connect to the Internet. Contact your ISP for the PPPoE username and password.

Procedure

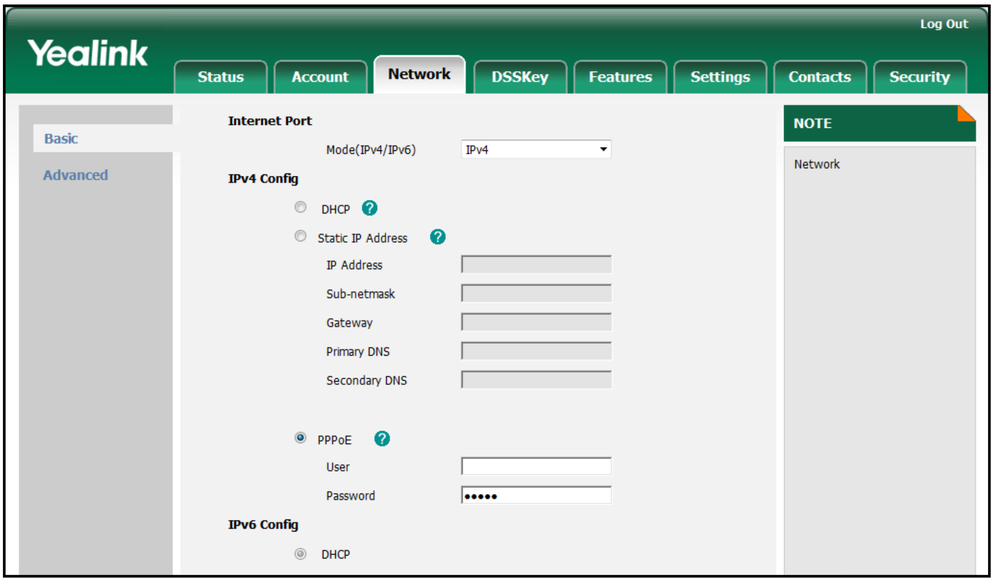
PPPoE can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Configure PPPoE on the IP phone. For more information, refer to PPPoE on page 235.
Local	Web User Interface	Configure PPPoE on the IP phone. **Navigate to:** http://<phoneIPAddress>/servlet?p=network&q=load
	Phone User Interface	Configure PPPoE on the IP phone.

To configure PPPoE via web user interface:

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

3. Enter the username and password in the corresponding fields.



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

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

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

To configure PPPoE via phone user interface:

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

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

Configuring Internet and PC Port Negotiation

There are two Ethernet ports on the rear of the IP phones: Internet port and PC port. You can configure the transmission method for each port to use to communicate over Ethernet. The IP phones support the following transmission methods:

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

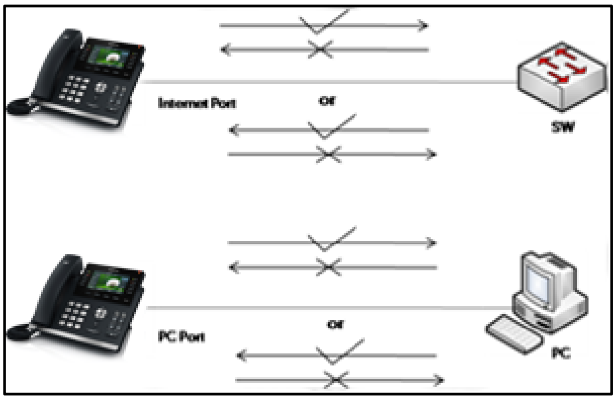
By default, the IP phones are configured to perform auto-negotiation on both Internet port and PC port.

Auto-negotiation

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

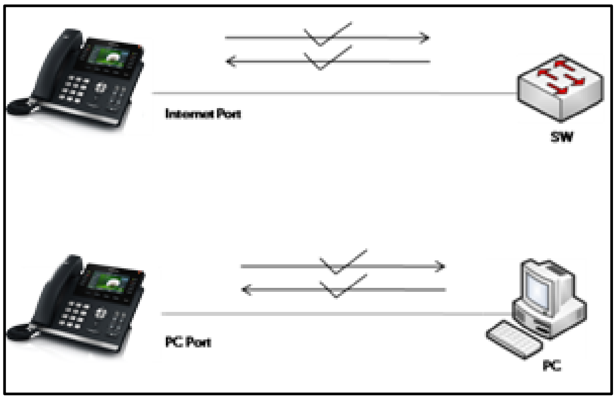
Half-duplex

Half-duplex transmission means that voice or data can be transmitted in both directions, but only one direction at a time. For example, 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 phones to transmit in 10Mbps or 100Mbps.



Full-duplex

Full-duplex transmission means that voice or data can be transmitted in both directions at the same time. For example, 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 phones to transmit in 10Mbps, 100Mbps or 1000Mbps.



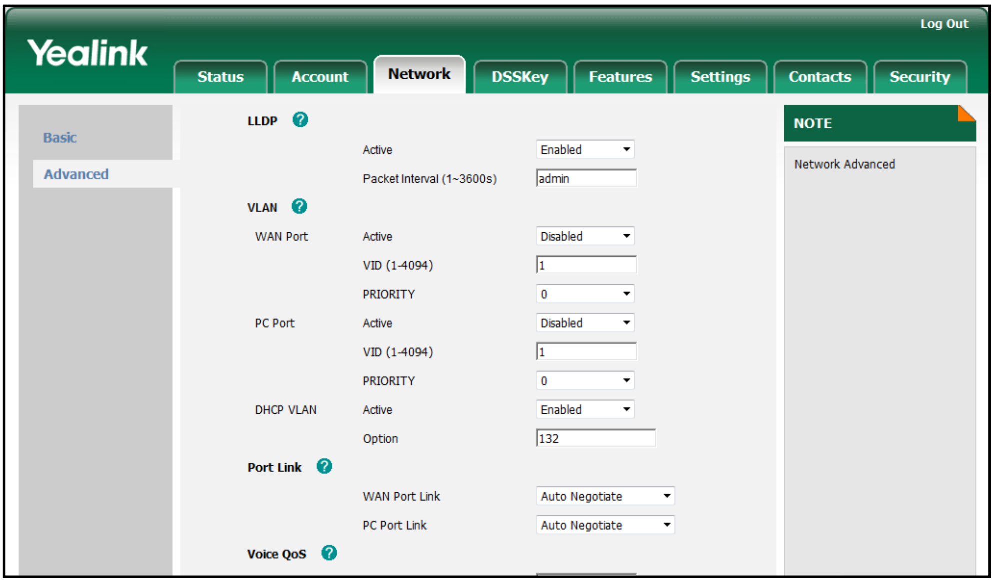
Procedure

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

Configuration File	<y000000000028>.cfg	Configure the transmission method of Ethernet port. For more information, refer to Internet and PC Ports Negotiation on page 236.
Local	Web User Interface	Configure the transmission method of Ethernet port. **Navigate to**: http://<phoneIPAddress>/servlet?p=network-adv&q=load

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

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



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

Creating Dial Plan

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

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

- Replace Rule
- Dial-now
- Area Code
- Block Out

The priority of matching dial plan is: Dial-now>Replace Rule>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", "12**abc**", etc.
x	The "x" can be used as a placeholder for any character. Example: "12x" would match "121", "122", "123", "12**a**", 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 "91**5**1234", "91**6**1234", "91**7**1234".
()	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 "**92**3", "**15**3", "**67**3", 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. You can create up to 20 replace rules for the IP phones. The replace rules can be created either one by one or in batch using a replace rule template. For more information on the replace rule template, refer to Replace Rule Template on page 209.

Procedure

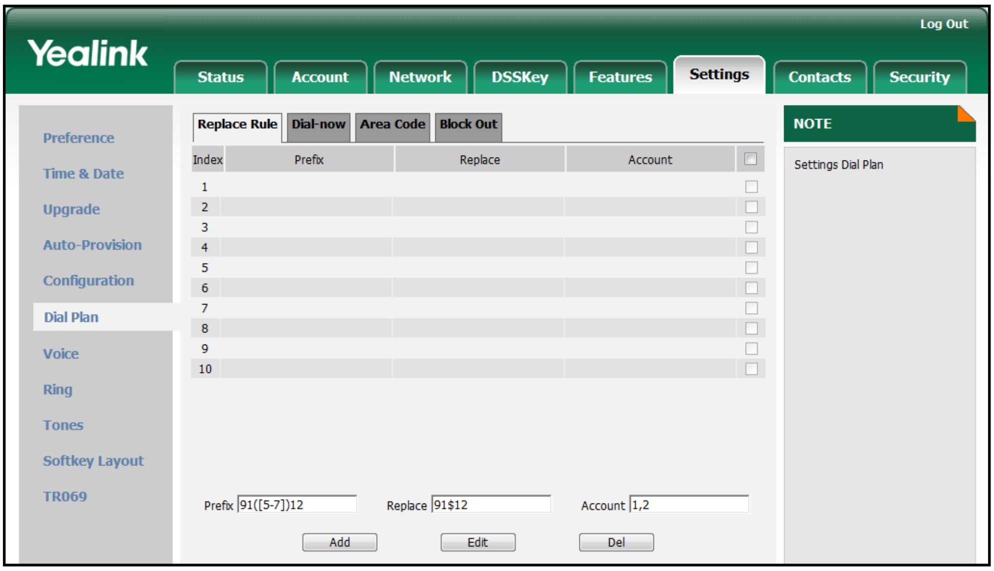
Replace rule can be created using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Create the replace rule for the IP phone. For more information, refer to Dial Plan on page 237.
Local	Web User Interface	Create the replace rule for the IP phone. **Navigate to:** http://<phoneIPAddress>/servlet ?p=settings-dialplan&q=load

To create the 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 the field blank or enter an invalid value, the replace rule applies 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 the numbers entered by the user. When entered numbers match the predefined dial-now rule, the IP phones will automatically dial out the numbers without pressing the send key. You can create up to 20 dial-now rules for the IP phones. The dial-now rules can be created either one by one or in batch using a dial-now rule template. For more information on the dial-now template, refer to Dial-now Template on page 210.

Delay Time for Dial-now Rule

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

Procedure

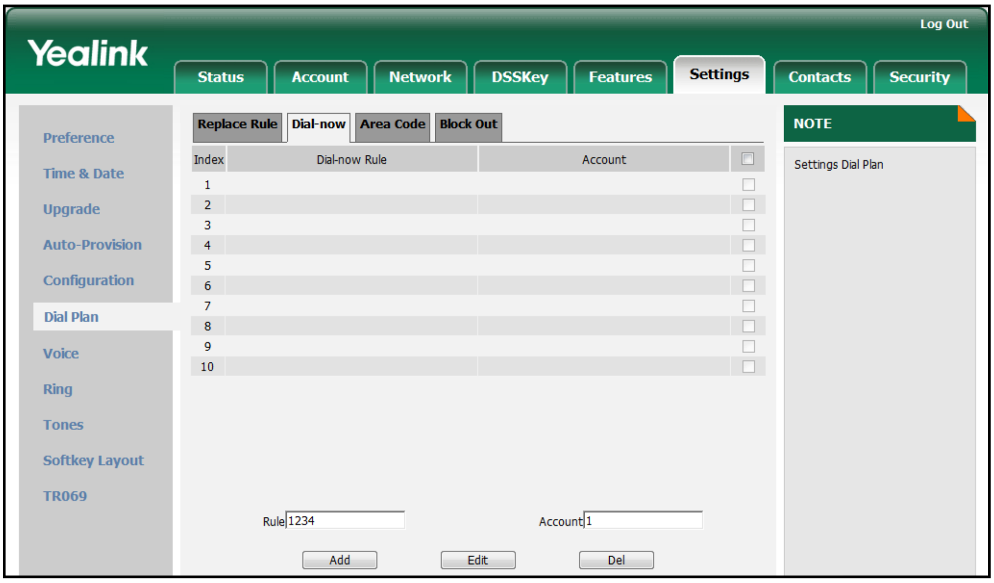
Dial-now rule can be created using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Create the dial-now rule for the IP phone. For more information, refer to Dial Plan on page 237. Configure the delay time for the dial-now rule. For more information, refer to Dial Plan on page 237.
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

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

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

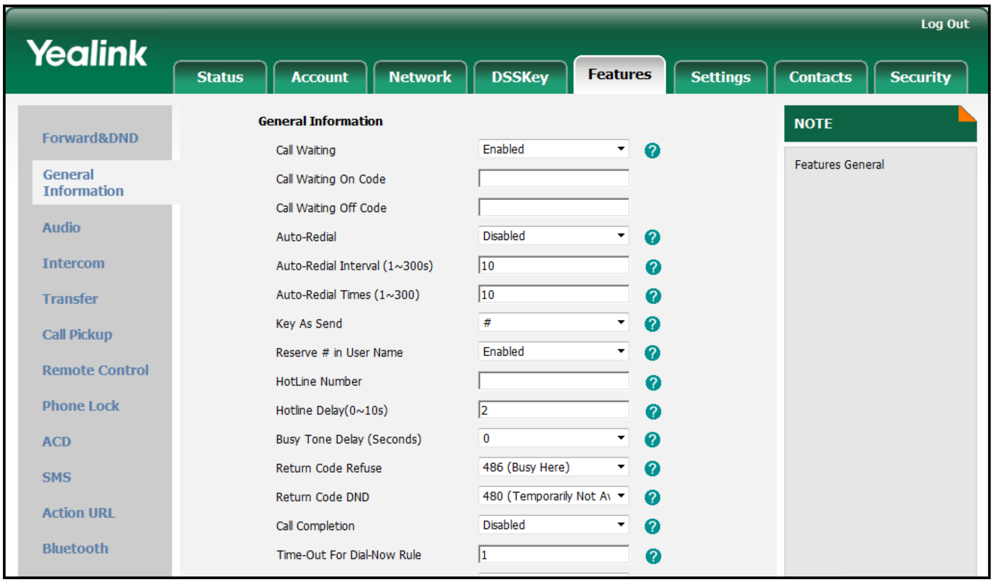
If you leave the field blank or enter an invalid value, the dial-now rule applies to all accounts on the IP phone.



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 phones will automatically add the area code to the beginning of the numbers and dial out. The IP phones only support one area code rule.

Procedure

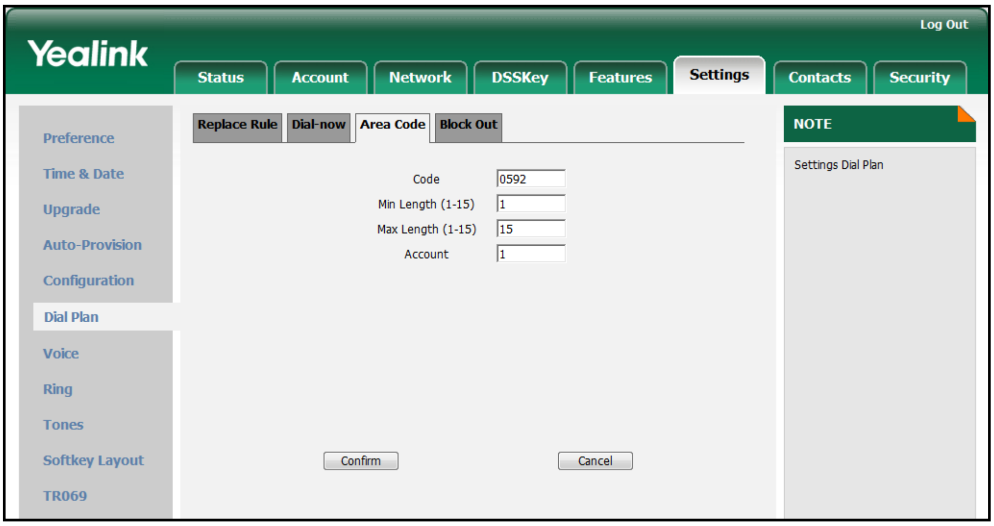
Area code rule can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Create the area code rule and specify the maximum and minimum lengths of the entered numbers. For more information, refer to Dial Plan on page 237.
Local	Web User Interface	Create the area code rule and specify the maximum and minimum lengths of the entered numbers. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-areacode&q=load

To configure an area code rule via web user interface:

1. Click on **Settings**->**Dial Plan**->**Area Code**.
2. Enter 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 the field blank or enter an invalid value, the area code rule applies to all accounts on the IP phone.



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

Block Out

Block out rule can prevent users from dialing out some specific numbers. When entered numbers match the predefined block out rule, the phone LCD screen prompts "Forbidden Number". You can create up to 10 block out rules.

Procedure

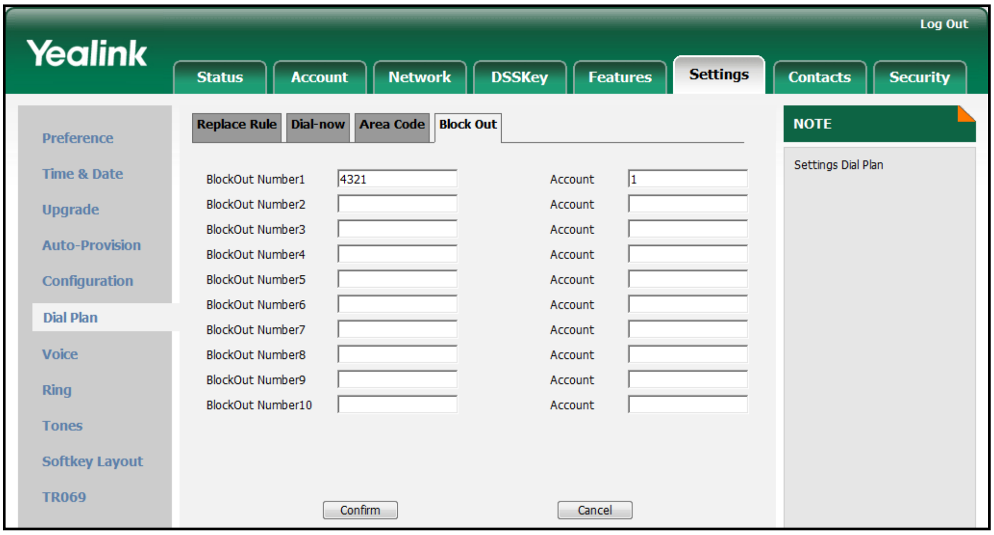
Block out rule can be created using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Create the block out rule for the IP phone. For more information, refer to Dial Plan on page 237.
Local	Web User Interface	Create the block out rule for the desired line. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-blackout&q=load

To create the block out rule via web user interface:

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

   If you leave the field blank or enter an invalid value, the block out rule applies to all accounts on the IP phone.



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

Configuring Basic Features

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

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

- Call Forward
- Call Transfer
- Network Conference
- Transfer on Conference Hang Up
- Directed Call Pickup
- Group Call Pickup
- Dialog-Info Call Pickup
- Call Return
- Call Park
- Web Server Type
- Calling Line Identification Presentation
- Connected Line Identification Presentation
- DTMF
- Suppress DTMF Display
- Transfer via DTMF
- Intercom

Wallpaper

Wallpaper is an image used as the background of the phone idle screen. Users can select an image from the IP phones' built-in background or customize wallpaper from personal pictures. For using the customized wallpaper, you need to upload the customized wallpaper in advanced.

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

Phone Model	Wallpaper Image Format	Resolution	Size
SIP-T46G	.jpg/.png/.bmp	<=480*272	<=5M

Procedure

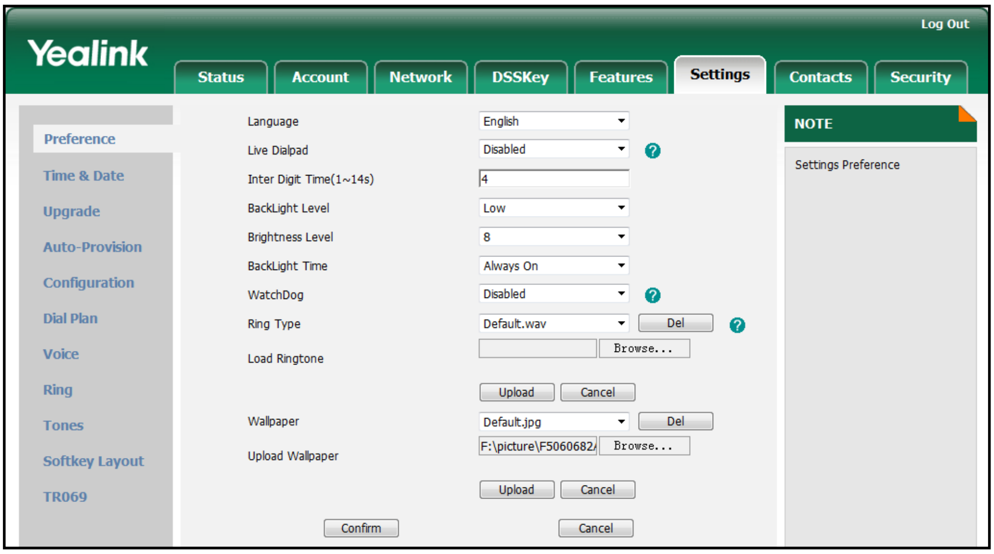
The wallpaper can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Specify the access URL of the customized wallpaper. For more information, refer to Access URL of Wallpaper Image on page 349.
Local	Web User Interface	Upload the customized

		wallpaper. Change the wallpaper via web user interface. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-preference&q=load
	Phone User Interface	Change the wallpaper via phone user interface.

To upload a customized wallpaper via web user interface:

1. Click on **Settings**->**Preference**.
2. In the **Upload Wallpaper** field, click **Browse** to select the wallpaper image from your local system.
3. Click **Upload** to upload the file.



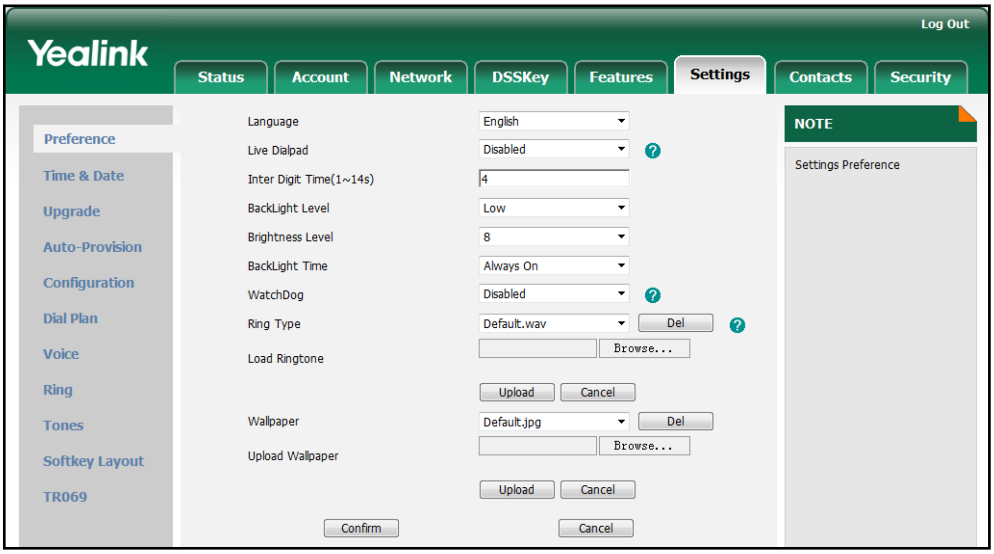
4. Click **Confirm** to accept the change.

   The customized wallpaper appears in the pull-down list of **Wallpaper**.

To change the wallpaper via web user interface:

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

2. Select the desired wallpaper from the pull-down list of **Wallpaper**.



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

To change the wallpaper via phone user interface:

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

Backlight

Backlight provides the brightness necessary for making the phone LCD screen readable in a darkened environment. Backlight On Intensity is used to adjust the backlight intensity of the LCD screen. Backlight time specifies the delay time to turn off or dusky the backlight when the IP phone is inactive. Backlight Idle Intensity decides whether the IP phone turns off or dusky the backlight of the LCD screen after a period of inactivity.

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

- **Always On:** Backlight is turned on permanently.
- **1min, 2min, 5min, 10min, 30min:** Backlight is turned off or dusky when the IP phone is inactive after a preset period of time (in seconds). It is automatically turned on if the status of the IP phone changes or any key is pressed.

Procedure

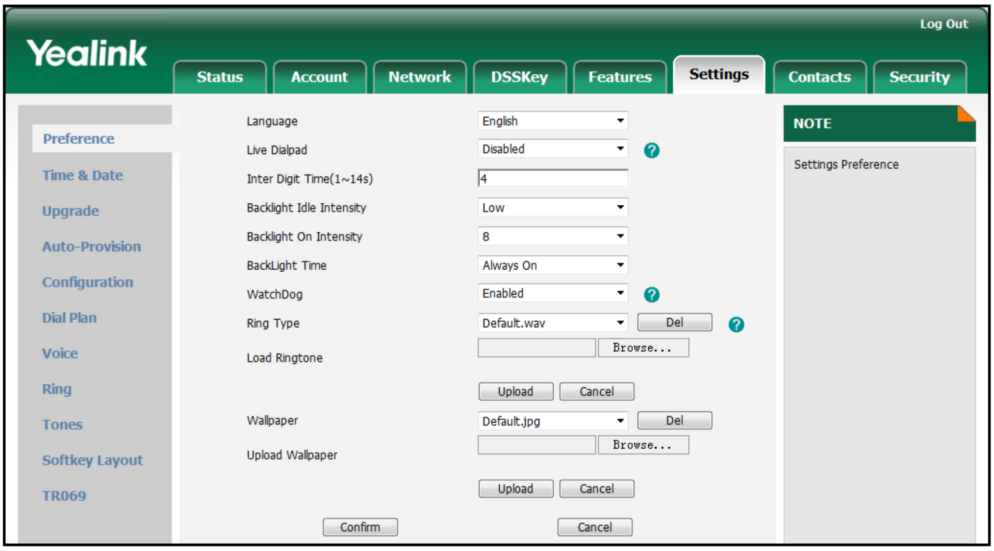
Backlight can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Configure the backlight of the LCD screen. For more information, refer to

		Backlight on page 241.
Local	Web User Interface	Configure the backlight of the LCD screen. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-preference&q=load
	Phone User Interface	Configure the backlight of the LCD screen.

To configure the backlight via web user interface:

1. Click on **Settings**->**Preference**.
2. Select the desired value from the pull-down list of **Backlight Idle Intensity**.
3. Select the desired value from the pull-down list of **Backlight On Intensity**.
4. Select the desired value from the pull-down list of **Backlight Time**.



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

To configure the backlight via phone user interface:

1. Press **Menu**->**Basic**->**Display**->**General**.
2. Press or , or the **Switch** soft key to select the desired level from the **Backlight On Intensity** field.
3. Press or , or the **Switch** soft key to select the desired value from the **Backlight Idle Intensity** field.
4. Press or , or the **Switch** soft key to select the desired time from the **Backlight Time** field.
5. Press the **Save** soft key to accept the change.

User Password

Several menu options are protected with two privilege levels, user and administrator, each with its own password. When logging in the web user interface, you need to enter the username and password for granting access to various menu options.

A user or an administrator can change the user password. IP phones support ASCII characters 32-126(0x20-0x7E) only in passwords. A valid password should be complex and contains at least 6 characters, where at least one character is numeric, and one character is alphabetic.

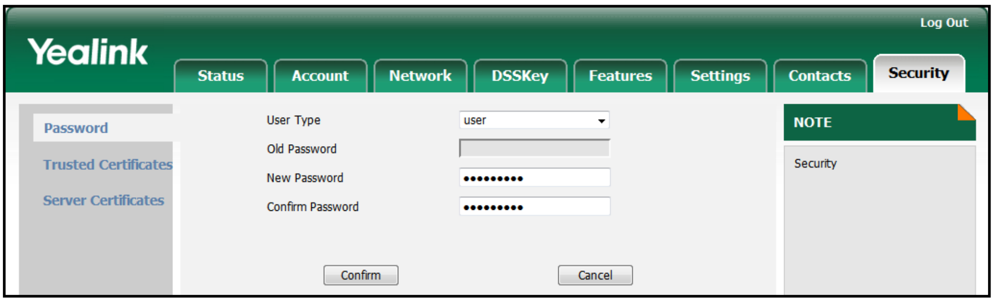
Procedure

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

Configuration File	<y000000000028>.cfg	Change the user password of the IP phone. For more information, refer to on User Password page 242.
Local	Web User Interface	Change the user password of the IP phone. **Navigate to:** http://<phoneIPAddress>/servlet?p=security&q=load

To change the user password via web user interface:

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



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

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

Administrator Password

Advanced menu options are restricted to an administrator. Users can configure them only if they have administrator privileges. The administrator password can be only changed by the administrator. The IP phones support ASCII characters 32-126(0x20-0x7E) only in passwords. A valid password should be complex and contains at least 6 characters, where at least one character is numeric, and one character is alphabetic.

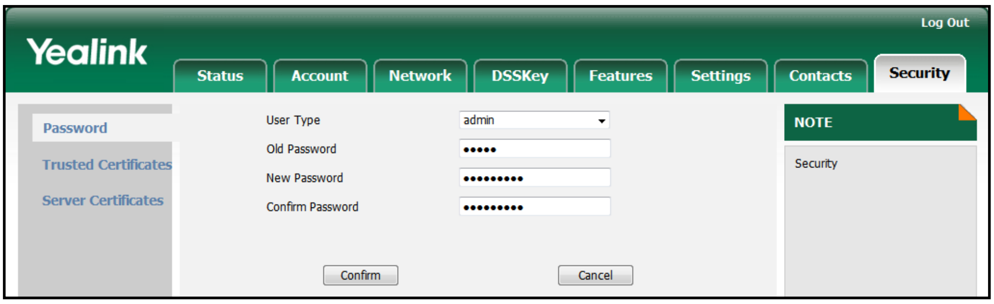
Procedure

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

Configuration File	<y000000000028>.cfg	Change the administrator password of the IP phone. For more information, refer to Administrator Password on page 243.
Local	Web User Interface	Change the administrator password. **Navigate to**: http://<phoneIPAddress>/servlet?p=security&q=load
	Phone User Interface	Change the administrator password of the IP phone.

To change the administrator password via web user interface:

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



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

To change the administrator password via phone user interface:

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

Phone Lock

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

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

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

Procedure

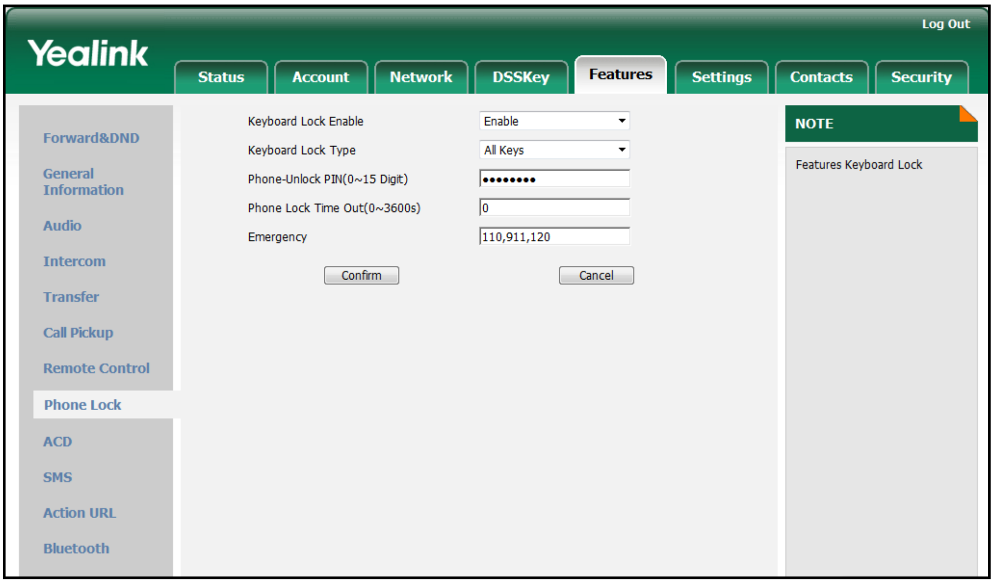
Phone lock can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Configure the type of phone lock. Change the unlock password. Configure the IP phone to automatically lock the keypad after a time interval. For more information, refer to Phone Lock on page 243. Assign a keypad lock key. For more information, refer to Keypad Lock Key on page 355.
Local	Web User Interface	Configure the type of phone lock. Change the unlock password. Configure the IP phone to automatically lock the keypad after a time interval. **Navigate to**:

		http://<phoneIPAddress>/servlet?p=features-phonelock&q=load Assign a keypad lock key. **Navigate to:** http://<phoneIPAddress>/servlet?p=dsskey&model=1&q=load&linepage=1
	Phone User Interface	Configure the type of phone lock. Assign a keypad lock key.

To configure phone lock via web user interface:

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

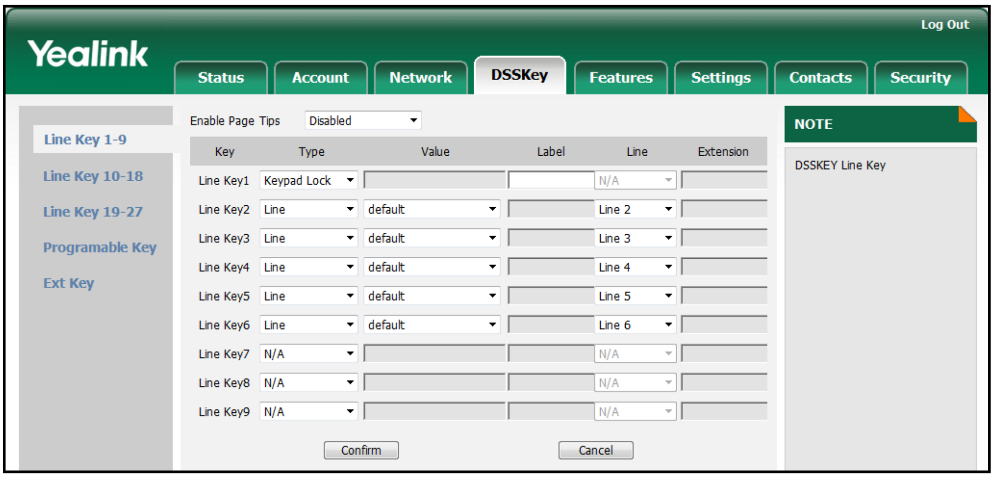


6. Click **Confirm** to accept the change.

To configure a keypad lock key via web user interface:

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

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



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

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

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

To configure a keypad lock key via phone user interface:

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

Date and Time

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

Time Zone

A time zone is a region on the 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 phones to obtain the date and time from the NTP server, you need to 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 near the start of spring and are adjusted 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. Usually there is no need to change this setting.

The following table lists the available methods for each feature:

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

Procedure

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

Configuration File	<y000000000028>.cfg	Configure the NTP server, time zone and DST. Configure the date and time formats. For more information, refer to Time and Date on page 245.

Local	Web User Interface	Configure the NTP server, time zone and DST. Configure the date and time manually. Configure the date and time formats. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-datetime&q=load
	Phone User Interface	Configure the NTP server and time zone. Configure the date and time manually. Configure the date and time formats.

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

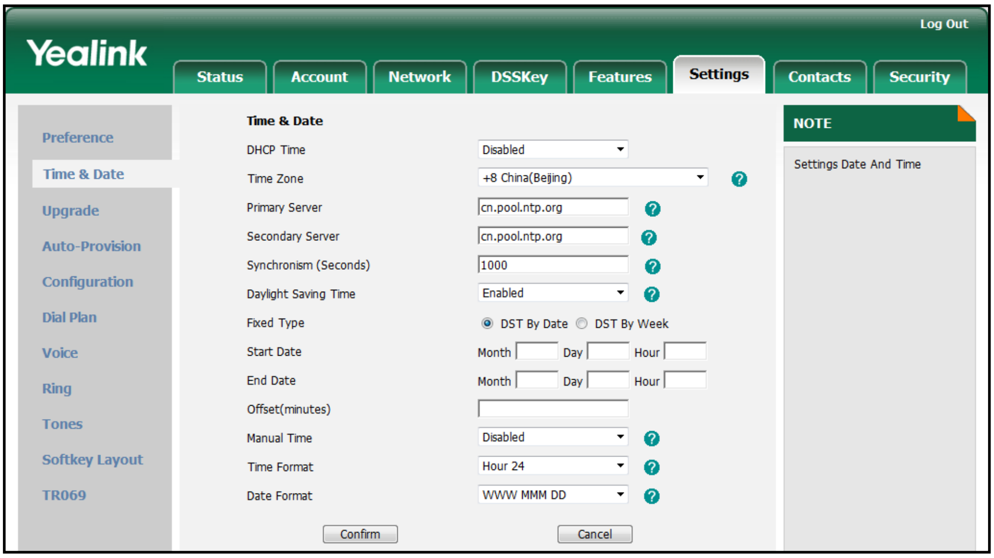
1. Click on **Settings**->**Time & Date**.
2. Select **Disabled** from the pull-down list of **Manual Time**.
3. Select the desired time zone from the pull-down list of **Time Zone**.
4. Enter the domain names or IP addresses in the **Primary Server** and **Second Server** fields respectively.
5. Enter the desired time interval in the **Synchronism (seconds)** 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.

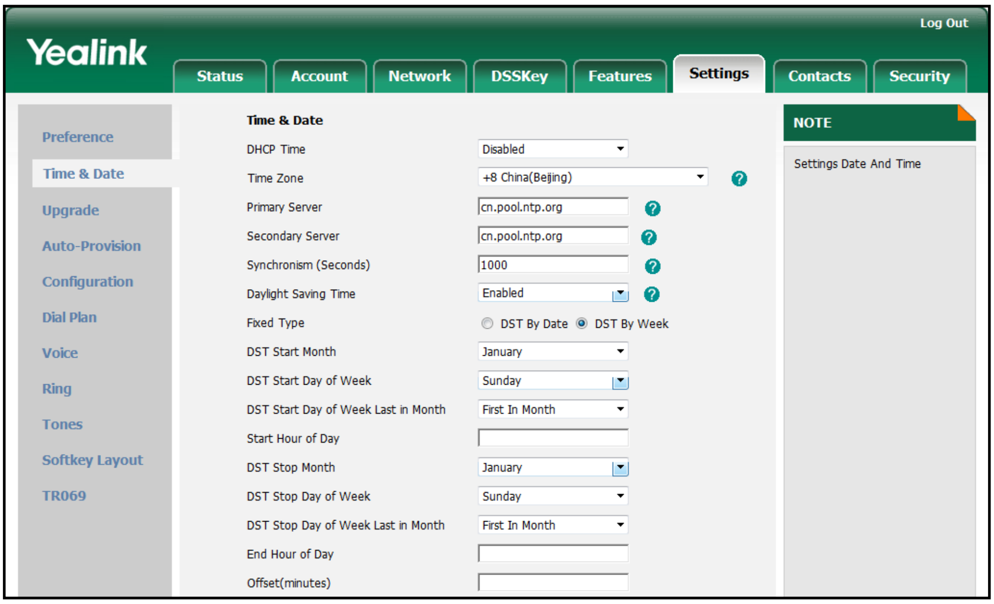


- Mark the **DST By Week** radio box in the **Fixed Type** field.

  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.

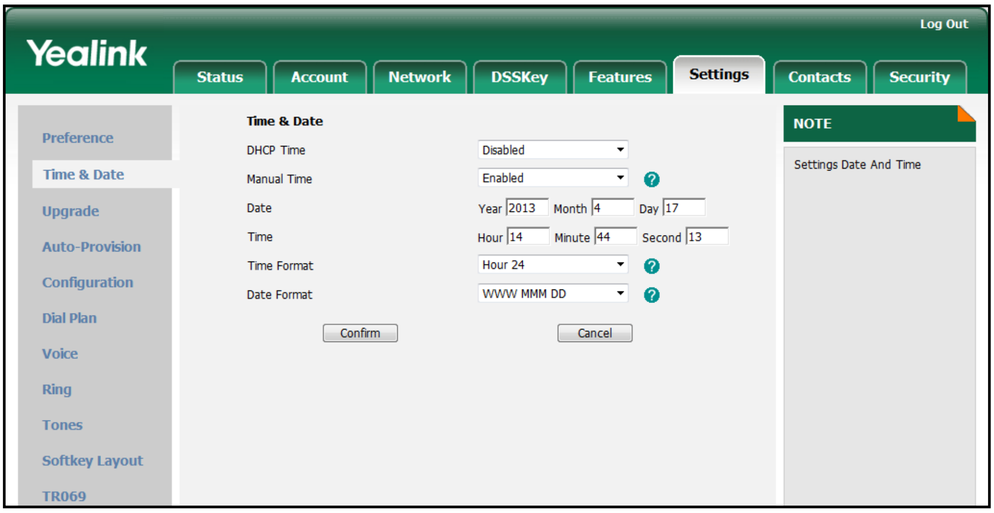


7. Enter the desired offset time in the **Offset (minutes)** field.
8. Click **Confirm** to accept the change.

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

1. Click on **Settings**->**Time & Date**.

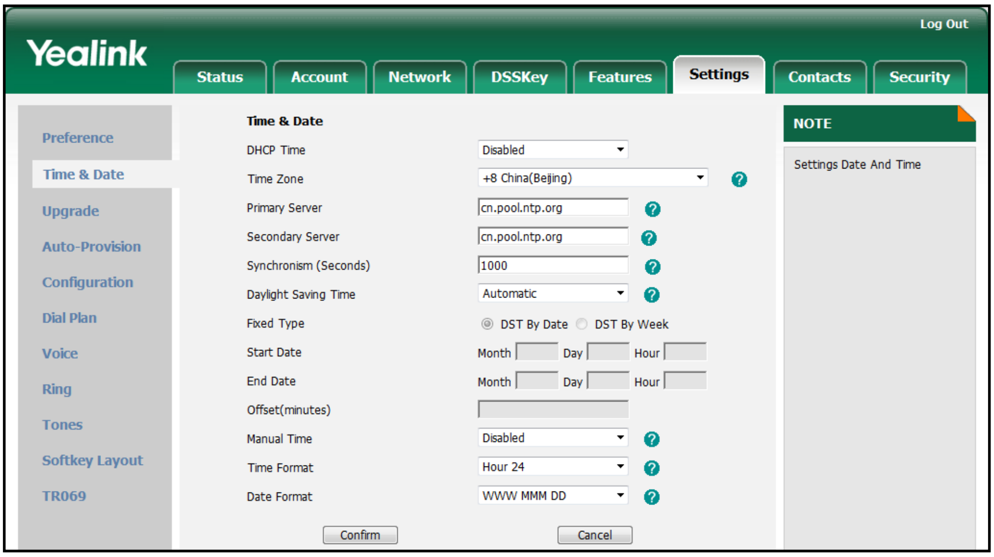
2. Select **Enabled** from the pull-down list of **Manual Time**.
3. Enter the date and time in the corresponding fields.



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

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

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



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

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

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

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

3. Enter the domain names or IP addresses in the **NTP Server 1** and **NTP Server 2** fields, respectively.
4. Press ◀ or, ▶ or the **Switch** soft key to select **Automatic** from the **Daylight Saving** field.
5. Press the **Save** soft key to accept the change.

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

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

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

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

Language

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

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

Phone User Interface	Web User Interface
English Chinese French German Italian Polish Portuguese Spanish Turkish	English Chinese French German Italian Turkish Portuguese Spanish

Loading Language Packs

All supported languages may not be available for selection. The languages available for selection depend on the language packs currently loaded on the IP phones. You can make languages available to use on the phone user interface by loading language packs to the IP phones. You can only load language packs to the IP phones using the configuration files.

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

Available Language	Associated Language Pack
English	lang+English.txt
Chinese_S	lang-Chinese_S.txt
Deutsch	lang-German.txt
French	lang-French.txt
Italian	lang-Italian.txt
Portuguese	lang-Portuguese.txt
Polish	lang-Polish.txt
Spanish	lang-Spanish.txt
Turkish	lang-Turkish.txt

Procedure

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

Configuration File	<y000000000028>.cfg	Specify the access URL of the language pack. For more information, refer to Language on page 250.

Specifying the Language to Use

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

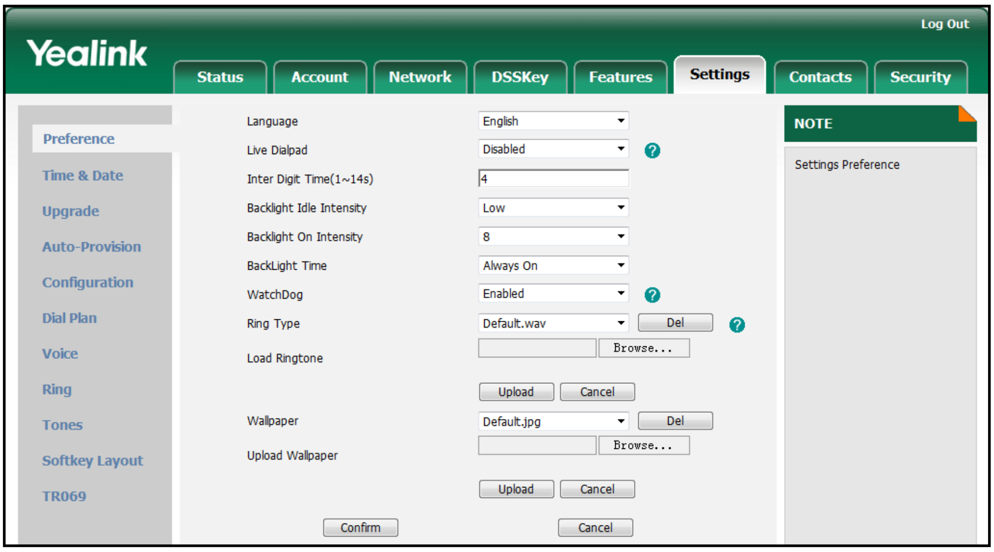
Procedure

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

Configuration File	<y000000000028>.cfg	Specify the languages for the phone user interface and the web user interface. For more information, refer to Language on page 250.
Local	Web User Interface	Specify the language for the web user interface. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-preference&q=load
	Phone User Interface	Specify the language for the phone user interface.

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

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



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

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

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

Softkey Layout

Softkey layout is used to customize the soft keys at the bottom of the phone LCD screen to best suit the needs of users. It can be configured based on the call states. In addition to specifying which soft keys to display, you can determine the display order of the soft keys. You can create a template about the softkey layout of the different call states. For more information on the softkey layout template, refer to Softkey Layout Template on page 211.

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

Call State		Default Soft Key	Optional Soft Key
CallFailed		NewCall Empty Empty Empty	Empty Switch Cancel
CallIn		Answer Forward Silence Reject	Empty Switch
Connecting	Connecting	Empty Empty Empty Cancel	Empty Switch
	SemiAttendTrans	Transfer Empty Empty Cancel	Empty Switch
Dialing		Send IME Delete Cancel	Empty History Directory Switch Line Selection Favorite Group Pickup Directed Pickup
RingBack	RingBack	Empty Empty	Empty Switch

Call State		Default Soft Key	Optional Soft Key
		Empty Cancel	
	SemiAttendTransBack	Transfer Empty Empty Cancel	Empty Switch
Talking	Talk	Transfer HOLD Conference Cancel	Empty MUTE SWAP NewCall Switch Answer Reject
	Hold	Transfer Resume NewCall Cancel	Empty Switch Answer Reject
	Held	Empty Empty Empty Cancel	Empty Switch Answer Reject NewCall
	PreTrans	Transfer IME Delete Cancel	Empty Directory Switch Send
	InConference	Empty Empty Empty Cancel	Empty Switch
	InConferenceTalk	Empty Empty Conference Cancel	Empty Switch

Call State		Default Soft Key	Optional Soft Key
	Conferenced	Empty Hold Split Cancel	Empty Switch Answer Reject Mute Manager

Procedure

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

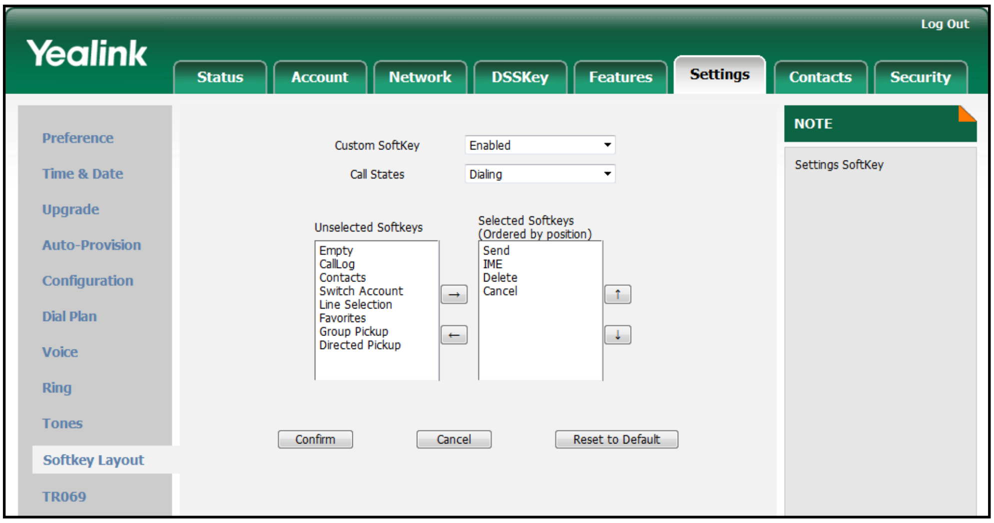
Configuration File	<y000000000028>.cfg	Specify the access URL of the softkey layout template. For more information, refer to Access URL of Softkey Layout on page 346.
Local	Web User Interface	Configure the softkey layout. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-softkey&q=load

To configure softkey layout via web user interface:

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

   The selected soft key appears in the **Selected Softkeys** column.
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, click ← .

To adjust the order of the soft key, click ↑ or ↓ .



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

Key as Send

The key as send feature allows assigning the pound key or star key as a send key. The send tone feature determines whether the IP phone plays a key tone when a user presses the send key.

Procedure

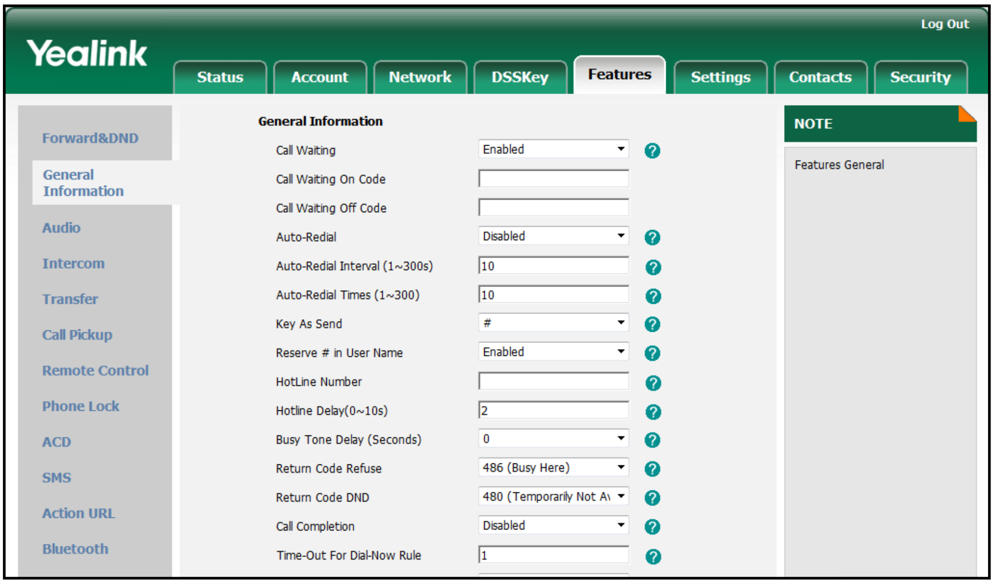
Key as send can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Configure the send key. Configure the send tone feature. For more information, refer to Key as Send on page 251.
Local	Web User Interface	Configure the send key. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-general&q=load Configure the send tone feature. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-audio&q=load
	Phone User Interface	Configure the send key.

To configure the send key via web user interface:

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

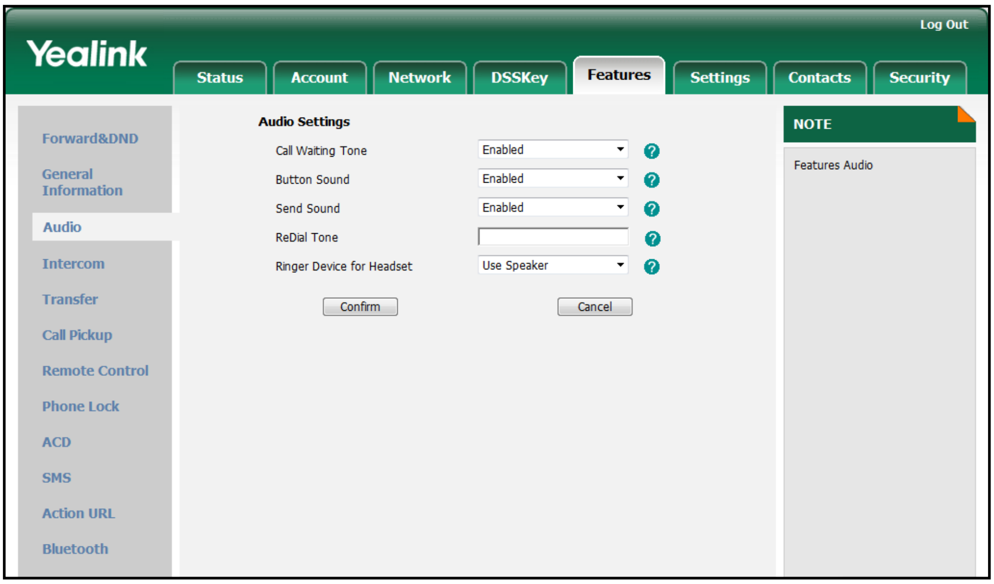
2. Select the desired value from the pull-down list of **Key As Send**.



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

To configure the send tone via web user interface:

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



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

To configure the send key via phone user interface:

1. Press **Menu**->**Call Feature**->**Others**->**General**.
2. Press or , or the **Switch** soft key to select **Key #** or **Key *** from the **Key As Send** field, or select **Disabled** to disable this feature.

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

Note

The send tone feature works only if the key tone feature is enabled. The key tone feature is enabled by default.

Hotline

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

Procedure

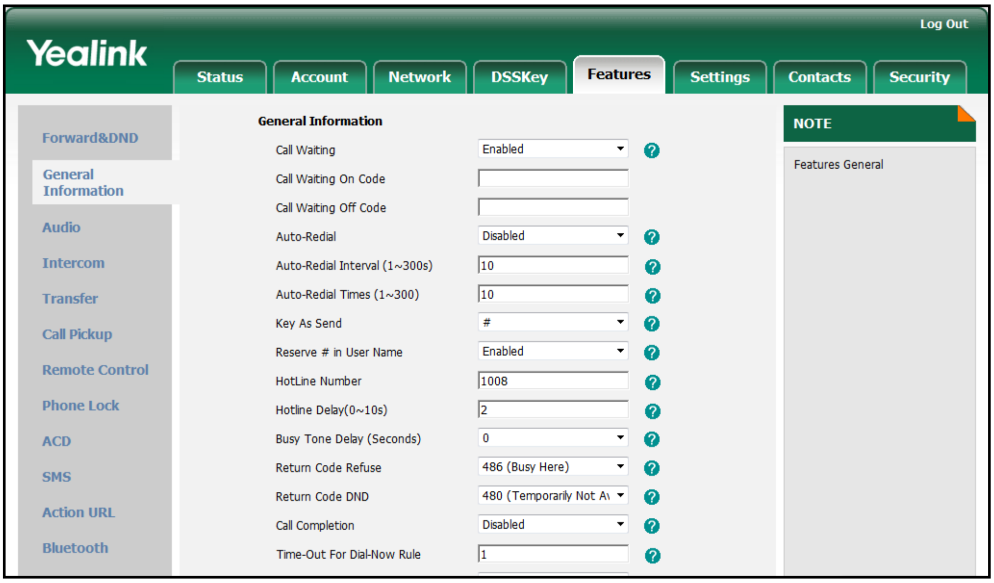
Hotline can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Configure the hotline number. Specify the time (in seconds) the IP phone waits to automatically dial out the hotline number. For more information, refer to Hotline on page 252.
Local	Web User Interface	Configure the hotline number. Specify the time (in seconds) the IP phone waits to 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 to automatically dial out the hotline number.

To configure hotline via web user interface:

1. Click on **Features**->**General Information**.
2. Enter the hotline number in the **Hotline Number** field.

3. Enter the delay time in the **Hotline Delay (0~10s)** field.



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

To configure hotline via phone user interface:

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

Call Log

Call log contains call information such as remote party identification, time and date, and call duration. The IP phones maintain a local call log. Call log consists of four lists: Dialed Calls, Received Calls, Missed Calls and Forwarded Calls. Each call log list supports to store 100 entries. To manage the entries of the call log lists, you should enable the IP phone to save call log in advance.

Procedure

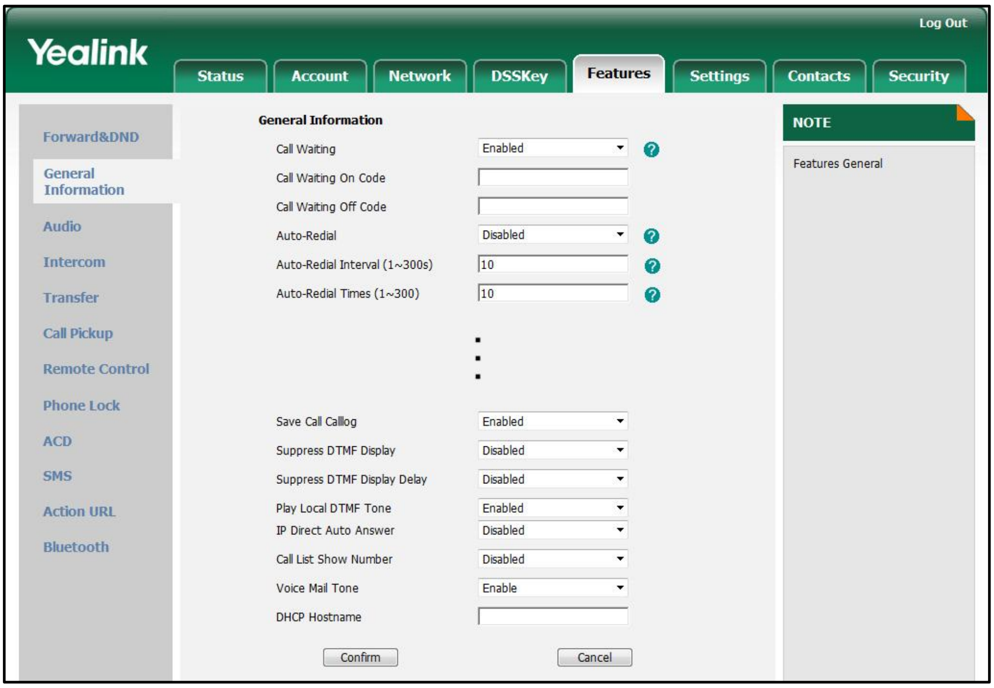
Call log can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Configure the call log. For more information, refer to Call Log on page 253.
Local	Web User Interface	Configure the call log. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

	Phone User Interface	Configure the call log.

To configure the call log via web user interface:

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



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

To configure the call log via phone user interface:

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

Missed Call Log

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

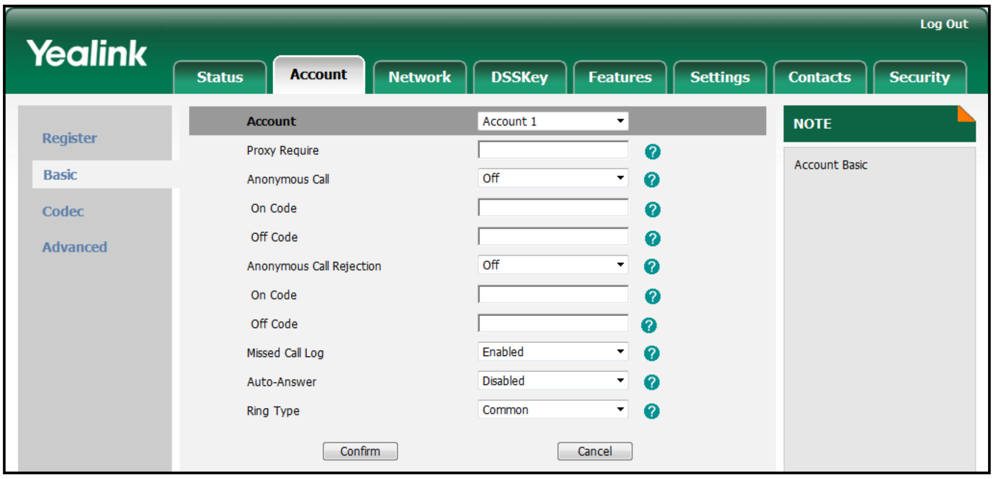
Procedure

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

Configuration File	<MAC>.cfg	Configure the missed call log feature. For more information, refer to Missed Call Log on page 254.
Local	Web User Interface	Configure the missed call log feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-basic&q=load&acc=0

To configure missed call log via web user interface:

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



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

Local Directory

The IP phone maintains a local directory. The local directory can store up to 1000 contacts. When adding a contact to the local directory, you can specify the account, ring tone and group for the contact in addition to name and phone numbers. The local directory can add new groups and add new contacts to different groups. The contacts can be created either one by one or in batch using a contact file. For more information on the contact file, refer to Local Contact File on page 213.

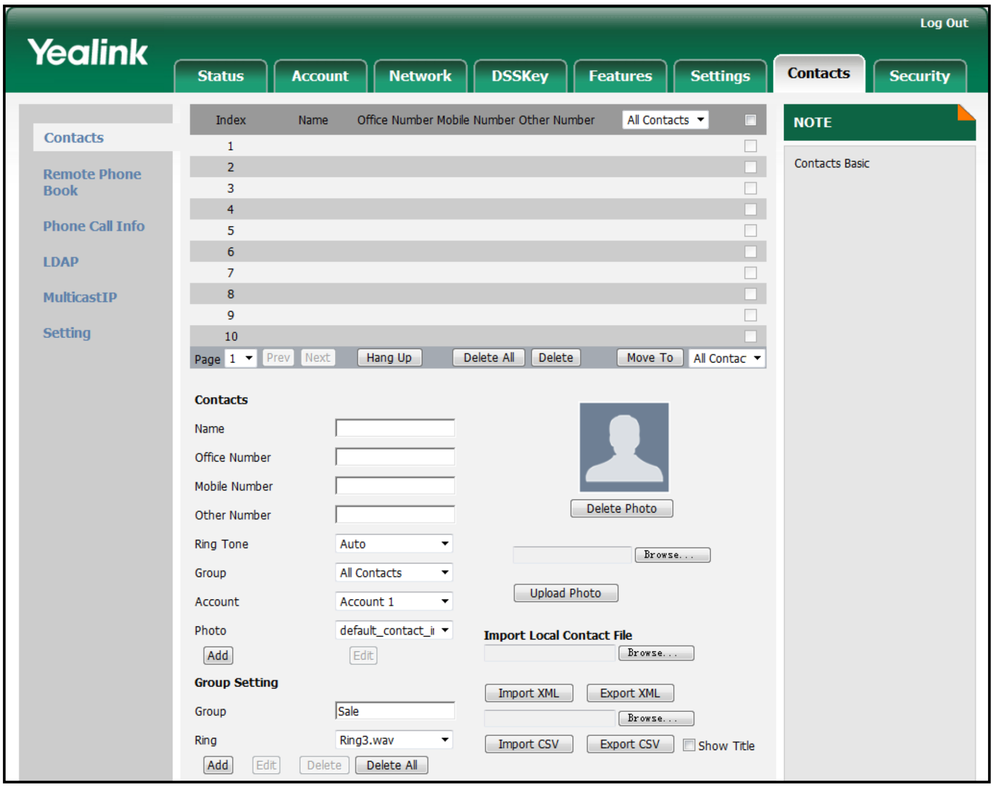
Procedure

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

Configuration File	<y000000000028>.cfg	Specify the access URL of the local contact file. For more information, refer to Access URL of Local Contact File on page 349.
Local	Web User Interface	Add a new group and a contact to the IP phone. **Navigate to:** http://<phoneIPAddress>/servlet?p=contactsbasic&q=load&num=1&group=
	Phone User Interface	Add a new group and a contact to the local directory directly.

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

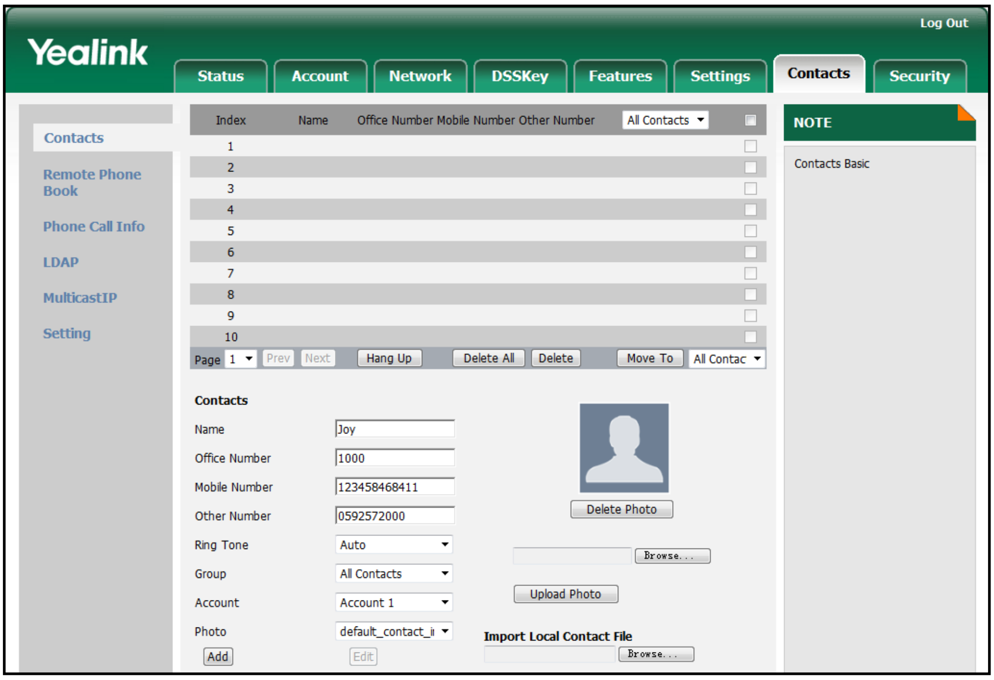
1. Click on **Contacts**->**Contacts**.
2. In the **Group Setting** block, enter the new group name in the **Group** field.
3. Select the desired group ring tone from the pull-down list of **Ring**.



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

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

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



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

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

1. Press **Menu**->**Directory**->**Local Contacts**.
2. Press the **Group** soft key.
3. Enter the desired group name in the **Group Name** field.
4. Press or to select the desired group ring tone from the **Ring Tones** field.
5. Press the **Save** soft key to accept the change or the **Back** soft key to cancel.

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

1. Press **Menu**->**Directory**->**Local Contacts**.
2. Select the desired contact group and 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 or , or the **Switch** soft key to select the desired photo from the **Photo** field.
8. Press the **Save** soft key to accept the change.

Live Dialpad

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

Procedure

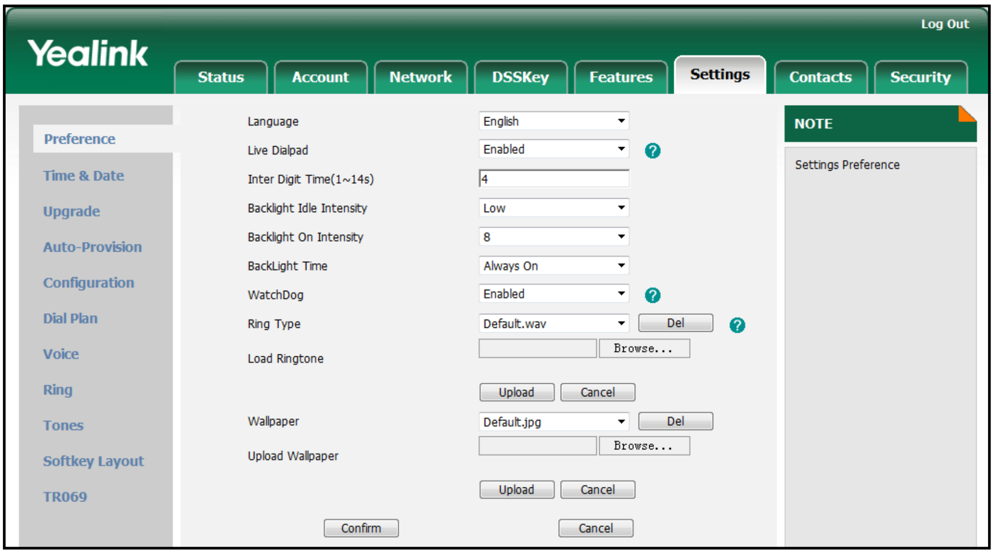
Live dialpad can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Configure the live dialpad feature. For more information, refer to Live Dialpad on page 255.
Local	Web User Interface	Configure the live dialpad feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-preference&q=load

To configure live dialpad via web user interface:

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

3. (If enabled) Enter the desired delay time (in seconds) in the **Inter Digit Time (1~14s)** field.



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

Call Waiting

The call waiting feature allows the IP phones to receive a new call when there is already an active call. The new call is presented to the user visually on the LCD screen. The call waiting tone feature enables the IP phones to play a short tone when receiving a new incoming call during a conversation. The tone is audible to remind the user of the new incoming call. The call waiting tone feature works only if the call waiting feature is enabled.

