4602 SIP Telephone
SIP Release 1.2
Administrator's Guide

16-300037
Issue 1.2
January 2005

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language as well as information regarding support for this product, while under warranty, is available through the following Web site: http://www.avaya.com/support.

Preventing Toll Fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there may be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Fraud Intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, in the United States and Canada, call the Technical Service Center's Toll Fraud Intervention Hotline at 1-800-643-2353.

Disclaimer

Avaya is not responsible for any modifications, additions or deletions to the original published version of this documentation unless such modifications, additions or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

How to Get Help

For additional support telephone numbers, go to the Avaya support Web site: http://www.avaya.com/support. If you are:

- Within the United States, click the *Escalation Contacts* link that is located under the *Support Tools* heading. Then click the appropriate link for the type of support that you need.
- Outside the United States, click the *Escalation Contacts* link that is located under the *Support Tools* heading. Then click the *International Services* link that includes telephone numbers for the international Centers of Excellence.

Providing Telecommunications Security

Telecommunications security (of voice, data, and/or video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf. Whereas, a "malicious party" is anyone (including someone who may be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based) or asynchronous (character-, message-, or packet-based) equipment or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company (including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Responsibility for Your Company's Telecommunications Security

The final responsibility for securing both this system and its networked equipment rests with you - Avaya's customer system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure:

- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products

TCP/IP Facilities

Customers may experience differences in product performance, reliability and security depending upon network configurations/design and topologies, even when the product performs as warranted.

Standards Compliance

Avaya Inc. is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Avaya Inc. The correction of interference caused by such unauthorized modifications, substitution or attachment will be the responsibility of the user. Pursuant to Part 15 of the Federal Communications Commission (FCC) Rules, the user is cautioned that changes or modifications not expressly approved by Avaya Inc. could void the user's authority to operate this equipment.

Product Safety Standards

This product complies with and conforms to the following international Product Safety standards as applicable:

Safety of Information Technology Equipment, IEC 60950, 3rd Edition, or IEC 60950-1, 1st Edition, including all relevant national deviations as listed in Compliance with IEC for Electrical Equipment (IECEE) CB-96A.

Safety of Information Technology Equipment, CAN/CSA-C22.2 No. 60950-00 / UL 60950, 3rd Edition, or CAN/CSA-C22.2 No. 60950-1-03 / UL 60950-1.

Safety Requirements for Information Technology Equipment, AS/NZS 60950:2000.

One or more of the following Mexican national standards, as applicable: NOM 001 SCFI 1993, NOM SCFI 016 1993, NOM 019 SCFI 1998

Electromagnetic Compatibility (EMC) Standards

This product complies with and conforms to the following international EMC standards and all relevant national deviations:

Limits and Methods of Measurement of Radio Interference of Information Technology Equipment, CISPR 22:1997, EN55022:1998, and AS/NZS 3548.

Information Technology Equipment – Immunity Characteristics – Limits and Methods of Measurement, CISPR 24:1997 and EN55024:1998, including:

- Electrostatic Discharge (ESD) IEC 61000-4-2
- Radiated Immunity IEC 61000-4-3
- Electrical Fast Transient IEC 61000-4-4
- Lightning Effects IEC 61000-4-5
- Conducted Immunity IEC 61000-4-6

Federal Communications Commission Statement

Part 15:

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Part 68: Answer-Supervision Signaling

Allowing this equipment to be operated in a manner that does not provide proper answer-supervision signaling is in violation of Part 68 rules. This equipment returns answer-supervision signals to the public switched network when:

- answered by the called station,
- answered by the attendant, or
- routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user.

This equipment returns answer-supervision signals on all direct inward dialed (DID) calls forwarded back to the public switched telephone network. Permissible exceptions are:

- A call is unanswered.
- A busy tone is received.
- A reorder tone is received.

Avaya attests that this registered equipment is capable of providing users access to interstate providers of operator services through the use of access codes. Modification of this equipment by call aggregators to block access dialing codes is a violation of the Telephone Operator Consumers Act of 1990.

Means of Connection

Connection of this equipment to the telephone network is shown in the following tables.

Canadian Department of Communications (DOC) Interference Information

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

Declarations of Conformity

United States FCC Part 68 Supplier's Declaration of Conformity (SDoC)

Avaya Inc. in the United States of America hereby certifies that the equipment described in this document and bearing a TIA TSB-168 label identification number complies with the FCC's Rules and Regulations 47 CFR Part 68, and the Administrative Council on Terminal Attachments (ACTA) adopted technical criteria.

Avaya further asserts that Avaya handset-equipped terminal equipment described in this document complies with Paragraph 68.316 of the FCC Rules and Regulations defining Hearing Aid Compatibility and is deemed compatible with hearing aids.

Copies of SDoCs signed by the Responsible Party in the U. S. can be obtained by contacting your local sales representative and are available on the following Web site: http://www.avaya.com/support.

All Avaya media servers and media gateways are compliant with FCC Part 68, but many have been registered with the FCC before the SDoC process was available. A list of all Avaya registered products may be found at: http://www.part68.org by conducting a search using "Avaya" as manufacturer.

European Union Declarations of Conformity

CE

Avaya Inc. declares that the equipment specified in this document bearing the "CE" (*Conformité Europeénne*) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (89/336/EEC) and Low Voltage Directive (73/23/EEC). This equipment has been certified to meet CTR3 Basic Rate Interface (BRI) and CTR4 Primary Rate Interface (PRI) and subsets thereof in CTR12 and CTR13, as applicable.

