



**ADMINISTRATOR GUIDE**

3.3.0 | September 2019 | 3725-86015-001B

# **Polycom® HDA50**



---

Copyright© 2019, Polycom, Inc. All rights reserved. No part of this document may be reproduced, translated into another language or format, or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Polycom, Inc.

6001 America Center Drive  
San Jose, CA 95002  
USA

**Trademarks** Polycom®, the Polycom logo and the names and marks associated with Polycom products are trademarks and/or service marks of Polycom, Inc. and are registered and/or common law marks in the United States and various other countries.



All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Polycom.

**Disclaimer** While Polycom uses reasonable efforts to include accurate and up-to-date information in this document, Polycom makes no warranties or representations as to its accuracy. Polycom assumes no liability or responsibility for any typographical or other errors or omissions in the content of this document.

**Limitation of Liability** Polycom and/or its respective suppliers make no representations about the suitability of the information contained in this document for any purpose. Information is provided "as is" without warranty of any kind and is subject to change without notice. The entire risk arising out of its use remains with the recipient. In no event shall Polycom and/or its respective suppliers be liable for any direct, consequential, incidental, special, punitive or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption, or loss of business information), even if Polycom has been advised of the possibility of such damages.

**End User License Agreement** BY USING THIS PRODUCT, YOU ARE AGREEING TO THE TERMS OF THE END USER LICENSE AGREEMENT (EULA) AT: <http://documents.polycom.com/indexes/licenses>. IF YOU DO NOT AGREE TO THE TERMS OF THE EULA, DO NOT USE THE PRODUCT, AND YOU MAY RETURN IT IN THE ORIGINAL PACKAGING TO THE SELLER FROM WHOM YOU PURCHASED THE PRODUCT.

**Patent Information** The accompanying product may be protected by one or more U.S. and foreign patents and/or pending patent applications held by Polycom, Inc.

**Open Source Software Used in this Product** This product may contain open source software. You may receive the open source software from Polycom up to three (3) years after the distribution date of the applicable product or software at a charge not greater than the cost to Polycom of shipping or distributing the software to you. To receive software information, as well as the open source software code used in this product, contact Polycom by email at [OpenSourceVideo@polycom.com](mailto:OpenSourceVideo@polycom.com).

**Customer Feedback** We are striving to improve our documentation quality and we appreciate your feedback. Email your opinions and comments to [DocumentationFeedback@polycom.com](mailto:DocumentationFeedback@polycom.com).

**Polycom Support** Visit the [Polycom Support](#) for End User License Agreements, software downloads, product documents, product licenses, troubleshooting tips, service requests, and more.

# Contents

---

- Before You Begin . . . . . 4**
  - Audience, Purpose, and Required Skills . . . . . 4
    - Related Documentation . . . . . 4
  - Getting Help . . . . . 4
    - Polycom and Partner Resources . . . . . 4
    - The Polycom Community . . . . . 5
    - Documentation Feedback . . . . . 5
  - Notational Conventions . . . . . 5
    - Canonical Fashion . . . . . 5
    - Literal Fashion . . . . . 6
    - Boolean Values . . . . . 6
    - Multiple Choice Values . . . . . 6
    - Parameter Values . . . . . 6
  
- Getting Started . . . . . 8**
  - Product Overview . . . . . 8
  - Port Setup and Configuration . . . . . 8
  
- Configuration and Management Interfaces . . . . . 9**
  - Web Server-Based Local Configuration . . . . . 9
  - Local Device Update and Management . . . . . 10
    - Firmware Update . . . . . 10
    - Customized AA Prompts Backup and Restore . . . . . 10
    - Backup Configuration . . . . . 11
    - Restore Configuration . . . . . 11
    - Reset Configuration Locally . . . . . 12
    - Reset Configuration Remotely . . . . . 12
  
- Device Interface . . . . . 13**
  - Headset Connection . . . . . 13
  - Phone Port Setup and Configuration . . . . . 13
    - Use the Device as a Paging System . . . . . 14
  - Available Features . . . . . 14

IP Routing and LAN Switching Features .....	14
IP Routing Features .....	14
LAN Switching Features .....	16
802.1X Authentication .....	17
<b>Status Pages .....</b>	<b>18</b>
System Status .....	18
WAN Status .....	18
Product Information .....	18
USB Headset Status .....	19
SP $n$ Service Status ( $n = 1, 2, 3, 4$ ) .....	19
OBiTALK Service Status .....	19
LAN Status .....	19
Call Status .....	20
Call History .....	20
Services, Phone, and Line Status .....	20
<b>Device Settings .....</b>	<b>21</b>
Codec Profile Features .....	21
Tone and Ring Patterns .....	21
Tone Profile Features .....	21
Field-1 Composition .....	21
Field-2 Composition .....	22
Field-3 to Field-6 Composition .....	22
Tone Examples .....	23
Ring Profile A & B .....	24
Ring Profile Features .....	25
Field-1 Composition .....	25
Field-2 to Field-5 Composition .....	25
<b>Call Routing .....</b>	<b>27</b>
Inbound Call Route Configuration .....	27
Outbound Call Route Configuration .....	29
Trunks, Endpoints, and Terminals .....	30
<b>Service Providers .....</b>	<b>33</b>
SIP Service Provider Features .....	33
SIP Registration .....	34
ITSP Driven Distinctive Ringing .....	38
RTP Statistics – the X-RTP-Stat Header .....	38
Media Loopback Service .....	38

Using SP <i>n</i> as a Proxy for a SIP IP Phone .....	39
Automated Attendant .....	40
Customizing AA Prompt Lists .....	40
Trunk Groups .....	41
<b>Parameter Reference Guide .....</b>	<b>42</b>
<b>Troubleshooting .....</b>	<b>106</b>
Phone Port Setup and Configuration .....	106
Possible Error Messages on Firmware Update Failure .....	107

# Before You Begin

---

This guide describes how to administer, configure, and provision Polycom® HDA50 devices.

## Audience, Purpose, and Required Skills

This guide is for a technical audience. You must be familiar with the following concepts before beginning:

- Current telecommunications practices, protocols, and principles
- Telecommunication basics, video teleconferencing, and voice or data equipment
- Open SIP networks and VoIP endpoint environments

## Related Documentation

For more information on HDA50, refer to the following documents on Polycom Support. These documents are written for service providers and system administrators.

- **Polycom® HDA50 Setup Sheet:** Includes information about cable connections, package contents, front panel LEDs, and safety and regulatory information.
- **Polycom® HDA50 Deployment Guide:** Includes information about configuration, device settings, initial configuration setup, and a provisioning parameter reference guide.

## Getting Help

For more information about installing, configuring, and administering Polycom products, see **Documents & Software** at [Polycom Support](#).

## Polycom and Partner Resources

In addition to this guide, the following documents and other resources provide details and resources:

- For Polycom Software releases and documentation, see [Polycom Voice Support](#).
- For user guides for Polycom voice products, refer to the product support page for your phone at [Polycom Voice Support](#).
- You can find Request for Comments (RFC) documents by entering the RFC number at <https://www.ietf.org/rfc/>.
- For information on IP PBX and softswitch vendors, see Polycom [Desktop Phone Compatibility](#).
- For information on Polycom Device Management Service for Service Providers (PDMS-SP), refer to the documentation on [Polycom Support](#).

To find all Polycom partner solutions, see [Strategic Global Partner Solutions](#).

## The Polycom Community

The [Polycom Community](#) gives you access to the latest developer and support information. Participate in discussion forums to share ideas and solve problems with your colleagues. To register with the Polycom Community, simply create a Polycom Online account. When logged in, you can access Polycom support personnel and participate in developer and support forums to find the latest information on hardware, software, and partner solutions topics.

## Documentation Feedback

We welcome your feedback to improve the quality of Polycom documentation.

You can email [Documentation Feedback](#) for any important queries or suggestions related to this documentation.

## Notational Conventions

This guide provides device configuration parameters and their values in the following formats:

- Canonical fashion
- Literal fashion

Both notational conventions point to the same parameters, but their appearances are different.

The canonical fashion simplifies locating parameters on the device's native web portal or on OBiTALK at <https://www1.obitalk.com>.

The literal fashion is required when provisioning or writing OBIPhoneXML apps.

### Canonical Fashion

This example shows the format of the canonical fashion.

- **Parameter Group Name::ParameterName** = Parameter Value {replace with actual value}

The **Parameter Group Name** is the heading of the parameter group on the left side panel of the device local configuration or OBiTALK Configuration web page. This string may contain spaces. When a group heading has more than one level, each level is separated with a –, such as:

- **Services Providers - ITSP Profile A – SIP:**

The **ParameterName** is the name of the parameter as shown on the web page and MUST NOT CONTAIN ANY SPACES. **Parameter Group Name** and **ParameterName** are separated by two colons (::), as shown in the first example above.

The **Parameter Value** is the literal value to assign to the named parameter and may contain spaces. You can omit **Parameter Group Name** or its top-level headings when the context is clear. For example:

- **SP1 Service::AuthUserName** = 4082224312
- **ITSP Profile A - SIP::ProxyServer** = sip.myserviceprovider.com

- **ProxyServerPort** = 5082

## Literal Fashion

These examples show the format of the literal fashion. The literal fashion is used when provisioning or writing OBIPhoneXML apps.

- **ParameterGroupName.ParameterName**.Parameter Value {replace-with-actual-value}
- **Parameter.Group.Name.ParameterGroupName.ParameterName**.Parameter Value

The **ParameterGroupName** is the name of the first parameter group in literal fashion. This string **MUST NOT CONTAIN ANY SPACES**, and always is terminated with a period, as shown. More than one **ParameterGroupName** *may be used*. The **ParameterGroupName** is case-sensitive.

The **ParameterName** is the name of the parameter, and always is terminated with a period, as shown. This string **MUST NOT CONTAIN ANY SPACES**. The **ParameterName** is case-sensitive.

The Parameter Value is the literal value to assign to the named parameter and may contain spaces. The Parameter Value is not case-sensitive, but it **MUST EXACTLY MATCH** the value when one or more choices are available.

When using the literal fashion in your XML, you need to exactly match the text string for **ParameterGroupName.ParameterName**.Parameter Value, but text formatting such as bold face is not required and will be removed when your script or app is processed.

## Boolean Values

You can identify parameters that take a Boolean value on your device's configuration web pages by a check box next to the parameter name. Throughout the document, we may loosely refer to a Boolean value as "enable/disable" or "yes/no", but the only valid Boolean parameter values to use in a device configuration file is either `true/false` or `True/False` (case-sensitive). This is equivalent to selecting or clearing the check box on the configuration web pages.

## Multiple Choice Values

You must provision parameters that take one of several valid options from a drop-down list on the device message with string values that match exactly one of those choices. Otherwise, the device uses the default choice. Matching the provisioned value against valid strings is case-sensitive and doesn't allow extra spaces.

When a choice must be selected, the device web page provides a drop-down menu for that parameter. Copy that value into your provisioning script.

## Parameter Values

When entering a parameter value from the web page or via provisioning, avoid adding extra white spaces before or after the parameter value. If the value is a comma-separated list of strings or contains attributes after a comma or semicolon, avoid adding extra white space before and after the delimiter.

For example: **CertainParameter** = 1,2,3,4;a;b;c



If a parameter value can include white spaces, such as **X\_DisplayLabel**, use just a single space and no extra space before and after the value.

For example: **X\_DisplayLabel** = My New Service

# Getting Started

---

The HDA50 is a VoIP adapter for USB headsets. It offers audio reliability in instances when you prefer to use a soft client for call management and control. Similar to a desk phone, it ensures that audio traffic is separated and prioritized.

You can manage the HDA50 configuration and network interaction directly through the device, the native device web interface, or the PDMS-SP portal at <https://www1.obitalk.com>.

## Product Overview

The Polycom HDA50 is an Open SIP USB headset adapter with the following features:

- SIP service provider or local system administrator support for up to four SIP accounts
- USB headset connectivity optimized for Plantronics headsets
- Aggregation and bridging of SIP services
- Automatic Attendant (AA) for simplified call routing
- High-quality voice encoding using G.711, G.7.22, G.726, G.729, Opus, and iLBC algorithms
- Recursive digit maps and associated call routing (outbound and inbound)

## *Port Setup and Configuration*

Make the following connections to use your device. For details, see the HDA50 Setup Sheet.

- **Power Connection** - Connect the supplied 12-volt power adapter to the device and the wall outlet or working power strip. Only use the power adapter supplied with the original packaging to power the device. Use of any power adapter other than what was provided with the device voids the warranty and may cause the unit to not function at all or cause undesired operation.
- **Internet Connection Setup and Configuration** - Connect an Ethernet cable from an available switch port to the Internet port. By default, the device requests IP, DNS, and Internet (WAN) Gateway IP addressing via DHCP.

# Configuration and Management Interfaces

---

The HDA50 provides these interfaces for local configuration and management:

- Device web page
- Remote configuration and management using PDMS-SP at <https://www1.obitalk.com>

## Web Server-Based Local Configuration

You can access the HDA50 device configuration web page using the IP address and default account credentials:

- For user access, the default user name and password are `user` and `user`.
- For administrator access, the default user name and password are `admin` and `admin`.

### *Access the Device Management Web Page*

Each device has its own built-in portal site at `http://{ip-address}` where `{ip-address}` is the IP address of the device. The native web portal offers configurable options and status information organized into a number of web pages.

If the device is already bootstrapped into your assigned PDMS-SP account, follow the procedure below to find the device's IP address.

#### Procedure

- 1 Log in to PDMS-SP.
- 2 Go to the **Manage Device** page and select the device by OBi number, MAC Address, or Serial Number.
- 3 Go to the **Configuration** tab and select **Local Configuration**.
- 4 You can find the IP address at **System Status > WAN Status > IPAddress**.
- 5 Enter the device IP address in the address field of your web browser.
- 6 When prompted, enter the user name and password.

Use the collapsible menu on the left side of the page to easily go to the various configuration parameter sections of the device.



In the PDMS-SP interface, Polycom recommends that you claim your device before you connect it to the internet. Use this method instead of adding the device. After you claim it, the device is associated with your account.

Submit every configuration page individually after changes are made on the page. Otherwise changes are discarded once you go to another page. Most changes require a reboot of the unit (by clicking the **Reboot** button) to take effect. However, you may reboot the unit just once after you have made and submitted all the necessary changes on all the pages.



When the device is operating in router mode, access the built-in web server from the LAN side or the WAN side. LAN side access is always allowed. For security reasons, the access from the WAN side can be disabled by configuration. WAN side access to the web server is disabled by default. You can enable this option on the device web page (from the LAN side).

For more information on using the PDMS-SP interface, refer to the *Polycom Device Management Service for Service Providers Administrator Guide* at [Polycom Support](#).

## Local Device Update and Management

You can manually update and manage your device.

### *Firmware Update*

You can upgrade the firmware for your device from the device management web page. Store the firmware file locally on a computer that you can access a web browser.

#### Procedure

- 1 Select the **System Management – Device Update** menu on the side panel of the web page.
- 2 Click the **Browse** button in the **Firmware Update** section of the page. In a file browser window, select the firmware file.
- 3 Click the **Update** button to start the upgrade process.

The process takes about 30 seconds to complete.



Don't disconnect the power from the device during this procedure. If the new firmware is upgraded successfully, the device reboots automatically to start running the new firmware. Otherwise, the web page shows an error message explaining why the upgrade failed.

To perform a multiple device upgrade, refer to the PDMS-SP procedure at <https://documents.polycom.com/bundle/pdms-sp-ag-current/page/t2733076.html>

For step 3, use the HDA50 firmware link <http://fw.obihai.com/HDA50-x-x-x-xxxx.fw>.

### *Customized AA Prompts Backup and Restore*

To restore an Automated Attendant (AA) prompt file, proceed exactly like a firmware upgrade via the web browser, but provide the device with the prompt file instead of a firmware file.

**Procedure**

- 1 Select the **System Management – Device Update** menu on the side panel of the web page.
- 2 Click the **Browse** button in the **Firmware Update** section of the page. In a file browser window, select the prompt file.
- 3 Click the **Update** button to start the upgrade process.



All the existing prompts in the device are removed first when applying the backup file. This process cannot be undone.

## Backup Configuration

You can backup and store the current configuration of the device as a file in XML format at a specified location. The default name of the file is `backupxxxxxxxxxxxx.xml`, where the `xxxxxxxxxxxx` represents the MAC address of unit.

**Procedure**

- 1 In the Web UI, go to **System Management > Device Update**.
- 2 Choose backup options. Refer to the table for more information on backup options.
- 3 Select **Backup** to start the process.
- 4 When prompted, save the.xml file.



Different web browsers might handle this differently. If the operation is blocked due to the security setting of the web browser, you should change the security setting temporarily to allow this operation to complete.

**Backup Options**

Option	Description	Default Setting
Incl. Running Status	If checked, the values of all status parameters are included in backup file. Otherwise, status parameters are excluded from the backup.	No
Incl. Default Value	If checked, the default values of parameters are included in the backup file. Otherwise, default values are excluded from the backup.	No
Use OBi Version	If not checked, the backup file uses XML tags that are compliant with TR-104 standard. Otherwise, the backup file is stored in an OBi proprietary format where the XML tags aren't compliant with TR-104, but the file size is smaller and the file is more readable.	No

## Restore Configuration

When restoring the configuration to a previous backup copy, you need to specify the backup file you want to restore to.

**Procedure**

- 1 Click the **Browse** button in the **Restore Configuration** section of the web page.
- 2 Select the **Restore** button to start the process.

The device automatically reboots after the restoration is complete.



All passwords and PINs are excluded from the backup file. Hence they aren't available to restore. Call history is excluded from the backup, but can be saved as an XML formatted file separately from the Call History web page.

## ***Reset Configuration Locally***

The **Reset Configuration** function resets the device to its factory default condition. Call history and various statistical information are removed at the same time. Use the device reset with extreme caution as the operation cannot be undone.

**Procedure**

- 1 Click **Reset** on the **Reset Configuration** web page. A confirmation window displays.
- 2 Click **OK** to confirm. The phone resets its configuration to its factory default condition.

The device automatically reboots after the factory reset process completes.

By default, the hardware reset button located via an opening on the underside of the device resets all settings. You can change reset behavior via configuration.

**Reset Configuration Options**

Option	Description	Default Setting
Router Configuration	When checked, click <b>Reset</b> to restore all your router configuration parameters to the factory defaults.	Yes
All Settings	When checked, click <b>Reset</b> to restore all configuration parameters to the factory defaults.	

## ***Reset Configuration Remotely***

You can reset the device configuration to its factory default condition remotely.

**Procedure**

- 1 Enter the following parameter into an XML configuration file: `<ParameterList X_Reset="All">`
- 2 In the PDMS-SP interface, use base profiles to push the XML file to the device. You can also go to **Restore Configuration** on the local web page.

# Device Interface

---

The HDA50 contains a number of configurable device interface ports. These provide connections for a headset, LAN, and computer connections.

## Headset Connection

Use the USB port on your HDA50 to connect a supported headset.

To configure headset settings, go to **Physical Interfaces > USB Port > USB Headset Settings** on the device web portal.

## Phone Port Setup and Configuration

A phone has a very basic interface for I/O of signaling or control messages.

The device Phone port supports input signaling and control messages comprising:

- On Hook
- Off Hook
- Hook Flash
- DTMF tones

The device Phone port supports output signaling and control messages comprising:

- Caller ID/CWCID
- MWI
- DTMF/Tone
- Ring
- Polarity Reversal
- CPC
- Power Denial

The device Phone port has a Maximum Sessions capacity of two. This isn't configurable. The device Phone port replies BUSY to a new incoming call when:

- The Phone port already has two calls in session.
- The Phone port is ringing the phone.
- The phone is in a dialing or fast busy state.
- The device is already in a fax call.

The device Phone port supports Call Waiting when a second call is an inbound call:

- Hook-Flash or press the **Flash** button to switch between calls.
- When the device Phone port goes On-Hook, this ends the current call and invokes a ring for the holding call. The device Phone port supports 3-way Calling when the second call is an outbound call.

On the first Hook-Flash during an active call, the device can make a second outbound call.

On the second Hook-Flash, the first call and the second outbound call are placed in a conference. To remove the second conferenced party, invoke a third Hook-Flash.

When the device goes On-Hook during a 3-way Call, this becomes a transfer when the second (outbound) call is ringing or connected. If the second call doesn't succeed, then the Phone port goes to an On Hook state and rings as the holding call is still on the line, or Hook-Flash to resume the first call.

The device Phone port can select from the following services to which it can complete a call:

- SP1 Service (SP1)
- SP2 Service (SP2)
- SP3 Service (SP3)
- SP4 Service (SP4)

## ***Use the Device as a Paging System***

The device may be used as a paging system to allow the device to automatically answer incoming calls, but not accept calls waiting.

### **Procedure**

- » Connect the device Phone port to an external PA system using an RJ11-to-line-out-connector, and enable the **UseForPagingOnly** parameter.

## **Available Features**

The HDA50 supports many IP routing, LAN and Auto Answer features.

### ***IP Routing and LAN Switching Features***

The HDA50 has two Ethernet ports labeled as the Internet port and the LAN port. The device works as a router by default. All the native voice services and features use the WAN port only when the HDA50 is in router mode. To use the device as a 3-port switch (in Bridge mode) change its **OperationMode** parameter from `Router` to `Bridge`. One of the switch ports is for internal use only.

### **IP Routing Features**

In router mode, the network connected to the Internet Port is the WAN side of the device, and the network connected to the LAN Port is the LAN side. You can connect the WAN side to another Ethernet switch or directory to an access device, such as a modem. The HDA50 routes traffic between the LAN side and the WAN side, allowing devices (such as PCs) attached to the LAN side to share Internet access. The HDA50 supports subnet masks as large as 255.255.255.0 to accommodate as many as 253 IP addresses on its LAN side subnet.



In addition to being a NAT (Network Address Translation) router, the HDA50 includes a DHCP server, a DNS forwarder, and a basic firewall. It supports port forwarding, DMZ, QoS, and VLAN (802.1Q). The maximum routing throughput between the WAN and the LAN side is approximately 30 Mbps. This speed can be achieved when there are no active calls in the system. Otherwise, speed is limited to accommodate the voice processing load. If the WAN side is connected to an Internet access device, the speed could be further limited by the Internet uplink and downlink.

The HDA50 acquires its WAN side IP address using one of the following methods:

- Static Address Assignment
- DHCP
- PPPoE

The HDA50 acquires its WAN side IP address using DHCP by default. Also by default, the HDA50's own DHCP server is enabled to support LAN side clients such as PCs. The default LAN side IP address of the router is 192.168.10.1.

Incoming packets received from the WAN side are forwarded by the router according to the following flow:

- If the firewall is enabled, discard the packet if it's rejected by any one of the active firewall components.
- If the sending host address matches a valid entry in an internal host binding table, queue the packet for local processing. The router updates the binding table.
- If the sending host address matches a valid entry in an internal NAT binding table, forward the packet to the corresponding LAN IP address. The router updates the NAT binding table.
- If the receiving port and protocol match a reserved pair to support an internal process, queue the packet for local processing.
- If the receiving port and protocol match a port forwarding rule, forward the packet to the LAN IP address according to that rule.
- If a DMZ host is configured, forward the packet to that LAN IP address.
- Queue the packet for internal processing.

## ***DHCP Server***

By default, the built-in DHCP server is enabled on the HDA50. It assigns IP address, network mask, DNS server, and default gateway address to the DHCP clients on the LAN side. The default gateway and DNS server have the same IP address as the LAN side IP address of the router. In the DHCP server configuration, you can select the range of client IP addresses to give out the Lease Time and the Local Domain Name. Furthermore, by using the DHCP reservation feature, you can reserve specific IP addresses for some devices with specific MAC addresses. See the [LAN Settings Parameter Guide](#) and [DHCP Reservation Parameter Guide](#) sections for more details.

## ***Firewall***

The firewall protects local processes and LAN side clients against certain basic threats from the WAN side (or the Internet), such as port scanning and a DOS (Denial of Service) attack. Use the firewall settings to turn on or off the following features:

- **NATRedirection** – If enabled, supports NAT Redirection, also known as NAT Loopback or Hairpin. The default is disabled.
- **DRDOSAttackProtection** – If enabled, protects against DOS attack. The default is disabled.

- **VPNPassthrough** – If disabled, blocks all VPN traffic. The default is enabled.

These features take effect if the firewall is enabled. Otherwise, they'll take on their respective default values.

## ***Port Forwarding***

You can define as many as 20 port forwarding rules on the device. For each rule, specify a range of ports and designate receiving LAN IP address. You can also specify a rule for each that specifies if it should only apply to packets transported over UDP, TCP, or both.

## ***DMZ***

The DMZ host is the default LAN client address that a packet received from the WAN side is forwarded to when the router fails to find a matching LAN IP address or matching local process. If the firewall is enabled, the packet is still subject to firewall inspection before forwarding to the DMZ host.