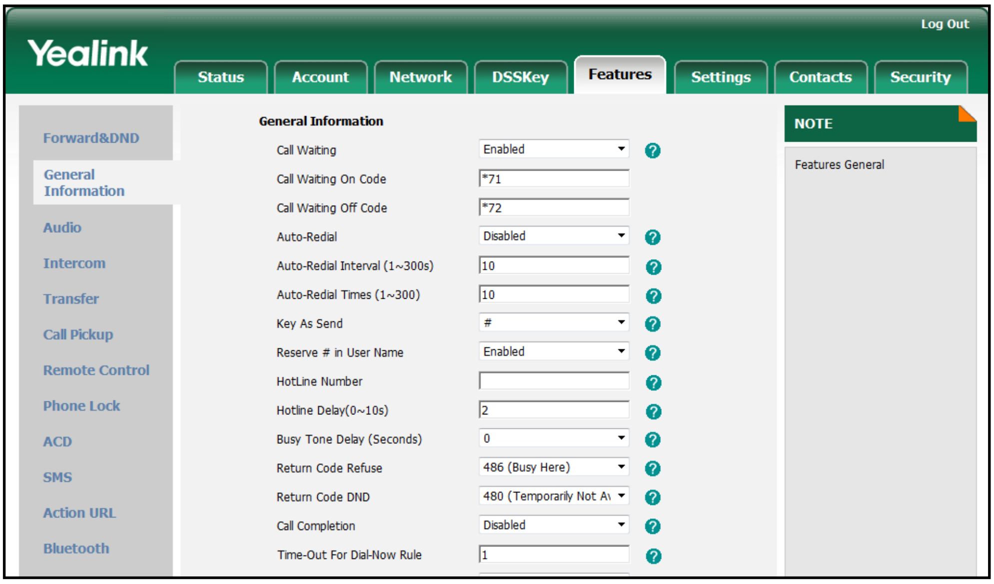
Procedure

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

Configuration File	<y000000000028>.cfg	Configure the call waiting feature. For more information, refer to Call Waiting on page 255.
Local	Web User Interface	Configure the call waiting feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load
	Phone User Interface	Configure the call waiting feature.

To configure call waiting via web user interface:

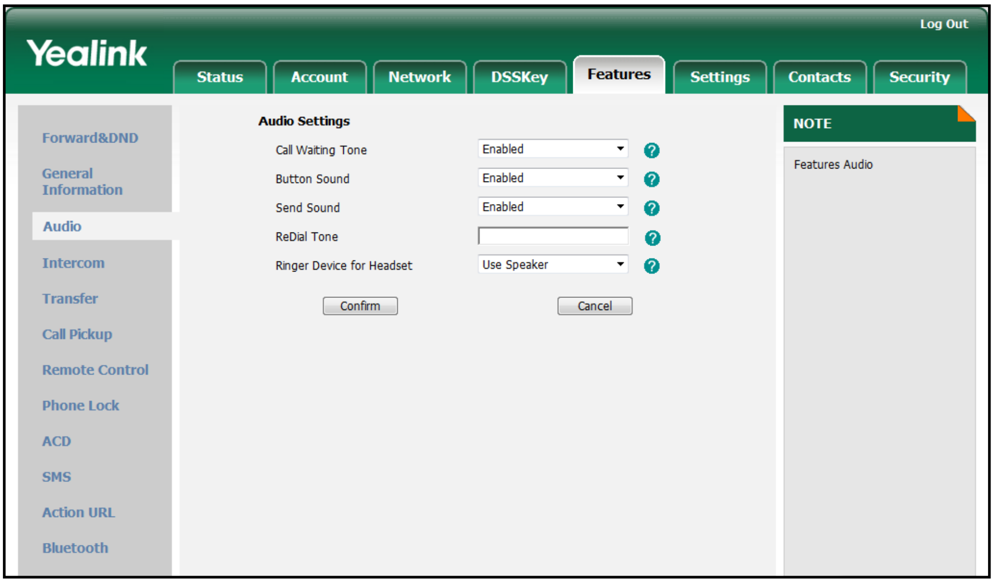
1. Click on **Features**->**General Information**.
2. Select the desired value from the pull-down list of **Call Waiting**.
3. (Optional.) Enter the call waiting on code in the **Call Waiting On Code** field.
4. (Optional.) Enter the call waiting off code in the **Call Waiting Off Code** field.



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

To configure the call waiting tone via web user interface:

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



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

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

1. Press **Menu**->**Call Feature**->**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

The auto redial feature allows the 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.

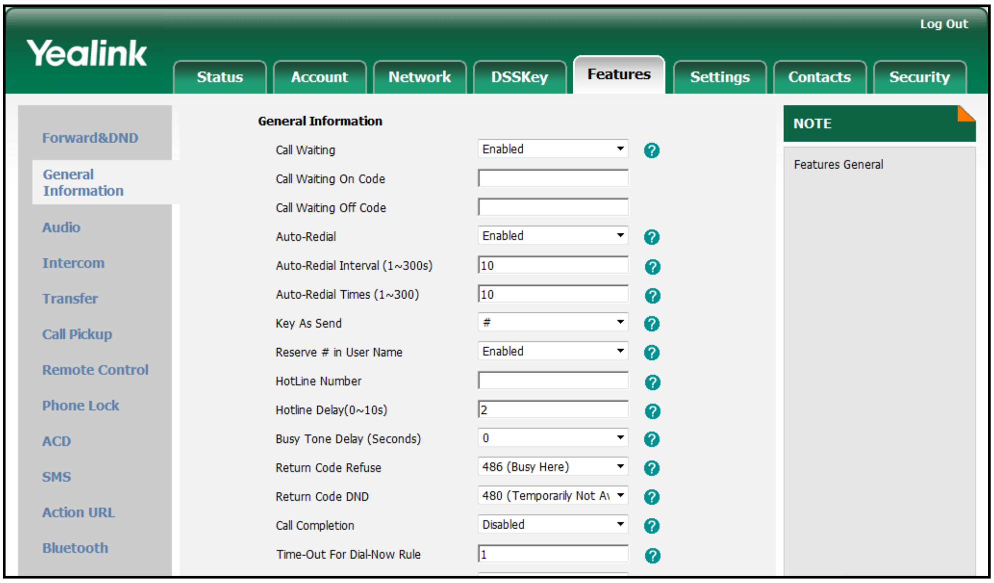
Configuration File	<y000000000028>.cfg	Configure the auto redial feature. For more information, refer to Auto Redial on page 256.
Local	Web User Interface	Configure the auto redial feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load
	Phone User Interface	Configure the auto redial feature.

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. (If enabled) Enter the desired time interval (in seconds) in the **Auto-Redial Interval (1~300s)** field.

   The default time interval is 10s.
4. (If enabled) Enter the desired times in the **Auto-Redial Times (1~300)** field.

The default times are 10.



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

To configure auto redial via phone user interface:

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

Auto Answer

The auto answer feature allows the IP phones to automatically answer an incoming call. The 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-account basis.

Procedure

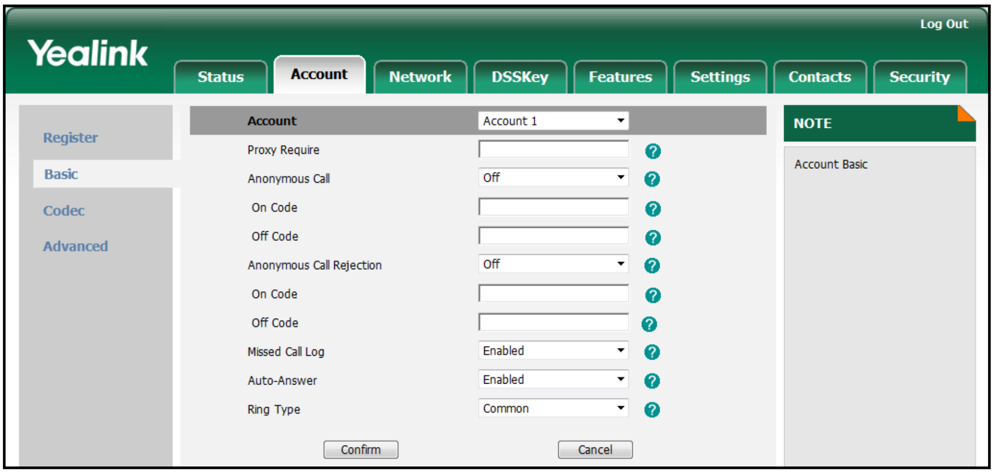
Auto answer can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure the auto answer feature. For more information, refer to Auto Answer on page 257.
Local	Web User Interface	Configure the auto answer feature. **Navigate to:**

		http://<phoneIPAddress>/servlet?p=account-basic&q=load&acc=0
	Phone User Interface	Configure the auto answer feature.

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 auto answer via phone user interface:

1. Press **Menu**->**Call Feature**->**Auto Answer**.
2. Select the desired line and then press the **Enter** soft key.
3. Press ◀ or ▶ , or the **Switch** soft key to select the desired value from the **Auto Answer** field.
4. Press the **Save** soft key to accept the change.

Call Completion

The call completion feature allows users to monitor the busy party and establish a call when the busy party becomes available to receive a call. There are several possible factors which can prevent a call from connecting successfully.

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

The 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 status changes of the busy party.

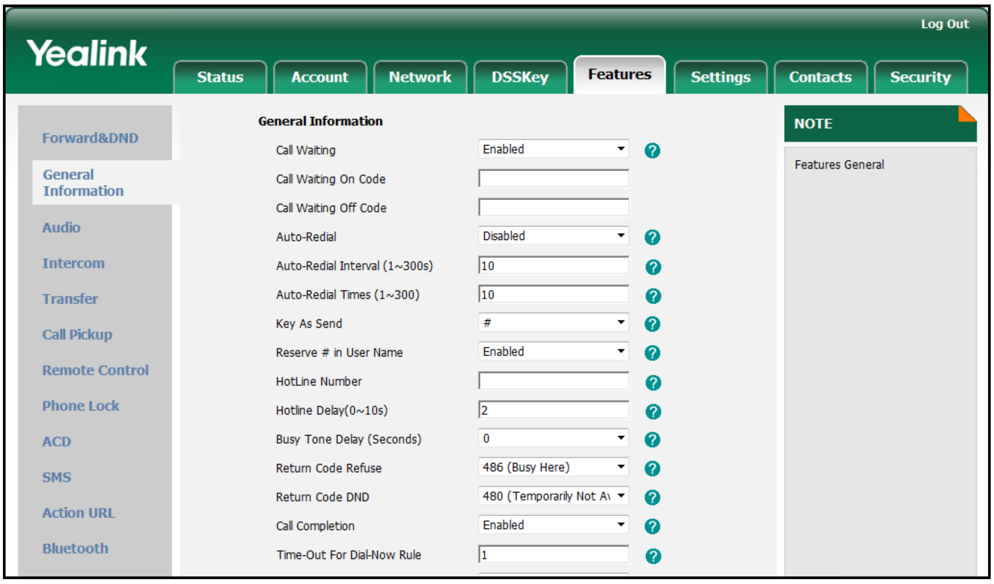
Procedure

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

Configuration File	<y000000000028>.cfg	Configure the call completion feature. For more information, refer to Call Completion on page 258.
Local	Web User Interface	Configure the call completion feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load
	Phone User Interface	Configure the call completion feature.

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**->**Call Feature**->**Others**->**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

The anonymous call feature allows the caller to block the identity from showing up to the callee when placing a call. The callee's phone LCD screen prompts an incoming call from anonymity.

The example of the SIP header for anonymity for reference:

```
Via: SIP/2.0/UDP 10.2.8.183:5063;branch=z9hG4bK1535948896
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=128043702
To: <sip:1011@10.2.1.199>
Call-ID: 1773251036@10.2.8.183
CSeq: 1 INVITE
Contact: <sip:1012@10.2.8.183:5063>
Content-Type: application/sdp
Allow: INVITE, INFO, PRACK, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REGISTER, SUBSCRIBE, REFER,
PUBLISH, UPDATE, MESSAGE
Max-Forwards: 70
User-Agent: Yealink SIP-T46G 28.71.0.10
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 or anonymous call off code configured on the IP phones is used to activate or deactivate the server-side anonymous call feature. They may vary on different servers.

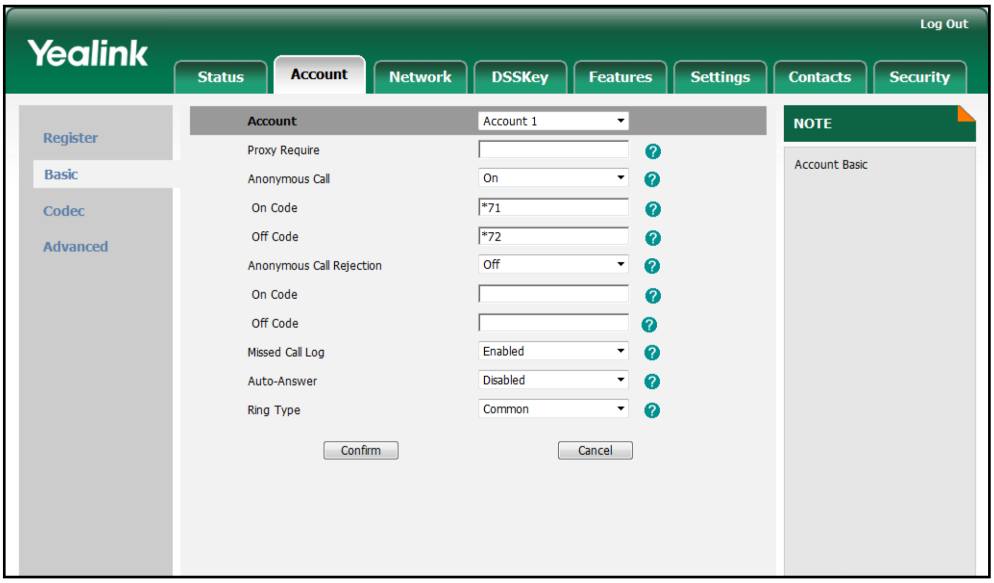
Procedure

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

Configuration File	<MAC>.cfg	Configure the anonymous call feature. For more information, refer to Anonymous Call on page 258.
Local	Web User Interface	Configure the anonymous call feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-basic&q=load&acc=0
	Phone User Interface	Configure the anonymous call feature.

To configure the anonymous call via web user interface:

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



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

To configure the anonymous call via phone user interface:

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

Anonymous Call Rejection

The anonymous call rejection feature allows the IP phones to automatically reject incoming calls from callers who deliberately block their identities from showing up. The anonymous caller's phone LCD screen presents "Anonymity Disallowed".

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

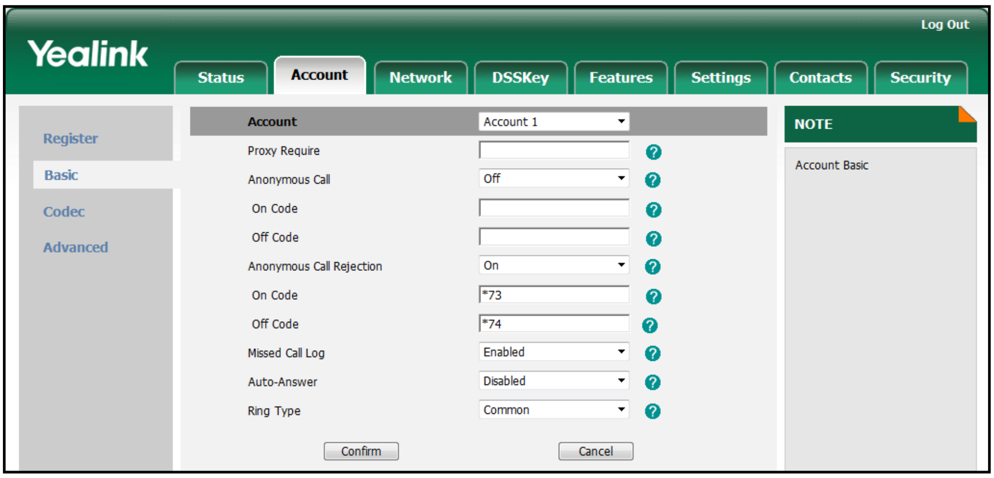
Procedure

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

Configuration File	<MAC>.cfg	Configure the anonymous call rejection feature. For more information, refer to Anonymous Call Rejection on page 259.
Local	Web User Interface	Configure the anonymous call rejection feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-basic&q=load&acc=0
	Phone User Interface	Configure the anonymous call rejection feature.

To configure anonymous call rejection via web user interface:

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



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

To configure anonymous call rejection via phone user interface:

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

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

Do Not Disturb

The Do Not Disturb (DND) feature allows the IP phones to ignore incoming calls. The DND feature is based on a phone or per-account depending on the DND mode. The following describes the two DND modes:

- **Phone** (default): When the DND mode is "Phone", it means the DND feature is effective for the IP phones.
- **Custom**: When the DND mode is "Custom", it means that you can configure the DND feature for each account.

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

The DND on code or DND off code configured on the IP phones is used to activate or 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 phones. The caller's phone LCD screen displays the received return code.

Procedure

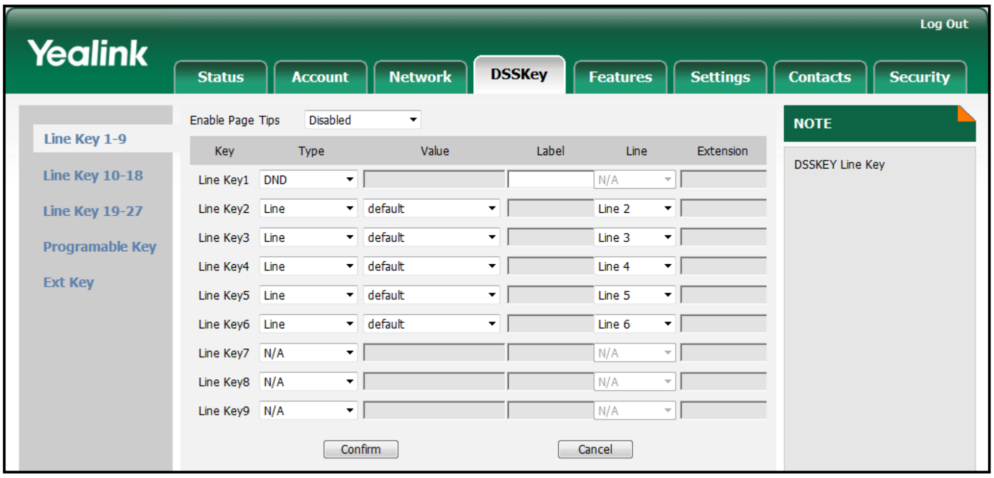
DND can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure the DND feature in the custom mode. For more information, refer to Do Not Disturb on page 261.
	<y000000000028>.cfg	Assign a DND key. For more information, refer to DND Key on page 355. Configure the DND mode. Configure the DND feature in the phone mode.

		Specify the return code and the reason of the SIP response message. For more information, refer to Do Not Disturb on page 261.
Local	Web User Interface	Assign a DND key. **Navigate to**: http://<phoneIPAddress>/servlet?p=dsskey&model=1&q=load&linepage=1 Configure the DND feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-forward&q=load Specify the return code and the reason of the SIP response message. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load
	Phone User Interface	Assign a DND key. Configure the DND feature.

To configure a DND key via web user interface:

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



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

To configure the DND feature via web user interface:

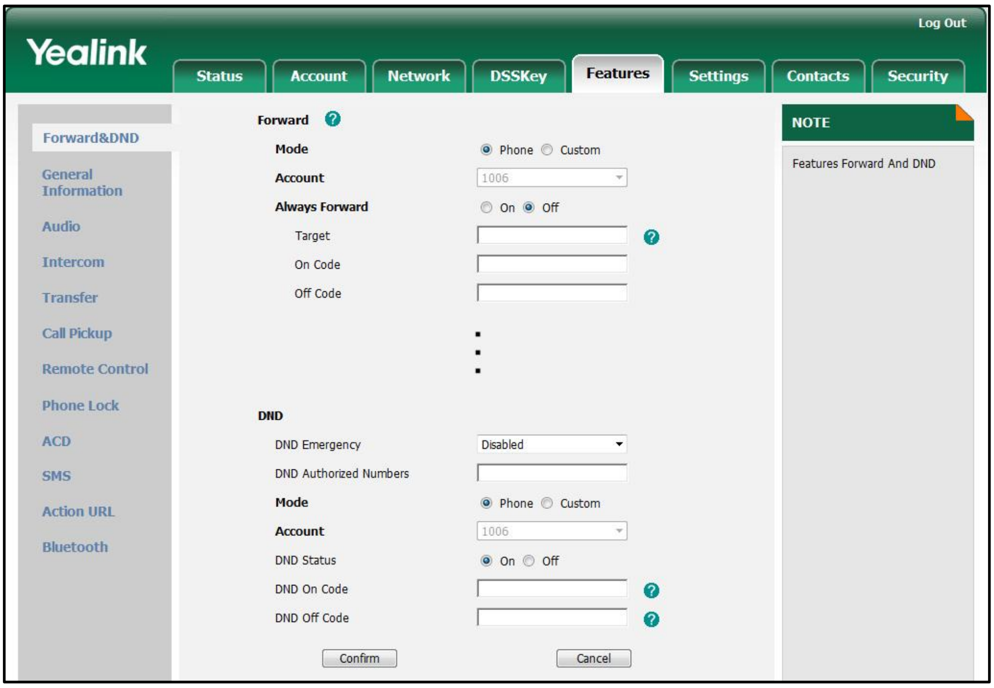
1. Click on **Features**->**Forward & DND**.
2. In the **DND** block, mark the desired radio box in the **Mode** field.

   a) If you select **Phone**:

      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.



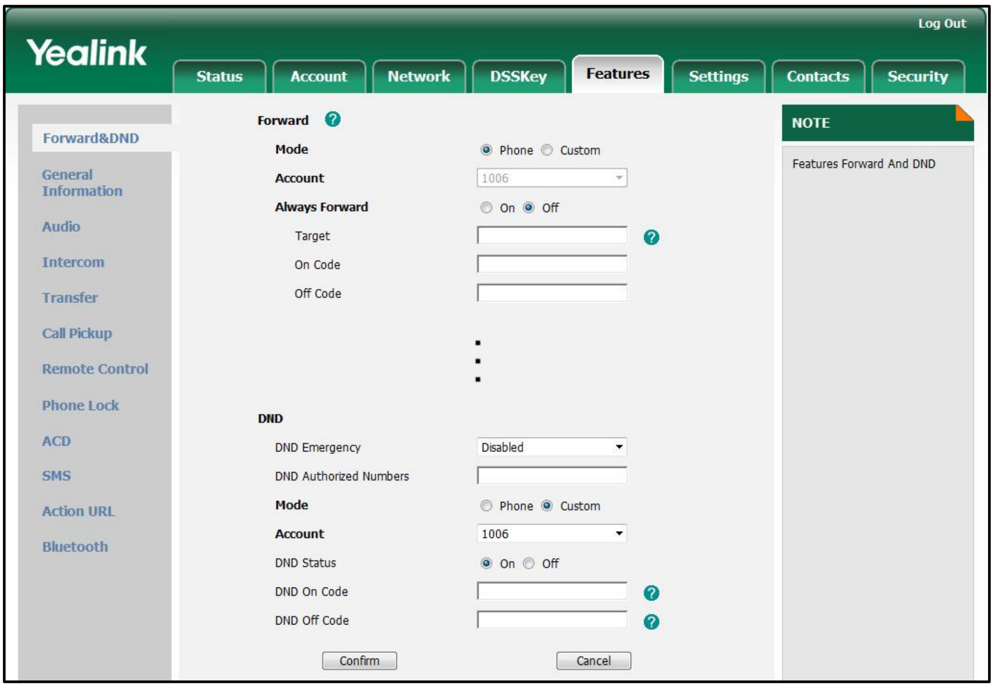
   b) If you select **Custom**:

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

      2) Mark the desired value in the **DND Status** field.

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

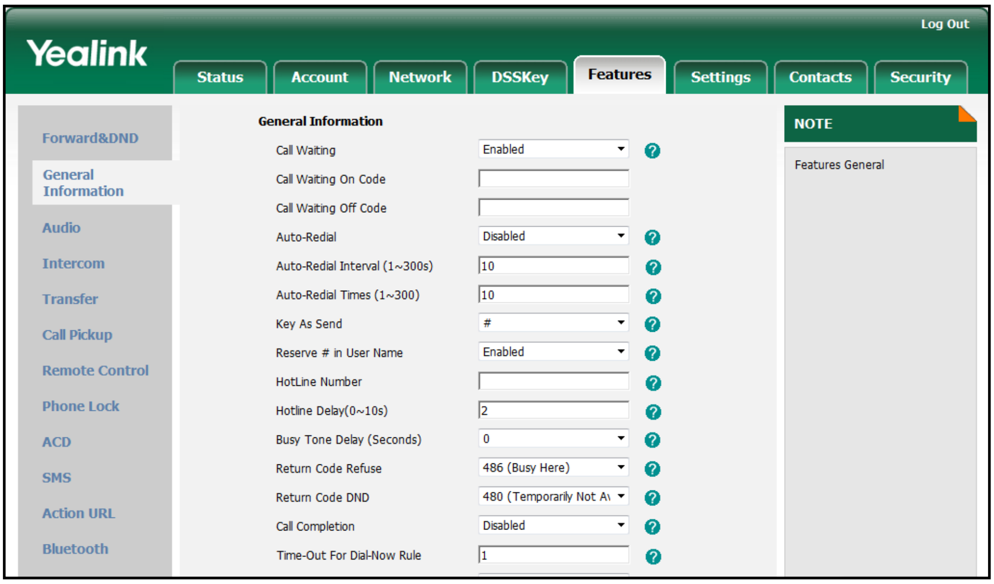
4) (Optional.) Enter the DND off code in the **DND Off Code** field.



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

To specify the return code and the reason via web user interface:

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



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

To configure a DND key via phone user interface:

1. Press **Menu**->**Call Feature**->**DSS Keys**.
2. Select the desired DSS key.

3. Press or , or the **Switch** soft key to select **Key Event** from the **Type** field.
4. Press or , or the **Switch** soft key to select **DND** from the **Key Event** field.
5. (Optional.) Enter the string that will appear on the LCD screen in the **Label** field.
6. Press the **Save** soft key to accept the change.

To configure 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 the accounts registered on the IP phone.
2. Press or to select the desired account.
3. Press or soft key to select **On** to activate DND.
4. Press the **Save** soft key to accept the change.

To configure DND in the custom mode for all accounts 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 the accounts registered on the IP phone.
2. Press the **All On** soft key to activate DND for all accounts.
3. 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 breaks, when one party releases a call. Busy tone delay defines a period of time for which the busy tone is audible.

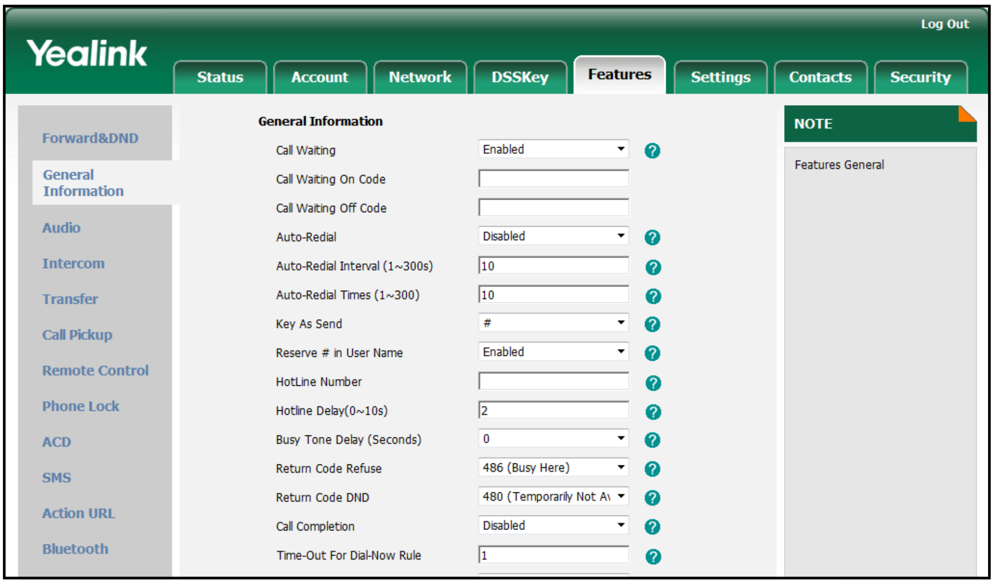
Procedure

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

Configuration File	<y000000000028>.cfg	Configure the busy tone delay feature. For more information, refer to Busy Tone Delay on page 264.
Local	Web User Interface	Configure the busy tone delay feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

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

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

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

Procedure

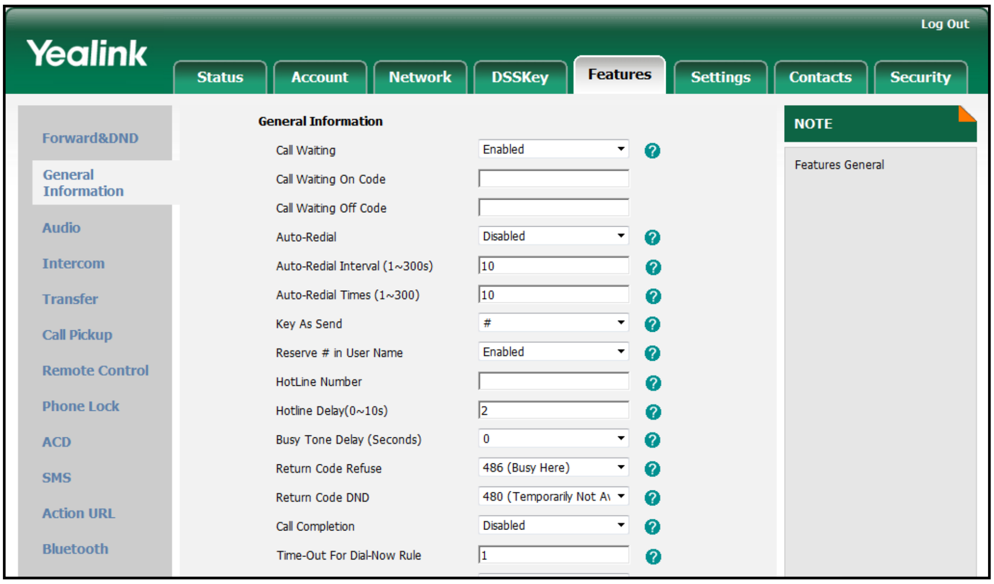
Return code for call rejection can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Configure the return code when refusing a call. For more information, refer to Return Code When Refuse on page 264.
Local	Web User Interface	Configure the return code when refusing a call. **Navigate to**:

		http://<phoneIPAddress>/servlet ?p=features-general&q=load

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

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

180 Ring Workaround

The 180 ring workaround feature 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 the IP phones to resume and play the local ringback tone upon a subsequent 180 message received.

Procedure

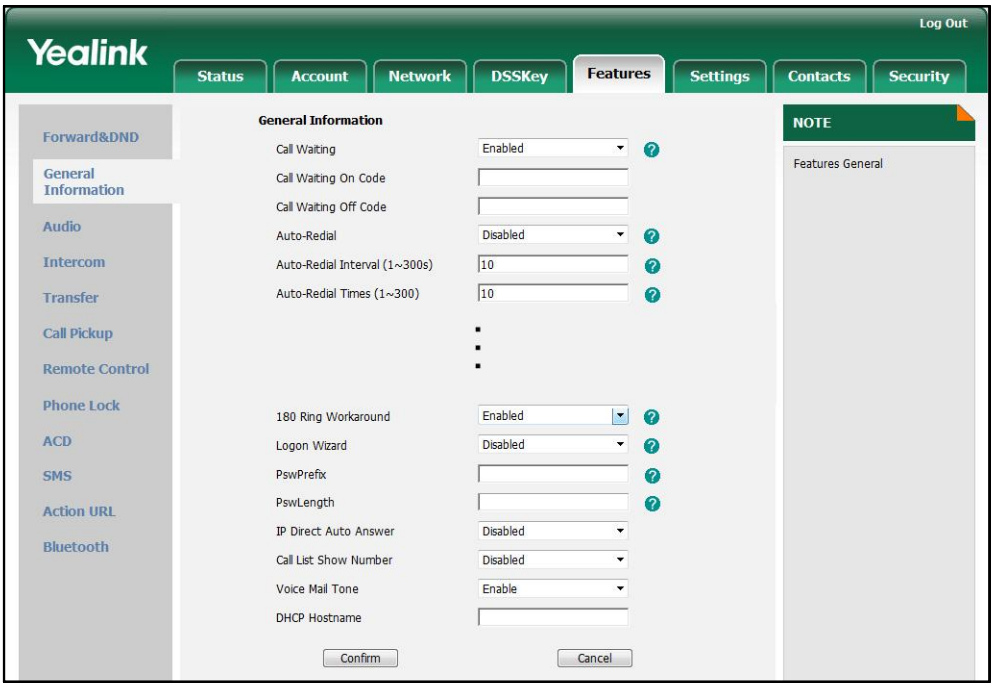
180 ring workaround can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Configure the 180 ring

		workaround feature. For more information, refer to 180 Ring Workaround on page 265.
Local	Web User Interface	Configure the 180 ring workaround feature. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-general&q=load

To configure 180 ring workaround via web user interface:

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



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

Use Outbound Proxy in Dialog

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

Note

To use this feature, make sure the outbound server is configured on the IP phone in advance.

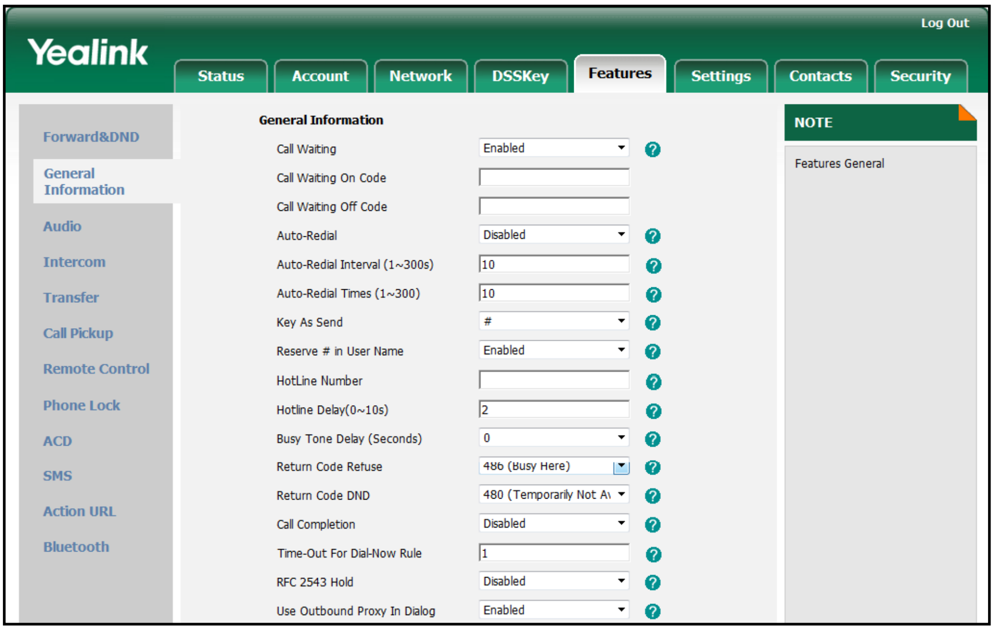
Procedure

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

Configuration File	<y000000000028>.cfg	Specify whether to use outbound proxy in a dialog. For more information, refer to Use Outbound Proxy in Dialog on page 265.
Local	Web User Interface	Specify whether to use outbound proxy in a dialog. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

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

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



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

SIP Session Timer

SIP session timers T1, T2 and T4 are SIP transaction layer timers defined in RFC 3261. Timer T1 is an estimate of the Round Trip Time (RTT) of transactions between a SIP client and SIP server. Timer T2 represents the maximum retransmitting time of any SIP request message. The re-transmitting and doubling of T1 continues 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 SIP 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 the SIP session timer feature. For more information, refer to SIP Session Timer on page 266.
Local	Web User Interface	Configure the SIP session timer feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

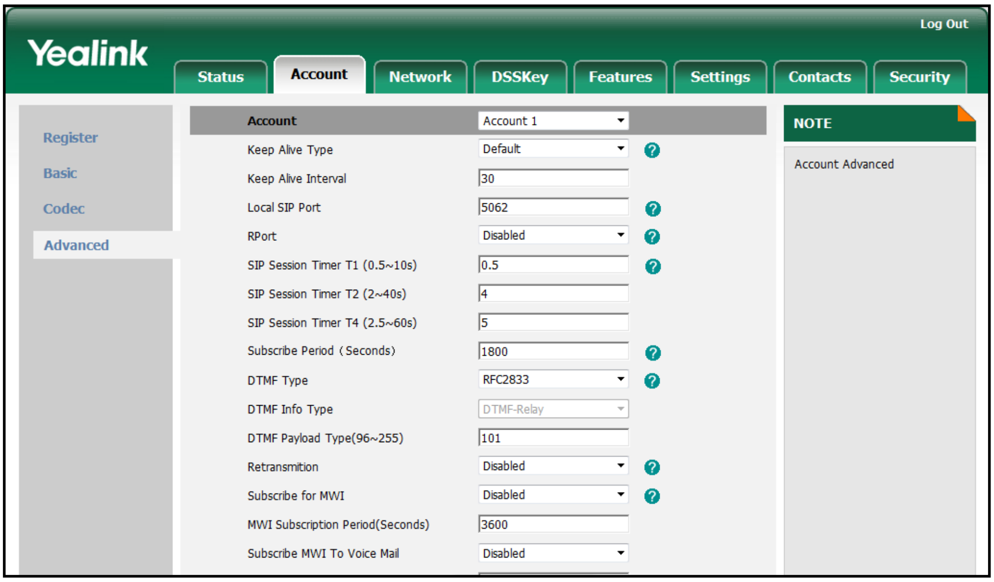
To configure the session timer via web user interface:

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

The session timer feature allows for a periodic refresh of SIP sessions through a re-INVITE or an UPDATE request to determine whether the SIP session is still active. Session timer is specified in RFC 4028. The 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 message at or before the negotiated session expiration.

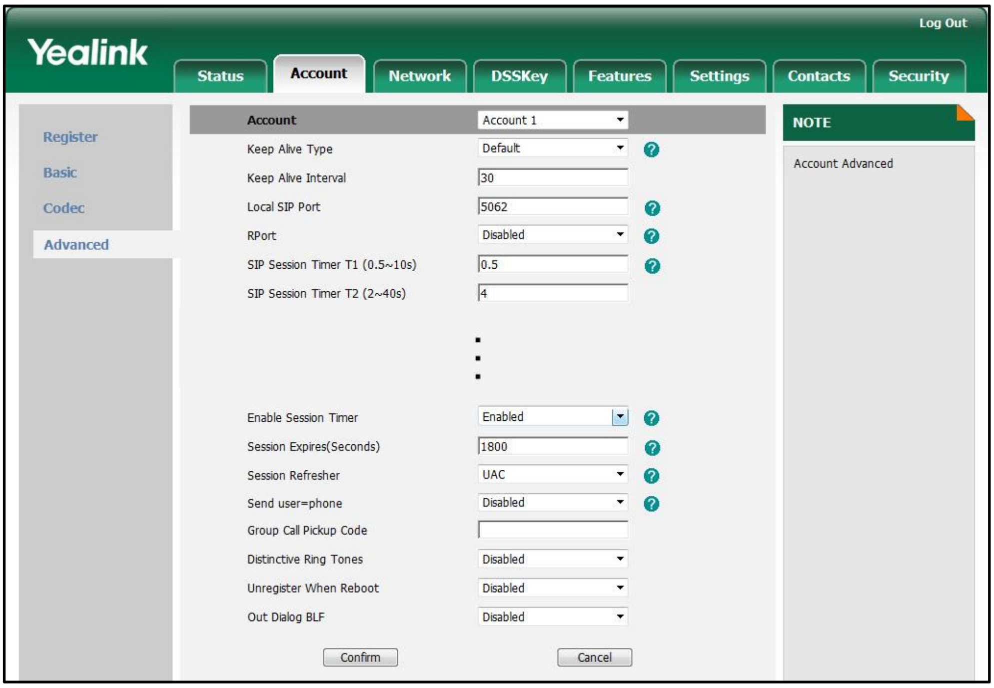
Procedure

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

Configuration File	<MAC>.cfg	Configure the session timer feature. For more information, refer to Session Timer on page 267.
Local	Web User Interface	Configure the session timer feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

To configure the 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 **Enable Session Timer**.
5. Enter the desired time interval in the **Session Expires (Seconds)** field.
6. Select the desired refresher from the pull-down list of **Session Refresher**.



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

Call Hold

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

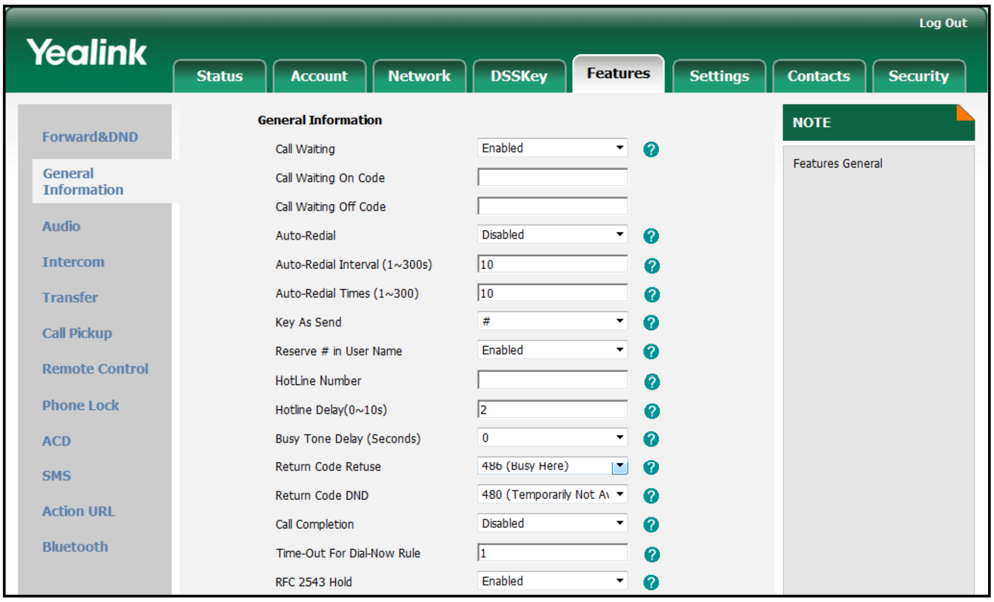
Procedure

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

Configuration File	<y000000000028>.cfg	Configure the call hold tone and call hold tone delay. Specify whether RFC 2543 (c=0.0.0.0) outgoing hold signaling is used. For more information, refer to Call Hold on page 268.
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

To configure the 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**.



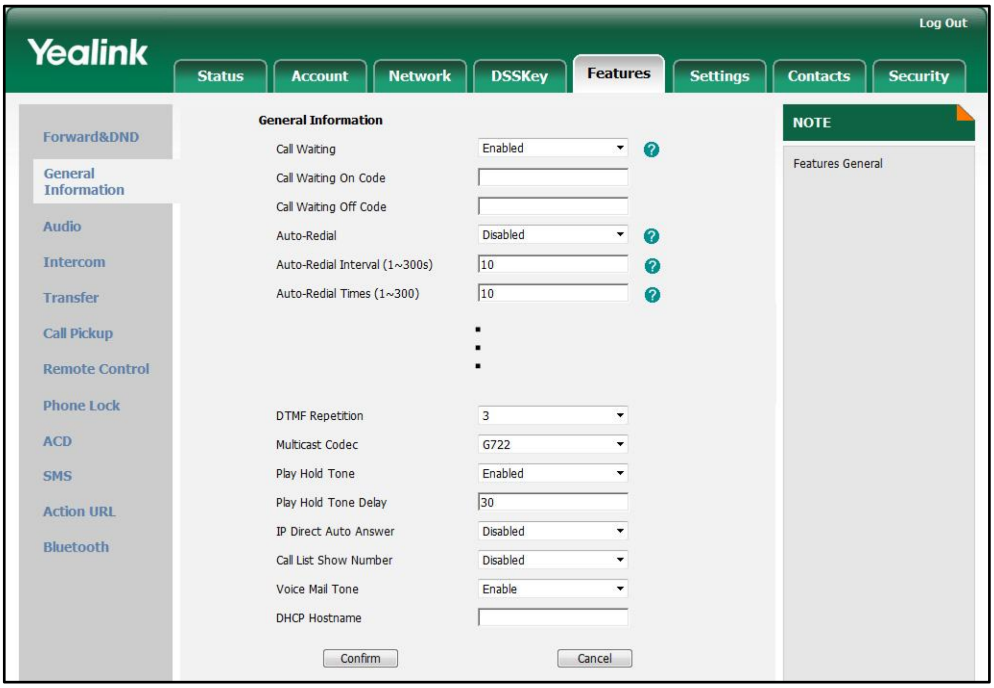
3. Click **Confirm** to accept the change.

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

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

2. Select the desired value from the pull-down list of **Play Hold Tone**.

3. Enter the desired time in the **Play Hold Tone Delay** field.



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

Call Forward

The call forward feature allows users to redirect an incoming call to a third party. The IP phones support to redirect an incoming INVITE message by responding with a 302 Moved Temporarily message. This response contains a Contact header with a new URI that should be tried. IP phones offer three types of forward:

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

The call forward feature is based on a phone or per-account depending on the call forward mode. The following describes the call forward modes:

- **Phone** (default): Call forward in phone mode means that the call forward feature is effective for the IP phone.
- **Custom:** Call forward in custom mode means that you can configure the call forward feature for each account.

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

Forward International

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

Procedure

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

Configuration File	<MAC>.cfg	Configure the call forward feature in custom mode. For more information, refer to Call Forward on page 269.
	<y000000000028>.cfg	Configure the call forward mode. Configure the call forward feature in phone mode. Configure the forward international feature. For more information, refer to Call Forward on page 269.
Local	Web User Interface	Configure the call forward feature. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-forward&q=load Configure the forward international feature. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-general&q=load
	Phone User Interface	Configure the call forward feature.

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.

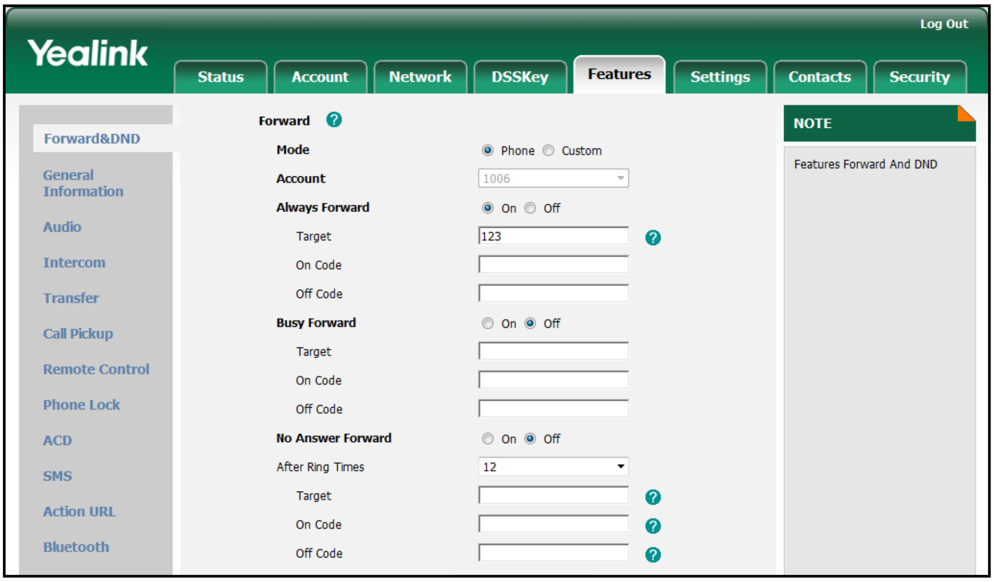
   a) If you select **Phone**:

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

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

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

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



b) If you select **Custom**:

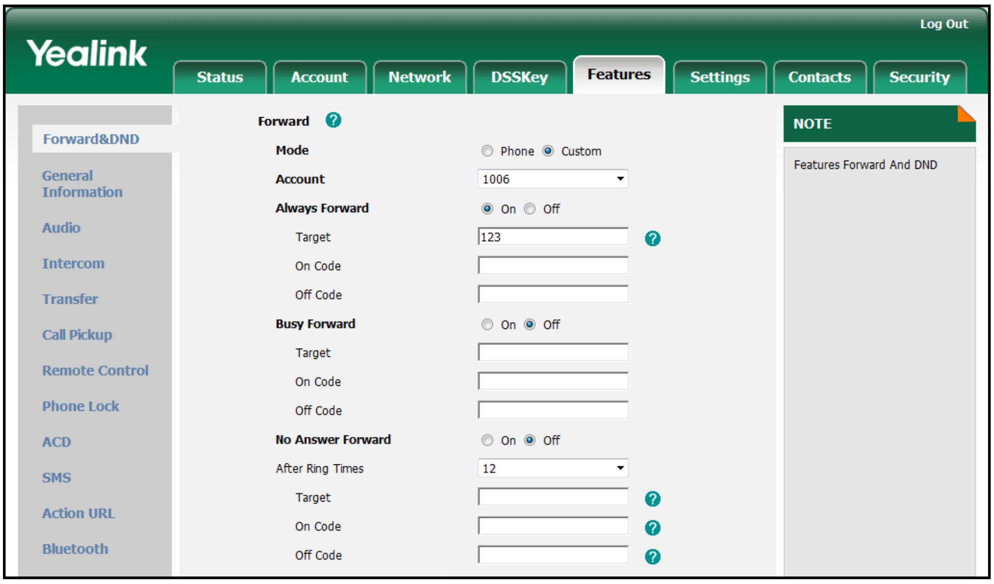
1) Select the desired account from the pull-down list of **Account**.

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

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

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

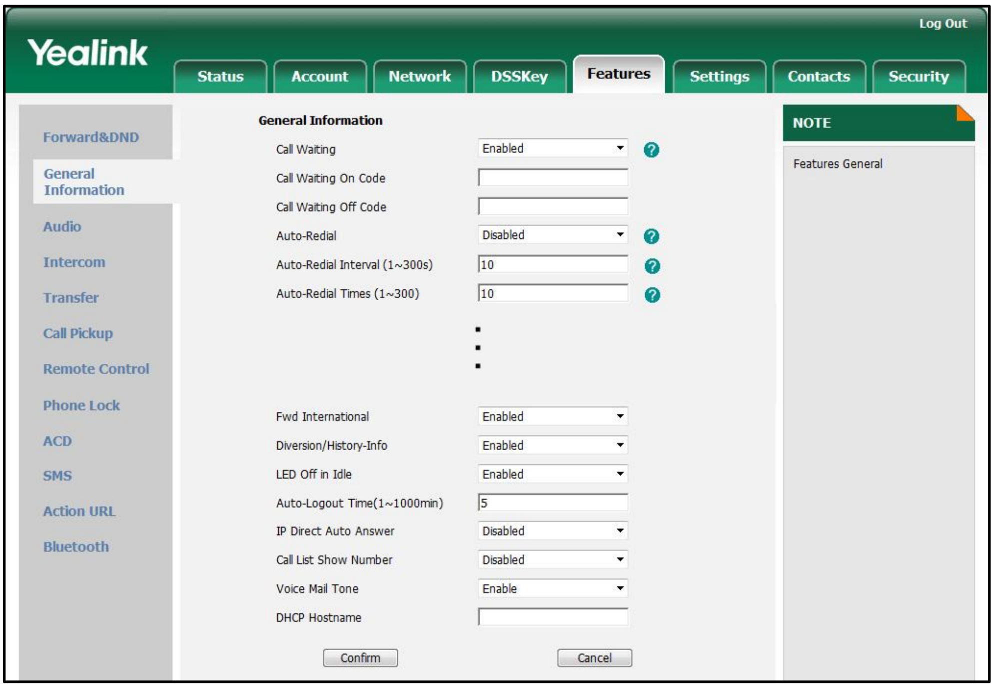
4) Select the ring time to wait before forwarding from the pull-down list of **After Ring Times** (only for the no answer forward).



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

To configure the forward international feature via web user interface:

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



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

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

1. Press **Menu**->**Call Feature**->**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 **Target** 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 **Target** 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 **Target** field.

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

      The default ring time is 12 seconds.

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

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

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

1. Press **Menu**->**Call Feature**->**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 **Target** 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 as below:

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 **Target** 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 as below:

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 **Target** 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 as below:

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

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

The LCD screen prompts “Copy to All Lines?”.

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

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

Call Transfer

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

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

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

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

Procedure

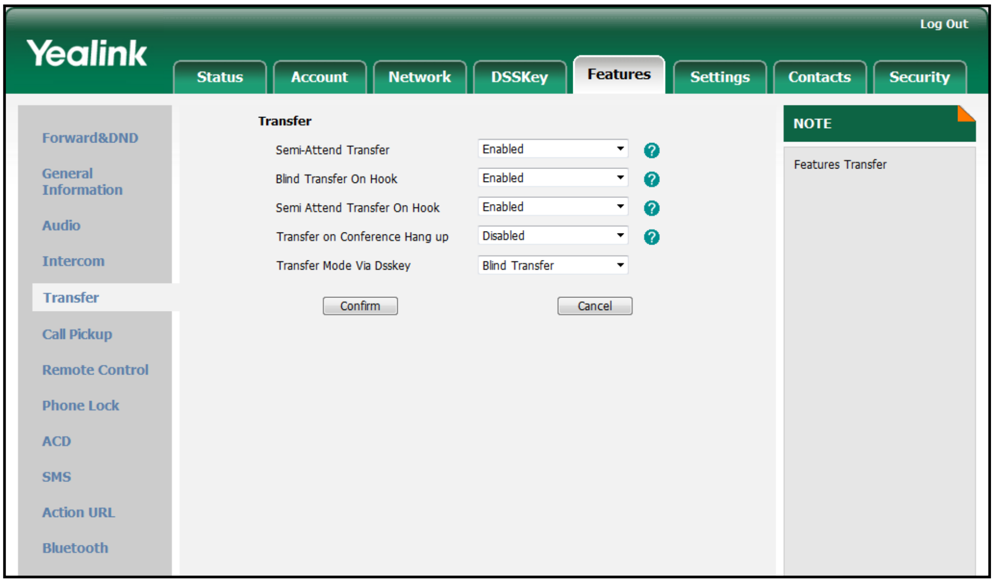
Call transfer can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Specify whether to complete the transfer through on-hook. Configure the semi-attended transfer feature. For more information, refer to Call Transfer on page 279.
Local	Web User Interface	Specify whether to complete the transfer through on-hook. Configure the semi-attended transfer feature. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-transfer&q=load

To configure call transfer via web user interface:

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

Transfer on Hook and **Semi 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

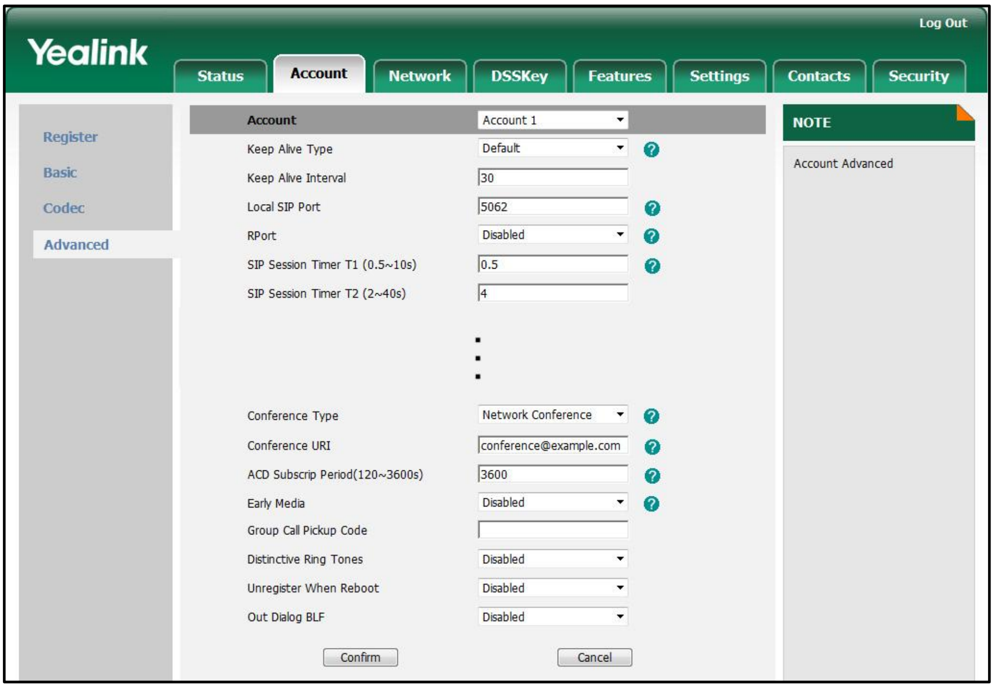
Network conference can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure the network conference. For more information, refer to Network Conference on page 280.
Local	Web User Interface	Configure the network conference. **Navigate to:** http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

To configure the network conference via web user interface:

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

3. Click on **Advanced**.
4. Select **Network** from the pull-down list of **Conference Type**.
5. Enter the conference URI in the **Conference URI** field.



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

Transfer on Conference Hang Up

For local conference, all parties release the call when the conference initiator drops the conference call. The transfer on conference hang up feature allows the other two parties remain connected when the conference initiator drops the conference call.

Procedure

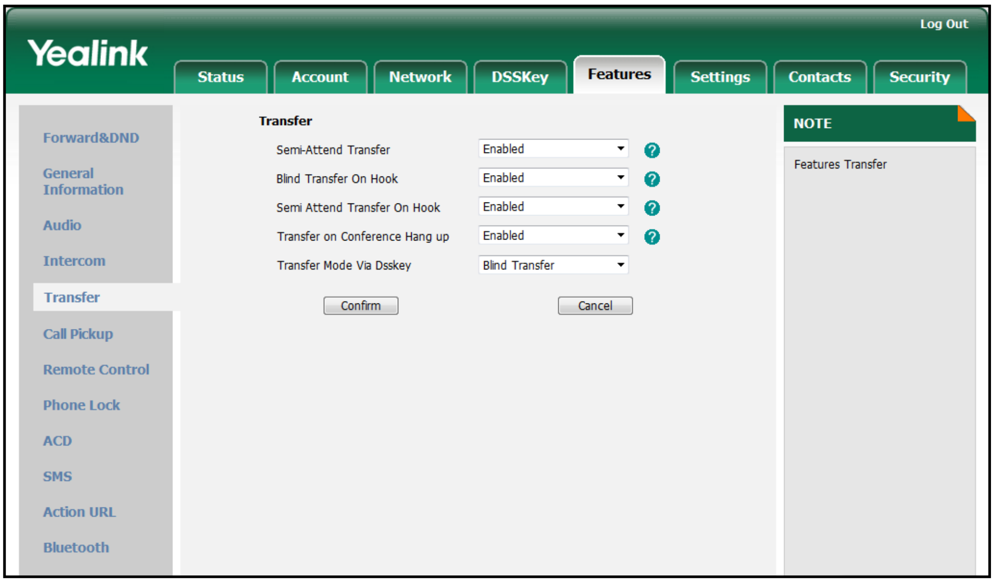
Transfer on conference hang up feature can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Configure the transfer on conference hang up feature. For more information, refer to Transfer on Conference Hang Up on page 281.
Local	Web User Interface	Configure the transfer on conference hang up feature. **Navigate to**: http://<phoneIPAddress>/servlet

		?p=features-transfer&q=load

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

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



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

Directed Call Pickup

Directed call pickup is used for picking up an incoming call on a specific extension. A user can pick up the incoming call using a directed pickup key or the DPickup soft key. This feature depends on support from a SIP server. Directed call pickup is implemented by dialing the directed call pickup code followed by a specific extension. The directed call pickup code can be configured on a phone or per-account basis.

Note

We recommend that you should not 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-account basis. For more information, refer to

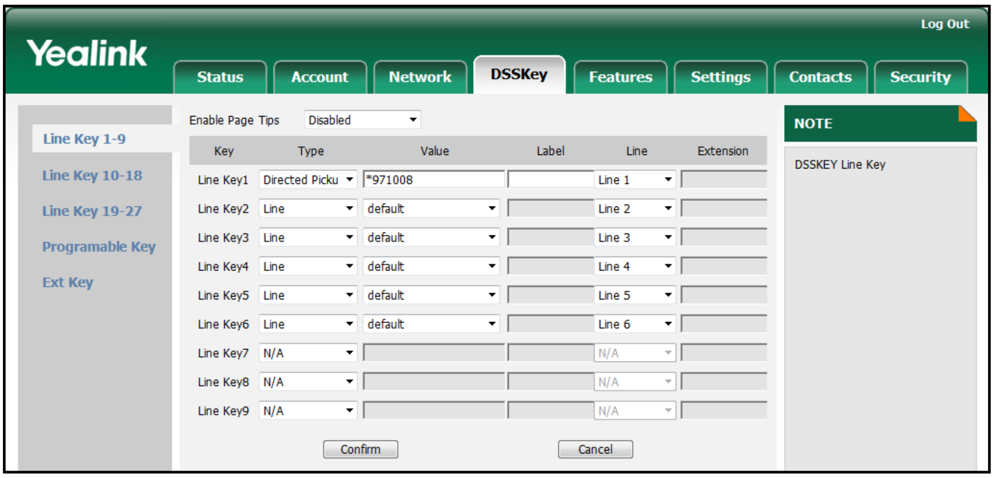
		Directed Call Pickup on page 282.
	<y000000000028>.cfg	Assign a directed call pickup key. For more information, refer to Directed Call Pickup Key on page 356. Configure the directed call pickup feature on a phone basis. For more information, refer to Directed Call Pickup on page 281.
Local	Web User Interface	Assign a directed call pickup key. **Navigate to:** http://<phoneIPAddress>/servlet?p=dsskey&model=1&q=load&linepage=1 Configure the directed call pickup feature on a phone basis. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-callpickup&q=load Configure the directed call pickup code on a per-account basis. **Navigate to:** http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0
	Phone User Interface	Assign a directed call pickup key.

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

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

field.

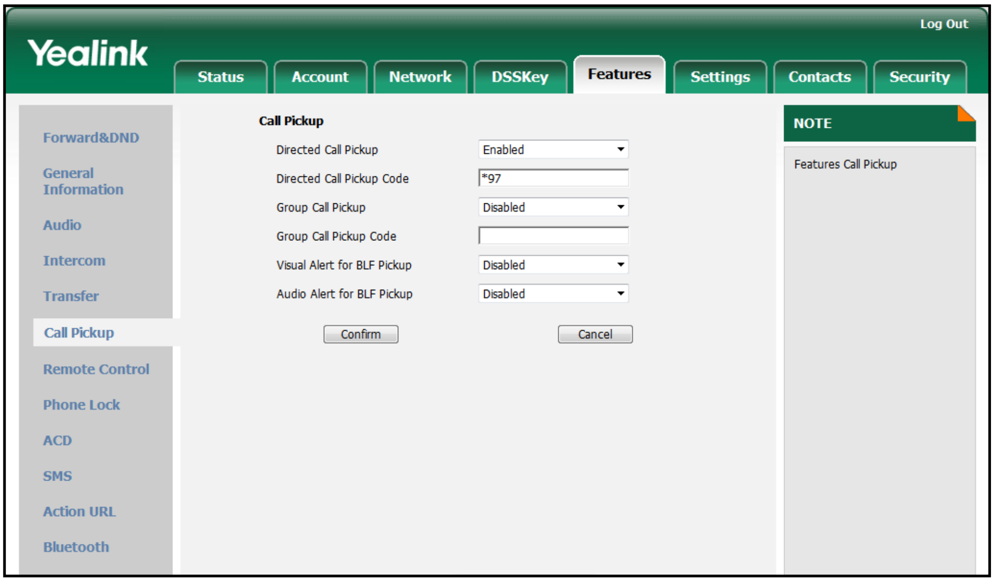
4. Select the desired line from the pull-down list of **Line**.



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

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

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

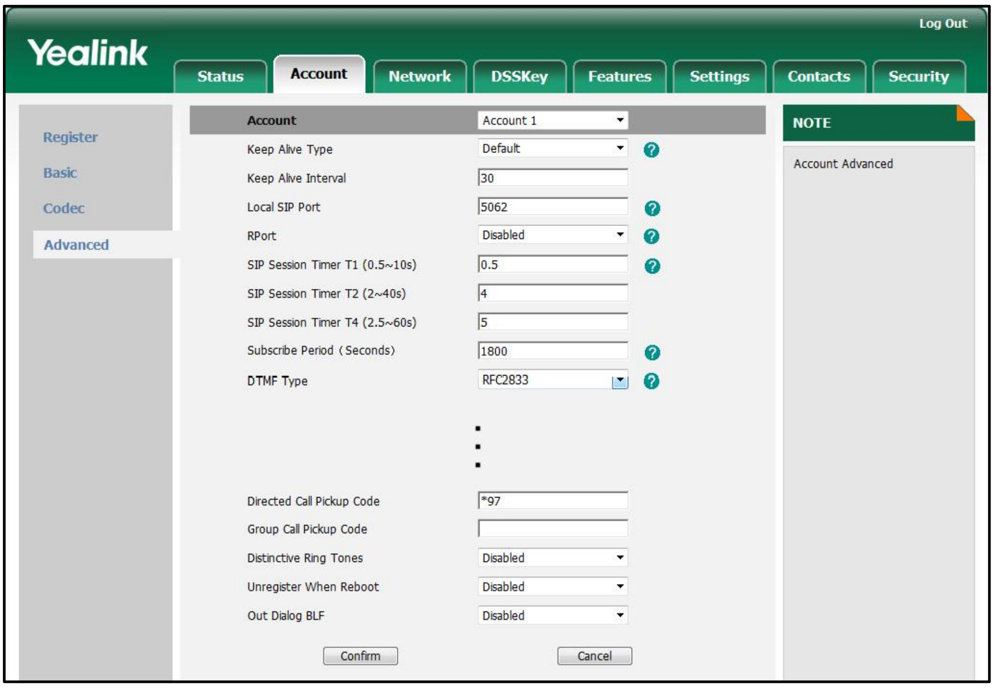


4. Click **Confirm** to accept the change.

To configure the directed call pickup code on a per-account 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**->**Call Feature**->**DSS Keys**.
2. Select the desired DSS key.
3. Press or , or the **Switch** soft key to select **Key Event** from the **Type** field.
4. Press or , or the **Switch** soft key to select **Pick Up** from the **Key Event** field.
5. Press or , or the **Switch** soft key to select the desired line from the **Account ID** field.
6. (Optional.) Enter the string that will appear on the LCD screen in the **Label** field.
7. Enter the directed call pickup code followed by the specific extension in the **Value** field.
8. 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 there are many incoming calls at the same time, the user will pick up the first incoming call. The user can pick up the incoming call using a group pickup key or the GPickup soft key. This feature depends on support from a SIP server. Group call pickup is implemented by dialing the group call pickup code. The group call pickup code can be configured on a phone or per-account basis.

Procedure

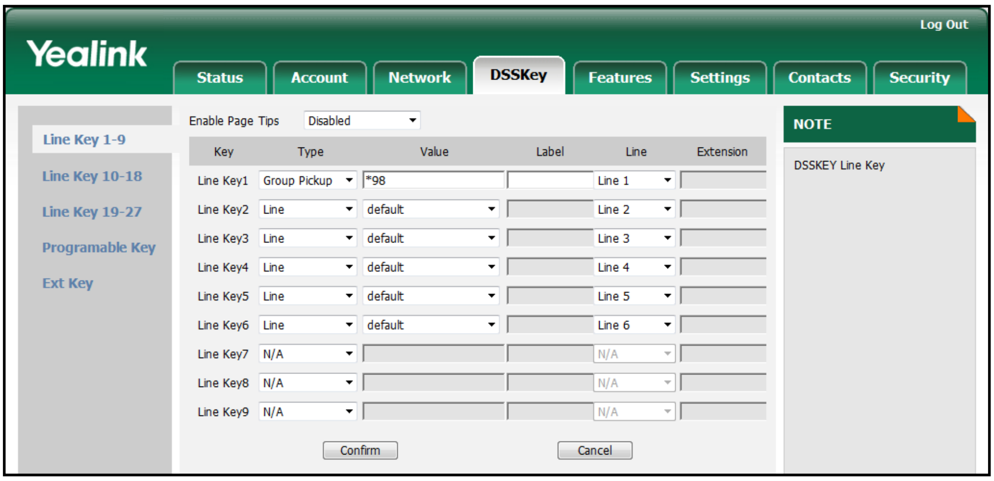
Group call pickup can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure the group call pickup code on a per-account basis. For more information, refer to Group Call Pickup on page 283.
	<y000000000028>.cfg	Assign a group call pickup key. For more information, refer to Group Call Pickup Key on page 357. Configure the group call pickup feature on a phone basis. For more information, refer to Group Call Pickup on page 282.
Local	Web User Interface	Assign a group call pickup key. **Navigate to:** http://<phoneIPAddress>/servlet?p=dsskey&model=1&q=load&linepage=1 Configure the 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-account basis. **Navigate to:** http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0
	Phone User Interface	Assign a group call pickup key.

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

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

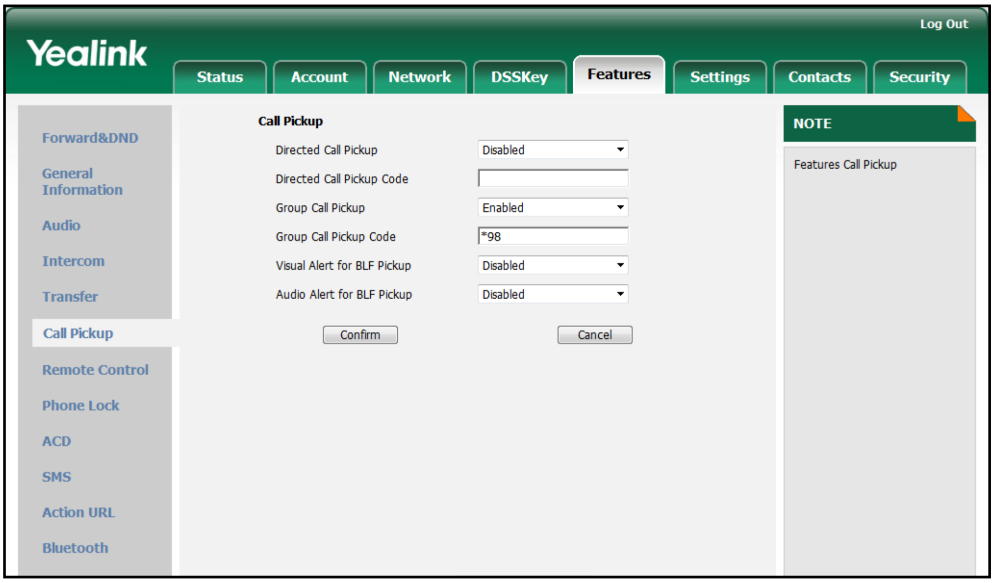
4. Select the desired line from the pull-down list of **Line**.



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

To configure the 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**.
3. Enter the group call pickup code in the **Group Call Pickup Code** field.

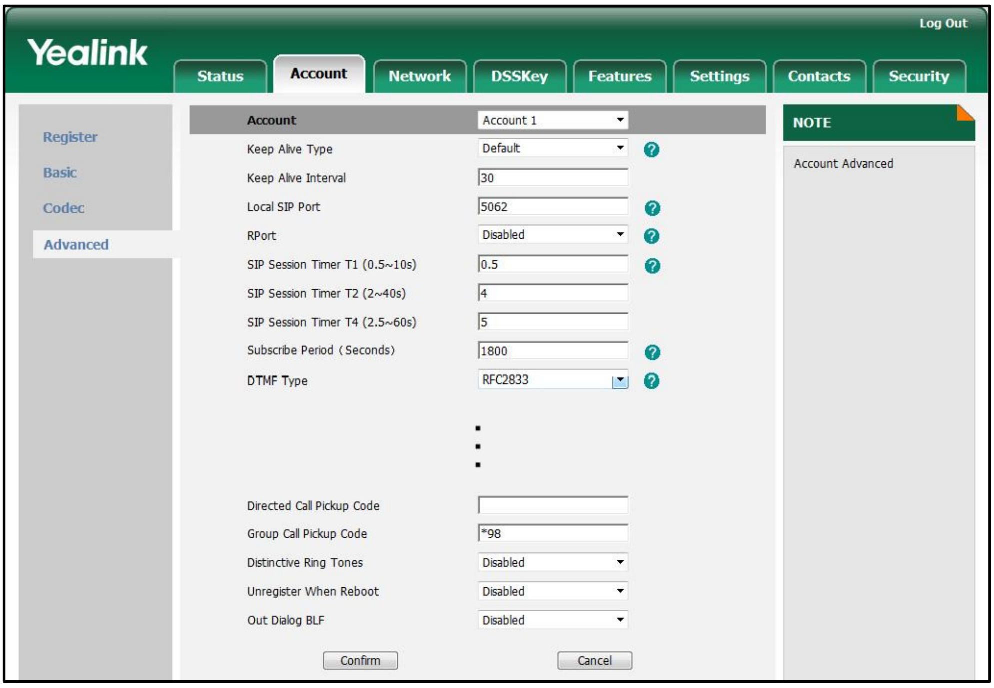


4. Click **Confirm** to accept the change.

To configure the group call pickup code on a per-account 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**->**Call Feature**->**DSS Keys**.
2. Select the desired DSS key.
3. Press or , or the **Switch** soft key to select **Key Event** from the **Type** field.
4. Press or , or the **Switch** soft key to select **Group Pickup** from the **Key Event** field.
5. Press or , or the **Switch** soft key to select the desired line from the **Account ID** field.
6. (Optional.) Enter the string that will appear on the LCD screen in the **Label** field.
7. Enter the group call pickup code in the **Value** field.
8. Press the **Save** soft key to accept the change.

Dialog-Info Call Pickup

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

The example of the dialog-info message carried in NOTIFY message for reference:


```
<?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

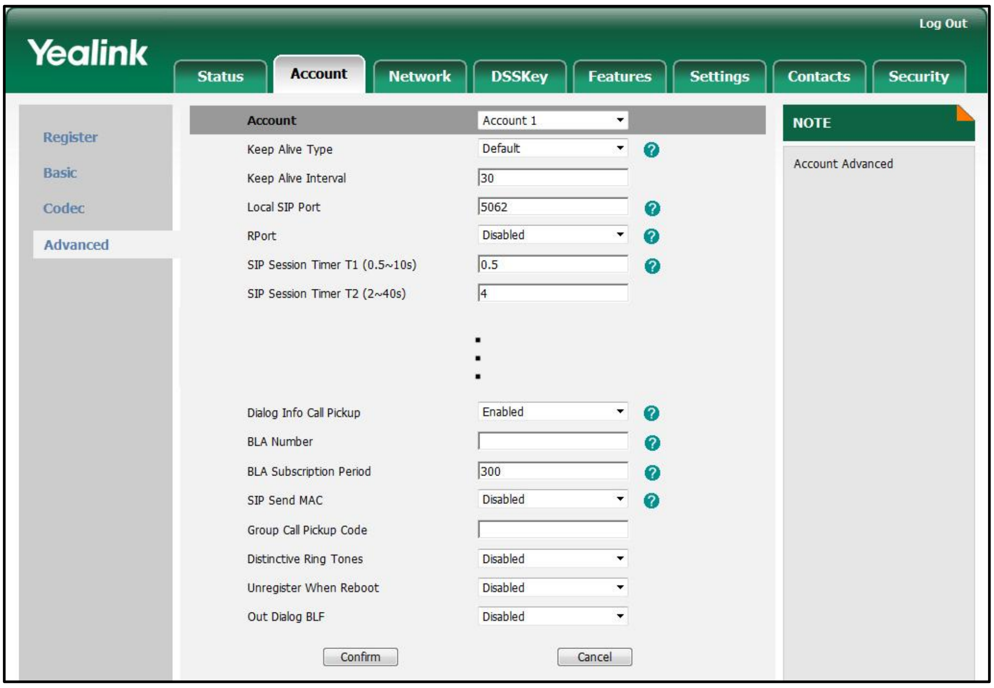
Dialog-Info Call Pickup can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure the Dialog-Info Call Pickup feature on the IP phone. For more information, refer to Dialog-Info Call PickupDialog-Info Call Pickup on page 284.
Local	Web User Interface	Configure the Dialog-Info Call Pickup feature on the IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

To configure Dialog-Info Call Pickup via web user interface:

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

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



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

Call Return

Call return, also known as last call return, provides convenience for a user to place a call back to the caller of the last incoming call. Call return is implemented on the IP phones using a call return key.