Copies of these Declarations of Conformity (DoCs) can be obtained by contacting your local sales representative and are available on the following Web site: http://www.avaya.com/support.

Japan

This is a Class B product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

To order copies of this and other documents:

Call: Avaya Publications Center
Voice 1.800.457.1235 or 1.207.866.6701
FAX 1.800.457.1764 or 1.207.626.7269

Write: Globalware Solutions
200 Ward Hill Avenue
Haverhill, MA 01835 USA
Attention: Avaya Account Management

E-mail: totalware@gwsmail.com

For the most current versions of documentation, go to the Avaya support Web site: http://www.avaya.com/support.

Contents

About This Guide

Overview

This guide covers how to administer the 4602/4602SW SIP (Session Initiation Protocol) Telephone. The 4602/4602SW SIP Telephone offers the latest advances in telephony systems. A primary administrative advantage is that updates and new features are downloaded to the phone without intervention or the need for phone replacement. Although the 4602/4602SW SIP Telephone is a basic IP telephone model, it shares many characteristics with higher-end IP telephones, including ease of operation for its users.

To use an Avaya SIP Solution, one or more servers must be configured for SIP and the SIP installation procedures must be completed. See Related Documentation for information about documentation on basic server setup and SIP installation.

Note:

This guide does not cover administration of non-SIP IP telephones. For information on administering any of the 4600 Series IP Telephones, see the *“4600 Series IP Telephone LAN Administrator’s Guide”* (Document Number 555-233-507).

The SIP telephone described in this document comes in two models, the 4602 and the 4602SW. The only difference between them is that the 4602SW SIP Telephone has a second Ethernet port and an internal switch for connecting a PC to the LAN. For purposes of this document, there is no difference in the administration between the 4602 and the 4602SW, and any reference to a 4602 SIP Telephone applies equally to a 4602SW SIP Telephone.

Intended Audience

This document is intended for telephone administrators.

Issue Date

This document was issued for the first time in June, 2004. This document was revised in September, 2004 for Release 1.1. The 1.1 Release includes new telephone parameters, the ability to switch from UDP to TCP as a SIP transport protocol, and additional information regarding the Avaya SIP Solution.

This document was revised in January, 2005 for Release 1.2, to incorporate the following new material:

- A section on moving SIP telephones from one location to another was added. See Moving a Telephone's Physical Location.
- A new Appendix C: Time Zone Determination, was added.
- A note indicating that an HTTP server is required for Avaya SIP Telephones was added to the Administrative Prerequisites section.

How to Use This Document

This Guide is organized to help you find topics in a logical manner. Read it from start to finish to get a thorough understanding of how to manage the 4602 SIP Telephone, or review the Table of Contents or Index to locate information specific to a task or function you want to perform.

Document Organization

This guide contains the following chapters and appendices:

Chapter 1: Introduction to Managing the 4602 SIP Telephone	Explains prerequisites, provides an administrative task checklist, and discusses the different approaches available for managing the telephone.
Chapter 2: Administering 4602 SIP Telephones	Provides details on converting 4602 Telephones from H.323 protocol to SIP protocol and setting the required parameters. This chapter also covers how to set up the configuration files, so that telephones are automatically configured during start up.
Chapter 3: Managing the Telephone Manually or Using the Web Interface	Covers using manual programming at the phone to override Web or other settings. Manual programming handles special situations and aids in investigating problems. Also provides procedures for using the Web interface to manage telephones in the system.
Chapter 4: Troubleshooting	This chapter explores basic and advanced troubleshooting concepts.
Appendix A: Configuration Parameters	Contains a complete listing and a brief description of all of the SIP telephone parameters.
Appendix B: Configuring a Dial Plan	Describes the syntax for and provides examples of specifying a dial plan for the phone.
Appendix C: Time Zone Determination	Specifies time zone coding for the Time Zone parameter.

Conventions Used

This guide uses the following textual, symbolic, and typographic conventions to help you interpret information.

Symbolic Conventions

Note:

This symbol precedes additional information about a topic. This information is not required to run your system

Important:

This symbol precedes information that calls attention to a situation that might cause problems or serious inconvenience.

CAUTION:

This symbol precedes information about a hazard that might potentially cause an interruption of service, loss of data, or harm to software.

Typographic Conventions

This guide uses the following typographic conventions:

`command`	Words printed in this type are commands that you enter into your system.
`message`	Words printed in this type are system messages.
Document	Blue underlined type indicates a section or sub-section in this document containing additional information about a topic.
"Document"	Italic type enclosed in quotes indicates a reference to an external document or a specific chapter/section of an external document.
italics	Italic type indicates the result of an action you take or a system response in step by step procedures.
Administrative	Words printed in bold type are menu or screen titles and labels, or items on menus and screens that you select or enter to perform a task, i.e., fields, buttons, icons and for general emphasis.

Related Documentation

The documents described in this section are available on the Avaya Web site, http://www.avaya.com/support.

For information on using the 4602 SIP Telephone see the *"4602 SIP Telephone User's Guide"* (Document Number 16-300035).

For information on using the Avaya SIP Solution with 4602 SIP Telephones, see the following documents:

"SIP Support in Avaya Communication Manager" (Document Number 555-245-705).