## ***QoS***

QoS (Quality of Service) refers to the prioritization of network traffic based on traffic type. On the HDA50, QoS policy applies to upstream traffic (LAN-to-WAN) only. Downstream QoS is up to the ISP / upstream routers and switches. The upstream traffic is prioritized according to its type of service as indicated by the DiffServ/TOS bits in the IP header of each packet. In the QoS settings, you can map the 64 possible types of service to one of the three priority classes: High, Medium, or Low. You also can specify the guaranteed minimum upstream bandwidth for each priority class. LAN side clients indicate the desired priority class of their outbound packets to the router by marking the DiffServ/TOS bits of their packets. See the [QoS Parameter Guide](#) section for more details.

In addition to the three priority classes, a fourth priority class known as the Restricted class is available. The Restricted class has the highest priority among the four classes. The guaranteed bandwidth for the Restricted class is set separately with its own parameter in the configuration.

The total guaranteed bandwidth allocated to all the four priority classes is equal to the total available bandwidth, specified in **UpStreamBandwidth** parameter in the QoS settings.

## ***VLAN Support in Router Mode***

In router mode, the HDA50 can support VLAN (802.1Q) on the WAN side. If you enable VLAN, the incoming packets on WAN that don't belong to the same VLAN are dropped. All outgoing packets on WAN are tagged with the VLAN ID. The VLAN support is transparent to the devices on the LAN side. The router removes the VLAN tag when forwarding packets to the LAN side.

## ***LAN Switching Features***

You can set the HDA50 to act as a 3-port switch. One of the ports is internal, while the two external ports (labeled as Internet and LAN) connect to other devices. This is the Bridge mode. In this mode, all the router features, such as DHCP server, firewall, and port forwarding, won't take effect. In this case, the QoS policy provides native voice traffic the highest priority (this behavior isn't configurable).

## VLAN Support in Bridge Mode

If you enable VLAN in Bridge mode, incoming packets that don't belong to the same VLAN are dropped. All outgoing packets are tagged with the configured VLAN ID. The packets switched directly between the external ports are not modified by the device.

## Auto Answer

The HDA50 headset adapter supports three methods to signal to the called device to auto-answer the call:

- **Call-Info:** The phone receives an answer-after=0 parameter in a Call-Info header in the INVITE request.
- **Alert-Info:** The phone receives info=alert-autoanswer;delay=0 parameters in an Alert-Info header in the INVITE request.
- **Talk Event:** The phone receives an in-dialog NOTIFY with event: Talk while a call is offering.

For incoming calls, your phone processes the “answer-after” parameter in a **Call-Info** header or the “info” and “delay” parameters in an **Alert-Info** header, whichever is present in the inbound INVITE. It automatically answers the call after ringing for the number of seconds specified in those parameters (usually 0).

When the phone automatically answers the call, all other ongoing calls are interrupted the standard way as this is a new call added to the foreground.

For the talk event, the phone answers immediately after receiving the talk event. Timing is therefore controlled by the system sending the event, which is usually driven by a user choosing to answer the call from their soft client.

## Turn off Auto Answer

You can also turn off the auto-answer feature.

- » Disable the **Physical Interfaces > USB Port > USB Headset Settings::AutoAnswerEnable** option.

## Auto-Answer Incoming Call Based on Inbound Call Routing Rules

The HDA50 can auto answer certain incoming calls based on inbound call routing rules by specifying a rule that routes the call to hs(autoans). You may autoanswer all calls or by using a rule to match specific digits, target only certain numbers for auto-answer.

Routing rules applied here will supersede any rules for auto-answer that may be received as part of **Alert-Info** or **Call-Info** headers. For example:

```
{hs(autoans;nobeep)},{@.4089991234}:hs(autoans;delay=2)},{hs}
```

The autoans syntax supports two optional semi-colon separated attributes:

- **nobeep:** Not to play a beep tone on answering. Default is to play the beep tone according to user preference setting.
- **delay={value in seconds}:** The number of seconds to ring before auto-answering the call. Default is 0.

## 802.1X Authentication

The device supports the following 802.1X authentication modes:

- Disable
- MD5
- TLS
- TTLS/MSCHAPv2
- PEAP-MSCHAPv2 (optional for all parameters)

You can set the authentication mode using the parameter **WAN Settings - Internet Settings::802\_1XMode**. Depending on the selected mode, you have to configure the additional authentication parameters listed in the following table.

### 802\_1X Authentication

Parameter	Description	(EAP) MD5	(EAP) TLS1.0	TTLS/MSCHAPv2
<b>802_1XIdentity</b>	A user name. If the value isn't needed, set the value as an empty string.	Required	Required	Required
<b>802_1XPassword</b>	A password or passphrase. If a password or passphrase isn't needed, set the value as an empty string.	Required	Required	Required
<b>802_1XAnonymousID</b>	When empty, anonymous identity is used in authentication.		Required	Required
<b>802_1XTLSecurityProfile</b>	Security profile for the 802.1x authentication.		Required	

# Status Pages

---

The device web page displays top level device and system statuses for the major features of your device.

## System Status

The System Status page is divided into several sections and provides information on the status of the device and some connected devices.

### *WAN Status*

This shows the status of the WAN (Ethernet) interface, includes assigned IP address, default gateway, and subnet mask.

### *Product Information*

This shows basic product information, and the system up-time with the last reboot reason code in parentheses. The following table defines the reboot reason codes.

#### Reboot Reason Codes

Reason Code	Description
0	Reboot on power cycle.
1	Operating system reboot.
2	Reboot after Firmware Update Via provisioning or phone (**6).
3	Reboot after new profile invoked.
4	Reboot after parameter value change or firmware has changed and invoked via device web page.
5	Reboot after factory reset using the device hardware PIN.
6	New profile invoked and profile URL changed.
7	Reboot from SIP Notify (Reserved).
8	Reboot from telephone port (IVR).
9	Reboot from web page — no change in parameter values or firmware.
10	Reboot during OBiTALK signup.
11	Reboot during OBiTALK signup.

**Reboot Reason Codes**

Reason Code	Description
12	Reboot after DHCP server offers IP, GW-IP, and/or netmask different from what the device is currently using.
13	Reboot on data networking link re-establishment.
15	Reboot from firmware update via provisioning.
16	Reboot for DHCP renewal.
18	Reboot on WAN IP address change.
19	Reboot on LAN IP address change.
23	Reboot via OBiPhone XML app.
29	Reboot from LLDP-MED change.

## **USB Headset Status**

This shows the device name and device status of the connected USB headset.

## **SP $n$ Service Status ( $n = 1, 2, 3, 4$ )**

The SP $n$  service status values indicate the current state of the service with regard to its configuration (or not) and if configured its registration status. If there are problems with the registration or authentication of the device with a prescribed service, the SIP 4xx error message displays here.

## **OBiTALK Service Status**

The status of the OBiTALK Service includes the following values:

- Status can be one of the following values:
  - Normal (User Mode): The service is functioning normally.
  - Backing Off: The service is currently down, and the device is taking a short pause before retrying the connection.
- CallState can be one of the following values:
  - $N$  Active Calls, where  $N = 0, 1, \dots$ , as many as the maximum number of calls allowed in the configuration.

## **LAN Status**

This page is available when the HDA50 is in router mode, and shows the status of devices currently on the LAN. There are two sections:

- **Attached Devices:** All the devices that the router has discovered on the LAN side. Each entry has a MAC address and an IP address.
- **DHCP Clients:** All the DHCP clients that have an active lease with the DHCP server. Each entry has a Client Name, a MAC address, an IP address, and the lease expiration time (in seconds).

## Call Status

This shows the status of a number of running call statistics and state parameters for each active call. For each entry on the call status page, the following buttons may be available:

- **Remove:** This button is available for all calls. Pressing this button ends that call.
- **Record:** This button is available for calls involving the Phone port only. Pressing this button allows you to record the current conversation in an audio (.au) file.

## Call History

The Call History page shows the last 400 calls made with the device. Detailed call information is available, including terminals involved, the name (if available) of the Peer endpoints making the call, and the direction / path the call took.

The Call History page also captures what time various events took place.

Save the call history by clicking on the **Save All** button. The Call History can be saved as an XML formatted file called `callhistory.xml`.

## Services, Phone, and Line Status

Find statistics relevant to  $SP_n$  on the  $SP_n$  Stats page (where  $n = 1, 2, 3, 4$ ).

See the [Parameter Reference Guide](#) for information on the parameters displayed on these pages.

# Device Settings

---

Device settings enable you to configure and customize your device's codec, ring profiles, and tones.

## Codec Profile Features

There are two codec profiles available on the devices. They are selectable per trunk (SP1/SP2/SP3/SP4/OBiTALK). To select a codec as the preferred codec in this profile, set the priority of that codec to be highest among all the enabled codecs in this profile. Each of the SP1, SP2, SP3, SP4, and OBiTALK services can be assigned a codec profile in its corresponding configuration. The codec list to use when setting up a call on the underlying service is formed from the list of enabled codecs in the chosen profile and ordered according to the assigned priorities in the profile.

For more information on codec profile parameters, see the [Codec Profile Parameter Guide](#) table in the [Parameter Reference Guide](#) section.

## Tone and Ring Patterns

Your device enables you to create customized tone patterns and ringtones.



Tone and Ring Profile A default settings are set for North American telephone standards. Tone and Ring Profile B default settings are set for Australian telephone standards.

## *Tone Profile Features*

The general format for tone profiles is: `[field-1];[field-2];[field-3];...;[field - 6]`

Use a semicolon to separate the configuration fields.



No spaces are allowed in the tone profile pattern.

## Field-1 Composition

This field describes frequency components used for tone synthesis and it supports as many as three different frequencies.



The frequency expression is a string of numeric values with the notation '+' or '-'. The numeric values are the frequency's decimal values in Hz and amplitude in dBm (maximum 3 dBm). Different frequencies are separated by a comma.

Example: 350-18,440-18,550+2

This example means:

- The first frequency at 350 Hz with strength at -18 dBm
- The second frequency at 440 Hz with strength at -18 dBm
- The third frequency at 550 Hz with strength at +2 dBm

## Field-2 Composition

This field describes the overall tone playback duration in seconds.

The expression is a numeric value, and supports as many as 3 decimated digits. The numeric value can be negative, zero, positive, or skipped:

- Negative value: tone plays indefinitely
- Zero value: tone playback is skipped
- Positive value: Normal playback duration
- No value: tone plays indefinitely

Example: 30.234

This example means:

- Tone playback terminates after 30.234 seconds

## Field-3 to Field-6 Composition

Field - 3/4/5/6 share the same definition, and each field describes one single cadence segment. Together, the four fields form a macro-segment, which is repeated until tone playback expires.

The expression is a string of numeric values with the special notation '/', '(', ')', and ','.

Its format is:  $t(f_0/on_0+off_0, f_1/on_1+off_1, f_2/on_2+off_2, f_3/on_3+off_3)$

- $t$ : the cadence segment duration in seconds
  - Negative value: tone plays indefinitely
  - No value: tone plays indefinitely
  - Zero value: the duration of this particular segment is zero
  - Positive value: Normal playback duration
- $f_0/1/2/3$ : a digit to describe which frequency component(s) are used for the synthesis, and can be one of following 8 options (0 through 7)
  - 0: No frequency specified (silent tone)
  - 1: The first frequency
  - 2: The second frequency
  - 3: The first and second frequencies
  - 4: The third frequency

- 5: The first and third frequencies
- 6: The second and third frequencies
- 7: The first and second frequencies if two or more than two frequency components, or the first frequency if only one frequency component is available.

If no value is provided for  $f_{0/1/2/3}$ , it automatically uses the combination of the first one or two available frequency components.

- $on_{0/1/2/3}$ : the tone active time in seconds
  - Negative value: Not allowed
  - No value: infinite tone active time
  - Others: normal tone active time (as many as 3 decimated digits)
- $off_{0/1/2/3}$ : the tone inactive time in seconds
  - Negative value: Not allowed
  - No value: infinite tone inactive time
  - Others: normal tone inactive time (as many as 3 decimated digits)

Example: 4 (1/.3+2.34,3/2+1.5)

This example means:

- Use the first frequency to generate a tone for 0.3 seconds
- Follow this tone with 2.34 seconds of silence
- Use a combination of the first and second frequencies to generate a tone for 2 seconds
- Follow this tone with 1.5 seconds of silence
- The cadence operates repeatedly for 4 seconds.

## Tone Examples

These examples show the interpretation of a few common tone patterns:

### ***Dial Tone***

DIAL, "350-18,440-18"

Dial tone is generated as a mixture of two frequency components:

350 Hz at -18 dBm and 440 Hz at -18 dBm

The expiration time is infinite, and tone active time is infinite.

### ***Busy Tone***

BUSY, "480-18,620-18;10;(.5+.5)"

Busy tone is generated as a mixture of two frequency components:

480 Hz at -18 dBm and 620 Hz at -18 dBm

The expiration time is exactly 10 seconds. It has only one cadence segment, which has tone active 0.5 second and tone inactive 0.5 second.

## Prompt Tone

PROMPT, "480-16;10"

Prompt tone is generated from a single frequency component:

480 Hz at –16 dBm. The expiration time is exactly 10 seconds. It has only one cadence segment, which has tone infinite active time.

## SIT Tone

SIT\_1, "985-16,1428-16,1777-16;20;(1/.380+0,2/.380+0,4/.380+0,0/0+4)"

Special information tone (SIT) is generated from a set of frequency components:

- First frequency: 985 Hz at –16 dBm
- Second frequency: 1428 Hz at –16 dBm
- Third frequency: 1777 Hz at –16 dBm

The expiration time is exactly 20 seconds. It has only one cadence segment, which includes 4 on-off sections. The segment has infinite repeating time:

- The first on-off section: generated by the first frequency component, and it has 0.38 tone second active time and 0 inactive time.
- The second on-off section: generated by the second frequency component, and it has 0.38 tone second active time and 0 inactive time.
- The third on-off section: generated by the third frequency component, and it has 0.38 tone second active time and 0 inactive time.
- The fourth on-off section: only generate silence since no frequency component is specified. It has tone 0 second active time and 4 seconds inactive time.

## Stutter Tone

STUTTER, "350-18,440-18;20;.2(.1+.1);()"

Stutter dial tone is generated from a mixture of two frequency components:

350 Hz at –18 dBm and 440 Hz at –18 dBm. The expiration time for the entire tone is exactly 20 seconds. It has two cadence segments.

- The first segment includes only one on-off sections, on 0.1 second and off 0.1 second, and on-off repeats for 2 seconds.
- The second segment includes one on-off section, and has infinite repeating time and infinite tone active time, and plays until the entire tone duration has elapsed.

For more information on Tone Profile A & B parameters, see the [Tone Profile A & B Parameter Guide](#) table in the [Parameter Reference Guide](#) section.

## Ring Profile A & B

The HDA50 provides two ring profiles that control associated call tones. You can customize each profile separately.

## Ring Profile Features

The general format of a ring profile is: `[field-1];[field-2];...;[field - 5]`

Use a semicolon to separate as many as five configuration fields.



No spaces are allowed in the tone profile pattern.

### Field-1 Composition

Field-1 describes the overall ringing duration in seconds.

The expression is a numeric value, and supports as many as 3 decimated digits.

The numeric value can be negative, zero, and positive:

- Negative value: Ringing lasts indefinitely
- No value: Ringing lasts infinitely
- Zero value: Ringing is skipped
- Positive value: Normal ringing duration

Example: `30.5`

This example illustrates a ringing tone that terminates after 30.5 seconds.

### Field-2 to Field-5 Composition

Fields-2/3/4/5 share the same definition, and each field describes one single cadence segment. Together, the four fields form a macro-segment, which is repeated until ringing expires.

The expression is a string of numeric values with the special notation '(' , ')' and ','

It has the format as per the following construct:

`t(on_0+off_0,on_1+off_1,on_2+off_2,on_3+off_3)`

`t`: The cadence segment duration in seconds.

- Negative value: Ringing indefinitely
- No value: Ringing indefinitely
- Zero value: Ringing is skipped
- Positive value: Normal ringing duration

`on_0/1/2/3`: The ring active time in seconds.

- Negative value: Not allowed
- 1No value: Infinite ring active time
- Others: Normal ring active time (as many as 3 decimated digits)

`off_0/1/2/3`: The ring inactive time in seconds

- Negative value: Not allowed

- No value: Infinite ring inactive time
- Others: Normal ring inactive time (as many as 3 decimated digits)

Example: 4 (.3+2.34, 2+1.5)

This example illustrates a ringing tone comprised of two segments. Ringing is active for 0.3 seconds, followed by 2.34 seconds of silence, then ringing for 2 seconds, and followed by 1.5 seconds of silence.

This cadence operates repeatedly for 4 seconds.

For more information on call waiting parameters, see the [Call Waiting Parameter Guide](#) table in the [Parameter Reference Guide](#) section.

For more information on ring profile parameters, see the [Ring Profile Parameter Guide](#) table in the [Parameter Reference Guide](#) section.

# Call Routing

Call Routing is the process by which the device sets up a call bridge or an endpoint call based on such information as the trunk on which the call originates, the caller's number, the called number, etc. Call Routing Rules are parameters used to instruct the device how to route calls. A call can transform into a call bridge or an endpoint call after being routed by the device according to the given routing rules.

Every call has to be originated from somewhere. From the device's perspective, calls originated from the trunk side are considered Inbound Calls, while calls originated from an endpoint are Outbound Calls. The call routing rule syntaxes for inbound calls and outbound calls are slightly different, and are explained in the following section.

## *Inbound Call Route Configuration*

Every trunk has a corresponding **InboundCallRoute** in the device configuration. It is a comma-separated list of rules where each rule is also surrounded by a pair of curly braces `{ }`. No extra white spaces are allowed. These rules tell the device how to handle an inbound call, such as sending it to the Phone port (and ringing the attached phone(s)), sending it to the Auto Attendant for further routing (interactively with the caller), or making another call on a specific trunk to bridge with this call.

The general format is:

```
InboundCallRoute := rule OR {rule}, {rule}, ...
```

Curly braces can be omitted if there is only one rule in the route. The OR operator is not part of the parameter syntax; it is used here to separate alternative values only.

A rule has the following format:

```
rule := peering-list : terminal-list
```

The following table shows the rule formats.

### Rule Formats

Rule	Format	Notes
<code>peering-list :</code>	<code>peering,peering,...</code>	Comma-separated list of 0 or more peering objects
<code>terminal-list :</code>	<code>terminal,terminal,...</code>	Comma-separated list of 0 or more terminal objects
<code>peering :</code>	<code>caller-list &gt; callee-list</code>	
<code>caller-list :</code>	<code>caller caller caller ...</code>	Vertical bar-separated list of 0 or more caller objects

**Rule Formats**

Rule	Format	Notes
callee-list :	callee callee callee  ...	Vertical bar-separated list of 0 or more callee objects
caller :	number OR embedded-digit-map OR ? OR @	? = anonymous, @ = any number but anonymous
callee :	number OR embedded-digit-map OR @	
terminal :	PHx OR AAx OR LIx (arg) OR SPx (arg) OR PPx (arg)	arg object is optional
arg :	cid > target	
x :	1 OR 2 OR 3...	Where applicable; can be omitted if x = 1
cid :	spoofed-caller-number OR \$1	
target :	number-to-call OR \$2	
embedded-digit-map :	(Mlabel) OR digit-map	

**Notes:**

- Terminal-list can be empty, which means to block this call. The preceding ':' can't be omitted. As many as four terminals can be specified in the list. The listed terminals are called/rung by the device simultaneously. This operation is known as forking the call. A terminal can be a trunk or an endpoint.
- Abbreviated terminal names are case-insensitive.
- Number and number-to-call are literal strings, such as 14089991234.
- Digit-map is just any proper digit map, such as (1xxx|xx.); make sure to include the enclosing parentheses.
- Spoofed-caller-number is a literal string, such as 14081112233, to be used as the caller number for making a new call on the specified trunk.
- (Mlabel) is a named digit map, where label is the abbreviated name of any terminal that has a digit map defined: SP1, SP2, SP3, SP4, LI1, PP, PH, PH2, HS, or AA.
- \$1 is an internal variable containing the value of the caller number of this inbound call, after any digit map transformation in the matched caller object of the matched peering object in the peering-list.
- \$2 is an internal variable containing the called number of this inbound call, after any digit map transformation in the matched callee object of the matched peering object in the peering-list.

**More notes on peering-list and peering objects:**

- Peering-list is optional in **InboundCallRoute**. If the peering-list is empty, the succeeding ':' can be omitted also. An empty peering-list implies a single peering object whose caller object list matches any caller number. That is, the following **InboundCallRoutes** are all equivalent:
  - ph
  - {ph}
  - {:ph}

```
> {?|@>@:ph}
```

- Callee-list in a peering object can be empty. It implies the callee object @, meaning any called number. The preceding '>' can be omitted if callee-list is empty.
- Caller-list in a peering object can be empty. It implies the caller-list @|?, meaning any caller number including anonymous. The succeeding '>' can't be omitted if caller-list is empty but not the callee-list.

More notes on the `arg`, `cid`, and `target` objects:

- The `cid` object inside an `arg` object is optional. If omitted, it implies no caller-ID spoofing when making the call on the specified trunk. The succeeding '>' can be omitted if `cid` is omitted.
- The `target` object inside an `arg` object is optional. If omitted, it implies the target \$2, which means to call the original called number after applying any necessary digit map transformation implied by the rule. The preceding '>' can't be omitted if `target` is omitted but `cid` is not.
- `arg` object is optional. If omitted, it implies the `arg` with the target \$2 and no `cid`. If `arg` is omitted, the succeeding parentheses () can be omitted also.

An inbound call matches a rule if its caller-number/callee-number matches one of the peering objects of the rule. Peering objects are tested in the order left and right, and the first matched peering object wins. Rules are also checked in the order left to right, and the first matched rule wins. Therefore it is important that you place the more specific rules first in the **InboundCallRoute** if multiple rules can potentially match the same inbound call.

## Outbound Call Route Configuration

Every endpoint has an **OutboundCallRoute** parameter in the device configuration. It tells the device where to send the call when the endpoint attempts to make a call. Endpoints can call each other or an outside number using one of the trunks. The **OutboundCallRoute** syntaxes are almost identical to those of the **InboundCallRoute**; the differences are mainly in the implied value when an optional field is omitted, no caller objects and one and only one terminal object per terminal-list in an **OutboundCallRoute**. Forking is not supported when routing outbound calls.

The general format is:

```
OutboundCallRoute := rule OR {rule}, {rule}, ...
```

Curly braces can be omitted if there is only one rule in the route. The OR operator is NOT part of the parameter syntax; it is used here to separate alternative values only.

A rule has the following format:

```
rule := callee-list : terminal
```

where

- `callee-list` := callee|callee|callee| ...(vertical bar separated list of 0 or more callee object)
- `callee` := number OR embedded-digit-map OR @ (@ = any number)
- `terminal` := PHx OR AAx OR LIx(arg) OR SPx(arg) OR PPx(arg) (arg object is optional)
- `arg` := cid > target
- `x` := 1 OR 2 OR 3...(where applicable; can be omitted if it is equal to 1)
- `cid` = spoofed-caller-number
- `target` = number-to-call OR \$2



- `embedded-digit-map = (Mlabel) OR digit-map`

## Notes:

- A terminal can be a trunk or another endpoint.
- Abbreviated terminal names are case-insensitive.
- Number and `number-to-call` are literal strings, such as 14089991234.
- `Digit-map` is just any proper digit map, such as `(1xxx|xx.)`; make sure to include the enclosing parentheses.
- `Spoofed-caller-number` is a literal string, such as 14081112233, to be used as the caller number for making a new call on the specified trunk.
- `(Mlabel)` is a named digit map where label is the abbreviated name of any terminal that has a digit map defined: SP1, SP2, LI, PP, PH, or AA.
- `$2` is an internal variable containing the called number of this outbound call, after any digit map transformation in the matched callee object.
- `Callee-list` can be empty, which implies the single callee object `@`, which means any called number. The succeeding `:` can be omitted also when `callee-list` is empty.

More notes on the `arg`, `cid`, and `target` objects:

- The `cid` object inside an `arg` object is optional. If omitted, it implies no caller-ID spoofing when making the call on the specified trunk. The succeeding `>` can be omitted if `cid` is omitted.
- The `target` object inside an `arg` object is optional. If omitted, it implies the target `$2`, which means to call the original called number after applying any necessary digit map transformation implied by the rule. The preceding `>` can't be omitted if `target` is omitted but not the `cid`.
- `arg` object is optional. If omitted, it implies the `arg` with the target `$2` and no `cid`.

An outbound call matches a rule if its called number matches one of the callee objects of the rule. Callee objects are tested in the order left and right, and the first matched callee wins. Rules are also checked in the order left to right, and the first matched rule wins. Therefore it is important that you place the more specific rules first in the **OutboundCallRoute** if multiple rules can potentially match the same outbound call.



Every endpoint has a digit map defined. The user dialed number is completely processed with the endpoint's digit map first before it is passed to the **OutboundCallRoute** for routing. Therefore, the number used for matching call routing rules has already incurred the transformations implied by the digit map.