Procedure

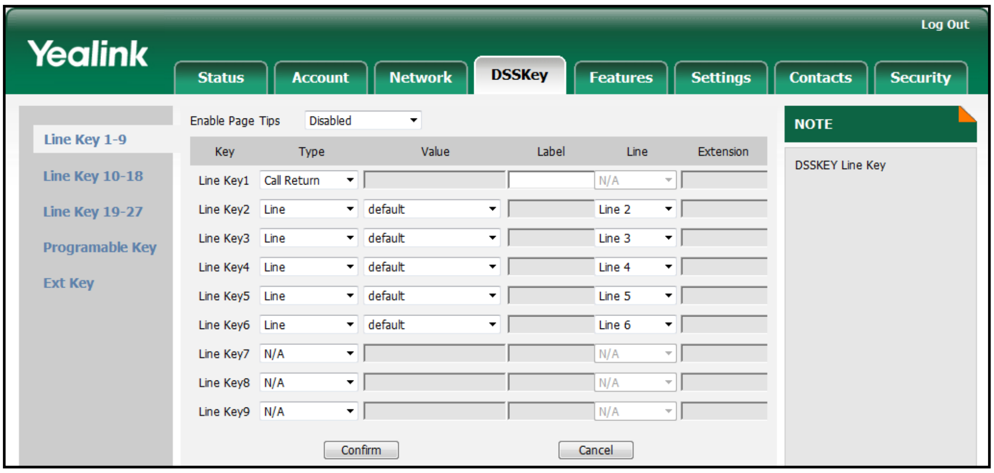
Call return key can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Assign a call return key. For more information, refer to Call Return Key on page 358.
Local	Web User Interface	Assign a call return key. **Navigate to**: http://<phoneIPAddress>/servlet?p=dsskey&model=1&q=load&linepage=1
	Phone User Interface	Assign a call return key.

To configure a call return key via web user interface:

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

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



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

To configure a call return key via phone user interface:

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

Call Park

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

Procedure

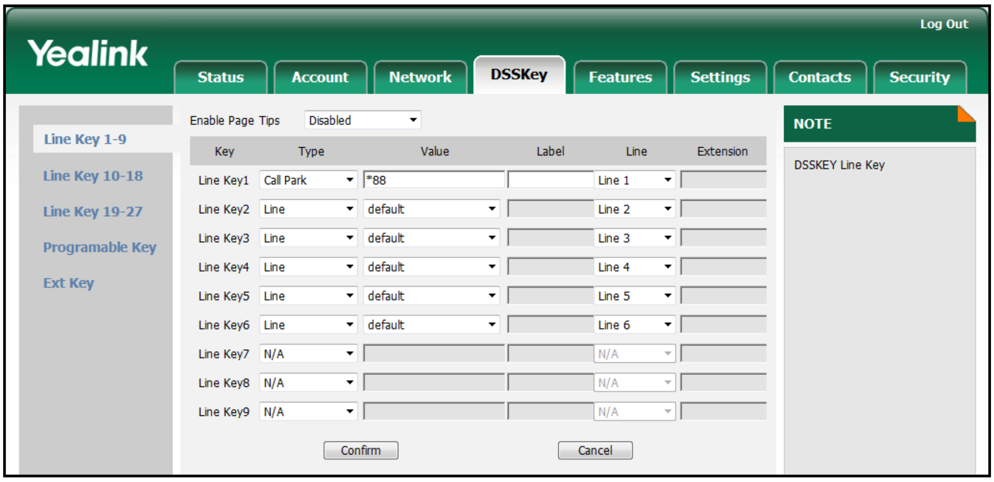
Call park key can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Assign a call park key. For more information, refer to Call Park Key on page 358.
Local	Web User Interface	Assign a call park key. **Navigate to**: http://<phoneIPAddress>/servlet?p=dsskey&model=1&q=loa

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

To configure a call park key via web user interface:

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



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

To configure a call park key via phone user interface:

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

Web Server Type

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

Procedure

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

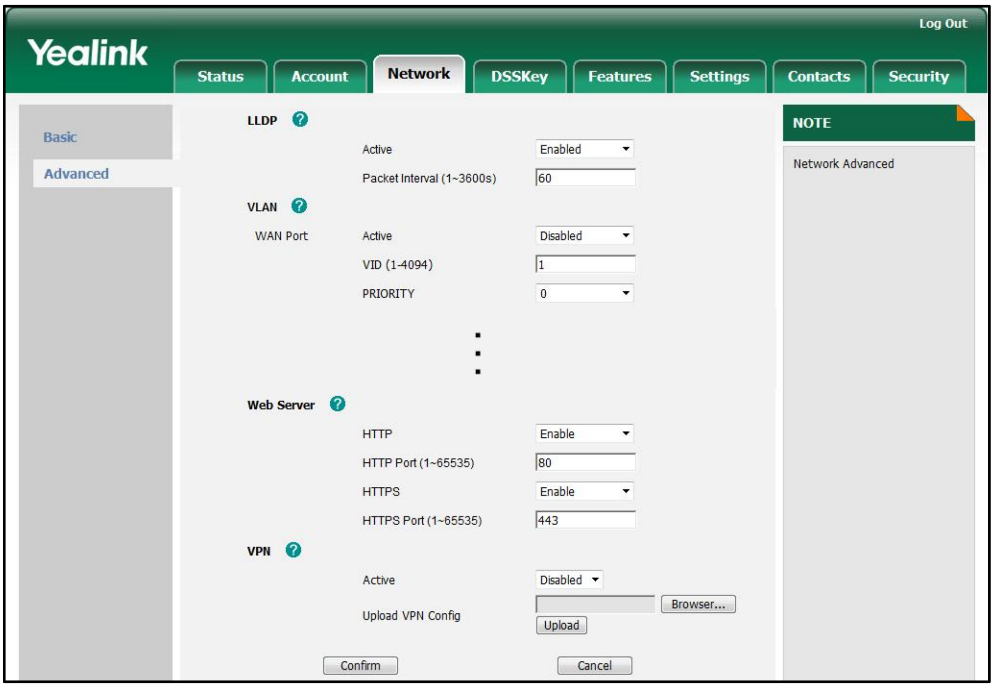
Configuration File	<y000000000028>.cfg	Specify the web access type, HTTP port and HTTPS port. For more information, refer to Web Server Type on page 284.
Local	Web User Interface	Specify the web access type, HTTP port and HTTPS port. **Navigate to:** http://<phoneIPAddress>/servlet?p=network-adv&q=load
	Phone User Interface	Specify the web access type.

To configure the web server type via web user interface:

1. Click on **Network**->**Advanced**.
2. In the **Web Server** field, select the desired value from the pull-down list of **HTTP**.
3. Enter the HTTP port in the **HTTP Port (1~65535)** field.

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

   The default HTTPS port is 443.



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

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

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

To configure the web server type via phone user interface:

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

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

Calling Line Identification Presentation

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

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

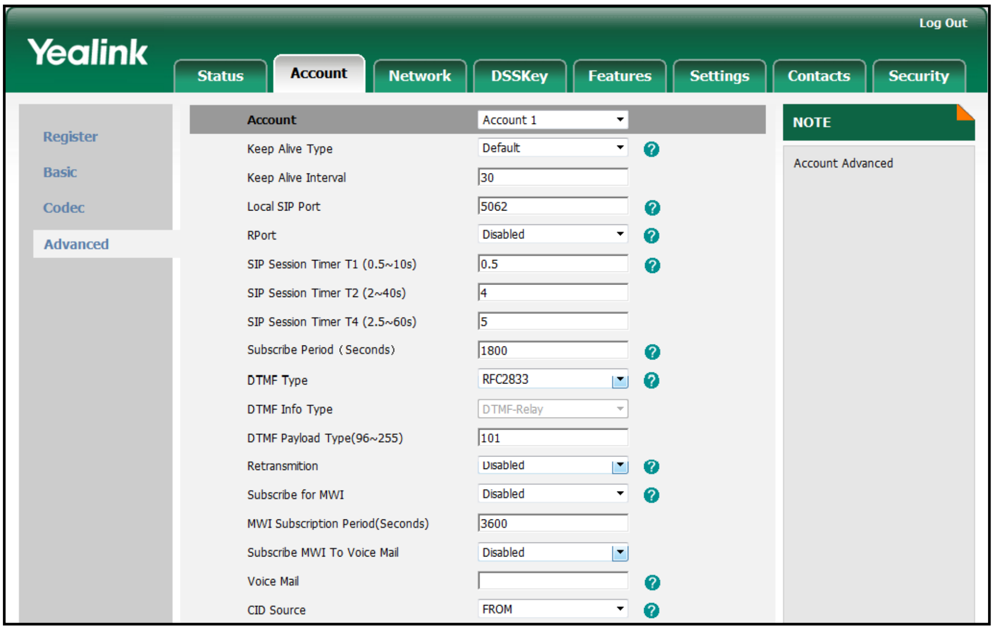
Procedure

CLIP can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure the presentation of the caller identity. For more information, refer to Calling Line Identification Presentation on page 286.
Local	Web User Interface	Configure the presentation of the caller identity. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

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

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



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

Connected Line Identification Presentation

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

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

Procedure

COLP can be configured only using the configuration files.

Configuration File	<MAC>.cfg	Configure the presentation of the callee identity. For more information, refer to Connected Line Identification Presentation on page 286.

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 press 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

There are 3 common methods of transmitting DTMF digits on SIP calls:

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

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

RFC 2833

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

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

INBAND

DTMF digits are transmitted within the audio of the IP phone conversation. It uses the same VoIP codec as your voice and is audible to the conversation partners.

SIP INFO

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

Procedure

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

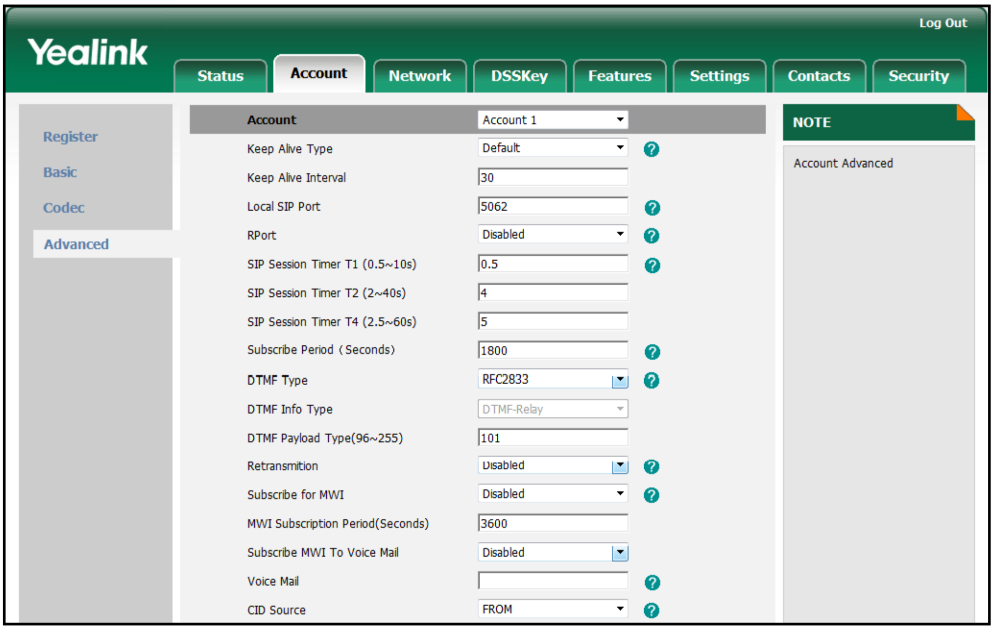
Configuration File	<MAC>.cfg	Configure the method of transmitting DTMF digit and the payload type. For more information, refer to DTMF on page 287.
	<y000000000028>.cfg	Configure the number of times for the IP phone to send the end RTP Event packet. For more information, refer to DTMF on page 287.
Local	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=load

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

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

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

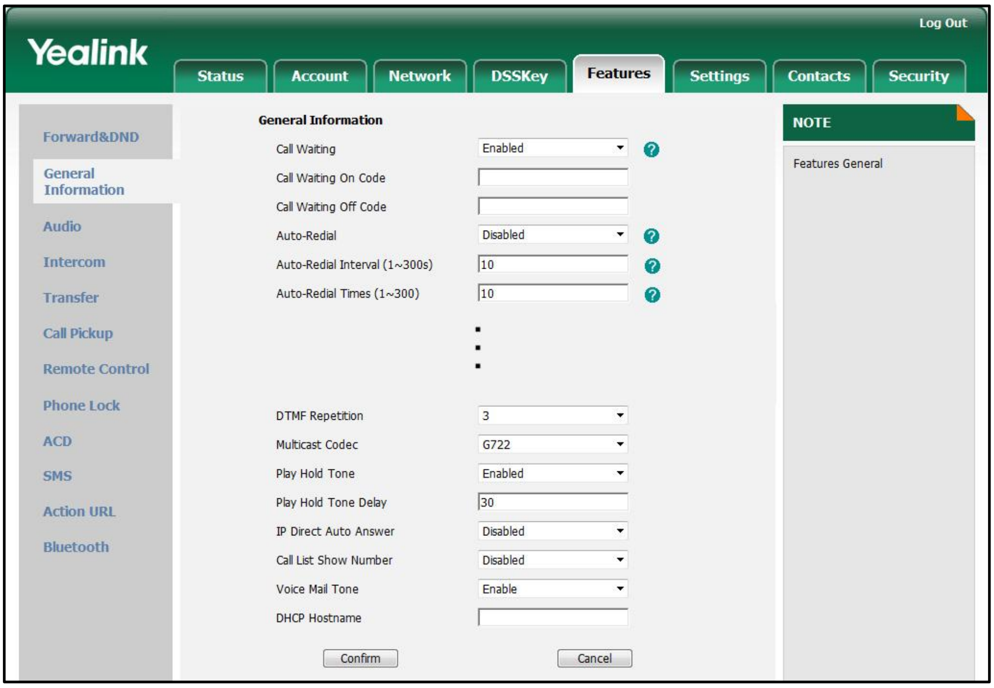
5. Enter the desired value in the **DTMF Payload Type (96~255)** field.



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

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

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



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

Suppress DTMF Display

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

Procedure

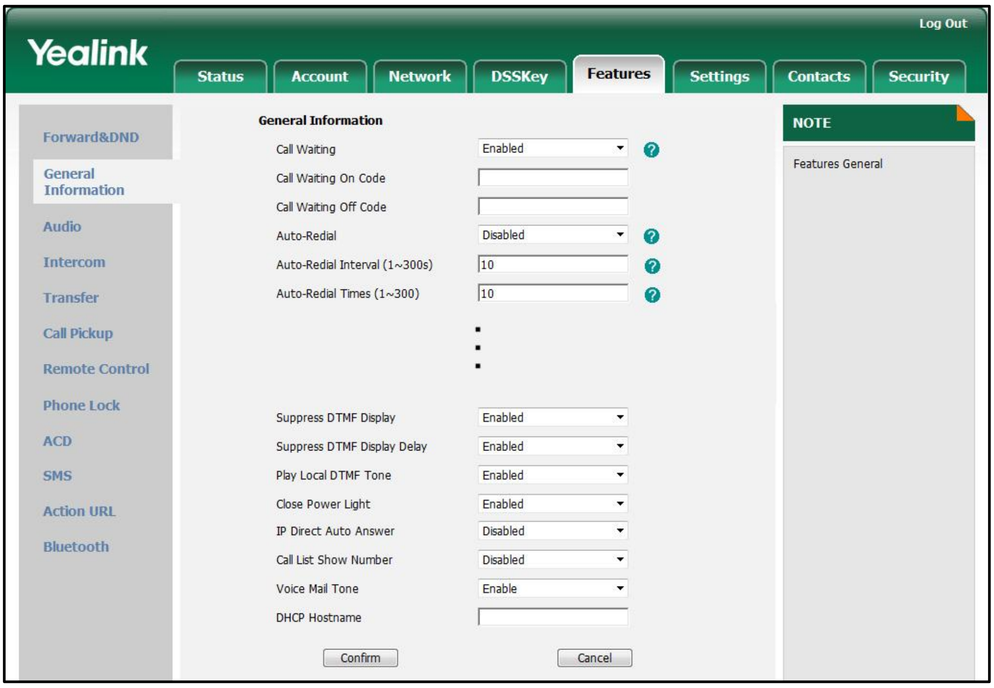
Configuration changes can be performed using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Configure the suppress DTMF display and suppress DTMF display delay features. For more information, refer to Suppress DTMF Display on page 289.
Local	Web User Interface	Configure the suppress DTMF display and suppress DTMF display delay features. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-general&q=load

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

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

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



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

Transfer via DTMF

On some traditional servers, call transfer is implemented via DTMF. The IP phones support to send the specified DTMF digits to the server for transferring a call to a third party.

Procedure

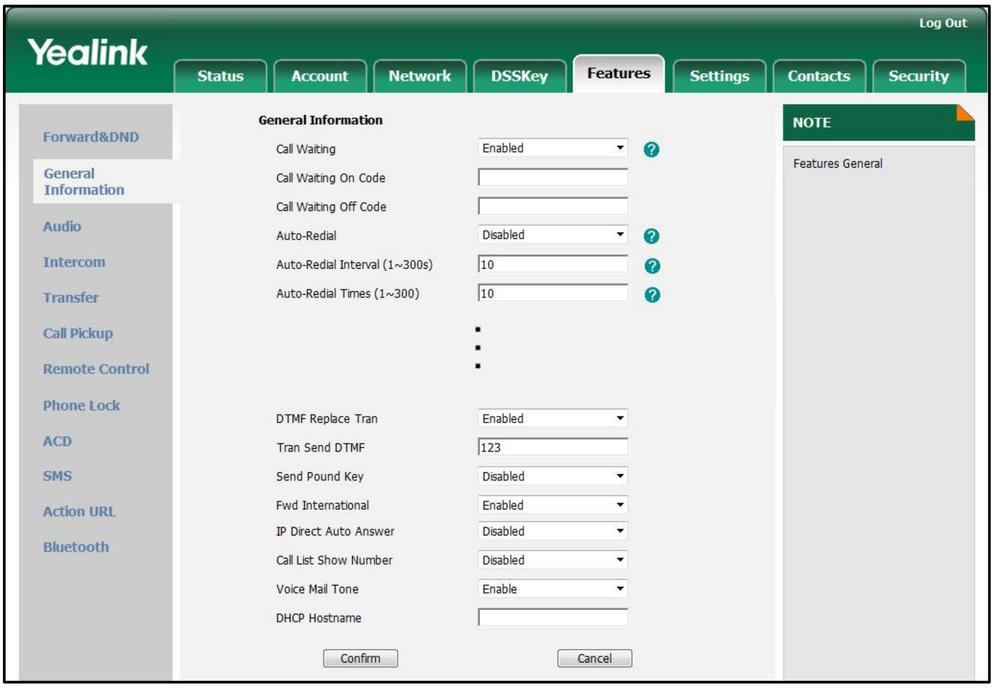
Configuration changes can be performed using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Configure the transfer via DTMF feature. For more information, refer to Transfer via DTMF on page 289.
Local	Web User Interface	Configure the transfer via DTMF feature. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-general&q=load

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

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

2. Select the desired value from the pull-down list of **DTMF Replace Tran**.
3. Enter the specified DTMF digits in the **Tran Send DTMF** field.



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

Intercom

The intercom feature allows establishing an audio conversation directly. The called phone picks up intercom calls automatically and establishes intercom conversations. This feature depends on support from a SIP server.

Outgoing Intercom Calls

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

Procedure

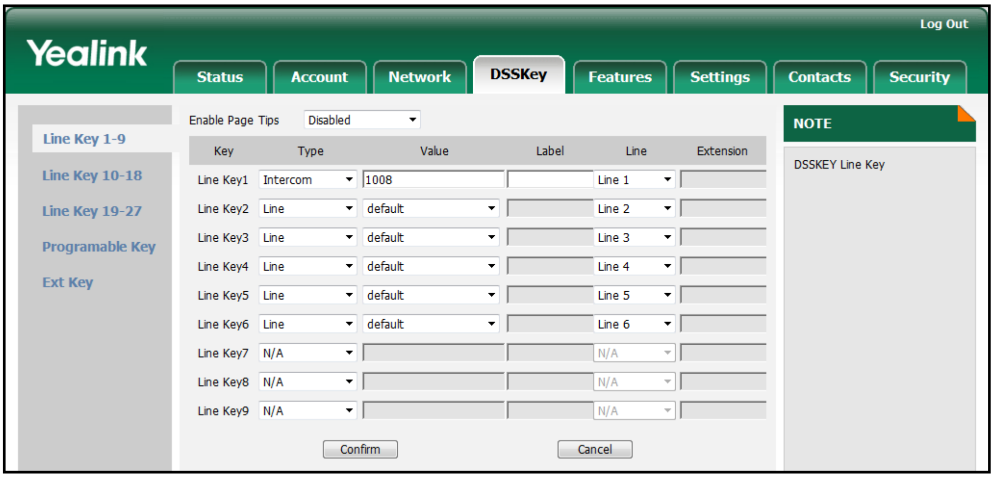
Intercom key can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Assign an intercom key. For more information, refer to Intercom **Key** on page 359.
Local	Web User Interface	Assign an intercom key. **Navigate to**:

		http://<phoneIPAddress>/servlet?p=dsskey&model=1&q=load&linepage=1
	Phone User Interface	Assign an intercom key.

To configure an intercom key via web user interface:

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



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

To configure an intercom key via phone user interface:

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

Incoming Intercom Calls

The way IP phones handle incoming intercom calls depends on the incoming intercom call configurations. The following describes each configuration parameter for incoming intercom calls.

Accept Intercom

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

Intercom Mute

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

Warning Tone

Warning Tone allows the IP phones to play a warning tone before answering an intercom call.

Intercom Barge

Intercom Barge allows the IP phones to automatically answer an incoming intercom call while there is already an active call on the IP phone. The active call will be put on hold.

Procedure

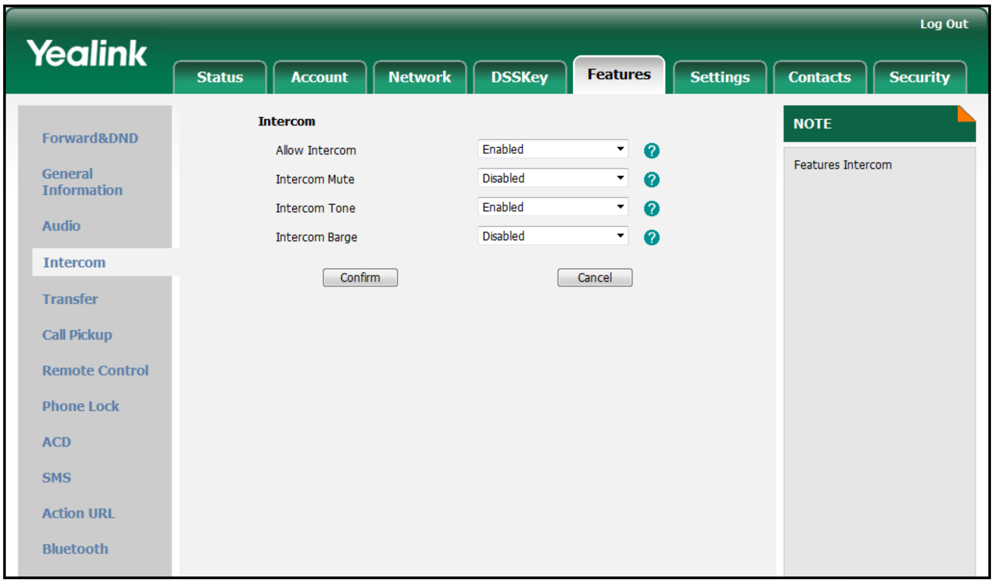
Incoming intercom calls can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Configure the incoming intercom call feature. For more information, refer to Incoming Intercom calls on page 290.
Local	Web User Interface	Configure the incoming intercom call feature. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-intercom&q=load
	Phone User Interface	Configure the incoming intercom call feature.

To configure intercom via web user interface:

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

2. Select the desired values from the pull-down lists of **Allow 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**, **Warning 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 Phonebook
- LDAP
- Busy Lamp Field
- Music on Hold
- Automatic Call Distribution
- Message Waiting Indicator
- Multicast Paging
- Call Recording
- Hot Desking
- Action URL
- Action URI
- Server Redundancy
- LLDP
- VLAN
- VPN
- Quality of Service
- Network Address Translation
- SNMP
- 802.1X Authentication
- TR-069 Device Management
- IPv6 Support

Distinctive Ring Tones

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

The Alert-Info header is in the following two formats:

Alert-Info: localIP/Bellcore-drN

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

- If the Alter-Info header contains the keyword "Bellcore-drN", the IP phone will play the Bellcore-drN ring tone (N=1,2,3,4,5).

  Example:

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

  The following table identifies the different Bellcore ring tone patterns and cadences.

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

Note

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

- If the Alert-Info header contains a remote URL, the IP phone will try to download the WAV ring tone file from the URL and then play the remote ring tone. If failing to download the file, the IP phone will plays the local ring tone associated with **info text**. If there is no text matched, the IP phone will play the local ring tone configured on the IP phone in about ten seconds.

  Example:

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

Procedure

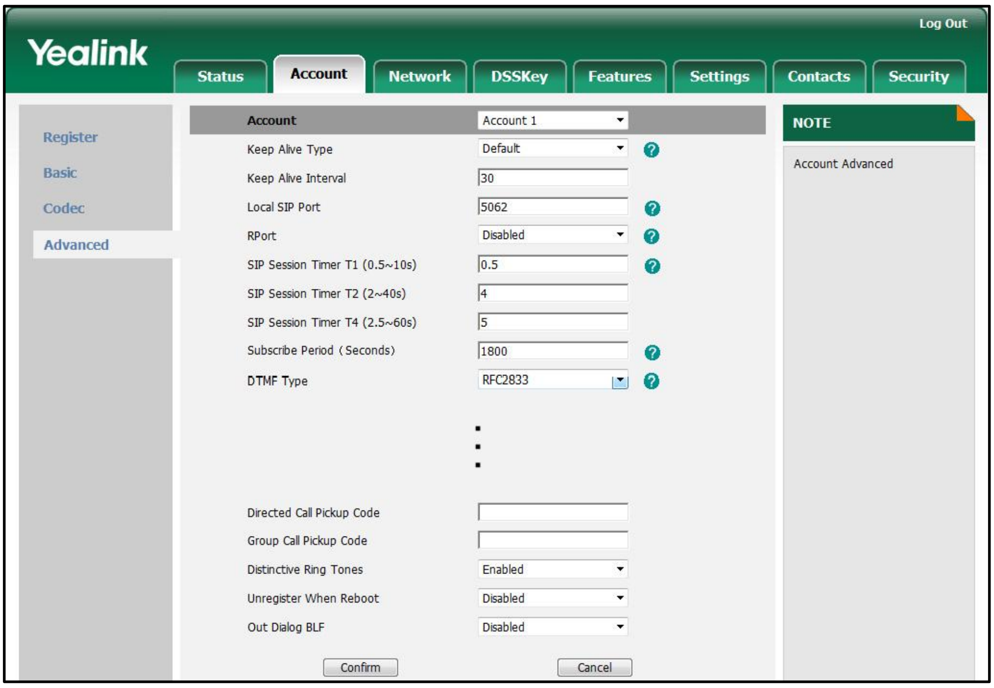
Distinctive ring tones can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure the distinctive ring tones feature. For more information, refer to Distinctive Ring Tones on page 292.
	<y000000000028>.cfg	Configure the internal ringer text and internal ringer file. For more information, refer to Distinctive Ring Tones on page 292.
Local	Web User Interface	Configure the distinctive ring tones feature. **Navigate to:** http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0 Configure the internal ringer text and internal ringer file. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-ring&q=load

To configure distinctive ring tones via web user interface:

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

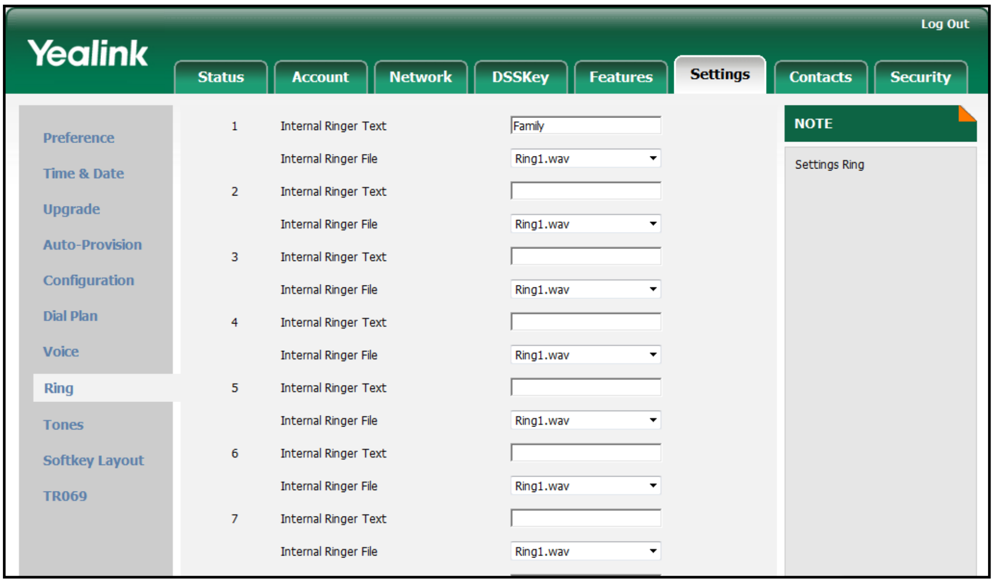
4. Select the desired value from the pull-down list of **Distinctive Ring Tones**.



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

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

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



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

Tones

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

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

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

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

Procedure

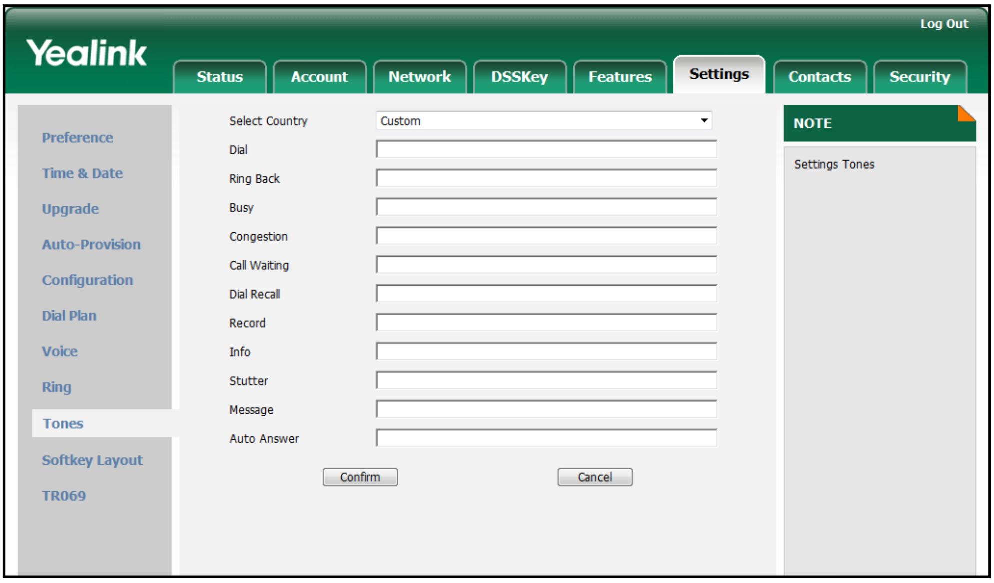
Tones can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Configure the tones for the IP phone. For more information, refer to Tones on page 294.
Local	Web User Interface	Configure the tones for the IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-tones&q=load

To configure tones via web user interface:

1. Click on **Settings**->**Tones**.
2. Select the desired type from the pull-down list of **Select Country**.

If you select **Custom**, you can customize the tone for indicating each condition of the IP phone.



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

Remote Phonebook

Remote phonebook is the phone book maintained centrally, which is stored on the remote server. Users just need the access URL of the remote phonebook. The IP phone can establish a connection with the remote server and download the entries, and then display the entries on the phone user interface. The IP phones support up to 5 remote phonebooks. All remote phonebooks must be less than 5MB in size. The remote phonebook can be customized. For more information, refer to Remote XML Phonebook on page 214.

The SRemote Name feature allows the IP phones to query the entry names from the remote phonebook when receiving incoming calls. The SRemote Name Flash Time feature defines how often the IP phones refresh the local cache of the remote phonebook.

Procedure

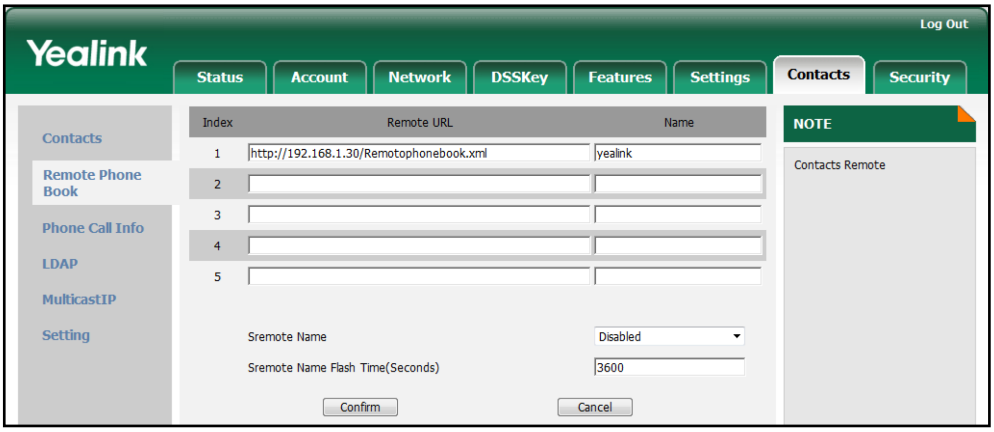
Remote phonebook can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Specify the access URL of the remote phonebook. For more information, refer to Remote Phonebook on page 296. Specify whether to query the entry names from the remote

		phonebook when the IP phone receives incoming calls. Specify how often the IP phone refreshes the local cache of the remote phonebook. For more information, refer to Remote Phonebook on page 296.
Local	Web User Interface	Specify the access URL of the remote phonebook. **Navigate to:** http://<phoneIPAddress>/servlet?p=contacts-remote&q=load Specify whether to query the contact names from the remote phonebook when the IP phone receives incoming calls. Specify how often the IP phone refreshes the local cache of the remote phonebook. **Navigate to:** http://<phoneIPAddress>/servlet?p=contacts-remote&q=load

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

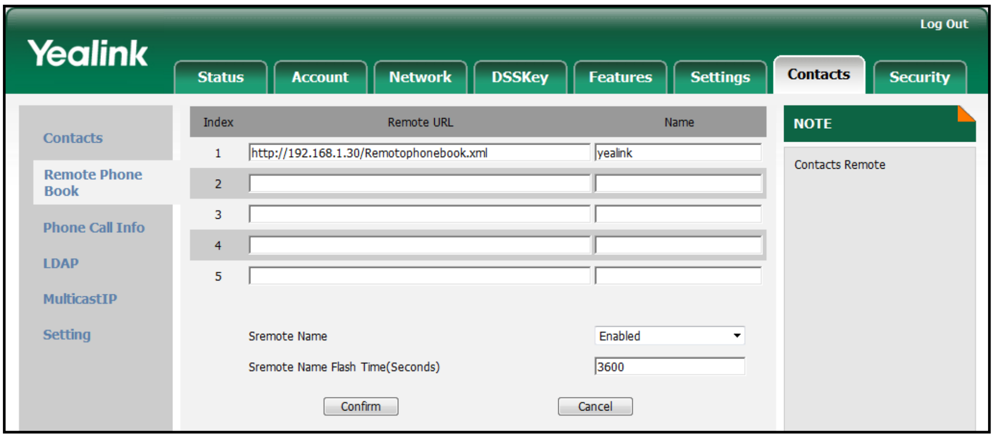
1. Click on **Contacts**->**Remote Phone Book**.
2. Enter the access URL in the **Remote URL** field.
3. Enter the name in the **Name** field.



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

To configure the remote phonebook via web user interface:

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



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

LDAP

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

The biggest plus for LDAP is that users can access the central LDAP directory of the corporation using the IP phones, so they do not need to maintain the local directory. Users can search and dial from the LDAP directory and save the LDAP entries to the local directory. The LDAP entries displayed on the IP phone are read only. Users can not add, edit or delete the LDAP entries. When an LDAP server is properly configured, the IP phone can look up entries from the LDAP server in a wide variety of ways. The LDAP server indexes all the data in its entries, and "filters" may be used to select just the desired contact or group, and return just the desired information.

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

There are two ways to perform an LDAP search on the IP phone:

- Simply start a search against LDAP by entering a number. All suitable entries will be shown according to your query setup.
- Assign a DSS key to be an LDAP key, and press the LDAP key to enter the LDAP Search interface when the IP phone is idle.

LDAP Attributes

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

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

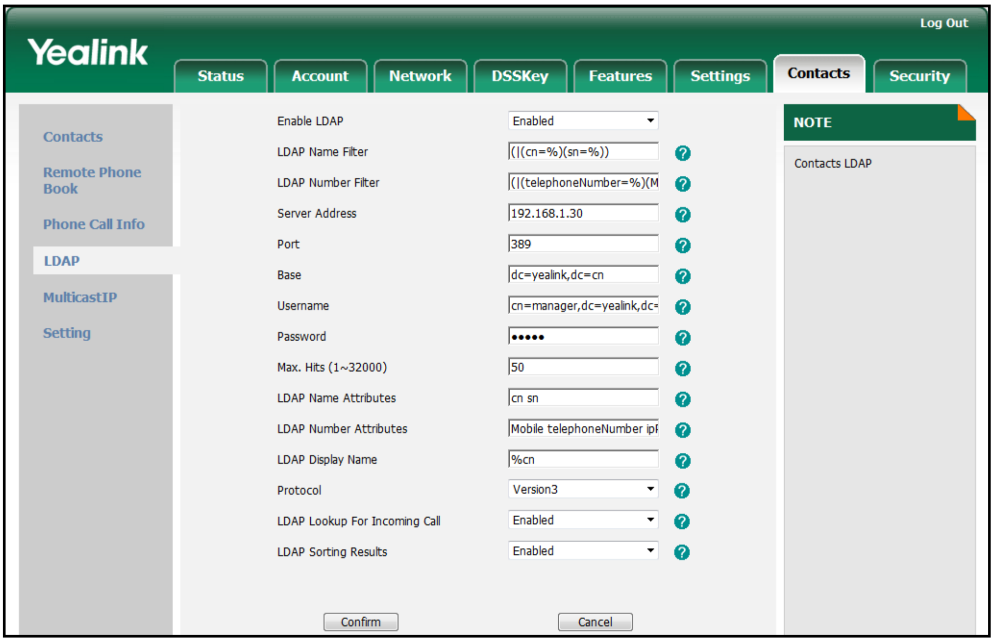
Procedure

LDAP can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Configure the LDAP feature. For more information, refer to LDAP on page 297. Assign an LDAP key. For more information, refer to LDAP Key on page 360.
Local	Web User Interface	Configure the LDAP feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=contacts-LDAP&q=load Assign an LDAP key. **Navigate to**: http://<phoneIPAddress>/servlet?p=dsskey&model=1&q=load&linepage=1
	Phone User Interface	Assign an LDAP key.

To configure LDAP via web user interface:

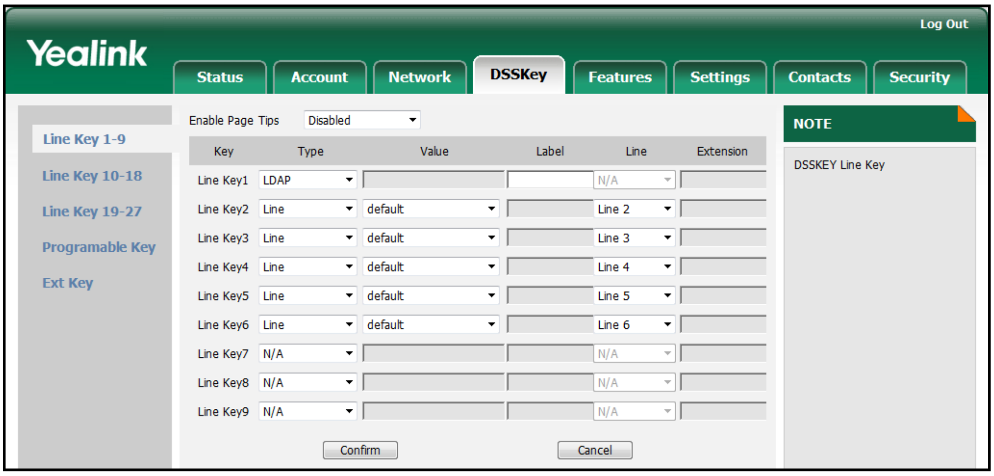
1. Click on **Contacts**->**LDAP**.
2. Select **Enabled** from the pull-down list of **Enable LDAP**.
3. Enter the values in the corresponding fields.
4. Select the desired values from the corresponding pull-down lists.



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

To configure an LDAP key via web user interface:

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

Busy Lamp Field

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

Visual Alert and Audio Alert for BLF Pickup

The BLF pickup feature allows supervisor to pick up the incoming call of the monitored user. The visual alert and audio alert for BLF pickup features allow the supervisor's phone to play an alert tone and display a visual prompt (e.g., "6001<-6002", 6001 is the monitored extension and receives an incoming call from 6002) when the monitored user receives an incoming call. In addition to BLF key, the visual alert for BLF pickup feature also enables the supervisor to pick up the incoming call of the monitored user by pressing the Pickup soft key directly. 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 91.

LED Off in Idle

The LED off in idle feature defines two flashing methods for the BLF key LED. The BLF key LED flashes as below:

Line key LED (configured as BLF key when LED Off in Idle is disabled)

LED Status	Description
Solid green	The monitored user is idle.
Solid red	The monitored user is busy. The call is parked against the monitored user's phone number.
Fast flashing red	The monitored user receives an incoming call.
Off	The monitored user does not exist.

Line key LED (configured as BLF key when LED Off in Idle is enabled)

LED Status	Description
Solid red	The monitored user is busy. The call is parked against the monitored user's phone number.
Fast flashing red	The monitored user receives an incoming call.
Off	The monitored user is idle. The monitored user does not exist.

Procedure

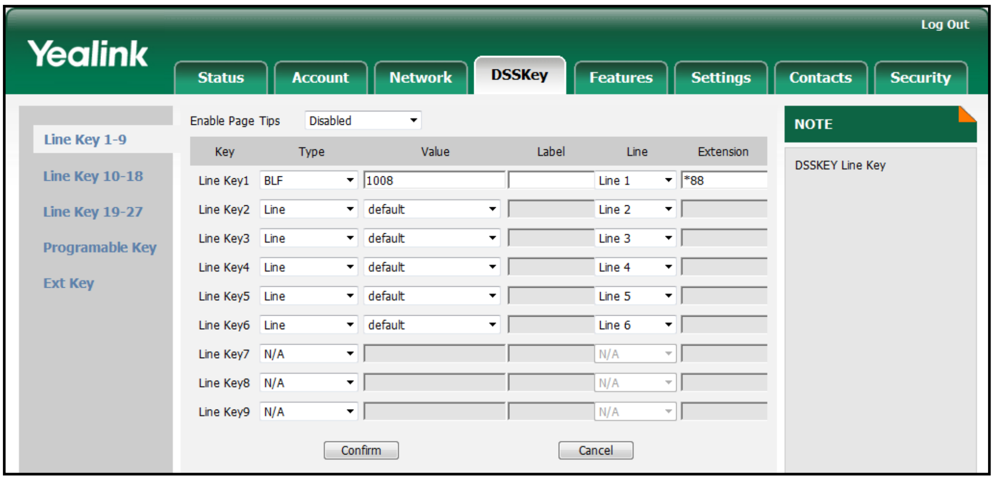
BLF can be configured using the configuration files or locally.

Configuration File	y000000000028.cfg	Assign a BLF key. For more information, refer to BLF Key on page 360. Specify whether to use the visual alert and audio alert for BLF pickup features. Configure the LED off in idle feature. For more information, refer to BLF on page 302.
Local	Web User Interface	Assign a BLF key. **Navigate to**: http://<phoneIPAddress>/servlet?p=dsskey&model=1&q=load&linepage=1 Specify whether to use the visual alert and audio alert for BLF pickup features. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-callpickup&q=load Configure the LED off in idle feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

	Phone User Interface	Assign a BLF key.

To configure a BLF key via web user interface:

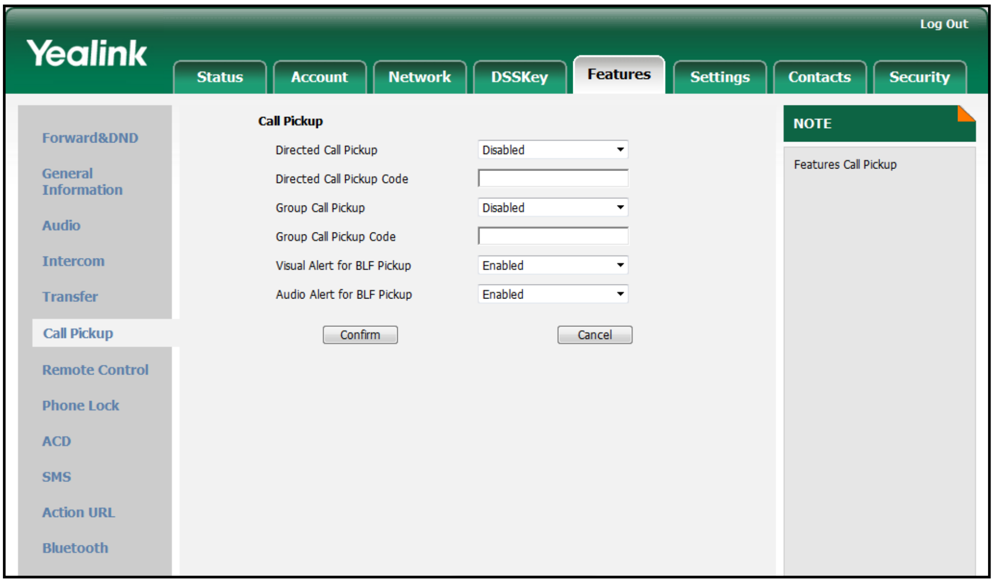
1. Click on **DSSKey**->**Line Key**.
2. In the desired DSS key field, select **BLF** from the pull-down list of **Type**.
3. Enter the phone number or extension you want to monitor in the **Value** field.
4. Select the desired line from the pull-down list of **Line**.
5. (Optional.) Enter the directed call pickup code in the **Extension** field.



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

To configure the visual alert and audio alert features via web user interface:

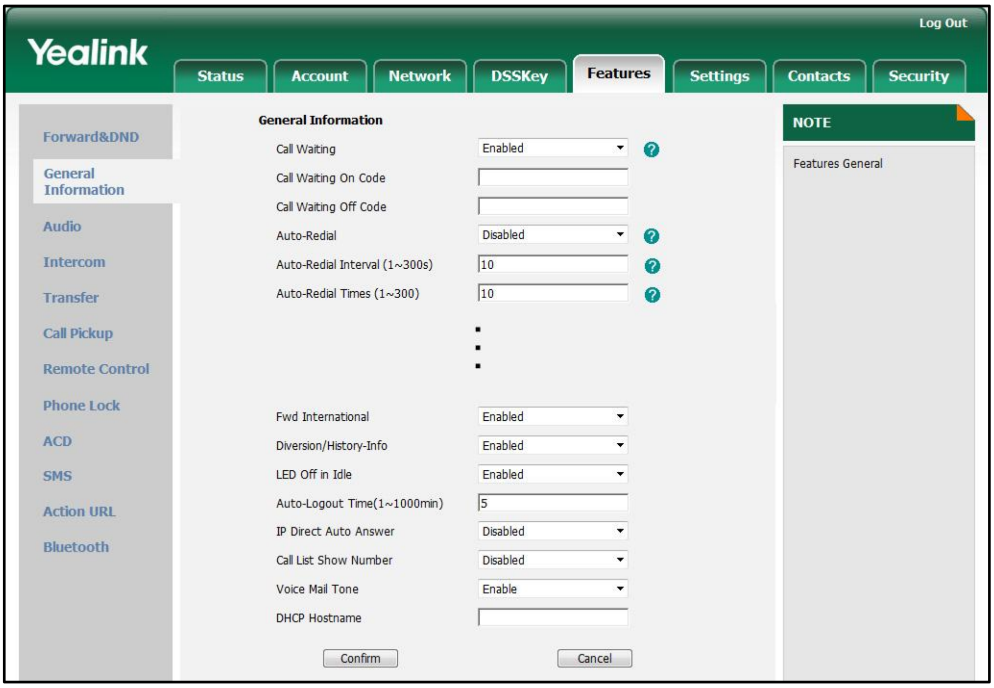
1. Click on **Features**->**Call Pickup**.
2. Select the desired value from the pull-down list of **Visual Alert for BLF Pickup**.
3. Select the desired value from the pull-down list of **Audio Alert for BLF Pickup**.



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

To configure the LED off in idle via web user interface:

1. Click on **Features**->**General Information**.
2. Select the desired value from the pull-down list of **LED Off in Idle**.



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

To configure a BLF key via phone user interface:

1. Press **Menu**->**Call Feature**->**DSS Keys**.
2. Select the desired DSS key.
3. Press or , or the **Switch** soft key to select **BLF** from the **Type** field.
4. Press or , or the **Switch** soft key to select the desired line from the **Account ID** field.
5. (Optional.) Enter the string that will appear on the LCD screen in the **Label** field.
6. Enter the phone number or extension you want to monitor in the **Value** field.
7. (Optional.) Enter the directed call pickup code in the **Extension** field.
8. Press the **Save** soft key to accept the change.

Music on Hold

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

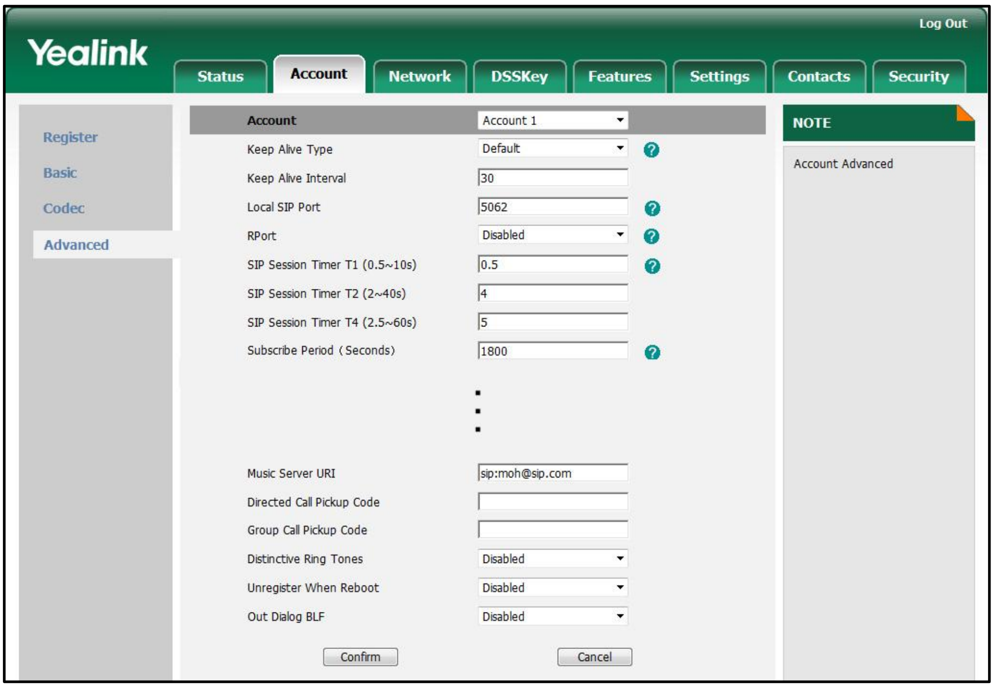
Procedure

Music on Hold can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure the MoH feature on a per-account basis. For more information, refer to Music on Hold on page 303.
Local	Web User Interface	Configure the MoH feature on a per-account basis. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

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



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

Automatic Call Distribution

Automatic Call Distribution (ACD) enables organizations to manage a large number of phone calls on an individual basis. ACD enables the use of the IP phones in a call-center role by automatically distributing incoming calls to available users, or agents. The ACD feature depends on support from a SIP server.

Note The ACD feature is disabled by default. You need to enable it in advance.

After the IP phone user logs into the queue, the server monitors the phone status and then decides whether to assign an incoming call to the user's IP phone. Whenever the IP phone user answers a call, or misses a call, the server automatically changes the phone status to unavailable. The IP phone will remain in this status until the IP phone user manually changes the phone status or the ACD auto available timer expires. When the timer expires, the phone status is automatically changed to available. The auto available timer feature depends on support from a SIP server.

You need to configure an ACD key for the user to log in the ACD system. The ACD key LED on the IP phone indicates the ACD status.

Procedure

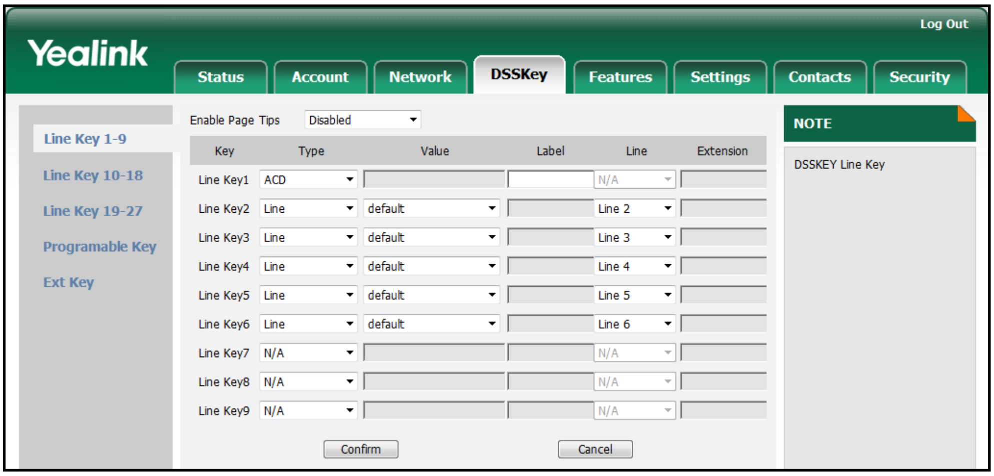
ACD can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure the ACD feature. For more information, refer to ACD on page 303.
	<y000000000028>.cfg	Assign an ACD key. For more information, refer to ACD Key on page 361. Configure the ACD auto available timer feature. For more information, refer to ACD on page 303.
Local	Web User Interface	Assign an ACD key. **Navigate to**: http://<phoneIPAddress>/servlet?p=dsskey&model=1&q=load&linepage=1 Configure the ACD auto available timer feature. **Navigate to**: http://<phoneIPAddress>/servlet

		?p=features-acd&q=load
	Phone User Interface	Assign an ACD key.

To configure an ACD key via web user interface:

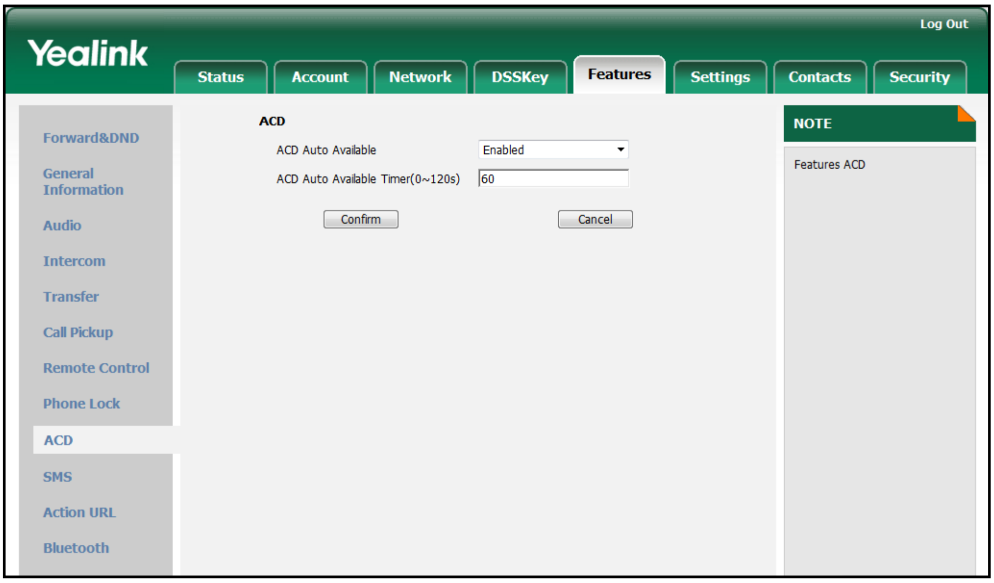
1. Click on **DSSKey**->**Line Key**.
2. In the desired DSS key field, select **ACD** from the pull-down list of **Type**.
3. Select the desired line from the pull-down list of **Line**.



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

To configure the ACD auto available timer feature via web user interface:

1. Click on **Features**->**ACD**.
2. Select the desired value from the pull-down list of **ACD Auto Available**.
3. Enter the desired timer in the **ACD Auto Available Timer (0~120s)** field.



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

To configure an ACD key via phone user interface:

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

Message Waiting Indicator

Message Waiting Indicator (MWI) is a feature that informs users that they have messages waiting in their mailboxes. This feature indicates how many messages are waiting without the users having to call their mailboxes. The IP phones support both audio and visual MWI when receiving new voice messages.

The IP phones support both solicited and unsolicited MWI. Unsolicited MWI is a server related feature.

Solicited MWI: MWI notification is subscription-based. 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 the MWI subscription feature on the IP phones.

Unsolicited MWI: MWI notification is not subscription-based. The 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.

Subscribe MWI to VM feature supports the IP phone can subscribe to the voice mail number for MWI service. Whether the phone subscribes the MWI messages to the account or the voice number MWI service depends on the server.

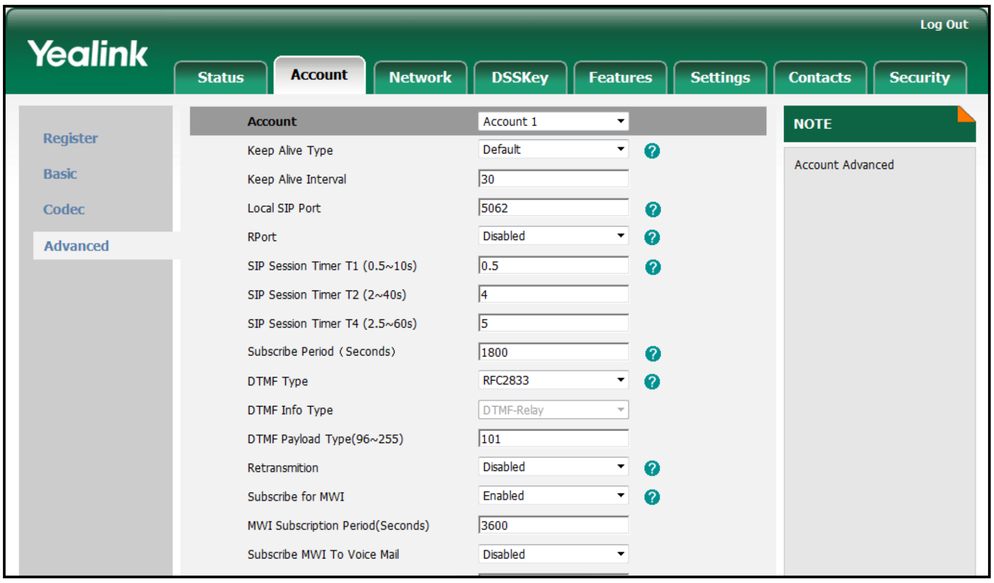
Procedure

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

Configuration File	<MAC>.cfg	Configure the MWI subscription feature on the IP phone. For more information, refer to Message Waiting Indicator on page 305.
Local	Web User Interface	Configure the MWI subscription feature on the IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

To configure the MWI subscription 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 **Subscribe for MWI**.
5. Enter the period time in the **MWI Subscription Period (Seconds)** field.



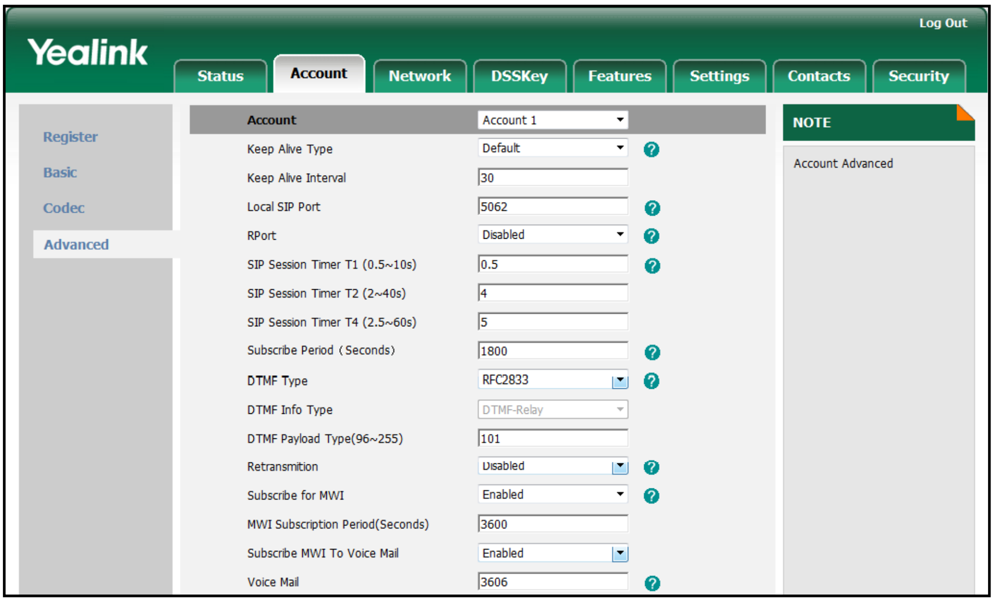
6. Click **Confirm** to accept the change.