"Converged Communications Server Installation and Administration" (Document Number 555-245-705).

"Avaya Extension to Cellular User's Guide" (Document Number 200-100-700).

"Avaya Extension to Cellular Off-PBX Station (OPS) Installation and Administration Guide" (Document Number 555-100-500).

To configure the Avaya SIP Solution for 4602 SIP Telephones, see *"4602 SIP Telephone Release 1.1 Quick Setup Guide"* (Document Number 16-300158).

Chapter 1: Introduction to Managing the 4602 SIP Telephone

Introduction

This chapter provides an overview of basic 4602 SIP Telephone management. It offers a checklist of administrative tasks and an overview of configuration processing.

Administrative Prerequisites

Certain hardware and software requirements must be in place prior to installing and administering a SIP telephone system. These features are covered in detail in the documents listed under Related Documentation in this guide. You can also find these related documents on the Avaya Web site, http://www.avaya.com/support.

Avaya's SIP Solution recommends specific configurations based on Avaya-supported OPS (Outboard Proxy SIP). For more information, see the *"4602 SIP Telephone Release 1.1 Quick Setup Guide."*

Important:
An HTTP server is required to operate Avaya SIP Telephones, and is available from a vendor of your choice. Avaya recommends Apache. For information about the Apache HTTP Server Project, see the http:\\httpd.apache.org Web site.

Once the prerequisites have been satisfied, you can proceed with administering Avaya 4602 SIP Telephones as IP endpoints.

Administrative Steps/Checklist

This checklist covers the steps the administrator takes to get the 4602 SIP Telephone system up and running.

Step	Action	Result
1.	Administers the SIP Proxy server.	Hardware is ready for startup.
2.	Performs H.323 to SIP conversion on all 4602 SIP Telephones. (See Chapter 2: Administering 4602 SIP Telephones for details)	SIP software is downloaded to all telephones.
3.	Determines the best way to administer telephones: • Use default values • Use DHCP to set certain required parameters • Use Web interface and/or dialpad to set certain other parameters (See Administrative Approaches for details.)	Phones are operative and ready for use.
4.	Configure a Dial Plan. (See Appendix B: Configuring a Dial Plan for details.)	Automatic dialing of internal/external calls, depending on how the plan is configured. Facilitates call routing and minimizes dialing delays.
5.	Distributes Extension Numbers and Passwords to users.	Users can log in (if required) and access their Web interface.

4602 SIP Telephone Administration Tools

The 4602 SIP Telephone has basic tools and capabilities to help administrators assign operating parameters and manage telephone settings and features. They are:

- Downloadable configuration files for setting common telephone parameters on startup,
- DHCP for setting additional parameters or modifying current parameters,
- Administrator's Web interface for setting/modifying most parameters on a phone-by-phone basis,
- Manual programming of any critical parameters from a telephone's dialpad, as needed, and
- Downloadable firmware updates (automatic for all phones and manual on a phone-by-phone basis).

Parameters that must be set for the phone(s) to operate properly are listed in Required Parameters in Chapter 2: Administering 4602 SIP Telephones. For a list of all operating parameters applicable to 4602 SIP Telephones, see Appendix A: Configuration Parameters.

Administrative Approaches

An administrator can choose one or any combination of options to configure 4602 SIP Telephones.

For example, the administrator would normally use the configuration files that are automatically downloaded during startup to assign all 4602 SIP Telephones a common set of [default] operating parameters. Then DHCP can assign parameters that overwrite the default values to groups of phones, perhaps those using a specific server or within a specific department. (Chapter 2: Administering 4602 SIP Telephones covers setting these group parameters.) The administrator would then use the Web interface to further configure certain parameters (for example, a user name) for single phones within the operating environment. Finally, the administrator or user can specify certain values, such as a password, using the telephone dialpad. (Chapter 3: Managing the Telephone Manually or Using the Web Interface covers the Web interface and manual commands.)

Another administrative approach can be to use a single telephone as verification that the system is operating properly before applying operating parameters to all phones in the system. In this scenario, **Startup** copies the default values and the administrator sets any overriding values on the phone using the Web interface (and the telephone dialpad, as applicable). After testing that the telephone works properly, all phones in the system are configured as described in the preceding paragraph.

CAUTION:

SIP uses a specific order to establish the parameters any telephone ultimately uses. Since data can be derived from many sources, be sure to understand which action or method of assigning/updating parameters takes precedence over another. See the next section, Parameter Sources and Their Precedence for information. Most importantly, be aware that a system or telephone restart always sets all parameters back to their default values.

Parameter Sources and Their Precedence

The following steps show the order in which telephone settings get assigned or updated. It is important to understand how these data sources interact to create the active configuration that the phone finally uses.

1. The first time, and only the first time a phone starts up, default values are copied to NVRAM. These default values are specified in Appendix A: Configuration Parameters.
2. Next, the telephone copies the NVRAM values for all parameters into the active configuration.
3. The phone then runs DHCP, if it is enabled, to obtain an IP Address, Subnet Mask, Gateway(s), DNS Server Address, and Configuration HTTP Server IP Address. These values overwrite the current values in the active configuration.
4. The phone then downloads a configuration file and uses the values in this file to overwrite the current values in the active configuration, unless the **OverrideWeb** parameter is disabled (see Appendix A: Configuration Parameters).