## Trunks, Endpoints, and Terminals

Your HDA50 is also a Voice Service Bridge (VSB) that supports multiple voice services. It can bridge calls across any of the supported services. A call bridge is a voice connection connecting two calls on the same or different voice services. Your HDA50 allows four concurrent independent call bridges. The following matrix shows the possible call bridge connections.

### Supported 2-way Call Bridges

	SP1 Service	SP2 Service	SP3 Service	SP4 Service	OBiTALK Service
SP1 Service	yes	yes	yes	yes	yes
SP2 Service	yes	yes	yes	yes	yes

**Supported 2-way Call Bridges**

	SP1 Service	SP2 Service	SP3 Service	SP4 Service	OBiTALK Service
SP3 Service	yes	yes	yes	yes	yes
SP4 Service	yes	yes	yes	yes	yes
OBiTALKService	yes	yes	yes	yes	yes

Each supported service is also referred to as a trunk. Each trunk is represented with a two-letter abbreviation and a numeral-based instance identifier:

- SP1 = the SP1 voice service (with ITSP A, B, C, or D)
- SP2 = the SP2 voice service (with ITSP A, B, C, or D)
- SP3 = the SP3 voice service (with ITSP A, B, C, or D)
- SP4 = the SP4 voice service (with ITSP A, B, C, or D)
- PP1 = the OBiTALK service

The instance identifier can be omitted when it equals 1. Thus, LI is equivalent to LI1. These short-hand notations are used heavily in configuring the device, as found in call routes, call forward numbers, and speed dials parameters. Unless stated otherwise, the abbreviated trunk names are case-insensitive.

In addition to all the call bridging functionalities, each device has a built-in physical Phone port for hooking up analog telephones or FAX machines. The device includes a set of features to support its Phone port to make it work as a full-featured Analog Telephone Adapter (ATA) device. Users can place and receive calls on the Phone port or USB port (using a USB headset) over any of the trunks.

The device also comes with an Auto Attendant (AA) for helping callers to direct their calls landed on the device. When an inbound call is received on the device, it can be routed to the AA, which then offers a menu of options to the caller to direct it further. It could be directed to ring an available Phone port, or bridged with another call on a trunk (which the AA “dials” or sets up on behalf of the caller).

The Phone port, headset port, and the AA entities in the device where calls can terminate, as opposed to the trunks, which rely on the corresponding service provider or local system administrator to terminate the call. In this document, the Phone port and the AA are endpoints. Like the trunks, each endpoint is represented by a 2-letter abbreviation and a numeral-based instance identifier:

- PH1 = the Phone port
- HS = Headset
- AA1 = the Auto Attendant

Unless stated otherwise, abbreviated endpoint names are case-insensitive. A trunk or an endpoint is also referred to as a terminal in this document.

The following matrix shows the possible call connections between the endpoints and the trunks.

**Supported Endpoint Calls on the Device**

	<b>Any Trunk</b>	<b>Phone Port</b>	<b>AA</b>
Any Trunk	n/a	yes	Yes
Phone Port (PHONE1 Port)	yes	no	Yes
AA	yes	yes	No

# Service Providers

---

This section of the configuration concerns all SIP based configurations. Each ITSP configuration is grouped together as an ITSP profile. The HDA50 refers to them as ITSP Profile A, B, C, and D. On the other hand, the SP service account specifics are grouped under the heading SP $n$  service, where  $n = 1, 2, 3, \text{ or } 4$ .

## ITSP Profile

Includes parameters **ProxyServer**, **Outbound Proxy**, and **DigitMap**, but does not include account specific parameters.

## SP Service

Includes account specific parameters such as **AuthUserName**, **AuthPassword**, **CallerIDName**, and **X\_ServProfile**. The **X\_ServProfile** parameter serves to match and determine which ITSP Profile parameters to use.

Voice Services

- SP1-6
- OBiTALK
- AA
- Gateways and Trunk Groups

## *SIP Service Provider Features*

The following section describes the SIP Service Provider features of the device. As many as four SIP accounts or SIP Trunks can be configured on the device. For the purpose of this document and elsewhere on the device web page, and documentation, and the OBiTALK portal, the term ITSP describes the entity providing the SIP Trunk service to the device. When the device is used in conjunction with an IP PBX, the IP PBX takes the place of the ITSP if it is the entity providing the SIP Trunk account credential and connectivity to the device.

Each ITSP configuration is grouped together as an ITSP Profile, referred to as ITSP Profiles A, B, C, and D. On the other hand, the SP service account specifics are grouped under the heading SP $n$  Service, where  $n = 1, 2, 3, \text{ or } 4$ . An ITSP Profile includes such parameters as **ProxyServer**, **OutboundProxy**, and **DigitMap**, but does not include account specific parameters. An SP Service includes account specific parameters such as **AuthUserName** (usually the phone number of the account), **AuthPassword**, **CallerIDName**, and **X\_ServProfile** (which ITSP Profile to assume). If the SP Services use the same ITSP, then only one ITSP Profile needs to be configured with all SP Services referred to the same profile.

From the device point of view, the SP $n$  Service using ITSP Profile  $X$  is enabled with the following minimal settings:

- **ITSP Profile  $X$  – SIP::ProxyServer** = *Not Blank*
- **SP $n$  Service::Enabled** = Yes

- **SPn Service::AuthUsername = Not Blank**

where  $X = A$  or  $B$ ,  $n = 1, 2, 3$ , or  $4$ . Otherwise, the service is considered disabled.

## SIP Registration

Devices can be set to periodically register with a SIP Proxy Server or SIP Registration Server. SIP Proxy Server and SIP Registration Server can be different, although they are usually the same in practice. SIP Proxy Server is a required parameter that must be configured on the device. The Registration Server is optional and assumed to be the same as the SIP Proxy Server if it is not configured on the device.

The main purpose of registration is to create and maintain a dynamic binding of the SIP account to the device's local contact address. The service provider can also rely on this periodic message to infer if the device is online and functional. Each device takes only one local IP address that is either statically assigned in the device's configuration, or dynamically obtained from a local DHCP server. The  $SPn$  services (for  $n = 1, 2, 3$ , and  $4$ ) each use a different local contact port for sending and receiving SIP messages (defaults are 5060, 5061, 5062, and 5063).



Dynamic address binding through periodic registration is not strictly necessary if the local IP address of the device does not change. The device's contact address can be statically configured on the Registration server.

## SIP Outbound Proxy Server

An outbound proxy server can be configured on the device such that all outbound requests are sent via the outbound proxy server instead of directly to the SIP Proxy Server or Registration Server.

If the outbound proxy server is listening at a non-standard port, the correct port value must be specified in the **OutboundProxyPort** parameter. The **OutboundProxy** can use a different transport protocol from the **ProxyServer**. The transport protocol to use to communicate with the **OutboundProxy** can be set in the **OutboundProxyTransport** parameters. If **OutboundProxyTransport** is TCP or TLS, your device initiates a TCP or TLS connection only with the **OutboundProxy**. All subsequent messages exchanged between your device and the servers MUST use the same connection. If for any reason the connection is closed, your device attempts to re-establish the connection with the **OutboundProxy** following an exponential back-off retry pattern.

Even though your device only exchanges messages directly with the **OutboundProxy**, the **ProxyServer**, **ProxyServerPort**, and **ProxyServerTransport** parameters are still very much relevant and important since the SIP requests sent by your phone to the server are formed based on these values, not based on the **OutboundProxy** value. The **OutboundProxy** value should never appear in the SIP requests generated by your device, unless the **OutboundProxy** parameter has the same value as **ProxyServer**.

Some server implementations include the outbound proxy server in a Record-Route header such that your device should not respect the locally configured **OutboundProxy** value after the initial INVITE is sent for a new call. This behavior can be achieved by enabling the **ITSP Profile X –**

**SIP::X\_BypassOutboundProxyInCall** option. However, this option has no effect when the **OutboundProxyTransport** is TCP or TLS, as your device always uses the same connection to send messages to the server.

## DNS Lookup of SIP Servers

When sending out SIP requests to the server, the device looks up the IP address of the server using standard DNS query if the server is specified as a domain name instead of an IP address. If an Outbound

Proxy Server is configured, it is used instead of the SIP Proxy Server or SIP Registration Server. The resolution of the server domain name into IP address is performed in the following manner:

- Try looking up the name as DNS A Record. If not found,
- Try looking up the name as DNS SRV Record. If not found,
- Try looking up the name as DNS SRV Record with “\_sip.\_udp.” prepended to the host name. If not found, fail the request.

If the result from the DNS query is an SRV record, the server port is taken from that record also. The server port value configured on the device is ignored. Otherwise, the server port is taken from the configured value or uses port 5060 if none is specified.

## ***NAT Traversal Considerations***

If the device sits behind a NAT router (typically the case), it can discover the mapped external address corresponding to its local SIP contact address as seen by the server in one of the following ways:

- From the “received=” and “rport=” parameters of the VIA header of the REGISTER response sent by the server. These two parameters tell the device its mapped IP address and port number. This method is used if periodic registration is enabled on the device.
- From the response to a STUN binding request the device sent to a STUN server. This method is used by enabling **X\_KeepAliveEnable** and setting **X\_KeepAliveMsgType** to “stun”. In that case, the STUN server is taken from **X\_KeepAliveServer**, if it is specified. Otherwise, the keep-alive messages are sent to the same server where a REGISTER request would be sent to. The latter is the most effective way of using STUN to discover the mapped external contact address.

The device always uses the mapped external contact address in all outbound SIP requests instead of its local contact address if one is discovered by either method discovered above.

## ***SIP Proxy Server Redundancy and Dual REGISTRATION***

Server Redundancy specifically refers to the device’s capability to a) look for a working server to REGISTER with from among a list of candidates, and b) switch to another server once the server that it currently registers with becomes unresponsive. In other words, device registration must be enabled in order to use the server redundancy feature. Other SIP requests, such as INVITE or SUBSCRIBE, are sent to the same server that the device currently registers with.

If Outbound Proxy Server is provided, server redundancy is applied to the Outbound Proxy Server instead of the REGISTRATION server. Server redundancy behavior is enabled by enabling the **ITSP Profile X – SIP::X\_ProxyServerRedundancy** parameter, which is disabled by default.

Another requirement for using the server redundancy feature is that the underlying server must be configured in the device as a domain name instead of an IP address. This allows the device to collect a list of candidate servers based on DNS query.

The domain name can be looked up as DNS A record or DNS SRV record. For A records, all the IP addresses returned by the DNS server are considered to have the same priority. For SRV records, the hosts returned by the DNS server can be each assigned a different priority.

After a list of candidate servers are obtained, the device first looks for a working server according to the stated priority. A *working server* means one that the device can successfully register with. This is known as the *Primary Server*. Subsequently, the device maintains registration with the primary server the usual way. However, if no working server is found after traversing the entire list, the device takes a short break and repeats the search in the same order.

While maintaining registration with the primary server, the device continually attempts to fall back to one of the candidate servers that has higher priority than the primary server, if any. The list of candidate servers that the device is trying to fall back on is known as the *primary fallback list*, which may be empty.

In addition, the device can be configured to maintain a secondary registration with a server that has lower or equal priority than the primary server. Secondary registration can be enabled by setting the parameter **X\_SecondaryRegistration** to YES. If **X\_ProxyServerRedundancy** is NO, however, **X\_SecondaryRegistration** does not take effect. If this feature is enabled, as soon as a primary server is found, the device searches for a working secondary server in the same manner from the list of candidate servers that are of lower or equal priority than the primary server. Similarly, once a secondary server is found, the device forms a *secondary fallback list* to continually attempt to fall back on if the list is not empty.

The interval for checking the primary fallback list and the secondary fallback list are configured in the **X\_CheckPrimaryFallbackInterval** and **X\_CheckSecondaryFallbackInterval** parameters. These parameters are specified in seconds and the default value is 60 for both.

Notes:

- If a secondary server exists it implies a primary server exists.
- If the secondary server exists, it immediately becomes the primary server when the current primary server fails. The device then starts searching for a new secondary server if the candidate set is not empty.
- The candidate list can change (be lengthened, shortened, priority changed, etc.) on every DNS renewal (based on the entry's TTL). The device rearranges the primary and secondary servers and fallback lists accordingly.

If the server redundancy feature is disabled, the device resolves only one IP address from the server's domain name, and won't try other IP addresses if the server is not responding.

## SIP Privacy

The device observes inbound caller privacy and decodes the caller's name and number from SIP INVITE requests by checking the FROM, P-Asserted-Identity (PAID), and Remote-Party-ID (RPID) message headers. All these headers can carry the caller's name and number information.

If PAID is present, the device takes the name and number from it. Otherwise, it takes the name and number from RPID if it is present, or from the FROM header otherwise. RPID, if present, includes the privacy setting desired by the caller. This privacy can indicate one of the following options:

- *off* = no privacy requested; the device shows name and number.
- *full* = full privacy requested; the device hides both name and number.
- *name* = name privacy requested; the device shows the number but hides the name.
- *uri* = uri privacy requested; the device shows the name but hides the number.

Regardless, if PAID exists or not, the device always takes the privacy setting from the RPID if it is present in the INVITE request.



If the resulting call name is Anonymous (case-insensitive), the device treats it as if the caller is requesting full privacy.

For outbound calls, the caller's preferred privacy setting can be stated by the device in a RPID header of the outbound INVITE request. To enable this behavior, the **ITSP Profile X – SIP::X\_InsertRemotePartyID** parameter must be set to YES or TRUE, which is the default value of this parameter. The device supports only two outbound caller privacy settings: privacy=off or privacy=full. The RPID header generated by the device carries the same name and number as the FROM header. If outbound caller-ID is blocked, the device sets privacy=full in RPID, and also sets the display name in the FROM and RPID headers to Anonymous for backward compatibility. The device won't insert PAID in outbound INVITE requests.

## STUN and ICE

The device supports standard STUN based on RFC3489 and RFC5389 for passing inbound RTP packets to the device sitting behind NATs. The parameters that control the STUN feature are found in the **ITSP Profile X – General::** section:

- **STUNEnable** – Enables this feature (default is NO or FALSE).
- **STUNServer** – The IP address or domain name of the external STUN server to use. The STUN feature is disabled if this value is blank, which is the default.
- **X\_STUNServerPort** – The STUN Server's listening UDP port. Default value is 3478 (standard STUN port).

The STUN feature used in this context is only for RTP packets, not SIP signaling packets, which typically do not require STUN. The device sends a STUN binding request right before making or answering a call on SP1/2. If the request is successful, the device decodes the mapped external address and port from the binding response and uses them in the m= and c= lines of its SDP offer or answer sent to the peer device. If the request fails, such as STUN server not found or not responding, the call goes on without using external address in the SDP.

Standard RTP requires the use of an even-numbered port in the m= line. If the external port is not an even number, the device changes the local RTP port and redoes STUN, and continues to do this as many as four times or until an even external port number is found. If the fourth trial still results in an odd external port number, the call goes on without using an external address in the SDP.

The device supports standard ICE based on RFC5245. ICE is done on a per-call basis for automatically discovering which peer address is the best route for sending RTP packets. To enable ICE on the device, set the **ITSP Profile X – General::X\_ICEEnable** parameter to YES (or TRUE). The default is NO (or FALSE).

ICE is effective if STUN is also enabled. However, STUN is not a requirement for using ICE on the device. If STUN is enabled and an external RTP address different from its local address is discovered, the device offers two ICE candidates in its SDP:

- The local (host) address (highest priority)
- The external (srflx or server reflexive) address

Otherwise, only the local host candidate is shown in the device's SDP.



The device uses the srflx address in the m= and c= lines of the SDP if STUN is enabled and successful.

If ICE is enabled and the peer's SDP has more than one candidate, the device sends STUN requests to each peer candidate from its local RTP port. As soon as it receives a response from the highest priority candidate, the device concludes ICE and uses this candidate to communicate with the peer. Otherwise, the



device allows as long as 5 seconds to wait for the response from all the candidates, and selects the highest priority candidate that has a response. Once ICE completes successfully, the device further applies symmetric RTP to determine the peer's RTP address (that is, sends them to the address from which the peer's RTP packets are coming).

## ITSP Driven Distinctive Ringing

The device offers 10 ring and 10 call-waiting tone patterns in each ring profile. These patterns are numbered from 1 to 10. Each pattern also comes with a configurable name. You can assign a different default ring to each trunk on the device.

An ITSP can tell the device which ring to use by name for a call routed to SP1/SP2 by inserting an Alert-Info header in the SIP INVITE sent to the device. The Alert-Info must include a URI. For example:

Alert-Info: `http://www.xyz.com/some-folder/bellcore-dr4`

When the device receives this, it looks for a ring tone name or call-waiting tone name in the ring profile that matches the Alert-Info URI. Ring tone names are not case sensitive. If a match is found, the device plays the corresponding ring or call-waiting tone. Otherwise, the device plays the default ring.

## RTP Statistics – the X-RTP-Stat Header

When ending an established call, the device can include a summary of the RTP statistics collected during the call in the SIP BYE request or the 200 response to the SIP BYE request sent by the peer device. The summary is carried in an X-RTP-Stat header in the form of a comma-separated list of fields. The reported fields are:

- PS = Number of Packets Sent
- PR = Number of Packets Received
- OS = Number of bytes sent
- OR = Number of bytes received
- PL = Number of packets lost
- JI = Jitter in milliseconds
- LA = Decode latency or jitter buffer size in milliseconds
- DU = Call duration in seconds
- EN = Last Encoder Used
- DE = Last Decoder Used

For example:

`X-RTP-Stat:PS=1234,OS=34560,PR=1236,OR=24720,JI=1,DU=1230,PL=0,EN=G711U, DE=G711U`

To enable the X-RTP-Stat feature, set the **ITSP Profile X – SIP::X\_InsertRTPStats** parameter to YES (or TRUE).

## Media Loopback Service

The device supports the media loopback draft as described in *draft-mmusic-media-loopback-13.txt*. The device supports the following media loopback features:

- Loopback modes: `loopback-source` and `loopback-mirror`

- Loopback types: `rtp-media-loopback` and `rtp-packet-loopback`
- Loopback packet formats: `encaprtp`, `loopbkprimer`

When the device acts as a loopback mirror, it always sends primer packets so that incoming packets can get through NAT/Firewall. The media loopback feature is controlled by the following parameters (in the **Phone Port – Calling Features** section):

- **AcceptMediaLoopback** – Enable device to accept incoming call that requests media loopback. Default is YES.
- **MediaLoopbackAnswerDelay** – The delay in ms before the device answers a media loopback call. Default is 0.
- **MediaLoopbackMaxDuration** – The maximum duration to allow for an incoming media loopback call. Default is 0, which means the duration is unlimited.

The device rejects an incoming media loopback call if:

- Phone port is off-hook.
- Phone port is ringing.

The device terminates an inbound media loopback call already in progress when:

- Phone port is off-hook.
- Phone port is ringing.

The outbound Media Loopback Call is not subjected to call duration limit; it lasts until the user hangs up or until the called device ends the call.

For more information on general ITSP parameters, see the [ITSP Profile A & B \(General and SP Info Settings\) Parameter Guide](#) table in the [Parameter Reference Guide](#) section.

For more information on ITSP SIP settings parameters, see the [ITSP SIP Settings Parameter Guide](#) table in the [Parameter Reference Guide](#) section.

For more information on ITSP RTP settings parameters, see the [ITSP RTP Settings Parameter Guide](#) table in the [Parameter Reference Guide](#) section.

## Using SP $n$ as a Proxy for a SIP IP Phone

An SP service can be set up as a proxy for a legacy IP phone to allow the phone to access the OBiTALK installed on the device. This proxy mode of operation must be explicitly enabled in the SP's configuration on the device. It is disabled by default. The IP phone using this proxy service is known as the *local\_client* of the SP service. It must be installed on the LAN side of the device.

In this mode, SP $n$  accepts SIP Registration from the client device from the LAN side, which must be using the same user-id and password as this SP $n$ 's **AuthUserName** and **AuthPassword** parameters for authentication. This client device can also send SIP INVITE to the device at this SP to make calls; this SP's **InboundCallRoute** must be set up with the proper routing rule to handle calls from the *local\_client*.

The SIP Proxy Server parameter on the client device must be sent to:

```
<obi-number>.pnn.obihai.com:<spn-user-agent-port>
```

where `<obi-number>` is the 9-digit OBi number of this device, and `<spn-user-agent-port>` is SP $n$ 's **X\_UserAgentPort** parameter.

For example, SP1 has a *local\_client* with the user-id 4086578118. The client wishes to make and receive calls on SP3. The SP1 **InboundCallRoute** shall include the following rule:

```
{4086578118>:sp3}
```

The SP3 **InboundCallRoute** shall be: {sp1(408657118@local\_client)}

For more information on SP $n$  services parameters, see the [SP \$n\$  Services Parameter Guide](#) table in the [Parameter Reference Guide](#) section.

## Automated Attendant

The device call processing Automated Attendant (AA) is invoked by including “aa” in the inbound call routing rule associated the interface on the device processing an incoming call. When connecting to the AA in this manner, there are two options at present.



The HDA50 supports only one session of AA at a time. Additional calls routed to the AA while a session is in progress are rejected by the AA as busy.

## Customizing AA Prompt Lists

AA does not play individual user prompts directly. Instead it plays a comma-separated list of prompt elements, known as a *Prompt List*. A prompt element can be a user prompt with optional parameters, or a control element. A user prompt is referred as %User<N>% where <N> = 1 – 10. In a prompt list this can be followed by a ;r=<start>-<end> parameter that specifies the range to play for that prompt, where

<start> = starting time mark in milliseconds. 0 is the default if <start> is omitted.

<end> = ending time mark in milliseconds. the end of the prompt is the default if <end> is omitted.

If the r= parameter is omitted, the full range of the prompt is played.

Examples:

%User1%;r=1000 means play the User1 prompt starting at 1000 ms mark to the end.

%User2% means play the entire User2 prompt from start to finish.

%User3%;r =1300-3720 means play the User3 prompt starting from the1300 ms mark to the 3720 ms mark.

%User4%;r=3200-1200 means don't play anything since <end> is less than <start>.

Each prompt list control elements starts with a ‘&’ in a prompt list. The following control elements are supported: &pause(<duration>) means pause playing for a number of seconds as given by the <duration> parameter.

An example prompt list:

```
%User1%;r=105,&pause(3),%User5%,%User9%;r=0-1350,&pause(15)
```

You can replace any of the following AA prompt lists with your own specified prompt lists:

### Automated Attendant Prompt Lists

AA Prompt List	System Default	Prompt To Be Played
Welcome	Welcome to OBi Attendant.	Once, at the beginning when the AA starts.
InvalidPin	Invalid PIN.	After user enters an invalid PIN.
EnterPin	Enter PIN.	Prompts user to enter a valid PIN.
MenuTitle	Main Menu.	Once, after Welcome and before announcing the menu options.
Menu	Press 1 to continue this call. Press 2 to make a new all. Press 3 to enter a callback number.	A couple of times after MenuTitle.
PleaseWait	Please wait while your call is being connected.	Once, after user enters a phone number to call.
EnterNumber	Enter number followed by the # key.	Prompts user to enter a valid number after option 2 or option 3 is selected by the user.
Bye	Thank you for choosing Obihai Technology. Goodbye.	When user presses * or # key to leave the AA.

For more information on user prompts parameters, see the [User Prompts Parameter Guide](#) table in the [Parameter Reference Guide](#) section.

For more information on Auto Attendant parameters, see the [Automated Attendant Parameter Guide](#) table in the [Parameter Reference Guide](#) section.

For more information on Auto Attendant prompt parameters, see the [Auto Attendant Prompt Parameter Guide](#) table in the [Parameter Reference Guide](#) section.

## Trunk Groups

As the name implies, a trunk group is a group of trunks. If a call is routed to a trunk group, the device picks one of the available trunks from the group to make the call. Availability of trunk is based on:

- Whether the trunk's digit map allows the number to call
- Whether the trunk has capacity to make one more call

As many as four trunk groups can be configured on a device. Each trunk group is conceptually another trunk with its own **DigitMap**. A trunk group and its associated **DigitMap** are referenced using the short names  $TG_n$  and  $(Mtg_n)$ , where  $n = 1, 2, 3, 4$ . They can be referenced in other digit maps and call routing rules so that calls can be routed to a particular trunk group.

Only trunks can be added to a trunk group. These include: PP1, SP1, SP2, SP3, SP4, LI1, VG1, VG2, ..., VG8, TG1, TG2, ... TG4. A TG can include another TG (that is, TG can be recursive). However, you must make sure this does not result in infinite recursion.

For more information on trunk group parameters, see the [Trunk Group Parameter Guide](#) table in the [Parameter Reference Guide](#) section.

# Parameter Reference Guide

This section lists the HDA50 parameters in the order shown on the device native web page.

Depending on your device or your settings, the device native web page may not present all of these parameters to you.