   The IP phone will subscribe to the account number for MWI service by default.

To enable the Subscribe MWI to VM 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 **Enabled** 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.

   The IP phone will subscribe to the voice mail number for MWI service using Subscribe MWI to WM feature.

Multicast Paging

The multicast paging feature allows the IP phones to send/receive Real-time Transport Protocol (RTP) stream to/from the pre-configured multicast address(es) without involving SIP signaling. You can specify up to 10 listening multicast addresses on IP phones.

Sending RTP Stream

Users can send an RTP stream without involving SIP signaling by pressing a configured multicast paging key. A multicast address (IP: Port) should be assigned to the multicast paging key, which is defined to transmit RTP stream to a group of designated the IP phones. When the IP phone sends the RTP stream to a pre-configured multicast address, each IP phone that has been configured to listen to the multicast address can receive the RTP stream. When the originator stops sending the RTP stream, the subscribers stop receiving the RTP stream.

Procedure

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

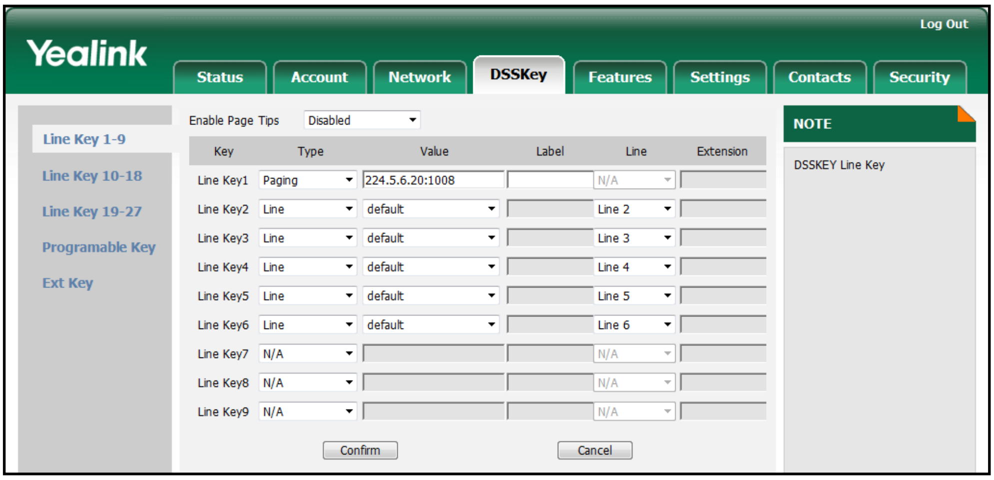
Configuration File	<y000000000028>.cfg	Assign a multicast paging key. For more information, refer to Multicast Paging Key on page

		362. Specifies a multicast codec for the IP phone to use for multicast RTP. For more information, refer to Sending RTP Stream on page 307.
Local	Web User Interface	Assign a multicast paging key. **Navigate to**: http://<phoneIPAddress>/servlet?p=dsskey&model=1&q=load&linepage=1 Specifies a multicast codec for the IP phone to use to send the RTP stream. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load
	Phone User Interface	Assign a multicast paging key.

To configure a multicast paging key via web user interface:

1. Click on **DSSKey**->**Line Key**.
2. In the desired DSS key field, select **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.

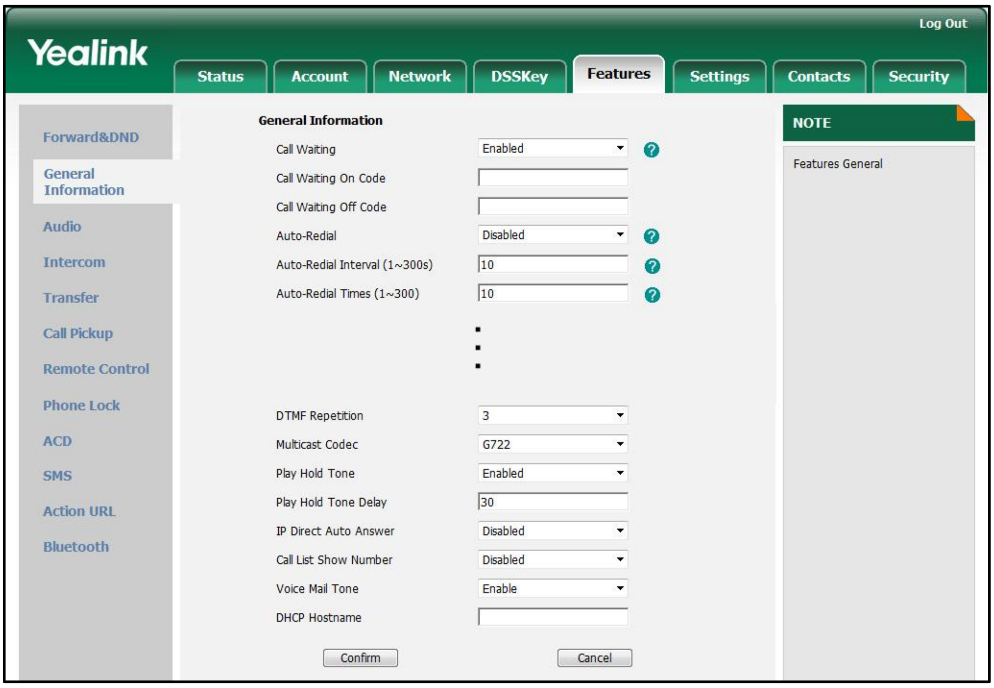


4. Click **Confirm** to accept the change.

To configure a 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 a multicast paging key via phone user interface:

1. Press **Menu**->**Call Feature**->**DSS Keys**.
2. Select the desired DSS key.
3. Press or , or the **Switch** soft key to select **Key Event** from the **Type** field.
4. Press or , or the **Switch** soft key to select **Paging** from the **Key Event** field.
5. (Optional.) Enter the string that will appear on the LCD screen in the **Label** field.
6. Enter the multicast IP address and port number in the **Value** field.
7. Press the **Save** soft key to accept the change.

Receiving RTP Stream

The IP phones can receive an RTP stream from the pre-configured multicast address(es) without involving SIP signaling. They can handle the incoming multicast paging calls differently depending on the configurations of Paging Barge and Paging Priority Active parameters.

Paging Barge

This parameter defines the priority of the voice call in progress, which can decide how the IP phone handles the incoming multicast paging calls when there is already a voice call on the IP phone. 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 on the IP phone. 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.

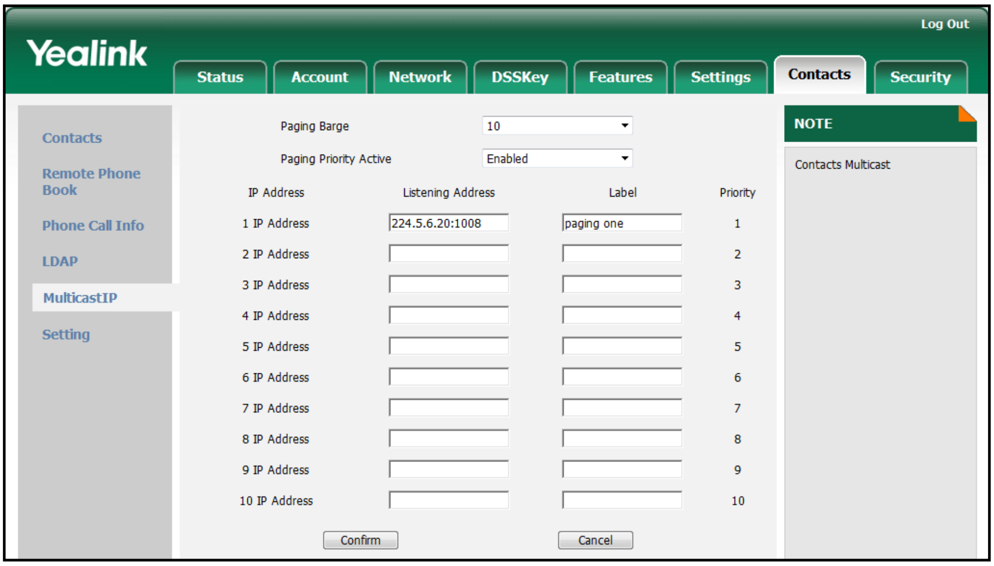
Configuration File	<y000000000028>.cfg	Configure the listening multicast address. Configure the Paging Barge and Paging Priority Active features. For more information, refer to Receiving RTP Stream on page 307.
Local	Web User Interface	Configure the listening multicast address. Configure the Paging Barge and Paging Priority Active features. **Navigate to**: http://<phoneIPAddress>/servlet?p=contacts-multicastIP&q=load

To configure a listening multicast address via web user interface:

1. Click on **Contacts->MulticastIP**.
2. Enter the listening multicast address and port number in the **Listening Address** field.

   1 is the highest priority and 10 is the lowest priority.
3. Enter the label in the **Label** field.

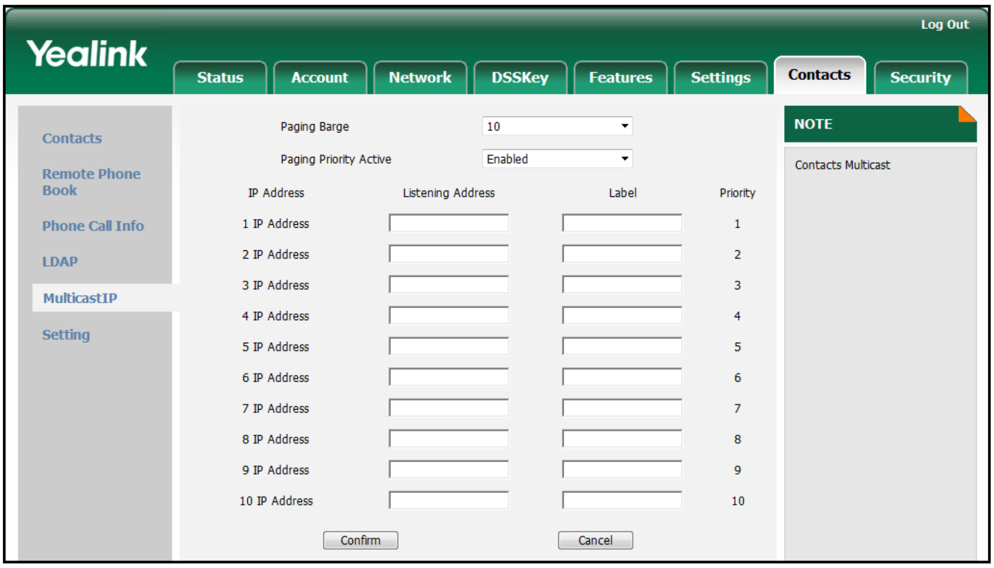
The label will appear on the LCD screen when receiving the RTP multicast.



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

To configure the paging barge and paging priority active features via web user interface:

1. Click on **Contacts**->**MulticastIP**.
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. The 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 an HTTP URL to the server. 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.

The example of a SIP INFO message for reference:

```
Via: SIP/2.0/UDP 10.1.4.148:5063;branch=z9hG4bK1139980711
From: "827" <sip:827@192.168.1.199>;tag=2066430997
To:<sip:614@192.168.1.199>;tag=371745247
Call-ID: 1895019940@10.1.4.148
CSeq: 2 INFO
Contact: <sip:827@10.1.4.148:5063>
Max-Forwards: 70
User-Agent: Yealink SIP-T46G 28.71.0.10
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.

The example of a SIP INFO message for reference:

```
Via: SIP/2.0/UDP 10.1.4.148:5063;branch=z9hG4bK1619489730
From: "827" <sip:827@192.168.1.199>;tag=1831694891
To:<sip:614@192.168.1.199>;tag=2228378244
Call-ID: 1051886688@10.1.4.148
CSeq: 3 INFO
Contact: <sip:827@10.1.4.148:5063>
Max-Forwards: 70
User-Agent: Yealink SIP-T46G 28.71.0.10
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.

The example of an HTTP GET message for reference:

```
Get /phonerecording.cgi?model=yealink HTTP/1.0\r\n
Request Method: GET
Request URI: /phonerecording.cgi?model=yealink
Request version: HTTP/1.0
Host: 10.1.2.224\r\n
User-agent: yealink SIP-T46G 28.71.0.10 00:16:65:11:30:68\r\n
```

If the recording is successfully started, the server will respond with a 200 OK message.

The example of a 200 OK message for reference:

```
<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.

The example of a 200 OK message for reference:

```
<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, then the server will respond with a 200 OK message.

The example of a 200 OK message for reference:

```
<YealinkIPPhoneText>
 <Title>
    </Title>
 <Text>
```

The recording session is successfully stopped.

</Text>

<YealinkIPPhoneText>

Procedure

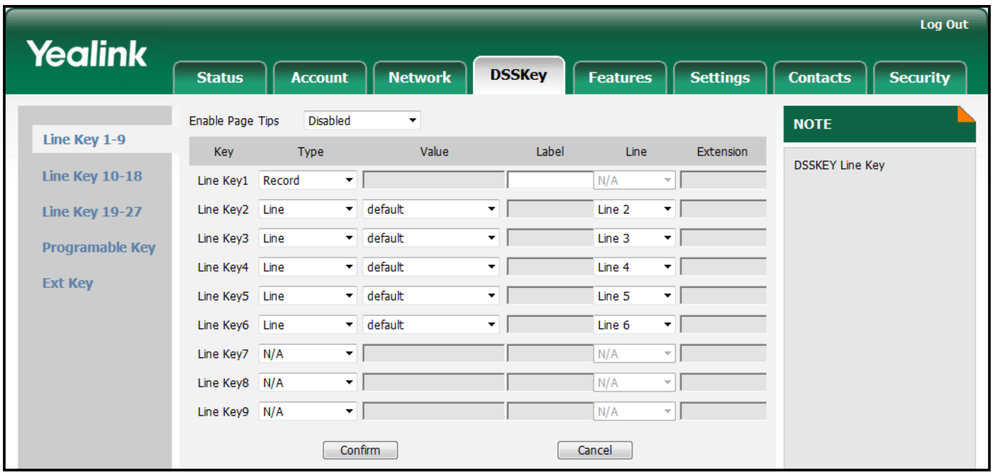
Call recording key can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Assign a record key. For more information, refer to Record Key on page 363. Assign a URL record key. For more information, refer to URL Record Key on page 363.
Local	Web User Interface	Assign a record key. Assign a URL record key. **Navigate to:** http://<phoneIPAddress>/servlet?p=dsskey&model=1&q=load&linepage=1
	Phone User Interface	Assign a record key. Assign a URL record key.

To configure a record key via web user interface:

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

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

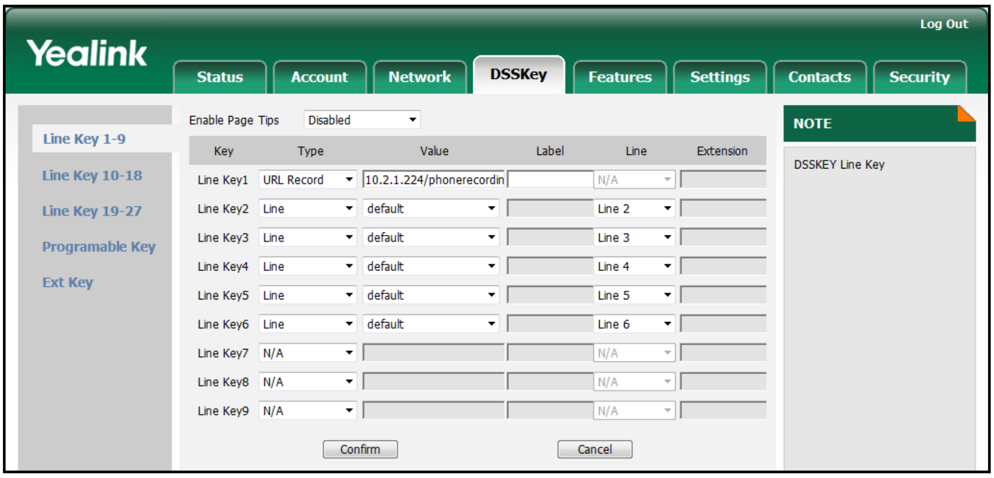


3. Click **Confirm** to accept the change.

To configure a URL record key via web user interface:

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

2. In the desired DSS key field, select **URL Record** from the pull-down list of **Type**.
3. Enter the URL in the **Value** field.



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

To configure a record key via phone user interface:

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

To configure a URL record key via phone user interface:

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

Hot Desking

Hot desking originates from the definition of being the temporary physical occupant of a work station or surface by a particular employee. A primary motivation for hot desking is cost reduction. Hot desking is regularly used in places where not all the employees are in the office at the same time, or not in the office for long periods at a time, which means actual personal offices would often be vacant, consuming valuable space and resources.

The hot desking feature allows a user to delete all accounts on the IP phone, register his account on line 1. In order to use this feature, you need to assign a hot desking key.

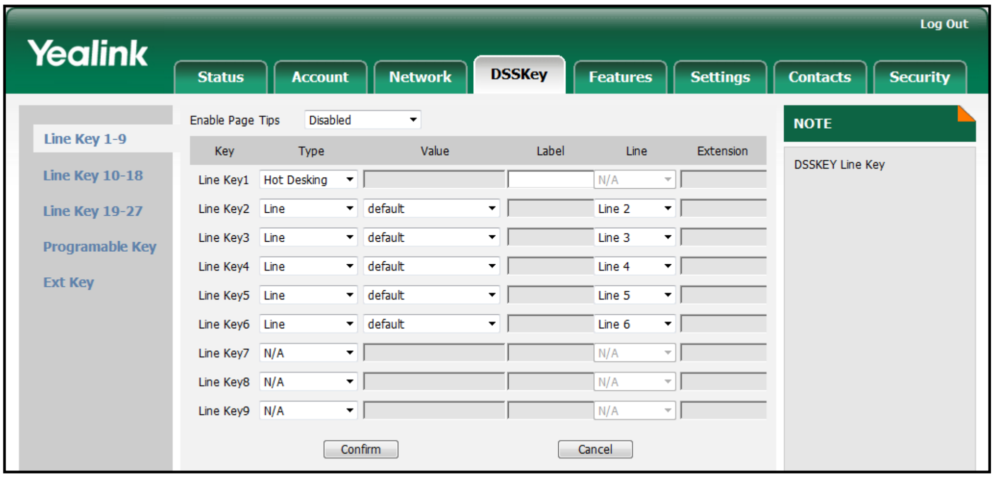
Procedure

Hot desking key can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Assign a hot desking key. For more information, refer to Hot Desking Key on page 364.
Local	Web User Interface	Assign a hot desking key. **Navigate to**: http://<phoneIPAddress>/servlet ?p=dsskey&q=load&model=1
	Phone User Interface	Assign a hot desking key.

To configure a hot desking key via web user interface:

1. Click on **DSSKey**->**Line Keys**.
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**->**Call Feature**->**DSS Keys**.
2. Select the desired DSS key.
3. Press or , or the **Switch** soft key to select **Key Event** from the **Type** field.
4. Press or , or the **Switch** soft key to select **Hot Desking** from the **Key Type** field.
5. (Optional.) Enter the string that will appear on the LCD screen in the **Label** field.
6. Press the **Save** soft key to accept the change.

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 be only triggered by the pre-defined events (e.g., log on). The valid URL formats are:

http://IP address of the server/help.xml?

and https://IP address of the server/help.xml?

The following table lists the pre-defined events for action URL.

Event	Description
Setup Completed	When the IP phone completes startup.
Registered	When the IP phone successfully registers an account.
Unregistered	When the IP phone logs off the registered account.
Register Failed	When the IP phone fails to register an account.
Off Hook	When the IP phone is off hook.
On Hook	When the IP phone is on hook.
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.
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 NoAnswer Forward	When the IP phone enables the no answer forward.
Close NoAnswer Forward	When the IP phone disables the no answer forward
Transfer Call	When the IP phone transfers a call.
Blind Transfer	When the IP phone blind transfers a call.
Attended Transfer	When the IP phone performs the attended transfer.
Hold	When the IP phone places a call on hold.
Unhold	When the IP phone retrieves a hold call.

Event	Description
Mute	When the IP phone mutes a call.
Unmute	When the IP phone unmutes a call.
Missed Call	When the IP phone misses a call.
IP Changed	When the IP address of the IP phone changes.
Forward Incoming Call	When the IP phone forwards an incoming call.
Reject Incoming Call	When the IP phone rejects an incoming call.
Answer New-In Call	When the IP phone answers a new call.
Transfer Finished	When the IP phone completes to transfer a call.
Transfer Failed	When the IP phone fails to transfer a call.
Idle to Busy	When the state of the IP phone changes from idle to busy.
Busy to Idle	When the state of phone changes from busy to idle.

An HTTP or HTTPS GET request may contain variable name and variable value, which are separated by "=". Each variable value starts with $ in the query part of the URL. The valid URL formats are: http://IP address of server/help.xml?variable name=$variable value and https://IP address of server/help.xml?variable name=$variable value. Variable name can be customized by users, while the variable value is pre-defined. For example, a URL *http://192.168.1.10/help.xml?mac=$mac* is specified for the event Mute, $mac will be dynamically replaced with the MAC address of the IP phone when the IP phone mutes a call.

The following table lists the pre-defined variable values.

Variable Value	Description
$mac	MAC address of the IP phone
$ip	The current IP address of the IP phone
$model	Phone model
$firmware	Phone firmware version
$active_url	The SIP URI of the current account when the IP phone places a call, receives an incoming call or establishes a call.
$active_user	The user part of the SIP URI for the current account when the IP phone places a call, receives an incoming call or establishes a call.
$active_host	The host part of the SIP URI for the current account when the IP phone places a call, receives an incoming

Variable Value	Description
	call or establishes a call.
$local	The SIP URI of the caller when the IP phone places a call. The SIP URI of the callee when the IP phone receives an incoming call.
$remote	The SIP URI of the callee when the IP phone places a call. The SIP URI of the caller when the IP phone receives an incoming call.
$display_local	The display name of the caller when the IP phone places a call. The display name of the callee when the IP phone receives an incoming call.
$display_remote	The display name of the callee when the IP phone places a call. The display name of the caller when the IP phone receives an incoming call.
$call_id	The call-id of the active call.

Procedure

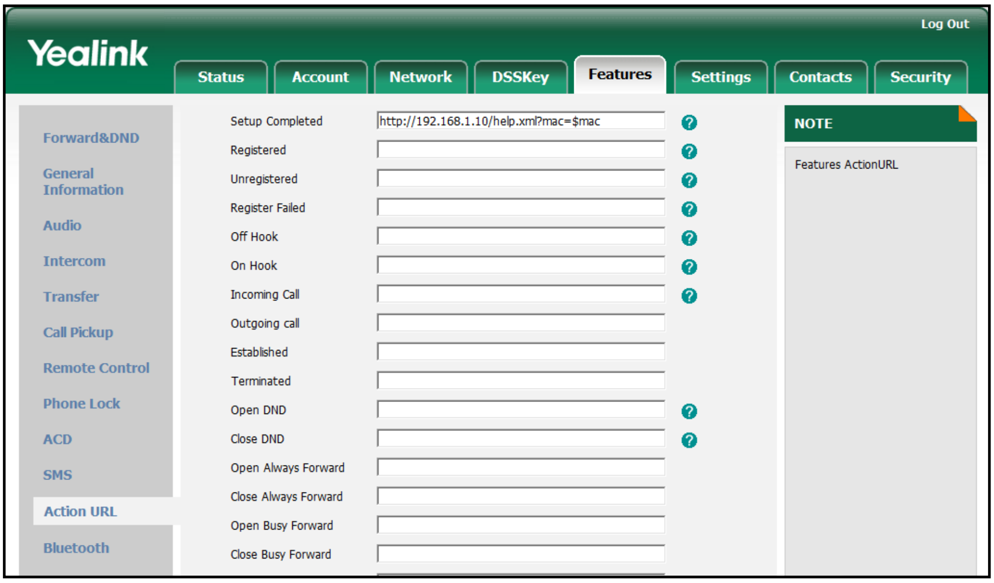
Action URL can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Configure the action URL on the IP phone. For more information, refer to Action URL on page 309.
Local	Web User Interface	Configure the action URL on the IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-actionurl&q=load

To configure action URL via web user interface:

1. Click on **Features**->**Action URL**.

2. Enter the action URLs in the corresponding fields.



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

Action URI

Opposite to action URL, action URI allows IP phones to interact with web server application by receiving and handling an HTTP or HTTPS GET request. When receiving a GET request, the IP phone will perform the specified action and respond with a 200 OK message. A GET request may contain variable named as "key" and variable value, which are separated by "=". The valid URI formats are:

http://phone IP address/servlet?key=variable value

and https://phone IP address/servlet?key=variable value

The following table lists the pre-defined variable values:

Variable Value	Phone Action
OK/ENTER	Press the OK key or the Enter soft key.
SPEAKER	Press the Speaker key.
F_TRANSFER	Press the TRANSFER key.
VOLUME_UP	Increase the volume.
VOLUME_DOWN	Decrease the volume.
MUTE	Mute the call.
F_HOLD	Press the HOLD key.
X	Press the X key.
0-9/*/POUND	Send the DTMF digit (0-9, * or #).

Variable Value	Phone Action
L1-L27	Press the Line key.
F_CONFERENCE	Press the Conference soft key.
F1-F4	Press the soft key.
MSG	Press the MESSAGE key.
HEADSET	Press the HEADSET key.
RD	Press the REDIAL key.
UP/DOWN/LEFT/RIGHT	Press the Navigation keys.
Reboot	Reboot the IP phone.
AutoP	Let the IP phone perform auto provisioning.
DNDOn	Activate the DND mode.
DNDOff	Deactivate the DND mode.

Note The variable value does not work with all events. For example, the variable value "MUTE" is only applicable when the IP phone is during a call.

For security reasons, the IP phones do not receive and handle the HTTP/HTTPS GET request by default. You need to specify the trusted IP address for action URI. When the IP phone receives a GET request from the specified IP address for the first time, the phone LCD screen prompts the message "Allow Remote Control?". You can specify one or more trusted IP addresses on the IP phone. You can also configure the IP phone to receive and handle the URI from any IP address.

Procedure

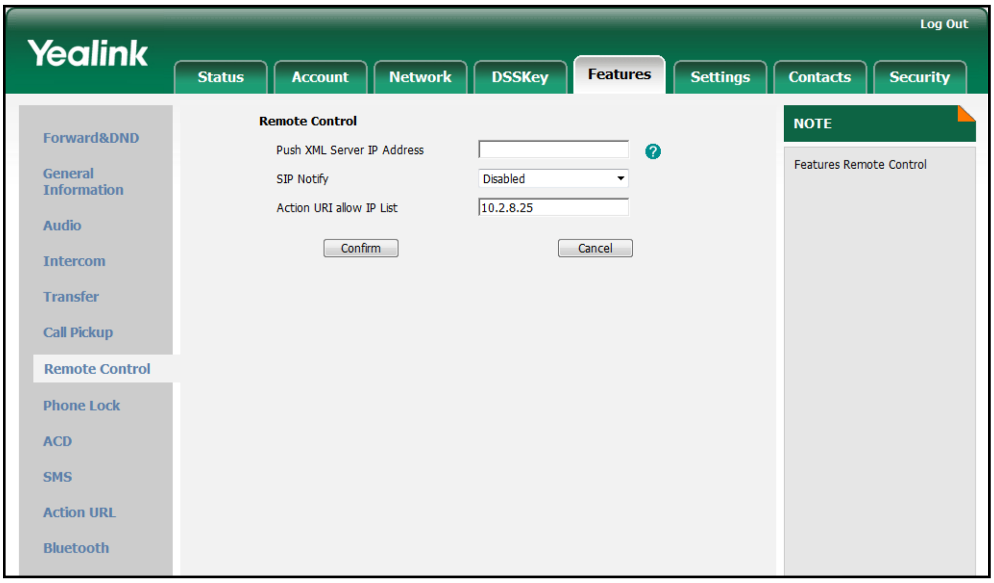
Specify the trusted IP address for Action URI using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Specify the trusted IP address(es) for sending the Action URI to the IP phone. For more information, refer to Action URI on page 311.
Local	Web User Interface	Specify the trusted IP address(es) for sending the Action URI to the IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-remotecontrl&q=load

To configure the trusted IP address(es) for Action URI via web user interface:

1. Click on **Features**->**Remote Control**.
2. Enter the IP address or any in the **Action URI allow IP List** field.

   Multiple IP addresses are separated by comma. 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.

Server Redundancy

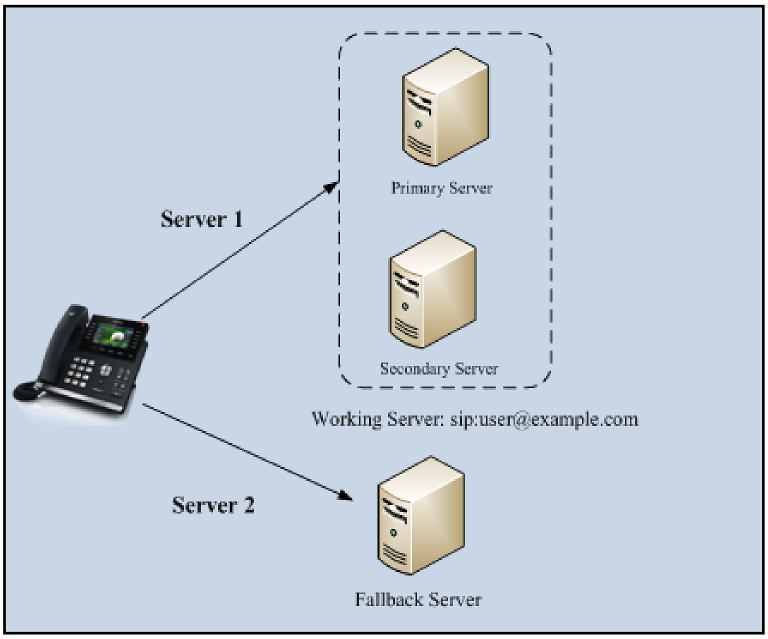
Server redundancy is often required in VoIP deployments to ensure continuity of phone service, for events where the server needs to be taken offline for maintenance, the server fails, or the connection between the IP phone and the server fails.

Two types of redundancy are possible. In some cases, a combination of the two may be deployed:

- **Failover:** In this mode, the full phone system functionality is preserved by having a second equivalent capability call server take over from the one that has gone down/off-line. This mode of operation should be done using the DNS mechanisms from the primary to the secondary server.
- **Fallback:** In this mode, a second less featured call server (fallback server) with SIP capability takes over call control to provide basic calling capability, but without some of the richer features offered by the working server (for example, shared lines, call recording and MWI). The 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 next. In the example, server redundancy for fallback and fail-over purposes is deployed. Two separate SIP servers (a working server and a fallback server) are configured for per line registration.



Working Server: Server 1 is configured with the domain name of the working server. For example, sip:user@example.com. DNS mechanism is used such that the working server is capable of resolving to multiple physical SIP servers for fail-over purpose. The working server is deployed in redundant pairs, designated as primary and secondary servers. The primary server is the highest priority server in a cluster of servers resolved by the DNS server. The secondary server backs up a primary server when the primary server fails. It offers the same functionality as the primary server.

Fallback Server: Server 2 is configured with the address of the fallback server. For example, 192.168.1.15. A fallback server offers lesser functionality than the working server.

Phone Registration

The registration methods of the fallback mode include:

- **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 richer features offered by the working server.
- **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.

SIP Server Domain Name Resolution

If a domain name is configured for a SIP server, the IP address(es) associated with that domain name will be discovered through DNS as specified by RFC 3263. The DNS query involves NAPTR, SRV and A queries, which allows the IP phone to adapt to various deployment environments. The IP phone performs the NAPTR query for the SRV pointer and service type (UDP, TCP and TLS), the SRV query on the record returned from the NAPTR for the host name and the port number, and the A query for the IP addresses.

If a port is set to 0 and the transport type is set to DNS-NAPTR, NAPTR and SRV queries will be tried before falling back to A queries. If no port is found through the DNS query, 5060 will be used. If an explicit port (except 0) is specified and the transport type is set to DNS-NAPTR, the only lookup will be an A query.

The following details the procedures of DNS query for the IP phone to resolve the domain name of working server into the IP address, port and transport protocol.

NAPTR (Naming Authority Pointer)

First, the IP phone sends the NAPTR query to get the SRV pointer and service type. The IP phone performs a NAPTR query for the domain name. The sample of the NAPTR records for reference:

	order	pref	flags	service	regexp	replacement
IN NAPTR	90	50	"s"	"SIP+D2T"	""	_sip._tcp.example.com
IN NAPTR	100	50	"s"	"SIP+D2U"	""	_sip._udp.example.com

Parameters are explained in the following table:

Parameter	Description
order	Specify preferential treatment for the specific record. The order is from lowest to highest, lower order is MORE preferred.
pref	Specify the preference to process multiple NAPTR records with the same order value. Lower value is MORE preferred.
flags	The flag "s" means to do an SRV lookup.
service	Specify the transport protocols supported by the domain: 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.

Parameter	Description
replacement	Specify a domain name to be used for the next query.

The IP phone picks the first record, because its order of 90 is lower than 100. The pref parameter is unimportant as there is no other record with order 90. The flag “s” indicates performing the SRV query next. TCP will be used, targeted to a host determined by an SRV query of “_sip._tcp.example.com”. If the flag of the NAPTR record returned is empty, the IP phone will use "sip:user@example.com" for the next NAPTR query.

SRV (Service Location Record)

The IP phone performs a SRV query on the record returned from the NAPTR for the host name and the port number. The sample of the SRV records for reference:

	Priority	Weight	Port	Target
IN SRV	0	1	5060	server1.example.com
IN SRV	0	2	5060	server2.example.com

Parameters are explained in the following table:

Parameter	Description
Priority	Specify preferential treatment for the specific host entry. Lower priority is MORE preferred.
Weight	When priorities are equal, weight is used to differentiate the preference. The preference is from highest to lowest. Again, 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 is 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 “server2.example.com" for the A query.

A (Host IP Address)

The IP phone performs an A query for the IP address of the target host name. The sample of an A record for reference:

IN A 62.10.1.10

Outgoing Call When the Working Server Connection Fails

When the user initiates a call, the phone will go through the following steps to connect the call:

1. Send the INVITE request to the primary server.
2. If the primary server does not respond correctly to the INVITE, then try and 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 fails 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

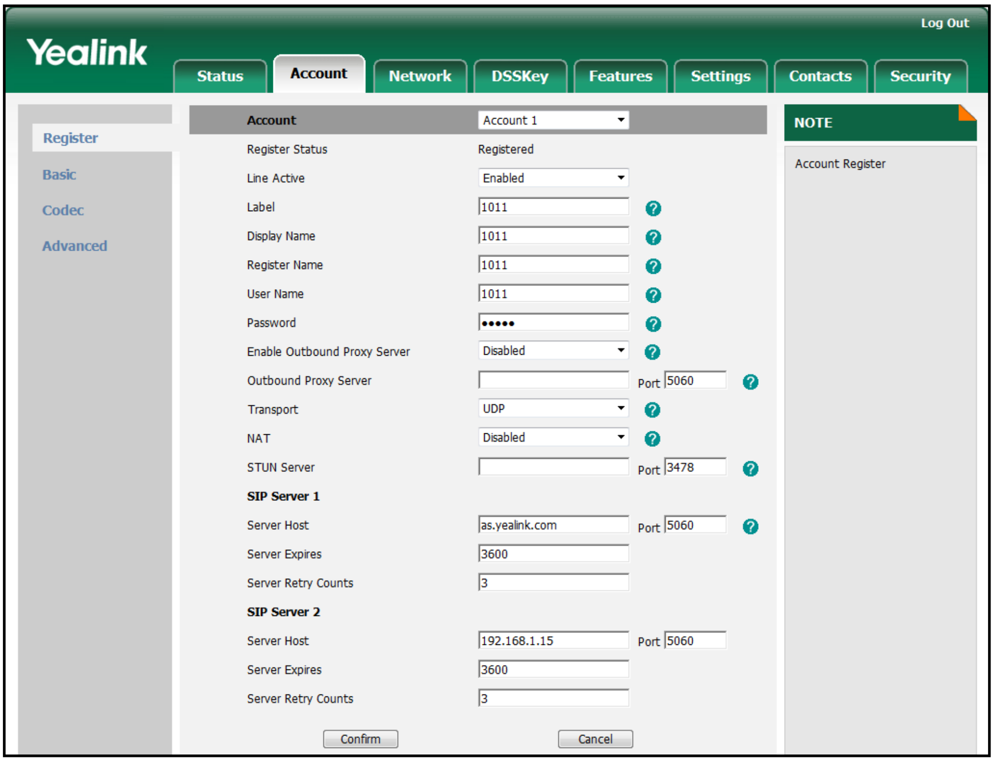
Server redundancy can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure the server redundancy on the IP phone. For more information, refer to Server Redundancy on page 311.
Local	Web User Interface	Configure the server redundancy on the IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-register&q=load&acc=0

To configure the server redundancy via web user interface:

1. Click on **Account**.
2. Select the desired account from the pull-down list of **Account**.
3. Select the desired value from the pull-down list of **Transport**.
4. Configure parameters of the SIP server 1 in the corresponding fields.

5. Configure parameters of the SIP server 2 in the corresponding fields.



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

LLDP

LLDP (Linker Layer Discovery Protocol) is a vendor-neutral Link Layer protocol. It allows IP phones to receive and/or transmit device-related information to directly connected devices on the network that are also using the protocol, and store the information that is learned about other devices. LLDP transmits information as packets called LLDP Data Units (LLDPDUs). An LLDPDU consists of a set of Type-Length-Value (TLV) elements, each of which contains a particular type of information about the device or port transmitting it.

LLDP-MED (Media Endpoint Discovery)

LLDP-MED is published by the Telecommunications Industry Association (TIA). It is an extension to LLDP that operates between endpoint devices and network connectivity devices. LLDP-MED provides the following capabilities for the IP phones:

- Capabilities Discovery -- allows LLDP-MED IP phones to determine the capabilities that the connected switch supports and has enabled.
- Network Policy -- provides voice VLAN configuration to notify IP phones which VLAN to use and QoS-related configuration for voice data. It provides a “plug and play” network environment.

- Power Management -- provides information related to how the IP phones are powered, power priority, and how much power IP phones need.
- Inventory Management -- provides a means to effectively manage the IP phones and the attributes of the IP phones such as model number, serial number and software revision.

TLVs supported by the IP phones are summarized in the following table:

TLV Type	TLV Name	Description
Mandatory TLVs	Chassis ID	The network address of the IP phone.
	Port ID	The MAC address of the IP phone.
	Time To Live	Seconds until data unit expires. The default value is 60s.
	End of LLDPDU	Marks end of LLDPDU.
Optional TLVs	System Name	Name assigned to the IP phone. The default value is "yealink".
	System Description	Description of the IP phone. The default value is "yealink".
	System Capabilities	The supported and enabled capabilities of phone. The supported capabilities are Bridge, Telephone and Router. The enabled capabilities are Bridge and Telephone by default.
	Port Description	Description of port that sent 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), 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.

TLV Type	TLV Name	Description
		The supported LLDP-MED TLV types are: LLDP-MED Capabilities, Network Policy, Extended Power via MDI-PD, Inventory.
	Network Policy	Port VLAN ID, application type, L2 priority and DSCP value.
	Extended Power-via-MDI	Power type, source, priority and value.
	Inventory – Hardware Revision	Hardware revision of phone.
	Inventory – Firmware Revision	Firmware revision of phone.
	Inventory – Software Revision	Software revision of phone.
	Inventory – Serial Number	Serial number of phone.
	Inventory – Manufacturer Name	Manufacturer name of phone. The default value is “yealink”.
	Inventory – Model Name	Model name of phone.
	Asset ID	Assertion identifier of phone. The default value is “asset”.

Procedure

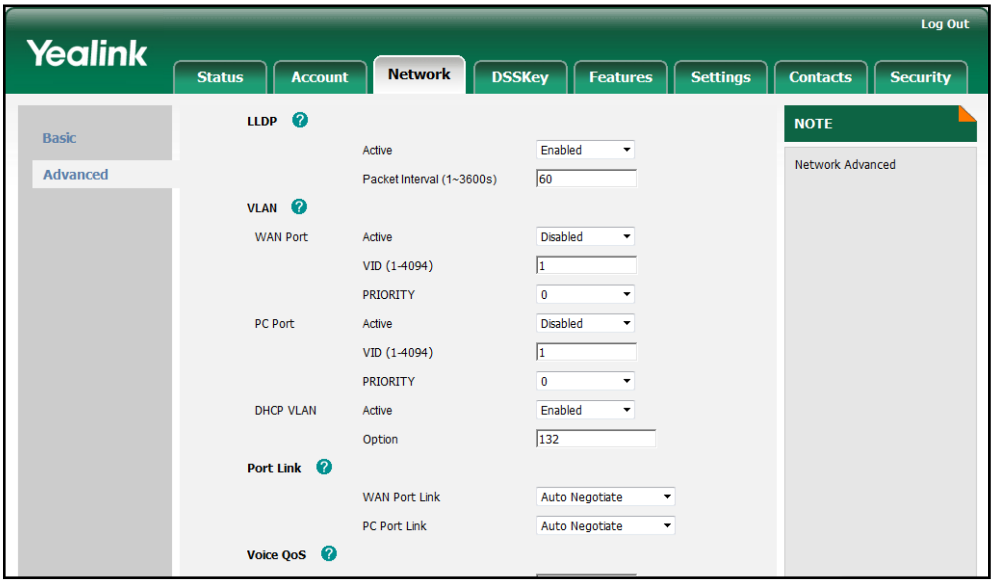
LLDP can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Configure the LLDP feature. For more information, refer to LLDP on page 311.
Local	Web User Interface	Configure the LLDP feature. **Navigate to:** http://<phoneIPAddress>/servlet?p=network-adv&q=load

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.

The valid values range from 1 to 3600.



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

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

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

VLAN

VLAN (Virtual Local Area Network) is used to logically divide a physical network into several broadcast domains. VLAN membership can be configured through software instead of physically relocating devices or connections. Grouping devices with a common set of requirements regardless of their physical location can greatly simplify network design. VLANs can address issues such as scalability, security, and network management.

The purpose of VLAN configurations on the IP phone is to insert tag with VLAN information to the packets generated by the IP phone. When VLAN is properly configured for the ports (internet port and PC port) on the IP phone, the IP phone will tag all packets from these ports with the VLAN ID. The switch receives and forwards the tagged packets to the corresponding VLAN according to the VLAN ID in the tag as described in IEEE Std 802.3.

The VLAN feature on the 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.

The IP phones support automatic discovery of the VLAN via LLDP or DHCP. The VLAN information can be also manually configured on the IP phones. The assignment takes place in this order: assignment via LLDP, manual configuration, and then assignment via DHCP.

VLAN Discovery via DHCP

IP phones support VLAN discovery via DHCP. When the VLAN Discovery method is set to DHCP, the IP phone will examine DHCP option for a valid VLAN ID. The predefined option 132 is used to supply the VLAN ID by default. You can customize the DHCP option used to request the VLAN ID.

Procedure

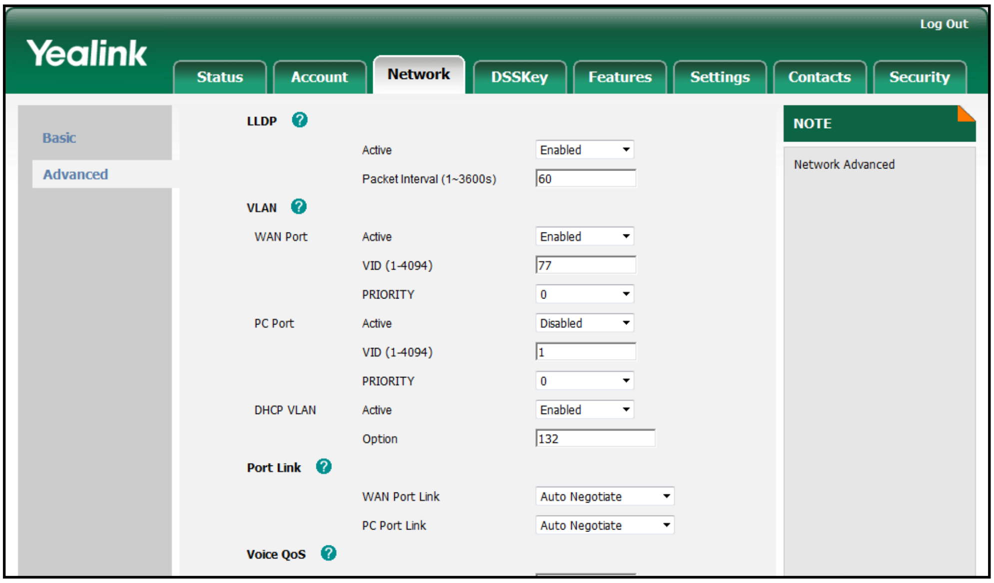
VLAN can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Configure VLAN for the Internet port. For more information, refer to VLAN on page 317. Configure VLAN for the PC port. For more information, refer to VLAN on page 317. Configure the DHCP VLAN discovery feature. For more information, refer to VLAN on page 317.
Local	Web User Interface	Configure VLAN for the Internet port and PC port and the DHCP VLAN discovery feature. **Navigate to:** http://<phoneIPAddress>/servlet?p=network-adv&q=load
	Phone User Interface	Configure VLAN for the Internet port and PC port.

To configure VLAN for Internet port via web user interface:

1. Click on **Network->Advanced**.
2. In the **VLAN** block, select the desired value from the pull-down list of **WAN Port Active**.
3. Enter the VLAN ID in the **VID (1-4094)** field.

4. Select the desired value (0-7) from the pull-down list of **PRIORITY**.



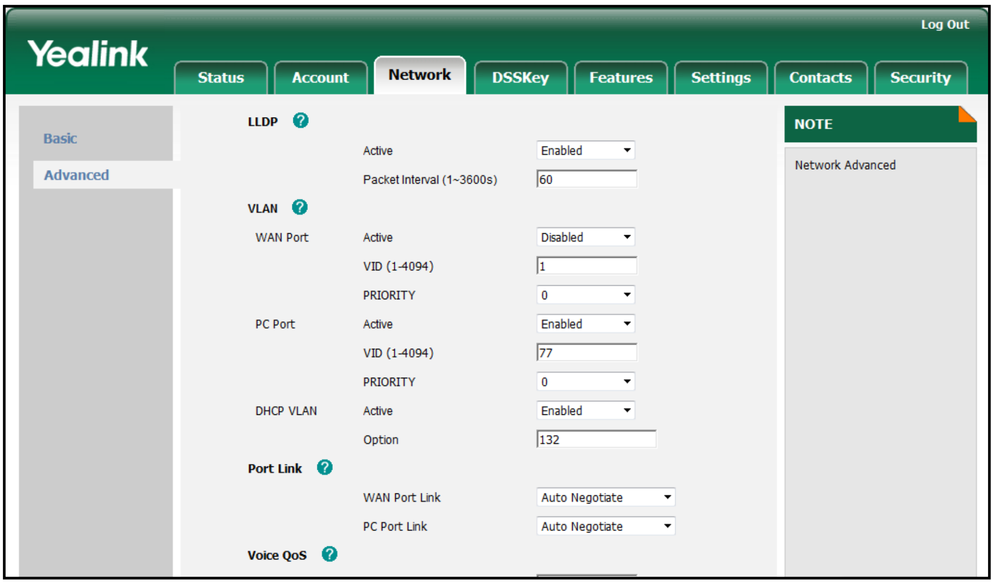
5. Click **Confirm** to accept the change.

   A dialog box pops up to prompt reboot to make the settings effective.

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

To configure VLAN for PC port via web user interface:

1. Click on **Network->Advanced**.
2. In the **VLAN** block, select the desired value from the pull-down list of **PC Port Active**.
3. Enter the VLAN ID in the **VID (1-4094)** field.
4. Select the desired value (0-7) from the pull-down list of **PRIORITY**.



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

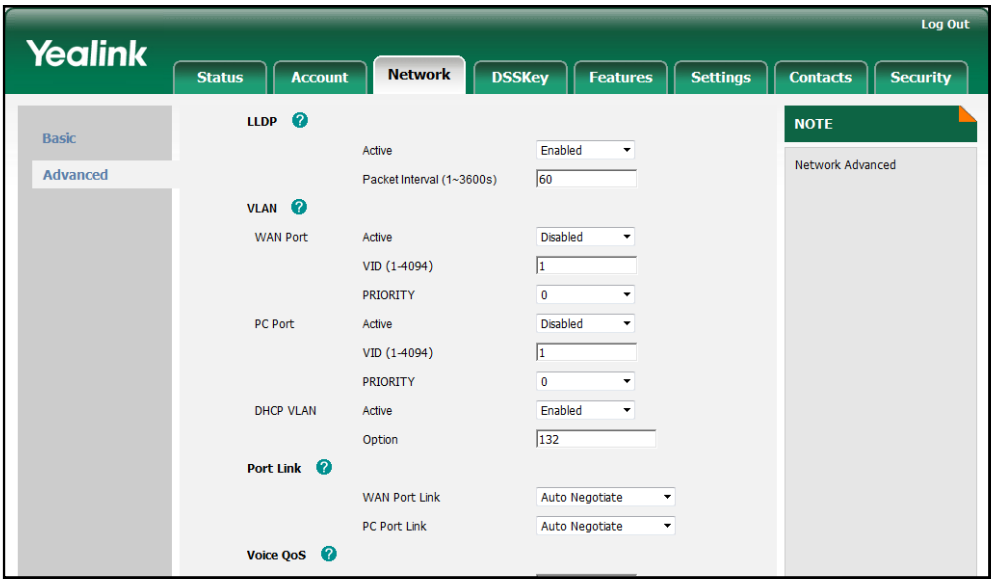
   A dialog box pops up to prompt that the settings will take effect after reboot.

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

To configure the DHCP VLAN discovery via web user interface:

1. Click on **Network**->**Advanced**.
2. In the **VLAN** block, select the desired value from the pull-down list of **DHCP VLAN Active**.
3. Enter the desired option in the **Option** field.

   The default option is 132.



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

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

To configure VLAN for Internet port (or PC port) via phone user interface:

1. Press **Menu**->**Advanced** (password: admin) ->**Network**->**VLAN**->**WAN Port** (or **PC Port**).
2. Press or , or the **Switch** soft key to select the desired value from the **VLAN Status** field.
3. Enter the VLAN ID (1-4094) in the **VID Number** field.
4. Enter the priority value (0-7) in the **Priority** field.
5. Press the **Save** soft key to accept the change.

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

VPN

VPN (Virtual Private Network) is a secured private network connection built on top of public telecommunication infrastructure, such as the Internet. It provides remote offices or individual users with secure access to their organization's network. VPN has become more prevalent due to the benefits: scalability, reliability, convenience and security. There are two types of VPN access: remote-access VPN (connecting an individual device to a network) and site-to-site VPN (connecting two networks together). Remote-access VPN allows employees to access their company's intranet from home or outside the office, and site-to-site VPN allows employees in geographically separated offices to share one cohesive virtual network. VPN can be also classified by the protocols used to tunnel the traffic. It provides security through tunneling protocols: IPSec, SSL, L2TP and PPTP.

The IP phones support SSL VPN. SSL VPN provides remote-access VPN capabilities through SSL. OpenVPN is a full featured SSL VPN software solution that creates secure connections in remote access facilities. It is designed to work with the TUN/TAP virtual networking interface. TUN and TAP are virtual network kernel devices. TAP simulates a link layer device and provides a virtual point-to-point connection. TUN simulates a network layer device and provides a virtual network segment. The IP phones support using OpenVPN to achieve the VPN feature. To prevent disclosure of private information, tunnel endpoints must authenticate each other before secure VPN tunnel is established. After the VPN feature is configured properly on the IP phone, the IP phone acts as a VPN client and uses the certificates to authenticate the VPN server.

To use the VPN feature, the compressed package of VPN-related files should be uploaded to the IP phone in advance. The file format of the compressed package must be .tar. The VPN-related files are: certificates (ca.crt and client.crt), key (client.key) and the configuration file (vpn.cnf) of the VPN client. For more information on how to package a tar file, refer to *VPN Feature on Yealink IP Phones*.

Procedure

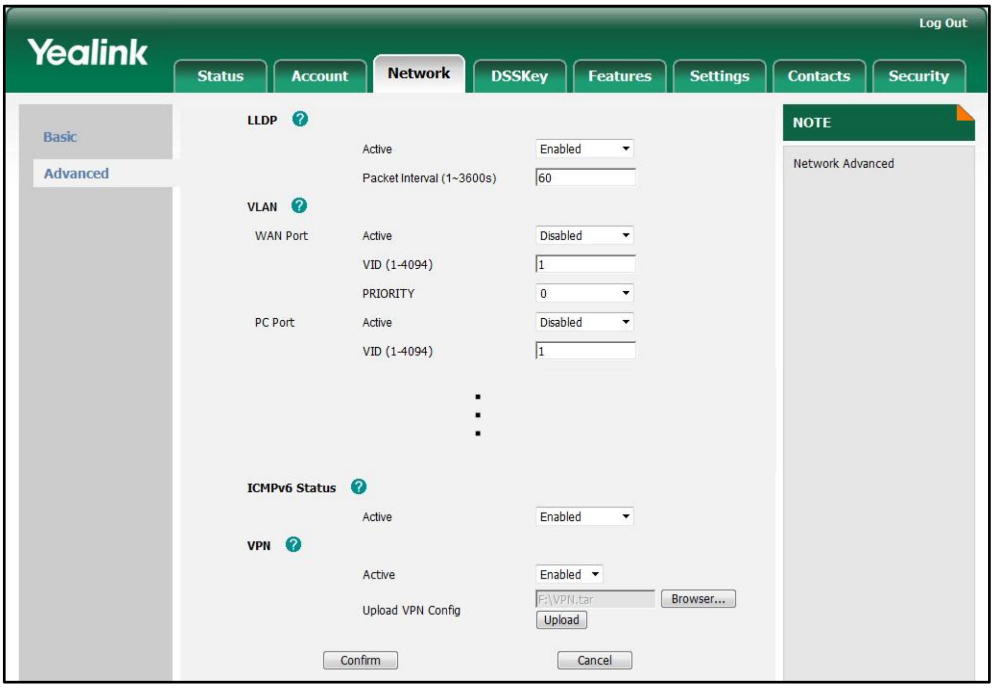
VPN can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Configure the OpenVPN feature and upload a tar file to the IP phone. For more information, refer to VPN on page 319.
Local	Web User Interface	Configure the OpenVPN feature and upload a tar package to the IP phone. **Navigate to:** http://<phoneIPAddress>/servlet?p=network-adv&q=load
	Phone User Interface	Configure the OpenVPN feature.

To upload the tar file to the IP phone and configure VPN via web user interface:

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

2. Click **Browse** to locate the tar package from the local system.
3. Click **Import** to import 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 **VPN Active**.
5. Click **Confirm** to accept the change.

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

To configure VPN via phone user interface after uploading the tar file:

1. Press **Menu**->**Advanced** (password: admin) ->**Network**->**VPN**.
2. Press ◀ or ▶ , or the **Switch** soft key to select the desired value from the **VPN Active** field.
3. Press the **Save** soft key to accept the change.

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

Quality of Service

Quality of Service (QoS) is the ability to provide different priorities to different packets in the network that allows 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 consider when configuring a modern QoS implementation, these include: bandwidth, delay, jitter and loss.

QoS provides better network service by providing the following features:

- Supporting dedicated bandwidth
- Improving loss characteristics
- Avoiding and managing network congestion
- Shaping network traffic
- Setting traffic priorities across the network

The Best-Effort service is the default QoS model in the IP networks. It provides no guarantees for data delivering, which means delay, jitter, packet loss and bandwidth allocation are unpredictable. Differentiated Services (DiffServ or DS) is the most widely supported 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. Each DSCP specifies a particular per-hop behavior (PHB) that is applied to a packet. A PHB refers to the packet scheduling, queuing, policing, or shaping behavior of a node on any given packet.

There are four standard PHBs available to construct a DiffServ-enabled network and achieve QoS:

- **Class Selector PHB** – is backwards compatible with IP precedence. Class Selector code points are of the form "xxx000". The first three bits are the IP precedence bits. These PHBs retain almost the same forwarding behavior as nodes that implement IP-precedence based classification and forwarding.
- **Expedited Forwarding PHB** – is the key ingredient in DiffServ model for providing a low-loss, low-latency, low-jitter and assured bandwidth service.
- **Assured Forwarding PHB** – defines a method by which BAs can be given different forwarding assurances.
- **Default PHB** – specifies that a packet marked with a DSCP value of "000000" gets the traditional best effort service from a DS-compliant node.

VoIP is extremely bandwidth and delay sensitive. QoS is a major issue in VoIP implementations. The issue is how to guarantee that packet traffic will 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

For VoIP transmissions to be intelligible to the receiver, voice packets should not be dropped, excessively delayed, or suffer varying delay. DiffServ model can guarantee high-quality voice transmission when the voice packets are configured 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, the SIP packets emanating from IP phones should be configured with a high transmission priority.

You can specify DSCPs for voice packets and SIP packets respectively.

Note

The DSCP value of voice traffic in the received LLDP packet will override the manual configuration.

Procedure

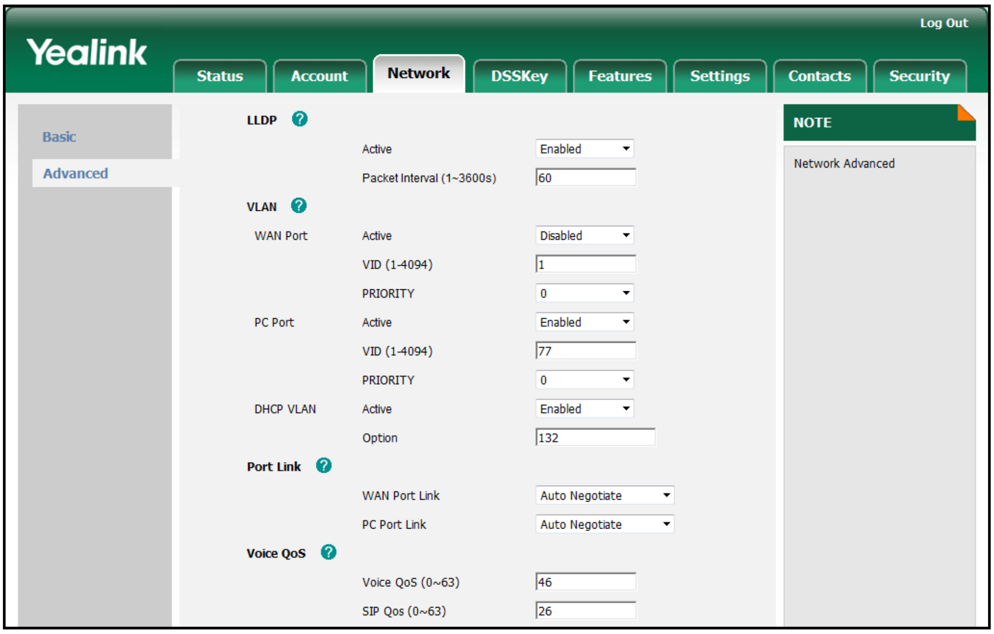
DSCPs for voice packets and SIP packets can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Configure the DSCPs for voice packets and SIP packets. For more information, refer to QoS on page 321.
Local	Web User Interface	Configure the DSCPs for voice packets and SIP packets. **Navigate to:** http://<phoneIPAddress>/servlet?p=network-adv&q=load

To configure DSCPs for voice packets and SIP packets via web user interface:

1. Click on **Network->Advanced**.
2. Enter the desired value in the **Voice QoS (0~63)** field.

3. Enter the desired value in the **SIP QoS (0~63)** field.



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

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

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

Network Address Translation

Network Address Translation (NAT) is essentially a translation table that maps public IP address and port combinations to private IP address and port combinations. This reduces the need for a large amount of public IP addresses. The NAT feature ensures security since each outgoing or incoming request must 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. It is 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, which is 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 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, which sends 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-account basis.

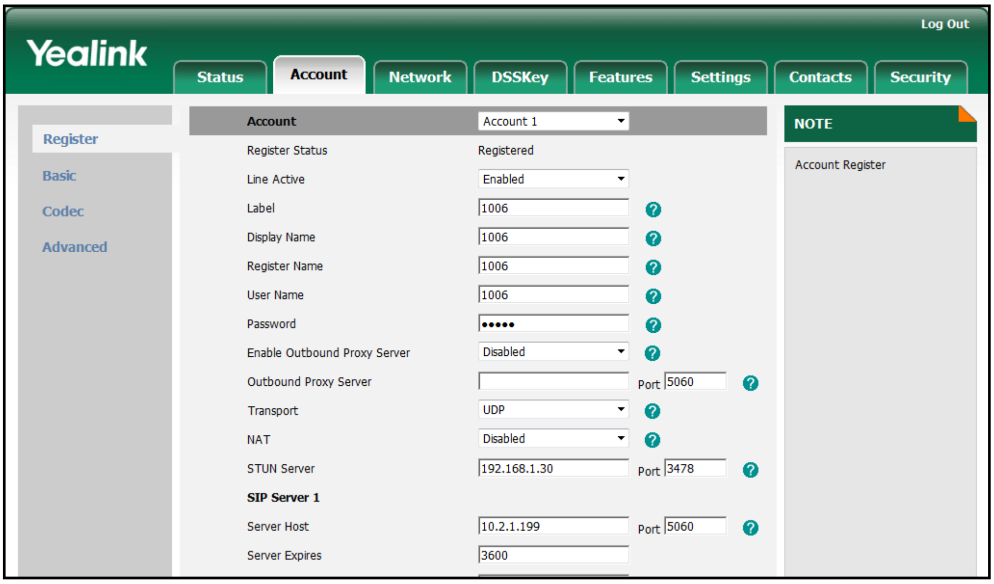
Procedure

NAT traversal and STUN server can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure the NAT traversal and STUN server on the IP phone. For more information, refer to Network Address Translation on page 321.
Local	Web User Interface	Configure the NAT traversal and STUN server on the IP phone. **Navigate to:** http://<phoneIPAddress>/servlet?p=account-register&q=load&acc=0

To configure the NAT traversal and STUN server via web user interface:

1. Click on **Account**.
2. Select the desired account from the pull-down list of **Account**.
3. Select **STUN** from the pull-down list of **NAT**.
4. Enter the IP address or the domain name in the **STUN Server** field.



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

SNMP

SNMP (Simple Network Management Protocol) is an Internet-standard protocol for managing devices on IP networks. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried by the managing applications. The variables accessible via SNMP are organized in hierarchies, which are described by Management Information Bases (MIBs).

IP phones only support SNMPv1 and SNMPv2. They act as SNMP clients, which receive requests from the SNMP server. The SNMP server may send requests from any available source port to the configured port on the client. The client then responds to the source port. IP phones only support the GET request from the SNMP server.

The following table lists the basic object identifiers (OIDs) supported by the IP phones:

MIB	OID	Description
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.1.0	The textual identification of the contact person for the IP phone, together with the contact information.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.2.0	An administratively-assigned name for the IP phone. If the name is unknown, the value is a zero-length string.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.3.0	The physical location of the IP phone.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.4.0	The time (in milliseconds) since the network management portion of the system was last re-initialized.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.5.0	The firmware version of the IP phone.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.6.0	The hardware version of the IP phone.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.7.0	The IP phone's model.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.8.0	The MAC address of the IP address.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.9.0	The IP address of the IP phone.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.10.0	The version of auto provisioning.

Procedure

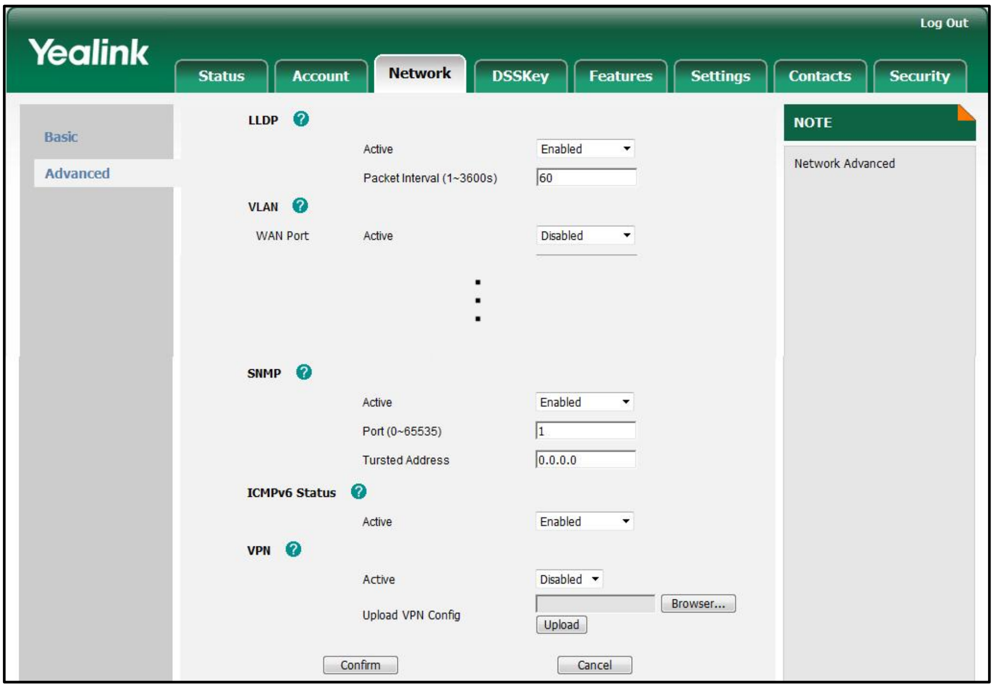
SNMP can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Configure SNMP on the IP phone. For more information, refer to SNMP on page 322.
Local	Web User Interface	Configure SNMP. **Navigate to:** http://<phoneIPAddress>/servlet?p=network-adv&q=load

To configure SNMP via web user interface:

1. Click on **Network**->**Advanced**.
2. In the **SNMP** block, select the desired value from the pull-down list of **Active**.
3. Enter the desired port in the **Port** field.
4. Enter the address(es) (IPv4, IPv6 or domain name) of the SNMP server in the **Trusted Address** field.

   Multiple addresses are separated by space.



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

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

802.1X Authentication

IEEE 802.1X authentication is an IEEE standard for Port-based Network Access Control (PNAC). It is 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. 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 username and password, to 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 using the EAP-MD5, EAP-TLS, PEAP-MSCHAPV2 and EAP-TTLS/EAP-MSCHAPv2 protocols for 802.1X authentication.

Procedure

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

Configuration File	<y000000000028>.cfg	Configure the 802.1X authentication on the IP phone. For more information, refer to 802.1X on page 324.
Local	Web User Interface	Configure the 802.1X authentication on the IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?p=network-adv&q=load
	Phone User Interface	Configure the 802.1X authentication on the IP phone.

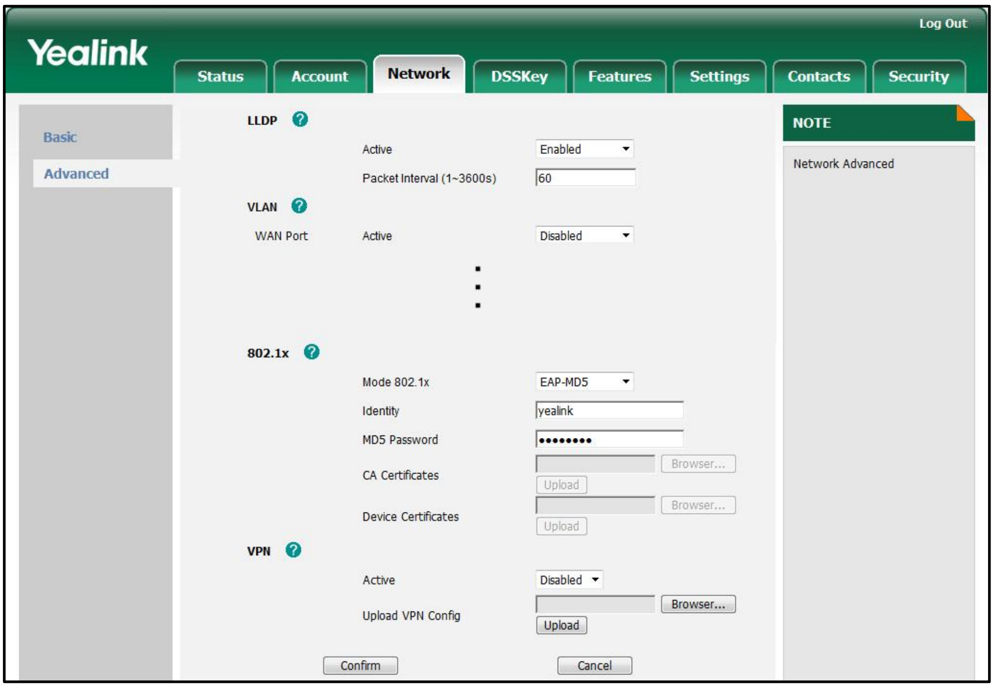
To configure the 802.1X via web user interface:

1. Click on **Network**->**Advanced**.
2. In the **802.1x** block, select the desired protocol from the pull-down list of **Mode 802.1x**.

   a) If you select **EAP-MD5**:

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

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



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

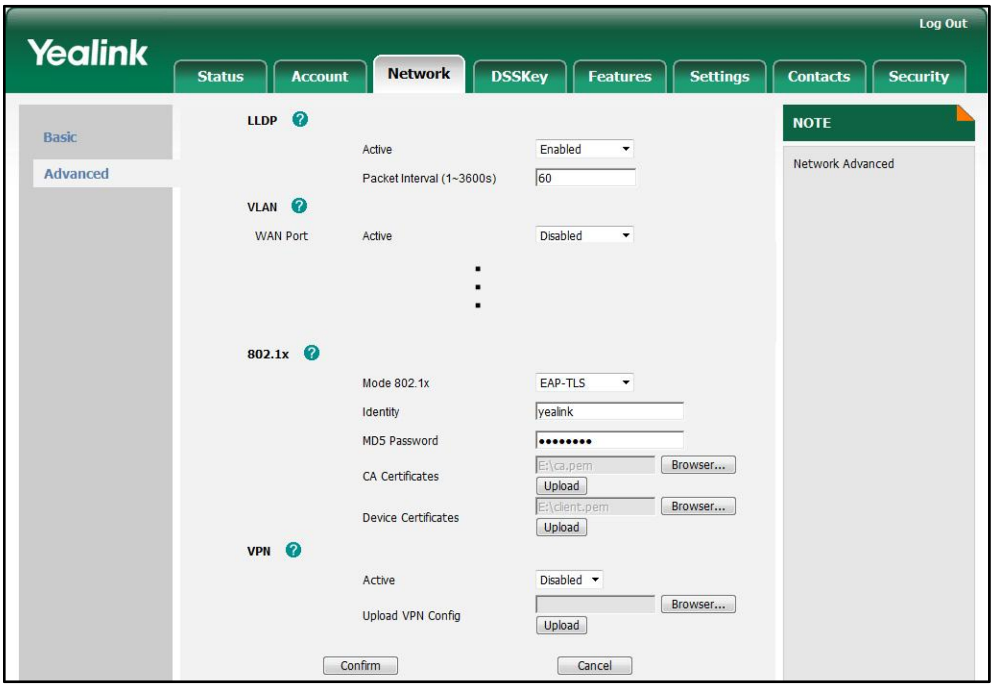
1) Enter the username for authentication in the **Identity** field.