To summarize the result of these four steps:

- Configuration file parameters have precedence over DHCP parameters.
- DHCP parameters have precedence over manually-configured parameters set using the Web interface or the telephone dialpad **`Setup`** command.

Note:

Using the **`Setup`** command (from either the Web interface or dialpad) before DHCP completes causes the saved setup values to overwrite the current values in NVRAM.

This precedence is important to understand if you plan to use a combination of parameter sources. It is also important to note that the dialpad **`Setup`** command and the Web interface both display data from the currently active configuration and not NVRAM. However, when values entered using either the Web interface or dialpad are saved, the displayed values overwrite the value in NVRAM.

Thus, in the configuration process, saving a value from the Web interface or the **`Setup`** command takes effect only after the phone reboots and re-reads the values. Even then, DHCP or configuration files always have precedence over manually entered or Web interface values.

Chapter 2: Administering 4602 SIP Telephones

Introduction

This chapter covers setting up your 4602 SIP Telephones. Conversion procedures from the factory-set protocol to SIP and back are provided. This chapter also lists the minimal set of parameters that must be defined prior to operating phones in a SIP environment.

Converting H.323 Protocol Phones to SIP

All 4602 telephones shipped from the factory are pre-loaded with code to use the H.323 protocol. This section provides a step-by-step procedure for loading a factory-fresh or previously used H.323 set with SIP software. The procedure for returning a set that has been loaded with SIP software back to the H.323 protocol appears later in this chapter.

The factory H.323 software and the SIP software each require a different provisioning environment. Some of the differences are:

- H.323 uses TFTP for file downloads and SIP uses HTTP downloads.
- H.323 uses script files for setting options and SIP uses configuration files.
- The binary file format for H.323 and SIP application and boot files differ. This difference requires using special H.323 binaries versions when converting from SIP, and special SIP binaries versions when converting from H.323. The term “different” means different from the version you would use during an upgrade not involving a protocol change.

To convert in either direction, both of the H.323 and SIP provisioning environments must be set up in advance.

Converting an H.323 Set to SIP

These steps assume you have a working H.323 environment. Before you begin the upgrade, be sure that you have:

- Preloaded the configuration HTTP server with the required SIP configuration (i.e., sip_4602D01A.txt), SIP application (sip_4602apXXXX.ebin), and SIP boot binary (i.e., sip_4602btXXXX.ebin) files. All files must be in the root of the server (i.e., http://192.168.0.1/sip_4602D01A.txt).
- Ensured that the SIP configuration file on the configuration HTTP server properly sets the **AppName** and **BootName** parameters.
- Set the DHCP server with a Site-Specific Option Number of 172 that specifies the parameter **ConfigHttpSrvr** (i.e., ConfigHttpSrvr=192.168.0.100).

  If you do not use the DHCP SSON to configure the HTTP server address, you must manually set the HTTP server's address. To set the server address manually, use the local **SETUP** command at each phone, or use the Web interface to set up the **ConfigHttpSrvr** value properly in each phone. Chapter 3: Managing the Telephone Manually or Using the Web Interface covers both Web and manual setup.
- Preloaded the special conversion version of the SIP boot binary (i.e., 323tosipXXXX.bin) and the appropriate script file (i.e., 46xxupgrade.scr) onto the TFTP server.

Automatically Upgrading All H.323 Telephone Sets

Follow these steps to automatically upgrade all H.323 telephone sets:

1. Modify the H.323 script to always download the special conversion version of the boot binary 323tosipXXXX.bin instead of the regular H.323 boot application.
2. Restart the phones via the switch.
3. When the phones restart, they download and run the special SIP conversion boot file, restart again, and then attempt to download a configuration file from the HTTP server.
4. The Configuration file points the phones to the new SIP boot and application binaries, which will be downloaded.
5. After the phones restart, they run using SIP.

Upgrading on a Set-By-Set Basis

Follow these steps to upgrade on a set-by-set basis:

1. Modify the H.323 script file on the TFTP server so that if the SIG option is set to SIP (SIG=2) from the phone, it downloads the special conversion version of the boot binary (323tosipXXXX.bin), instead of the regular H.323 boot application.
2. From an H.323 phone, press **Mute** then enter **SIG#** using the dial pad. Press ***** until the value **SIP** displays (this step assumes your script file is looking for a SIG value of 2 to indicate SIP).
3. Restart the phone by pressing **Mute** then entering **RESET#** using the dial pad. Press ***** and then # when prompted.

   The phone restarts and downloads the special conversion version SIP boot file from the TFTP server.
4. When the phone restarts, it boots using the SIP boot file, restarts again, and then attempts to download a configuration file from the HTTP server.

   Note:

   > If you are not using DHCP, you must manually configure the set. Use the local **SETUP** command to configure an IP address, subnet mask, Gateway, and configuration HTTP server into the phone before proceeding.
5. The configuration file points the phone to the new application binary, which will be downloaded.

   After the phone restarts, it runs using SIP.

Converting a SIP Set Back to H.323

These steps assume you have a working SIP environment. Before you begin the conversion, you must do the following:

- Preload the TFTP server with the required H.323 script, application, and boot binary files that are normally used by an H.323 4602 phone.
- Preload the special conversion version of the H.323 boot binary (sipto323XXXX.ebin) onto the HTTP server.

  Note:

  > The SIP to H.323 conversion is performed only on a set-by-set basis.