## System Status Settings

Parameter	Description	Example Value
<i>WAN Status</i>		
<b>AddressingType</b>	Method currently used by the phone to get an IP address assignment.	DHCP
<b>IPAddress</b>	IP address currently assigned to the phone when using static IP addressing.	192.168.15.165
<b>SubnetMask</b>	Subnet mask to use when using static IP addressing.	255.255.255.0
<b>DefaultGateway</b>	Gateway to use when using static IP addressing.	192.168.15.1
<b>DNSServer1</b>	URL for domain name server 1 when using static IP addressing.	8.4.4.4
<b>DNSServer2</b>	URL for domain name server 2 when using static IP addressing.	4.2.2.2
<b>MACAddress</b>	MAC address installed on the phone.	9CADEF90004E
<b>LLDP-MEDStatus</b>	Enables LLDP media endpoint discovery for improved network connections.	Enabled
<b>802_1XStatus</b>	802_1X status.	
<b>802_1XAuthenticationStatus</b>	802_1X authentication status.	Held
<b>SWPortLinkStatus</b>	Status of the switch port (the port connecting the phone to the Internet).	Link:Y; Spd:100F; Auto:N
<b>PCPortLinkStatus</b>	Status of the PC port (the port connecting the phone to an auxiliary PC).	Link:N; Spd:100F; Auto:Y
<b>Stats</b>	Ethernet statistics.	P/E: Rx=82276/0; Tx=5538/0

**Call Status**

Status	Description
Terminal ID	A short name to identify each call terminal: Phone, SP1, SP2, SP3, SP4, SP5, SP6, OBiTALK.
State	Call State.
Peer Name	Call Peer's Name.
Peer Number	Call Peer's Number.
Start Time	Starting time of the call.
Duration	Duration of the call.
Peer RTP Address	The peer address and port where RTP packets are sent to.
Local RTP Address	The local address and port where RTP packets are sent from.
RTP Transport	The transport used for RTP (UDP, TCP, or SSL).
Audio Codec	The audio encoder and decoder being used for this call.
RTP Packetization (ms)	The transmitted and received packet sizes in milliseconds.
RTP Packet Count	Total number of RTP packets transmitted and received thus far.
RTP Byte Count	Total number of RTP bytes transmitted and received thus far.
Peer Clock Differential Rate	Clock difference between this phone and the peer in ppm (parts per million).
Packets in Jitter Buffer	Number of packets in the Jitter Buffer.
Packets Out-of-Order	Number of received RTP packets that are out of order.
Packets (10ms) Interpolated	Number of frames interpolated.
Packets Lost	Number of incoming RTP packets assumed lost.
Packet Loss Rate	Amount of incoming RTP packets assumed lost rate in percent.
Packet Drop Rate	Amount of incoming RTP packets dropped in percent.
Jitter Buffer Length	Size of the current jitter buffer in milliseconds.
Received Interarrival Jitter	Average measured network jitter in the received direction in milliseconds.
DTMF Digits Received	Number of DTMF digits received.
Jitter Buffer Underruns	Amount of jitter buffer underruns during the call.
Jitter Buffer Overruns	Amount of jitter buffer overruns during the call.
Sequence number discontinuities	Number of times a discontinuity is encountered in the sequence number of the incoming RTP stream.
Round-Trip Propagation Delay	A measurement of the round trip propagation delay of RTP packets.

**Call Status**

Status	Description
End System Delay	Contribution to the overall end-to-end system delay by this end-point in milliseconds as defined in RFC3611.
Peer End System Delay	Contribution to the overall end-to-end system delay by the peer end-point in milliseconds as defined in RFC3611.
MOS-LQ	The estimated mean opinion score for listening quality.
MOS-SQ	The estimated mean opinion score for conversational quality.

**Call History**

This page shows the calls in the call history, in order of most recent to oldest.

The following buttons are available:

- **Remove All:** Pressing this button erases the entire call history.
- **Save All:** Pressing this button saves the call history to the `callhistory.xml` file.

The **Call History** page isn't available on the [OBiTALK.com](http://OBiTALK.com) website.

**SP Services Settings**

Parameter	Description	Default Setting
<i>Reset Statistics, n = 1 – 6</i>		
<b>ResetStatistics</b>	Check this option and press <b>Submit</b> to reset the statistics for this SP Service.	NA
<i>RTP Statistics, n = 1 – 6</i>		
<b>PacketsSent</b>	Total RTP packets sent on this line.	NA
<b>PacketsReceived</b>	Total RTP packets received on this line.	NA
<b>BytesSent</b>	RTP payload bytes sent for this line.	NA
<b>BytesReceived</b>	RTP payload bytes received for this line.	NA
<b>PacketsLost</b>	Number of RTP packets lost on this line.	NA
<b>Overruns</b>	Number of times a jitter buffer overrun was received on this line.	NA
<b>Underruns</b>	Number of times a jitter buffer underrun was received on this line.	NA

**PHONE Port Status**

Status	Description
Port Status	
State	Status of the Phone 1 and Phone 2 ports.
LoopCurrent	Loop current in mA for Phone 1 and Phone 2 ports.
VBAT	Battery voltage for Phone 1 and Phone 2 ports.
TipRingVoltage	Sensed differential between tip and ring voltage for Phone 1 and Phone 2 ports.
LastCallerInfo	Last caller ID for Phone 1 and Phone 2 ports.

Statistics relevant to  $SP_n$  can be found on the  $SP_n$  Stats page (where  $n = 1, 2, 3, 4$ ).

**Services, Phone, and Line Status Parameter Guide**

Parameter	Description	Default Setting
<b>ResetStatistics</b>		
<b>ResetStatistics</b>	Resets the statistics for this voice service.	N/A
<b>RTP Statistics</b>		
<b>PacketsSent</b>	Total RTP packets sent on this line.	N/A
<b>PacketsReceived</b>	Total RTP packets received on this line.	N/A
<b>BytesSent</b>	RTP payload bytes sent for this line.	N/A
<b>BytesReceived</b>	RTP payload bytes received for this line.	N/A
<b>PacketsLost</b>	Number of RTP packets lost on this line.	N/A
<b>Overruns</b>	Number of times receive jitter buffer overrun on this line.	N/A
<b>Underruns</b>	Number of times receive jitter buffer underrun on this line.	N/A

**Port Status Parameter Guide**

Parameter	Description	Default Setting
<b>Port Status</b>		
<b>State</b>	Port status, such as on-hook, off-hook, ringing.	N/A
<b>LoopCurrent</b>	Loop current in mA.	N/A



## Port Status Parameter Guide

Parameter	Description	Default Setting
<b>VBAT</b>	Phone port battery voltage in volts.	N/A
<b>TipRingVoltage</b>	Sensed differential Tip/Ring voltage in volts.	N/A
<b>LastCallerInfo</b>	Caller ID of previous call.	N/A

## Network Settings Parameter Guide

Parameter	Description	Default Setting
<b>Internet Settings</b>		
<b>AddressingType</b>	The method used for assigning IP address, subnet mask, default gateway, etc., to the device. Choose from: <ul style="list-style-type: none"> <li><b>DHCP</b>: IP address, default gateway, etc. are assigned by DHCP Server</li> <li><b>Static</b>: IP address, default gateway, etc. are taken from the manually configured values.</li> <li><b>PPPoE</b>: IP address default gateway, etc. are acquired by PPPoE Protocol (OBi202, OBi302 only).</li> </ul>	DHCP
<b>IPAddress</b>	IP address to assign to the device when <b>AddressingType</b> is set to <i>Static</i> .	
<b>SubnetMask</b>	Subnet mask to use when <b>AddressingType</b> is set to <i>Static</i> .	
<b>DefaultGateway</b>	Default gateway IP address to assign to the device when <b>AddressingType</b> is set to <i>Static</i> .	
<b>DNSServer1</b>	IP address of the first DNS server to use, in addition to the ones obtained from the DHCP server when DHCP is also enabled. If <b>AddressingType</b> is set to <i>Static</i> , the device only uses <b>DNSServer1</b> and <b>DNSServer2</b> for DNS lookup. It tries as many as five DNS servers when attempting to resolve a domain name. <b>DNSServer1</b> and <b>DNSServer2</b> are tried first, whichever is specified, and then the addresses obtained from the DHCP Server if available.	
<b>DNSServer2</b>	IP address of the second DNS server to use, in addition to the ones obtained from the DHCP server when DHCP is also enabled. If <b>AddressingType</b> is set to <i>Static</i> , the device only uses <b>DNSServer1</b> and <b>DNSServer2</b> for DNS lookup. It tries as many as five DNS servers when attempting to resolve a domain name. <b>DNSServer1</b> and <b>DNSServer2</b> are tried first, whichever is specified, and then the addresses obtained from the DHCP Server if available.	
<b>Local Time</b>		
<b>CurrentLocalTime</b>	Current local date and time of the device (read-only parameter).	

## Network Settings Parameter Guide

Parameter	Description	Default Setting
<b>Time Service Settings</b>		
<b>NTPServer1</b>	Host name or IP address of the first NTP server.	pool.ntp.org
<b>NTPServer2</b>	Host name or IP address of the second NTP server.	
<b>LocalTimeZone</b>	<p>Local time zone. Choose from:</p> <ul style="list-style-type: none"> <li>• GMT-12:00 (Int'l Dateline West)</li> <li>• GMT-11:00 (Samoa)</li> <li>• GMT-10:00 (Hawaii)</li> <li>• GMT-09:00 (Alaska)</li> <li>• GMT-08:00 (Pacific Time)</li> <li>• GMT-07:00 (Mountain Time)</li> <li>• GMT-06:00 (Central Time)</li> <li>• GMT-05:00 (Eastern Time)</li> <li>• GMT-04:00 (Atlantic Time)</li> <li>• GMT-03:30 (Newfoundland)</li> <li>• GMT-03:00 (Buenos Aires, Greenland)</li> <li>• GMT-02:00 (Mid-Atlantic)</li> <li>• GMT-01:00</li> <li>• GMT+00:00 (London, Lisbon)</li> <li>• GMT+01:00 (Rome, Paris, Madrid)</li> <li>• GMT+02:00 (Athens, Cairo)</li> <li>• GMT+03:00 (Moscow, Baghdad)</li> <li>• GMT+04:00 (Abu Dhabi)</li> <li>• GMT+04:30 (Kabul)</li> <li>• GMT+05:00 (Islamabad, Karachi)</li> <li>• GMT+05:30 (New Delhi)</li> <li>• GMT+05:45 (Kathmandu)</li> <li>• GMT+06:00</li> <li>• GMT+07:00 (Bangkok, Jakarta)</li> <li>• GMT+08:00 (Beijing, HK, Singapore)</li> <li>• GMT+09:00 (Tokyo, Seoul)</li> <li>• GMT+10:00 (Sydney, Guam)</li> <li>• GMT+11:00 (Solomon Is.)</li> <li>• GMT+12:00 (Fiji, Auckland)</li> </ul>	GMT-08:00 (Pacific Time)
<b>DaylightSavingTimeEnable</b>	Enables daylight saving time on the unit.	Yes

## Network Settings Parameter Guide

Parameter	Description	Default Setting
<b>DaylightSavingTimeStart</b>	Daylight Saving Time Start Date. Format: month/day/weekday/hh:mm:ss, where month=1-12, day=±(1-31), weekday=0,1-7 (0=special, 1=Monday, 7=Sunday), hh=0-23, mm=0-59, ss=0-59. If weekday=0, daylight saving starts on the given month/day; otherwise it starts on the weekday on or after the given month/day if day > 0, or on the weekday on or before the last-day-of-given-month+day+1 (note that day = -1 equivalent to last day of the month). :ss can be omitted if the value is 0. :mm:ss can be omitted if mm and ss are both 0.	3/8/7/2
<b>DaylightSavingTimeEnd</b>	Daylight Saving Time End Date. Same format as Start Date.	11/1/7/2
<b>DaylightSavingTimeDiff</b>	Amount of time to add to current time during Daylight Saving Time. Format: [-]hh:mm:ss. :ss can be omitted if it is 0. :mm:ss can be omitted if both are 0.	1
<b>DNS Control</b>		
<b>DNSQueryOrder</b>	When more than one DNS servers are available, the unit attempts to resolve a domain name by querying each server sequentially until a successful result is received. The parameter controls the order in querying the servers. Choose from: <ul style="list-style-type: none"> <li>DNS Server1, DNS Server2, DHCP Offered DNS Servers</li> <li>DHCP Offered DNS Servers, DNS Server1, DNS Server2</li> </ul>	DNS Server1, DNS Server2, DHCP Offered DNS Servers
<b>DNSQueryDelay</b>	When multiple DNS servers are available, the unit attempts to resolve a domain name by querying each server sequentially until a successful result is received. This parameter controls the number of seconds between successive DNS query made by the unit for a given domain name. Choose from 0 to 5 seconds.	2

## Network Settings Parameter Guide

Parameter	Description	Default Setting
<b>Local DNS Records</b>		
<b>N where N = 1 – 32</b>	<p>One of 32 <b>Local DNS Records</b> (numbered 1 – 32). Each record is a mini script of the following format:</p> <pre>Name=A,A,A,...</pre> <p>or</p> <pre>Name=R,R,R,...</pre> <p>where <i>Name</i> represents the domain name to be resolved locally, and has the format <code>prefix+domain</code> (such as <code>machine.sip+obihai.com</code>). Everything after '+' is considered as the domain to be appended to the host field in each <i>R</i> on the right hand side. '+' is optional; if missing, the full domain must be used in every <i>R</i>.</p> <p><i>A</i> represents an <i>A</i> record that is just an IP address, such as <code>192.168.12.17</code>.</p> <p><i>R</i> represents an SRV record and has the format:</p> <pre>{host:port,pri,wt}</pre> <p>where</p> <ul style="list-style-type: none"> <li><i>host</i> is a host name with or without domain part (such as <code>xyz</code>, <code>xyz.abc.com.</code>). A dot (.) at the end of host indicates it is a complete host name that does not require the domain to be appended.</li> <li><i>port</i> is a port number (such as 5060)</li> <li><i>pri</i> is the priority. Valid value is 0 (highest) – 65535 (lowest)</li> <li><i>wt</i> is the weight. Valid value is 0 (lowest) – 65535 (highest). <i>wt</i> is optional. If not specified, the default is 1.</li> <li><i>pri</i> is optional only if <i>wt</i> is not specified. 1 is the default if not specified.</li> <li><i>port</i> is optional. The default to use is based on the protocol (5060 for SIP, 80 for HTTP, and so forth).</li> </ul> <p>The enclosing curly braces { } are also optional if there is only one <i>R</i>; or if there is no comma used inside the <i>R</i>.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li><code>_sip._udp+obihai.com=abc,xyz,pqr:5080,{mmm,2},{super.abc.com.}</code></li> <li><code>abc.obihai.com=192.168.15.118,192.168.15.108</code></li> </ul> <p>If the <i>A</i> record of a given host name can't be found in any of the <b>Local DNS Records</b>, the device attempts to resolve it using external DNS queries.</p> <p>Any change applied to <b>Local DNS Record</b> needs a reboot in order to take effect.</p>	

## WAN Settings Parameter Guide

Parameter	Description	Default Setting
<b>Internet Settings</b>		
<b>AddressingType</b>	The method used for assigning IP address, subnet mask, default gateway, etc., to the device. Choose from: <ul style="list-style-type: none"> <li><b>DHCP</b>: IP address, default gateway, etc. are assigned by DHCP Server</li> <li><b>Static</b>: IP address, default gateway, etc. are taken from the manually configured values</li> <li><b>PPPoE</b>: IP address default gateway, etc. are acquired by PPPoE Protocol (OBI202, OBI302 only)</li> </ul>	DHCP
<b>IPAddress</b>	The IP address to assign to the device when <b>AddressingType</b> is set to <i>Static</i> .	
<b>SubnetMask</b>	The subnet mask to use when <b>AddressingType</b> is set to <i>Static</i> .	
<b>DefaultGateway</b>	The default gateway IP address to assign to the device when <b>AddressingType</b> is set to <i>Static</i> .	
<b>DNSServer1</b>	IP address of the first DNS server to use, in addition to the ones obtained from the DHCP server when DHCP is also enabled. If <b>AddressingType</b> is set to <i>Static</i> , the device only uses <b>DNSServer1</b> and <b>DNSServer2</b> for DNS lookup. It tries as many as five DNS servers when attempting to resolve a domain name. <b>DNSServer1</b> and <b>DNSServer2</b> are tried first, whichever is specified, and then the addresses obtained from the DHCP Server if available.	
<b>DNSServer2</b>	IP address of the second DNS server to use, in addition to the ones obtained from the DHCP server when DHCP is also enabled. If <b>AddressingType</b> is set to <i>Static</i> , the device only uses <b>DNSServer1</b> and <b>DNSServer2</b> for DNS lookup. It tries as many as five DNS servers when attempting to resolve a domain name. <b>DNSServer1</b> and <b>DNSServer2</b> are tried first, whichever is specified, and then the addresses obtained from the DHCP Server if available.	
<b>PPPoEACName</b>	PPPoE access concentrator name. Enter if it is required.	
<b>PPPoEServiceName</b>	PPPoE service name. Enter if it is required.	
<b>PPPoEUsername</b>	PPPoE account username provided by your ISP.	
<b>PPPoEPassword</b>	PPPoE account password.	
<b>VLANID</b>	Valid range is 0 – 4094 (4095 is reserved). 0 means VLAN is disabled and egress packets are not tagged by the device. This setting applies to all packets sent by the device.	0

## WAN Settings Parameter Guide

Parameter	Description	Default Setting
<b>VLANPriority</b>	Choose from 0 – 7. This setting applies to all packets sent by the device.	0
<b>802_1XMode</b>	Authentication is enabled or disabled with the selected mode. Choice of: <ul style="list-style-type: none"> <li>• Disable</li> <li>• MD5</li> <li>• TLS</li> <li>• TTLS-MSCHAPv2</li> <li>• PEAP-MSCHAPv2</li> </ul>	Disable
<b>802_1XIdentity</b>	User name for 802.1x authentication.	None
<b>802_1XPassword</b>	Password for EAP-MD5, EAP-TTLS Private key, and EAP-TTLS/MSCHAPv2 modes.	None
<b>802_1XAnonymousID</b>	Anonymous ID. If empty, an anonymous ID is used in authentication.	None
<b>802_1XTLSecurityProfile</b>	Security profile for 802.1x authentication. Choices are 1 or 2.	1
<b>Local Time</b>		
<b>CurrentLocalTime</b>	Current local date and time of the device (read only).	
<b>Time Service Settings</b>		
<b>NTPServer1</b>	Host name or IP address of the first NTP server.	pool.ntp.org
<b>NTPServer2</b>	Host name or IP address of the second NTP server.	

## WAN Settings Parameter Guide

Parameter	Description	Default Setting
<b>LocalTimeZone</b>	<p>Local time zone. Choose from:</p> <ul style="list-style-type: none"> <li>• GMT-12:00 (Int'l Dateline West)</li> <li>• GMT-11:00 (Samoa)</li> <li>• GMT-10:00 (Hawaii)</li> <li>• GMT-09:00 (Alaska)</li> <li>• GMT-08:00 (Pacific Time)</li> <li>• GMT-07:00 (Mountain Time)</li> <li>• GMT-06:00 (Central Time)</li> <li>• GMT-05:00 (Eastern Time)</li> <li>• GMT-04:00 (Atlantic Time)</li> <li>• GMT-03:30 (Newfoundland)</li> <li>• GMT-03:00 (Buenos Aires, Greenland)</li> <li>• GMT-02:00 (Mid-Atlantic)</li> <li>• GMT-01:00</li> <li>• GMT+00:00 (London, Lisbon)</li> <li>• GMT+01:00 (Rome, Paris, Madrid)</li> <li>• GMT+02:00 (Athens, Cairo)</li> <li>• GMT+03:00 (Moscow, Baghdad)</li> <li>• GMT+04:00 (Abu Dhabi)</li> <li>• GMT+04:30 (Kabul)</li> <li>• GMT+05:00 (Islamabad, Karachi)</li> <li>• GMT+05:30 (New Delhi)</li> <li>• GMT+05:45 (Kathmandu)</li> <li>• GMT+06:00</li> <li>• GMT+07:00 (Bangkok, Jakarta)</li> <li>• GMT+08:00 (Beijing, HK, Singapore)</li> <li>• GMT+09:00 (Tokyo, Seoul)</li> <li>• GMT+10:00 (Sydney, Guam)</li> <li>• GMT+11:00 (Solomon Is.)</li> <li>• GMT+12:00 (Fiji, Auckland)</li> </ul>	GMT-08:00 (Pacific Time)
<b>DaylightSavingTimeEnable</b>	Enables daylight saving time on the unit.	Yes
<b>DaylightSavingTimeStart</b>	<p>Daylight Saving Time Start Date. Format: month/day/weekday/hh:mm:ss, where month=1-12, day=±(1-31), weekday=0, 1-7 (0=special, 1=Monday, 7=Sunday), hh=0-23, mm=0-59, ss=0-59.</p> <p>If weekday=0, daylight saving starts on the given month/day; otherwise it starts on the weekday on or after the given month/day if day &gt; 0, or on the weekday on or before the last-day-of-given-month+day+1 (note that day = -1 equivalent to last day of the month).</p> <p>:ss can be omitted if the value is 0.</p> <p>:mm:ss can be omitted if mm and ss are both 0.</p>	3/8/7/2

## WAN Settings Parameter Guide

Parameter	Description	Default Setting
<b>DaylightSavingTimeEnd</b>	Daylight Saving Time End Date. Same format as Start Date.	11/1/7/2
<b>DaylightSavingTimeDiff</b>	Amount of time to add to current time during Daylight Saving Time. Format: [-]hh:mm:ss. :ss can be omitted if it is 0. :mm:ss can be omitted if both are 0.	1
<b>DNS Control</b>		
<b>DNSQueryOrder</b>	When more than one DNS servers are available, the unit attempts to resolve a domain name by querying each server sequentially until a successful result is received. The parameter controls the order in querying the servers. Choose from: <ul style="list-style-type: none"> <li>DNS Server1, DNS Server2, DHCP Offered DNS Servers</li> <li>DHCP Offered DNS Servers, DNS Server1, DNS Server2</li> </ul>	DNS Server1, DNS Server2, DHCP Offered DNS Servers
<b>DNSQueryDelay</b>	When more than one DNS servers are available, the unit attempts to resolve a domain name by querying each server sequentially until a successful result is received. This parameter controls the number of seconds between successive DNS query made by the unit for a given domain name. Choose from 0 to 5.	2



## WAN Settings Parameter Guide

Parameter	Description	Default Setting
<b>Local DNS Records</b>		
<b>N where N = 1 – 32</b>	<p>One of 32 <b>Local DNS Records</b> (numbered 1 – 32). Each record is a mini script of the following format:</p> <pre>Name=A,A,A,... or Name=R,R,R,...</pre> <p>where <i>Name</i> represents the domain name to be resolved locally, and has the format <code>prefix+domain</code> (such as <code>machine.sip+obihai.com</code>). Everything after '+' is considered as the domain to be appended to the host field in each <i>R</i> on the right hand side. '+' is optional; if missing, the full domain must be used in every <i>R</i>.</p> <p><i>A</i> represents an <i>A</i> record that is just an IP address, such as <code>192.168.12.17</code>.</p> <p><i>R</i> represents an SRV record and has the format: <code>{host:port,pri,wt}</code> where</p> <ul style="list-style-type: none"> <li><i>host</i> is a host name with or without domain part (such as <code>xyz</code>, <code>xyz.abc.com</code>). A dot (.) at the end of host indicates it is a complete host name that does not require the domain to be appended.</li> <li><i>port</i> is a port number (such as 5060)</li> <li><i>pri</i> is the priority. Valid value is 0 (highest) – 65535 (lowest)</li> <li><i>wt</i> is the weight. Valid value is 0 (lowest) – 65535 (highest). <i>wt</i> is optional. If not specified, the default is 1.</li> <li><i>pri</i> is optional only if <i>wt</i> is not specified. 1 is the default if not specified.</li> <li><i>port</i> is optional. The default to use is based on the protocol (5060 for SIP, 80 for HTTP, and so forth).</li> </ul> <p>The enclosing curly braces { } are also optional if there is only one <i>R</i>; or if there is no comma used inside the <i>R</i>.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li><code>_sip._udp+obihai.com=abc,xyz,pqr:5080,{mmm,2}, {super.abc.com.}</code></li> <li><code>abc.obihai.com=192.168.15.118,192.168.15.108</code></li> </ul> <p>If the <i>A</i> record of a given host name can't be found in any of the <b>Local DNS Records</b>, the device attempts to resolve it using external DNS queries.</p> <p>Any change applied to <b>Local DNS Record</b> needs a reboot in order to take effect.</p>	

## LAN Settings Parameter Guide

Parameter	Description	Default Setting	
<b>LAN Settings</b>			
<b>CurrentRouterIPAddress</b>	The current IP address of the router on the LAN side (read only). It is blank if the device is operating in bridge mode.		
<b>OperationMode</b>	The Networking Operation Mode for the device. It can be one of the following values: <ul style="list-style-type: none"> <li>Router</li> <li>Bridge</li> </ul>	Router	
<b>RouterIPAddress</b>	The LAN side IP address to be used by the router. If it conflicts with the WAN side IP address, the device automatically picks a different LAN side IP address to resolve the conflict.	192.168.10.1	
<b>SubnetMask</b>	The LAN side Subnet Mask to be used by the router. It can be one of the following values: <ul style="list-style-type: none"> <li>255.255.255.0</li> <li>255.255.255.128</li> <li>255.255.255.192</li> <li>255.255.255.224</li> <li>255.255.255.240</li> <li>255.255.255.248</li> </ul>	255.255.255.0	
<b>DHCP Server Settings</b>			
<b>Enable</b>	Enables the DHCP Server on the LAN side.	Yes	
<b>ClientAddressRangeStart</b>	Together with the <b>CurrentRouterIPAddress</b> and <b>SubnetMask</b> parameters, this parameter determines the starting IP address to assign to DHCP clients. The value of this parameter is the starting value of the lower bits of the 32-bit starting IP address not masked by the <b>SubnetMask</b> , and it MUST fit within the unmasked range of the <b>SubnetMask</b> . Here are some examples:	100	
<b>SubnetMask</b>	<b>CurrentRouter IPAddress</b>	<b>ClientAddress RangeStart</b>	<b>First Client IP Address</b>
255.255.255.0	192.168.10.1	100	192.168.10.100
255.255.255.0	192.168.2.1	50	192.168.2.50
<b>MaximumClients</b>	The size of the IP address range from which to pick addresses to assign to DHCP clients that are not in the DHCP reservation list. If the range extends to addresses outside of the <b>SubnetMask</b> , a red exclamation mark (!) is shown next to the value on the device web page.	50	
<b>AddressLeaseTime</b>	IP address lease time in minutes.	1440	
<b>LocalDomainName</b>	Local Domain Name for the LAN.		