2) Leave the **MD5 Password** field blank.

3) In the **CA Certificate** field, click **Browse** to select the desired CA certificate (*.pem,*.crt, *.cer or *.der) from your local system.

4) In the **Device Certificate** field, click **Browse** to select the desired client certificate (*.pem or *.cer) from your local system.

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



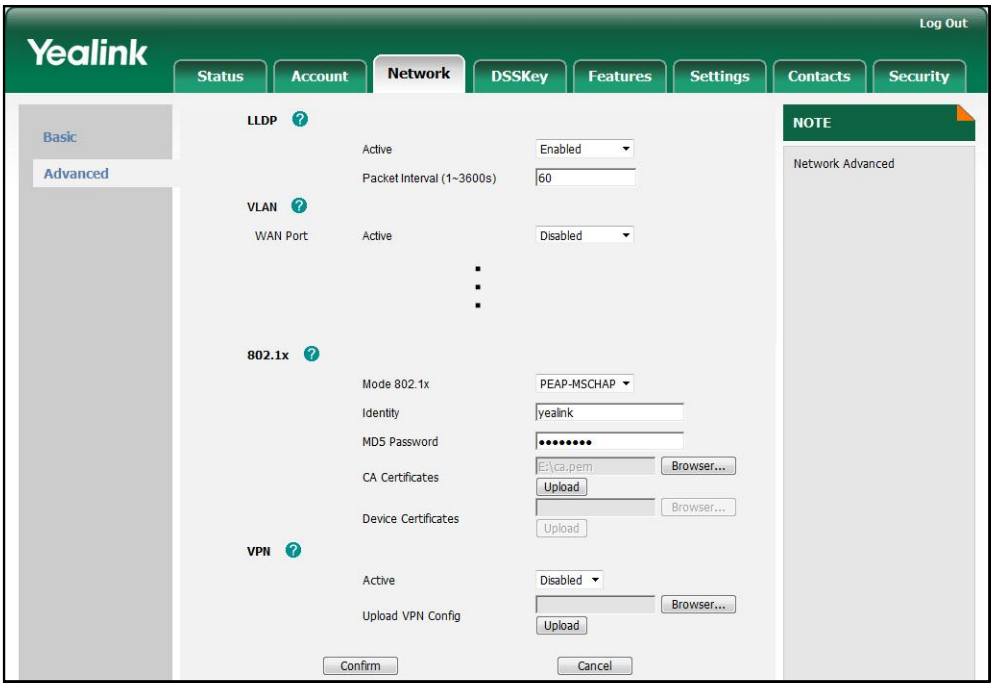
c) If you select **PEAP-MSCHAPV2**:

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

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

3) In the **CA Certificate** field, click **Browse** to select the desired certificate (*.pem,*.crt, *.cer or *.der) from your local system.

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



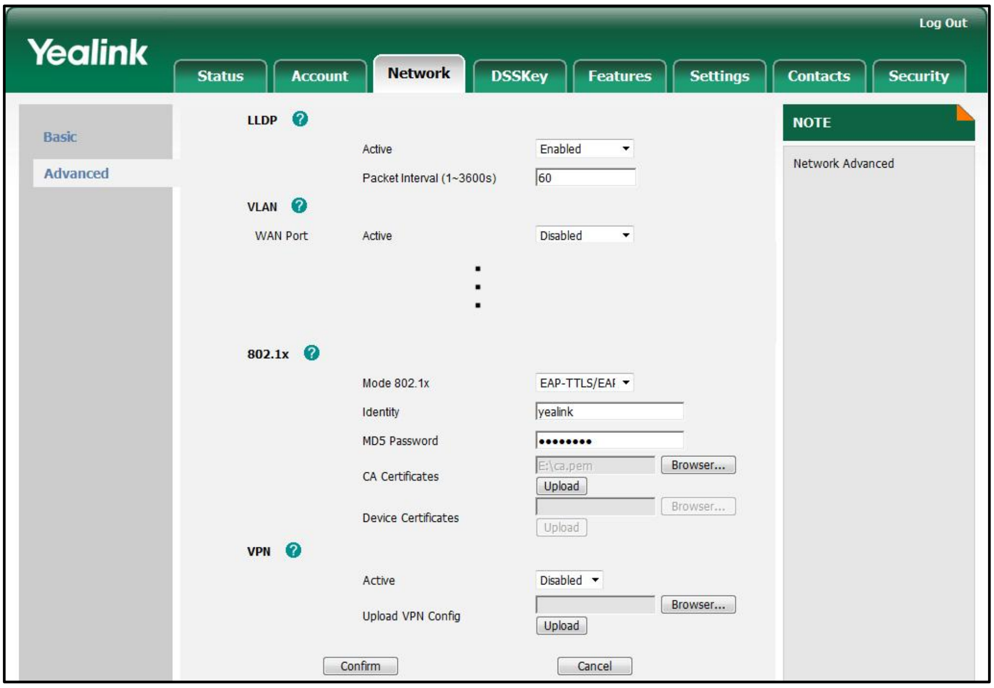
d) If you select **EAP-TLS/EAP-MSCHAPV2**:

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

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

3) In the **CA Certificate** field, click **Browse** to select the desired certificate (*.pem,*.crt, *.cer or *.der) from your local system.

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



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

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

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

To configure the 802.1X via phone user interface after:

1. Press **Menu**->**Advanced** (password: admin) ->**Network**->**802.1x**.

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 username for authentication in the **Identity** field.

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

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

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

      2) Leave the **Password** field blank.

   c) If you select **PEAP-MSCHAPV2**:

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

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

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

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

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

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

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

TR-069 Device Management

TR-069 is a technical specification, which is defined by the Broadband Forum. It defines a mechanism that encompasses secure auto-configuration of a CPE (Customer-Premises Equipment), and also 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.

The 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

RPC Method	Description
	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.
FactoryReset	This method resets the CPE to its factory default state.
TransferComplete	This method informs the ACS of the completion (either successful or unsuccessful) of a file transfer initiated by an earlier Download or Upload method call.
AddObject	This method is used to add a new instance of an object defined on the CPE.
DeleteObject	This method is used to remove a particular instance of an object.

Procedure

TR-069 can be configured using the configuration files or locally.

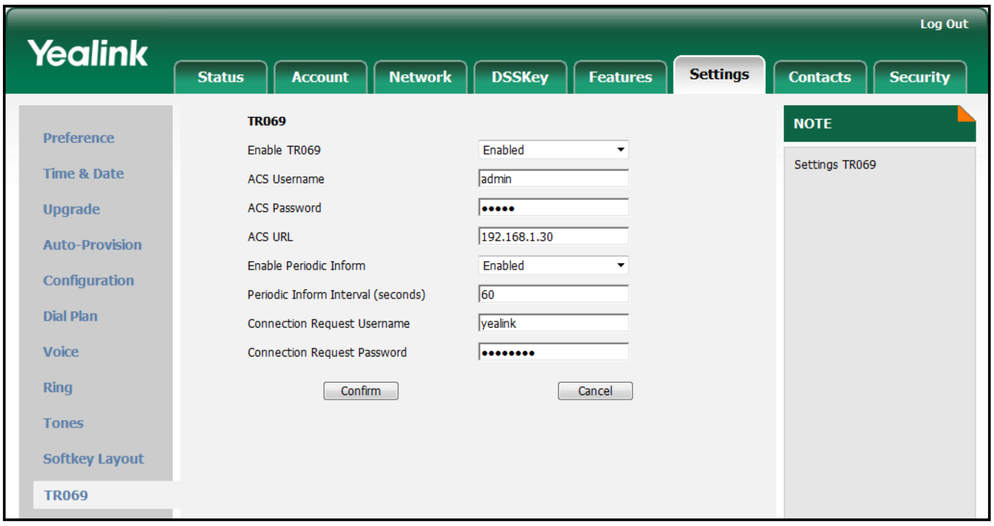
Configuration File	<y000000000028>.cfg	Configure theTR-069 feature. For more information, refer to TR-069 on page 325.
Local	Web User Interface	Configure the TR-069 feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-preference&q=load

To configure TR-069 via web user interface:

1. Click on **Settings**->**TR069**.
2. Select **Enabled** from the pull-down list of **Enable TR069**.
3. Enter the username 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 username 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 that was designed as a replacement for the current IPv4 protocol. IPv6 was 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, which consists of eight groups of four hexadecimal digits separated by colons. VoIP network based on IPv6 can ensure QoS, a set of service requirements to deliver performance guarantee while transporting traffic over the network.

IP phones support IPv4 only addressing mode, IPv6 only addressing mode, as well as an IPv4/IPv6 dual stack addressing mode.

IPv6 Address Assignment Method

IP phones support the following 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 on the IP phone, it is important that the IP phone is connected to a network with at least one IPv6 router connected. This

router is configured by the network administrator and sends out Router Advertisement announcements onto the link. These announcements can allow the on-link connected IP phone to configure itself with IPv6 address, as specified in RFC 4862.

- **Stateful DHCPv6:** The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) has been standardized by the IETF through RFC3315. DHCPv6 enables DHCP servers to pass configuration parameters such as IPv6 network addresses to IPv6 nodes. It offers the capability of automatic allocation of reusable network addresses and additional configuration flexibility. This protocol is a stateful counterpart to "IPv6 Stateless Address Autoconfiguration", and can be used separately or in addition to the stateless autoconfiguration to obtain configuration parameters.

Note

If the IP phone enables the SLAAC and DHCPv6 features both, the phone will obtain the IP address from the SLAAC and obtain the other network parameters from DHCPv6.

Procedure

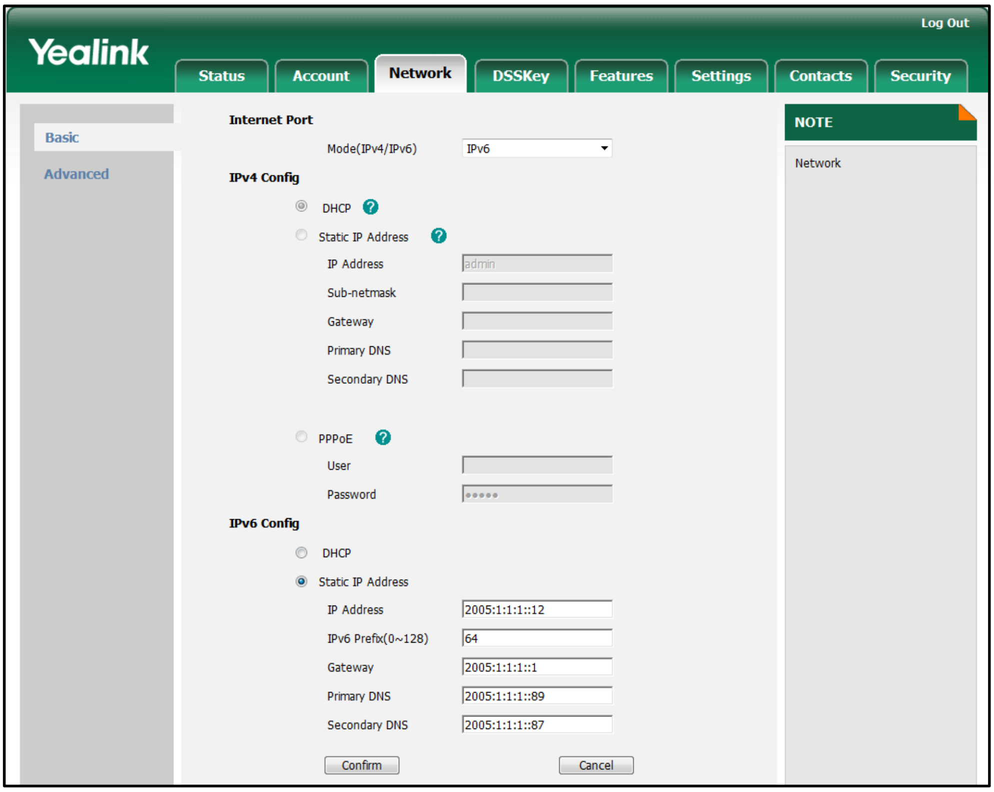
IPv6 can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Configure the IPv6 address assignment method. For more information, refer to IPv6 on page 329.
Local	Web User Interface	Configure the IPv6 address assignment method. **Navigate to:** http://<phoneIPAddress>/servlet?p=network&q=load

To configure IPv6 address assignment method via web user interface:

1. Click on **Network->Basic**.
2. Select the desired address mode (IPv6 or IPv4&IPv6) from the pull-down list of **Internet Port Mode**.
3. In the **IPv6 Config** block, mark the **DHCP** or the **Static IP Address** radio box.

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



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

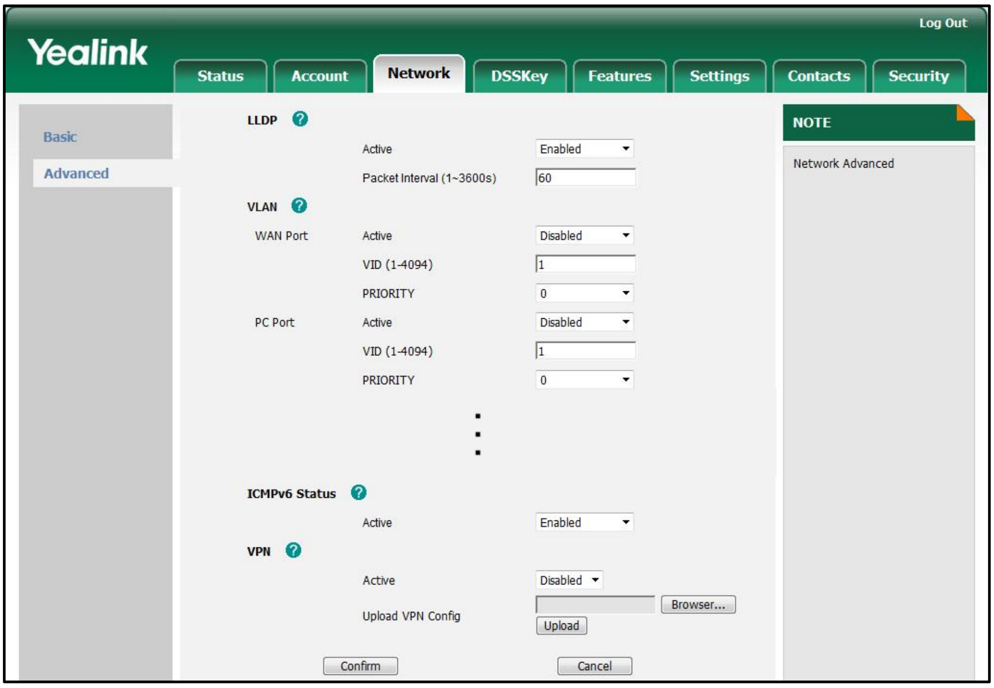
   A dialog box pops up to prompt that the settings will take effect after reboot.

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

To configure the SLAAC feature via web user interface:

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

2. In the **ICMPv6 Status** block, select the desired value from the pull-down list of **Active**.



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

To configure IPv6 address via phone user interface:

1. Press **Menu**->**Advanced** (password: admin) ->**Network**->**WAN Port**.
2. Press or to select the desired address mode from the **IP Mode** field.
3. Press or to highlight **IPv6** and press the **Enter** soft key.
4. Press or to select the desired IPv6 address assignment method.

   If you select the **Static IP**, configure the IPv6 address and other configuration parameters in the corresponding fields.
5. Press the **Save** soft key to accept the change

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

Configuring Audio Features

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

- Headset Prior
- Dual Headset
- Audio Codecs
- Acoustic Clarity Technology

Headset Prior

The headset prior feature 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

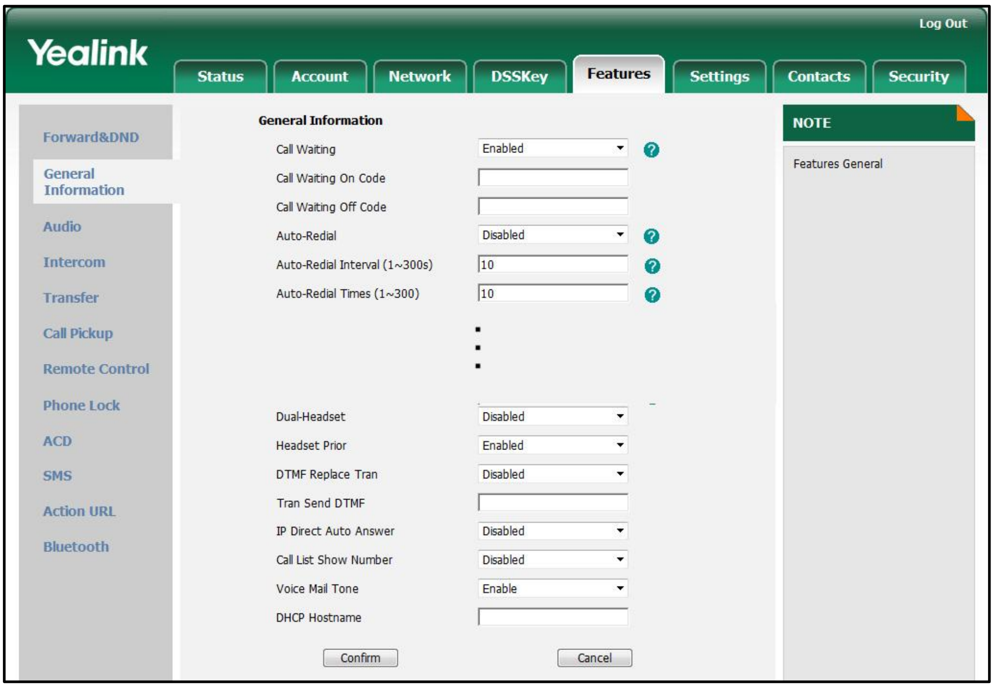
Headset prior can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Configure the headset prior feature. For more information, refer to Head Prior on page 332.
Local	Web User Interface	Configure the headset prior feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

To configure headset prior via web user interface:

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

2. Select the desired value from the pull-down list of **Headset Prior**.



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

Dual Headset

The dual headset feature allows users to use two headsets on one IP phone. To use this feature, the users need to physically connect two headsets to the headset jack and handset jack respectively. Once the IP phone joins in a call, the user with the headset connected to the headset jack has a full-duplex conversation, while the user with the headset connected to the handset jack is only allowed to listen to.

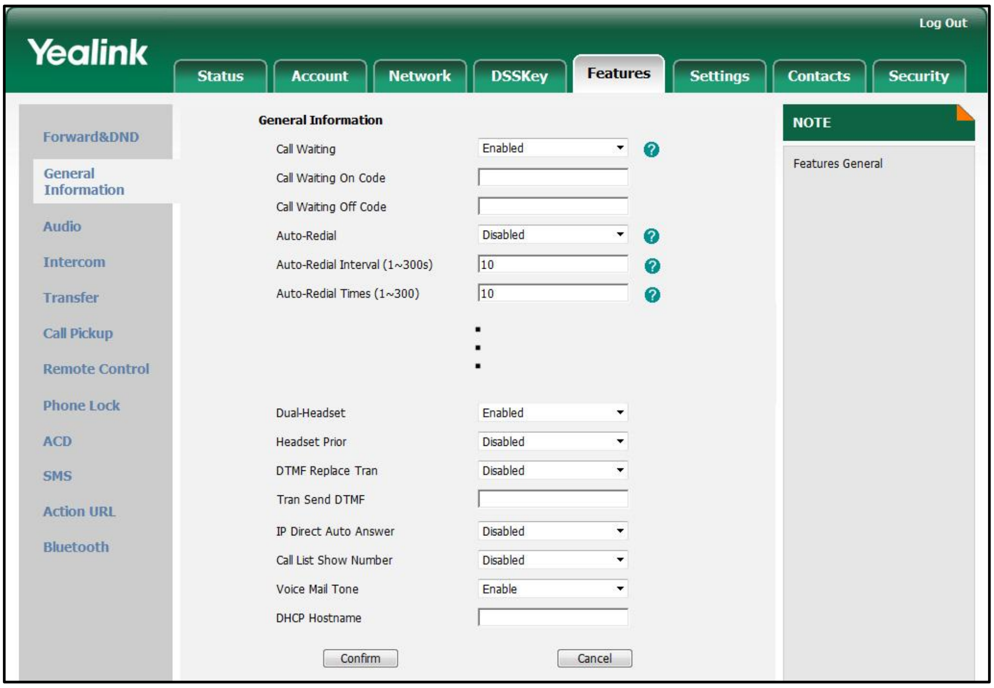
Procedure

Dual headset can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Configure the dual headset feature. For more information, refer to Dual Headset on page 333.
Local	Web User Interface	Configure the dual headset feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

To configure dual headset via web user interface:

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



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

Audio Codecs

CODEC is an abbreviation of COmpress-DECompress. It is 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 transmission of the audio.

The default codecs used on IP phones are summarized in the following table:

Codec	Algorithm	Bit Rate	Sample Rate	Packetization Time
PCMA	G.711 a-law	64 Kbps	8 Ksps	20ms
PCMU	G.711 u-law	64 Kbps	8 Ksps	20ms
G729	G.729	8 Kbps	8 Ksps	20ms
G722	G.722	64 Kbps	16 Ksps	20ms

In addition to the codecs introduced above, IP phones also support the codecs: G723_53, G723_63, G726_16, G726_24, G726_32, G726_40, iLBC, iLBC_13_3, iLBC_15_2 and GSM. You can configure the preferred codecs to use on a per-account basis instead of using the default codecs. You can also configure the priorities for the enabled codecs. 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
PCMU	Configuration Files Web User Interface	1	0
PCMA	Configuration Files Web User Interface	2	8
G729	Configuration Files Web User Interface	3	18
G722	Configuration Files Web User Interface	4	9
G723_53	Configuration Files Web User Interface	0	4
G723_63	Configuration Files Web User Interface	0	4
G726_16	Configuration Files Web User Interface	0	112
G726_24	Configuration Files Web User Interface	0	102
G726_32	Configuration Files Web User Interface	0	99
G726_40	Configuration Files Web User Interface	0	104
iLBC	Configuration Files	0	102
iLBC_13_3	Configuration Files	0	97
iLBC_15_2	Configuration Files	0	97
GSM	Configuration Files Web User Interface	0	3

Packetization Time

Ptime (Packetization Time) is measurement of the duration (in milliseconds) of the audio data in each RTP packet sent to the destination, and hence it defines how much network bandwidth is used for transfer of the RTP stream. Before establishing a conversation, codec and ptime are negotiated through SIP signaling. The valid values of ptime range from 10 to 60, in increments of 10 milliseconds. The default ptime is 20ms. You can also disable the ptime negotiation.

Procedure

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

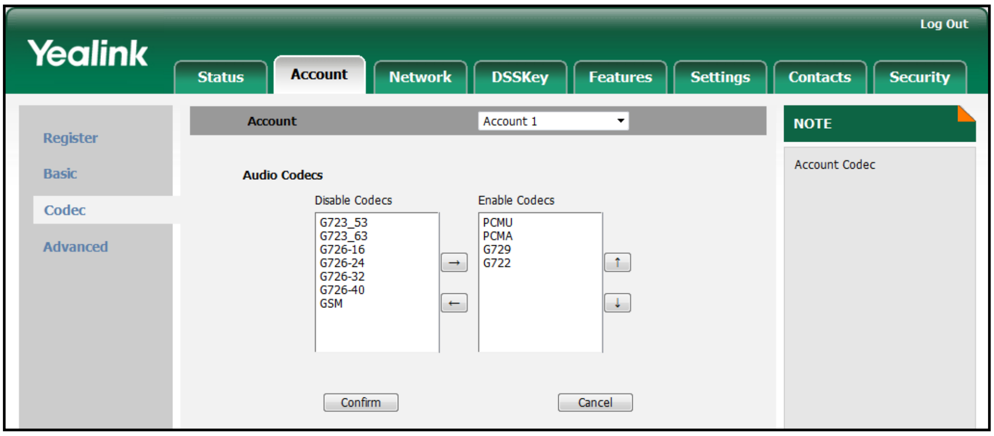
Configuration File	<MAC>.cfg	Configure the codecs to use on a per-account basis. Configure the priority and rtpmap for the enabled codec. For more information, refer to Audio Codecs on page 333. Configure the ptime. For more information, refer to Audio Codecs on page 333.
Local	Web User Interface	Configure the codecs and adjust the priority of the enabled codecs on a per-account basis. Configure the ptime. **Navigate to:** http://<phoneIPAddress>/servlet?p=account-codec&q=load&acc=0

To configure the codecs and adjust the priority of the enabled codecs on a per-account basis via web user interface:

1. Click on **Account**.
2. Select the desired account from the pull-down list of **Account**.
3. Click on **Codec**.
4. Select the desired codec from the **Disable Codecs** column and click →.

   The selected codec appears in the **Enable Codecs** column.
5. Repeat the step 4 to add more codecs to the **Enable Codecs** column.
6. To remove the codec from the **Enable Codecs** column, click ←.

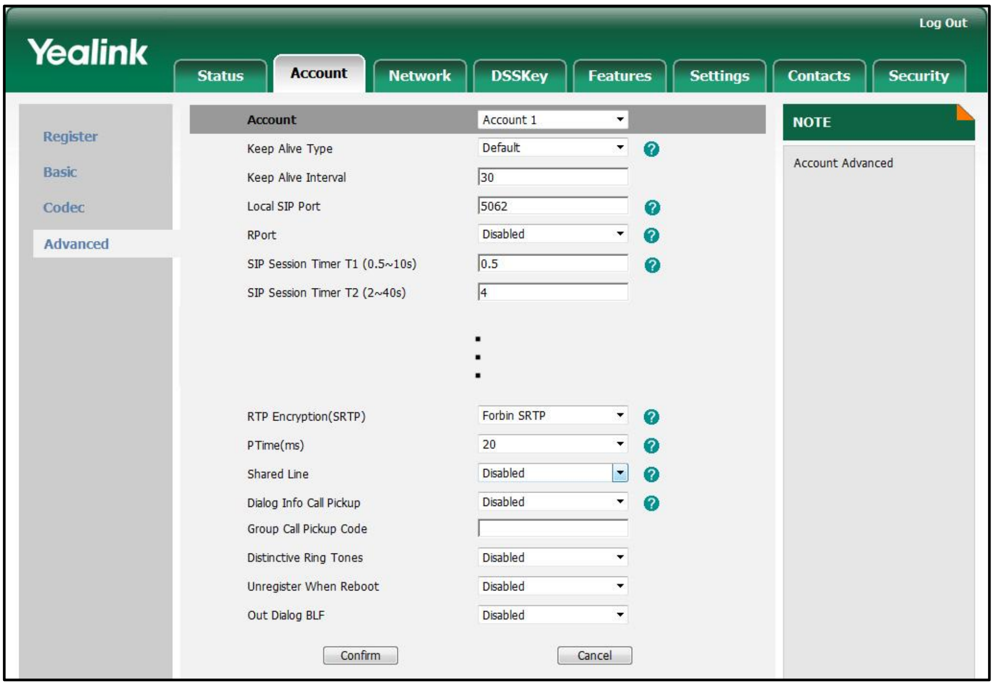
7. To adjust the order of the enabled codecs, click ↑ or ↓ .



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

To configure the Ptime on a per-account 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 remove acoustic echo from a voice communication in order to improve the voice quality. It also increases the capacity achieved through silence suppression by preventing echo from traveling across a network. IP phones employ advanced AEC for hands-free operation. Echo cancellation is done using the echo canceller.

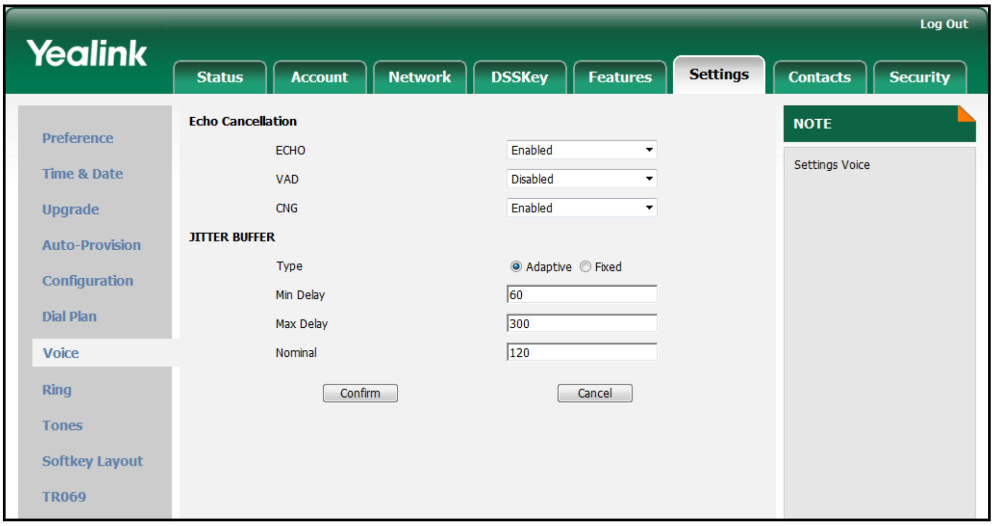
Procedure

AEC can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Configure the AEC feature. For more information, refer to Acoustic Echo Cancellation on page 337.
Local	Web User Interface	Configure the AEC feature. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-voice&q=load

To configure AEC via web user interface:

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



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

Voice Activity Detection

Voice Activity Detection (VAD) is used in speech processing to detect the presence or absence of human speech. When detecting period of "silence", VAD replaces that silence efficiently with special packets that indicate silence is occurring. It can facilitate speech processing, and can also be used to 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 on network bandwidth.

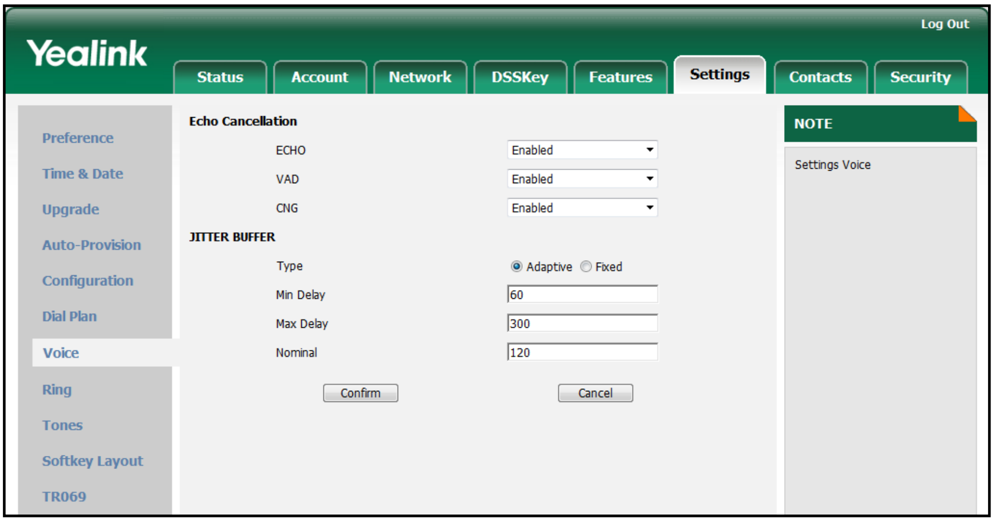
Procedure

VAD can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Configure the VAD feature. For more information, refer to Voice Activity Detection on page 337.
Local	Web User Interface	Configure the VAD feature. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-voice&q=load

To configure VAD via web user interface:

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



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

Comfort Noise Generation

Comfort Noise Generation (CNG) is used to generate background noise for voice communications during periods of silence that occur during the conversation. It is part of the silence suppression or VAD handling for VoIP technology. CNG, in conjunction with VAD algorithms, quickly determines 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.

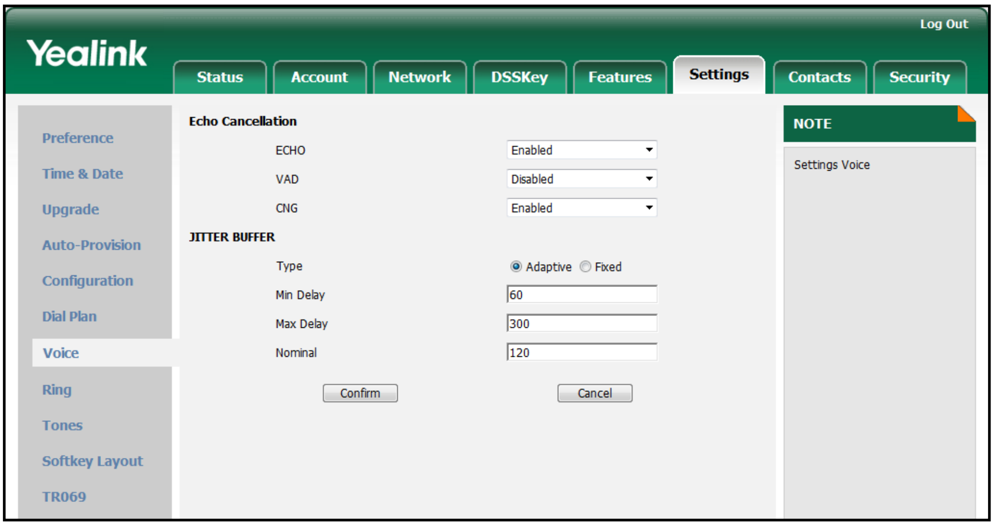
Procedure

CNG can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Configure the CNG feature. For more information, refer to Comfort Noise Generation on page 337.
Local	Web User Interface	Configure the CNG feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-voice&q=load

To configure CNG via web user interface:

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



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

Jitter Buffer

Jitter buffer is a shared data area where voice packets can be collected, stored, and sent to the voice processor in evenly spaced intervals. Jitter is variations in packet arrival time, can occur because of network congestion, timing drift or route changes. The jitter buffer, which is located at the receiving end of the voice connection, intentionally delays the arriving packets so that the end user experiences a clear connection with very little sound distortion. IP phones support two types of jitter buffers: static and dynamic. A static jitter buffer adds the fixed delay to voice packets. You can configure the delay time for the static jitter buffer on IP phones. A dynamic jitter buffer is capable of adapting the changes in the network's delay. The range of the delay time for the dynamic jitter buffer added to packets can be also configured on IP phones.

Procedure

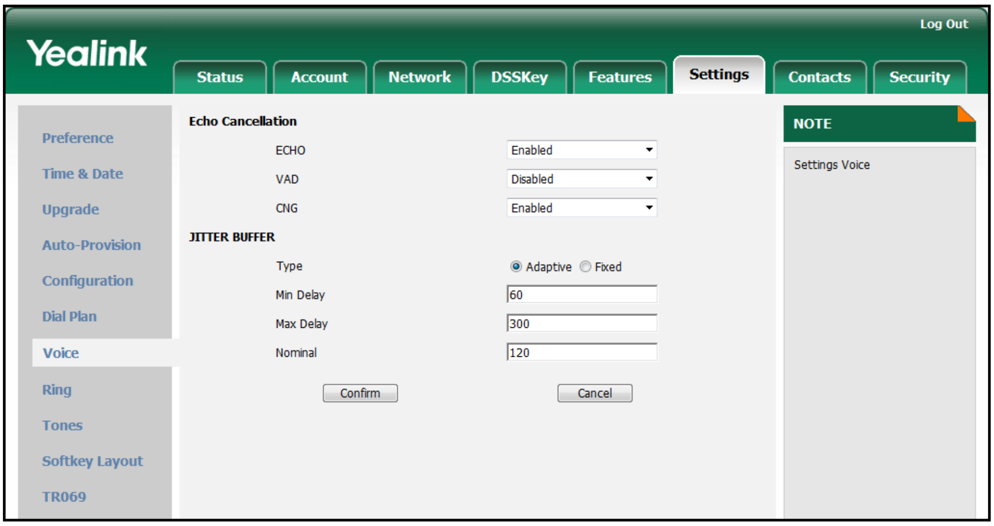
Jitter buffer can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Configure the mode of jitter buffer and the delay time for jitter buffer. For more information, refer to Jitter Buffer on page 338.
Local	Web User Interface	Configure the mode of jitter buffer and the delay time for jitter buffer. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-voice&q=load

To configure Jitter Buffer via web user interface:

1. Click on **Settings**->**Voice**.
2. Mark the desired radio box in the **Type** field.
3. Enter the minimum delay time for adaptive jitter buffer in the **Min Delay** field.
4. Enter the maximum delay time for adaptive jitter buffer in the **Max Delay** field.

5. Enter the fixed delay time for fixed jitter buffer in the **Normal** field.



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

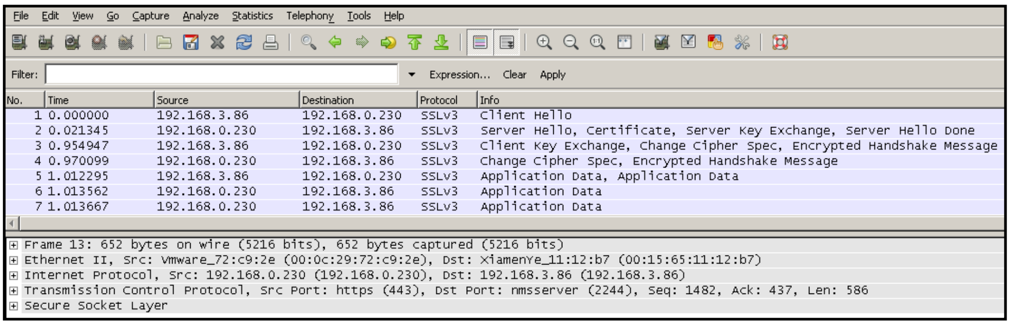
The TLS protocol is a commonly-used protocol for providing communications privacy and managing the security of message transmission. The TLS allows IP phones to communicate with other remote parties and connect to the HTTPS URL for provisioning in a way that is designed to prevent eavesdropping and tampering.

The TLS protocol is composed of two layers: the TLS Record Protocol and the 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 use asymmetric cryptography for authentication of key exchange, symmetric encryption for confidentiality, and message authentication codes for message 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 and the decryption key are the same one.
- **Asymmetric encryption**: For asymmetric encryption, you cannot tell the decryption key from the encryption key and vice versa. Each user has a pair of cryptographic keys – a public encryption key and a private decryption key. The information encrypted by the public key can only be decrypted by the corresponding private key and vice versa. Usually, the receiver keeps its private key. The public key is known by the sender, so the sender sends the information encrypted by the known public key, and then the receiver uses the private key to decrypt it.

The following figure illustrates the TLS messages exchanged between the IP phone and TLS server to establish an encrypted communication channel:



Step1: The IP phone sends "Client Hello" message proposing SSL options.

Step2: Server responds with "Server Hello" message selecting the SSL options, sends its public key information in "Server Key Exchange" message and concludes its part of the negotiation with "Server Hello Done" message.

Step3: The IP phone sends session key information (encrypted with server's public key) in the "Client Key Exchange" message.

Step4: Server sends "Change Cipher Spec" message to activate the negotiated options for all future messages it will send.

IP phones can encrypt SIP with TLS, which is called SIPS. When TLS is enabled for an account, the SIP message of this account will be encrypted, and a lock icon will appear on the phone LCD screen after the successful TLS negotiation.

Certificates

The certificates are used to the TLS negotiation. The digital certificate (also known as a public key certificate), is actually an electronic document that mainly contains a public key and identity information of the certificate owner. And there will be other information such as the unique serial number, the issuer, the validity date of the certificate. By verifying the information in the certificate, it can be told that whether the sender of the certificate is trustable. If no, there won't be further transmission. If yes, the receiver will use the public key in the certificate to go further.

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 the server is trusted based on the trusted certificates list. You can upload custom certificates to the IP phone. The IP phone supports upload 10 custom certificates at most. The format of the certificates must be *.pem,*.cer,*.crt and *.der.
- **Server Certificate**: When the other clients request a TLS connection with the IP phone, the IP phone sends the server certificate to the clients for authentication. The IP phone presets the unique phone certificate at the factory. You can only upload one server certificate to the IP phone. The unique phone certificate will be

not overwritten by the new one. The format of the certificates must be *.pem and *.cer.

You can specify the IP phone whether to authenticate the certificate sent by the connecting server 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 IP phone to accept the type of certificates: default certificates, custom certificates, or all certificates. Common Name Validation feature supports the IP phone to mandatory validate the common name of the CA certificates.

Procedure

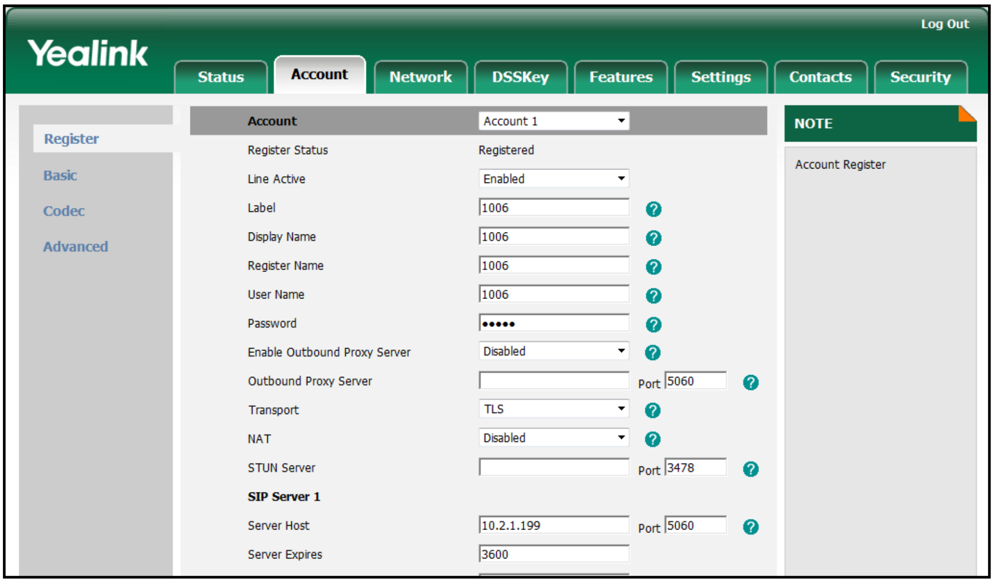
Configuration changes can be performed using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure TLS on a per-account basis. For more information, refer to TLS on page 339.
	<y000000000028>.cfg	Configure the trusted certificates feature. Configure the server certificates feature. For more information, refer to TLS on page 339. Upload the trusted certificates. Upload the server certificates. For more information, refer to Uploading Certificates on page 341.
Local	Web User Interface	Configure TLS on a per-account basis. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-register&q=load&acc=0Configure the trusted certificates feature. Upload the trusted certificates. **Navigate to**: http://<phoneIPAddress>/servlet?p=trusted-cert&q=load Configure the server certificates feature. Upload the server certificates.

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

To configure TLS on a per-account basis via web user interface:

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

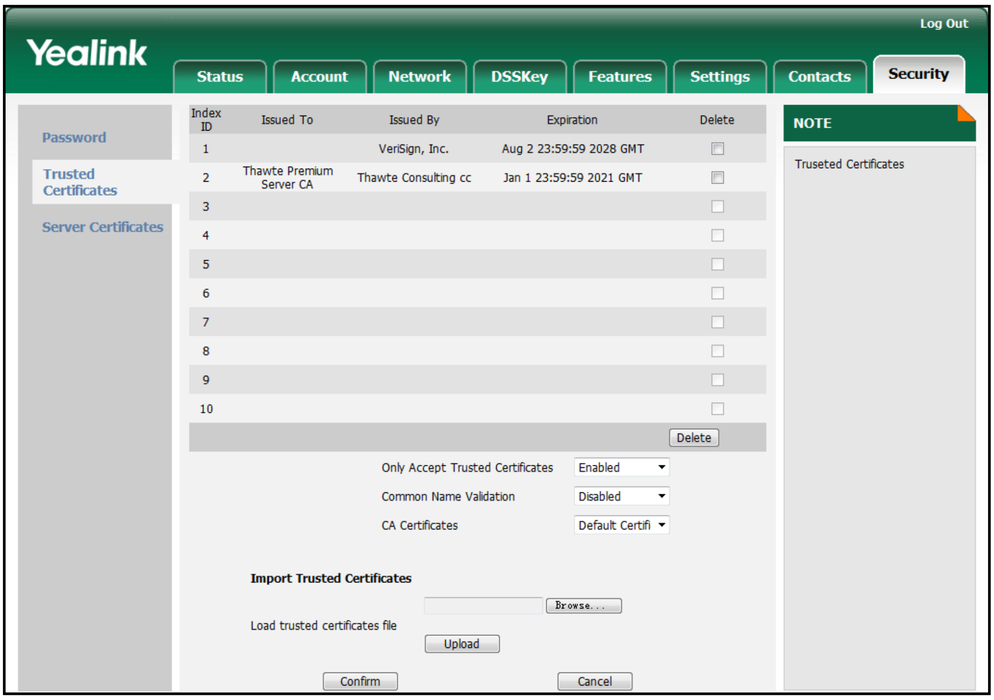


4. Click **Confirm** to accept the change.

To configure the trusted certificates feature via web user interface:

1. Click on **Security->Trusted Certificates**.
2. Select the desired value from the pull-down list of **Only Accept Trusted Certificates**.
3. Select the desired value from the pull-down list of **Common Name Validation**.

4. Select the desired value from the pull-down list of **CA Certificates**.



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

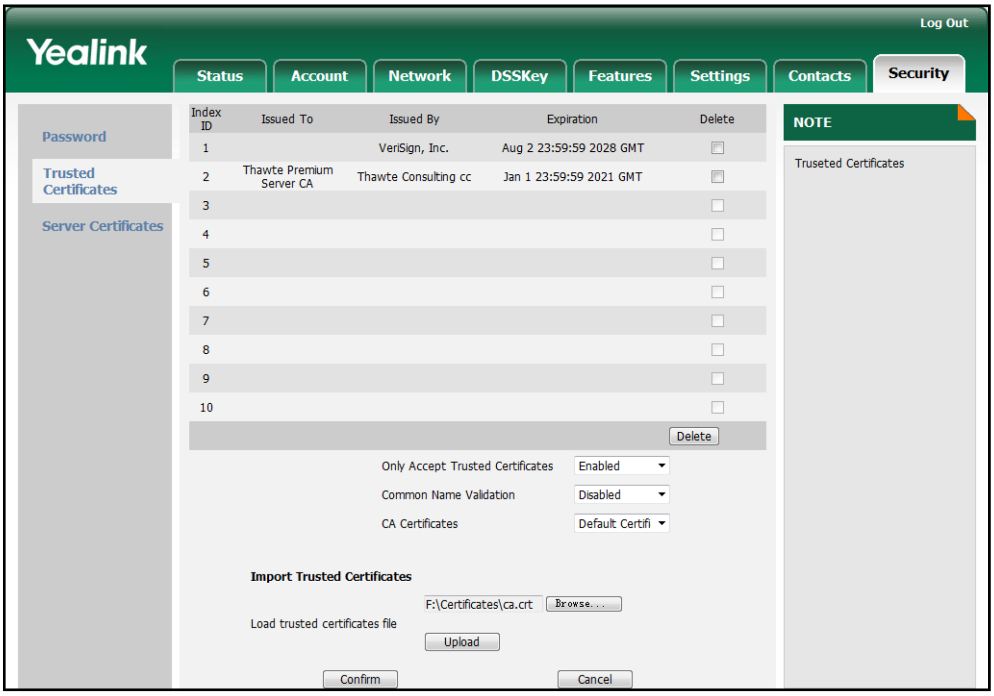
   A dialog box pops up to prompt that the settings will take effect after reboot.

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

To upload a trusted certificate via web user interface:

1. Click on **Security**->**Trusted Certificates**.

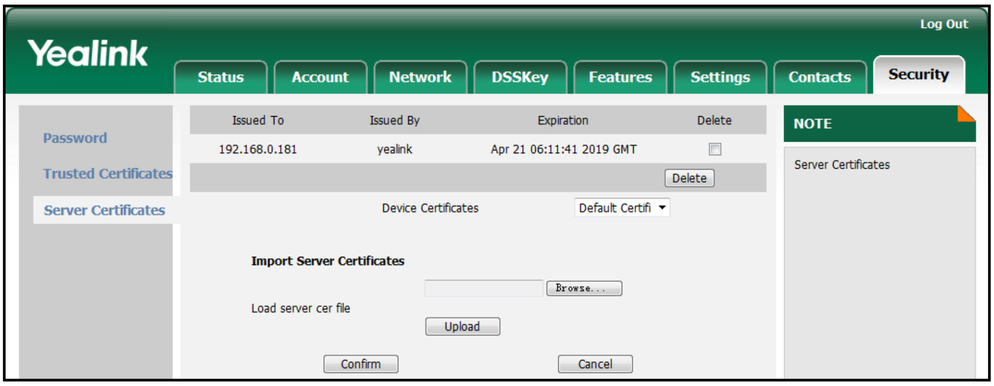
2. Click **Browse** to select the certificate (*.pem,*.crt, *.cer or *.der) from your local system.



3. Click **Upload** to upload the certificate.

To configure the server certificates feature via web user interface:

1. Click on **Security**->**Server Certificates**.
2. Select the desired value from the pull-down list of **Device Certificates**.



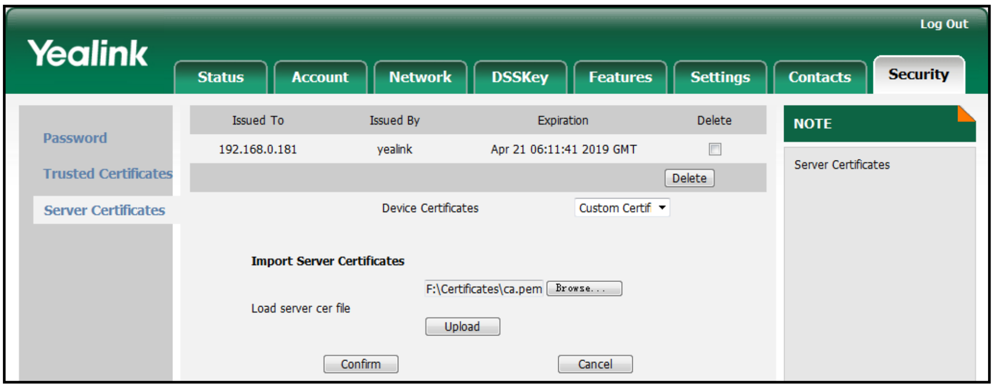
3. Click **Confirm** to accept the change.

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

To upload a server certificate via web user interface:

1. Click on **Security**->**Server Certificates**.

2. Click **Browse** to select the certificate (*.pem or *.cer) from your local system.



3. Click **Upload** to upload the certificate.

   The dialog box pops up to prompt "Success: The Server Certificate has been loaded! Rebooting, please wait…".

Secure Real-Time Transport Protocol

Secure Real-Time Transport Protocol (SRTP) provides means of encrypting the RTP streams during VoIP phone calls to avoid interception and eavesdropping. The parties participating in the call should enable the 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.

The example of the RTP encryption algorithm carried in the SDP of the INVITE message for reference:

```
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. The callee answers the call and responses with a 200 OK message carrying the negotiated RTP encryption algorithm.

The example of the RTP encryption algorithm carried in the SDP of the 200 OK message for reference:

```
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
```

You can configure the SRTP feature on a per-account basis. When SRTP is enabled on both IP phones, the RTP streams will be encrypted, and a lock icon appears on the LCD screen of each IP phone after the 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 193 .

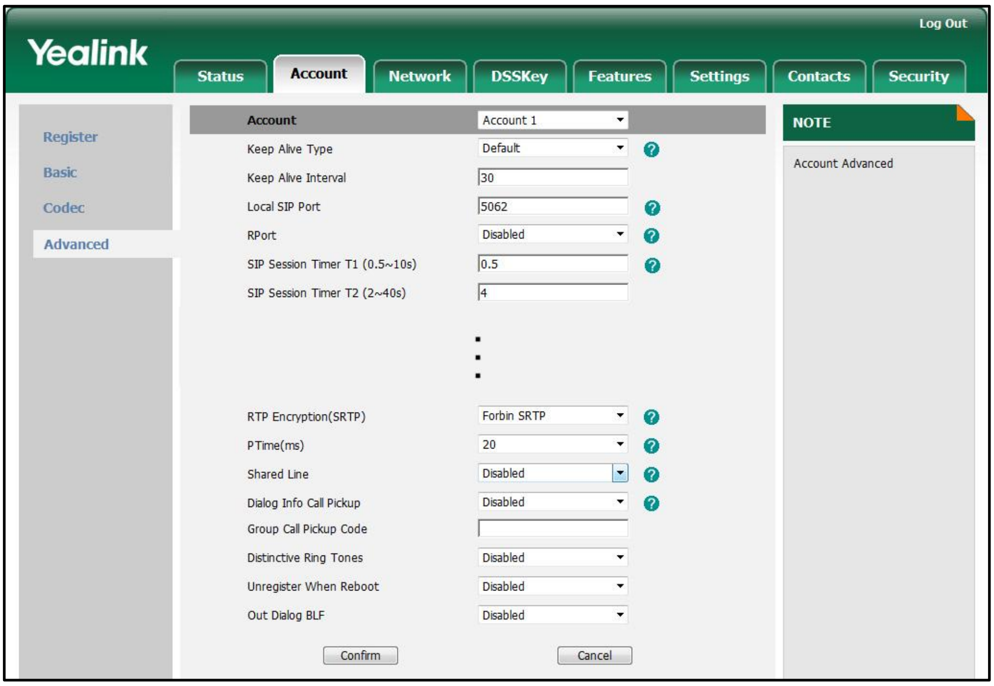
Procedure

SRTP can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure the SRTP feature on a per-account basis. For more information, refer to SRTP on page 342.
Local	Web User Interface	Configure the SRTP feature on a per-account basis. **Navigate to:** http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

To configure the 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. Click **Confirm** to accept the change.

Encrypting Configuration Files

The IP phone can download the encrypted configuration files from the provisioning server to protect against unauthorized access and tampering of sensitive information (i.e., login passwords, registration information). Configuration files can be encrypted using a command line tool. The encryption algorithm is AES 128. From a Microsoft Windows command line, you can use the Yealink-supplied encryption tool called "EncryptUtilityWindows.exe" to encrypt the <y000000000028>.cfg and <MAC>.cfg files respectively.

Note

Yealink also supplies an encryption tool (EncryptUtilityLinux.exe) to support Linux platforms if required.

You can also encrypt the configuration files using the Yealink Configuration Conversion Tool. For more information, refer to *Yealink Configuration Conversion Tool User Guide*.

The filename extension of the encrypted configuration files must be .cfg. The Common AES key is used to encrypt and decrypt the <y000000000028>.cfg file and the

MAC-Oriented AES key is used to encrypt and decrypt the <MAC>.cfg file. The AES keys must be 16 characters. The AES key should be configured on the IP phone for decrypting before provisioning.

Procedure to Encrypt Configuration Files

To encrypt the <y000000000028>.cfg file:

1. Place the “EncryptUtilityWindows.exe” tool and <y000000000028>.cfg file to the same directory (i.e., D:\).
2. Open a command line window application (i.e., DOS window).
3. Enter the following command, and then press the <Enter> key.

```
D:EncryptUtilityWindows.exe 123456789abcdef0 e F:\y000000000000.cfg
D:\y000000000000.cfg
```

```
#D:EncryptUtilityWindows.exe <a 16-character secret key> e <a new
directory and file name of the encrypted configuration file> <the
directory and file name of the original configuration file>
```

4. Place the encrypted configuration file to the root directory of the provisioning server.

The way for encrypting the <MAC>.cfg file is the same as the <y000000000028>.cfg file. After encrypting the configuration files, you need to configure the AES keys on the IP phone.

Procedure

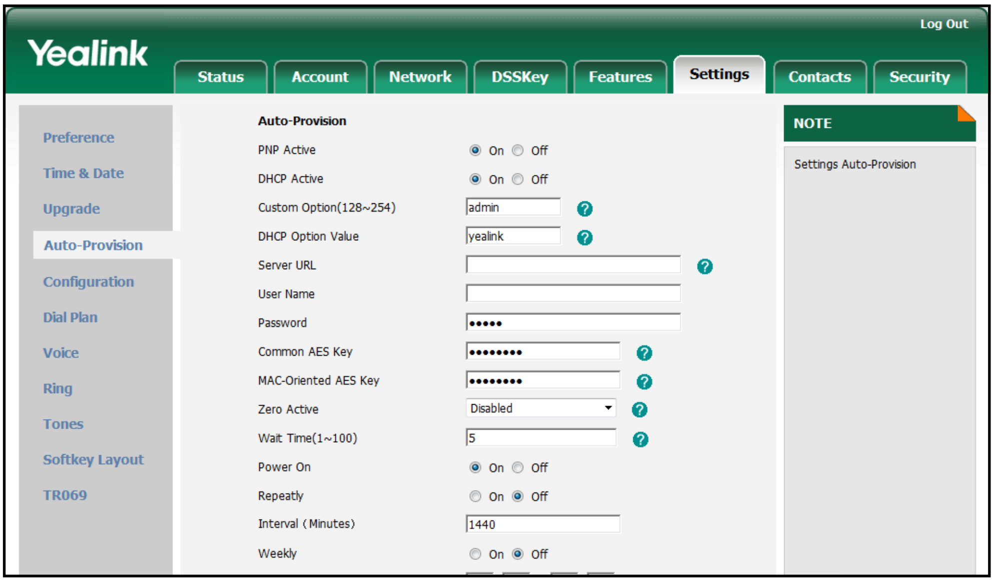
AES keys can be configured using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Configure the AES keys. For more information, refer to Configuring AES Keys on page 342.
Local	Web User Interface	Configure the AES keys. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-autop&q=load

To configure the AES keys via web user interface:

1. Click on **Settings**->**Auto-Provision**.

2. Enter the values in the **Common AES Key** and **MAC-Oriented AES Key** fields.



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

Upgrading the Firmware

This chapter provides information about upgrading the IP phone firmware. There are two methods used to upgrade the firmware on the IP phone:

- Upgrade the firmware manually from the local system
- Upgrade the firmware from the provisioning server automatically.

The associated firmware for SIP-T46G IP phone is 28.x.x.x.rom.

Note

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

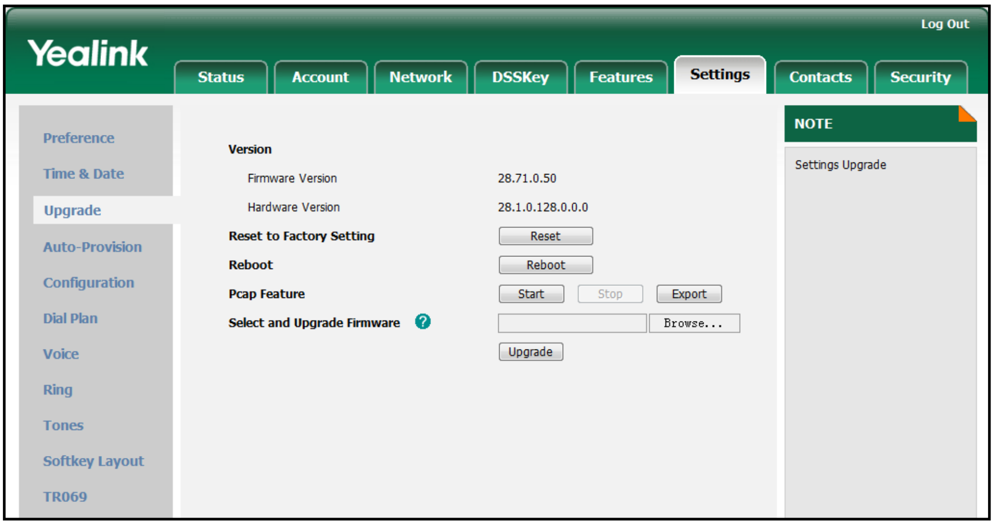
Upgrade via Web User Interface

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

To upgrade the firmware manually via web user interface:

1. Click on **Settings**->**Upgrade**.
2. Click **Browse**.
3. Select the firmware from the local system.
4. Click **Upgrade**.

The 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 upgrading.

Note

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

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

Upgrade Firmware from the Provisioning Server

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

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

- IP phones check for both configuration files and firmware stored on the provisioning server during booting up.
- IP phones automatically check for configuration files and firmware at a fixed interval or at specific time.

You can configure the way for IP phones to check for configuration files and firmware.

Procedure

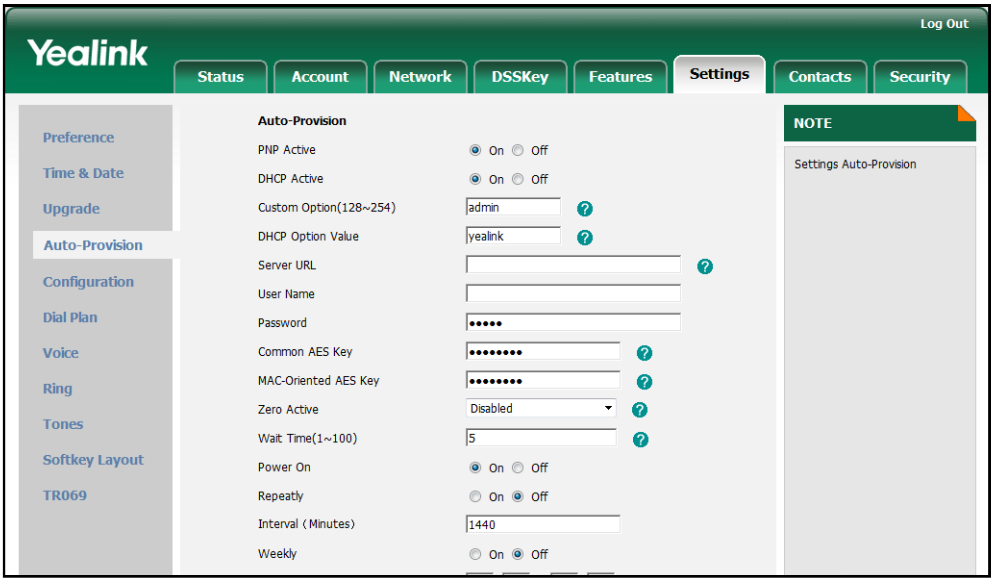
Configuration changes can be performed using the configuration files or locally.

Configuration File	<y000000000028>.cfg	Configure the way for the IP phone to check for configuration files. Specify the access URL of the firmware. For more information, refer to Upgrading the Firmware on page 343.
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

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

1. Click on **Settings->Auto-Provision**.

2. Mark the desired radio box in the **Power On** field.



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

When the "Power On" is set to **On**, the IP phone will check for both firmware and configuration files stored on the provisioning server during booting up.

Resource Files

When configuring some features, you may need to upload resource files to the IP phone. The resources files can be local contact directory, remote phonebook and so on. Ask the Yealink field application engineer for the resource file templates. If the resource file is to be used for all IP phones of the same model, the access URL of the resource file is best specified in the <y000000000028>.cfg file. However, if you want to specify the desired phone to use the resource file, the access URL of the resource file should be specified in the <MAC>.cfg file.

This chapter provides the detailed information on how to customize the following resource files and specify the access URL:

- Replace Rule Template
- Dial-now Template
- Softkey Layout Template
- Local Contact File
- Remote XML Phonebook
- Specifying the Access URL of Resource Files

Replace Rule Template

You can create multiple replace rules using the replace rule template. After preparing the replace rule template, you need to place the replace rule template to the root directory of the provisioning server and specify the access URL in the configuration files.

When editing a replace rule template, remember 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 IDs. The digit 0 stands for all lines, multiple line IDs are separated by comma.
- At most 20 replace rules can be added to the IP phone.
- The expression syntax in the replace rule template is the same as introduced in the section Creating Dial Plan on page 23.

Procedure

Use the following procedures to customize a replace rule template.

Customizing a replace rule template:

1. Open the template file using an ASCII editor.
2. Add the following string to the template, each starting on a separate line:

   <Data Prefix="" Replace="" LineID=""/>

   Where:

   Prefix="" specifies the numbers to be replaced.

   Replace="" specifies the alternate string instead of what the user enters.

   LineID="" specifies the desired line(s) for this rule. When leaving it blank, this replace rule will apply to all lines.
3. Specify the values within double quotes.
4. Place this file to the root directory of the provisioning server.

The following is 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

You can create multiple dial-now rules using the dial-now template. After preparing the dial-now template, you need to place the dial-now template to the root directory of the provisioning server and specify the access URL in the configuration files.

When editing a dial-now template, remember 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 comma.
- At most 20 rules can be added to the IP phone.
- The expression syntax in the dial-now rule template is the same as introduced in the section Creating Dial Plan on page 23.

Procedure

Use the following procedures to customize a dial-now template.

Customizing a dial-now template:

1. Open the template file using an ASCII editor.
2. Add the following string to the template, each starting on a separate line:

   <Data DialNowRule="" LineID=""/>

   Where:

   DialNowRule="" specifies the dial-now rule.

   LineID="" specifies the desired line(s) for this rule. When leaving it blank, the IP phone will apply to all lines.
3. Specify the values within double quotes.
4. Place this file to the root directory of the provisioning server.

The following is an example of a dial-now template:

```
<DialNow>
  <Data DialNowRule="1234" LineID="1"/>
  <Data DialNowRule="52[0-6]" LineID="1"/>
  <Data DialNowRule="xxxxxx" LineID=""/>
</DialNow>
```

Softkey Layout Template

You can create the softkey layout of different call states respectively using the softkey layout templates. The call states are CallFailed, CallIn, Connecting, Dialing, RingBack and Talking. After preparing the templates, place the templates to the root directory of the provisioning server and specify the access URL in the configuration files.

When editing a softkey layout template, remember 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 phone LCD screen.
- Create the 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 phone LCD screen.
- Create the 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 phone LCD screen by default.

Procedure

Use the following procedures to customize a softkey layout template.

Customizing a softkey layout template:

1. Open the template file using an ASCII editor.
2. For each soft key that you want to enable, add the following string to the file. Each starts on a separate line:

   <Key Type=""/>

   Where:

   Key Type="" specifies the enabled soft key (This value cannot be blank).

   For each disabled soft key and each default soft key that you want to add, add the same string introduced above.
3. Specify the values within double quotes.
4. Place this file to the root directory of the provisioning server.

The following is 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>
```

Local Contact File

You can add contacts one by one on the IP phone directly. In some cases, you may want to add multiple contacts to the IP phone at the same time or share the contacts on many IP phones. You can create a local contact file, and then place the local contact file to the root directory of the provisioning server, specify the access URL of the contact file in the configuration files.

When editing a local contact file, remember 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 the contact or the group, the format of the value must be Auto, Resource:RingN.wav (for the default system ring tone) or Custom:Name.wav (for the customized ring tone).
- When specifying the desired line for the contact, the valid values are 0 and line ID, 0 stands for all lines, multiple line IDs are separated by comma.

Procedure

Use the following procedures to customize a local contact file.

Customizing a local contact file:

1. Open the template file using an ASCII editor.
2. For each contact that you want to add, add the following string to the file. Each starts on a separate line:

   <contact display_name="" office_number="" mobile_number="" other_number="" line="" ring="" group_id_name="" default_photo="" />

   Where:

   display_name="" specifies the name of the contact (This value cannot be blank or duplicated).

   office_number ="" specifies the office number of the contact.

   mobile_number="" specifies the mobile number of the contact.

   other_number="" specifies the other number of the contact.

   line="" specifies the line you want to add this contact to.

   ring="" specifies the ring tone for this contact.

   group_id_name="" specifies the existing group you want to add the contact to.

   default_photo="" specifies the photo for this contact.
3. 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.