Upgrading on a Set-By-Set Basis

This procedure resets all the parameters H.323 code uses to their default values, including resetting the SIG flag to the H.323 default value.

1. Use the administrator's Web interface of the SIP phone you want to convert. Go to the **Network Settings** page and make sure the Configuration HTTP Server IP Address is properly set.
2. Go to the **Firmware Update** page. Specify the special conversion version of the H.323 boot binary (sipto323XXXX.ebin) as the **File to download**.
3. Click **Download Now** to download the file.

   The phone downloads the file. When completed, the message `Firmware upgrade successful` *displays.*
4. Click **Reset** to reset the phone.

   The phone restarts, looking to the TFTP server to download a script file. *The messages* `Starting` and `DHCP, press * for Setup` *display*.

   Note:

   If you are not using DHCP, you must manually configure the set. Use the local **ADDR** command to configure an IP address, subnet mask, gateway, and TFTP server into the phone before proceeding.
5. Press ***** to enter the address configuration command.

   The phone displays `phone=xxx.xxx.xxx.xxx, new=`.
6. Press ***** several times to scroll through the values without making changes. When the message `no new values, #=OK` displays, press **#**.

   The display goes blank.
7. Press **Mute R E S E T #** (Mute 73738 #).
8. Press **#** to reset all values, then press **#** again to restart the phone.

   The script specifies a new boot and/or application file, which is then downloaded. After the phone restarts, it runs using H.323.

Setting Parameters

Many installations use DHCP and configuration files to automate setting telephone parameters. This section describes how to use DHCP and configuration files for this purpose.

Using DHCP Settings

You can use DHCP to provide these settings:

- IP Address (**IPAddress**)
- Subnet Mask (**SubNetMask**)
- Router IP Address (**GatewayAddress**)
- DNS Address (**DnsAddress**)

If a site-specific option (SSON) is set, it can provide:

- HTTP server for Configuration files (**ConfigHttpSrvr**)

Only the value of **ConfigHttpSrvr** may be specified using the Site-Specific Option Number (SSON).

The SSON must contain a name=value pair, for example, *ConfigHttpSrvr=192.168.0.10*.

Using Configuration Files

The phone looks for configuration files in the HTTP server's root directory.

Note:

To use configuration files, the **ConfigHttpSrvr** value must be set using the site specific option (SSON) in DHCP, or manually through either the Web interface or the dialpad **SETUP** command.

Configuration files are either:

- Model-specific

  or

- Telephone-specific

Phone startup checks the HTTP server for a telephone-specific configuration file. The file must be stored on the HTTP server and named in the format:

sip_aabbccddeeff.txt where *aabbccddeeff* is the MAC address of the telephone that will use the configuration file.

Note:

The MAC address is printed on the bar code label on the bottom of the phone. You can also use the **`V I E W`** command (**Mute 8 4 3 9 #**) to display the MAC address.

If a telephone-specific file is not found, startup then looks for a model-specific file. For the 4602 SIP Telephones, the model-specific file will be one of the following:

- **4602D01A.txt** for the 4602 Telephone
- **4602D02A.txt** for the 4602SW Telephone

Configuration files can be broken into several pieces to separate often-modified parameters from those that don't change from time-to-time or model-to-model. Use the **`Include`** command to specify additional parameters in the main configuration file.

Note:

`Include` commands can *only* be specified in the main configuration file, and the commands *must* be located at the end of the file.

Each parameter must appear on its own line in the configuration file. Enter a name/value pair for each parameter in the configuration file. The name and value may be separated by an arbitrary number of spaces or tabs.

The configuration file ignores upper and lower case. However, note that case may be important in the filenames specified for AppName and BootName, depending on your HTTP server. Spaces are not permitted in any of the configuration values.

To include comments in a configuration file, use # (the pound sign) as the first character in the comment line.

Configuration File Examples

Figure 1: Configuration File Examples

4602D01A.txt

```
# This configuration file is version 1.0 created on 9/15/03.
AppName sip_4602ap0079.ebin
BootName sip_4602bt0079.ebin
# Includes must be at the end of the main configuration file only
Include   common.txt
```

comon.txt

```
# This common configuration file is version 1.0 created on 9/15/03.
Hotline 5000
MsgButtonUrl 77777
DstEnable 1
DstEnd 0430
DstStart 1026
DialPlan 911|[1-8]xxx|9xxxxxxx|90|91xxxxxxxxxx
ForcedLogin 1
CallFwdAddress sip:voicemail@avaya.com
DTFormat       2
ProxyServers   192.168.0.9:5060
RegistrarServers 192.168.0.9:5060
```

Required Parameters

Certain parameters must be specified for the 4602 SIP Telephone to operate properly in most SIP environments. Those required parameters are:

- IP Address (**IPAddress**) - Usually supplied by DHCP, but can be manually configured from the dialpad or using the Web interface.
- Subnet Mask (**SubNetMask**) - Usually supplied by DHCP, but can be manually configured from the dialpad or using the Web interface.
- Gateway (**GatewayAddress**) - Usually supplied by DHCP, but can be manually configured from the dialpad or using the Web interface.
- DNS Server IP Address (**DnsAddress**) - Usually supplied by DHCP, but can be manually configured from the dialpad or using the Web interface. This parameter must be supplied if a domain is specified for the proxy or registrar.