**DHCP Reservation Parameter Guide**

Parameter	Description	Default Setting
<b>(Reservation) 1 – 20</b>		
<b>Enable</b>	Enables this reservation.	No
<b>ClientName</b>	An optional name for easy identification of the client.	
<b>ClientMACAddress</b>	Client MAC address in the format <code>xx:xx:xx:xx:xx:xx</code> where each <code>x</code> is a hex digit that can be in upper or lower case.	
<b>ReservedIPAddress</b>	The IP address to reserve for this client.	

**Firewall and DMZ Parameter Guide**

Parameter	Description	Default Setting
<b>Firewall Settings</b>		
<b>Enable</b>	Enables the firewall.	No
<b>NATRedirection</b>	Supports NAT Redirection, also known as NAT Loopback or Hairpin. This setting takes effect only if the firewall is enabled. Otherwise this feature is disabled.	No
<b>DRDOSAttackProtection</b>	Enables protection against Distributed Reflection Denial of Service. This setting takes effect only if the firewall is enabled. Otherwise this feature is disabled.	No
<b>VPNPassthrough</b>	Allows VPN (L2TP, PPTP, and IPSEC) traffic to pass through if enabled; otherwise all VPN traffic is blocked. This setting takes effect only if the firewall is enabled. Otherwise this feature is <i>enabled</i> .	Yes
<b>DMZ Settings</b>		
<b>Enable</b>	Enables DMZ Service.	No
<b>HostIPAddress</b>	The IP address of the DMZ server.	

**Port Forwarding Parameter Guide**

Parameter	Description	Default Setting
<b>Port Forwarding</b>		
<b>Enable</b>	Enables this port forwarding rule.	
<b>RuleDescription</b>	Description of this rule.	

## Port Forwarding Parameter Guide

Parameter	Description	Default Setting
<b>Protocol</b>	The transport protocol for the specified port range in this rule. It can take one of the following values: <ul style="list-style-type: none"> <li>• TCP: TCP only</li> <li>• UDP: UDP only</li> <li>• Both: TCP and UDP</li> </ul>	
<b>StartingPort</b>	Starting port number of the forwarded port range.	
<b>EndingPort</b>	Ending port number of the forwarded port range. If it is the same as <b>StartingPort</b> , only the one port equal to the <b>StartingPort</b> is forwarded.	
<b>ServerIPAddress</b>	The LAN side IP address to forward the packet to when it is received at a port on the WAN side within the port range in this rule with matching transport protocol.	

## QoS Parameter Guide

Parameter	Description	Default Setting
<b>QoS General Setting</b>		
<b>Enable</b>	Enables QoS Service (take effect in router mode only).	No
<b>UpStreamBandwidth</b>	The total upstream bandwidth in kbps.	2048
<b>RestrictedBandwidth</b>	The guaranteed bandwidth for Restricted class traffic in kbps.	512
<b>Priority Class Bandwidth Allocation</b>		
<b>High</b>	The guaranteed uplink bandwidth allocation weight for High Priority class traffic. It must be a value between 1 and 10.	5
<b>Medium</b>	The guaranteed uplink bandwidth allocation weight for Medium Priority class traffic. It must be a value between 1 and 10.	3
<b>Low</b>	The guaranteed uplink bandwidth allocation weight for Low Priority class traffic. It must be a value between 1 and 10.	2
<b>DSCP to Priority Class Mapping</b>		
<b>N (N = 0 – 63)</b>	The priority class to be assigned to the packet that has the DSCP code equal to N in the IP header. Choose from: <ul style="list-style-type: none"> <li>• Restricted</li> <li>• High</li> <li>• Medium</li> <li>• Low</li> </ul> Restricted class has the highest priority.	For N = 8, 10, 12, or 14, the default is Low. For N = 48 or 56, the default is High. For all other DSCP codes, the default is Medium.

## Auto Provisioning Parameter Guide

Parameter	Description	Default Setting
<b>Auto Firmware Update</b>		
<b>Method</b>	<p>Current operational method of auto firmware updating. Choose from:</p> <ul style="list-style-type: none"> <li>• <b>Disabled</b>: Do not check for f/w upgrade from <b>FirmwareURL</b>.</li> <li>• <b>System Start</b>: Check for f/w upgrade from <b>FirmwareURL</b> just once on system start.</li> <li>• <b>Periodically</b>: Check for f/w upgrade from <b>FirmwareURL</b> on system start, and then periodically at the interval specified in the <b>Interval</b> parameter.</li> </ul> <p>The first firmware upgrade check on system start is performed after a random delay of 0 to 30 seconds.</p>	Disabled
<b>Interval</b>	<p>When <b>Method</b> is set to <b>Periodically</b>, this is the number of seconds between each checking of f/w upgrade check from <b>FirmwareURL</b>. If value is 0, the device checks once only on system start (equivalent to setting <b>Method</b> to <b>System Start</b>).</p>	0
<b>FirmwareURL</b>	<p>URL of firmware package. URL must include scheme. Supported schemes are <code>http://</code> and <code>tftp://</code></p>	
<b>DnsLookupType</b>	<p>Controls what type of DNS record to lookup. Choose from:</p> <ul style="list-style-type: none"> <li>• A Record Only</li> <li>• SRV Record Only</li> <li>• Try Both</li> </ul>	A Record Only
<b>DnsSrvPrefix</b>	<p>Controls whether to add a standard prefix to the domain name when looking up a SRV Record. For HTTP and HTTPS, the prefix to add is <code>_http._tcp.</code>. For TFTP, the prefix to add is <code>_tfto._udp.</code> Choose from:</p> <ul style="list-style-type: none"> <li>• No Prefix</li> <li>• With Prefix</li> <li>• Try Both</li> </ul>	No Prefix
<b>Username</b>	User name for authentication, if needed, if scheme is <code>http://</code>	
<b>Password</b>	Password for authentication, if needed, if scheme is <code>http://</code>	
<b>ITSP Provisioning</b>		
<b>Method</b>	<p>Current operational method of Provisioning. Choose from:</p> <ul style="list-style-type: none"> <li>• <b>Disabled</b>: Do not download from <b>ConfigURL</b>.</li> <li>• <b>System Start</b>: Download from <b>ConfigURL</b> just once on system start.</li> <li>• <b>Periodically</b>: Download from <b>ConfigURL</b> on system start, and then periodically at the interval specified in the <b>Interval</b> parameter.</li> </ul> <p>First download on system start is performed after a random delay of 30 to 90 seconds if there is a firmware update scheduled at the beginning, or a random delay of 10 to 70 seconds.</p>	System Start

## Auto Provisioning Parameter Guide

Parameter	Description	Default Setting
<b>Interval</b>	When <b>Method</b> is set to <code>Periodically</code> , this is the number of seconds between download from <b>ConfigURL</b> . If value is 0, device downloads once only on system start (equivalent to setting <b>Method</b> to <code>System Start</code> ).	0
<b>ConfigURL</b>	URL of config file.	<code>tftp://\$DHC POPT66/\$MAC .xml</code>
<b>DnsLookupType</b>	Controls what type of DNS record to lookup. Choose from: <ul style="list-style-type: none"> <li>A Record Only</li> <li>SRV Record Only</li> <li>Try Both</li> </ul>	A Record Only
<b>DnsSrvPrefix</b>	Controls whether to add a standard prefix to the domain name when looking up a SRV Record. For HTTP and HTTPS, the prefix to add is <code>_http._tcp..</code> For TFTP, the prefix to add is <code>_tfto._udp..</code> Choose from: <ul style="list-style-type: none"> <li>No Prefix</li> <li>With Prefix</li> <li>Try Both</li> </ul>	No Prefix
<b>GPRM0 to GPRM7</b>	Non-volatile generic parameters that can be referenced in other parameters, such as <b>ConfigURL</b> .	
<b>TPRM0 to TPRM3</b>	Temporary variables used in scripts for <b>ConfigURL</b> . Please refer to device provisioning guide for examples on how to use these variables.	
<b>OBiTALK Provisioning</b>		
<b>Method</b>	Current operational method of Provisioning. Choose from: <ul style="list-style-type: none"> <li><code>Disabled</code>: Do not download from <b>ConfigURL</b>.</li> <li><code>System Start</code>: Download from <b>ConfigURL</b> just once on system start.</li> <li><code>Periodically</code>: Download from <b>ConfigURL</b> on system start, and then periodically at the interval specified in the <b>Interval</b> parameter.</li> </ul> First download on system start is performed after a random delay of 30 to 90 seconds if there is a firmware update scheduled at the beginning, or a random delay of 10 to 70 seconds.	System Start
<b>Interval</b>	When <b>Method</b> is set to <code>Periodically</code> , this is the number of seconds between download from <b>ConfigURL</b> . If value is 0, device downloads once only on system start (equivalent to setting <b>Method</b> to <code>System Start</code> ).	0
<b>ConfigURL</b>	URL of config file.	<code>tftp://\$DHC POPT66/\$MAC .xml</code>

## Auto Provisioning Parameter Guide

Parameter	Description	Default Setting
<b>DnsLookupType</b>	Controls what type of DNS record to lookup. Choose from: <ul style="list-style-type: none"> <li>A Record Only</li> <li>SRV Record Only</li> <li>Try Both</li> </ul>	A Record Only
<b>DnsSrvPrefix</b>	Controls whether to add a standard prefix to the domain name when looking up an SRV Record. For HTTP and HTTPS, the prefix to add is <code>_http._tcp..</code> For TFTP, the prefix to add is <code>_tfto._udp..</code> Choose from: <ul style="list-style-type: none"> <li>No Prefix</li> <li>With Prefix</li> <li>Try Both</li> </ul>	No Prefix
<b>GPRM0 to GPRM7</b>	Non-volatile generic parameters that can be referenced in other parameters, such as <b>ConfigURL</b> .	
<b>TPRM0 to TPRM3</b>	Temporary variables used in scripts for <b>ConfigURL</b> . Please refer to the <i>Polycom® OBi ATA Device Deployment Guide</i> for examples on how to create these variables.	
<b>User-Defined Macro 0–3 (\$UDM0 – \$UDM3)</b>		
<b>Value</b>	The value can be any plain text or a valid canonical parameter name preceded by a \$ sign. For example: <b>\$X_DeviceManagement.WebServer.Port</b> You must not enclose the parameter name following the \$ sign with braces or parentheses.	
<b>ExpandIn</b>	This is a comma-separated list of canonical parameter names, where the macro expansion can be used. As many as three parameter names can be specified. Specify <i>ANY</i> to allow the macro to expand in any parameter. Example: <code>X_DeviceManagement.HTTPClient.UserAgent</code> There is no \$ sign in front of the parameter name. The macro can't be used in any parameter value if this value is set to blank (the default)	
<b>SyntaxCheckResult</b>	This is read only status value regarding the syntax of the UDM. <i>Pass</i> means that this UDM is valid. Otherwise, it shows the syntax error detected by the device either in the <b>Value</b> or <b>ExpandIn</b> parameters of the UDM.	

**\$MACRO Expansion Supported by the Device**

Macro Name	Description	Where It Can Be Used
MAC	Device MAC address, such as 9CADEF000000	ANY
MACC	Device MAC address with colons, such as 9C:AD:EF:00:00:00	ANY
mac	Device MAC address in lower case with colons, such as 9c:ad:ef:00:00:00	ANY
FWV	Firmware version, such as 1.0.3.1626	ANY
HWV	Hardware version, such as 2.8	ANY
IPA	Current device IP address, such as 192.168.15.100	ANY
DM	Device Model Name, such as OBi200	ANY
DMN	Device model number, such as 200	ANY
OBN	Device OBi number, such as 200123456	ANY
DSN	Device S/N, such as 88B01NA00000	ANY
GPRM $n$ $n=0-7$	Value Auto Provisioning::GPRM $n$	<b>Auto Provisioning::ConfigURL,</b> <b>Auto Firmware</b> <b>Update::FirmwareURL</b>
TPRM $n$ $n=0-3$	Value of <b>Auto Provisioning::TPRM<math>n</math></b>	<b>Auto Provisioning::ConfigURL,</b> <b>Auto Firmware</b> <b>Update::FirmwareURL</b>
UDM $n$ , $n=0-3$	Value of <b>User-Defined Macro <math>n</math>::Value</b>	The value of <b>User-Defined Macro <math>n</math>::ExpandIn</b>

**Device Administration Parameter Guide**

Parameter	Description	Default Setting
<b>Web Server</b>		
Port	Web server port number.	80
AdminPassword	Administrator password, case-sensitive.	admin
UserPassword	User password, case-sensitive.	user
AccessFromWAN	Allows accessing device management web pages from the WAN side.	No
<b>IVR</b>		
Enable	Enables IVR for local configuration.	Yes



## Device Administration Parameter Guide

Parameter	Description	Default Setting
Password	IVR access password (must be all digits).	
<b>Syslog</b>		
Server	IP address of the Syslog server where the device sends syslog debug messages to. If the value is blank, syslog is disabled.	
Port	Syslog server port number.	514
Level	Syslog message level.	7
TAG	A string of text no longer than 32 characters to prepend every syslog message sent out by this unit.	
<b>HTTP Client</b>		
UserAgent	Value of the User-Agent header in all HTTP Requests that are used in firmware upgrade and auto provisioning.	\$DM
TimeOut	A time limit specified in number of seconds such that any file download (firmware or configuration file) by the device via HTTP must be completed within this limit or the device aborts and concludes that the operation has failed for the reason of "taking too long to complete".	600
ProxyServer	IP address of the web-proxy server.	
ProxyServerPort	Port number of the web-proxy service.	
ProxyAuthUsername	The User ID for authenticating (BASIC or DIGEST) to web-proxy service.	
ProxyAuthPassword	The password (corresponding to <b>AuthUserName</b> ) for authentication.	
BypassProxyServerForLocalAddress	Enables device to bypass the web-proxy for services residing in the same network subnet as the device.	
BypassProxySubnetList	A list of network subnets where the software bypasses the configured web-proxy. The device sends requests directly to the IP addresses of any services in the same network subnet as the device.	
<b>TLSPPlatform CACERT n (X_DeviceManagement.PlatformCACert.n.), n = 1, 2</b>		
DownloadURL	URL to download certificate.	None
MD5Checksum	MD5 checksum of the certificate file to be downloaded. Failure to provide this causes the phone to try to download the same file on every reboot or restart.	None
CommonName	The Common Name set in the installed certificate. Read-only status field.	None
FingerPrint	SHA1 fingerprint of the installed certificates.	None
Obsolete	When set to true, the certificate is deleted from the phone. Also, the certificate downloading process is ignored.	False

**Custom DeviceCert n (X\_DeviceManagement.CustomDeviceCert.n.), n = 1, 2**

## Device Administration Parameter Guide

Parameter	Description	Default Setting
<b>DownloadURL</b>	URL to download certificate.	None
<b>MD5Checksum</b>	MD5 checksum of the downloaded certificate.	None
<b>CommonName</b>	The Common Name set in the installed certificate. Read-only status field.	None
<b>FingerPrint</b>	SHA1 fingerprint of the installed certificates.	None
<b>Obsolete</b>	When set to true, the device is deleted from the phone. Also, the certificate downloading process is ignored.	False
<b><i>TLSPPlatform Profile n (X_DeviceManagement.TLSPPlatform.n.), n = 1, 2</i></b>		
<b>CipherSuite</b>	The cipher suite to use in a TLS profile (the encryption algorithms to support in establishing a TLS connection according to the TLS profile specification configured on the phone).	None
<b>CACertList</b>	The CA Certificate List to use in a TLS profile. Choice of: <ul style="list-style-type: none"> <li>• Default</li> <li>• Default+P1</li> <li>• Default+P2</li> <li>• All</li> <li>• Platform1</li> <li>• Platform2</li> <li>• Platform1+2</li> </ul>	Default
<b>DeviceCert</b>	The Device Certificate List to use in a TLS profile. Choice of: <ul style="list-style-type: none"> <li>• Polycom</li> <li>• Custom1</li> <li>• Custom2</li> </ul>	Polycom

## ITSP Profile A &amp; B (General and SP Info Settings) Parameter Guide

Parameter	Description	Default Setting
<b>General ITSP Settings</b>		
<b>Name</b>	Human-readable string to identify the profile instance. Maximum length is 127 characters.	
<b>SignalingProtocol</b>	Signaling protocol for this ITSP. <ul style="list-style-type: none"> <li>• SIP</li> </ul>	SIP

## ITSP Profile A &amp; B (General and SP Info Settings) Parameter Guide

Parameter	Description	Default Setting
<b>DTMFMethod</b>	Method to pass DTMF digits to peer device. Choose from: <ul style="list-style-type: none"> <li><b>Inband</b>: DTMF tones are sent as inband audio signal</li> <li><b>RFC2833</b>: DTMF tone events are relayed per RFC2833</li> <li><b>SIPInfo</b>: DTMF tones are relayed with SIP INFO request</li> <li><b>Auto</b>: Method to use based on call setup negotiation (either Inband or RFC2833 can be negotiated).</li> </ul>	Auto
<b>X_UseFixedDurationRFC2833DTMF</b>	When relaying DTMF digit events on this trunk using RFC2833, the RFC2833 RTP packets normally keep streaming for as long as the digit is pressed. With this option set to TRUE, the device sends only one RTP digit event packet with a fixed duration of 150 ms regardless how long the digit has been pressed.	FALSE
<b>DigitMap</b>	A digit map to restrict the numbers that can be dialed or called with this service. See the <a href="#">Trunks, Endpoints, and Terminals</a> section for a description of digit map syntaxes. Maximum length is 511 characters.	(1xxxxxxxxxxx <1>[2-9]xxxxxxxxxxx 011xx. xx.)
<b>STUNEnable</b>	Enables device to send a STUN binding request for its RTP port prior to every call.	No
<b>STUNServer</b>	IP address of domain name of the STUN Server to use.	
<b>X_STUNServerPort</b>	UDP listen port of the STUN Server.	3478
<b>X_ICEEnable</b>	Enables device to use ICE algorithm to find the best peer RTP address to forward RTP traffic for every call.	No
<b>X_SymmetricRTPEnable</b>	Enables device to apply symmetric RTP behavior on every call: That is, send RTP to peer at the address where incoming RTP packets are received from.	No
<b>Service Provider Info</b>		
<b>Name</b>	Human-readable string identifying this service provider. Maximum length is 127 characters.	
<b>URL</b>	Website of this service provider. Maximum length is 127 characters.	
<b>ContactPhoneNumber</b>	Phone number to contact this service provider. Maximum length is 31 characters.	
<b>EmailAddress</b>	Email address to contact this service provider. Maximum length is 127 characters.	

## ITSP SIP Settings Parameter Guide

Parameter	Description	Default Setting
<b>ProxyServer</b>	Host name or IP address of the SIP proxy server.	
<b>ProxyServerPort</b>	Destination port to connect to the SIP server.	5060
<b>ProxyServerTransport</b>	Transport protocol to connect to SIP server. Choose from: <ul style="list-style-type: none"> <li>• UDP</li> <li>• TCP</li> <li>• TLS</li> </ul>	UDP
<b>RegistrarServer</b>	Host name or IP address of the SIP registrar. If a value is specified, device sends REGISTER to the given server; otherwise REGISTER is sent to <b>ProxyServer</b> .	
<b>RegistrarServerPort</b>	Destination port to connect to SIP registrar.	5060
<b>RegistrarServerTransport</b>	Transport protocol to connect to registrar. This parameter is reserved for future. The only choice is UDP.	UDP
<b>UserAgentDomain</b>	CPE domain string. If empty, device uses <b>ProxyServer</b> as its own domain to form its AOR (Address Of Record) or Public Address when constructing SIP messages (for example, in the FROM header of outbound SIP Requests). If <b>SPn Service::URI</b> is specified, additional rules applied in forming the AOR. See the description of the <b>URI</b> parameter for more details and examples.	
<b>UserAgentTransport</b>	Transport protocol for incoming call control signaling. This parameter is reserved for future. The only choice is UDP.	UDP
<b>OutboundProxy</b>	Host name or IP address of the outbound proxy. Outbound proxying is disabled if this parameter is blank.	
<b>OutboundProxyPort</b>	Destination port to be used in connecting to the outbound proxy.	5060
<b>X_OutboundProxyTransport</b>	Controls the SIP transport for the outbound proxy server, which can be different from that of the proxy server. Choose from: <ul style="list-style-type: none"> <li>• UDP</li> <li>• TCP</li> <li>• TLS</li> <li>• Follow ProxyServerTransport</li> </ul>	Follow ProxyServerTransport

## ITSP SIP Settings Parameter Guide

Parameter	Description	Default Setting
<b>X_BypassOutboundProxyInCall</b>	Enables bypassing the <b>OutboundProxy</b> inside the SIP dialog.	No
<b>RegistrationPeriod</b>	Nominal interval between device register in seconds.	60
<b>X_RegistrationMargin</b>	Number of seconds before current registration expires that the device should re-Register (for example, 5 seconds). If value is less than one, it is interpreted as a fraction of the current expires value (for example, 0.1 of 60 seconds is 6 seconds). If value is 0 or blank, the device determines a proper margin on its own.	
<b>TimerT1</b>	Value of SIP timer T1 in ms.	500
<b>TimerT2</b>	Value of SIP timer T2 in ms.	4000
<b>TimerT4</b>	Value of SIP timer T4 in ms.	5000
<b>TimerA</b>	Value of SIP timer A in ms.	500
<b>TimerB</b>	Value of SIP timer B in ms.	32000
<b>TimerD</b>	Value of SIP timer D in ms.	32000
<b>TimerE</b>	Value of SIP timer E in ms.	500
<b>TimerF</b>	Value of SIP timer F in ms.	32000
<b>TimerG</b>	Value of SIP timer G in ms.	500
<b>TimerH</b>	Value of SIP timer H in ms.	32000
<b>TimerI</b>	Value of SIP timer I in ms.	5000
<b>TimerJ</b>	Value of SIP timer J in ms.	32000
<b>TimerK</b>	Value of SIP timer K in ms.	5000
<b>InviteExpires</b>	Invite request Expires header value in seconds.	60
<b>ReInviteExpires</b>	Re-invite Expires header value in seconds.	10
<b>RegisterExpires</b>	Register Expires header value in seconds (not used at the moment).	3600
<b>RegistersMinExpires</b>	Register Min-Expires header value in seconds (not used at the moment).	15
<b>RegisterRetryInterval</b>	Register retry interval in seconds.	30