4. Specify the values within double quotes.
5. Place this file to the root directory of the provisioning server.

The following is an example of a local contact file:

```
<root_contact>
  <contact display_name="John" office_number="1001"
  mobile_number="12345678910" other_number="" line="0" ring="Auto"
  group_id_name="All Contacts" default_photo=""/>
  <contact display_name="Alice" office_number="1002" mobile_number=""
  other_number="" line="2" ring="Resource:Ring2.wav"
  group_id_name="Friend" default_photo=""/>
</root_contact>
<root_group>
  <group display_name="Friend" ring=""/>
  <group display_name="Family" ring="Resource:Ring1.wav"/>
</root_group>
```

Remote XML Phonebook

The IP phone can access 5 remote phonebooks. You can customize the remote XML phonebook for the IP phone as required. Before specifying the access URL of the remote phonebook in the configuration files, you need to create a remote XML phonebook and then place it to the provisioning server.

When creating an XML phonebook, remember the following:

- <YealinkIPPhoneDirectory> indicates the start of a phonebook and </YealinkIPPhoneDirectory> indicates the end of a phonebook.
- <DirectoryEntry> indicates the start of a contact and </DirectoryEntry> indicates the end of a contact.

Procedure

Use the following procedures to customize an XML phonebook.

Customizing an XML phonebook:

1. Open the template file using an ASCII editor.
2. For each contact that you want to add, add the following strings to the IP phonebook. Each starts on a separate line:

<Name>*Mary*</Name>

<Telephone>*1001*</Telephone>

Where:

Specify the contact name between <Name> and </Name>.

Specify the contact number between <Telephone> and </Telephone>.

3. Specify the values within double quotes.
4. Place this file to the root directory of the provisioning server.

The following is an example of an XML phonebook:

```
<YealinkIPPhoneDirectory>
     <DirectoryEntry>
         <Name>Jack</Name>
         <Telephone>1003</Telephone>
     </DirectoryEntry>
     <DirectoryEntry>
         <Name>John</Name>
         <Telephone>1004</Telephone>
     </DirectoryEntry>
     <DirectoryEntry>
         <Name>Marry</Name>
         <Telephone>1005</Telephone>
     </DirectoryEntry>
</YealinkIPPhoneDirectory>
```

Specifying the Access URL of Resource Files

Access URL of the resource file can be configured in the configuration files:

Configuration File	<y000000000028>.cfg	Configure the access URL of the replace rule template. For more information, refer to Access URL of Replace Rule Template on page 345.
Configuration File	<y000000000028>.cfg	Configure the access URL of the dial-now rule template. For more information, refer to Access URL of Dial-now Template on page 346.

Configuration File	<y000000000028>.cfg	Configure the access URL of the softkey layout template. For more information, refer to Access URL of Softkey Layout Template on page 346.
Configuration File	<y000000000028>.cfg	Configure the access URL of the local contact file. For more information, refer to Access URL of Local Contact File on page 349.
Configuration File	<y000000000028>.cfg	Configure the access URL of the remote XML phonebook. For more information, refer to Access URL of Remote XML Phonebook on page 349.

Troubleshooting

This chapter provides an administrator with general information for troubleshooting some common problems that may encounter while using the SIP-T46G IP phone.

Troubleshooting Methods

The IP phone can provide feedback in a variety of forms such as log files, packets, status indicators and so on, which helps an administrator quickly find out the reasons for the failure and do the troubleshooting more easily.

The following are some methods for you to learn more about the working status of your IP phone and quickly find out the reasons for the failure.

- Viewing Log Files
- Capturing Packets
- Enabling the Watch Dog Feature
- Getting Information from Status Indicators
- Analyzing Configuration Files

Viewing Log Files

The IP phone can log various events to log files. So if your IP phone encounters some problems, commonly the log files are used. You can export the log files to a syslog server or the local system. You can specify the location for which to save log files for troubleshooting purposes using the configuration files or the web user interface. You can also set the system log level to specify the severity level of the logs to be reported to a log file. The system log level is 6 by default.

In the configuration files, you can use the following parameters to configure log settings:

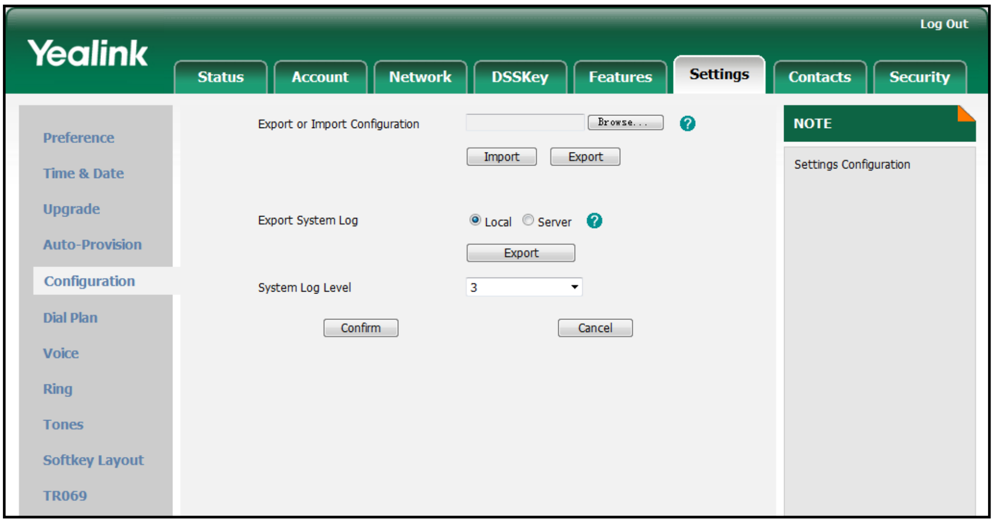
- **syslog.server** -- Specify the IP address of the syslog server where to export the log files.
- **syslog.log_level** -- Specify the severity level of the logs to be reported to a log file (Changes to this parameter via web user interface require a reboot).

For more information on the log setting configuration parameters, refer to Log Settings on page 350.

To configure the level of the log files via web user interface:

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

2. Select the desired level from the pull-down list of **System Log Level**.



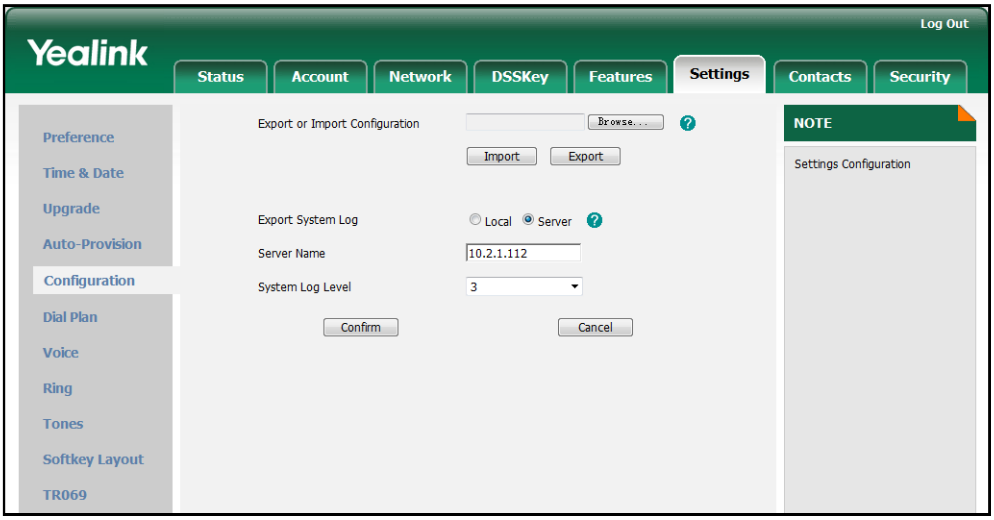
3. Click **Confirm** to accept the change.

   A dialog box pops up to prompt "Do you want to restart your machine?"

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

To export log files to a syslog server via web user interface:

1. Click on **Settings**->**Configuration**.
2. In the **Export System Log** block, mark the **Server** radio box.
3. Enter the address of the syslog server in the **Server Name** field.

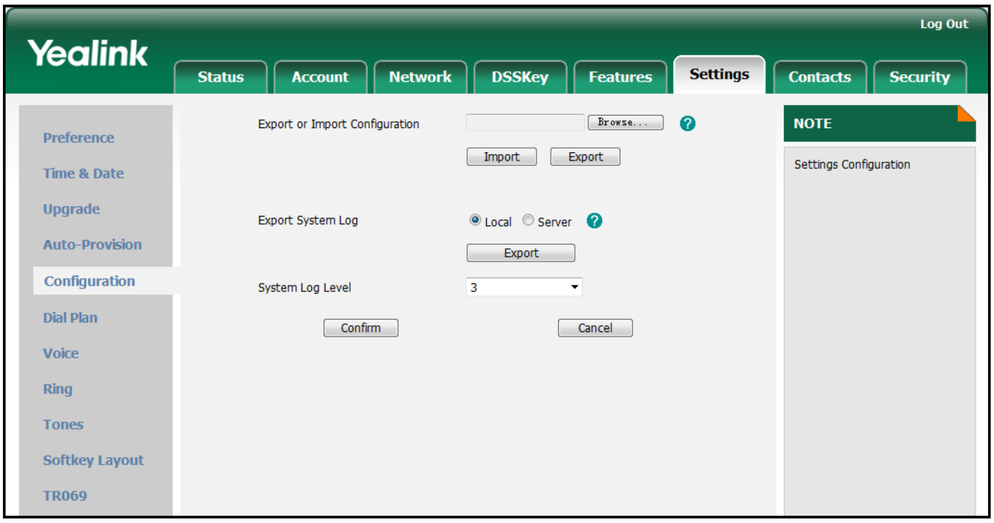


4. Click **Confirm** to accept the change.

To export log files to the local system via web user interface:

1. Click on **Settings**->**Configuration**.
2. In the **Export System Log** block, mark the **Local** radio box.
3. 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:

```
 190 root      2856 S    /bin/sh /boot/script/netapp.sh
 197 root     22484 S    /boot/bin/rtServer.exx
 210 root      2856 S    /usr/sbin/telnetd
 211 root     17448 S    /boot/bin/autoServer.exx
 249 root      3440 S    ./sbin/lighttpd -f /phone/bin/lighttpd/config/lighttp
 252 root     18924 S    /phone/www/WEB-INFO/bin/fcgiServer.exx
 263 root      2856 S    /sbin/syslogd -S -O /tmp/log/000000000000.log -s 200
 275 root      2856 S    /bin/sh /phone/scripts/phoneapp.sh
 276 root      6092 S    ./pcap.exx
 291 root      140m S    /phone/bin/dskPhone.exx -qws
 300 root         0 SW<  [ethTx/0]
 301 root         0 SW<  [ethStatus/0]
 309 root      5060 S    /boot/bin/lldpd
 310 root      5572 S    /boot/bin/lldpd
 357 root         0 DW   [hwthread]
 358 root         0 DW   [hausioctl]
 359 root         0 SW<  [frameProfiler]
 360 root         0 DW<  [Cadence]
 369 root     14016 S    /phone/bin/vaServer -q -w -m ANY=5
 388 root      2920 S    /phone/bin/snmpd -c /etc/snmpd.conf
 389 root      2856 S    /bin/sh /phone/scripts/sipapp.sh
 396 root     41396 S N  /phone/bin/sipServer.exx
 415 root      1628 S    /phone/bin/busybox udhcpc -b -i eth0 -a -s /boot/bin/
 487 root      2856 S    sh -c cd /tmp;ifconfig >> log/000000000000.log;ps >>
 489 root      3180 R    ps
Mar 12 03:32:58 fcgiServer.exx: HttpResponseImpl::write() Begin. size= 1;count=1024
Mar 12 03:32:58 fcgiServer.exx: HttpResponseImpl::commitHeader() Begin
Mar 12 03:32:58 fcgiServer.exx: HttpResponseImpl::commitHeader() End2
Mar 12 03:32:58 fcgiServer.exx: HttpResponseImpl::write() End.write 1024 bytes
Mar 12 03:32:58 fcgiServer.exx: HttpResponseImpl::write() Begin. size= 1;count=1024
Mar 12 03:32:58 fcgiServer.exx: HttpResponseImpl::commitHeader() Begin
Mar 12 03:32:58 fcgiServer.exx: HttpResponseImpl::commitHeader() End
```

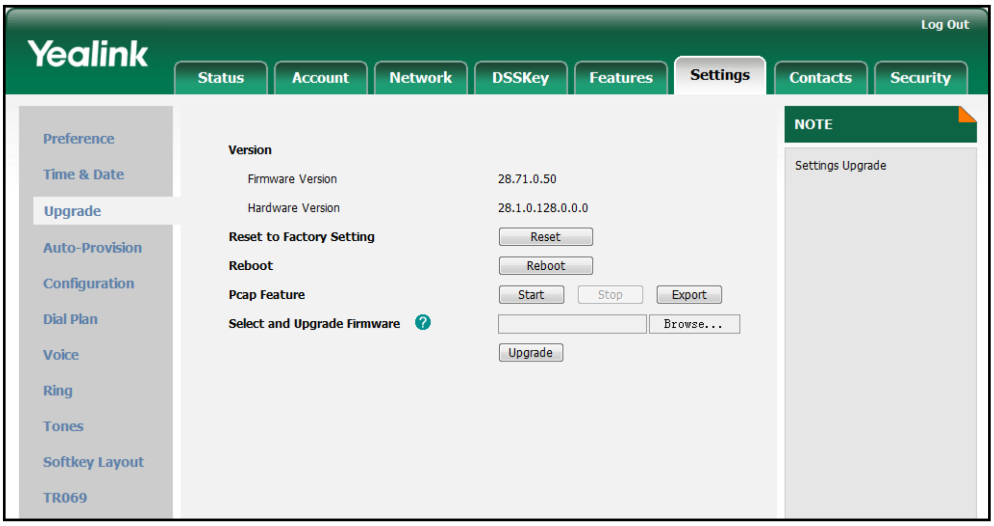
Capturing Packets

You can capture packets in two ways: capturing the packets via web user interface or using the Ethernet software. You can analyze the packets captured for troubleshooting purposes.

To capture packets via web user interface:

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

2. Click **Start** to begin capturing signal traffic.
3. Reproduce the issue to get stack traces.
4. Click **Stop** to end capturing.
5. Click **Export** to open file download window, and then save the file to your local system.



To capture packets using the Ethernet software:

Connect the IP phone's Internet port with the PC to the same HUB, and then use Sniffer, Ethereal or Wireshark software to capture the packets. You can also set a mirror port in the switch to monitor the port of the connected IP phone.

Enabling the Watch Dog Feature

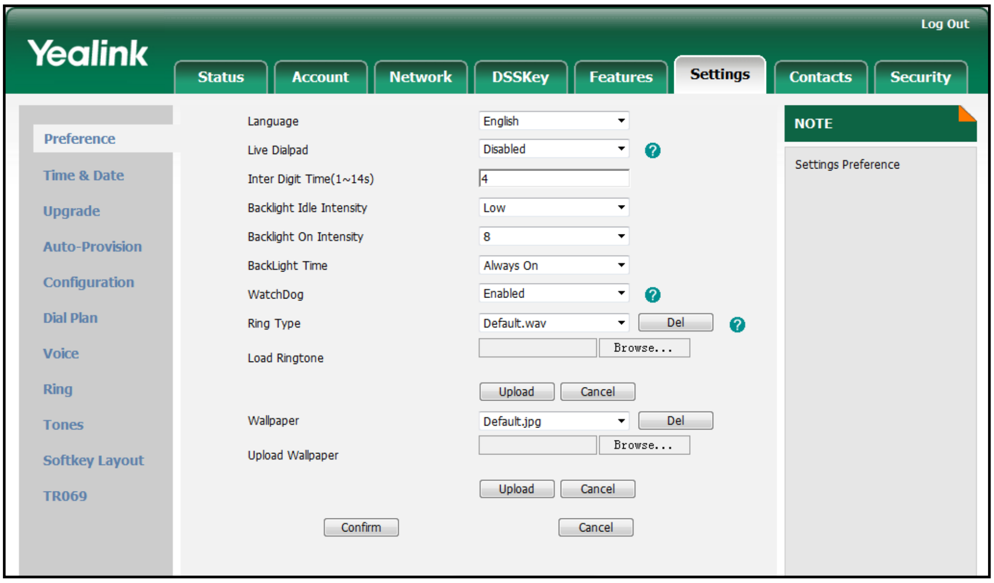
The IP phones support a troubleshooting feature called Watch Dog, which help you monitor the IP phones status and provide the ability to automatically reboot. When the Watch Dog feature is enabled, the IP phones will automatically reboot when it detects a fatal failure. This feature can be configured using the configuration files or the web user interface.

You can use the "watch_dog.enable" parameter to configure the Watch Dog feature in the configuration files. For more information, refer to Watch Dog on page 351.

To configure the Watch Dog feature via web user interface:

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

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



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

Getting Information from Status Indicators

Status indicators may consist of the power LED, message key indicator, line key indicator, headset key indicator and the on-screen icon or error messages.

The following are two examples of getting the phone information from status indicators:

- If a LINK failure of the IP phone is detected, a prompting message "Network Unavailable" and the icon  indicate the current network LINK status.
- If the power LED is off, the IP phone is powered off.

For more information on the icons, refer to Reading Icons on page 13.

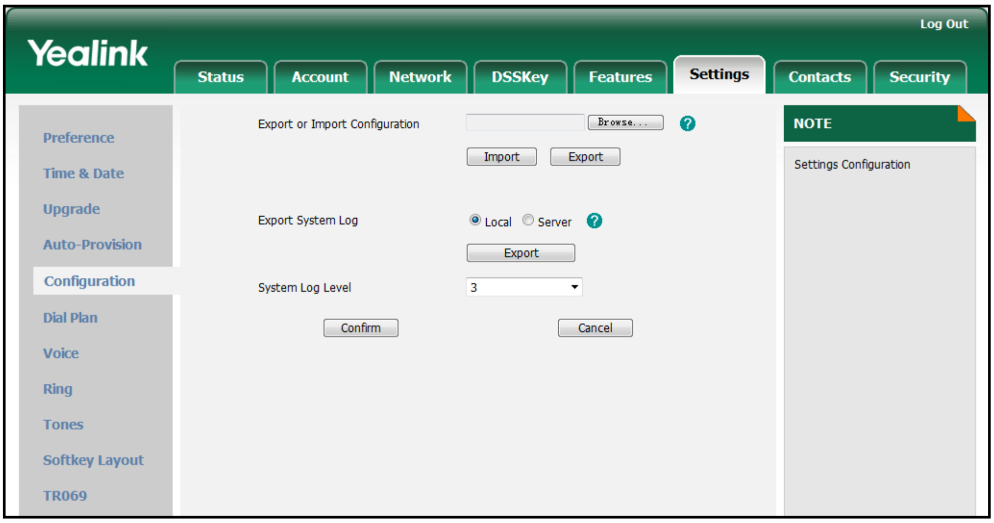
Analyzing Configuration Files

Using the wrong parameters may have an impact on your phone performance. You can export configuration files to check the current configuration of the IP phone and troubleshoot as necessary.

To export 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.



Troubleshooting Solutions

This section describes solutions to some common scenarios that may occur while using the IP phone. If you encounter a scenario which is not listed in this section, contact your Yealink reseller for further support.

Why is the phone LCD screen blank?

Do one of the following:

- Check that the power LED is on to ensure the IP phone is powered on.
- Ensure the IP phone is properly plugged into a functional AC outlet.
- Ensure that the IP phone isn't plugged into a plug controlled by a switch that is off.
- If the IP phone is plugged into a power strip, try plugging it directly into a wall outlet instead.
- If your phone is powered from PoE, ensure you use a PoE compliant switch or hub.

Why does the IP phone not 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 the Ethernet cable is not damaged.
- Ensure the IP address and other network parameters are set correctly.

- Ensure that the switch or hub in your network is operational.

How do I find the basic information of the IP phone?

Press the OK key when the IP phone is idle to check the basic information of the IP phone, such as IP address and firmware version.

Why does the IP phone not upgrade the firmware successfully?

Do one of the following:

- Ensure that the target firmware is not the same as the current used 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 the web browser is not closed and refreshed when upgrading the firmware using the web user interface.

Why does the IP phone not display time and date correctly?

Check if you have configured your phone 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 audio during a call?

During a call, you may experience poor audio, including intermittent voice, low volume, echo or other noise. Possibilities are as following:

- Problems may occur simply because the users are seated too far out of recommended microphone range and sound faint, or are seated too close to sensitive microphones and cause feedback.
- Intermittent voice is mainly caused by packet loss and jitter. Packet loss may be due to network congestion. Jitter is mainly due to message recombination of transmission or receiving equipment, such as timeout handling, retransmission mechanism or buffer under run.
- Noisy equipment, such as a computer or a fan, may make it difficult for hear the voice from the other party clearly. Turn off any noisy equipment in the room such as fans.
- A line issue may also cause this problem. Disconnect the old line and redial the call

to see if another line provides better connection.

What is the difference between a remote phonebook and a local phonebook?

A remote phonebook is placed on a server, while a local phonebook is placed on the IP phone flash. A remote phonebook can be used by everyone that can access the server, while a local phonebook can only be used by a specific phone itself. A remote phonebook is always used as a central phonebook for a company. That is, every staff in the company can load this phonebook and each time they are trying to open a remote phonebook, the data is passed real-time from the certain server.

What is the difference between user name, register name and display name?

Both user name and register name are defined by the server. A user name is used to identify the account while a register name matched with a password is used for authentication if the server requires. Display name is the caller ID that will be displayed on the callee's phone LCD screen. Some server configuration may override the local configuration.

Is there a SIP message that can make the IP phone reboot?