- Proxy Server (**ProxyServers**) - A comma-separated list of up to three numeric IP addresses or domain names for the proxy server. If only a domain is specified, a SIP SRV record for the proxy must be configured in the DNS server and the port must be set to **0** (zero).
- Registrar Server (**RegistrarServers**) - A numeric IP address or domain name for the Registrar server. If only a domain is specified, a SIP SRV record for the registrar must be configured in the DHCP server and the port must be set to **0** (zero).
- User Name (**SipName**) - The user name used to register the phone with the registrar.
- Password (**SipPwd**) - The password used to register the phone with the registrar.

If you are using configuration files, you must also specify:

- Configuration Server IP Address (**ConfigHttpSrvr**) - The location of both configuration files and binary image files

If you want to automatically set the time, you must specify:

- SNTP Server IP Address (**SntpServers**)

The remaining parameters can usually be left at their default values, as shown in Appendix A: Configuration Parameters. However, for the best operation, review all parameters to ensure that the default value will provide the desired operation.

Chapter 3: Managing the Telephone Manually or Using the Web Interface provides information on using the Web interface or the telephone dialpad to manually set parameters.

DNS Address Resolution

DNS is used only to look up SRV records when domains are specified for the proxy or registrar servers.

Forced Login Passwords

The Forced Login feature requires telephone users to enter their numeric user names and passwords using the dialpad. User entry replaces downloading logins in a configuration file or setting logins from the Web interface. Enable this feature by setting the **ForcedLogin** parameter to **1** (see Appendix A: Configuration Parameters).

Moving a Telephone's Physical Location

Reasons for moving a telephone might be due to an office relocation or to transfer a telephone from one user to another. Before moving a specific telephone for which an extension has been registered, the phone must first either be logged off or cleared.

If the **ForcedLogin** parameter is **1** (Enabled), perform a **MUTE LOGOFF**, as described in Local Commands for Manual Configuration in Chapter 3. Doing so unregisters the telephone from the server. After moving the phone, log in using the old extension and password, then have the user change the password, if applicable.

If the **ForcedLogin** parameter is **0** (Disabled), perform a **MUTE CLEAR**, as described in Local Commands for Manual Configuration in Chapter 3. Clearing the phone returns it to the factory default state. After moving the phone, you must reset any manually-set parameters via static addressing or DHCP.

Specifying a Domain Name for the Registrar and/or Proxy Servers

You can specify a domain name instead of a numeric IP address for the registrar and/or proxy servers. Use a domain name when you want to do an SRV lookup to find the appropriate server the phone(s) should use. When specifying a domain name, leave the **RegistrationDomain** parameter blank. Also, be aware of the following restrictions regarding Domain Names and/or Port Numbers:

- When using a domain name, the Port for that server (if configured) must be set to zero (**0**).
- When a numeric IP address is used instead of a domain name, the Port for that server must be set to **5060**.
- When using a domain name, you must also configure either a TCP or UDP SRV DNS record (not both) for that domain in your DNS.
- If you are using a CCS (Converged Communications Server) proxy, you must specify the the Domain Name in addition to the registrar/proxy's IP address.

Specifying a Registration Domain

If you use a FDQN (fully-qualified Domain Name) or a numeric IP address rather than specifying a domain for the registrar and/or proxy servers, use the **RegistrationDomain** parameter to specify the domain with which you want to register.

Switching from UDP to TCP

As of Release 1.1, TCP (Transmission Control Protocol) is available as an alternate transport protocol to UDP (User Datagram Protocol). Depending on your implementation, you can switch from UDP to TCP using the **SipProtocol** parameter.

Chapter 3: Managing the Telephone Manually or Using the Web Interface

Introduction

This chapter covers using the Web interface to manage a specific 4602 SIP Telephone. This chapter also provides the manual commands which can be accessed using the telephone dialpad to set certain parameters.

Setting an IP Address in the Telephone

Before you access the Web interface, first make sure the phone has a usable IP address. You must enter the IP address of the phone whose settings you want to review or update before you log in to the administrative Web interface.

As described in Parameter Sources and Their Precedence in Chapter 1: Introduction to Managing the 4602 SIP Telephone, by default, the phone tries to use DHCP first to set the:

- IP Address
- Subnet Mask
- Gateway
- DNS Server
- HTTP Server for Configuration Files and Firmware Binaries (using the site-specific option)

Alternately, you can manually set the IP address using the telephone dial pad. This establishes contact to set the other parameters via the Web interface.

Determining the IP Address

To verify the IP address currently assigned to the telephone, follow this procedure:

1. With the phone idle, press **Mute** and enter **I N F O #** using the dialpad.

   The phone displays `Info View` *and* `*=End #=Next`

2. Press **#**.

   The phone displays `IP address DHCP` *or* `IP address Static` *and the numeric IP address.*

3. To exit the **INFO** mode and return the phone to normal operation, press *.

Using the Telephone Dialpad to Set the IP Address

To manually set the telephone's IP address, follow these steps:

1. Plug in the phone and watch for the prompt `Press * for Setup`.
2. When the prompt displays, press the * key.

   The phone displays `Clear All Values` *and* `*=No #=Yes`.

3. Press *

   The phone displays `DHCP=On/Off` *and* `*=Toggle #=OK *=`.

4. Press * until `DHCP=Off` displays.
5. Press **#.**

   The phone displays `IP Addr=?` *and* `Speaker=? #=OK *=`.