## ITSP SIP Settings Parameter Guide

Parameter	Description	Default Setting
<b>X_RegisterRetryResponseCode</b>	A set of SIP register error response codes and the corresponding retry delay (in seconds) specified in a digit map format. See the default value on the right as an example, where the value to the left of the colon of each rule represents a set of 3-digit response codes and the value to the right of the colon is the waiting time in seconds. If the waiting time is given as a range (with a '-'), a randomized waiting time within the specified range is used.	(<40[17]:w120> <40[34]:w120> <99[01]:w120-200> [4-9]xx)
<b>DSCPMark</b>	Diffserv code outgoing SIP packets.	0
<b>VLANIDMark</b>	VLAN ID for outgoing SIP signaling packets.	0
<b>EthernetPriorityMark</b>	Ethernet priority code for outgoing SIP signaling packets.	3
<b>X_UseRefer</b>	Enables using SIP REFER for call transfer. If disabled, device bridges the call instead when performing a call transfer (which consumes some resources on the device).	No
<b>X_ReferAOR</b>	Enables using the target's AOR (Address of Record or public address) in Refer-To header of SIP REFER. If disabled, the target's Contact is used instead.	Yes
<b>X_Use302ToCallForward</b>	Enables using the 302 response to INVITE for call forward. If disabled, device bridges the call legs instead when forwarding a call (and consumes some resources on the device).	Yes
<b>X_UserAgentName</b>	If a value is specified, device includes a User-Agent header in all SIP Requests, or a Server header in all SIP responses, that contains exactly the given value.	OBIHAI/\${DM}-\${FWV}
<b>X_ProcessDateHeader</b>	Enables the device to decode the DATE header sent by the ITSP in a 200 response to its REGISTER. The DATE header specifies the current GMT time and the device can use to adjust its local time and date without relying on NTP.	Yes
<b>X_InsertRemotePartyID</b>	Enables the device to include a Remote-Party-ID header in its outbound SIP INVITE to indicate to the ITSP the caller's preferred privacy setting (either full or none).	Yes
<b>X_SessionRefresh</b>	Enables session refresh signaling (with SIP Re-INVITE) during a connected call. This allows the device to detect if the connection with the peer is broken abnormally so it can release the call. Disable this option if the ITSP does not support Re-INVITE sent from the client device.	Yes

## ITSP SIP Settings Parameter Guide

Parameter	Description	Default Setting
<b>X_AccessList</b>	A comma-separated list of IP addresses such that the device only accepts SIP requests coming from one of the given addresses. If the list is empty, the device accepts SIP requests from any IP address.	
<b>X_InsertRTPStats</b>	Enables the device to include a X-RTP-Stat header in a BYE request or 200 response to BYE request at the end of an established call. This header contains a summary of RTP statistics collected during the call.	Yes
<b>X_MWISubscribe</b>	Enables the device to SUBSCRIBE to the message-summary event package to support MWI and VMWI service. The device handles NOTIFY of this event package regardless of whether <b>MWISubscribe</b> is enabled.	No
<b>X_MWISubscribeURI</b>	Blank implies to use the same URL as REGISTER for the TO and FROM header as well as the Request-URI. Otherwise, if the URI does not contain '@', it is user as the userid field in TO/FROM header as well as the Request-URI, which are otherwise same as REGISTER. If the URI contains '@', it is used in the TO and FROM header as well as the Request-URI as is. The device forms the Request-URI of SUBSCRIBE the same way as the TO header, with an additional port number.	
<b>X_MWISubscribeExpires</b>	Periodic interval to renew SUBSCRIBE.	3600
<b>X_RegSubscribe</b>	Enables subscription to the "reg" event package.	No
<b>X_RegSubscribeExpires</b>	Expires value for subscription to the "reg" event package.	3761
<b>X_ProxyServerRedundancy</b>	Enables proxy redundancy feature on the device. To use this feature, device registration must be enabled and the SIP Registration Server or Outbound Proxy Server must be configured as a domain name.	No
<b>X_SecondaryRegistration</b>	Enables device to register with a secondary server in addition to the primary server. <b>X_ProxyServerRedundancy</b> must be enabled for this parameter to take effect.	No
<b>X_CheckPrimaryFallbackInterval</b>	Interval in seconds at which the device checks the primary fallback list of candidate servers.	60
<b>X_CheckSecondaryFallbackInterval</b>	Interval in seconds at which the device checks the secondary fallback list of candidate servers.	60

## ITSP SIP Settings Parameter Guide

Parameter	Description	Default Setting
<b>X_ProxyRequire</b>	If this parameter is not blank, the device includes a Proxy-Require header stating the value of this parameter in all SIP requests sent to the ITSP.	
<b>X_MaxForward</b>	Value for the Max-Forward header in all SIP requests sent by the device.	70
<b>X_AcceptLanguage</b>	If this parameter is not blank, the device includes an Accept-Language header stating the value of this parameter in all SIP requests sent to the ITSP.	
<b>X_DnsSrvAutoPrefix</b>	Enables letting the device automatically prepend a standard prefix to the domain name when querying DNS Server to resolve the <b>ProxyServer</b> or <b>OutboundProxy</b> name as a SRV record. The standard prefix is <code>_sip._udp.</code> for SIP over UDP, <code>_sip._tcp.</code> for SIP over TCP, and <code>_sip._tls.</code> for SIP over TLS.	No
<b>X_UserEqPhone</b>	Includes the parameter 'user=phone' in Request-URI and To-URI of outbound INVITE.	No
<b>X_CallWaitingIndication</b>	Enables including an indication in an 18x response to the calling peer if this is a call- waiting situation.	No
<b>X_Support100rel</b>	Enables support for RFC3262 (reliable provisional SIP responses). If enabled, the device announces this support in a SIP Supported header, and requires a caller to use this option if the caller also supports this feature.	No
<b>X_DiscoverPublicAddress</b>	Enables letting the device use the public IP address and port it has discovered as its SIP Contact address.	Yes
<b>X_UsePublicAddressInVia</b>	Enables using the discovered external IP address (instead of the unit's assigned local IP address) in outbound Via header.	No
<b>X_PublicIPAddress</b>	A static public IPv4 address, if specified, is used by the device to form its SIP Contact address.	
<b>X_UseRport</b>	Enables letting the device insert a blank rport parameter in the VIA header our outbound SIP messages. This option should be turned off if you are using port forwarding on the external router to route inbound SIP messages to the device.	Yes
<b>X_UseCompactHeader</b>	Enables using compact form SIP message header names.	No



## ITSP SIP Settings Parameter Guide

Parameter	Description	Default Setting
<b>X_FaxPassThroughSignal</b>	Selects the signaling method to indicate to the peer to switch to FAX passthrough. Choose from: <ul style="list-style-type: none"> <li>ReINVITE</li> <li>RFC2833</li> <li>Auto</li> <li>None</li> </ul>	ReINVITE
<b>X_EchoServer</b>	Name or IP address of an echo server for SIP ALG detection.	
<b>X_EchoServerPort</b>	Listening of the echo server for SIP ALG detection.	
<b>X_EnableRFC2543CallHold</b>	Enables interpretation of call hold indication per RFC2543.	

## ITSP RTP Settings Parameter Guide

Parameter	Description	Default Setting
<b>RTP</b>		
<b>LocalPortMin</b>	Base of port range for tx/rx RTP with this SP.	16600
<b>LocalPortMax</b>	Top of port range for tx/rx RTP with this SP.	16798
<b>KeepAliveInterval</b>	Interval in seconds between sending keep alive packet on an RTP channel that is currently in idle (due to call hold for instance). RTP keepalive is disabled if the value of this parameter is set to 0.	0
<b>DSCPMark</b>	Diffserv code for outgoing RTP packets with this SP.	0
<b>RTCP</b>		
<b>Enable</b>	Enables RTCP.	No
<b>TxRepeatInterval</b>	RTCP packet transmission interval in milliseconds.	10000
<b>LocalCName</b>	The canonical name to use in RTCP messages. If blank, the device uses <userid>@<local_IP_address> as its canonical name.	
<b>X_RTCPMux</b>	Enables using an rtcp-mux attribute in SDP (send and receive RTCP on the same port as RTP).	No

## SPn Services Parameter Guide

Parameter	Description	Default Setting
<b>SPn Service</b>		
<b>Enable</b>	Enables this line.	Yes
<b>X_ServProvProfile</b>	Selects a Service Provider Profile for this service. Choose from A or B.	A
<b>X_RingProfile</b>	Selects a Ring Profile to ring the Phone port with for incoming calls on this service that are routed to the Phone port. The ringing pattern is taken from the given profile. Choose from A or B.	A
<b>X_CodecProfile</b>	Selects a Codec Profile for all calls on this service. Choose from A or B.	A
<b>X_InboundCallRoute</b>	Routing rule for directing incoming calls on this service. The available options are <code>ph</code> , <code>ph2</code> and <code>hs</code> . See the <a href="#">Trunks, Endpoints, and Terminals</a> section for a description of the syntaxes for specifying this parameter.	<code>ph</code>
<b>X_RegisterEnable</b>	Enables registration for this line. If set to YES, device sends periodic SIP REGISTER to the service provider according to the settings in the ITSP Profile. Otherwise, device does not send any SIP REGISTER for the service.	Yes
<b>X_NoRegNoCall</b>	Enables blocking making or receiving calls on this service unless registration with the SIP server is successful.	No
<b>X_KeepAliveEnable</b>	Enables sending keep alive message. If set to YES, device sends periodic keep-alive messages to the destination specified in <b>X_KeepAliveServer</b> and <b>X_KeepAliveServerPort</b> , at the interval specified in <b>X_KeepAliveExpires</b> . The content of this message is the ASCII string "keep-alive\r\n".	No
<b>X_KeepAliveExpires</b>	Keep-alive period in seconds.	15
<b>X_KeepAliveServer</b>	Host name or IP address of keep-alive server.	
<b>X_KeepAliveServerPort</b>	UDP port of the keep-alive server.	5060
<b>X_KeepAliveMsgType</b>	The type of keep alive messages to send out periodically if keep-alive is enabled. It can be one of the following choices: <ul style="list-style-type: none"> <li><code>keep-alive</code>: The string "keep-alive"</li> <li><code>empty</code>: A blank line</li> <li><code>stun</code>: A standard STUN binding request; device uses the binding response to form its contact address for REGISTRATION</li> <li><code>custom</code>: Use the value of <b>X_CustomKeepAliveMsg</b></li> </ul>	<code>keep-alive</code>

## SPn Services Parameter Guide

Parameter	Description	Default Setting
<b>X_CustomKeepAliveMsg</b>	<p>Defines the custom message to be used when <b>X_KeepAliveMsgType</b> is "custom". The value should have the following format:</p> <pre>mtd=NOTIFY;event=&lt;whatever&gt;;user=&lt;anyone&gt;</pre> <p>where</p> <ul style="list-style-type: none"> <li>NOTIFY can be replaced by any other SIP method, such as PING,</li> <li>event parameter is optional and is only applicable if method is NOTIFY. If event is not specified, the 'keep-alive' event is used with NOTIFY</li> <li>user parameter is optional. If not specified, the request-uri won't have a userid, and the TO header field uses the same userid as the FROM header (which is the local account userid). If user is specified, it is used as the userid in the Request-URI and TO header.</li> </ul> <p>SIP messages for keep-alive are sent only once without retransmission. The device ignores responses to the SIP messages.</p>	
<b>X_UserAgentPort</b>	UDP port where the device sends and listens for SIP messages.	5060
<b>DirectoryNumber</b>	Directory number associated with this service.	
<b>X_DefaultRing</b>	Default ring pattern number to ring the Phone port for incoming calls on this trunk that are routed to the Phone port according to the <b>InboundCallRoute</b> of this service. The ring pattern is taken from the selected Ring Profile. Choose from 1 through 10.	1
<b>X_CallOnHoldRing</b>	Pattern to ring Phone port when holding a call on this trunk that has been connected to the Phone port. Typically this is a very short distinctive ring pattern that serves as a reminder to the user that a call is being on hold. The ring pattern is taken from the selected Ring Profile. Choose from No Ring, or 1 through 10.	8
<b>X_RepeatDialRing</b>	The ring pattern number to use to ring the Phone port when a repeat dial operation on this trunk is successful as the called party is either ringing or answered.	5
<b>X_BargeInRing</b>	Call Waiting Ring pattern to ring the Phone port when the incoming call is requesting to barge-in. This is applicable in a call-waiting scenario on the Phone port.	4
<b>X_CallParkedRing</b>	Ring pattern to ring the Phone port only as a reminder that there are calls parked in the parking lot. This feature is applicable only in an OBiPLUS solution.	10

## SPn Services Parameter Guide

Parameter	Description	Default Setting
<b>X_SipDebugOption</b>	<p>Enables sending SIP signaling debug information to the syslog server (if one is configured on the device). Choose from:</p> <ul style="list-style-type: none"> <li>• <code>Disable</code> (do not send SIP signaling debug information)</li> <li>• <code>Log All Messages</code></li> <li>• <code>Log All Except REGISTER Messages</code></li> </ul>	Disable
<b>X_SipDebugExclusion</b>	A list of SIP methods to exclude from the syslog for this SP service. For example: <code>notify, subscribe</code> .	
<b>X_SatelliteMode</b>	<p>Enables satellite mode on this trunk. In this mode, the user must explicitly sign on (using * code) to receive phone calls on this trunk. The SIP REGISTER sent by the device to the ITSP on this trunk indicates if the user wants to sign on (and therefore takes over the incoming calls for this account). This feature is only applicable if the service is provided by an OBIPLUS system.</p>	No
<b>X_Proxy</b>	<p>Enables proxy mode operation on this SP service. If enabled, the SP accepts SIP Registration from one client device from the LAN side, which must be using the same user-id and password as this SP's <b>AuthUserName</b> and <b>AuthPassword</b> parameters for authentication. The client device, known as the <i>local_client</i>, may send SIP INVITE to the device at this SP to make calls. This SP's <b>InboundCallRoute</b> must be set up with the proper routing rule to handle calls from the <i>local_client</i>.</p> <p>The SIP Proxy Server parameter on the local client should be set to:</p> <pre>&lt;obi-number&gt;.pnn.obihai.com:&lt;sp-user-agent-port&gt;</pre> <p>where <code>&lt;obi-number&gt;</code> is the 9-digit OBi number of this device and <code>&lt;sp-user-agent-port&gt;</code> is this SP's <b>X_UserAgentPort</b> parameter.</p> <p>For example, SP1 has a <i>local_client</i> with the userid 4086578118 and the client wants to make and receive calls using SP3. The SP1 <b>InboundCallRoute</b> shall include the following rule:</p> <pre>{4086578118}:sp3}</pre> <p>The SP3 <b>InboundCallRoute</b> shall be:</p> <pre>{sp1(408657118@local_client)}</pre>	No

## SPn Services Parameter Guide

Parameter	Description	Default Setting
<b>X_ProxyClientConfig</b>	<p>A list of device attributes separated by a space or newline character for provisioning a device with the given MAC address and model number. Each attribute has the syntax <code>&lt;attribute-name&gt;=&lt;attribute-value&gt;</code> with no white space before and after the '=' sign. Every character within the pair of double quotes is taken as the attribute's value.</p> <p>The following attributes are supported:</p> <ul style="list-style-type: none"> <li>• <b>mac:</b> Required. The MAC address of the device in 12-hex-digit format, such as "008e3c123456".</li> <li>• <b>model:</b> Required. The make/model of the phone, such as "Cisco/SPA504G".</li> <li>• <b>ext:</b> Required. The extension number assigned to the phone, such as "104". The account is installed on Ext 1 of the phone.</li> <li>• <b>dm:</b> Optional. The dial plan on Ext 1 of the phone, such as "<code>([1-5]xx [67][0-9*][0-9*] 9,1 xxx xxx xxxx 9,011 xx. 8,&lt;:1408&gt;[2-9]xxxxxx 8,1 xxx xxx xxxx 8,011 xx.)</code>".</li> <li>• <b>mohs:</b> Optional. The extension number of the MOH Server, such as "69*".</li> <li>• <b>bn:</b> Optional. A function button to be configured with the attributes that follow. Valid values are "1", "2", ... as many as the maximum number of programmable function buttons on that phone model. A <b>bn</b> attribute is followed by one or more of the <b>fn</b>, <b>va</b>, and <b>la</b> attributes. The end of a <b>bn</b> section is marked by another <b>bn</b> attribute. You must insert a <b>bn="0"</b> attribute after the last button.</li> <li>• <b>fn:</b> Required. A code that represents the function served by the current button. This attribute must be located somewhere between two <b>bn</b> attributes. The following codes are defined: <ul style="list-style-type: none"> <li>▲ "Ext 1": A line key for calls on phone's Ext 1 account.</li> <li>▲ "Speed Dial": A speed dial. Requires a <b>va</b> attribute with the target number as the value.</li> <li>▲ "BLF": Classic BLF. Requires a <b>va</b> attribute with the extension number to monitor as the value.</li> <li>▲ "Send To Leave VM": Blind transfers the current active call to leave voicemail. Requires a <b>va</b> attribute with the target mailbox ID, such as "00", "01", ..., as the value.</li> <li>▲ "Send To Park": Blind transfers the current call to a parking lot partition. Requires a <b>va</b> attribute with the parking lot partition mask, such as "0*", "1*", "***", ... as the value.</li> </ul> </li> </ul>	

## SPn Services Parameter Guide

Parameter	Description	Default Setting
<b>X_ProxyClientConfig</b> (cont.)	<ul style="list-style-type: none"> <li>▲ "Monitor VM": Monitors if new voicemail is available in a mailbox. Requires a <code>va</code> attribute with the target mailbox ID, such as "00", "01", ... as the value.</li> <li>▲ "Monitor Park": Monitors a parking lot partition. Requires a <code>va</code> attribute with the target parking lot partition mask, such as "0*", "1*", "***", ... as the value.</li> <li>▲ "Monitor Night Mode": Monitors the system's day/night mode status. No <code>va</code> attribute required.</li> <li>▲ "Auto Night Mode": Monitors if the system's auto day/night mode switching feature is active. No <code>va</code> attribute required.</li> <li>▲ "Sign On/Off": Lets user sign on/off an extension. Requires a <code>va</code> attribute with the extension number to sign on/off as the value, such as "101".</li> </ul> <ul style="list-style-type: none"> <li>• <code>va</code>: Required if the function code requires it. This attribute must be located somewhere between two <code>bn</code> attributes.</li> <li>• <code>1a</code>: Optional. If present, it must be somewhere between two <code>bn</code> attributes. A string label to display on the phone screen next to the current function key. For example "\$USER", "Park", "Night". It should be no longer than 7 characters due to space limitation. This attribute does not apply for a sidecar button.</li> </ul> <p>Other than "Ext 1" and the generic "Speed Dial" function, all the other button functions are only applicable if the service installed on this SP is from an OBiPLUS system. This parameter is useful only if the <b>X_Proxy</b> parameter is enabled. In that case, the device provides a configuration file based on the attributes given in this parameter, upon request from an IP phone with the matching MAC address. The IP phone must be installed on the LAN side of the device and must be one of the following make/models:</p> <ul style="list-style-type: none"> <li>• Cisco/SPA303</li> <li>• Cisco/SPA504G</li> <li>• Cisco/SPA508G</li> <li>• Cisco/SPA509G</li> <li>• Cisco/SPA525G</li> </ul>	
<b>X_AcceptResync</b>	<p>Controls whether to accept a SIP NOTIFY request with <code>event=resync</code> to trigger a reboot of the device (so it can download new f/w or configuration upon boot up). Choose from:</p> <ul style="list-style-type: none"> <li>• <code>no</code>: Do not accept resync trigger</li> <li>• <code>yes with authentication</code>: Accept after challenging the sender</li> <li>• <code>yes without authentication</code>: Accept without challenging the sender</li> </ul>	yes without authentication

## SPn Services Parameter Guide

Parameter	Description	Default Setting
<b>SPn SIP Credentials</b>		
<b>AuthUserName</b>	The User ID to authenticate to a SIP UAS (User Agent Server) when an outbound SIP request sent by the device is challenged by the UAS with a 401 or 407 Response.	
<b>AuthPassword</b>	The password (corresponding to <b>AuthUserName</b> ) to authenticate to a SIP UAS (User Agent Server) when an outbound SIP request sent by the device is challenged by the UAS with a 401 or 407 Response.	
<b>URI</b>	<p>This parameter affects the way the AOR is formed by the device in outbound SIP Requests. The AOR has the format: <code>user@domain</code></p> <p>If the value of URI is empty, device gets the user portion of its AOR from the <b>AuthUserName</b>, and the domain portion the value of ITSP Profile's <b>UserAgentDomain</b> if it is not empty, or that of the <b>ProxyServer</b> otherwise.</p> <p>If the value URI is not empty and does not contain "@", it is used as the user portion of the AOR while the domain portion is formed the usual way.</p> <p>If the value of URI contains "@", it is interpreted as a full AOR and device takes it as the AOR as is.</p> <p><b>Examples:</b></p> <p>Let <b>ProxyServer</b> = <code>sip.myitsp.com</code>, <b>AuthUserName</b> = <code>4089991123</code>, <b>URI</b>=<code>[empty]</code>, <b>UserAgentDomain</b>=<code>[empty]</code>, then AOR = <code>4089991123@sip.myitsp.com</code></p> <p>Change <b>UserAgentDomain</b> to <code>users.myitsp.com</code>, then AOR = <code>4089991123@users.myitsp.com</code></p> <p>Change <b>URI</b> to <code>bobdylan</code>, then AOR = <code>bobdylan@users.myitsp.com</code></p> <p>Change <b>URI</b> to <code>bobdylan@superusers.myitsp.com</code>, then AOR = <code>bobdylan@superusers.myitsp.com</code></p> <p>In all cases, the device uses <b>AuthUserName</b> and <b>AuthUserPassword</b> to compute authorization if challenged by a 401 or 407 response.</p>	
<b>SPn Calling Features</b>		
<b>CallerIDName</b>	Displays name to identify the subscriber. The display name field is usually inserted in a FROM header in outbound SIP requests (such as INVITE) for the purpose of displaying a Caller ID Name on the recipient's device.	

## SPn Services Parameter Guide

Parameter	Description	Default Setting
<b>MaxSessions</b>	The maximum number of simultaneous calls that can be established on this service.	2
<b>CallForwardOnNoAnswerRingCount</b>	Number of rings to be considered by the device as no answer to an incoming call.	2
<b>X_BlockedCallers</b>	A comma-separated list of as many as 10 caller numbers to block from calling this service.	
<b>MWIEnable</b>	Enables Message Waiting Indication Service for this service. If enabled, device plays stutter dial tone on the Phone port (or PHONE1 port) when there are new messages for the subscriber. It also turns on VMWI signal on the Phone port (or PHONE1 port) if <b>X_VMWIEnable</b> is set to Yes.	No
<b>MWIEnable2</b>	Enables Message Waiting Indication Service for this service. If enabled, device plays stutter dial tone on the PHONE2 port when there are new messages for the subscriber. It also turns on VMWI signal on the PHONE2 port if <b>X_VMWIEnable</b> is set to Yes.	No
<b>X_VMWIEnable</b>	Enables Visual Message Waiting Indication for this service for the Phone port (or PHONE1 port).	No
<b>X_VMWIEnable2</b>	Enables Visual Message Waiting Indication for this service for the PHONE2 port.	No
<b>MessageWaiting</b>	This state parameter indicates if there are any new messages for this subscriber on the service provider's voicemail system.	No
<b>X_BridgedOutboundCallMaxDuration</b>	Limit on the call duration in seconds for all outbound calls that are bridged from the same or another trunk. A blank or 0 value implies the call duration is not limited.	
<b>X_AcceptDialogSubscription</b>	Enables the device to accept SUBSCRIBE to this trunk's dialog event package.	No
<b>X_SRTP</b>	Enables SRTP. Choose from: <ul style="list-style-type: none"> <li>• <b>Disable SRTP:</b> Do not use SRTP for all calls; the call fails if the peer insists on using SRTP only.</li> <li>• <b>Use SRTP Only:</b> Require all calls to use SRTP. The call fails if the peer does not support SRTP.</li> <li>• <b>Use SRTP When Possible:</b> Use SRTP for a call if the peer supports SRTP. Otherwise, fall back to use regular unencrypted SRTP.</li> <li>• <b>Offer Both SRTP and RTP:</b> Tells the service to accept either SRTP/SAVP or RTP/AVP offer, and the device makes its own SDP offer with both SRTP/SAVP and RTP/AVP in the SIP message.</li> </ul>	Use SRTP When Possible



## OBiTALK Service Settings Parameter Guide

Parameter	Description	Default Setting
<b>Enable</b>	Enables the OBiTALK Service (the built-in free voice service that comes with every OBi Device).	Yes
<b>LocalPort</b>	The UDP or TCP port used by the device to send and listens for OBiTALK messages.	10000
<b>TryMultiplePorts</b>	Enables the device to try a few random UDP ports until it can successfully join the OBiTALK network.	No
<b>DisplayName</b>	Display name to identify the subscriber, for the purpose of displaying a Caller ID Name on the recipient's device.	
<b>DigitMap</b>	Digit map to restrict numbers that can be dialed or called with this service. See the <a href="#">Trunks, Endpoints, and Terminals</a> section for a description of the syntaxes for specifying a Digit Map.	( <ob>xxxxxxxx x   obxxxxxxxx )
<b>InboundCallRoute</b>	Routing rule for directing incoming calls on this service. The default rule is to send all incoming calls to the Phone port (ph). See the <a href="#">Trunks, Endpoints, and Terminals</a> section for a description of the syntaxes for specifying this parameter.	Ph
<b>RingProfile</b>	Selects a Ring Profile to ring the Phone port with when an incoming call is routed to the Phone port. Choose from A or B.	A
<b>CodecProfile</b>	Selects a Codec Profile to be used for all calls on this service. Choose from A or B.	A
<b>DefaultRing</b>	Default ring pattern number to ring the Phone port for incoming calls on this trunk that are routed to the Phone port according to the <b>InboundCallRoute</b> of this service. The ring pattern is taken from the selected Ring Profile. Choose from 1 through 10.	2
<b>CallOnHoldRing</b>	Pattern to ring Phone port when holding a call on this trunk that has been connected to the Phone port. Typically this is a very short distinctive ring pattern that serves as a reminder to the user that a call is being on hold. The ring pattern is taken from the selected Ring Profile. Choose from No Ring, or 1 through 10.	8
<b>RepeatDialRing</b>	The ring pattern number to use to ring the Phone port when a repeat dial operation on this trunk is successful as the called party is either ringing or answered.	4

### OBiTALK Service Settings Parameter Guide

Parameter	Description	Default Setting
<b>DTMFMethod</b>	Method to pass DTMF digits to peer device. Choose from: <ul style="list-style-type: none"> <li><b>Inband</b>: DTMF tone are sent as inband audio signal</li> <li><b>RFC2833</b>: DTMF tone events are relayed per RFC2833</li> <li><b>SIPInfo</b>: DTMF tones are relayed with SIP INFO request</li> <li><b>Auto</b>: Method to use based on call setup negotiation (either Inband or RFC2833 can be negotiated)</li> </ul>	Auto
<b>UseFixedDurationRFC2833DTMF</b>	When relaying DTMF digit events on this trunk using RFC2833, the RFC2833 RTP packets normally keep streaming for as long as the digit is pressed. With this option set to TRUE, the device sends only one RTP digit event packet with a fixed duration of 150 ms regardless how long the digit has been pressed.	FALSE

### OBiTALK Calling Features Parameter Guide

Parameter	Description	Default Setting
<b>CallForwardOnNoAnswerRingCount</b>	Number of rings to be considered by the device as no answer to an incoming call.	2
<b>BlockedCallers</b>	A comma-separated list of as many as 10 caller numbers to block from calling this service.	
<b>MaxSessions</b>	The maximum number of simultaneous calls that can be established on this service.	2

### OBiTALK Inbound Direct Dialing Authentication Parameter Guide

Parameter	Description	Default Setting
<b>AuthMethod</b>	The OBiTALK protocol allows incoming calls to indicate a target number that is different from this device's OBi number. The device in that case attempts to establish and bridge the call to the target number according to the rules configured in the trunk's <b>InboundCallRoute</b> parameter. Hence this device acts as a gateway and the method is referred to direct dialing or 1-stage dialing (versus 2-stage dialing via the Auto Attendant). Since the caller is not able to enter a PIN in such cases, an automated method based on signaling protocol must be used to authenticate the caller if authentication is required. Choose from: <ul style="list-style-type: none"> <li><b>None</b>: Disable authentication</li> <li><b>HTTP Digest</b>: Use HTTP Digest with User-ID and Password pairs. (x=1,2,3,4) must be specified, otherwise authentication is disabled.</li> </ul>	HTTP Digest
<b>AuthUserID1</b>	One of 4 user IDs for authenticating direct dialing callers.	
<b>AuthPassword1</b>	One of 4 passwords for authenticating direct dialing callers.	
<b>AuthUserID2</b>	One of 4 user IDs for authenticating direct dialing callers.	