Yes. The IP phone will reboot only if the header in a SIP NOTIFY message contains an additional string "reboot=true". The 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
```

What can I do if I forget the administrator password?

A factory reset can restore the original password. Please try to long press the OK key when the IP phone is idle, which should lead you to make a factory reset.

How to increase the volume on Speaker & on Headset?

The volumes in different cases are separated. You can use the volume key under the navigation keys to increase or decrease the voice volume. You can press the volume key to adjust the ringer volume when the phone is idle. You can also press the volume key to adjust the receiver volume of currently used audio devices (handset, speakerphone or headset), when the phone is in the dialing interface or during a call.

What is auto provisioning?

Auto provisioning is a term referring to the update of the IP phones, including updates on most of the configuration parameters, local phonebook, firmware and so on. You can use auto provisioning on a single phone, but it makes more sense in mass updates.

What is PnP?

Plug and Play (PnP) is a method for the IP phones to get the provisioning server address. If the IP phone is PnP enabled, it broadcasts the PNP subscribe message to obtain a provisioning server address during booting up. 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 that server address. PNP depends on support from a SIP server.

Why does the IP phone not apply the configuration?

Do one of the following:

- Ensure the configuration is set correctly.
- Reboot the IP phone. Some configurations require a reboot to take effect.
- Ensure the configuration is applicable to the IP phone model when configuring IP phones with configuration files.
- The configuration may depend on support from the server.

What do “on code” and “off code” mean?

They are codes that the IP phone will send to the server when there’s a certain action. 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.

Take the on code for Always Forward for example, if you set the Always Forward on code to be *78 (the code 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 simultaneously. Then the server configures the Always Forward feature as configured on the phone side. Hence, the server is able to get the right status of the extension.

How to solve the IP conflict problem?

Do one of the following:

- Try to set another available IP address for the IP phone.
- Check the configuration of the network via phone user interface at the path **Menu**->**Advanced**->**Network**->**WAN Port**. If Static IP Client is selected, select DHCP IP Client instead.

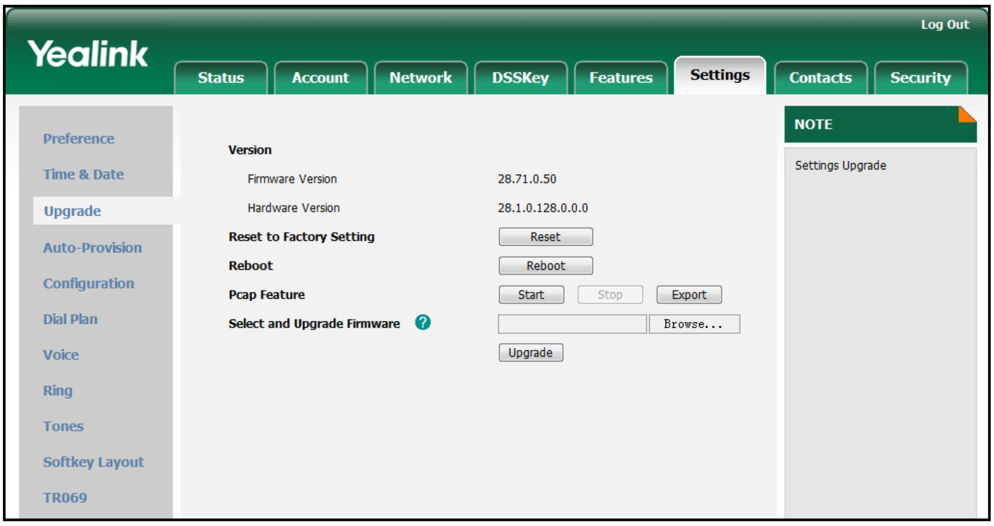
How to reset your phone to factory configurations?

Reset your phone to factory configurations after you have tried almost all troubleshooting suggestions but do not resolve the problem. You need to note that all customized settings will be overwritten after resetting. Do not power off until the phone starts up successfully.

To reset your phone via web user interface:

1. Click on **Settings**->**Upgrade**.
2. Click **Reset** in the **Reset to Factory Settings** field.

   The web user interface prompts the message "Do you want to reset to factory?".



3. Click **OK** to confirm the resetting.

   The phone will be reset to factory sucessfully after startup.

Note Reset of the phone may take a few minutes. Do not power off until the phone starts up successfully.

Appendix

Appendix A: Glossary

802.1x — an IEEE Standard for port-based Network Access Control (PNAC). It is 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.

ACD (Automatic Call Distribution) — used to distribute calls from large volumes of incoming calls to the registered IP phone users.

ACS (Auto Configuration server) — responsible for auto-configuration of the Central Processing Element (CPE).

Cryptographic Key — a piece of variable data that is fed as input into a cryptographic algorithm to perform operations such as encryption and decryption, or signing and verification.

DHCP (Dynamic Host Configuration Protocol) — built on a client-server model, where designated DHCP server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts.

DHCP Option — can be configured for specific values and enabled for assignment and distribution to DHCP clients based on server, scope, class or client-specific levels.

DNS (Domain Name System) — a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network.

EAP-MD5 (Extensible Authentication Protocol-Message Digest Algorithm 5) — only provides authentication of the EAP peer to the EAP server but not mutual authentication.

EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) — Provides for mutual authentication, integrity-protected cipher suite negotiation between two endpoints.

PEAP-MSCHAPV2 (Protected Extensible Authentication Protocol-Microsoft Challenge Handshake Authentication Protocol Version 2) — Provides for mutual authentication, but does not require a client certificate on the IP phone.

FAC (Feature Access Code) — special patterns of characters that are dialed from a phone keypad to invoke particular features.

HTTP (Hypertext Transfer Protocol) — used to request and transmit data on the World Wide Web.

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) — a widely-used communications protocol for secure communication over a network.

IEEE (Institute of Electrical and Electronics Engineers) — a non-profit professional association headquartered in New York City that is dedicated to advancing technological innovation and excellence.

LAN (Local Area Network) — used to interconnects network devices in a limited area such as a home, school, computer laboratory, or office building.

MIB (Management Information Base) — a virtual database used for managing the entities in a communications network.

OID (Object Identifier) — assigned to an individual object within a MIB.

PNP (Plug and Play) — a term used to describe the characteristic of a computer bus, or device specification, which facilitates the discovery of a hardware component in a system, without the need for physical device configuration, or user intervention in resolving resource conflicts.

ROM (Read-only Memory) — a class of storage medium used in computers and other electronic devices.

RTP (Real-time Transport Protocol) — provides end-to-end service for real-time data.

TCP (Transmission Control Protocol) — a transport layer protocol used by applications that require guaranteed delivery.

UDP (User Datagram Protocol) — a protocol offers non-guaranteed datagram delivery.

URI (Uniform Resource Identifier) — a compact sequence of characters that identifies an abstract or physical resource.

URL (Uniform Resource Locator) — specifies the address of an Internet resource.

VLAN (Virtual LAN) -- a group of hosts with a common set of requirements, which communicate as if they were attached to the same broadcast domain, regardless of their physical location.

VoIP (Voice over Internet Protocol) — a family of technologies used for the delivery of voice communications and multimedia sessions over IP networks.

WLAN (Wireless Local Area Network) — a type of local area network that uses high-frequency radio waves rather than wires to communicate between nodes.

XML-RPC (Remote Procedure Call Protocol) — which uses XML to encode its calls and HTTP as a transport mechanism.

Appendix B: Time Zones

Time Zone	Time Zone Name
–11:00	Samoa
–10:00	United States-Hawaii-Aleutian
–10:00	United States-Alaska-Aleutian
–09:00	United States-Alaska Time
–08:00	Canada(Vancouver, Whitehorse)
–08:00	Mexico(Tijuana, Mexicali)
–08:00	United States-Pacific Time
–07:00	Canada(Edmonton, Calgary)
–07:00	Mexico(Mazatlan, Chihuahua)
–07:00	United States-Mountain Time
–07:00	United States-MST no DST
–06:00	Canada-Manitoba(Winnipeg)
–06:00	Chile(Easter Islands)
–06:00	Mexico(Mexico City, Acapulco)
–06:00	United States-Central Time
–05:00	Bahamas(Nassau)
–05:00	Canada(Montreal, Ottawa, Quebec)
–05:00	Cuba(Havana)
–05:00	United States-Eastern Time
–04:30	Venezuela(Caracas)
–04:00	Canada(Halifax, Saint John)
–04:00	Chile(Santiago)
–04:00	Paraguay(Asuncion)
–04:00	United Kingdom-Bermuda(Bermuda)
–04:00	United Kingdom(Falkland Islands)
–04:00	Trinidad&Tobago
–03:30	Canada- New Foundland(St.Johns)
–03:00	Denmark-Greenland(Nuuk)
–03:00	Argentina(Buenos Aires)
–03:00	Brazil(no DST)
–03:00	Brazil(DST)
–02:00	Brazil(no DST)
–01:00	Portugal(Azores)
0	GMT
0	Greenland
0	Denmark-Faroe Islands(Torshavn)
0	Ireland(Dublin)
0	Portugal(Lisboa, Porto, Funchal)
0	Spain-Canary Islands(Las Palmas)

Time Zone	Time Zone Name
0	United Kingdom(London)
0	Morocco
+01:00	Albania(Tirane)
+01:00	Austria(Vienna)
+01:00	Belgium(Brussels)
+01:00	Caicos
+01:00	Chad
+01:00	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)
+02:00	Syria(Damascus)
+03:00	East Africa Time
+03:00	Iraq(Baghdad)
+03:00	Russia(Moscow)
+03:30	Iran(Teheran)
+04:00	Armenia(Yerevan)
+04:00	Azerbaijan(Baku)
+04:00	Georgia(Tbilisi)
+04:00	Kazakhstan(Aktau)
+04:00	Russia(Samara)

Time Zone	Time Zone Name
+05:00	Kazakhstan(Aqtobe)
+05:00	Kyrgyzstan(Bishkek)
+05:00	Pakistan(Islamabad)
+05:00	Russia(Chelyabinsk)
+05:30	India(Calcutta)
+06:00	Kazakhstan(Astana, Almaty)
+06:00	Russia(Novosibirsk, Omsk)
+07:00	Russia(Krasnoyarsk)
+07:00	Thailand(Bangkok)
+08:00	China(Beijing)
+08:00	Singapore(Singapore)
+08:00	Australia(Perth)
+09:00	Korea(Seoul)
+09:00	Japan(Tokyo)
+09:30	Australia(Adelaide)
+09:30	Australia(Darwin)
+10:00	Australia(Sydney, Melbourne, Canberra)
+10:00	Australia(Brisbane)
+10:00	Australia(Hobart)
+10:00	Russia(Vladivostok)
+10:30	Australia(Lord Howe Islands)
+11:00	New Caledonia(Noumea)
+12:00	New Zealand(Wellington, Auckland)
+12:45	New Zealand(Chatham Islands)
+13:00	Tonga(Nukualofa)

Appendix C: Configuration Parameters

This appendix describes the parameters you can set in the configuration files for the IP phone. The configuration files are <y000000000028>.cfg and <MAC>.cfg.

Setting Parameters in Configuration Files

You can set specific parameters in the configuration files for configuring IP phones. The <y000000000028>.cfg and <MAC>.cfg files are stored on the provisioning server. The IP phone checks for configuration files and looks for resource files when restarting the IP phone. The <y000000000028>.cfg file stores configurations for all phones of the same model. The <MAC>.cfg file stores configurations specific to the IP phone with that MAC address.

Configuration changes made in the <MAC>.cfg file override the configuration settings in the <y000000000028>.cfg file.

Basic and Advanced Parameters

DHCP

Parameter- network.internet_port.type	Configuration File <y000000000028>.cfg
Description	Defines the Internet port type. **Note**: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer
Default Value	0
Range	**Valid values are:** **0**-DHCP **1**-PPPoE **2**-Static IP Address
Example	network.internet_port.type= 0

Static Network Settings

Parameter- network.internet_port.type	Configuration File <y000000000028>.cfg
Description	Defines the Internet port type. **Note**: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer
Default Value	0
Range	**Valid values are:** **0**-DHCP **1**-PPPoE **2**-Static IP Address
Example	network.internet_port.type = 2

Parameter- network.internet_port.ip	Configuration File <y000000000028>.cfg
Description	Configures the IP address when the Internet port type is configured as Static IP Address. **Note**: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	IP Address
Default Value	Blank
Range	Not Applicable
Example	network.internet_port.ip = 192.168.1.20

Parameter- network.internet_port.mask	Configuration File <y000000000028>.cfg
Description	Configures the subnet mask when the Internet port type is configured as Static IP Address. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.

Format	IP Address
Default Value	Blank
Range	Not Applicable
Example	network.internet_port.mask = 255.255.255.0

Parameter- network.internet_port.gateway	**Configuration File** <y000000000028>.cfg
Description	Configures the default gateway when the Internet port type is configured as Static IP Address. **Note**: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	IP Address
Default Value	Blank
Range	Not Applicable
Example	network.internet_port.gateway = 192.168.1.254

Parameter- network.primary_dns	**Configuration File** <y000000000028>.cfg
Description	Configures the primary DNS server when the Internet port type is configured as Static IP Address. **Note**: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	IP Address
Default Value	202.101.103.55
Range	Not Applicable
Example	network.primary_dns = 202.101.103.5

Parameter- network.secondary_dns	Configuration File <y000000000028>.cfg
Description	Configures the secondary DNS server when the Internet port type is configured as Static IP Address. **Note**: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	IP Address
Default Value	202.101.103.56
Range	Not Applicable
Example	network.secondary_dns = 202.101.103.6

PPPoE

Parameter- network.internet_port.type	Configuration File <y000000000028>.cfg
Description	Defines the Internet port type. **Note**: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer
Default Value	0
Range	**Valid values are:** **0**-DHCP **1**-PPPoE **2**-Static IP Address
Example	network.internet_port.type= 1

Parameter- network.pppoe.user	Configuration File <y000000000028>.cfg
Description	Configures the PPPoE username when the Internet port type is configured as PPPoE. **Note**: If you change this parameter, the IP phone will reboot to make the change take effect.

Format	String
Default Value	Blank
Range	Not Applicable
Example	network.pppoe.user = xmyealink

Parameter- network.pppoe.password	**Configuration File** <y000000000028>.cfg
Description	Configures the PPPoE password when the Internet port type is configured as PPPoE. **Note**: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	String
Default Value	Blank
Range	Not Applicable
Example	network.pppoe.password = yealink123

Internet and PC Ports Negotiation

Internet Port Negotiation

Parameter- network.internet_port.speed_duplex	**Configuration File** <y000000000028>.cfg
Description	Specifies the transmission method of Internet port. **Note**: We recommend that you do not change this parameter.
Format	Integer
Default Value	0
Range	**Valid values are:** **0**-Auto negotiate **1**-Full duplex, 10Mbps **2**-Full duplex, 100Mbps **3**-Half duplex, 10Mbps **4**-Half duplex, 100Mbps **5**-Full duplex, 1000Mbps

Example	network.internet_port.speed_duplex = 0

PC Port Negotiation

Parameter- network.pc_port.speed_duplex	**Configuration File** <y000000000028>.cfg
Description	Specifies the transmission method of PC port. **Note**: We recommend that you do not change this parameter.
Format	Integer
Default Value	0
Range	**Valid values are:** **0**-Auto negotiate **1**-Full duplex, 10Mbps **2**-Full duplex, 100Mbps **3**-Half duplex, 10Mbps **4**-Half duplex, 100Mbps **5**-Full duplex, 1000Mbps
Example	network.pc_port.speed_duplex = 0

Dial Plan

Replace Rule

Parameter- dialplan.replace.prefix.X =	**Configuration File** <y000000000028>.cfg
Description	Specifies the string you want to replace. X ranges from 1 to 20.
Format	String
Default Value	Blank
Range	Not Applicable
Example	dialplan.replace.prefix.1 = 91([5-7])12

Parameter- dialplan.replace.replace.X =	**Configuration File** <y000000000028>.cfg
Description	Specifies the alternate string instead of what the user enters.

	X ranges from 1 to 20.
Format	String
Default Value	Blank
Range	Not Applicable
Example	dialplan.replace.replace.1 = 91$12

Parameter- dialplan.replace.line_id.X =	**Configuration File** <y000000000028>.cfg
Description	Specifies the desired line to apply this replace rule. X ranges from 1 to 20. **Note**: Multiple line IDs are separated by comma.
Format	String
Default Value	Blank
Range	Not Applicable
Example	dialplan.replace.line_id.1 = 1,2

Dial-now

Parameter- dialplan.dialnow.rule.X =	**Configuration File** <y000000000028>.cfg
Description	Specifies the string used to match the numbers entered by the user. When entered numbers match the predefined dial-now rule, the IP phone will automatically dial out the numbers without pressing the send key. X ranges from 1 to 20.
Format	String
Default Value	Blank
Range	Not Applicable
Example	dialplan.dialnow.rule.1 = 2216

Parameter- dialplan.dialnow.rule.X =	**Configuration File** <y000000000028>.cfg
Description	Specifies the desired line to apply this

	dial-now rule. X ranges from 1 to 20. **Note**: Multiple line IDs are separated by comma.
Format	String
Default Value	Blank
Range	Not Applicable
Example	dialplan.dialnow.line_id.1 = 1,2,3

Parameter- phone_setting.dialnow_delay	**Configuration File** <y000000000028>.cfg
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.
Format	Integer
Default Value	1
Range	0 to 14
Example	phone_setting.dialnow_delay = 1

Area Code

Parameter- dialplan.area_code.code	**Configuration File** <y000000000028>.cfg
Description	Defines the area code to add before the entered numbers.
Format	Integer
Default Value	Blank
Range	Not Applicable
Example	dialplan.area_code.code = 010

Parameter- dialplan.area_code.min_len	**Configuration File** <y000000000028>.cfg
Description	Sets the minimum length of the entered numbers.
Format	Integer
Default Value	1
Range	1 to 15
Example	dialplan.area_code.min_len = 2

Parameter- dialplan.area_code.max_len	**Configuration File** <y000000000028>.cfg
Description	Sets the maximum length of the entered numbers. **Note**: The value must be larger than the minimum length.
Format	Integer
Default Value	15
Range	1 to 15
Example	dialplan.area_code.max_len = 13

Parameter- dialplan.area_code.line_id	**Configuration File** <y000000000028>.cfg
Description	Specifies the desired line to apply this area code rule. **Note**: Multiple line IDs are separated by comma.
Format	Integer
Default Value	Blank (for all lines)
Range	**Valid values are**: 1 to 6
Example	dialplan.area_code.line_id = 1,2

Block Out

Parameter- dialplan.block_out.number.x	Configuration File <y000000000028>.cfg
Description	Specifies the block out numbers. X ranges from 1 to 10.
Format	String
Default Value	Blank
Range	Not Applicable
Example	dialplan.block_out.number.1 = 0000

Parameter- dialplan.block_out.line_id.x	Configuration File <y000000000028>.cfg
Description	Specifies the desired line to apply this block out rule. X ranges from 1 to 10. **Note**: Multiple line IDs are separated by comma.
Format	Integer
Default Value	Blank (for all lines)
Range	**Valid values are**: 1 to 6
Example	dialplan.block_out.line_id.1 = 1,2,3

Backlight

Parameter- phone_setting.active_backlight_level	Configuration File <y000000000028>.cfg
Description	Configures the backlight level used to adjust the backlight intensity of the LCD screen Level 3 is the brightest.
Format	Integer
Default Value	2
Range	1 to 3

Example	phone_setting.active_backlight_level = 1

Parameter- phone_setting.backlight_time	**Configuration File** <y000000000028>.cfg
Description	Configures the backlight time (in seconds) used to specify the delay time to turn off the backlight when the IP phone is inactive. If set to 60 (60s), the LCD backlight is turned off when the IP phone is inactive for 60 seconds.
Format	Integer
Default Value	30
Range	**Valid values are:** **0**-Always off **1**-Always on **15**-15s **30**-30s **60**-60s **120**-120s
Example	phone_setting.backlight_time = 0

User Password

Parameter- security.user_password	**Configuration File** <y000000000028>.cfg
Description	Sets a new user password for the IP phone. The IP phone uses "user" as the default user password. **Note**: IP phones support ASCII characters 32-126(0x20-0x7E) only in passwords.
Format	username:new password
Default Value	user
Range	ASCII characters 32-126(0x20-0x7E)
Example	security.user_password = user:password123

Administrator Password

Parameter- security.user_password	Configuration File <y000000000028>.cfg
Description	Sets a new administrator password for the IP phone. The IP phone uses "admin" as the default administrator password. **Note**: IP phones support ASCII characters 32-126(0x20-0x7E) only in passwords.
Format	administrator username:new password
Default Value	admin
Range	ASCII characters 32-126(0x20-0x7E)
Example	security.user_password = admin:password000

Phone Lock

Parameter- phone_setting.lock	Configuration File <y000000000028>.cfg
Description	Specifies the type of phone lock. Menu Key: The Menu soft key is locked. Function Key: MESSAGE, Redial, HOLD, MUTE, TRAN, OK, X, navigation keys, soft keys and line keys are locked. All Keys: All keys are locked, except the Volume key. If set to 0 (Disabled), the IP phone lock feature is disabled.
Format	Integer
Default Value	0
Range	**Valid values are:** **0**-Disabled **1**-Menu Key **2**-Function Keys **3**-All Keys
Example	phone_setting.lock = 2

Parameter- phone_setting.phone_lock.unlock_pin	**Configuration File** <y000000000028>.cfg
Description	Sets a new unlock password. Once the IP phone is locked, you can use "123" as the default password to unlock it. **Note**: IP phones support numeric characters only in password.
Format	Numeric characters only
Default Value	123
Range	0 to 15 characters
Example	phone_setting.phone_lock.unlock_pin = 123456

Parameter- phone_setting.phone_lock.lock_time_out	**Configuration File** <y000000000028>.cfg
Description	Configures the IP phone to automatically lock the keypad after a delay time (in seconds). If set to 0 (0s), the keypad will not be locked automatically. In this case, you can long press the pound key to lock the keypad only. **Note**: This parameter works only if the IP phone lock type is preset.
Format	Integer
Default Value	0
Range	0 to 3600
Example	phone_setting.phone_lock.lock_time_out = 8

Time and Date

NTP Server

Parameter- local_time.ntp_server1	Configuration File <y000000000028>.cfg
Description	Sets the IP address or the domain name of the primary NTP server.
Format	IP Address or Domain Name
Default Value	cn.pool.ntp.org
Range	Not Applicable
Example	local_time.ntp_server1 = 192.168.0.5

Parameter- local_time.ntp_server2	Configuration File <y000000000028>.cfg
Description	Sets the IP address or the domain name of the secondary NTP server. If the primary NTP server is not configured or cannot be accessed, the IP phone will request the time and date from the secondary NTP server.
Format	IP Address or Domain Name
Default Value	cn.pool.ntp.org
Range	Not Applicable
Example	local_time.ntp_server2 = 192.168.0.5

Parameter- local_time.interval	Configuration File <y000000000028>.cfg
Description	Sets the IP phone to update time and date from the NTP server at regular intervals (in seconds).
Format	Integer
Default Value	1000
Range	Not Applicable
Example	local_time.interval = 1200

Time Zone

Parameter- local_time.time_zone	Configuration File <y000000000028>.cfg
Description	Defines the time zone. For more available time zone list, refer to Appendix B: Time Zones on page 229.
Format	Not Applicable
Default Value	+8
Range	-11 to +13
Example	local_time.time_zone = +9

Parameter- local_time.time_zone_name	Configuration File <y000000000028>.cfg
Description	Defines the desired time zone name. For more available time zone name list, refer to Appendix B: Time Zones on page 229.
Format	String
Default Value	China(Beijing)
Range	Not Applicable
Example	local_time.time_zone_name = Korea(Seoul)

DST

Parameter- local_time.summer_time	Configuration File <y000000000028>.cfg
Description	Enables or disables the use of Daylight Saving Time (DST).
Format	Integer
Default Value	2
Range	**Valid values are:** **0**-Disabled **1**-Enabled **2**-Automatic
Example	local_time.summer_time = 2

Parameter- local_time.dst_time_type	**Configuration File** <y000000000028>.cfg
Description	Configures the DST type. **Note**: It works only if the parameter "local_time.summer_time" is set to 1 (Enabled).
Format	Integer
Default Value	Blank
Range	**Valid values are:** **0**-By Date **1**-By Week
Example	local_time.dst_time_type = 1

Parameter- local_time.start_time	**Configuration File** <y000000000028>.cfg
Description	Specifies the time to start DST. If "local_time.dst_time_type" is set to 0 (By Date), use the mapping: MM: 1=Jan, 2=Feb,..., 12=Dec DD:1=the first day in a month,..., 31= the last day in a month HH:0=1am, 1=2am,..., 23=12pm If "local_time.dst_time_type" is set to 1 (By Week), use the mapping: Month: 1=Jan, 2=Feb,..., 12=Dec Week of 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=1am, 1=2am,..., 23=12pm **Note**: It works only if the parameter "local_time.summer_time" is set to 1 (Enabled).
Format	**The value formats are:** • MM/DD/HH (For By Date) • Month/Week of Month/Day of Week/Hour of Day (For By Week)
Default Value	1/1/0

Range	1to 12/1 to 31/0 to 23 (for By Date) 1 to 12/1 to 5/1 to 7/0 to 23 (for By Week)
Example	local_time.start_time = 5/20/12

Parameter- local_time.end_time	**Configuration File** <y000000000028>.cfg
Description	Specifies the time to end DST. If "local_time.dst_time_type" is set to 0 (By Date), use the mapping: MM: 1=Jan, 2=Feb,…, 12=Dec DD:1=the first day in a month,…, 31= the last day in a month HH:0=1am, 1=2am,…, 23=12pm If "local_time.dst_time_type" is set to 1 (By Week), use the mapping: Month: 1=Jan, 2=Feb,…, 12=Dec Week of 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=1am, 1=2am,…, 23=12pm **Note**: It works only if the parameter "local_time.summer_time" is set to 1 (Enabled).
Format	**The value formats are:** • MM/DD/HH (For By Date) • Month/Week of Month/Day of Week/Hour of Day (For By Week)
Default Value	12/31/23
Range	1to 12/1 to 31/0 to 23 (For By Date) 1 to 12/1 to 5/1 to 7/0 to 23 (For By Week)
Example	local_time.end_time = 10/25/22

Parameter- local_time.offset_time	**Configuration File** <y000000000028>.cfg
Description	Sets the offset time (in minutes) of DST. **Note**: It works only if the parameter "local_time.summer_time" is set to 1

	(Enabled).
Format	Integer
Default Value	60
Range	-300 to +300
Example	local_time.offset_time = 120

Time Format

Parameter- local_time.time_format	**Configuration File** <y000000000028>.cfg
Description	Sets the time format. If set to 0 (12 Hour), the time display uses 12 hour format. If set to 1 (24 Hour), the time display uses 24 hour format.
Format	Integer
Default Value	1
Range	**0**-12 Hour **1**-24 Hour
Example	local_time.time_format = 0

Date Format

Parameter- local_time.date_format	**Configuration File** <y000000000028>.cfg
Description	Sets the date format. IP phones support various date formats. You can change the desired format according to your requirement.
Format	Integer
Default Value	0
Range	**Valid values are:** **0**-WWW MMM DD **1**-DD-MMM-YY **2**-YYYY-MM-DD **3**-DD/MM/YYYY **4**-MM/DD/YY **5**-DD MMM YYYY **6**-WWW DD MMM

Example	local_time.date_format = 1

Language

Parameter- gui_lang.url	**Configuration File** <y000000000028>.cfg
Description	Specifies the access URL of the language pack. **Note**: The language packs you load are dependent on available language packs from the provisioning server. You can download the language pack to the phone user interface only.
Format	URL
Default Value	Blank
Range	Not Applicable
Example	The following example uses HTTP to download the language pack "lang-Italian.txt"(Italian) from the provisioning server 192.168.10.25. gui_lang.url = http://192.168.10.25/lang-Italian.txt

Parameter- lang.wui	**Configuration File** <y000000000028>.cfg
Description	Specifies the language used on the web user interface. **Note**: The default language used on the web user interface depends on the language preferences of your browser. If the language of your browser is not supported by the IP phone, the web user interface will use English by default.
Format	Text
Default Value	Not Applicable
Range	**Valid values are:** English

	Chinese French German Italian Portuguese Spanish Turkish
Example	lang.wui = French

Parameter- lang.gui	**Configuration File** <y000000000028>.cfg
Description	Specifies the language used on the phone user interface.
Format	Text
Default Value	English
Range	**Valid values are:** English Chinese French German Italian Polish Portuguese Spanish Turkish
Example	lang.gui = English

Key as Send

Parameter- features.pound_key.mode	**Configuration File** <y000000000028>.cfg
Description	Defines the "#" or "*" key as the send key. If set to 0 (Disabled), neither "#" nor "*" can be used as a send key. If set to 1(# key), the pound key is used as the send key. If set to 2(* key), the asterisk key is used as the send key.

Format	Integer
Default Value	1
Range	**Valid values are:** **0**-Disabled **1**-# key **2**-* key
Example	features.pound_key.mode = 0

Parameter- features.send_key_tone	**Configuration File** <y000000000028>.cfg
Description	Enables or disables the IP phone to play a tone when a user presses a send key. If set to 1 (Enabled), the IP phone plays a tone when a user presses a send key. **Note**: It works only if the key tone is enabled. So you should set the parameter "features.key_tone" to 1 (Enabled) in advance.
Format	Integer
Default Value	1
Range	**0**-Disabled **1**-Enabled
Example	features.send_key_tone = 0

Hotline

Parameter- features.hotline_number	**Configuration File** <y000000000028>.cfg
Description	Configures the hotline number. It specifies a number that the IP phone automatically dials out when lifting the handset, pressing the speakerphone key or the line key. Leaving it blank disables the hotline feature.
Format	String
Default Value	Blank

Range	Not Applicable
Example	features.hotline_number = 3601

Parameter- features.hotline_delay	**Configuration File** <y000000000028>.cfg
Description	Specifies the waiting time (in seconds) the IP phone automatically dials out the hotline number. If set to 0 (0s), the IP phone immediately dials out the preconfigured hotline number when you lift the handset, press the speakerphone key or press the line key. If set to a value greater than 0, the IP phone waits the specified seconds before dialing out the predefined hotline number when you lift the handset, press the speakerphone key or press the line key.
Format	Integer
Default Value	4
Range	0 to 10
Example	features.hotline_delay = 30

Call Log

Parameter- features.history_save_display	**Configuration File** <y000000000028>.cfg
Description	Enables or disables the IP phone to display the Save Call Log option on the web user interface. If set to 0 (Disabled), the Save Call Log option is hidden on the web user interface. If set to 1 (Enabled), you can enable or disable the call log feature via web user interface.
Format	Boolean
Default Value	1
Range	**0**-Disabled **1**-Enabled

Example	features.history_save_display = 0

Parameter- features.save_call_history	**Configuration File** <y000000000028>.cfg
Description	Enables or disables the IP phone to save call log. If set to 0 (Disabled), the IP phone cannot log the dialed calls, received calls, missed calls and the forwarded calls in the call log lists.
Format	Boolean
Default Value	1
Range	**0**-Disabled **1**-Enabled
Example	features.save_call_history = 0

Missed Call Log

Parameter- account.x.missed_calllog	**Configuration File** <MAC>.cfg
Description	Enables or disables the missed call log feature for account X. If 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 set to 1 (Enabled), a prompt message "<number> New Missed Call(s)" along with an indicator icon is displayed on the IP phone idle screen when the IP phone misses calls. X ranges from 1 to 6.
Format	Boolean
Default Value	1
Range	**0**-Disabled **1**-Enabled
Example	account.1.missed_calllog = 1

Live Dialpad

Parameter- phone_setting.predial_autodial	Configuration File <y000000000028>.cfg
Description	Configures live dialpad feature. If set to 1 (Enabled), the IP phone automatically dials out the entered phone number without having to press any key.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	phone_setting.predial_autodial = 1

Call Waiting

Parameter- call_waiting.enable	Configuration File <y000000000028>.cfg
Description	Enables or disables the call waiting feature. If set to 0 (Disabled), a new incoming call is automatically rejected by the IP phone with a busy message while during a call. If set to 1 (Enabled), the phone LCD screen presents a new incoming call while during a call.
Format	Boolean
Default Value	1
Range	**0**-Disabled **1**-Enabled
Example	call_waiting.enable = 1

Parameter- call_waiting.tone	Configuration File <y000000000028>.cfg
Description	Enables or disables the playing of a call waiting tone when the IP phone receives an incoming call during a call. If set to 1 (Enabled), the IP phone performs 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).
Format	Boolean
Default Value	1
Range	**0**-Disabled **1**-Enabled
Example	call_waiting.tone = 1

Auto Redial

Parameter- auto_redial.enable	**Configuration File** <y000000000028>.cfg
Description	Enables or disables the IP phone to automatically redial the called number when it is busy. If set to 1 (Enabled), the IP phone dials the previous dialed out number automatically when the dialed number is busy.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	auto_redial.enable = 1

Parameter- auto_redial.interval	**Configuration File** <y000000000028>.cfg
Description	Sets 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.
Format	Integer
Default Value	10
Range	1 to 300

Example	auto_redial.interval = 30

Parameter- auto_redial.times	**Configuration File** <y000000000028>.cfg
Description	Sets the redial times for the IP phone. The IP phone tries to redial the dialed number as many times as configured till the callee answers the call.
Format	Integer
Default Value	10
Range	1 to 300
Example	auto_redial.times = 8

Auto Answer

Parameter- account.x.auto_answer	**Configuration File** <MAC>.cfg
Description	Enables or disables the auto answer feature for account X. If set to 1 (Enabled), the IP phone can automatically answer an incoming call. X ranges from 1 to 6. **Note**: The IP phone cannot automatically answer the incoming call during a call even if auto answer is enabled.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	account.1.auto_answer = 1

Call Completion

Parameter- features.call_completion_enable	Configuration File <y000000000028>.cfg
Description	Enables or disables the call completion feature. If a user places a call and the callee is temporarily not available to answer the call, the call completion feature allows notifying the user when the callee becomes available to receive a call. If set to 1 (Enabled), the caller is notified when the callee becomes available to receive a call.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	features.call_completion_enable = 1

Anonymous Call

Parameter- account.x.anonymous_call	Configuration File <MAC>.cfg
Description	Enables or disables the anonymous call feature for account X. If set to 1 (Enabled), the IP phone blocks 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.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	account.1.anonymous_call = 1

Parameter- account.x.anonymous_call_oncode	Configuration File <MAC>.cfg
Description	Sets the anonymous call on code to activate the server-side anonymous call feature for account X (optional). X ranges from 1 to 6.
Format	String
Default Value	Blank
Range	Not Applicable
Example	account.1.anonymous_call_oncode = *72

Parameter- account.x.anonymous_call_offcode	Configuration File <MAC>.cfg
Description	Sets the anonymous call off code to deactivate the server-side anonymous call feature for account X (optional). X ranges from 1 to 6.
Format	String
Default Value	Blank
Range	Not Applicable
Example	account.1.anonymous_call_offcode = *73

Anonymous Call Rejection

Parameter- account.x.reject_anonymous_call	Configuration File <MAC>.cfg
Description	Enables or disables the anonymous call rejection feature for account X. If set to 1 (Enabled), the IP phone automatically rejects incoming calls from users enabled the anonymous call feature. The anonymous user's phone LCD screen presents "Anonymity Disallowed".

	X ranges from 1 to 6.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	account.1.reject_anonymous_call = 1

Parameter- account.x.anonymous_reject_oncode	**Configuration File** <MAC>.cfg
Description	Sets the anonymous call rejection on code to activate the server-side anonymous call rejection feature for account X (optional). X ranges from 1 to 6.
Format	String
Default Value	Blank
Range	Not Applicable
Example	account.1.anonymous_reject_oncode = *74

Parameter- account.x.anonymous_reject_offcode	**Configuration File** <MAC>.cfg
Description	Sets the anonymous call rejection off code to deactivate the server-side anonymous call rejection feature for account X (optional). X ranges from 1 to 6.
Format	String
Default Value	Blank
Range	Not Applicable
Example	account.1.anonymous_reject_offcode = *73

Do Not Disturb

Return Message When DND

Parameter- features.dnd_refuse_code	Configuration File <y000000000028>.cfg
Description	Defines return codes and reason of the SIP response message when rejecting an incoming call for DND. A specific reason is displayed on the caller's phone LCD screen. If set to 486 (Busy here), the caller's phone LCD screen displays the reason "Busy here" when the callee enables the DND feature.
Format	Integer
Default Value	480
Range	**Valid values are:** **404**-No Found **480**-Temporarily not available **486**-Busy here
Example	features.dnd_refuse_code = 486

DND Mode

Parameter- features.dnd_mode	Configuration File <y000000000028>.cfg
Description	Sets the DND mode for the IP phone. If set to 0 (Phone), the DND feature is effective for the IP phone. If set to 1 (Custom), you can configure the DND feature for each account.
Format	Integer
Default Value	0
Range	**0**-Phone **1**-Custom
Example	features.dnd_mode = 0

DND in Phone Mode

Parameter- features.dnd.enable	Configuration File <y000000000028>.cfg
Description	Enables or disables the DND feature. If set to 1 (Enabled), the IP phone rejects incoming calls on all accounts.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	features.dnd.enable = 1

Parameter- features.dnd.on_code	Configuration File <y000000000028>.cfg
Description	Sets the DND on code to activate the server-side DND feature.
Format	String
Default Value	Blank
Range	Not Applicable
Example	features.dnd.on_code = *71

Parameter- features.dnd.off_code	Configuration File <y000000000028>.cfg
Description	Sets the DND off code to deactivate the server-side DND feature.
Format	String
Default Value	Blank
Range	Not Applicable
Example	features.dnd.off_code = *72

DND in Custom Mode

Parameter- account.x.dnd.enable	Configuration File <MAC>.cfg
Description	Enables or disables the DND feature for

	account X. If set to 1 (Enabled), the IP phone rejects incoming calls on account x. X ranges from 1 to 6.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	account.1.dnd.enable = 1

Parameter- account.x.dnd.on_code	**Configuration File** <MAC>.cfg
Description	Sets the DND on code to activate the server-side DND feature for account X (optional). X ranges from 1 to 6.
Format	String
Default Value	Blank
Range	Not Applicable
Example	account.1.dnd.on_code = *73

Parameter- account.x.dnd.off_code	**Configuration File** <MAC>.cfg
Description	Sets the DND off code to deactivate the server-side DND feature for account X (optional). X ranges from 1 to 6.
Format	String
Default Value	Blank
Range	Not Applicable
Example	account.1.dnd.off_code = *74

Busy Tone Delay

Parameter- features.busy_tone_delay	**Configuration File** <y000000000028>.cfg
Description	Configures a period of time (in seconds) for which the busy tone is audible on the IP phone. When one party releases the call, a busy tone is audible to the other party indicating that the call connection breaks. If set to 3 (3s), a busy tone is audible for 3 seconds on the IP phone.
Format	Integer
Default Value	0
Range	**Valid values are:** **0**-0s **3**-3s **5**-5s
Example	features.busy_tone_delay = 3

Return Code When Refuse

Parameter- features.normal_refuse_code	**Configuration File** <y000000000028>.cfg
Description	Defines return codes and messages when rejecting an incoming call. A specific return message is displayed on the caller's phone LCD screen. If set to 486 (Busy here), the caller's phone LCD screen displays the message "Busy here" when the callee rejects the incoming call.
Format	Integer
Default Value	486
Range	**Valid values are:** **404**-No Found **480**-Temporarily not available **486**-Busy here

Example	features.normal_refuse_code = 480

180 Ring Workaround

Parameter- phone_setting.is_deal180	Configuration File <y000000000028>.cfg
Description	Enables or disables the IP phone to deal with the 180 SIP message received after the 183 SIP message. If set to 1 (Enabled), the IP phone resumes and plays the local ringback tone upon a subsequent 180 message received.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	phone_setting.is_deal180 = 1

Use Outbound Proxy in Dialog

Parameter- sip.use_out_bound_in_dialog	Configuration File <y000000000028>.cfg
Description	Enables or disables the IP phone to send the SIP messages to the outbound proxy server. If set to 1 (Enabled), all the SIP request messages from the IP phone will be forced to send to the outbound proxy server.
Format	Boolean
Default Value	1
Range	**0**-Disabled **1**-Enabled
Example	sip.use_out_bound_in_dialog = 0

SIP Session Timer

Parameter- account.x.advanced.timer_t1	Configuration File <MAC>.cfg
Description	Configures the SIP session timer T1 (in seconds) for account X. T1 is an estimate of the Round Trip Time (RTT) of transactions between a SIP client and SIP server. X ranges from 1 to 6.
Format	Float
Default Value	0.5
Range	Not Applicable
Example	account.1.advanced.timer_t1 = 1

Parameter- account.x.advanced.timer_t2	Configuration File <MAC>.cfg
Description	Configures the session timer T2 (in seconds) for account X. T2 represents the maximum retransmitting time of any SIP request message. The re-transmitting and doubling of T1 continues until the retransmitting time reaches the T2 value. X ranges from 1 to 6.
Format	Float
Default Value	4
Range	Not Applicable
Example	account.1.advanced.timer_t2 = 5

Parameter- account.x.advanced.timer_t4	Configuration File <MAC>.cfg
Description	Configures the session timer of T4 (in seconds) for account X. T4 represents the time the network will take

	to clear messages between the SIP Client and SIP Server. X ranges from 1 to 6.
Format	Float
Default Value	5
Range	Not Applicable
Example	account.1.advanced.timer_t4 = 10

Session Timer

Parameter- account.x.session_timer.enable	**Configuration File** <MAC>.cfg
Description	Enables or disables the session timer for account X. If set to 1 (Enabled), IP phone sends periodic re-INVITE requests to refresh the session during a call. X ranges from 1 to 6.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	account.1.session_timer.enable = 1

Parameter- account.x.session_timer.expires	**Configuration File** <MAC>.cfg
Description	Configures the IP phone to refresh the session during a call at regular intervals (in seconds) for account X. If set to 1800 (1800s), the IP phone refreshes the session during a call before 1800 seconds. X ranges from 1 to 6.
Format	Integer
Default Value	1800
Range	1-9999

Example	account.1.session_timer.expires = 300

Parameter- account.x.session_timer.refresher	**Configuration File** <MAC>.cfg
Description	Configures the session timer refresher for account X. If set to 0 (UAC), refreshing the session is performed by the IP phone. If set to 1 (UAS), refreshing the session is performed by a SIP server. X ranges from 1 to 6.
Format	Integer
Default Value	0
Range	**Valid values are:** **0**-UAC **1**-UAS
Example	account.1.session_timer.refresher = 1

Call Hold

Parameter- features.play_hold_tone.enable	**Configuration File** <y000000000028>.cfg
Description	Enables or disables the IP phone to play a tone when there is a hold call on the IP phone.
Format	Boolean
Default Value	1
Range	**0**-Disabled **1**-Enabled
Example	features.play_hold_tone.enable = 1

Parameter- features.play_hold_tone.delay	**Configuration File** <y000000000028>.cfg
Description	Specifies the interval (in seconds) at which the IP phone plays a hold tone. If set to 30 (30s), the IP phone plays 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).
Format	Integer
Default Value	30
Range	Not Applicable
Example	features.play_hold_tone.delay = 60

Parameter- sip.rfc2543_hold	**Configuration File** <y000000000028>.cfg
Description	Specifies whether RFC 2543 (c=0.0.0.0) outgoing hold signaling is used. If set to 0 (Disabled), use SDP media direction attributes (such as a=sendonly) per RFC 3264 when putting a call on hold. If set to 0 (Enabled), use SDP media connection address c=0.0.0.0 per RFC 2543 when putting a call on hold.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	sip.rfc2543_hold = 1

Call Forward

Call Forward Mode

Parameter- features.fwd_mode	**Configuration File** <y000000000028>.cfg
Description	Sets the call forward mode for the IP phone. If set to 0 (Phone), the call forward feature is effective for the IP phone. If set to 1 (Custom), you can configure the call forward feature for each account.

Format	Integer
Default Value	0
Range	**0**-Phone **1**-Custom
Example	features.fwd_mode = 0

Call Forward in Phone Mode

Always Forward

Parameter- forward.always.enable	**Configuration File** < y000000000028 >.cfg
Description	Enables or disables the always forward feature. If set to 1 (Enabled), incoming call are forwarded to the destination number immediately.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	forward.always.enable = 1

Parameter- forward.always.target	**Configuration File** < y000000000028 >.cfg
Description	Defines the destination number of the always forward.
Format	String
Default Value	Blank
Range	Not Applicable
Example	forward.always.target = 3601

Parameter- forward.always.on_code	**Configuration File** < y000000000028 >.cfg
Description	Sets the always forward on code to activate the server-side always forward feature.
Format	String

Default Value	Blank
Range	Not Applicable
Example	forward.always.on_code = *72

Parameter- forward.always.off_code	**Configuration File** < y000000000028 >.cfg
Description	Sets the always forward off code to deactivate the server-side always forward feature.
Format	String
Default Value	Blank
Range	Not Applicable
Example	forward.always.off_code = *73

Busy Forward

Parameter- forward.busy.enable	**Configuration File** < y000000000028 >.cfg
Description	Enables or disables the busy forward feature. If set to 1 (Enabled), incoming calls are forwarded to the destination number when the callee is busy.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	forward.busy.enable = 1

Parameter- forward.busy.target	**Configuration File** < y000000000028 >.cfg
Description	Defines the destination number of the busy forward.
Format	String
Default Value	Blank
Range	Not Applicable

Example	forward.busy.target = 3602

Parameter- forward.busy.on_code	**Configuration File** < y000000000028 >.cfg
Description	Sets the busy forward on code to activate the server-side busy forward feature.
Format	String
Default Value	Blank
Range	Not Applicable
Example	forward.busy.on_code = *74

Parameter- forward.busy.off_code	**Configuration File** < y000000000028 >.cfg
Description	Sets the busy forward off code to deactivate the server-side busy forward feature.
Format	String
Default Value	Blank
Range	Not Applicable
Example	forward.busy.off_code = *75

No Answer Forward

Parameter- forward.no_answer.enable	**Configuration File** < y000000000028 >.cfg
Description	Enables or disables the no answer forward feature. If set to 1 (Enabled), incoming calls are forward to the destination number after a period of ring time.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	forward.no_answer.enable = 1

Parameter- forward.no_answer.target	Configuration File < y000000000028 >.cfg
Description	Defines the destination number of the no answer forward.
Format	String
Default Value	Blank
Range	Not Applicable
Example	forward.no_answer.target = 3603

Parameter- forward.no_answer.timeout	Configuration File < y000000000028 >.cfg
Description	Defines a period of ring time to wait before forwarding the incoming call. The interval of the ring time is n*6 (0≤n≤20), the valid values ranges from 0 to 20.
Format	Integer
Default Value	2
Range	0 to 20
Example	forward.no_answer.timeout = 5

Parameter- forward.no_answer.on_code	Configuration File < y000000000028 >.cfg
Description	Sets the no answer forward on code to activate the server-side no answer forward feature.
Format	String
Default Value	Blank
Range	Not Applicable
Example	forward.no_answer.on_code = *76

Parameter- forward.no_answer.off_code	Configuration File < y000000000028 >.cfg
Description	Sets the no answer forward off code to deactivate the server-side no answer

	forward feature.
Format	String
Default Value	Blank
Range	Not Applicable
Example	forward.no_answer.off_code = *77

Call Forward in Custom Mode

Always Forward

Parameter- account.x.always_fwd.enable	**Configuration File** <MAC>.cfg
Description	Enables or disables the always forward feature for account X. If set to 1 (Enabled), incoming calls to the account X are forwarded to the destination number immediately. X ranges from 1 to 6.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	account.1.always_fwd.enable = 1

Parameter- account.x.always_fwd.target	**Configuration File** <MAC>.cfg
Description	Defines the destination number of the always forward for account X. X ranges from 1 to 6.
Format	String
Default Value	Blank
Range	Not Applicable
Example	account.1.always_fwd.target = 3601

Parameter- account.x.always_fwd.on_code	Configuration File <MAC>.cfg
Description	Sets the always forward on code activate the server-side always forward feature for account X. X ranges from 1 to 6.
Format	String
Default Value	Blank
Range	Not Applicable
Example	account.1.always_fwd.on_code = *72

Parameter- account.x.always_fwd.off_code	Configuration File <MAC>.cfg
Description	Sets the always forward off code to deactivate the server-side always forward feature for account X. X ranges from 1 to 6.
Format	String
Default Value	Blank
Range	Not Applicable
Example	account.1.busy_fwd.off_code = *73

Busy Forward

Parameter- account.x.busy_fwd.enable	Configuration File <MAC>.cfg
Description	Enables or disables the busy forward feature for account X. If set to 1 (Enabled), incoming calls to the account X are forwarded to the destination number when the callee is busy. X ranges from 1 to 6.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled

Example	account.1.busy_fwd.enable = 1

Parameter- account.x.busy_fwd.target	**Configuration File** <MAC>.cfg
Description	Defines the destination number of the busy forward for account X. X ranges from 1 to 6.
Format	String
Default Value	Blank
Range	Not Applicable
Example	account.1.busy_fwd.target = 3602

Parameter- account.x.busy_fwd.on_code	**Configuration File** <MAC>.cfg
Description	Sets the busy forward on code to activate the server-side busy forward feature for account X. X ranges from 1 to 6
Format	String
Default Value	Blank
Range	Not Applicable
Example	account.1.busy_fwd.on_code = *74

Parameter- account.x.busy_fwd.off_code	**Configuration File** <MAC>.cfg
Description	Sets the busy forward off code to deactivate the server-side busy forward feature for account X (optional). X ranges from 1 to 6
Format	String
Default Value	Blank
Range	Not Applicable
Example	account.1.busy_fwd.off_code = *75

No Answer Forward

Parameter- account.x.timeout_fwd.enable	Configuration File <MAC>.cfg
Description	Enables or disables the no answer forward feature for account X. If set to 1 (Enabled), incoming calls to the account X are forward to the destination number after a period of ring time. X ranges from 1 to 6.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	account.1.timeout_fwd.enable = 1

Parameter- account.x.timeout_fwd.target	Configuration File <MAC>.cfg
Description	Defines the destination number of the no answer forward for account X. X ranges from 1 to 6.
Format	String
Default Value	Blank
Range	Not Applicable
Example	account.1.timeout_fwd.target = 3603

Parameter- account.x.timeout_fwd.timeout	Configuration File <MAC>.cfg
Description	Defines a period of ring time to wait before forwarding the incoming call for account X. The interval of the ring time is n*6 (0≤n≤20), the valid values ranges from 0 to 20. X ranges from 1 to 6.
Format	Integer
Default Value	2
Range	0 to 20

Example	account.1.timeout_fwd.timeout = 5

Parameter- account.x.timeout_fwd.on_code	**Configuration File** <MAC>.cfg
Description	Sets the no answer forward on code to activate the server-side no answer forward feature for account X. X ranges from 1 to 6.
Format	String
Default Value	Blank
Range	Not Applicable
Example	account.1.timeout_fwd.on_code = *76

Parameter- account.x.timeout_fwd.off_code	**Configuration File** <MAC>.cfg
Description	Sets the no answer forward off code to activate the server-side no answer forward feature for account X. X ranges from 1 to 6.
Format	String
Default Value	Blank
Range	Not Applicable
Example	account.1.timeout_fwd.off_code = *77

Fwd International

Parameter- forward.international.enable	**Configuration File** <y000000000028>.cfg
Description	Enables or disables the IP phone to forward an incoming call to an international phone number (the prefix is 00).
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	forward.international.enable = 1

Call Transfer

Parameter-transfer.blind_tran_on_hook_enable	Configuration File <y000000000028>.cfg
Description	Enables or disables the IP phone to complete the blind transfer through on-hook.
Format	Boolean
Default Value	1
Range	**0**-Disabled **1**-Enabled
Example	transfer.blind_tran_on_hook_enable = 1

Parameter-transfer.on_hook_trans_enable	Configuration File <y000000000028>.cfg
Description	Enables or disables the IP phone to complete the semi-attended transfer or the attended transfer through on-hook.
Format	Boolean
Default Value	1
Range	**0**-Disabled **1**-Enabled
Example	transfer.on_hook_trans_enable = 1

Parameter-transfer.semi_attend_tran_enable	Configuration File <y000000000028>.cfg
Description	Specifies whether to display the missed call prompt on the destination party’s phone.
Format	Boolean
Default Value	1
Range	**0**-Disabled **1**-Enabled
Example	transfer.semi_attend_tran_enable = 1

Network Conference

Parameter- account.x.conf_type	Configuration File <MAC>.cfg
Description	Defines the conference type for account X. If set to 0 (Local), conferences are set up on the IP phone locally. If set to 2 (Network Conference), conferences are set up by the server. X ranges from 1 to 6.
Format	Integer
Default Value	0
Range	**Valid values are:** **0**-Local **2**-Network Conference
Example	account.1.conf_type = 2

Parameter- account.x.conf_uri	Configuration File <MAC>.cfg
Description	Defines the conference URI for account X. X ranges from 1 to 6. **Note**: It works only if the parameter "account.x.conf_type" is set to 2 (Network Conference).
Format	String
Default Value	Blank
Range	Not Applicable
Example	account.1.conf_uri = conference@domain.com

Transfer on Conference Hang Up

Parameter- transfer.tran_others_after_conf_enable	**Configuration File** <y000000000028>.cfg
Description	Enables or disables the Transfer on Conference Hang Up feature. If enabled, the other two parties remain connected when the conference initiator drops the conference call. **Note**: It is only applicable to the local conference.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	transfer.tran_others_after_conf_enable = 1

Directed Call Pickup

Phone Basis

Parameter- features.pickup.direct_pickup_enable	**Configuration File** <y000000000028>.cfg
Description	Enables or disables the IP phone to display the DPickup soft key when the IP phone is off-hook.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	features.pickup.direct_pickup_enable = 1

Parameter- features.pickup.direct_pickup_code	**Configuration File** <y000000000028>.cfg

Description	Configures the directed call pickup code on a phone basis. **Note**: The directed call pickup code configured on a per-account basis takes precedence over that configured on a phone basis.
Format	String
Default Value	Blank
Range	Not Applicable
Example	features.pickup.direct_pickup_code = *97

Per-account Basis

Parameter- account.x.direct_pickup_code	**Configuration File** <y000000000028>.cfg
Description	Configures the directed call pickup code on a per-account basis. X ranges from 1 to 6. **Note**: The directed call pickup code configured on a per-account basis takes precedence over that configured on a phone basis.
Format	String
Default Value	Blank
Range	Not Applicable
Example	account.1.direct_pickup_code = *68

Group Call Pickup

Phone Basis

Parameter- features.pickup.group_pickup_enable	**Configuration File** <y000000000028>.cfg
Description	Enables or disables the IP phone to display the GPickup soft key when the IP phone is off-hook.
Format	Boolean

Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	features.pickup.group_pickup_enable = 1

Parameter- features.pickup.group_pickup_code	**Configuration File** <y000000000028>.cfg
Description	Configures the group call pickup code on a phone basis. **Note**: The group call pickup code configured on a per-account basis takes precedence over that configured on a phone basis.
Format	String
Default Value	Blank
Range	Not Applicable
Example	features.pickup.group_pickup_code = *98

Per-account Basis

Parameter- account.x.group_pickup_code	**Configuration File** <y000000000028>.cfg
Description	Configures the group call pickup code on a per-account basis. X ranges from 1 to 6. **Note**: The group call pickup code configured on a per-account basis takes precedence over that configured on a phone basis.
Format	String
Default Value	Blank
Range	Not Applicable
Example	account.1.group_pickup_code = *69

Dialog-Info Call Pickup

Parameter- account.x.dialoginfo_callpickup	Configuration File <MAC>.cfg
Description	Configures the Dialog-Info Call Pickup feature for account X. If set to 1 (Enabled), call pickup is implemented through SIP signals. X ranges from 1 to 6.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	account.1.dialoginfo_callpickup = 1

Web Server Type

Parameter- wui.http_enable	Configuration File <y000000000028>.cfg
Description	Enables or disables the IP phone to access its web user interface using HTTP protocol. **Note**: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Boolean
Default Value	1
Range	**0**-Disabled **1**-Enabled
Example	wui.http_enable = 1

Parameter- network.port.http	Configuration File <y000000000028>.cfg
Description	Configures the HTTP port to access the web user interface of the IP phone. The default HTTP port is 80. **Note**: If you change this parameter, the IP

	phone will reboot to make the change take effect.
Format	Integer
Default Value	80
Range	1 to 65535
Example	network.port.http = 90

Parameter- wui.https_enable	**Configuration File** <y000000000028>.cfg
Description	Enables or disables the IP phone to access its web user interface using HTTPS protocol. **Note**: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Boolean
Default Value	1
Range	**0**-Disabled **1**-Enabled
Example	wui.https_enable = 1

Parameter- network.port.https	**Configuration File** <y000000000028>.cfg
Description	Configures the HTTPS port to access the web user interface of the IP phone. The default HTTPS port is 443. **Note**: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer
Default Value	443
Range	1 to 65535
Example	network.port.https = 100

Calling Line Identification Presentation

Parameter- account.x.cid_source	Configuration File <MAC>.cfg
Description	Configures the presentation of the caller identity 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.
Format	Integer
Default Value	0
Range	0 to 5
Example	account.1.cid_source = 2

Connected Line Identification Presentation

Parameter- account.x.cp_source	Configuration File <MAC>.cfg
Description	Configures the presentation of the callee identity for account X. **0**-RPID-FROM (Derives the name and number of the callee from the "RPID" header preferentially. If the server does not send the "RPID" header, derives from the "From" header). **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.
Format	Integer
Default Value	0
Range	0 to 2
Example	account.1.cp_source = 2

DTMF

Parameter- account.x.dtmf.type	**Configuration File** <MAC>.cfg
Description	Specifies the DTMF type for account X. If set to 0 (INBAND), DTMF digits are transmitted in the voice band (G.711). If set to 1 (RFC 2833), DTMF digits are transmitted by RTP Events compliant to RFC 2833. If set to 2 (SIP INFO), DTMF digits are transmitted by the SIP INFO messages. If set to 3 (AUTO+SIP INFO), negotiates with the other end to use INBAND or RFC 2833, if there is no negotiation, using SIP INFO by default. X ranges from 1 to 6.
Format	Integer
Default Value	1
Range	**Valid values are:** **0**-INBAND **1**-RFC 2833

	2-SIP INFO **3**-AUTO+SIP INFO
Example	account.1.dtmf.type = 2

Parameter- account.x.dtmf.dtmf_payload	**Configuration File** <MAC>.cfg
Description	Configures the RFC 2833 payload type. X ranges from 1 to 6.
Format	Integer
Default Value	101
Range	96 to 127
Example	account.1.dtmf.dtmf_payload = 101

Parameter- account.x.dtmf.info_type	**Configuration File** <MAC>.cfg
Description	Configures the DTMF info type when the DTMF type is configured as "SIP INFO" or "AUTO+SIP INFO". X ranges from 1 to 6.
Format	Integer
Default Value	0
Range	**Valid values are:** **0**-Disabled **1**-DTMF-Relay **2**-DTMF **3**-Telephone-Event
Example	account.1.dtmf.info_type = 3

Parameter- features.dtmf.repetition	**Configuration File** <y000000000028>.cfg
Description	Configures the number of times for the IP phone to send the end RTP EVENT packet.
Format	Integer
Default Value	3
Range	1 to 3

Example	features.dtmf.repetition = 2

Suppress DTMF Display

Parameter- features.dtmf.hide	Configuration File <y000000000028>.cfg
Description	Enables or disables the IP phone to suppress the display of DTMF digits. If set to 1 (Enabled), the DTMF digits are displayed as asterisks.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	features.dtmf.hide = 1

Parameter- features.dtmf.hide_delay	Configuration File <y000000000028>.cfg
Description	Enables or disables the IP phone to display the DTMF digits for a short period before displaying asterisks. **Note:** It works only if the parameter “features.dtmf.hide” is set to 1 (Enabled).
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	features.dtmf.hide_delay = 1

Transfer via DTMF

Parameter- features.dtmf.replace_tran	Configuration File <y000000000028>.cfg
Description	Enables or disables the transfer via DTMF feature. If set to 0 (Disabled), the IP phone enters into

	the transfer to screen when pressing the transfer key during a call. If set to 1 (Enabled), the IP phone transmits the specified DTMF digits to the server when pressing the transfer key during a call, and then complete the transfer.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	features.dtmf.replace_tran = 1

Parameter- features.dtmf.transfer	**Configuration File** <y000000000028>.cfg
Description	Specifies the DTMF digits to be transmitted to complete the transfer. **Note:** It works only if the parameter "features.dtmf.replace_tran" is set to 1 (Enabled).
Format	String
Default Value	Blank
Range	Valid values are: 0-9, *, # and A-D.
Example	features.dtmf.transfer = 123

Incoming Intercom calls

Parameter- features.intercom.allow	**Configuration File** <y000000000028>.cfg
Description	Enables or disables the IP phone to automatically answer an incoming intercom call. If set to 0 (Disabled), the IP phone rejects incoming intercom calls and sends a busy signal to the caller. If set to 1 (Enabled), the IP phone automatically answers an incoming intercom call.

Format	Boolean
Default Value	1
Range	**0**-Disabled **1**-Enabled
Example	features.intercom.allow = 1

Parameter- features.intercom.mute	**Configuration File** <y000000000028>.cfg
Description	Enables or disables the IP phone to mute the microphone when answering an intercom call. If set to 0 (Disabled), the microphone is un-muted for incoming calls. If set to 1 (Enabled), the microphone is muted for intercom calls.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	features.intercom.mute = 1

Parameter- features.intercom.tone	**Configuration File** <y000000000028>.cfg
Description	Enables or disables the IP phone to play a warning tone when receiving an intercom call. If set to 0 (Disabled), the IP phone automatically answers the intercom call without a warning tone. If set to 1 (Enabled), the IP phone plays a warning tone to alert you before answering the intercom call.
Format	Boolean
Default Value	1
Range	**0**-Disabled **1**-Enabled

Example	features.intercom.tone = 1

Parameter- features.intercom.barge	**Configuration File** <y000000000028>.cfg
Description	Enables or disables the IP phone to automatically answer an incoming intercom call while there is already an active call on the IP phone. If set to 0 (Disabled), the IP phone handles an incoming intercom call like a waiting call while there is already an active call on the IP phone. If set to 1 (Enabled), the IP phone automatically answers the intercom call while there is already an active call on the IP phone and put the active call on hold.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	features.intercom.barge = 1

Distinctive Ring Tones

Parameter- features.alert_info_tone	**Configuration File** <y000000000028>.cfg
Description	Enables and disables the IP phone to map the keywords in the Alert-info header to the specified Bellcore ring tones.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	features.alert_info_tone = 1

Parameter- account.x.alert_info_url_enable	Configuration File <MAC>.cfg
Description	Enables or disables the distinctive ring tones feature for account X. X ranges from 1 to 6.
Format	Boolean
Default Value	0
Range	**0**-Enabled **1**-Disabled
Example	account.1.alert_info_url_enable = 1

Parameter- distinctive_ring_tones.alert_info.x.text	Configuration File <y000000000028>.cfg
Description	Specifies the texts to map the keywords contained in the SIP header. X ranges from 1 to 10.
Format	Text
Default Value	Blank
Range	Not Applicable
Example	distinctive_ring_tones.alert_info.1.text = family

Parameter- distinctive_ring_tones.alert_info.x.ringer	Configuration File <y000000000028>.cfg
Description	Specifies the desired ring tones for each text. The value ranges from 0 to 8, the digit stands for the appropriate ring tone. X ranges from 1 to 10.
Format	Integer
Default Value	0
Range	**Valid values are**: **0**-Default.wav

	1-Ring1.wav 2-Ring2.wav 3-Ring3.wav 4-Ring4.wav 5-Ring5.wav 6-Ring6.wav 7-Ring7.wav 8-Ring8.wav
Example	distinctive_ring_tones.alert_info.1.ringer = 2

Tones

Parameter- voice.tone.country	**Configuration File** <y000000000028>.cfg
Description	Configures the tone type for the IP phone.
Format	Text
Default Value	Custom
Range	**Valid values are:** • 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	voice.tone.country = Austria

Parameter- voice.tone.dial voice.tone.ring voice.tone.busy voice.tone.congestion voice.tone.callwaiting voice.tone.dialrecall voice.tone.record voice.tone.info voice.tone.stutter voice.tone.message voice.tone.autoanswer	**Configuration File** <y000000000028>.cfg
Description	Customizes the tone for each condition. tonelist = element[,element] [,element]... Where **element** = !F1+F2+F3+F4/Duration **F**: the frequency of the tone (ranges from 200 to 7000 Hz). If set to 0 (0Hz), it means that the phone does not play tone. A tone can be composited at most four different frequencies (value format: F1+F2+F3+F4). **D**: the time duration (in milliseconds, ranges from 0 to 30000ms) of ringing the tone. You can configure at most eight different tones for one condition, each tone separated by comma (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.
Format	F/D or !F/D
Default Value	Blank
Range	Not Applicable
Example	voice.tone.dial = 800+200/1000, 0/100, 500/1200, 500+600+950+1500/5000

Remote Phonebook

Parameter- features.remote_phonebook.enable	**Configuration File** <y000000000028>.cfg
Description	Enables or disables the IP phone to perform a remote phonebook search when receiving an incoming call.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	features.remote_phonebook.enable = 1

Parameter- features.remote_phonebook.flash_time	**Configuration File** <y000000000028>.cfg
Description	Sets how often to refresh the local cache of the remote phonebook. If set to 3600 (3600s), the IP phone refreshes the local cache of the remote phonebook every 3600 seconds.
Format	Integer
Default Value	3600
Range	120 to 2592000
Example	features.remote_phonebook.flash_time = 1800

LDAP

Parameter- ldap.enable	Configuration File <y000000000028>.cfg
Description	Enables or disables the LDAP feature on the IP phone.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	ldap.enable =1

Parameter- ldap.name_filter	Configuration File <y000000000028>.cfg
Description	Specifies the name attribute for LDAP searching. The "*" symbol in the filter stands for any character. The "%" symbol in the filter stands for the entering string used as the prefix of the filter condition.
Format	String
Default Value	Blank
Range	Not Applicable
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 phone LCD screen.

Parameter- ldap.number_filter	Configuration File <y000000000028>.cfg
Description	Specifies the number attribute for LDAP searching. The "*" symbol in the filter stands for any character. The "%" symbol in the filter stands for the entering string used as the prefix of the filter condition.
Format	String
Default Value	Blank
Range	Not Applicable
Example	ldap.number_filter =

	(|(telephoneNumber=%)(Mobile=%)(ipPhone=%)) When the number prefix of the telephoneNumber, Mobile or ipPhone of the contact record matches the search criteria, the record will be displayed on the phone LCD screen.

Parameter- ldap.host	Configuration File <y000000000028>.cfg
Description	Specifies the domain name or IP address of the LDAP server.
Format	IP Address or Domain Name
Default Value	0.0.0.0
Range	Not Applicable
Example	ldap.host = 192.168.1.20

Parameter- ldap.port	Configuration File <y000000000028>.cfg
Description	Specifies the LDAP server port.
Format	Integer
Default Value	389
Range	Not Applicable
Example	ldap.port = 390

Parameter- ldap.base	Configuration File <y000000000028>.cfg
Description	Specifies the LDAP search base which corresponds to the location in the LDAP phonebook from which the LDAP search request begins. The search base narrows the search scope and decreases directory search time.
Format	String
Default Value	Blank
Range	Not Applicable
Example	ldap.base = dc=yealink,dc=cn

Parameter- ldap.user	Configuration File <y000000000028>.cfg
Description	Specifies the user name uses to login the LDAP server. This parameter can be left blank in case the server allows anonymous to login. Otherwise you will need to provide the username to access the LDAP server.
Format	String
Default Value	Blank
Range	Not Applicable
Example	ldap.user = cn=manager,dc=yealink,dc=cn

Parameter- ldap.password	Configuration File <y000000000028>.cfg
Description	Specifies the password to login the LDAP server. This parameter can be left blank in case the server allows anonymous to login. Otherwise you will need to provide the password to access the LDAP server.
Format	String
Default Value	Blank
Range	Not Applicable
Example	ldap.password = secret

Parameter- ldap.max_hits	Configuration File <y000000000028>.cfg
Description	Specifies the maximum number of search results to be returned by the LDAP server. If the value of the "Max.Hits" is blank, the LDAP server will return all searched results. Please note that a very large value of the "Max. Hits" will slow down the LDAP search speed, therefore it should be configured according to the available bandwidth.
Format	Integer
Default Value	50
Range	1 to 32000

Example	ldap.max_hits = 60

Parameter- ldap.name_attr	**Configuration File** <y000000000028>.cfg
Description	Specifies the name attributes of each record to be returned by the LDAP server. It compresses the search results. You can configure multiple name attributes separated by space.
Format	String
Default Value	Blank
Range	Not Applicable
Example	ldap.name_attr = cn sn

Parameter- ldap.numb_attr	**Configuration File** <y000000000028>.cfg
Description	Specifies the number attributes of each record to be returned by the LDAP server. It compresses the search results. You can configure multiple number attributes separated by space.
Format	String
Default Value	Blank
Range	Not Applicable
Example	ldap.numb_attr = telephoneNumber

Parameter- ldap.display_name	**Configuration File** <y000000000028>.cfg
Description	Specifies the display name of the contact record displayed on the LCD screen. **Note**: It must start with "%" symbol.
Format	String
Default Value	Blank
Range	Not Applicable
Example	ldap.display_name = %cn The cn of the contact record is displayed on the

	LCD screen.

Parameter- ldap.version	Configuration File <y000000000028>.cfg
Description	Specifies the LDAP protocol version supported by the IP phone. Make sure the protocol value corresponds with the version assigned on the LDAP server.
Format	Integer
Default Value	3
Range	2 or 3
Example	ldap.version = 3

Parameter- ldap.call_in_lookup	Configuration File <y000000000028>.cfg
Description	Enables or disables the IP phone to perform an LDAP search when receiving an incoming call.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	ldap.call_in_lookup = 1

Parameter- ldap.ldap_sort	Configuration File <y000000000028>.cfg
Description	Enables or disables the IP phone to sort the search results in alphabetical order or numerical order.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	ldap.ldap_sort = 1

BLF

Visual and Audio Alert for BLF Pickup

Parameter-features.pickup.blf_visual_enable	Configuration File <y000000000028>.cfg
Description	Enables or disables the IP phone to display a visual prompt when the monitored user receives an incoming call.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	features.pickup.blf_visual_enable = 1

Parameter-features.pickup.blf_audio_enable	Configuration File <y000000000028>.cfg
Description	Enables or disables the IP phone to play an alert tone when the monitored user receives an incoming call.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	features.pickup.blf_audio_enable = 1

LED Off in Idle

Parameter-features.blf_and_callpark_idle_led_enable	Configuration File <y000000000028>.cfg
Description	Enables or disabled the LED off in idle feature.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	features.blf_and_callpark_idle_led_enable = 1

Music on Hold

Parameter- account.x.music_server_uri	Configuration File <MAC>.cfg
Description	Specifies the Music on Hold server address. Examples for valid values: <10.1.3.165>, 10.1.3.165, sip:moh@ucap.com, <sip:moh@ucap.com>, <yealink.com> or yealink.com. X ranges from 1 to 6. **Note**: The DNS query in this parameter only supports A query.
Format	String
Default Value	Blank
Range	Not Applicable
Example	account.1.music_server_uri =<10.1.3.165>

ACD

Parameter- account.X.acd.enable	Configuration File <MAC>.cfg
Description	Enables or disables the ACD feature for account X. X ranges from 1 to 6.
Format	Boolean
Default Value	0
Value	**0**- Disabled **1**- Enabled
Example	account.X.acd.enable = 1

Parameter- account.X.acd.available	Configuration File <MAC>.cfg
Description	Enables or disables the IP phone to display the available or unavailable soft key after the phone logs into the ACD system. X ranges from 1 to 6.
Format	Boolean

Default Value	0
Value	**0**- Disabled **1**- Enabled
Example	account.X.acd.available = 1

Parameter- account.X.acd.user_id	**Configuration File** <MAC>.cfg
Description	Configures the user ID used to log in the ACD system. X ranges from 1 to 6.
Format	String
Default Value	Blank
Value	Not Applicable
Example	account.X.acd.user_id = 3606

Parameter- account.X.acd.password	**Configuration File** <MAC>.cfg
Description	Configures the password used to log in the ACD system. X ranges from 1 to 6.
Format	String
Default Value	Blank
Value	Not Applicable
Example	account.X.acd.password = 123456

Parameter- acd.auto_available	**Configuration File** <y000000000028>.cfg
Description	Enables or disables the ACD auto available timer feature. If set to 1 (Enabled), the IP phone automatically changes the phone status to available.
Format	Boolean
Default Value	0
Value	**0**- Disabled **1**- Enabled
Example	acd.auto_available = 1

Parameter- acd.auto_available_timer	Configuration File <y000000000028>.cfg
Description	Specifies the length of time (in seconds) before the IP phone state is automatically reset to “available”.
Format	Integer
Default Value	60
Value	0 to 120
Example	acd.auto_available_timer = 80

Message Waiting Indicator

Parameter- account.x.subscribe_mwi	Configuration File <MAC>.cfg
Description	Enables or disables the IP phone to subscribe the message waiting indicator for account X. If set to 1 (Enabled), the IP phone sends a SUBSCRIBE message to the server for message-summary updates. X ranges from 1 to 6.
Format	Boolean
Default Value	0
Value	**0**-Disabled **1**-Enabled
Example	account.1.subscribe_mwi = 0

Parameter- account.x.subscribe_mwi_expires	Configuration File <MAC>.cfg
Description	Configures MWI subscribe expiry time (in seconds) for account X. The IP phone is able to successfully refresh the SUBCRIBE for message-summary events before expiration of the SUBSCRIBE dialog. X ranges from 1 to 6. **Note**: It works only if the parameter “account.x.subscribe_mwi” is set to 1

	(Enabled).
Format	Integer
Default Value	3600
Value	0 to 84600
Example	account.1.subscribe_mwi_expires = 3600

Parameter- account.X.subscribe_mwi_to_vm	**Configuration File** <MAC>.cfg
Description	Enables or disables a subscription to the voice mail number for MWI service for account X. X ranges from 1 to 6.
Format	Boolean
Default Value	0
Value	**0**-Disabled **1**-Enabled
Example	account.1.subscribe_mwi_to_vm = 1

Parameter- voice_mail.number.X	**Configuration File** <MAC>.cfg
Description	Configures the voice mail number for account X. X ranges from 1 to 6. **Note**: It works only if the parameter "account.X.subscribe_mwi_to_vm" is set to 1 (Enabled).
Format	String
Default Value	Black
Value	Not Applicable
Example	voice_mail.number.1 = 3606

Sending RTP Stream

Parameter- multicast.codec	Configuration File <y000000000028>.cfg
Description	Specifies a multicast codec for the IP phone to use to send an RTP stream.
Format	string
Default Value	G722
Range	**Valid values are:** • PCMU • PCMA • G729 • G722 • G726-16 • G726-24 • G726-32 • G726-40 • G723_53
Example	multicast.codec = G722

Receiving RTP Stream

Parameter- multicast.receive_priority.enable	Configuration File <y000000000028>.cfg
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. If 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.
Format	Boolean
Default Value	1
Range	**0**-Disabled **1**-Enabled

Example	multicast.receive_priority.enable =1

Parameter- multicast.receive_priority.priority	**Configuration File** < y000000000028 >.cfg
Description	Configures the priority of multicast paging calls. 1 is the highest priority, 10 is the lowest priority. If set to 0, all incoming multicast paging calls will be automatically ignored.
Format	Integer
Default Value	10
Range	0 to10
Example	multicast.receive_priority.priority = 10

Parameter- multicast.listen_address.x.label	**Configuration File** < y000000000028 >.cfg
Description	Configures the label to be displayed on the LCD screen when receiving the RTP multicast. X ranges from 1 to 10.
Format	String
Default Value	Blank
Range	Not Applicable
Example	multicast.listen_address.1.label = 10

Parameter- multicast.listen_address.x.ip_address	**Configuration File** < y000000000028 >.cfg
Description	Configures the multicast address and port number that the IP phone listens to. X ranges from 1 to 10. **Note**: The valid multicast IP addresses range from 224.0.0.0 to 239.255.255.255.
Format	String

Default Value	Blank
Range	Not Applicable
Example	multicast.listen_address.1.ip_address = 224.5.6.20:10008

Action URL

Parameter-	Configuration File
action_url.setup_completed = action_url.log_on = action_url.log_off = 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 =	<y000000000028>.cfg

action_url.ip_change = action_url.forward_incoming_call = action_url.reject_incoming_call = action_url.call_interrupt = action_url.call_remote_busy = action_url.call_remote_canceled = action_url.answer_new_incoming_call = action_url.reject_new_incoming_call= action_url.cancel_callout = action_url.remote_busy = action_url.transfer_finished = action_url.transfer_failed =	
Description	Specifies the URL for the predefined event. The value format is: http://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 • $display_remote • $call_id
Format	URL
Default Value	Not Applicable
Range	Not Applicable
Example	action_url.mute = http://192.168.0.20/help.xml?model=$model

Action URI

Parameter- features.action_uri_limit_ip	Configuration File <y000000000028>.cfg
Description	Specifies the address(es) from which Action URI will be accepted. For discontinuous IP addresses, each IP address is separated by comma. 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 cannot receive or handle any HTTP GET request. If set to "any", the IP phone accepts and handles HTTP GET requests from any IP address.
Format	IP Address
Default Value	Blank
Range	IP address or any
Example	features.action_uri_limit_ip = any

Server Redundancy

Parameter- account.x.naptr_build	Configuration File <MAC>.cfg
Description	Specifies the type of the SRV query when the NAPTR query returns no result. X ranges from 1 to 6.
Format	Integer
Default Value	0
Range	**Valid values are:** **0**-UDP **1**-Mutiple Types

Example	account.1.naptr_build = 3

Parameter- account.x.fallback.redundancy_ty pe	**Configuration File** <MAC>.cfg
Description	Configures the registration mode for the IP phone in fallback mode. X ranges from 1 to 6.
Format	Integer
Default Value	0
Range	**Valid values are:** **0**-Concurrent registration **1**-Successive registration
Example	account.1.fallback.redundancy_type = 1

Parameter- account.x.fallback.timeout	**Configuration File** <MAC>.cfg
Description	Configures the time interval (in seconds) for the IP phone to detect whether the working server is available by sending the registration request after the fallback server takes over the call control. It is only applicable to successive registration mode. X ranges from 1 to 6.
Format	Integer
Default Value	120
Range	10 to 2147483647
Example	account.1.fallback.timeout = 160

Parameter- account.x.transport	**Configuration File** <MAC>.cfg
Description	Configures the transport type for account X. 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.
Format	Integer
Default Value	0
Range	**Valid values are:** **0**-UDP **1**-TCP **2**-TLS **3**-DNS-NAPTR
Example	account.1.transport = 3

Parameter- account.x.sip_server.y.address	**Configuration File** <MAC>.cfg
Description	Configures the IP address or domain name of the SIP server. X ranges from 1 to 6. Y ranges from 1 to 2.
Format	IP Address or Domain Name
Default Value	Blank
Range	Not Applicable
Example	account.1.sip_server.1.address = as.yealink.com

Parameter- account.x.sip_server.y.port	**Configuration File** <MAC>.cfg
Description	Configures the SIP server port. X ranges from 1 to 6. Y ranges from 1 to 2.
Format	Integer
Default Value	5060
Range	0 to 65535
Example	account.1.sip_server.1.port = 5060

Parameter- account.1.sip_server.1.expires	Configuration File <MAC>.cfg
Description	Configures the registration expires (in seconds). X ranges from 1 to 6. Y ranges from 1 to 2.
Format	Integer
Default Value	3600
Range	30 to 2147483647
Example	account.1.sip_server.1.expires = 3500

Parameter- account.x.sip_server.y.transport_type	Configuration File <MAC>.cfg
Description	Configures the transport type for the SIP server. X ranges from 1 to 6. Y ranges from 1 to 2.
Format	Integer
Default Value	0
Range	**Valid values are:** **0**-UDP **1**-TCP **2**-TLS **3**-DNS-NAPTR
Example	account.1.sip_server.1.transport_type = 3

Parameter- account.x.sip_server.y.retry_counts	Configuration File <MAC>.cfg
Description	Configures the retry times for the IP phone to resend requests when the server does not respond correctly. X ranges from 1 to 6. Y ranges from 1 to 2.
Format	Integer

Default Value	3
Range	0 to 65535
Example	account.1.sip_server.1.retry_counts = 3

Parameter- account.x.sip_server.y.failback_mode	**Configuration File** <MAC>.cfg
Description	Configures the way in which the phone fails back to the primary server for call control when in the failover mode. X ranges from 1 to 6. Y ranges from 1 to 2.
Format	Integer
Default Value	0
Range	**Valid values are:** **0**-newRequests: all requests are forwarded to the primary server first, regardless of the secondary server that was used. **1**-DNSTTL: the IP phone will retry to use the primary server after the timeout of the DNSTTL configured for the SIP server. **2**-registration: the IP phone will retry to use the primary server when the SIP server's registration requires renewal. **3**-duration: the IP phone will retry to use the primary server after the timeout defined by the account.x.failback_timeout parameter.
Example	account.1.sip_server.1.failback_mode = 3

Parameter- account.x.sip_server.y.failback_timeout	**Configuration File** <MAC>.cfg
Description	Configures the time interval (in seconds) for the IP phone to detect whether the primary server is available by sending the registration request after the secondary server takes over the call control.

	X ranges from 1 to 6. Y ranges from 1 to 2.
Format	Integer
Default Value	3600
Range	0 to 65535
Example	account.1.sip_server.1.failback_timeout = 3200

Parameter- account.x.sip_server.y.register_on_enable	**Configuration File** <MAC>.cfg
Description	Enables or disables the IP phone to register to the secondary server before sending requests to the secondary server in the failover mode. X ranges from 1 to 6. Y ranges from 1 to 2.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	account.1.sip_server.1.register_on_enable = 1

LLDP

Parameter- network.lldp.enable	**Configuration File** <y000000000028>.cfg
Description	Enables or disables the LLDP feature on the IP phone. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Boolean
Default Value	1
Range	**0**-Disabled **1**-Enabled

Example	network.lldp.enable = 1

Parameter- network.lldp.packet_interval	**Configuration File** <y000000000028>.cfg
Description	Configures the amount of time (in seconds) between the transmissions of LLDP packet. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. It works only if the parameter "network.lldp.enable" is set to 1 (Enabled).
Format	Integer
Default Value	60
Range	1 to 3600
Example	network.lldp.packet_interval = 150

VLAN

Internet Port

Parameter- network.vlan.internet_port_enable	**Configuration File** <y000000000028>.cfg
Description	Enables or disables the IP phone to insert VLAN tag on packet from the Internet port. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	network.vlan.internet_port_enable = 1

Parameter- network.vlan.internet_port_vid	**Configuration File** <y000000000028>.cfg
Description	Configures the VLAN ID that is associated with the particular VLAN.

	Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer
Default Value	0
Range	0 to 4094
Example	network.vlan.internet_port_vid = 1

Parameter- network.vlan.internet_port_priority	**Configuration File** <y000000000028>.cfg
Description	Specifies the priority value used for passing VLAN packets. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer
Default Value	0
Range	0 to 7
Example	network.vlan.internet_port_priority = 1

PC Port

Parameter- network.vlan.pc_port_enable	**Configuration File** <y000000000028>.cfg
Description	Enables or disables the IP phone to insert VLAN tag on packet from the PC port. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	network.vlan.pc_port_enable = 1

Parameter- network.vlan.pc_port_vid	Configuration File <y000000000028>.cfg
Description	Configures the VLAN ID that is associated with the particular VLAN. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer
Default Value	1
Range	1 to 4094
Example	network.vlan.pc_port_vid = 1

Parameter- network.vlan.pc_port_priority	Configuration File <y000000000028>.cfg
Description	Specifies the priority value used for passing VLAN packets. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer
Default Value	0
Range	0 to 7
Example	network.vlan.pc_port_priority = 1

DHCP VLAN Discovery

Parameter- network.vlan.dhcp_enable	Configuration File <y000000000028>.cfg
Description	Enables or disables the DHCP VLAN discovery feature on the IP phone. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Boolean
Default Value	1
Range	**0**-Disabled **1**-Enabled

Example	network.vlan.dhcp_enable = 1

Parameter- network.vlan.dhcp_option	**Configuration File** <y000000000028>.cfg
Description	Specifies the option of the OpenVPN tar package.
Format	String
Default Value	Blank
Range	Not Applicable
Example	network.vlan.dhcp_option = 132,140,

VPN

Parameter- network.vpn_enable	**Configuration File** <y000000000028>.cfg
Description	Enables or disables the VPN feature on the IP phone. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	network.vpn_enable = 1

Parameter- openvpn.url	**Configuration File** <y000000000028>.cfg
Description	Specifies the access URL of the OpenVPN tar package.
Format	String
Default Value	Blank
Range	Not Applicable
Example	openvpn.url = http://192.168.10.25/OpenVPN.tar

QoS

Parameter- network.qos.rtptos	Configuration File <y000000000028>.cfg
Description	Configures the DSCP for voice packets. The default DSCP value for RTP packets is 46 (Expedited Forwarding). **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer
Default Value	46
Range	0 to 63
Example	network.qos.rtptos = 50

Parameter- network.qos.signaltos	Configuration File <y000000000028>.cfg
Description	Configures the DSCP for SIP packets. The default DSCP value for SIP packets is 26 (Assured Forwarding). **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer
Default Value	26
Range	0 to 63
Example	network.qos.signaltos = 30

Network Address Translation

Parameter- account.x.nat.nat_traversal	Configuration File <MAC>.cfg
Description	Enables or disables the NAT traversal for account X. X ranges from 1 to 6.

Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	account.1.nat.nat_traversal = 1

Parameter- account.x.nat.stun_server	**Configuration File** <MAC>.cfg
Description	Specifies the IP address or the domain name of the STUN server for account X. X ranges from 1 to 6.
Format	IP Address or Domain Name
Default Value	Blank
Range	Not Applicable
Example	account.1.nat.stun_server = 192.168.1.20

Parameter- account.x.nat.stun_port	**Configuration File** <MAC>.cfg
Description	Specifies the port of the STUN server. X ranges from 1 to 6.
Format	Integer
Default Value	3478
Range	1024 to 65000
Example	account.1.nat.stun_port = 3479

SNMP

Parameter- network.snmp.enable	**Configuration File** <y000000000028>.cfg
Description	Enables or disables the SNMP feature on the IP phone. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.

Format	Boolean
Default Value	1
Range	**0**-Disabled **1**-Enabled
Example	network.snmp.enable = 0

Parameter- network.snmp.port	**Configuration File** <y000000000028>.cfg
Description	Specifies the port used for SNMP communication. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer
Default Value	161
Range	0 to 65535
Example	network.snmp.port = 1008

Parameter- network.snmp.trust_ip	**Configuration File** <y000000000028>.cfg
Description	Specifies the SNMP server addresses from which GET requests will be accepted. You can specify one or more addresses, multiple addresses are separated by space. If the value is set to “0.0.0.0”, the IP phone can accept and handle GET requests from any IP address. If the value is left blank, the IP phone cannot receive or handle any GET request. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.
Format	IP Address (IPv4 or IPv6) or Domain Name
Default Value	0.0.0.0
Range	At most 255 characters

Example	network.snmp.trust_ip = 192.168.1.50 server@manager.com

802.1X

Parameter- network.802_1x.mode	**Configuration File** <y000000000028>.cfg
Description	Specifies the types of the 802.1X authentication to use on the IP phone. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer
Default Value	0
Range	**Valid values are:** **0**-Disabled **1**-EAP-MD5 **2**-EAP-TLS **3**-PEAP-MSCHAPV2 **4**-EAP-TTLS/EAP-MSCHAPv2
Example	network.802_1x.mode = 1

Parameter- network.802_1x.identity	**Configuration File** <y000000000028>.cfg
Description	Enters the identity used for authenticating the IP phone. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.
Format	String
Default Value	Blank
Range	Not Applicable
Example	network.802_1x.identity = admin

Parameter- network.802_1x.md5_password	Configuration File <y000000000028>.cfg
Description	Enters the password used for authenticating the IP phone. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. It is only applicable to EAP-MD5, PEAP-MSCHAPV2 and EAP-TTLS/EAP-MSCHAPv2 protocols.
Format	String
Default Value	Blank
Range	Not Applicable
Example	network.802_1x.md5_password = admin123

Parameter- network.802_1x.root_cert_url	Configuration File <y000000000028>.cfg
Description	Specifies the access URL of the root certificate used for authentication. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. It is only applicable to EAP-TLS, PEAP-MSCHAPV2 and EAP-TTLS/EAP-MSCHAPv2 protocols. The format of the certificate must be *.pem, *.crt, *.cer or *.der.
Format	String
Default Value	Blank
Range	Not Applicable
Example	network.802_1x.root_cert_url = http://192.168.1.10/ca.pem

Parameter- network.802_1x.client_cert_url	Configuration File <y000000000028>.cfg
Description	Specifies the access URL of the client certificate used for authentication.

	Note: If you change this parameter, the IP phone will reboot to make the change take effect. It is only applicable to the EAP-TLS protocol. The format of the certificate must be *.pem or *.cer.
Format	String
Default Value	Blank
Range	Not Applicable
Example	network.802_1x.client_cert_url = http://192.168.1.10/ client.pem

TR-069

Parameter- managementserver.enable	**Configuration File** <y000000000028>.cfg
Description	Enables or disables the TR-069 feature on the IP phone. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	managementserver.enable = 1

Parameter- managementserver.username	**Configuration File** <y000000000028>.cfg
Description	Enters the username to authenticate with the ACS. This string is set to the empty string if no authentication is required. **Note:** If you change this parameter, the phone will reboot to make the change take effect.
Format	String
Default Value	Blank
Range	Not Applicable

Example	managementserver.username = user1

Parameter-managementserver.password	Configuration File <y000000000028>.cfg
Description	Enters the password to authenticate with the ACS. This string is set to the empty string if no authentication is required. **Note:** If you change this parameter, the phone will reboot to make the change take effect.
Format	String
Default Value	Blank
Range	Not Applicable
Example	managementserver.password = pwd123

Parameter-managementserver.url	Configuration File <y000000000028>.cfg
Description	Specifies the URL of the ACS. **Note:** If you change this parameter, the phone will reboot to make the change take effect.
Format	String
Default Value	Blank
Range	Not Applicable
Example	managementserver.url = http://192.168.1.20/acs/

Parameter-managementserver.connection_request_username	Configuration File <y000000000028>.cfg
Description	Sets the username for the IP phone to authenticate the incoming connection requests. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.
Format	String
Default Value	Blank

Range	Not Applicable
Example	managementserver.connection_request_username = acsuser

Parameter- managementserver.connection_request_password	**Configuration File** <y000000000028>.cfg
Description	Sets the password for the IP phone to authenticate the incoming connection requests. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.
Format	String
Default Value	Blank
Range	Not Applicable
Example	managementserver.connection_request_password = acspwd

Parameter- managementserver.periodic_inform_enable	**Configuration File** <y000000000028>.cfg
Description	Enables or disables the IP phone to periodically report its configuration information to the ACS. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Boolean
Default Value	1
Range	**0**-Disabled **1**-Enabled
Example	managementserver.periodic_inform_enable = 1

Parameter- managementserver.periodic_in	**Configuration File** <y000000000028>.cfg

form_interval	
Description	Sets the interval (in seconds) to report its configuration information to the ACS. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer
Default Value	60
Range	Not Applicable
Example	managementserver.periodic_inform_interval = 120

IPv6

Parameter- network.ip_address_mode	**Configuration File** <y000000000028>.cfg
Description	Specifies the IP address mode. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer
Default Value	0
Range	**Valid values are:** **0**-IPv4 **1**-IPv6 **2**-IPv4&IPv6
Example	network.ip_address_mode = 2

Parameter- network.ipv6_internet_port.type	**Configuration File** <y000000000028>.cfg
Description	Specifies the IPv6 address assignment method. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer

Default Value	0
Range	**Valid values are:** **0**-DHCP **1**-Static
Example	network.ipv6_internet_port.type = 1

Parameter- network.ipv6_internet_port.ip	**Configuration File** <y000000000028>.cfg
Description	Configures the IPv6 address. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.
Format	IP Address
Default Value	Blank
Range	Not Applicable
Example	network.ipv6_internet_port.ip = 2026:1234:1:1:215:65ff:fe1f:caa

Parameter- network.ipv6_prefix	**Configuration File** <y000000000028>.cfg
Description	Specifies the prefix of the IPv6 address. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer
Default Value	64
Range	0 to 128
Example	network.ipv6_prefix = 68

Parameter- network.ipv6_internet_port.gateway	**Configuration File** <y000000000028>.cfg
Description	Configures the gateway when the Internet port type is defined as Static IP Address. **Note:** If you change this parameter, the IP

	phone will reboot to make the change take effect.
Format	IP Address
Default Value	Blank
Range	Not Applicable
Example	network.ipv6_internet_port.gateway = 3036:1:1:c3c7:c11c:5447:23a6:255

Parameter- network.ipv6_primary_dns	**Configuration File** <y000000000028>.cfg
Description	Configures the primary DNS server when the Internet port type is defined as Static IP Address. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.
Format	IP Address
Default Value	Blank
Range	Not Applicable
Example	network.ipv6_primary_dns = 3036:1:1:c3c7:c11c:5447:23a6:256

Parameter- network.ipv6_secondary_dns	**Configuration File** <y000000000028>.cfg
Description	Configures the secondary DNS server when the Internet port type is defined as Static IP Address. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.
Format	IP Address
Default Value	Blank
Range	Not Applicable
Example	network.ipv6_secondary_dns = 2026:1234:1:1:c3c7:c11c:5447:23a6

Parameter- network.ipv6_icmp_v6.enable	Configuration File <y000000000028>.cfg
Description	Enables or disables the ICMPv6 feature. If set to 1 (enabled), the IP phone obtains the parameters of the IPv6 from the ICMPv6 protocol. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Boolean
Default Value	1
Range	**0**-Disabled **1**-Enabled
Example	network.ipv6_icmp_v6.enable = 0

Audio Feature Parameters

Head Prior

Parameter- features.headset_prior	Configuration File <y000000000028>.cfg
Description	Enables or disables the headset prior feature. If set to 1 (enabled), a user needs to press the HEADSET key to activate the headset mode. The headset mode will not be deactivated until the user presses the HEADSET key again.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	features.headset_prior = 1

Dual Headset

Parameter- features.headset_training	Configuration File <y000000000028>.cfg
Description	Enables or disables the dual headset feature. If set to 1 (Enabled), users can use two headsets on one phone. When the IP phone joins in a cal, the users with the headset connected to the headset jack have a full-duplex conversation, while the users with the headset connected to the handset jack are only allowed to listen to.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	features.headset_training = 1

Audio Codecs

Parameter- account.X.codec.Y.enable	Configuration File <MAC>.cfg
Description	Enables or disables the IP phone to use the specific codec for account X. X ranges from 1 to 6. Y ranges from 0 to 13.
Format	Boolean
Default Value	When Y=0, the default value is 1; When Y=1, the default value is 1; When Y=2, the default value is 0; When Y=3, the default value is 0; When Y=4, the default value is 1; When Y=5, the default value is 1; When Y=6, the default value is 0; When Y=7, the default value is 0; When Y=8, the default value is 0;

	When Y=9, the default value is 0; When Y=10, the default value is 0; When Y=11, the default value is 0; When Y=12, the default value is 0; When Y=13, the default value is 0.
Range	**0**-Disabled **1**-Enabled
Example	account.1.codec.1.enable = 1

Parameter- account.X.codec.Y.payload_type	**Configuration File** <MAC>.cfg
Description	Specifies the codec for account X to use. X ranges from 1 to 6. Y ranges from 0 to 13.
Format	String
Default Value	When Y=0, the default value is PCMU; When Y=1, the default value is PCMA; When Y=2, the default value is G723_53; When Y=3, the default value is G723_63; When Y=4, the default value is G729; When Y=5, the default value is G722; When Y=6, the default value is iLBC; When Y=7, the default value is G726_16; When Y=8, the default value is G726_24; When Y=9, the default value is G726_32; When Y=10, the default value is G726_40; When Y=11, the default value is iLBC_13_3; When Y=12, the default value is iLBC_15_2; When Y=13, the default value is GSM.
Range	**Valid values are:** • PCMU • PCMA • G729 • G722 • G723_53 • G723_63 • G726_16

	• G726_24 • G726_32 • G726_40 • iLBC • iLBC_13_3 • iLBC_15_2 • GSM
Example	account.1.codec.1.payload_type = G723_53

Parameter- account.X.codec.Y.priority	**Configuration File** <MAC>.cfg
Description	Specifies the priority for the codec. X ranges from 1 to 6. Y ranges from 0 to 13.
Format	Integer
Default Value	When Y=0, the default value is 1; When Y=1, the default value is 2; When Y=2, the default value is 0; When Y=3, the default value is 0; When Y=4, the default value is 3; When Y=5, the default value is 4; When Y=6, the default value is 0; When Y=7, the default value is 0; When Y=8, the default value is 0; When Y=9, the default value is 0; When Y=10, the default value is 0; When Y=11, the default value is 0; When Y=12, the default value is 0; When Y=13, the default value is 0.
Range	Not Applicable
Example	account.1.codec.1.priority = 1

Parameter- account.X.codec.Y.rtpmap	**Configuration File** <MAC>.cfg
Description	Configures the rtpmap.

	X ranges from 1 to 6. Y ranges from 0 to 13.
Format	Integer
Default Value	When Y=1, the default value is 0; When Y=1, the default value is 8; When Y=2, the default value is 4; When Y=3, the default value is 4; When Y=4, the default value is 18; When Y=5, the default value is 9; When Y=6, the default value is 102; When Y=7, the default value is 112; When Y=8, the default value is 102; When Y=9, the default value is 99; When Y=10, the default value is 104; When Y=11, the default value is 97; When Y=12, the default value is 97; When Y=13, the default value is 3.
Range	0 to 127
Example	account.1.codec.1.rtpmap = 120

Ptime

Parameter- account.x.ptime	**Configuration File** <MAC>.cfg
Description	Configures the ptime (in milliseconds) for the codec. X ranges from 1 to 6.
Format	Integer
Default Value	20
Range	**Valid values are:** 0 (Disabled) 10, 20, 30, 40, 50, 60
Example	account.1.ptime = 30

Acoustic Echo Cancellation

Parameter- voice.echo_cancellation	Configuration File <y000000000028>.cfg
Description	Enables or disables the AEC feature on the IP phone.
Format	Boolean
Default Value	1
Range	**0**-Disabled **1**-Enabled
Example	voice.echo_cancellation = 1

Voice Activity Detection

Parameter- voice.vad	Configuration File <y000000000028>.cfg
Description	Enables or disables the VAD feature on the IP phone.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled
Example	voice.vad = 1

Comfort Noise Generation

Parameter- voice.cng	Configuration File <y000000000028>.cfg
Description	Enables or disables the CNG feature on the IP phone.
Format	Boolean
Default Value	1
Range	**0**-Disabled **1**-Enabled
Example	voice.cng = 1

Jitter Buffer

Parameter- voice.jib.adaptive	**Configuration File** <y000000000028>.cfg
Description	Configures the type of jitter buffer.
Format	Integer
Default Value	1
Range	**Valid values are:** **0**-Fixed **1**-Adaptive
Example	voice.jib.adaptive = 1

Parameter- voice.jib.min	**Configuration File** <y000000000028>.cfg
Description	Configures the minimum delay time for jitter buffer. **Note**: It works only if the parameter "voice.jib.adaptive" is set to 1 (Adaptive).
Format	Integer
Default Value	0
Range	Not Applicable
Example	voice.jib.min = 1

Parameter- voice.jib.max	**Configuration File** <y000000000028>.cfg
Description	Configures the maximum delay time for jitter buffer. **Note**: It works only if the parameter "voice.jib.adaptive" is set to 1 (Adaptive).
Format	Integer
Default Value	300
Range	Not Applicable
Example	voice.jib.max = 200

Parameter- voice.jib.normal	Configuration File <y000000000028>.cfg
Description	Configures the fixed delay time for jitter buffer. **Note**: It works only if the parameter "voice.jib.adaptive" is set to 0 (Fixed).
Format	Integer
Default Value	120
Range	Not Applicable
Example	voice.jib.mormal = 100

Security Feature Parameters

TLS

Parameter- account.x.transport	Configuration File <MAC>.cfg
Description	Configures the transport type for account X. If set to 2 (TLS), the SIP message of this account will be encrypted after the successful TLS negotiation. X ranges from 1 to 6.
Format	Integer
Default Value	0 (UDP)
Range	**Valid values are:** **0**-UDP **1**-TCP **2**-TLS **3**-DNS-NAPTR
Example	account.1.transport = 2

Parameter- security.trust_certificates	Configuration File <y000000000028>.cfg
Description	Enables or disables the IP phone to authenticate the connecting server.

	Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Boolean
Default Value	1
Range	**0**-Disabled **1**-Enabled
Example	security.trust_certificates = 1

Parameter- security.ca_cert	**Configuration File** <y000000000028>.cfg
Description	Specifies the type of certificates the IP phone used to authenticate the connecting server. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Boolean
Default Value	0
Range	**0**-Default certificates **1**-Custom certificates **2**-All certificates
Example	security.ca_cert = 1

Parameter- security.cn_validation	**Configuration File** <y000000000028>.cfg
Description	Enables or disables the IP phone to mandatorily validate the CommonName or subjectAltName of the certificate sent by the connecting server. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Boolean
Default Value	0
Range	**0**-Disabled **1**-Enabled

Example	security.cn_validation = 1

Parameter- security.dev_cert	**Configuration File** <y000000000028>.cfg
Description	Specifies the type of certificates the IP phone sends for authentication. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Boolean
Default Value	0
Range	**0**-Default certificates **1**-Custom certificates
Example	security.dev_cert = 1

Uploading Certificates

Parameter- trusted_certificates.url	**Configuration File** <y000000000028>.cfg
Description	Specifies the access URL of the certificate used to authenticate the connecting server. **Note**: The certificate you want to upload must be in .pem, .crt, .cer or .der format.
Format	String
Default Value	Blank
Range	Not Applicable
Example	trusted_certificates.url = http://192.168.1.20/tc.crt

Parameter- server_certificates.url	**Configuration File** <y000000000028>.cfg
Description	Specifies the access URL of the certificate the IP phone sends for authentication. **Note**: The certificate you want to upload must be in .pem or .cer format.
Format	String

Default Value	Blank
Range	Not Applicable
Example	server_certificates.url = http://192.168.1.20/ca.pem

SRTP

Parameter- account.x.srtp_encryption	**Configuration File** <MAC>.cfg
Description	Configures whether to use voice encryption service. If the set to 1 (Forced), the IP phone is forced to using SRTP during a call. If set to 2 (Negotiated), the IP phone will negotiate with the other IP phone what type of encryption to utilize for the session. X ranges from 1 to 6.
Format	Integer
Default Value	0
Value	**Valid values are:** **0**-Disabled **1**-Forced **2**-Negotiated
Example	account.1.srtp_encryption = 0

Configuring AES Keys

Parameter- auto_provision.aes_key_16.com	**Configuration File** <y000000000028>.cfg
Description	Configures the AES key which is used to encrypt or decrypt the <y000000000028>.cfg file.
Format	String () >< | "& cannot be included.
Default Value	Blank
Range	16 characters

Example	auto_provision.aes_key_16.com = 0123456789abcdef

Parameter- auto_provision.aes_key_16.mac	**Configuration File** <y000000000028>.cfg
Description	Configures the AES key which is used to encrypt or decrypt the <MAC>.cfg file.
Format	String () ><| "& cannot be included.
Default Value	Blank
Range	16 characters
Example	auto_provision.aes_key_16.mac = 0123456789abmins

Upgrading the Firmware

Parameter- auto_provision.mode	**Configuration File** <y000000000028>.cfg
Description	Specifies the auto provision mode.
Format	Integer
Default Value	0
Range	**Valid values are:** **0**-Disabled **1**-Power on (when the IP phone boots) **4**-Repeatedly (at a fixed interval) **5**-Weekly (at the specified time) **6**-Power on + Repeatedly **7**-Power on + Weekly
Example	auto_provision.mode = 1

Parameter- auto_provision.schedule.periodic_ minute	**Configuration File** < y000000000028 >.cfg
Description	Sets the interval (in minutes) for the IP phone to check new configuration files. **Note**: It works only if the parameter

	"auto_provision.mode" is set to 4(Repeatedly) or 6 (Power on + Repeatedly).
Format	Integer
Default Value	1440
Range	1 to 43200
Example	auto_provision.schedule.periodic_minute = 1000

Parameter- auto_provision.schedule.time_from	**Configuration File** < y000000000028 >.cfg
Description	Configures the start time of day in 24-hour period for the IP phone to check new configuration files. **Note**: It works only if the parameter "auto_provision.mode" is set to 5(Weekly) or 7(Power on + Weekly).
Format	00:00
Default Value	00:00
Range	00:00 to 23:59
Example	auto_provision.schedule.time_from = 01:30

Parameter- auto_provision.schedule.time_to	**Configuration File** < y000000000028 >.cfg
Description	Configures the end time of day in 24-hour period for the IP phone to check new configuration files. **Note**: It works only if the parameter "auto_provision.mode" is set to 5(Weekly) or 7(Power on + Weekly).
Format	00:00
Default Value	00:00
Range	00:00 to 23:59
Example	auto_provision.schedule.time_to = 21:30

Parameter- auto_provision.schedule.dayofweek	Configuration File < y000000000028>.cfg
Description	Defines the desired day(s) of a week for the IP phone to check new configuration.
Format	Integer
Default Value	0123456
Range	**Valid values are:** **0**-Sunday **1**-Monday **2**-Tuesday **3**-Wednesday **4**-Thursday **5**-Friday **6**-Saturday
Example	auto_provision.schedule.time_to = 123

Parameter- firmware.url	Configuration File <y000000000028>.cfg
Description	Specifies the access URL of the firmware.
Format	String
Default Value	Blank
Range	Not Applicable
Example	firmware.url = http://192.168.1.20/2.70.0.50.rom

Resource Files

Access URL of Replace Rule Template

Parameter- dialplan_replace_rule.url	Configuration File <y000000000028>.cfg
Description	Specifies the access URL of the replace rule template.
Format	URL

Default Value	Blank
Range	Not Applicable
Example	dialplan_replace_rule.url = http://192.168.10.25/dialplan.xml

Access URL of Dial-now Template

Parameter- dialplan_dialnow.url	**Configuration File** <y000000000028>.cfg
Description	Specifies the access URL of the dial-now template.
Format	URL
Default Value	Blank
Range	Not Applicable
Example	dialplan_dialnow.url = http://192.168.10.25/dialnow.xml

Access URL of Softkey Layout Template

Parameter- custom_softkey_call_failed.url	**Configuration File** <y000000000028>.cfg
Description	Specifies the access URL of the customized file for the soft key presented on the phone LCD screen when in the CallFailed state.
Format	URL
Default Value	Not Applicable
Range	Not Applicable
Example	The following example uses HTTP to download the CallFailed state file from the "XMLfiles" directory on provisioning server 10.2.8.16 using 8080 port. custom_softkey_call_failed.url = http://10.2.8.16:8080/XMLfiles/CallFailed.xml

Parameter- custom_softkey_call_in.url	Configuration File <y000000000028>.cfg
Description	Specifies the access URL of the customized file for the soft key presented on the phone LCD screen when in the CallIn state.
Format	URL
Default Value	Not Applicable
Range	Not Applicable
Example	The following example uses HTTP to download the CallIn state file from the "XMLfiles" directory on provisioning server 10.2.8.16 using 8080 port. custom_softkey_call_in.url = http://10.2.8.16:8080/XMLfiles/CallIn.xml

Parameter- custom_softkey_connecting.url	Configuration File <y000000000028>.cfg
Description	Specifies the access URL of the customized file for the soft key presented on the phone LCD screen when in the Connecting state.
Format	URL
Default Value	Not Applicable
Range	Not Applicable
Example	The following example uses HTTP to download the Connecting state file from the "XMLfiles" directory on provisioning server 10.2.8.16 using 8080 port. custom_softkey_connecting.url = http://10.2.8.16:8080/XMLfiles/Connecting.xml

Parameter- custom_softkey_dialing.url	Configuration File <y000000000028>.cfg
Description	Specifies the access URL of the customized file for the soft key presented on the phone LCD screen when in the Dialing state.

Format	URL
Default Value	Not Applicable
Range	Not Applicable
Example	The following example uses HTTP to download the Dialing state file from the "XMLfiles" directory on provisioning server 10.2.8.16 using 8080 port. custom_softkey_dialing.url = http://10.2.8.16:8080/XMLfiles/Dialing.xml

Parameter- custom_softkey_ring_back.url	**Configuration File** <y000000000028>.cfg
Description	Specifies the access URL of the customized file for the soft key presented on the phone LCD screen when in the RingBack state.
Format	URL
Default Value	Not Applicable
Range	Not Applicable
Example	The following example uses HTTP to download the RingBack state file from the "XMLfiles" directory on provisioning server 10.2.8.16 using 8080 port. custom_softkey_ring_back.url = http://10.2.8.16:8080/XMLfiles/RingBack.xml

Parameter- custom_softkey_talking.url	**Configuration File** <y000000000028>.cfg
Description	Specifies the access URL of the customized file for the soft key presented on the phone LCD screen when in the Talking state.
Format	URL
Default Value	Not Applicable
Range	Not Applicable
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

Access URL of Local Contact File

Parameter- local_contact.data.url	Configuration File <y000000000028>.cfg
Description	Specifies the access URL of the local contact file.
Format	URL
Default Value	Blank
Range	Not Applicable
Example	local_contact.data.url = http://192.168.10.25/contactData1.xml

Access URL of Remote XML Phonebook

Parameter- remote_phonebook.data.x.url	Configuration File <y000000000028>.cfg
Description	Specifies the access URL of the remote XML phonebook. X ranges from 1 to 5.
Format	URL
Default Value	Blank
Range	Not Applicable
Example	remote_phonebook.data.1.url = http://192.168.1.20/phonebook.xml

Access URL of Wallpaper Image

Parameter- wallpaper_upload.url	Configuration File <y000000000028>.cfg
Description	Specifies the access URL of the wallpaper

	image.
Format	URL
Default Value	Blank
Range	Not Applicable
Example	wallpaper_upload.url = http://192.168.10.25/wallpaper.jpg

Troubleshooting

Log Settings

Parameter- syslog.server	**Configuration File** <y000000000028>.cfg
Description	Specifies the IP address of the syslog server where to export the log files. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.
Format	IP Address
Default Value	Blank
Range	Not Applicable
Example	syslog.server = 192.168.1.50

Parameter- syslog.log_level	**Configuration File** <y000000000028>.cfg
Description	Specifies the severity level of the logs to be reported to a log file. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.
Format	Integer
Default Value	3
Range	0 to 6
Example	syslog.log_level = 2

Watch Dog

Parameter- watch_dog.enable	Configuration File <y000000000028>.cfg
Description	Enables or disables the Watch Dog feature.
Format	Boolean
Default Value	1
Range	**0**-Disabled **1**-Enabled
Example	watch_dog.enable = 1

Configuring DSS Key

This section provides the DSS key parameters you can configure on the IP phone.

Various key features can be assigned to the DSS key. The parameters of the DSS key are detailed in the following:

Parameter- linekey.x.line	Configuration File <y000000000028>.cfg
Description	Specifies the desired line to apply the key feature. X ranges from 1 to 27. The value 0 stands for **Auto** (the first available line). **0 stands for Line1 when assigning the following features:** • BLF • Call Park • Directed Pickup • ACD • Voice Mail • Custom Button **When assigning the following features, you do not need to configure this parameter:** • DTMF • Prefix • Local Group • XML Group • XML Browser

	• LDAP • Conference • Forward • Hold • DND • Call Return • SMS • Record • URL Record • Multicast Paging • Group Listening • Private Hold • Zero Touch • URL • Keypad Lock • Favorite
Format	Integer
Default Value	0 (Auto)
Range	**Valid values are**: 0 to 6
Example	linekey.1.line = 2

Parameter- linekey.x.value	**Configuration File** <y000000000028>.cfg
Description	Specifies the value for some key features. X ranges from 1 to 27.
Format	String
Default Value	Blank
Range	Not Applicable
Example	When assigning the Speed Dial to the line key, this parameter is used to specify the number you want to dial out. linekey.1.value = 1001

Parameter- linekey.x.pickup_value	**Configuration File** <y000000000028>.cfg
Description	Specifies the pickup code for the BLF

	feature. This parameter only applies to the BLF feature. X ranges from 1 to 27.
Format	String
Default Value	Blank
Range	Not Applicable
Example	linekey.1.pickup_value = *88

Parameter- linekey.x.type	**Configuration File** <y000000000028>.cfg
Description	Specifies the key feature for the line key. X ranges from 1 to 27. **Valid types are:** • N/A (default for line key 7-27) • Conference • Forward • Transfer • Hold • DND • Call Return • SMS • Call Pickup • Call Park • DTMF • Voicemail • Speed Dial • Intercom • Line (default for line key 1-6) • BLF • URL • Group Listening • Hot Desking • XML Group • Group Pickup • Multicast Paging • Record • XML Browser • URL Record • LDAP

	• Prefix • Zero Touch • ACD • Local Group • Keypad Lock • Custom Button • Favorite
Format	Integer
Default Value	0 (N/A)
Range	**Valid values are:** **0**-N/A(default for line key 7-27) **1**-Conference **2**-Forward **3**-Transfer **4**-Hold **5**-DND **7**-Call Return **8**-SMS **9**-Call Pickup **10**-Call Park **11**-DTMF **12**-Voicemail **13**-SpeedDial **14**-Intercom **15**-Line(default for line key 1-6) **16**-BLF **17**-URL **18**-Group Listening **22**-XML Group **23**-Group Pickup **24**-Multicast Paging **25**-Record **27**-XML browser **34**-Hot Desking **35**-URL Record **38**-LDAP **40**-Prefix **41**-Zero Touch **42**-ACD **45**-Local Group **48**-Custom Button **50**-Keypad Lock **61**-Favorite

Example	linekey.1.type = 8

Parameter- linekey.x.xml_phonebook	Configuration File <y000000000028>.cfg
Description	Specifies the desired phonebook when multiple phonebooks are configured on the IP phone. This parameter only applies to the Local Group/XML Group features. X ranges from 1 to 27.
Format	Integer
Default Value	0
Range	Not Applicable
Example	Specify the second phonebook when there are three BroadSoft groups are configured on the IP phone. linekey.1.xml_phonebook = 2

Keypad Lock Key

Parameter- linekey.x.type	Configuration File <y000000000028>.cfg
Description	Configures a line key to be **Keypad Lock** key on the IP phone. The digit 50 stands for the key type **Keypad Lock**. X ranges from 1 to 27.
Format	Integer
Value	50
Example	linekey.1.type = 50

DND Key

Parameter- linekey.x.type	Configuration File <y000000000028>.cfg
Description	Configures a line key to be DND key on the

	IP phone. The digit **5** stands for the key type **DND**. X ranges from 1 to 27.
Format	Integer
Value	5
Example	linekey.1.type = 5

Directed Call Pickup Key

Parameter- linekey.x.type	**Configuration File** <y000000000028>.cfg
Description	Configures a line key to be directed call pickup key on the IP phone. The digit **9** stands for the key type **Call Pickup**. X ranges from 1 to 27.
Format	Integer
Value	9
Example	linekey.1.type = 9

Parameter- linekey.x.line	**Configuration File** <y000000000028>.cfg
Description	Specifies the desired line to apply the directed call pickup key. X ranges from 1 to 27.
Format	Integer
Range	**Valid values are**: 0 to 5
Example	linekey.1.line = 1

Parameter- linekey.x.value	**Configuration File** <y000000000028>.cfg
Description	Specifies the directed call pickup feature code followed by the number of monitored extension.

	X ranges from 1 to 27.
Format	String
Range	Not Applicable
Example	linekey.1.value = *971001

Group Call Pickup Key

Parameter- linekey.x.type	**Configuration File** <y000000000028>.cfg
Description	Configures a line key to be group call pickup key on the IP phone. The digit **23** stands for the key type **Group Pickup**. X ranges from 1 to 10.
Format	Integer
Value	23
Example	linekey.1.type = 23

Parameter- linekey.x.line	**Configuration File** <y000000000028>.cfg
Description	Specifies the desired line to apply the group call pickup key. X ranges from 1 to 10.
Format	Integer
Range	**Valid values are**: 0 to 6
Example	linekey.1.line = 1

Parameter- linekey.x.value	**Configuration File** <y000000000028>.cfg
Description	Specifies the group call pickup feature code. X ranges from 1 to 27.
Format	String

Range	Not Applicable
Example	linekey.1.value = *98

Call Return Key

Parameter- linekey.x.type	**Configuration File** <y000000000028>.cfg
Description	Configures a line key to be call return key on the IP phone. The digit **7** stands for the key type **Call Return**. X ranges from 1 to 27.
Format	Integer
Value	7
Example	linekey.2.type = 7

Call Park Key

Parameter- linekey.x.type	**Configuration File** <y000000000028>.cfg
Description	Configures a line key to be call park key on the IP phone. The digit **10** stands for the key type **Call Park**. X ranges from 1 to 27.
Format	Integer
Value	10
Example	linekey.2.type = 10

Parameter- linekey.x.line	**Configuration File** <y000000000028>.cfg
Description	Specifies the desired line to apply the call park key. X ranges from 1 to 27.
Format	Integer

Range	**Valid values are**: 0 to 5
Example	linekey.2.line = 0

Parameter- linekey.x.value	**Configuration File** <y000000000028>.cfg
Description	Specifies the call park feature code. X ranges from 1 to 27.
Format	String
Range	Not Applicable
Example	linekey.2.value = *99

Intercom Key

Parameter- linekey.x.type	**Configuration File** <y000000000028>.cfg
Description	Configures a line key to be the intercom key. The digit **14** stands for the key type **Intercom**. X ranges from 1 to 27.
Format	Integer
Value	14
Example	linekey.2.type = 14

Parameter- linekey.x.line	**Configuration File** <y000000000028>.cfg
Description	Specifies the desired line to apply the intercom key. X ranges from 1 to 27.
Format	Integer
Range	**Valid values are**: 0 to 6
Example	linekey.2.line = 1

Parameter- linekey.x.value	Configuration File <y000000000028>.cfg
Description	Specifies the intercom number. X ranges from 1 to 27.
Format	String
Range	Not Applicable
Example	linekey.2.value = 1008

LDAP Key

Parameter- linekey.x.type	Configuration File <y000000000028>.cfg
Description	Configures a line key to be LDAP key on the IP phone. The digit **38** stands for the key type **LDAP**. X ranges from 1 to 27.
Format	Integer
Value	38
Example	linekey.2.type = 38

BLF Key

Parameter- linekey.x.type	Configuration File <y000000000028>.cfg
Description	Configures a line key to be BLF key on the IP phone. The digit **16** stands for the key type **BLF**. X ranges from 1 to 27.
Format	Integer
Value	16
Example	linekey.3.type = 16

Parameter- linekey.x.line	Configuration File <y000000000028>.cfg
Description	Specifies the desired line to apply the BLF

	key. X ranges from 1 to 27.
Format	Integer
Range	**Valid values are**: 0 to 5
Example	linekey.3.line = 2

Parameter- linekey.x.value	**Configuration File** <y000000000028>.cfg
Description	Specifies the number of the monitored user. X ranges from 1 to 27.
Format	String
Range	Not Applicable
Example	linekey.3.value = 1008

Parameter- linekey.x.pickup_value	**Configuration File** <y000000000028>.cfg
Description	Specifies the pickup code for the BLF feature. This parameter only applies to the BLF feature. X ranges from 1 to 27.
Format	String
Default Value	Blank
Range	Not Applicable
Example	linekey.3.pickup_value = *88

ACD Key

Parameter- linekey.x.type	**Configuration File** <y000000000028>.cfg
Description	Configures a line key to be an ACD key on the IP phone. The digit **42** stands for the key type **ACD**. X ranges from 1 to 27.

Format	Integer
Value	42
Example	linekey.2.type = 42

Parameter- linekey.x.line	**Configuration File** <y000000000028>.cfg
Description	Specifies the desired line to apply the ACD key. X ranges from 1 to 27.
Format	Integer
Range	**Valid values are**: 0 to 5
Example	linekey.2.line = 1

Multicast Paging Key

Parameter- linekey.x.type	**Configuration File** <y000000000028>.cfg
Description	Configures a line key to be a multicast paging key on the IP phone. The digit **24** stands for the key type **Multicast Paging**. X ranges from 1 to 27.
Format	Integer
Value	24
Example	linekey.2.type = 24

Parameter- linekey.x.value	**Configuration File** <y000000000028>.cfg
Description	Specifies the multicast IP address and port number. **Note**: The valid multicast IP addresses range from 224.0.0.0 to 239.255.255.255.
Format	IP Address
Range	224.0.0.0 to 239.255.255.255.

Example	linekey.3.value = 224.5.5.6:10008

Record Key

Parameter- linekey.x.type	**Configuration File** <y000000000028>.cfg
Description	Configures a line key to be a record key on the IP phone. The digit **25** stands for the key type **Record**. X ranges from 1 to 27.
Format	Integer
Value	25
Example	linekey.2.type = 25

URL Record Key

Parameter- linekey.x.type	**Configuration File** <y000000000028>.cfg
Description	Configures a line key to be a URL record key on the IP phone. The digit **35** stands for the key type **URL Record**. X ranges from 1 to 27.
Format	Integer
Value	35
Example	linekey.2.type = 35

Parameter- linekey.x.value	**Configuration File** <y000000000028>.cfg
Description	Specifies the URL to record a call. X ranges from 1 to 10.
Format	String
Default Value	Blank
Range	Not Applicable
Example	linekey.1.value =

	http://10.1.2.224/phonerecording.cgi

Hot Desking Key

Parameter- linekey.x.type	Configuration File <y000000000028>.cfg
Description	Configures a line key to be a hot desking key on the IP phone. The digit **34** stands for the key type **hot desking**. X ranges from 1 to 27.
Format	Integer
Value	34
Example	linekey.2.type = 34

Appendix D: SIP (Session Initiation Protocol)

This section describes how the Yealink SIP-T46G 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 2327—SDP: Session Description Protocol
- RFC 2387—The MIME Multipart / Related Content-type
- RFC 2976—The SIP INFO Method
- 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 3311—The Session Initiation Protocol (SIP) UPDATE Method
- RFC 3325—SIP Asserted Identity
- RFC 3515—The Session Initiation Protocol (SIP) Refer Method
- RFC 3555—MIME Type of RTP Payload Formats
- RFC 3611—RTP Control Protocol Extended reports (RTCP XR)
- RFC 3665—Session Initiation Protocol (SIP) Basic Call Flow Examples
- draft-ietf-sip-cc-transfer-05.txt—SIP Call Control - Transfer
- 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 3891—The Session Initiation Protocol (SIP) "Replaces" Header
- RFC 3892—The Session Initiation Protocol (SIP) Referred-By Mechanism
- RFC 3968—The Internet Assigned Number Authority (IANA) Header Field Parameter Registry for the Session Initiation Protocol (SIP)
- RFC 3969—The Internet Assigned Number Authority (IANA) Uniform Resource Identifier (URI) Parameter Registry for the Session Initiation Protocol (SIP)
- RFC 4028—Session Timers in the Session Initiation Protocol (SIP)
- RFC 4235—An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP)
- RFC 4662—Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists
- draft-levy-sip-diversion-04.txt—Diversion Indication in SIP
- draft-anil-sipping-bla-02.txt—Implementing Bridged Line Appearances (BLA) Using Session Initiation Protocol (SIP)
- draft-ietf-sip-privacy-04.txt—SIP Extensions for Network-Asserted Caller Identity and Privacy within Trusted Networks
- draft-levy-sip-diversion-06.txt—Diversion Indication in SIP
- draft-ietf-sipping-cc-conferencing-03.txt—SIP Call Control - Conferencing for User Agents
- draft-ietf-sipping-rtcp-summary-02.txt —Session Initiation Protocol Package for Voice Quality Reporting Event
- draft-ietf-sip-connect-reuse-04.txt—Connection Reuse in 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	The Yealink SIP-T46G IP phones support mid-call changes such as putting a call on hold as signaled by a new INVITE that contains an existing Call-ID.
ACK	Yes	
CANCEL	Yes	
BYE	Yes	
OPTIONS	Yes	
SUBSCRIBE	Yes	
NOTIFY	Yes	
REFER	Yes	
PRACK	Yes	
INFO	Yes	
MESSAGE	Yes	
UPDATE	Yes	
PUBLISH	Yes	

SIP Header

The following SIP request headers are supported:

Method	Supported	Notes
Accept	Yes	
Alert-Info	Yes	
Allow	Yes	

Method	Supported	Notes
Allow-Events	Yes	
Authorization	Yes	
Call-ID	Yes	
Call-Info	Yes	
Contact	Yes	
Content-Length	Yes	
Content-Type	Yes	
CSeq	Yes	
Diversion	Yes	
Event	Yes	
Expires	Yes	
From	Yes	
Max-Forwards	Yes	
Min-SE	Yes	
P-Asserted-Identity	Yes	
P-Preferred-Identity	Yes	
Proxy-Authenticate	Yes	
Proxy-Authorization	Yes	
RAck	Yes	
Record-Route	Yes	
Refer-To	Yes	
Referred-By	Yes	
Remote-Party-ID	Yes	
Replaces	Yes	
Require	Yes	
Route	Yes	
RSeq	Yes	
Session-Expires	Yes	
Subscription-State	Yes	
Supported	Yes	

Method	Supported	Notes
To	Yes	
User-Agent	Yes	
Via	Yes	

SIP Responses

The following SIP responses are supported:

1xx Response—Information Responses

1xx Response	Supported	Notes
100 Trying	Yes	
180 Ringing	Yes	
181 Call Is Being Forwarded	Yes	
183 Session Progress	Yes	

2xx Response—Successful Responses

2xx Response	Supported	Notes
200 OK	Yes	
202 Accepted	Yes	In REFER transfer.

3xx Response—Redirection Responses

3xx Response	Supported	Notes
300 Multiple Choices	Yes	
301 Moved Permanently	Yes	
302 Moved Temporarily	Yes	

4xx Response—Request Failure Responses

4xx Response	Supported	Notes
400 Bad Request	Yes	
401 Unauthorized	Yes	

4xx Response	Supported	Notes
402 Payment Required	Yes	
403 Forbidden	Yes	
404 Not Found	Yes	
405 Method Not Allowed	Yes	
406 Not Acceptable	No	
407 Proxy Authentication Required	Yes	
408 Request Timeout	Yes	
409 Conflict	No	
410 Gone	No	
411 Length Required	No	
413 Request Entity Too Large	No	
414 Request-URI Too Long	Yes	
415 Unsupported Media Type	Yes	
416 Unsupported URI Scheme	No	
420 Bad Extension	No	
421 Extension Required	No	
423 Interval Too Brief	Yes	
480 Temporarily Unavailable	Yes	
481 Call/Transaction Does Not Exist	Yes	
482 Loop Detected	Yes	
483 Too Many Hops	No	
484 Address Incomplete	Yes	
485 Ambiguous	No	
486 Busy Here	Yes	
487 Request Terminated	Yes	
488 Not Acceptable Here	Yes	
491 Request Pending	No	
493 Undecipherable	No	

5xx Response—Server Failure Responses

5xx Response	Supported	Notes
500 Internal Server Error	Yes	
501 Not Implemented	Yes	
502 Bad Gateway	No	
503 Service Unavailable	No	
504 Gateway Timeout	No	
505 Version Not Supported	No	

6xx Response—Global Responses

6xx Response	Supported	Notes
600 Busy Everywhere	Yes	
603 Decline	Yes	
604 Does Not Exist Anywhere	No	
606 Not Acceptable	No	

SIP Session Description Protocol (SDP) Usage

SDP Headers	Supported
v—Protocol version	Yes
o—Owner/creator and session identifier	Yes
a—Media attribute	Yes
c—Connection information	Yes
m—Media name and transport address	Yes
s—Session name	Yes
t—Active time	Yes

Appendix E: SIP Call Flows

SIP uses six request methods:

- INVITE—Indicates a user is being invited to participate in a call session.
- ACK—Confirms that the client has received a final response to an INVITE request.
- BYE—Terminates a call and can be sent by either the caller or the callee.
- CANCEL—Cancels any pending searches but does not terminate a call that has already been accepted.
- OPTIONS—Queries the capabilities of servers.
- REGISTER—Registers the address listed in the To header field with a SIP server.

The following types of responses are used by SIP and generated by the IP phone or the SIP server:

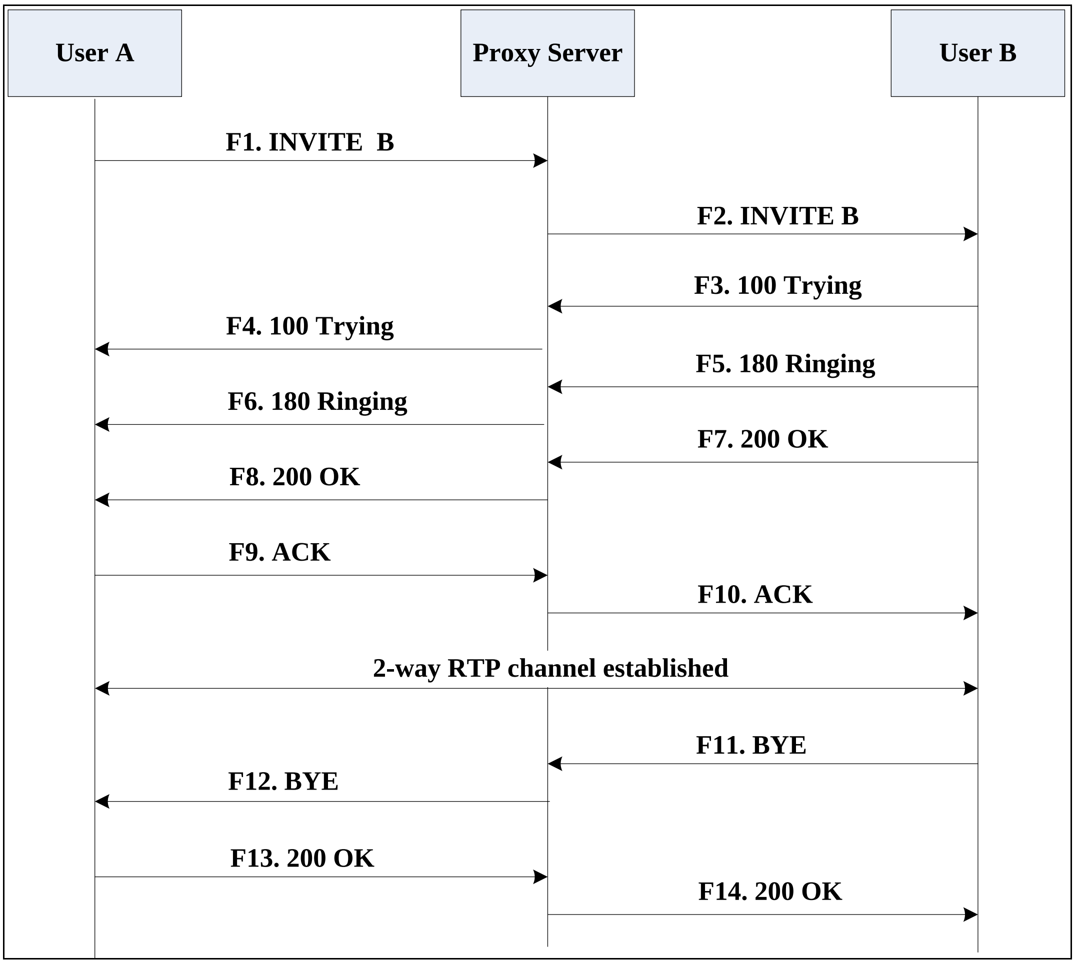
- SIP 1xx—Informational Responses
- SIP 2xx—Successful Responses
- SIP 3xx—Redirection Responses
- SIP 4xx—Client Failure Responses
- SIP 5xx—Server Failure Responses
- SIP 6xx—Global Failure Responses

Successful Call Setup and Disconnect

The following figure illustrates the scenario of a successful call. In this scenario, the two end users are User A and User B. User A and User B are located at the 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.

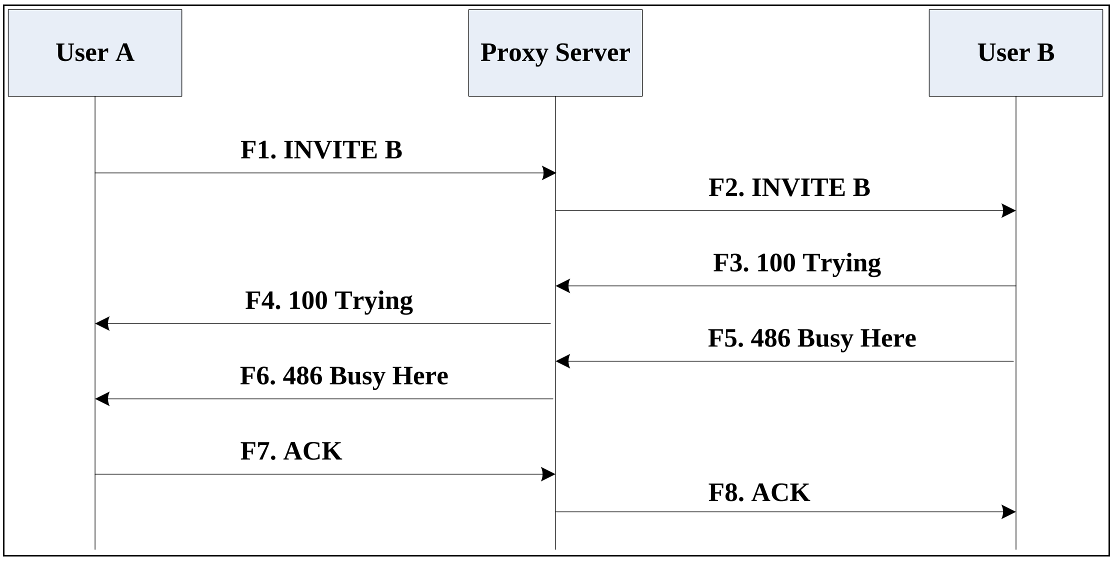
Unsuccessful Call Setup—Called User is Busy

The following figure illustrates the scenario of an unsuccessful call due to the reason of the called user being busy. In this scenario, the two end users are User A and User B. User A and User B are located at the 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.
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.

Step	Action	Description
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.

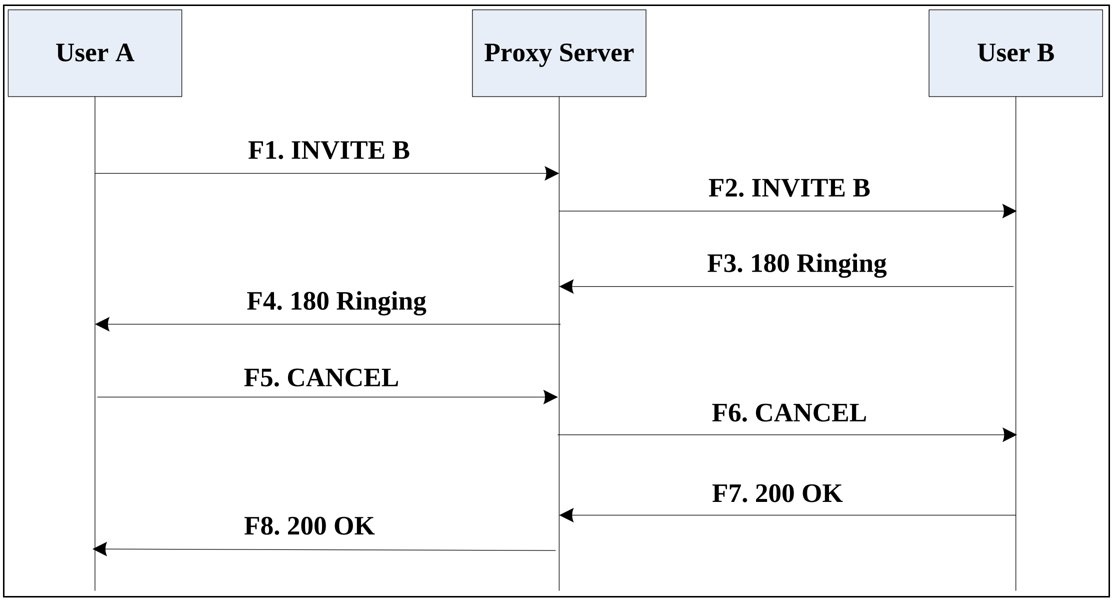
Unsuccessful Call Setup—Called User Does Not Answer

The following figure illustrates the scenario of an unsuccessful call due to the reason of the called user not answering the call. In this scenario, the two end users are User A and User B. User A and User B are located at the 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 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	The proxy server forwards the SIP CANCEL request to notify User B that

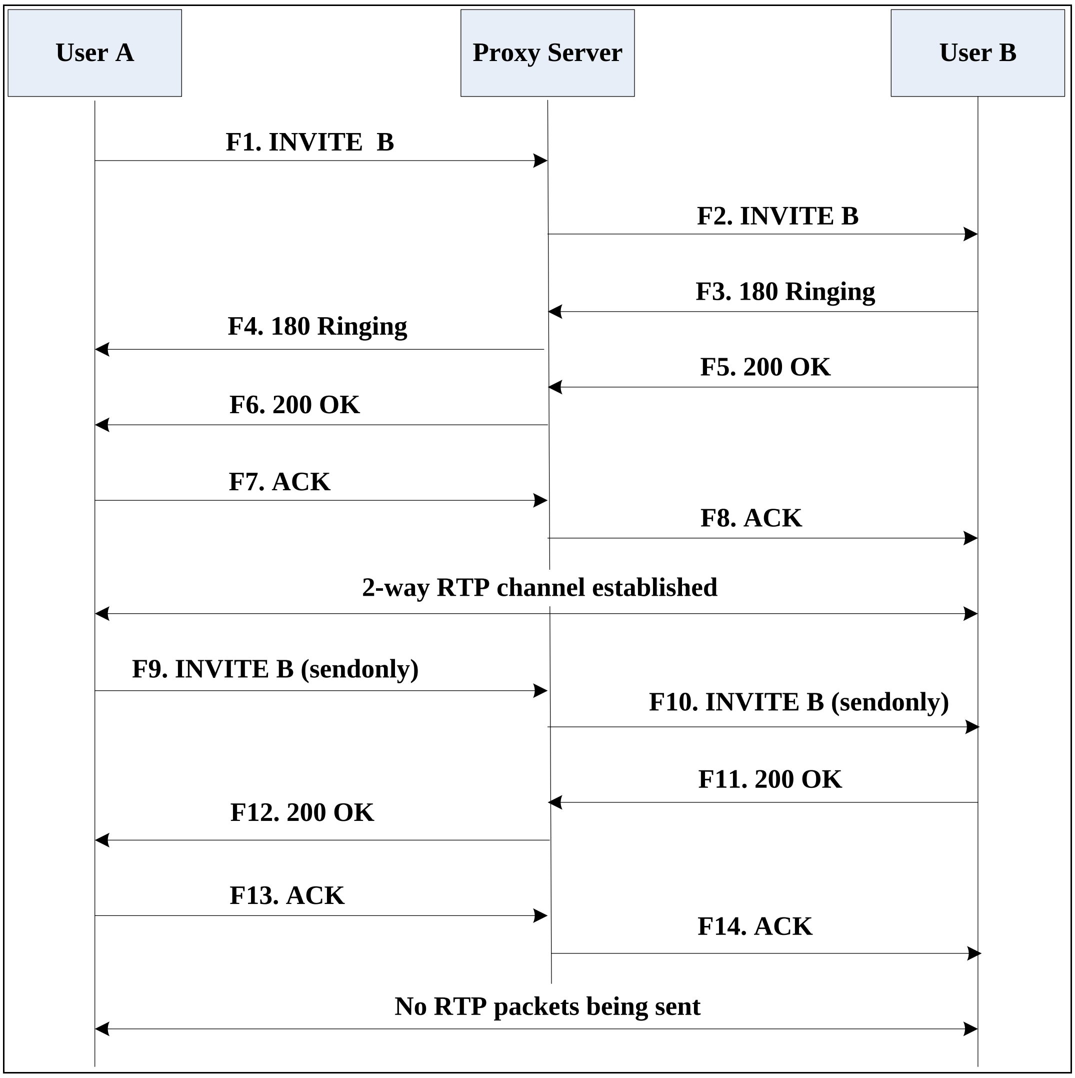
Step	Action	Description
	User B	User A wants to disconnect the call.
F7	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The SIP 200 OK response indicates that User B has received the CANCEL request.
F8	200 OK—Proxy Server to User A	The proxy server forwards the SIP 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 the Yealink SIP IP phones.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.
3. User A puts User B on hold.



Step	Action	Description
F1	INVITE—User A to Proxy Server	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 the proxy server that the connection has been made.
F6	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the connection has been made.

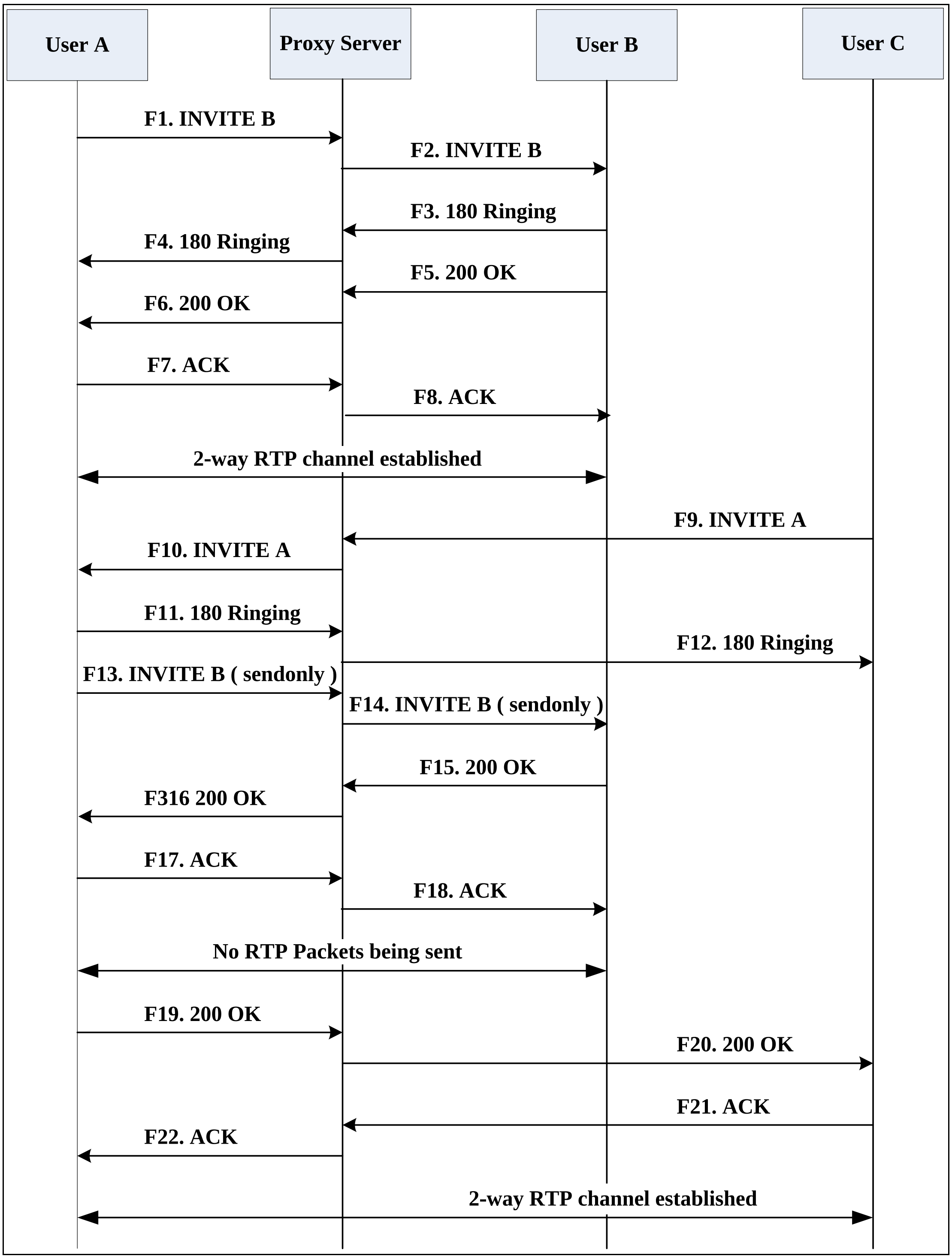
Step	Action	Description
F7	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F8	ACK—Proxy Server to User B	The proxy server sends the SIP ACK to User B. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.
F9	INVITE—User A to Proxy Server	User A sends a mid-call INVITE request to the proxy server with new SDP session parameters, which are used to place the call on hold.
F10	INVITE—Proxy Server to User B	The proxy server forwards the mid-call INVITE message to User B.
F11	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the INVITE is successfully processed.
F12	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK response to User A. The 200 OK response notifies User B is successfully put on hold.
F13	ACK—User A to Proxy Server	User A sends an ACK message to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now temporarily inactive. No RTP packets are being sent.
F14	ACK—Proxy Server to User B	The proxy server sends the ACK message to User B. The ACK confirms that the proxy server has received the 200 OK response.

Successful Call Setup and Call Waiting

The following figure illustrates a successful call between Yealink SIP IP phones in which parties are in a call, one of the participants receives a call from a third party, then answers the incoming call. 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. 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.

Step	Action	Description
F7	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server, The ACK confirms that User A has received the 200 OK response. The call session is now active.
F8	ACK—Proxy Server to User B	The proxy server sends the SIP ACK to User B. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.
F9	INVITE—User C to Proxy Server	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.

Step	Action	Description
F13	INVITE—User A to Proxy Server	User A sends a mid-call INVITE request to the proxy server with new SDP session parameters, which are used to place the call on hold.
F14	INVITE—Proxy Server to User B	The proxy server forwards the mid-call INVITE message to User B.
F15	200 OK—User B to Proxy Server	User B sends a 200 OK to the proxy server. The 200 OK response indicates that the INVITE was successfully processed.
F16	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK response to User A. The 200 OK response notifies User B is successfully put on hold.
F17	ACK—User A to Proxy Server	User A sends an ACK message to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now temporarily inactive. No RTP packets are being sent.
F18	ACK—Proxy Server to User B	The proxy server sends the ACK message to User B. The ACK confirms that the proxy server has received the 200 OK response.
F19	200 OK—User A to Proxy Server	User A sends a 200 OK response to the proxy server. The 200 OK response notifies that the connection has been made.
F20	200 OK—Proxy Server User C	The proxy server forwards the 200 OK message to User C.
F21	ACK—User C to Proxy Server	User C sends a SIP ACK to the proxy server. The ACK confirms that User C has received the 200 OK response. The call session is now active.
F22	ACK—Proxy Server to User A	The proxy server forwards the SIP ACK to User A to confirm that User C has received the 200 OK response.

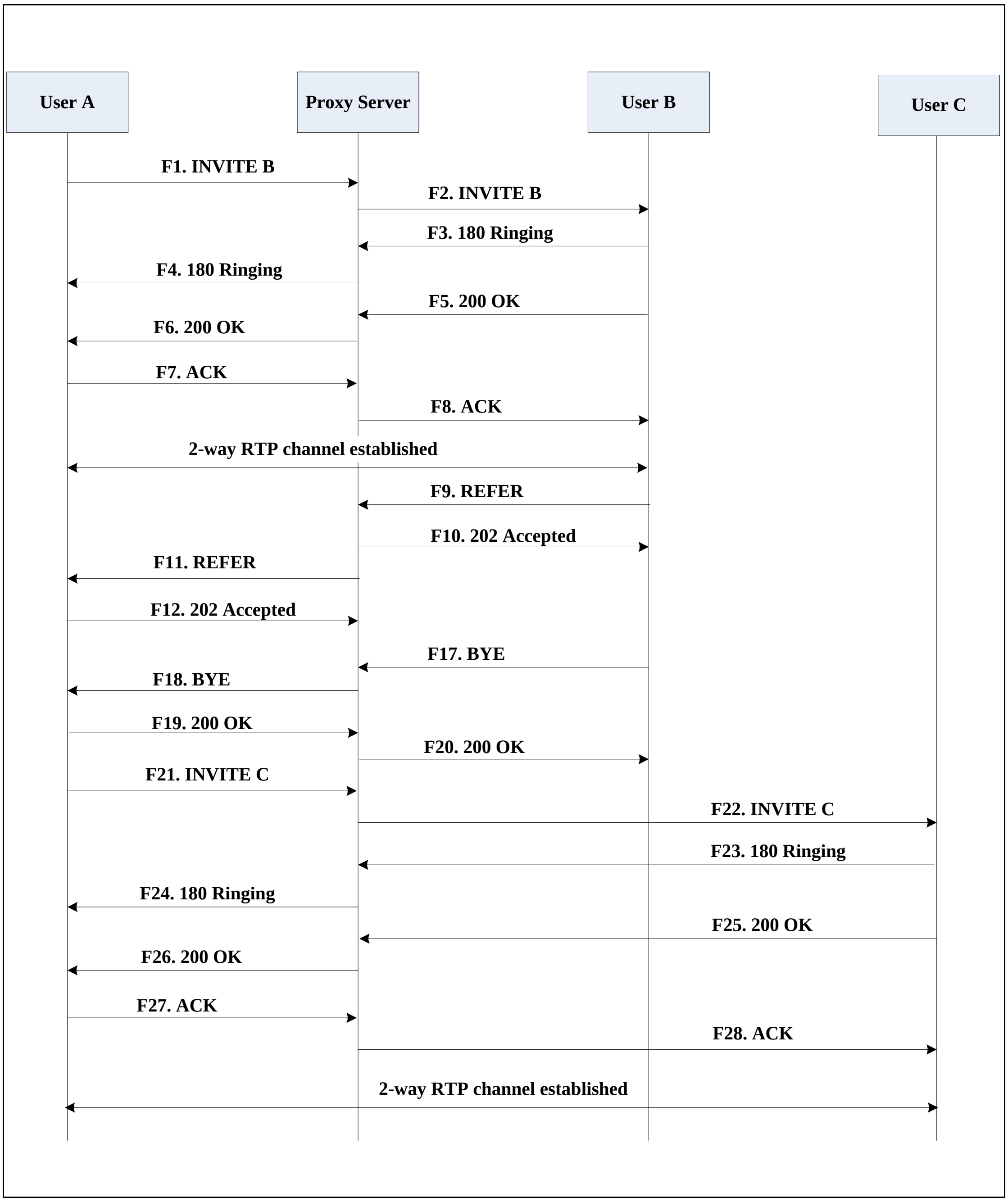
Call Transfer without Consultation

The following figure illustrates a successful call between Yealink SIP IP phones in which two parties are in a call and then one of the parties transfers the call to a third party without consulting the third party. 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.


User A
Proxy Server
User B
User C
F1. INVITE B
F2. INVITE B
F3. 180 Ringing
F4. 180 Ringing
F5. 200 OK
F6. 200 OK
F7. ACK
F8. ACK
2-way RTP channel established
F9. REFER
F10. 202 Accepted
F11. REFER
F12. 202 Accepted
F17. BYE
F18. BYE
F19. 200 OK
F20. 200 OK
F21. INVITE C
F22. INVITE C
F23. 180 Ringing
F24. 180 Ringing
F25. 200 OK
F26. 200 OK
F27. ACK
F28. ACK
2-way RTP channel established

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 connection has been made.

Step	Action	Description
F7	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server, The ACK confirms that User A has received the 200 OK response. The call session is now active.
F8	ACK—Proxy Server to User B	The proxy server sends the SIP ACK to User B. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.
F9	REFER—User B to Proxy Server	User B sends a REFER message to the proxy server. User B performs a blind transfer of User A to User C.
F10	202 Accepted—Proxy Server to User B	The proxy server sends a SIP 202 Accept response to User B. The 202 Accepted response notifies User B that the proxy server has received the REFER message.
F11	REFER—Proxy Server to User A	The proxy server forwards the REFER message to User A.
F12	202 Accepted—User A to Proxy Server	User A sends a SIP 202 Accept response to the proxy server. The 202 Accepted response indicates that User A accepts the transfer.
F13	BYE—User B to Proxy Server	User B terminates the call session by sending a SIP BYE request to the proxy server. The BYE request indicates that User B wants to release the call.
F14	BYE—Proxy Server to User A	The proxy server forwards the BYE request to User A.
F15	200OK—User A to Proxy Server	User A sends a SIP 200 OK response to the proxy server. The 200 OK response confirms that User A has received the BYE request.
F16	200OK—Proxy Server to User B	The proxy server forwards the SIP 200 OK response to User B.
F17	INVITE—User A to Proxy Server	User A sends a SIP INVITE request to the proxy server. In the INVITE request, a unique Call-ID is generated and the Contact-URI field indicates that User A

Step	Action	Description
		requests the call.
F18	INVITE—Proxy Server to User C	The proxy server maps the SIP URI in the To field to User C.
F19	180 Ringing—User C to Proxy Server	User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F20	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User C is being alerted
F21	200OK—User C to Proxy Server	User C sends a SIP 200 OK response to the proxy server. The 200 OK response notifies the proxy server that the connection has been made.
F22	200OK—Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A.
F23	ACK— User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F24	ACK—Proxy Server to User C	The proxy server forwards the ACK message to User C. The ACK confirms that User A has received the 200 OK response. The call session is now active.

Call Transfer with Consultation

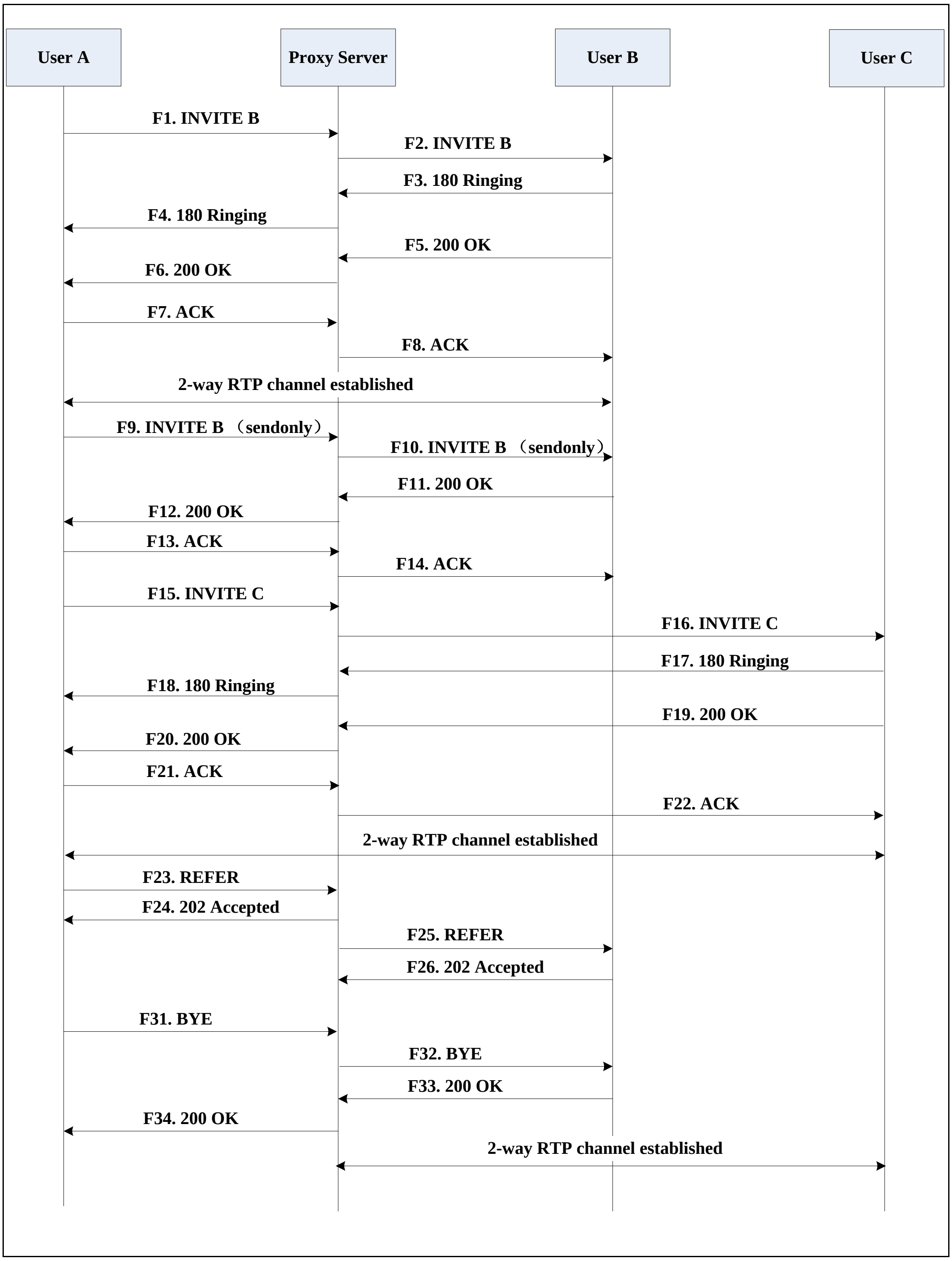
The following figure illustrates a successful call between Yealink SIP IP phones in which two parties are in a call and then one of the parties transfers the call to the third party with consultation. This is called attended transfer. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.
3. User A calls User C.
4. User C answers the call.

5. User A transfers the call to User C.

   Call is established between User B and User C.



Step	Action	Description
F1	INVITE—User A to Proxy Server	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 connection has been made.

Step	Action	Description
F7	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server, The ACK confirms that User A has received the 200 OK response. The call session is now active.
F8	ACK—Proxy Server to User B	The proxy server sends the SIP ACK to User B. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.
F9	INVITE—User A to Proxy Server	User A sends a mid-call INVITE request to the proxy server with new SDP session parameters, which are used to place the call on hold.
F10	INVITE—Proxy Server to User B	The proxy server forwards the mid-call INVITE message to User B.
F11	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the INVITE was successfully processed.
F12	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK response to User A. The 200 OK response notifies User B is successfully put on hold.
F13	ACK—User A to Proxy Server	User A sends an ACK message to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now temporarily inactive. No RTP packets are being sent.
F14	ACK—Proxy Server to User B	The proxy server sends the ACK message to User B. The ACK confirms that the proxy server has received the 200 OK response.
F15	INVITE—User A to Proxy Server	User A sends a SIP INVITE request to the proxy server. In the INVITE request, a unique Call-ID is generated and the Contact-URI field indicates that User A requests the call.
F16	INVITE—Proxy Server to User	The proxy server maps the SIP URI to in the To field to User C. The proxy server

Step	Action	Description
	C	sends the INVITE request to User C.
F17	180 Ringing—User C to Proxy Server	User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F18	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User C is being alerted.
F19	200OK—User C to Proxy Server	User C sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F20	200OK—Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A. The 200 OK response notifies User A that the connection has been made.
F21	ACK— User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F22	ACK—Proxy Server to User C	The proxy server forwards the ACK message to User C. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.
F23	REFER—User A to Proxy Server	User A sends a REFER message to the proxy server. User A performs a transfer of User B to User C.
F24	202 Accepted—Proxy Server to User A	The proxy server sends a SIP 202 Accepted response to User A. The 202 Accepted response notifies User A that the proxy server has received the REFER message.
F25	REFER—Proxy Server to User B	The proxy server forwards the REFER message to User B.
F26	202 Accepted—User B to Proxy Server	User B sends a SIP 202 Accept response to the proxy server. The 202 Accepted

Step	Action	Description
		response indicates that User B accepts the transfer.
F27	BYE—User A to Proxy Server	User A terminates the call session by sending a SIP BYE request to the proxy server. The BYE request indicates that User A wants to release the call.
F28	BYE—Proxy Server to User B	The proxy server forwards the BYE request to User B.
F29	200OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that User B has received the BYE request.
F30	200OK—Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A.

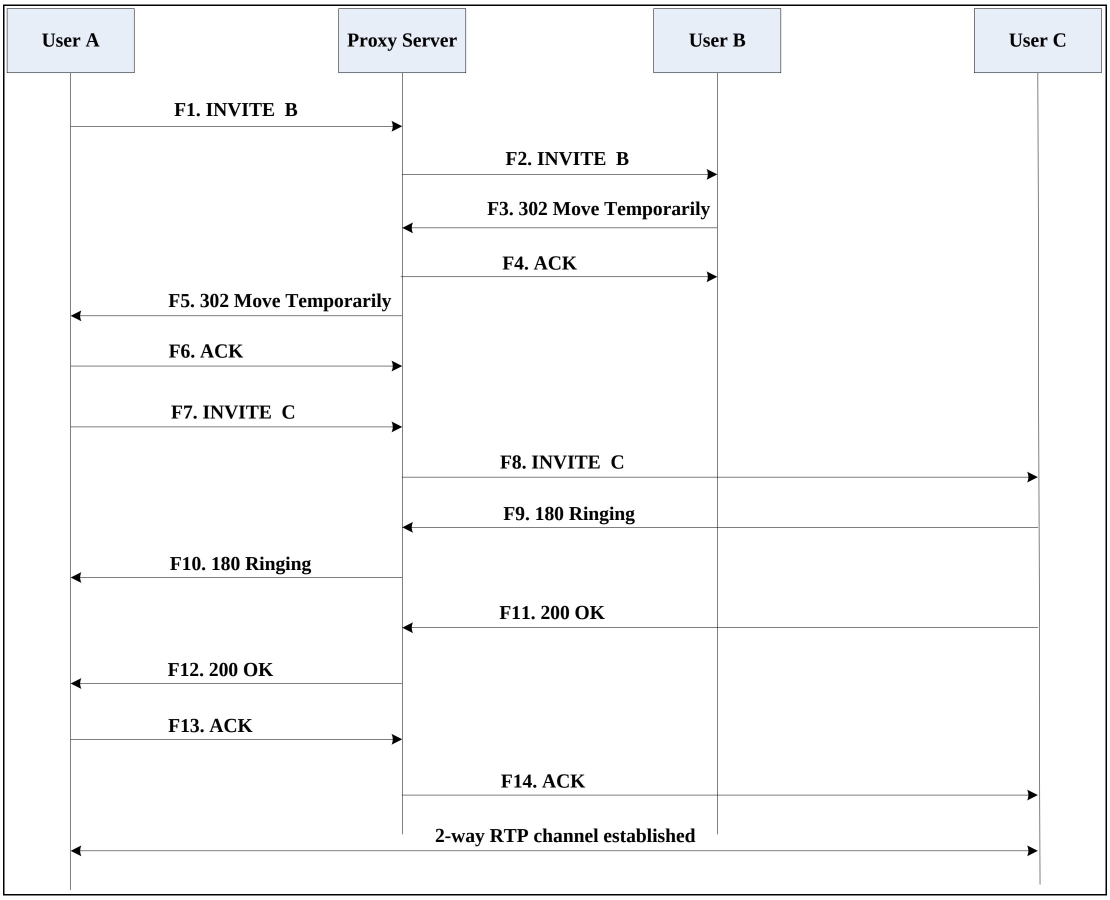
Always Call Forward

The following figure illustrates successful call forwarding between Yealink SIP IP phones in which User B has enabled always call forward. The incoming call is immediately forwarded to User C when User A calls User B. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User B enables always call forward, and the destination number is User C.
2. User A calls User B.
3. User B forwards the incoming call to User C.
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. • The media capability User A is ready to receive is specified. • The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	302 Move Temporarily—User B to Proxy Server	User B sends a SIP 302 Moved Temporarily message to the proxy server. The message indicates that User B is not available at SIP phone B. User B rewrites the contact-URI.
F4	ACK—Proxy Server to User B	The proxy server sends a SIP ACK to User B, the ACK message notifies User B that the proxy server has received the 302 Move Temporarily message.
F5	302 Move Temporarily—Proxy Server to User A	The proxy server forwards the 302 Moved Temporarily message to User A.
F6	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK message notifies the proxy server that User A has received the 302 Move Temporarily message.

Step	Action	Description
F7	INVITE—User A to Proxy Server	User A sends a SIP INVITE request to the proxy server. In the INVITE request, a unique Call-ID is generated and the Contact-URI field indicates that User A requested the call.
F8	INVITE—Proxy Server to User C	The proxy server maps the SIP URI in the To field to User C. The proxy server sends the SIP INVITE request to User C.
F9	180 Ringing—User C to Proxy Server	User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F10	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User C is being alerted.
F11	200OK—User C to Proxy Server	User C sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F12	200OK—Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A. The 200 OK response notifies User A that the connection has been made.
F13	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F14	ACK—Proxy Server to User C	The proxy server forwards the ACK message to User C. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.

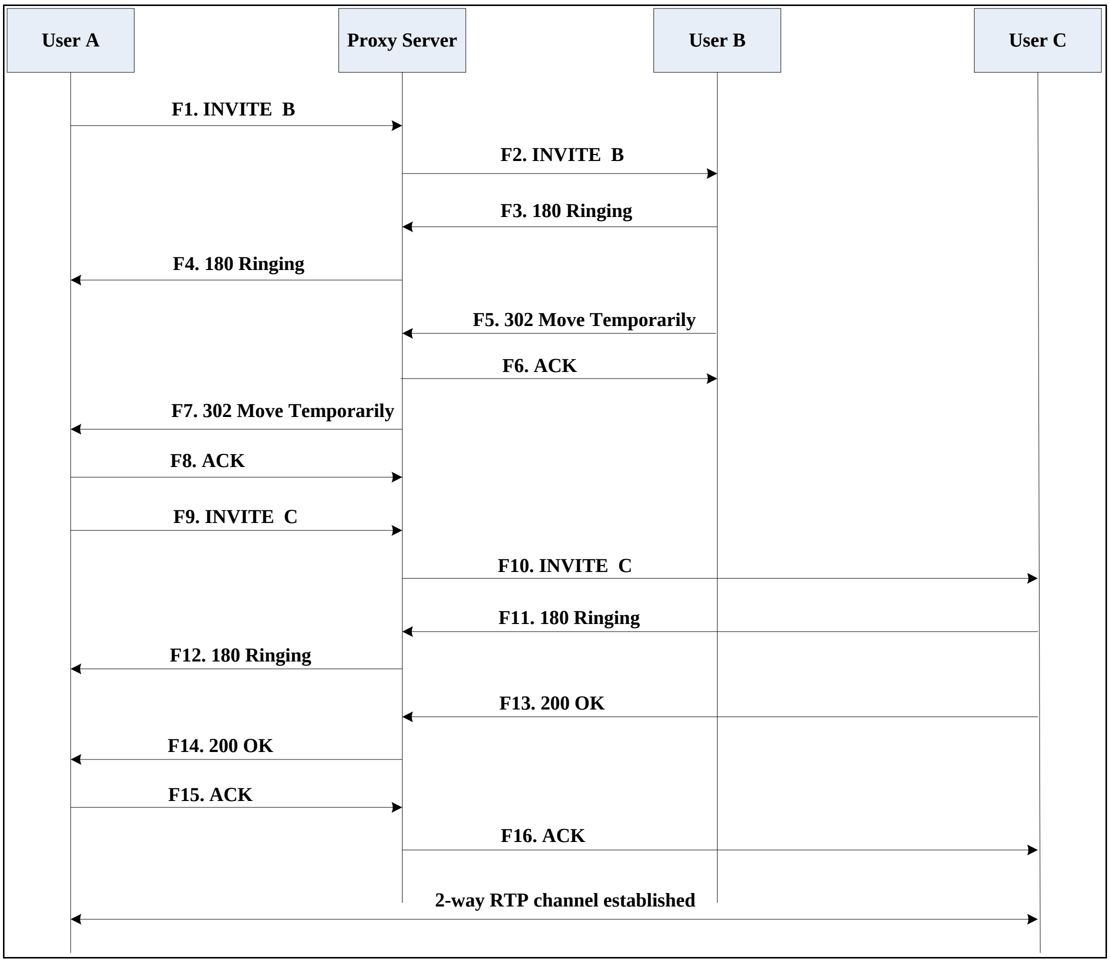
Busy Call Forward

The following figure illustrates successful call forwarding between Yealink SIP IP phones in which User B has enabled busy call forward. The incoming call is forwarded to User C when User B is busy. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User B enables busy call forward, and the destination number is User C.
2. User A calls User B.
3. User B is busy.
4. User B forwards the incoming call to User C.
5. User C answers the call.

   Call is established between User A and User C.



Step	Action	Description
F1	INVITE—User A to Proxy Server	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.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	180 Ringing—User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	302 Move Temporarily—User B to Proxy Server	User B sends a SIP 302 Moved Temporarily message to the proxy server. The message indicates that User B is not available at SIP phone B. User B rewrites the contact-URI.
F6	ACK—Proxy Server to User B	The proxy server sends a SIP ACK to User B, the ACK message notifies User B that the proxy server has received the

Step	Action	Description
		ACK message.
F7	302 Move Temporarily—Proxy Server to User A	The proxy server forwards the 302 Moved Temporarily message to User A.
F8	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK message notifies the proxy server that User A has received the ACK message.
F9	INVITE—User A to Proxy Server	User A sends a SIP INVITE request to the proxy server. In the INVITE request, a unique Call-ID is generated and the Contact-URI field indicates that User A requests the call.
F10	INVITE—Proxy Server to User C	The proxy server forwards the SIP INVITE request to User C.
F11	180 Ringing—User C to Proxy Server	User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F12	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User C is being alerted.
F13	200OK—User C to Proxy Server	User C sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F14	200OK—Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A.
F15	ACK— User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F16	ACK—Proxy Server to User C	The proxy server sends the ACK message to User C.

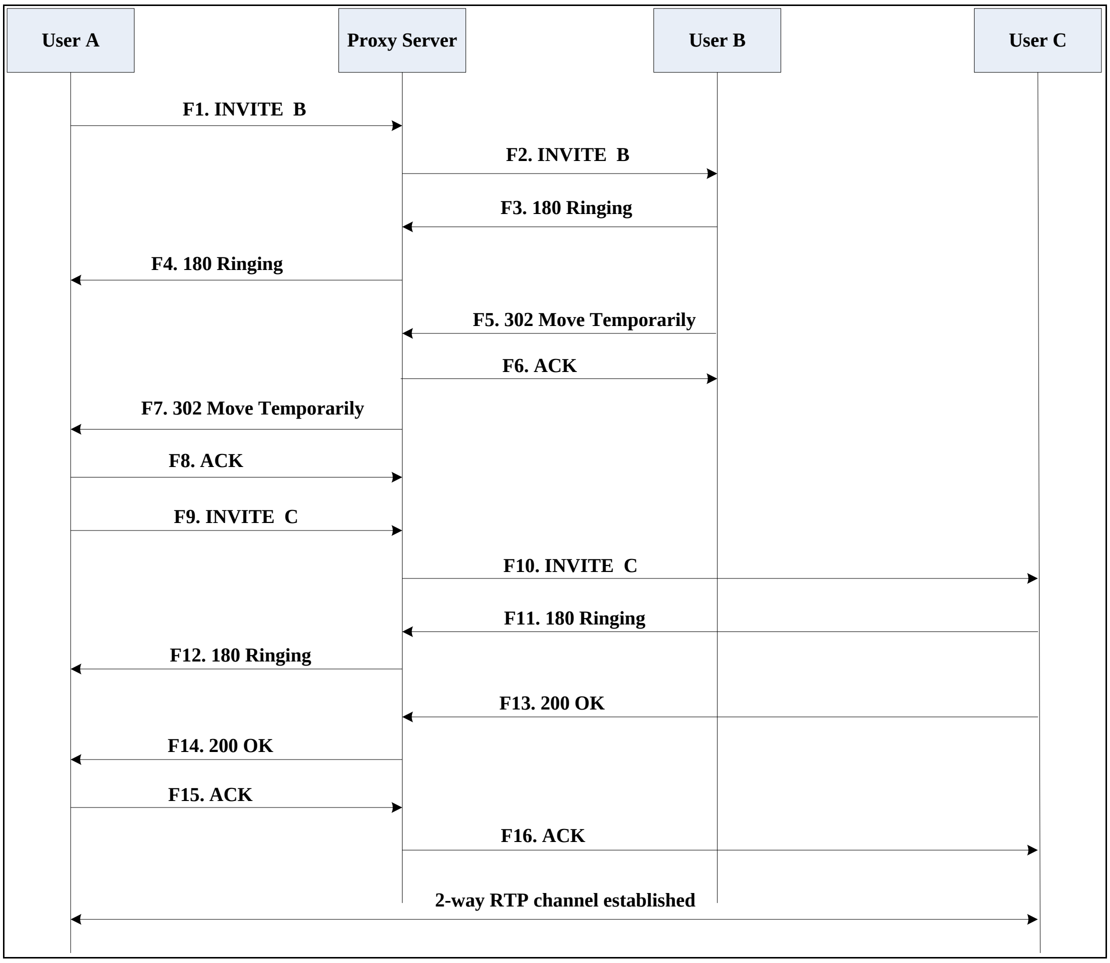
No Answer Call Forward

The following figure illustrates successful call forwarding between Yealink SIP IP phones in which User B has enabled no answer call forward. The incoming call is forwarded to User C when User B does not answer the incoming call after a period of time. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User B enables no answer call forward, and the destination number is User C.
2. User A calls User B.
3. User B does not answer the incoming call.
4. User B forwards the incoming call to User C.
5. User C answers the call.

   Call is established between User A and User C.



Step	Action	Description
F1	INVITE—User A to Proxy Server	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.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	180 Ringing—User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	302 Move Temporarily—User B to Proxy Server	User B sends a SIP 302 Moved Temporarily message to the proxy server. The message indicates that User B is not available at SIP phone B. User B rewrites the contact-URI.
F6	ACK—Proxy Server to User B	The proxy server sends a SIP ACK to User B, the ACK message notifies User B that the proxy server has received the

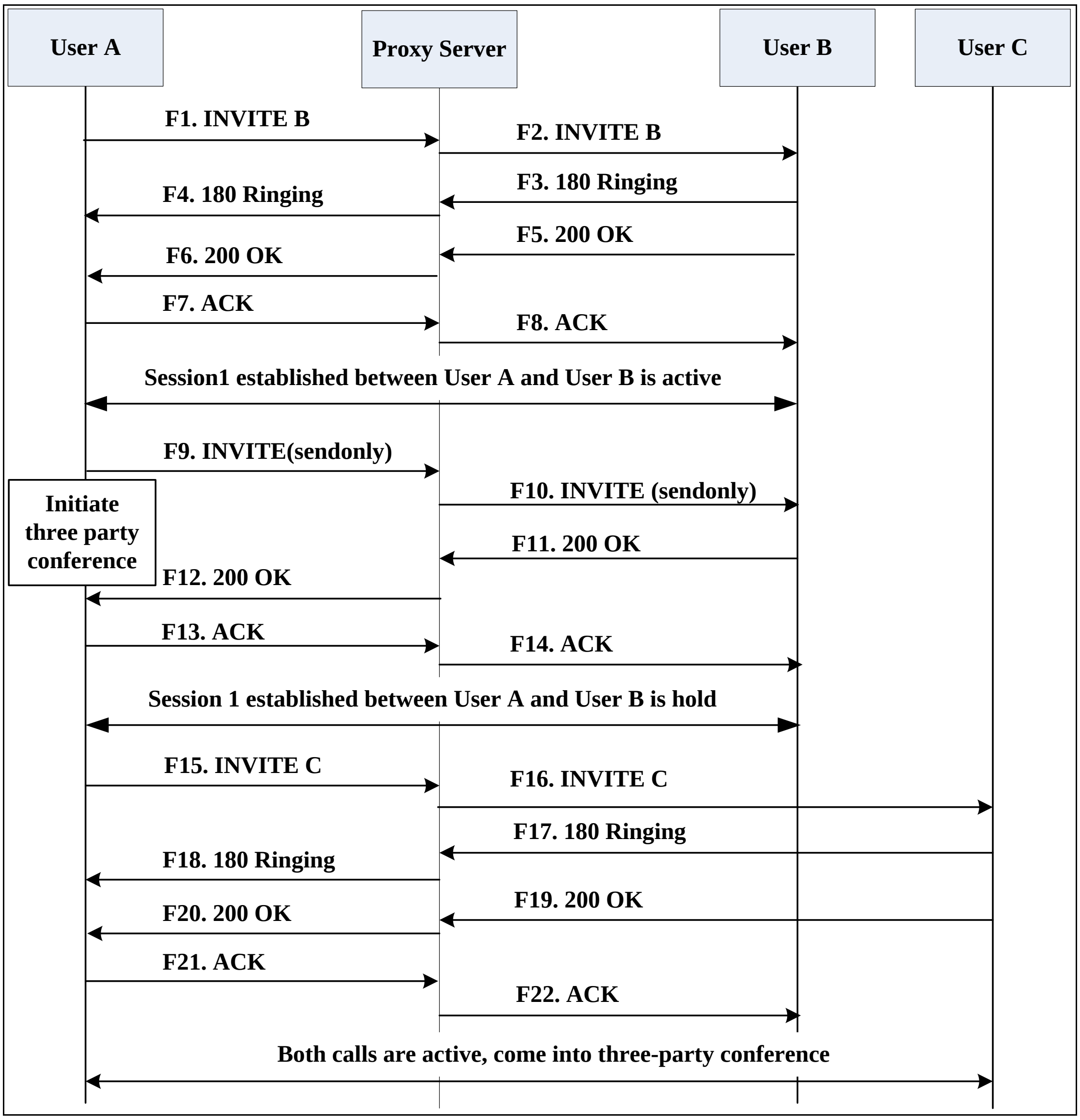
Step	Action	Description
		ACK message.
F7	302 Move Temporarily—Proxy Server to User A	The proxy server forwards the 302 Moved Temporarily message to User A.
F8	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK message notifies the proxy server that User A has received the ACK message.
F9	INVITE—User A to Proxy Server	User A sends a SIP INVITE request to the proxy server. In the INVITE request, a unique Call-ID is generated and the Contact-URI field indicates that User A requests the call.
F10	INVITE—Proxy Server to User C	The proxy server forwards the SIP INVITE request to User C.
F11	180 Ringing—User C to Proxy Server	User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F12	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User C is being alerted.
F13	200OK—User C to Proxy Server	User C sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F14	200OK—Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A. The 200 OK response notifies User A that the connection has been made.
F15	ACK— User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F16	ACK—Proxy Server to User C	The proxy server sends the ACK message to User C. The ACK confirms that the proxy server has received the 200 OK response.

Call Conference

The following figure illustrates successful 3-way calling between Yealink SIP-T46G IP phones in which User A mixes two RTP channels and therefore establishes a conference between User B and User C. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.
3. User A puts User B on hold.
4. User A calls User C.
5. User C answers the call.
6. User A mixes the RTP channels and establishes a conference between User B and User C.


User A
Proxy Server
User B
User C
F1. INVITE B
F2. INVITE B
F3. 180 Ringing
F4. 180 Ringing
F5. 200 OK
F6. 200 OK
F7. ACK
F8. ACK
Session1 established between User A and User B is active
F9. INVITE(sendonly)
F10. INVITE (sendonly)
Initiate three party conference
F11. 200 OK
F12. 200 OK
F13. ACK
F14. ACK
Session 1 established between User A and User B is hold
F15. INVITE C
F16. INVITE C
F17. 180 Ringing
F18. 180 Ringing
F19. 200 OK
F20. 200 OK
F21. ACK
F22. ACK
Both calls are active, come into three-party conference

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.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. Proxy server forwards the INVITE message to User B.
F3	180 Ringing—User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F6	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the connection has been made.

Step	Action	Description
F7	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F8	ACK—Proxy Server to User B	The proxy server sends the SIP ACK to User B. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.
F9	INVITE—User A to Proxy Server	User A sends a mid-call INVITE request to the proxy server with new SDP session parameters, which are used to place the call on hold.
F10	INVITE—Proxy Server to User B	The proxy server forwards the mid-call INVITE message to User B.
F11	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the INVITE is successfully processed.
F12	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK response to User A. The 200 OK response notifies User A that User B is successfully put on hold.
F13	ACK—User A to Proxy Server	User A sends the ACK message to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now temporarily inactive. No RTP packets are being sent.
F14	ACK—Proxy Server to User B	The proxy server sends the ACK message to User B. The ACK confirms that the proxy server has received the 200 OK response.
F15	INVITE—User A to Proxy Server	User A sends a SIP INVITE request to the proxy server. In the INVITE request, a unique Call-ID is generated and the Contact-URI field indicates that User A requests the call.
F16	INVITE—Proxy Server to User	The proxy server maps the SIP URI in the To field to User C. The proxy server

Step	Action	Description
	C	sends the SIP INVITE request to User C.
F17	180 Ringing—User C to Proxy Server	User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F18	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User C is being alerted.
F19	200OK—User C to Proxy Server	User C sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F20	200OK—Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A. The 200 OK response notifies User A that the connection has been made.
F21	ACK— User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F22	ACK—Proxy Server to User C	The proxy server sends the ACK message to User C. The ACK confirms that the proxy server has received the 200 OK response.

Appendix F: Sample Configuration File

This section provides the sample configuration file necessary to configure the IP phone. Any line starts with a pound sign (#) is considered to be a comment, unless the # is contained within double quotes. For Boolean fields, 0 = disabled, 1 = enabled.

This file contains sample configurations for the <y000000000028>.cfg or <MAC>.cfg file. The parameters included here are examples only. Not all possible parameters are shown in the sample configuration file. You can configure or comment the values as you required. The settings in the <y000000000028>.cfg file will be overridden by settings which also appear in the <MAC>.cfg file.

T46G Sample Configuration File