6. Use the dialpad to enter the **IP address**, then press **#**. (If applicable, press the **Speaker** button to backspace.)

   The phone displays `Mask=?` *and* `Speaker=<- #=OK *=`.

7. Enter the **SubNet Mask**, then press **#**.

   The phone displays `Gateway=?` *and* `Speaker=? #=OK *=`.

8. Enter either the **Router address** or **Gateway address**, then press **#**.
9. You may optionally specify other parameters, when prompted. Or, if you plan to complete programming from the Web interface, press **#** in response to all other prompts.

   The phone displays `Saving Values` *and then* `Starting`. *The telephone then reboots using the values entered*.

Accessing the Telephone's Web Interface

After the telephone receives the IP address either from DHCP or manually by Using the Telephone Dialpad to Set the IP Address, access the administrator's Web interface.

1. Enter **http://aaa.bbb.ccc.ddd** into the address bar of your PC's internet browser, where *aaa.bbb.ccc.ddd* is the IP address assigned to the telephone whose settings you want to view or update.

   You are prompted to enter a login and password.

   Note:

   The default administrator's login is **admin** and the default password is **barney**.

2. Enter **your login** and **your password**. Use the default values if you have not set up your own login and password.

   Connection proceeds and the browser displays the administrator's Main (Home) page.

Bypassing an Internet Proxy

Some networks require all browsers to use a proxy for Internet access. If you have a problem accessing the Web interface, it might be because of the browser's use of a proxy. To bypass the proxy when accessing the phone's Web interface, follow these steps for Internet Explorer:

1. Open Internet Explorer on your PC and click the menu item, **Tools**.
2. Select **Internet Options**.
3. Select the **Connections** tab and then click the **LAN Settings** button.
4. If **Use a proxy server for your LAN** is selected, click the **Advanced** button. If it is not selected, you are not using a proxy and can return to Step 1 in Accessing the Telephone's Web Interface without proceeding further.

   Note:

   De-select this option to turn the proxy off in order to access a large number of phones directly by IP address.

5. In the **Exceptions** box, enter the **IP address** for the phone you want to administer.
6. Click **OK** to close all of the dialogue boxes and return to Step 1 in Accessing the Telephone's Web Interface.

Main (Home) Page

The Home page provides access to several administrative Web pages. They are:

- **Network & QoS** - used to view or modify a phone's Internet Protocol or Quality of Service settings.
- **Firmware Update** - used to view or modify the file name from which a software download is taken or the Configuration HTTP Server. You can also initiate a firmware download using this page.
- **SIP Settings** - used to view or modify this phone's SIP registration or server information.
- **Phone Settings** - used to view or modify phone settings such as the Date/Time format, messages button URI, ring type, button click feedback, and other phone-specific features and settings.
- **Call Handling** - used to view or modify call handling feature settings such as Call Forwarding, Call Waiting, Call Hold, Do Not Disturb, Speed Dial, and HotLine.
- **Admin Security** - used to view or modify the administrative password for a phone.
- **User Security** - used to view or modify the user password for (user) Web interface access.
- **Network Status** - displays a phone's current IP and QoS settings.
- **Hardware Status** - displays a phone's current Model Number, CPU attribute and MAC address.
- **Firmware Status** - displays the Boot or Application filename and the HTTP configuration server from which this phone obtains its operating parameters.
- **Reset** - re-boots the telephone, restoring all parameters to their default settings.

Note:

Always click the **Save** button after modifying one or more values on any of the pages listed above. Updates do not occur until you save your data.

Switching to the User Web Interface

The user Web interface is helpful in debugging problems with a specific phone.

To switch to the user Web interface, re-establish a Web connection to the telephone using the appropriate user password when prompted. The user Web interface is described in detail in the *"4602 SIP User's Guide."*

Local Commands for Manual Configuration

This section describes how to use the telephone's manual configuration capabilities.

The following table outlines the local commands available through the telephone dialpad. Local commands are useful when debugging problems at the phone. To enter manual commands during startup, press the # (pound) key when prompted to, or after startup, press # any time the phone is idle.

Command Mnemonic	Numeric Equivalent	Description/Use
MuteSETUP#	**Mute73837#**	Use this command to view or modify these parameters: DHCP On/Off, IP Address, Subnet Mask, Gateway, HTTP Configuration Server Address, Proxy Server Address, Registrar Server Address, 802.1Q Tagging On/Off, and VLAN ID. Only numeric values are permitted, which could cause difficulty entering file paths. Since slashes (//) are not permitted with this local command, all files must be located in the root directory. The Web interface, however, allows full entry of a URI and path, and may be a better choice for setup tasks. The Setup values entered here are those used in the telephone's active configuration. Setup values may differ from those stored in NVRAM if they have been modified by DHCP or a configuration file (see Parameter Sources and Their Precedence). Use this command to set a phone to a known, working set of parameters when debugging the phone.
MuteINFO#	**Mute4636#**	Displays the current settings of: IP Address, Subnet Mask, Gateway, Link Speed, Proxy Server Address, Registrar Server Address, SNTP Server Address, 802.1Q Tagging On/Off, Current Application File Name, Current Boot File Name, Configuration File Date, Firmware Version and Build Date, Model Number, MAC Address, and Serial Number. The values displayed are those of the currently active configuration. Use this command when debugging phone problems, to verify that the critical operating parameters in the phone have been set to the correct values.
MuteRESET#	**Mute73738#**	Resets the phone. Using this command is easier than a reset by unplugging the telephone's cord.