**OBiTALK Inbound Direct Dialing Authentication Parameter Guide**

Parameter	Description	Default Setting
<b>AuthPassword2</b>	One of 4 passwords for authenticating direct dialing callers.	
<b>AuthUserID3</b>	One of 4 user IDs for authenticating direct dialing callers.	
<b>AuthPassword3</b>	One of 4 passwords for authenticating direct dialing callers.	
<b>AuthUserID4</b>	One of 4 user IDs for authenticating direct dialing callers.	
<b>AuthPassword4</b>	One of 4 passwords for authenticating direct dialing callers.	



If **AuthPassword** is specified, **AuthUserID** can be set to blank to let the device use the default value, which is a special hash of the **AuthPassword**. This is only applicable if the external gateway is also a device that understands how to generate the default **AuthUserID** using the same hash function.

**Automated Attendant Parameter Guide**

IVR Announcement Number	Attendant Announcement	What Happens Next
1	Press 1 to continue this call.	Ring the device.
2	Press 2 to make a new call.	If <b>UsePIN</b> authentication is enabled and the user enters a matching PIN, the device attendant immediately prompts the user to enter a PIN followed by the pound (#) key. If the entered PIN is not a match, the attendant gives the user two additional attempts to enter the PIN. If the third attempt does not match, the attendant announces a thank you message and disconnects the call.
3	Press 3 to enter a callback number.	If a valid number is entered, AA says "Thank you" and "Goodbye", hangs up, and then calls the number in back 2 seconds. If the given number is invalid, AA plays SIT tone followed by an error message. Tips: Caller can dial 00# to have the AA call back his current number.

**Automated Attendant Prompt List**

AA Prompt List	System Default	Prompt To Be Played
Welcome	Welcome to OBi Attendant.	Once, at the beginning when the AA starts.
InvalidPin	Invalid PIN.	After user enters an invalid PIN.

**Automated Attendant Prompt List**

AA Prompt List	System Default	Prompt To Be Played
EnterPin	Enter PIN.	Prompts user to enter a valid PIN.
MenuTitle	Main Menu.	Once, after <b>Welcome</b> and before announcing the menu options.
Menu	Press 1 to continue this call. Press 2 to make a new all. Press 3 to enter a callback number.	A couple of times after <b>MenuTitle</b> .
PleaseWait	Please wait while your call is being connected.	Once, after user enters a phone number to call.
EnterNumber	Enter number followed by the # key.	Prompts user to enter a valid number after option 2 or option 3 is selected by the user.
Bye	Thank you for choosing Obihai Technology. Goodbye.	When user presses * or # key to leave the AA.

**User Prompts Parameter Guide**

Parameter	Description	Default Setting
<b>User&lt;N&gt;Description</b> <N> = 1-10	A text string that describes the contents of this user prompt.	
<b>User&lt;N&gt;Length</b> <N> = 1-10	This is a read-only status parameter. It shows the space occupied by this prompt in number of milliseconds.	
<b>SpacedUsed</b>	This is a read-only status parameter. It shows the amount of recording space used in number of milliseconds.	
<b>SpaceAvailable</b>	This is a read-only status parameter. It shows the amount of recording space remaining in number of milliseconds.	

## Auto Attendant Parameter Guide

Parameter	Description	Default Setting
<b>Enable</b>	Enables AA. If enabled, the AA answers an incoming call that has been routed to it after a period as specified in <b>AnswerDelay</b> . If disabled, the AA won't attempt to answer any incoming call.	Yes
<b>DigitMap</b>	Once the AA answers an incoming call, it presents the caller with an option to make a further call using one of the available voice services on the device. This Digit map serves to restrict the numbers that can be dialed or called via this AA option. See the <a href="#">Trunks, Endpoints, and Terminals</a> section for a description of the syntaxes to specify a digit map.	<pre> ([1-9]x?* (Mpli)   [1-9]   [1-9] [0-9]   &lt;00:\$1&gt; 0  **1 (Msp1)   **2 (Msp2)  **3 (Msp3)   **4 (Msp4)  **70 (Mli)  **8 (Mbt)  * *81 (Mbt)  **82 (Mbt2)   **9 (Mpp)   (Mpli) ) </pre>
<b>OutboundCallRoute</b>	After the caller dials a number that is acceptable by the AA (according to its <b>DigitMap</b> ) to make a further call, the device uses this outbound call routing rule to determine the service with which to make this call. See the <a href="#">Trunks, Endpoints, and Terminals</a> section for a description of the syntaxes to specify this parameter. Forking to multiple numbers in an AA outbound call is supported on the OBi202. For example, on the OBi202 you may have a rule like this: {0:ph,ph2}, which forks to ring both PHONE1 and PHONE2. You can have as many as four destinations in a forking rule.	<p>For OBi:200/OBi300:</p> <pre> { ([1-9]x?* (Mpli) ):pp}, {0:ph}, { (&lt;**1:&gt; (Msp1) ):sp1}, { (&lt;**2:&gt; (Msp2) ):sp2}, { (&lt;**3:&gt; (Msp3) ):sp3}, { (&lt;**4:&gt; (Msp4) ):sp4}, { (&lt;**70:&gt; (Mli) ):li}, { (&lt;**82:&gt; (Mbt2) ):bt2}, { (&lt;**81:&gt; (Mbt) ):bt}, { (&lt;**8:&gt; (Mbt) ):bt}, { (&lt;**9:&gt; (Mpp) ):pp}, { (Mpli) :pli} </pre> <p>For OBi:202/OBi302:</p> <pre> { ([1-9]x?* (Mpli) ):pp}, {0:ph.ph2}, { (&lt;**1:&gt; (Msp1) ):sp1}, { (&lt;**2:&gt; (Msp2) ):sp2}, { (&lt;**3:&gt; (Msp3) ):sp3}, { (&lt;**4:&gt; (Msp4) ):sp4}, { (&lt;**70:&gt; (Mli) ):li}, { (&lt;**82:&gt; (Mbt2) ):bt2}, { (&lt;**81:&gt; (Mbt) ):bt}, { (&lt;**8:&gt; (Mbt) ):bt}, { (&lt;**9:&gt; (Mpp) ):pp}, { (Mpli) :pli} </pre>
<b>AnswerDelay</b>	Period of time in milliseconds that the AA waits before answering an incoming call that has been routed to it.	4000

## Auto Attendant Parameter Guide

Parameter	Description	Default Setting
<b>NumberOnNoInput</b>	In the case that the caller does not enter any option from the top level menu after the menu has been announced for 3 times, the AA directs the caller to the number specified in this parameter. If this number is not specified, the AA terminates the current call. According to the default <b>DigitMap</b> and <b>OutboundCallRoute</b> , calling 0 means calling the Phone port.	0
<b>UsePIN</b>	Enables using a PIN to authenticate callers when they select the option to make a further call. If PIN1, PIN2, PIN3, and PIN4 are all empty, device treats it as if UsePIN is set to No. Otherwise, the caller must enter one of the non-empty PIN in order to proceed.	No
<b>PIN1</b>	PIN code to make a call (must be all digits). Maximum length = 15 digits.	
<b>PIN2</b>	PIN code to make a call (must be all digits). Maximum length = 15 digits.	
<b>PIN3</b>	PIN code to make a call (must be all digits). Maximum length = 15 digits.	
<b>PIN4</b>	PIN code to make a call (must be all digits). Maximum length = 15 digits.	

## Auto Attendant Prompt Parameter Guide

Parameter	Description	Default Setting
<b>Welcome</b>	Prompt List to replace the system's <b>Welcome</b> message.	
<b>InvalidPin</b>	Prompt List to replace the system's <b>InvalidPin</b> message.	
<b>EnterPin</b>	Prompt List to replace the system's <b>EnterPin</b> message.	
<b>MenuTitle</b>	Prompt List to replace the system's <b>MenuTitle</b> message.	
<b>Menu</b>	Prompt List to replace the system's <b>Menu</b> message.	
<b>PleaseWait</b>	Prompt List to replace the system's <b>PleaseWait</b> message.	
<b>EnterNumber</b>	Prompt List to replace the system's <b>EnterNumber</b> message.	
<b>Bye</b>	Prompt List to replace the system's <b>Bye</b> message.	

## Voice Gateway Parameter Guide

Parameter	Description	Default Setting
<b>Voice Gateway <math>n</math> (<math>n=1-8</math>)</b>		
<b>Enable</b>	Enables this voice gateway.	Yes
<b>Name</b>	An arbitrary user-friendly name to identify this gateway (optional).	
<b>AccessNumber</b>	The gateway's OBiTALK number, including trunk information, such as: <code>PP (ob200112334)</code> or <code>PP (ob200112334)</code> If the value is blank, the device treats this VG as disabled. Starting with release 1.2, this can also be set to a SIP URL, such as: <code>SP1 (sip.mycompany.com:5060)</code> or <code>SP2 (192.168.15.113)</code>	
<b>DigitMap</b>	<b>DigitMap</b> for this VG. It can be referenced as <code>(Mvgn)</code> .	<code>(x.x)</code>
<b>AuthUserID</b>	A user ID to authenticate with the gateway.	
<b>AuthPassword</b>	A password to authenticate with the gateway.	

## Trunk Group Parameter Guide

Parameter	Description	Default Setting
<b>Trunk Group <math>n</math> (<math>n=1-4</math>)</b>		
<b>Enable</b>	Enables this trunk group.	Yes
<b>Name</b>	An arbitrary user friendly name to identify this trunk group (optional).	
<b>TrunkList</b>	A comma-separated list of names of trunks to include in this trunk group.	For TG1, the default is: <code>sp1, sp2, sp3, sp4</code> For other TG, the default is (blank)
<b>DigitMap</b>	Digit map associated with this trunk group. It can be referenced as <code>(Mtn)</code> .	For TG1, the default is <code>(1xxxxxxxxxxx &lt;1&gt;[2-9]xxxxxxxx 011xx. xx.)</code>

## Phone Port Parameter Guide

Parameter	Description	Default Setting
<b>Phone Port</b>		
<b>Enable</b>	Enables the Phone port.	Yes

## Phone Port Parameter Guide

Parameter	Description	Default Setting
<b>DigitMap</b>	<p>Restricts the numbers that can be dialed or called from the Phone port. If the caller dials a number that is not allowed by the digit map, the device plays a SIT tone followed by a short error message to let the caller know that the dialed number is invalid.</p> <p>See the <a href="#">Trunks, Endpoints, and Terminals</a> section for a description of the syntaxes to specify a digit map.</p>	<pre>([1-9]x?* (Mpli)   [1-9]S9   [1-9] [0-9]S9   911   **0   ***   #   ##   **70 (Mli)   **8 (Mbt)   **81 (M bt)   **82 (Mbt2)   **1 (Msp1)   **2 (Msp2)   **3 (Msp3)   **4 (Msp4)   **9 (Mpp)   (Mpli) )</pre>
<b>OutboundCallRoute</b>	<p>After the caller dials a number that is acceptable according to the <b>DigitMap</b>, the device uses this outbound call routing rule to determine that service to make this call with. If no appropriate call route is found, the device plays a SIT tone followed by a short error message to let the caller know that there is no call route to place the call.</p> <p>See the <a href="#">Trunks, Endpoints, and Terminals</a> section for a description of the syntaxes to specify this parameter.</p>	<p>For OBi200/OBi300:</p> <pre>{ ([1-9]x?* (Mpli) ):pp}, { (&lt;##:&gt; ):li}, { (&lt;**70:&gt; (Mli) ):li}, { (&lt;**82:&gt; (Mbt2) ):bt2}, { (&lt;**81:&gt; (Mbt) ):bt}, { (&lt;**8:&gt; (Mbt) ):bt}, { **0:aa }, { ***:aa2 }, { (&lt;**1:&gt; (Msp1) ):sp1}, { (&lt;**2:&gt; (Msp2) ):sp2}, { (&lt;**3:&gt; (Msp3) ):sp3}, { (&lt;**4:&gt; (Msp4) ):sp4}, { (&lt;**9:&gt; (Mpp) ):pp}, { (Mpli) :pli}</pre> <p>For OBi202/OBi302 PHONE2:</p> <pre>{ ([1-9]x?* (Mpli) ):pp}, { (&lt;##:&gt; ):li}, { (&lt;#:&gt; ):ph}, { (&lt;**70:&gt; (Mli) ):li}, { (&lt;**82:&gt; (Mbt2) ):bt2}, { (&lt;**81:&gt; (Mbt) ):bt}, { (&lt;**8:&gt; (Mbt) ):bt}, { **0:aa }, { ***:aa2 }, { (&lt;**1:&gt; (Msp1) ):sp1}, { (&lt;**2:&gt; (Msp2) ):sp2}, { (&lt;**3:&gt; (Msp3) ):sp3}, { (&lt;**4:&gt; (Msp4) ):sp4}, { (&lt;**9:&gt; (Mpp) ):pp}, { (Mpli) :pli}</pre>



## Phone Port Parameter Guide

Parameter	Description	Default Setting
<b>ToneOnPrimaryServiceDown</b>	Selects the tone to play in place dial tone when the service corresponding to the Primary Line is out-of-service. Choose from: <ul style="list-style-type: none"> <li>No Tone</li> <li>Normal Dial Tone</li> <li>SIT Tone 1</li> <li>SIT Tone 2</li> <li>SIT Tone 3</li> <li>SIT Tone 4</li> </ul>	Normal Dial Tone
<b>Ringer</b>		
<b>RingFrequency</b>	Ringer frequency in Hz (14 to 68) to apply to the Phone port when ringing.	20
<b>RingVoltage</b>	Peak ringer voltage in volts (55 to 82) to apply to the Phone port when ringing.	70
<b>RingWaveform</b>	Ringer waveform to apply to the Phone port when ringing. Choose from: <ul style="list-style-type: none"> <li>Sinusoidal</li> <li>Trapezoidal</li> </ul>	Sinusoidal
<b>InterleavedRing</b>	When both Phone ports are ringing, enabling this option causes the device to interleave the ring signal applied to each port to reduce the chance of overloading the power supply.	No
<b>Port Settings</b>		
<b>OnHookTipRingVoltage</b>	Tip/Ring Voltage when the attached phone is on hook (30 V to 52 V).	46
<b>OffHookCurrentMax</b>	Maximum supported current (15 mA to 45 mA) when the attached phone is off-hook.	20

## Phone Port Parameter Guide

Parameter	Description	Default Setting
<b>Impedance</b>	Phone port impedance setting. Choose from (units in ohms if not specified): <ul style="list-style-type: none"> <li>• 600</li> <li>• 900</li> <li>• 270+(750  150 nF)</li> <li>• 220+(820  120 nF)</li> <li>• 370+(620  310 nF)</li> <li>• 320+(1050  230 nF)</li> <li>• 350+(1000  210 nF)</li> <li>• 200+(680  100 nF)</li> <li>• 600+2.16 uF</li> <li>• 900+2.16 uF</li> <li>• 600+1 uF</li> <li>• 220+(820  115 nF)</li> </ul>	600
<b>DTMFPlaybackLevel</b>	Out of band DTMF tone playback level in dBm (–90 to 3).	–15
<b>CallerIDMethod</b>	Caller ID delivery standard. Choose from: <ul style="list-style-type: none"> <li>• FSK (Bell202)</li> <li>• FSK (V.23)</li> <li>• DTMF (Finland, Sweden)</li> <li>• DTMF (Denmark)</li> </ul>	FSK (Bell202)
<b>CallerIDTrigger</b>	Triggering event for on-hook Caller ID signal generation. Choose from: <ul style="list-style-type: none"> <li>• After First Ring</li> <li>• After Polarity Reversal</li> <li>• Before First Ring</li> </ul>	After First Ring
<b>ChannelTxGain</b>	Transmit gain in dB (–12 to 12) to apply to signal sent from the device to the attached phone(s).	0
<b>ChannelRxGain</b>	Receive gain in dB (–12 to 12) to apply to signal received by the device from the attached phone(s).	0

## Phone Port Parameter Guide

Parameter	Description	Default Setting
<b>SilenceDetectSensitivity</b>	<p>Phone port silence detection servers the purpose of driving silence suppression in RTP transmission when the phone Call terminates on SP1/2 or OBiTALK Service and silence suppression is enabled.</p> <p>This parameter sets a sensitivity level for the device silence detection algorithm. Choose from:</p> <ul style="list-style-type: none"> <li>• Low (harder to detect silence)</li> <li>• Medium (suggested)</li> <li>• High (easier to detect silence)</li> </ul>	Medium
<b>Calling Features</b>		
<b>CallCommandSignalMethod</b>	<p>Selects the method to signal a command to the device when the phone is off-hook with an active call in connected state, while there is a second call on hold or ringing. Choose from:</p> <ul style="list-style-type: none"> <li>• N. America (uses hook switch events only)</li> <li>• Nordic Regions (R1, R2, ...), where R = hook flash or the 'R' button,</li> <li>• R0: Reject the second incoming call (applicable only if the second call is ringing)</li> <li>• R1: End current call, resume/answer the second call</li> <li>• R2: Hold current call, resume/answer the second call</li> <li>• R3: Conference the two calls</li> <li>• R4: Transfer second call peer to the first (not applicable if second call is ringing)</li> </ul>	N. America
<b>CallerIDEnable</b>	<p>Enables Caller ID Signal generation. This option can be set to Yes even if the attached phone is not capable of displaying Caller ID. There is no harm in sending Caller ID signal while the phone is in the on hook state.</p>	Yes

## Phone Port Parameter Guide

Parameter	Description	Default Setting
<b>CallWaitingCallerIDEnable</b>	<p>Enables Call Waiting Caller ID (CWCID) Signal generation.</p> <p>The CWCID signal is sent to the phone when it is in the off hook state. It starts with a handshake between the device and the attached phone, by exchanging audible short tones. The device proceeds with the transmission of the remaining Caller ID signal only if the handshake succeeds (with a phone is capable of displaying CWCID). In that case the phone mutes the handset earpiece until the CWCID signal is complete. Some users however may still find the audible handshake tones objectionable, especially if their phones do not support CWCID. Set this option to No if you don't want the CWCID feature, or don't have phones that can display CWCID.</p>	Yes
<b>MWIEnable</b>	<p>Enables MWI Signal (stutter dial tone) generation. If enabled, any SP voice service enabled on the device that has MWI Service enabled triggers the generation of stutter dial tone if there are new voicemails for the subscriber on the service provider's voicemail system.</p>	Yes
<b>VMWIEnable</b>	<p>Enables VMWI Signal generation. If enabled, any SP voice service enabled on the device that has VMWI Service enabled triggers the generation of VMWI signal if there are new voicemails for the subscriber on the service provider's voicemail system.</p>	Yes

## Phone Port Parameter Guide

Parameter	Description	Default Setting
<b>CallTransferEnable</b>	<p>Enables Call Transfer. Call Transfer, if enabled, is initiated by the user by hanging up the phone in one of the following scenarios:</p> <ul style="list-style-type: none"> <li>• One call on hold while a second outgoing call ringing (Case 1)</li> <li>• One call on hold while a second outgoing call connected (Case 2)</li> <li>• One call connected while a second outgoing call ringing (Case 3)</li> <li>• 3-way conference with both calls connected (Case 4)</li> </ul> <p>If Call Transfer is disabled, hanging up the phone in the above scenarios ends all the calls except for the one that is holding, which remains on hold (Cases 1 and 2).</p>	Yes
<b>ConferenceCallEnable</b>	<p>Enables 3-way Conference Call w/ local audio mixing. Conference Call, if enabled, is initiated by the user by hook flashing the phone in one of the following scenarios:</p> <ul style="list-style-type: none"> <li>• One call on hold while a second outgoing call ringing (Case 1)</li> <li>• One call on hold while a second outgoing call connected (Case 2)</li> </ul> <p>Case 1 is an early conference, where the second conferencee is still ringing. The other two parties may converse while hearing ringback tone in the back-ground until the third party answers. In either case, the user can end the call with the second conferencee by hook flashing another time and the call reverts to a 2-way call.</p> <p>If Conference Call service is disabled, then hook flashing the phone resumes the holding call but ends the second outgoing call in Case 1, and swaps between the two calls in Case 2 (as in a call waiting situation).</p>	Yes

## Phone Port Parameter Guide

Parameter	Description	Default Setting
<b>UseExternalConferenceBridge</b>	Enables using an external conference bridge for conference calls (SIP only). In addition, the following rule  <pre>{cbridge:SPx(bridge-userid)}</pre> must also be added to the Phone port's <b>OutboundCallRoute</b> parameter, where x=1,2,3,4, and bridge-userid the userid of the conference bridge SUA. The keyword cbridge is hard-coded and must not be changed.	No
<b>ToneProfile</b>	Selects a Tone Profile for call progress tone generation. Choose from A or B.	A
<b>LastDialedNumber</b>	Last number dialed out on the Phone port.	
<b>LastCallerNumber</b>	Last caller's number that rings the Phone port.	
<b>AcceptMediaLoopback</b>	Enables the device to accept incoming media loopback calls.	Yes
<b>MediaLoopbackAnswerDelay</b>	Delay in milliseconds before the device answers an incoming media loopback call.	0
<b>MediaLoopbackMaxDuration</b>	Maximum duration in seconds to allow for an inbound media loopback call. Set the value to blank or 0 to make it unlimited.	0
<b>RepeatDialInterval</b>	Interval in seconds between retry in a repeat dial operation.	30
<b>RepeatDialExpires</b>	Duration of time in seconds when a repeat dial operation remains active.	1800
<b>GenerateCPCSignal</b>	Controls when the device should generate a CPC signal when the remote party hangs up on an established call. Choose from: <ul style="list-style-type: none"> <li>• Never</li> <li>• For Inbound Calls Only</li> <li>• For Outbound Calls Only</li> <li>• For Inbound and Outbound Calls</li> </ul>	For Inbound and Outbound Calls
<b>EnablePHONEPortBargeln</b>	Enables the caller to barge in when he calls the other Phone port from this Phone port while the other Phone port has an active call in progress, on-hold, or ringing.	Yes