```
#!version:1.0.0.1
#Note: This file header cannot be edited or deleted.
```

#Network Settings

```
network.internet_port.type =

#Configure the WAN port type; 0-DHCP, 1-PPPoE, 2-Static IP Address.
#If the WAN port type is configured as DHCP, you do not need to set the
#following network parameters.
#If the WAN port type is configured as Static IP Address, configure the
#following parameters.

network.internet_port.ip =

network.internet_port.mask =

network.internet_port.gateway =

network.primary_dns=

network.secondary_dns =

#If the WAN port type is configured as PPPoE, configure the following
#parameters.
network.pppoe.user =
network.pppoe.password =
```

#Dial Plan Settings

```
dialplan.area_code.code =
dialplan.area_code.min_len =
dialplan.area_code.max_len =
dialplan.area_code.line_id =
dialplan.block_out.number.1 =
dialplan.block_out.line_id.1 =
dialplan.dialnow.rule.X =
dialplan.dialnow.line_id.X =
```

```
dialplan.replace.prefix.X =
dialplan.replace.replace.X =
dialplan.replace.line_id.X =
```

#Time Settings

```
local_time.time_zone =
local_time.time_zone_name =
local_time.ntp_server1 =
local_time.ntp_server2 =
local_time.interval =
local_time.dhcp_time =
```

```
#Use the following parameters to set the time and date manually.
local_time.manual_time_enable =
local_time.date_format =
local_time.time_format =
```

#Auto DST Settings

```
local_time.summer_time =
local_time.dst_time_type =
local_time.start_time =
local_time.end_time =
local_time.offset_time =
```

#Phone Lock

```
phone_setting.lock =
phone_setting.phone_lock.unlock_pin =
phone_setting.phone_lock.lock_time_out =
```

#Language

```
lang.wui =
lang.gui =
```

#Call Waiting

```
call_waiting.enable =
call_waiting.tone =
```

#Auto Redial

```
auto_redial.enable =
auto_redial.interval =
auto_redial.times =
```

#Call Hold

```
features.play_hold_tone.enable =
features.play_hold_tone.delay =
```

```
sip.rfc2543_hold =
```

#Hotline

```
features.hotline_number =
features.hotline_delay =
```

#Web Server Type

```
wui.http_enable =
network.port.http =
wui.https_enable =
network.port.https =
```

#DTMF Suppression

```
features.dtmf.hide =
features.dtmf.hide_delay =
```

#Call Forward

 # In Phone Mode

```
features.fwd_mode = 0
forward.always.enable =
forward.always.target =
forward.always.on_code =
forward.always.off_code =
forward.busy.enable =
forward.busy.target =
forward.busy.on_code =
forward.busy.off_code =
forward.no_answer.enable =
forward.no_answer.target =
forward.no_answer.timeout =
forward.no_answer.on_code =
forward.no_answer.off_code =
```

 # In Custom Mode

```
features.fwd_mode = 1
account.1.always_fwd.enable =
account.1.always_fwd.target =
account.1.always_fwd.on_code =
account.1.busy_fwd.off_code =
account.1.busy_fwd.enable =
account.1.busy_fwd.target =
account.1.busy_fwd.on_code =
account.1.busy_fwd.off_code =
account.1.timeout_fwd.enable =
```

```
account.1.timeout_fwd.target =
account.1.timeout_fwd.timeout =
account.1.timeout_fwd.on_code =
account.1.timeout_fwd.off_code =
```

#Call Transfer

```
transfer.semi_attend_tran_enable =
transfer.blind_tran_on_hook_enable =
transfer.on_hook_trans_enable =
transfer.tran_others_after_conf_enable =
```

#Call Conference

```
account.1.conf_type =
account.1.conf_uri =
```

#DTMF

```
account.1.dtmf.type =
account.1.dtmf.dtmf_payload =
account.1.dtmf.info_type =
```

#Distinctive Ring Tones

```
account.1.alert_info_url_enable =
distinctive_ring_tones.alert_info.1.text =
distinctive_ring_tones.alert_info.1.ringer =
```

#Tones

```
voice.tone.dial =
voice.tone.ring =
voice.tone.busy =
voice.tone.congestion =
voice.tone.callwaiting =
voice.tone.dialrecall =
voice.tone.record=
voice.tone.info =
voice.tone.stutter =
voice.tone.message =
voice.tone.autoanswer =
```

#Remote Phonebook

```
features.remote_phonebook.enable =
features.remote_phonebook.flash_time =
```

#LDAP

```
ldap.name_filter =
```

```
ldap.number_filter =
ldap.host = 0.0.0.0
ldap.port = 389
ldap.base =
ldap.user =
ldap.password =
ldap.max_hits =
ldap.name_attr =
ldap.numb_attr =
ldap.display_name =
ldap.version =
ldap.search_delay =
ldap.call_in_lookup =
ldap.ldap_sort =
```

#Action URL

```
action_url.setup_completed =
action_url.log_on =
action_url.log_off =
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.forward_incoming_call =
action_url.reject_incoming_call =
action_url.answer_new_incoming_call =
action_url.transfer_finished =
action_url.transfer_failed =
```

#SNMP

```
network.snmp.enable =
network.snmp.port =
network.snmp.trust_ip =
```

#Access URL of Resource Files

```
dialplan_dialnow.url =
dialplan_replace_rule.url =
local_contact.data.url =
remote_phonebook.data.1.url =
wallpaper_upload.url =
```

Index

G

H

I

J

K

L

M

N

P

Q

R

S

T

U

V

W