## Phone Port Parameter Guide

Parameter	Description	Default Setting
<b>UseForPagingOnly</b>	Enables the device to be used for paging only when the Phone port is connected to an external PA system (via a RJ11 to line out connector, available from many electronics shops). In such configuration the Phone port is expected to be “off-hook” all the time. The device automatically answers an incoming call and won’t accept call-waiting.	No
<b>TransferWhenHolding</b>	This option provides a short cut to transfer a call to a fixed preconfigured number without dialing it. If a valid number is specified for this parameter, the device transfers the call to the given number when the phone hook flashes and then on-hook (which normally leaves the call holding if this parameter is not specified). The valid number should be a complete number with trunk information, such as SP1 (14083334567).	
<b>EndHoldingCallWhenHangUp</b>	If enabled, when a user hangs up while a call is still on hold, the device ends that call instead of alerting the same to the user (with a short ring).	No
<b>MOHServiceNumber</b>	The number to call to get music streamed to the remote party when the remote party is placed on hold.	
<b>PlaySITOnCallFailureCodes</b>	A list of (3-digit) error response codes on outbound calls to trigger SIT w/ optional announcement of the error. The device plays fast busy tone without any announcement for all other call failure codes. The codes must be specified collectively as a digit map.	( [4-9] xx)
<b>PlaySITWithAnnouncement</b>	Enables including announcement of the error when an outbound call has failed.	Yes

## Timers

## Phone Port Parameter Guide

Parameter	Description	Default Setting
<b>HookFlashTimeMax</b>	<p>Hook Flash is a quick transition of the phone's hook switch from Off-Hook state to On-Hook state, and back to Off-Hook state.</p> <p>This parameter specifies the upper time limit in milliseconds such that if the hook switch stays at the intermediate On-Hook state for longer than this time limit, the device won't recognize the state transition as a HOOK FLASH event, but instead as an ON HOOK event followed by an OFF HOOK event.</p>	900
<b>HookFlashTimeMin</b>	<p>Hook Flash is a quick transition of the phone's hook switch from Off-Hook state to On-Hook state, and back to Off-Hook state.</p> <p>This parameter specifies the lower time limit in milliseconds such that if the hook switch stays at the intermediate On-Hook state for less than this time limit, the device won't recognize the state transition as a HOOK FLASH event, but consider the hook switch remains at Off-Hook state throughout the transition (in other words, the transition is discarded as a glitch if it happens too quickly).</p>	100
<b>CPCDelayTime</b>	A short delay in milliseconds before the device generates a CPC signal to the Phone port after the far end has hung up during a call.	2000
<b>CPCDuration</b>	The device generates CPC (Calling Party Control) Signal by removing power from the Phone port for a short period. This parameter specifies the length of this period in milliseconds. CPC signal tells the attached phone equipment that the far end has ended the call.	500
<b>DigitMapLongTimer</b>	Value of the long inter-digit timer (in seconds) when collecting dialed digits according to the <b>DigitMap</b> on this Phone port. This timer governs the timeout when one or more patterns are partially matched or a variable length pattern (that can accommodate one or more optional digits) is matched.	10



## Phone Port Parameter Guide

Parameter	Description	Default Setting
<b>DigitMapShortTimer</b>	Value of the short inter-digit timer (in seconds) when collecting dialed digits according to the <b>DigitMap</b> on this Phone port. This timer governs the timeout when a fixed length pattern has been matched while one or more other patterns can be potentially matched with more input digits.	2

## Tip Ring Voltage Polarity

<b>IdlePolarity</b>	Tip/Ring voltage polarity the line is idle, before a call is connected, or after one side hangs up. Choose from <code>Forward</code> or <code>Reverse</code> .	<code>Forward</code>
<b>ConnectPolarity</b>	Tip/Ring voltage polarity when the line is connected on a call. Choose from <code>Forward</code> or <code>Reverse</code> . By using a different polarity for an Idle and a Connected line, the device effectively generates a polarity reversal signal to the Phone port, which signals the attached phone equipment that the call is either connected or ended.	<code>Forward</code>

## USB Port Parameter Guide

Parameter	Description	Default Setting
USB Headset Settings		
<b>AutoAnswerEnable</b>	Enables auto answer.	Yes
<b>IncomingNotification</b>	Sets the notification preference for incoming calls between the headset and the HDA50.	Built-in
<b>ToneProfile</b>	Selects a Tone Profile for call progress tone generation.	A
<b>WideBandAudio</b>	Notifies SIP is the HDA50 supports Wideband Codecs audio.	No
<b>OutboundNumber</b>	Sets the number to dial for outbound calls. If left blank, the device uses the last dialed number.	pp (ob22222222 2)

## Codec Profile Parameter Guide

Parameter	Description	Default Setting
<b>G711U Codec</b>		
<b>Codec</b>	Codec name.	G711U
<b>BitRate</b>	Bit rate in bits/sec. Informational only, not configurable.	64000
<b>Enable</b>	Enables this codec.	Yes
<b>SilenceSuppression</b>	Enables silence suppression for this codec.	No
<b>PacketizationPeriod</b>	Packet size in ms.	20
<b>Priority</b>	Priority assigned to this codec (1 is the highest).	1
<b>PayloadType</b>	Standard payload type for this codec. Informational only, not configurable.	0
<b>G711A Codec</b>		
<b>Codec</b>	Codec name.	G711A
<b>BitRate</b>	Bit rate in bits/sec. Informational only, not configurable.	64000
<b>Enable</b>	Enables this codec.	Yes
<b>SilenceSuppression</b>	Enables silence suppression for this codec.	No
<b>PacketizationPeriod</b>	Packet size in ms.	20
<b>Priority</b>	Priority assigned to this codec (1 is the highest).	2
<b>PayloadType</b>	Standard payload type for G711-alaw. Informational only, not configurable.	8
<b>G729 Codec</b>		
<b>Codec</b>	Codec name.	G729
<b>BitRate</b>	Bit rate in bits/sec. Informational only, not configurable.	8000
<b>Enable</b>	Enables this codec.	Yes
<b>SilenceSuppression</b>	Enables silence suppression for this codec.	No
<b>PacketizationPeriod</b>	Packet size in ms.	20
<b>Priority</b>	Priority assigned to this codec (1 is the highest).	3
<b>PayloadType</b>	Standard payload type for G729. Informational only, not configurable.	18
<b>iLBC Codec</b>		

## Codec Profile Parameter Guide

Parameter	Description	Default Setting
<b>Codec</b>	Codec name.	iLBC
<b>BitRate</b>	Bit rate in bits/sec. Informational only, not configurable.	13333
<b>Enable</b>	Enables this codec.	No
<b>SilenceSuppression</b>	Enables silence suppression for this codec.	No
<b>PacketizationPeriod</b>	Packet size in ms.	30
<b>Priority</b>	Priority assigned to this codec (1 is the highest).	5
<b>PayloadType</b>	Dynamic Payload type for this codec. Valid range is 96–127.	98
<b>FAX Event</b>		
<b>Codec</b>	Codec name. This codec can be used for relaying FAX tone event using RTP.	fax-event
<b>Enable</b>	Enables this codec.	No
<b>PayloadType</b>	Dynamic Payload type to be used to indicate this event.	100
<b>FaxEvents</b>	Comma-separated list of event IDs to indicate (such as CED, CNG).	32
<b>Telephone Event</b>		
<b>Codec</b>	Codec Name. This codec is for relaying DTMF events using RTP.	telephone-event
<b>Enable</b>	Enables this codec.	Yes
<b>PayloadType</b>	Dynamic Payload type to be used for RFC2833 telephone (DTMF) events. Valid range is 96–127.	101
<b>Encap RTP</b>		
<b>Codec</b>	Codec Name. This codec is used to encapsulate RTP packets during a packet loopback call.	encaprtp
<b>PayloadType</b>	Dynamic Payload type for this codec. Valid range is 96–127.	107
<b>Loopback Primer</b>		
<b>Codec</b>	Codec name. The device uses this codec when it acts as a media loopback mirror and before receiving any packets from the loopback source during a media loopback call.	loopbkprimer
<b>PayloadType</b>	Dynamic Payload type for this codec. Valid range is 96–127.	108
<b>Codec Settings</b>		

## Codec Profile Parameter Guide

Parameter	Description	Default Setting
<b>G726BitPacking</b>	Two values to choose from: <ul style="list-style-type: none"> <li>big-endian</li> <li>little-endian</li> </ul>	big-endian
<b>T38Enable</b>	Enables the use of T38 (FAX Relay).	Yes
<b>T38Redundancy</b>	The packet redundancy factor to use when operating T38 relay. Choose from: <ul style="list-style-type: none"> <li>0 (no redundancy)</li> <li>1</li> <li>2 (higher redundancy, consumes more network bandwidth)</li> </ul>	
<b>FaxPassThroughCodec</b>	The codec to use when operating in the FAX pass-through mode. Choose from: <ul style="list-style-type: none"> <li>G711U</li> <li>G711A</li> </ul>	G711U

## Tone Profile A &amp; B Parameter Guide

Parameter	Description	Default Setting
<b>Dial Tone</b>		
<b>ToneName</b>	Dial Tone.	
<b>TonePattern</b>	Obihai Tone Pattern Script.	350-18,440-18;20
<b>Ringback Tone</b>		
<b>ToneName</b>	Ringback Tone.	
<b>TonePattern</b>	Obihai Tone Pattern Script.	440-18,480-18;-1;(2+4)
<b>Busy Tone</b>		
<b>ToneName</b>	Busy Tone.	
<b>TonePattern</b>	Obihai Tone Pattern Script.	480-18,620-18;10;(.5+.5)
<b>Reorder Tone</b>		
<b>ToneName</b>	Reorder tone or Fast busy.	
<b>TonePattern</b>	Obihai Tone Pattern Script.	480-18,620-18;10;(.25+.25)
<b>Confirmation Tone</b>		
<b>ToneName</b>	Confirmation Tone.	
<b>TonePattern</b>	Obihai Tone Pattern Script.	600-18;1;(.2+.2)

## Tone Profile A &amp; B Parameter Guide

Parameter	Description	Default Setting
<b>Holding Tone</b>		
<b>ToneName</b>	Holding Tone played when peer holding the call.	
<b>TonePattern</b>	Obihai Tone Pattern Script.	800-18;30;(.1+10)
<b>Second Dial Tone</b>		
<b>ToneName</b>	Second Dial Tone played when dialing second call in a 3-way call.	
<b>TonePattern</b>	Obihai Tone Pattern Script.	385-18,484-18;20
<b>Stutter Dial Tone</b>		
<b>ToneName</b>	Stutter Dial Tone.	
<b>TonePattern</b>	Obihai Tone Pattern Script.	350-18,440-18;20;2(.1+.1);()
<b>Howling Tone</b>		
<b>ToneName</b>	Howling Tone for off-hook warning.	
<b>TonePattern</b>	Obihai Tone Pattern Script.	480+3,620+3;10;(.125+.125)
<b>Prompt Tone</b>		
<b>ToneName</b>	Prompt Tone to prompt user to enter a number for configuration, such as speed dial.	
<b>TonePattern</b>	Obihai Tone Pattern Script.	480-16;20
<b>Call Forwarded Dial Tone</b>		
<b>ToneName</b>	Call Forwarded Dial Tone: A special dial tone to indicate call-forward-all is active.	Not configurable.
<b>TonePattern</b>	Obihai Tone Pattern Script.	350-18,440-18;20;(.2+.2)
<b>DND Dial Tone</b>		
<b>ToneName</b>	DND Dial Tone: A special dial tone to indicate DND is active.	Not configurable.
<b>TonePattern</b>	Obihai Tone Pattern Script.	350-18,440-18;20;(.2+.2)
<b>Conference Tone</b>		
<b>ToneName</b>	Conference Tone (indicates a 3-way conference call has started).	Not configurable.
<b>TonePattern</b>	Obihai Tone Pattern Script.	350-16;10;(.1+.1,.1+9.7)
<b>SIT Tone 1</b>		

## Tone Profile A &amp; B Parameter Guide

Parameter	Description	Default Setting
<b>ToneName</b>	Special Information Tone 1.	Not configurable.
<b>TonePattern</b>	Obihai Tone Pattern Script.	985-16,1428-16,1777-16;20;(1/.380+0,2/.380+0,4/.380+0,0/0+4)
<b>SIT Tone 2</b>		
<b>ToneName</b>	Special Information Tone 2.	Not configurable.
<b>TonePattern</b>	Obihai Tone Pattern Script.	914-16,1371-16,1777-16;20;(1/.274+0,2/.274+0,4/.380+0,0/0+4)
<b>SIT Tone 3</b>		
<b>ToneName</b>	Special Information Tone 3.	Not configurable.
<b>TonePattern</b>	Obihai Tone Pattern Script.	914-16,1371-16,1777-16;20;(1/.380+0,2/.380+0,4/.380+0,0/0+4)
<b>SIT Tone 4</b>		
<b>ToneName</b>	Special Information Tone 4.	Not configurable.
<b>TonePattern</b>	Obihai Tone Pattern Script.	985-16,1371-16,1777-16;20;(1/.380+0,2/.380+0,4/.380+0,0/0+4)
<b>Outside Dial Tone</b>		
<b>ToneName</b>	Outside Dial Tone.	Not configurable.
<b>TonePattern</b>	Obihai Tone Pattern Script.	385-16;10
<b>R-Command Tone</b>		
<b>ToneName</b>	R-Command Tone.	Not configurable.
<b>TonePattern</b>	Obihai Tone Pattern Script.	400-16;5
<b>Paging Tone</b>		
<b>ToneName</b>	Paging Tone.	Not configurable.
<b>TonePattern</b>	Obihai Tone Pattern Script.	480-16;1;(.2+.2)

## Call Waiting Parameter Guide

Parameter	Description	Default Setting
<b>Call Waiting Tone 1</b>		
<b>ToneName</b>	Distinctive Call Waiting Tone 1. An incoming SIP INVITE may include the same name in an Alert-Info header to choose this ring.	Bellcore-dr1

## Call Waiting Parameter Guide

Parameter	Description	Default Setting
<b>TonePattern</b>	Obihai Tone Pattern Script.	440-18;30; (.25+10)
<b>Call Waiting Tone 2</b>		
<b>ToneName</b>	Distinctive Call Waiting Tone 2. An incoming SIP INVITE may include the same name in an Alert-Info header to choose this ring.	Bellcore-dr2
<b>TonePattern</b>	Obihai Tone Pattern Script.	440-18;30; (.1+.1, .3+.1, .1+10)
<b>Call Waiting Tone 3</b>		
<b>ToneName</b>	Distinctive Call Waiting Tone 3. An incoming SIP INVITE may include the same name in an Alert-Info header to choose this ring.	Bellcore-dr3
<b>TonePattern</b>	Obihai Tone Pattern Script.	440-18;30; (.1+.1, .1+10)
<b>Call Waiting Tone 4</b>		
<b>ToneName</b>	Distinctive Call Waiting Tone 4. An incoming SIP INVITE may include the same name in an Alert-Info header to choose this ring.	Bellcore-dr4
<b>TonePattern</b>	Obihai Tone Pattern Script.	440-18;30; (.1+.1, .1+.1, .1+10)
<b>Call Waiting Tone 5</b>		
<b>ToneName</b>	Distinctive Call Waiting Tone 5. An incoming SIP INVITE may include the same name in an Alert-Info header to choose this ring.	Bellcore-dr5
<b>TonePattern</b>	Obihai Tone Pattern Script.	440-18;30; (.3+.1, .1+.1, .3+10)
<b>Call Waiting Tone 6</b>		
<b>ToneName</b>	Distinctive Call Waiting Tone 6. An incoming SIP INVITE may include the same name in an Alert-Info header to choose this ring.	User-dr1
<b>TonePattern</b>	Obihai Tone Pattern Script.	440-18;30; (.1+.1, .3+.2, .3+10)
<b>Call Waiting Tone 7</b>		
<b>ToneName</b>	Distinctive Call Waiting Tone 7. An incoming SIP INVITE may include the same name in an Alert-Info header to choose this ring.	User-dr2
<b>TonePattern</b>	Obihai Tone Pattern Script.	440-18;30; (.3+.1, .3+.1, .1+10)
<b>Call Waiting Tone 8</b>		
<b>ToneName</b>	Distinctive Call Waiting Tone 8. An incoming SIP INVITE may include the same name in an Alert-Info header to choose this ring.	User-dr3

**Call Waiting Parameter Guide**

Parameter	Description	Default Setting
<b>TonePattern</b>	Obihai Tone Pattern Script.	440-18;30;(.3+2)
<b>Call Waiting Tone 9</b>		
<b>ToneName</b>	Distinctive Call Waiting Tone 9. An incoming SIP INVITE may include the same name in an Alert-Info header to choose this ring.	User-dr4
<b>TonePattern</b>	Obihai Tone Pattern Script.	440-18;30;(.3+2)
<b>Call Waiting Tone 10</b>		
<b>ToneName</b>	Distinctive Call Waiting Tone 10. An incoming SIP INVITE may include the same name in an Alert-Info header to choose this ring.	User-dr5
<b>TonePattern</b>	Obihai Tone Pattern Script.	440-18;30;(.3+2)

**Ring Profile Parameter Guide**

Parameter	Description	Default Setting
<b>Ring Pattern 1</b>		
<b>RingName</b>	Name of the ring. An incoming SIP INVITE may include the same name in an Alert-Info header to choose this ring.	Bellcore-dr1
<b>RingPattern</b>	Obihai tone cadence script.	60;(2+4)
<b>Ring Pattern 2</b>		
<b>RingName</b>	Name of the ring. An incoming SIP INVITE may include the same name in an Alert-Info header to choose this ring.	Bellcore-dr2
<b>RingPattern</b>	Obihai tone cadence script.	60;(.3+.2,1+.2,.3+4)
<b>Ring Pattern 3</b>		
<b>RingName</b>	Name of the ring. An incoming SIP INVITE may include the same name in an Alert-Info header to choose this ring.	Bellcore-dr3
<b>RingPattern</b>	Obihai tone cadence script.	60;(.8+.4,.8+4)
<b>Ring Pattern 4</b>		
<b>RingName</b>	Name of the ring. An incoming SIP INVITE may include the same name in an Alert-Info header to choose this ring.	Bellcore-dr4
<b>RingPattern</b>	Obihai tone cadence script.	60;(.4+.2,.3+.2,.8+4)



## Ring Profile Parameter Guide

Parameter	Description	Default Setting
<b>Ring Pattern 5</b>		
<b>RingName</b>	Name of the ring. An incoming SIP INVITE may include the same name in an Alert-Info header to choose this ring.	Bellcore-dr5
<b>RingPattern</b>	Obihai tone cadence script.	60; (.2+.2, .2+.2, .2+.2, 1+4)
<b>Ring Pattern 6</b>		
<b>RingName</b>	Name of the ring. An incoming SIP INVITE may include the same name in an Alert-Info header to choose this ring.	User-dr1
<b>RingPattern</b>	Obihai tone cadence script.	60; (.2+.4, .2+.4, .2+4)
<b>Ring Pattern 7</b>		
<b>RingName</b>	Name of the ring. An incoming SIP INVITE may include the same name in an Alert-Info header to choose this ring.	User-dr2
<b>RingPattern</b>	Obihai tone cadence script.	60; (.4+.2, .4+.2, .4+4)
<b>Ring Pattern 8</b>		
<b>RingName</b>	Name of the ring. An incoming SIP INVITE may include the same name in an Alert-Info header to choose this ring.	User-dr3
<b>RingPattern</b>	Obihai tone cadence script.	60; (.25+9.75)
<b>Ring Pattern 9</b>		
<b>RingName</b>	Name of the ring. An incoming SIP INVITE may include the same name in an Alert-Info header to choose this ring.	User-dr4
<b>RingPattern</b>	Obihai tone cadence script.	60; (.25+9.75)
<b>Ring Pattern 10</b>		
<b>RingName</b>	Name of the ring. An incoming SIP INVITE may include the same name in an Alert-Info header to choose this ring.	User-dr5
<b>RingPattern</b>	Obihai tone cadence script.	60; (.25+9.75)



## File Sharing Parameter Guide

Parameter	Description	Default Setting
<b>File Sharing</b>		
<b>EnableAccessFromWAN</b>	<p>While accessing files on the attached USB storage device from the LAN side of the device is always enabled, accessing the files from the WAN side can be disabled. By enabling this option you allow access to the files from the WAN side. This option applies to all levels of access (admin, user, and anonymous).</p> <p>If this option is disabled, you are denied from accessing the files from the WAN when you click on the File Explorer link on the device web page even if you have logged in as the admin.</p> <p>This option needs a reboot for this change to take effect.</p>	Yes
<b>Anonymous User</b>		
<b>Enable</b>	<p>By enabling this option, you allow anonymous (read-only) access to the files on the USB storage device using this link: <code>http://&lt;obi-address&gt;/obi_share/anonymous</code></p> <p>The user is challenged to enter any UserID or Password in this case.</p>	No
<b>HomeDirectory</b>	<p>The Home Directory for anonymous level access, such that user can't navigate the file system above this directory.</p> <p>Maximum length of this field is 256 characters.</p> <p>A blank value is the same as slash (/), which allows navigation all the way to the root of the file system.</p>	/obi_share/anonymous
<b>FileFilter</b>	<p>A list of semicolon (;) separated filename filters to limit the type of files this user can see. Each filter MUST be of the format: <code>*.&lt;file-type&gt;</code></p> <p>where <code>&lt;file-type&gt;</code> is a literal string (no wildcards or space), such as <code>jpg</code>, <code>pdf</code>, <code>mp3</code>, and so forth, and <code>*</code> is a wildcard that matches any valid filename string.</p> <p>For example: <code>*.jpg;*.pdf;*.mp3;*.mov</code>.</p> <p>Maximum length of this field is 256 characters.</p>	
<b>User <math>N</math> (<math>N = 1</math> to <math>10</math>)</b>		
<b>Enable</b>	Allow users to login for file sharing with the <b>UserID</b> and <b>Password</b> for User $N$	No
<b>UserID</b>	<p><b>UserID</b> is case-sensitive. It must be an alphanumeric string, must not start with a number, and must not contain any spaces.</p> <p>Maximum length is 64 characters.</p>	user $N$
<b>Password</b>	<p>Password is case-sensitive. It must be an alphanumeric string and must not contain any spaces.</p> <p>Maximum Password length is 64 characters.</p>	

## File Sharing Parameter Guide

Parameter	Description	Default Setting
<b>HomeDirectory</b>	The Home Directory for anonymous level access, such that user can't navigate the file system above this directory. Maximum length of this field is 256 characters. A blank value is same as slash (/), which allows navigation all the way to the root of the file system.	/obi_share/user N
<b>FileFilter</b>	A list of semicolon (;) separated filename filters to limit the types of filters this user can see. Each filter MUST be of the format: *.<file-type> where <file-type> is a literal string (no wildcards or space), such as jpg, pdf, mp3, and so forth, and * is a wildcard that matches any valid filename string. For example: *.jpg, *.pdf, *.mp3, *.mov . Maximum length of this field is 256 characters.	*
<b>WriteEnable</b>	By enabling write access to the file system, you enable the user to upload, copy, remove, rename, cut and paste files, or create, remove, and rename directories on the USB storage device.	No

# Troubleshooting

---

If you experience issues with your HDA50 device, try the following solutions to resolve certain issues.

## Retrieve the Device IP Address

### To set up and configure your phone

If you are unable to access the device IP address from PDMS-SP or the main network router that the HDA50 is connected to, retrieve the device IP using a analog telephone.

After an analog phone is attached to your device, use the following procedure.

### To retrieve the device IP address

#### Procedure

- 1 Connect an analog telephone to the device **Phone** port.
- 2 From a phone attached to the device, dial \* \* \* to access the device Config Attendant.
- 3 Select **1** to hear the IP address of the device read back to you. Write this down.

## Access Device Web Portal

Each HDA50 device has its own built-in portal site at `http://{ip-address}` where {ip-address} is the IP address of the device. The native web portal offers configurable options and status information organized into a number of web pages.

### To access device web portal

- 1 Enter the device's IP address into your web browser using the format `http://0.0.0.0`.
- 2 Enter administrator credentials to access the web portal. The default user name and password are both `admin`.

## Possible Error Messages on Firmware Update Failure

The following table lists the possible error messages encountered when a firmware upgrade fails.

### Error Messages for Firmware Update Failure

Error Message	Description	Suggested Solution
Firmware Package Checksum Error	A corrupted firmware package file was used for the update.	Check the file and / or redownload the firmware package and try again.
System Is Busy	The device is busy because one of the phone services is in an active call or device provisioning is in progress.	Try to update again later.
Firmware Is Not Modified	The device is already running the same firmware as the one selected for update.	No need to upgrade.