1 of 2

Command Mnemonic	Numeric Equivalent	Description/Use (continued)
`MuteCLEAR#`	**Mute25327#**	Returns the phone to its factory default state, clearing all manually-entered data from the dialpad or Web interfaces, including the Web access passwords. Passwords are cleared to their default values and DHCP is enabled. Use this command to reset the phone to a known state when the user or administrator password has been lost.
`MuteLOGOFF#`	**Mute564633#**	Unregisters the phone from the SIP Registrar. This command is only applicable if **ForcedLogin** is set to **1** (Enabled). **MuteLOGOFF#** prevents others from using the phone. The phone is unusable until the registered user logs back in.
		2 of 2

Chapter 4: Troubleshooting

Introduction

This chapter provides basic and advanced troubleshooting procedures.

Basic Troubleshooting Chart

Problem/Symptom	Suggested Solution
Phone does not activate when it is plugged in and nothing appears on the display.	The set may not be receiving power. Double check that the Ethernet cable is plugged into the jack labeled and that the power source is plugged into a working outlet.
Phone has information on the display, but does not respond to button presses.	Try restarting the phone by unplugging the Ethernet cable plugged into the jack labeled and then plugging it back in.
Display shows an error or informational message.	This could indicate a network problem. Contact the network administrator.
Audio quality is poor on both the handset and speaker. You may hear clipped, garbled, or severely delayed speech.	Various potential network problems may be causing this problem. Contact the network administrator. Swap out the phone to ensure it is not defective.
No audio from the handset, but speaker works okay.	Check that the handset is properly plugged into the phone. Try swapping a handset from a similar phone to see if the handset or cord is defective.
The Web interface doesn't work or works intermittently.	Try bypassing the proxy server, using the Bypassing an Internet Proxy procedure in Chapter 3: Managing the Telephone Manually or Using the Web Interface. The phone's IP address may also have changed since you last accessed the Web interface. Use Determining the IP Address to ensure that you are using the proper address to connect to the Web interface.

Advanced Troubleshooting Chart

Problem/Symptom	Suggested Solution
The telephone displays: `No Service`	The phone is unable to register with the Registrar server. Verify that the proper **SipName** and **SipPwd** are specified for registration. Also check that the server is operating.
The telephone displays: `Duplicate IP Address`	The phone has been given an IP address that is already in use. If you are using a manually-configured IP address, use the **`Setup local`** command to choose a free IP address.
Problems downloading a configuration file or other files.	Closely observe the error message on the telephone display when the phone starts up for hints as to the problem's cause. The problem may be due to an improperly named configuration file (see Using Configuration Files), an improperly specified server address, an unreachable server, an error in configuration of the files on the HTTP server, or an error in the AppName, BootName, or Include value that was specified.
Speed dialing using the telephone keypad does not work.	You have inadvertently enabled the HotLine feature, which disables speed dialing. Avaya does not support the HotLine feature. To correct, you must set the **HotLine** parameter value to **0** (zero).

Appendix A: Configuration Parameters

Introduction

The chart below provides a key to the abbreviations used in the column labeled “Source(s)” in Table 1: 4602 SIP Telephone Parameters.

Source	Abbreviation
DHCP ACK	DHCP
DHCP Site Specific Option	SSON
Configuration File	CFG
Manual Entry Using Setup	MAN
Web Interface - User	WEBU
Web Interface - Administrator	WEBA

Table 1: 4602 SIP Telephone Parameters lists all telephone parameters.

Table 1: 4602 SIP Telephone Parameters

Parameter	Value Type	Value	Default	Source(s)
AppName	Up to 32 alphanumeric characters	Application image name for the telephone. An application name is specified in a configuration file and is checked against the NVRAM version to decide if a new version needs to be downloaded. The NVRAM value is updated after a successful download and a successful flash programming sequence.	Last correctly downloaded file name.	CFG, WEBA

1 of 8

Table 1: 4602 SIP Telephone Parameters (continued)

Parameter	Value Type	Value	Default	Source(s)
BootName	Up to 32 alphanumeric characters	Boot image name for the telephone. A new boot name is specified in a configuration file and is checked against the NVRAM version to decide if a new version needs to be downloaded. The NVRAM value is updated after a successful download and a successful flash programming sequence.	Last correctly downloaded file name.	CFG, WEBA
BusyRouting	1 ASCII character	Specifies how to handle a call while the phone is busy. On multiline phones this happens only when all call appearances are in use. 0 = Supply a Busy Here return code 1 = Supply a Busy Everywhere return code 2 = Forward the call to CallFwdAddress if assigned, otherwise return a Busy Here code.	0	CFG, WEBA, WEBU
CallFwd	Up to 2 ASCII characters	Call forwarding is set to: 0 = Calls are not forwarded 1 = Calls are forwarded without ringing first [2-9] = Calls are forwarded after 2-9 six second intervals (correlates to rings for nominal 2 second on, 4 second off).	0	CFG, WEBA, WEBU
CallFwdAddress	Up to 64 ASCII characters	SIP URL that calls are forwarded to. Example: sip:1001@elitecorpusa.com	0.0.0.0	CFG, WEBA, WEBU
CallWaiting	1 ASCII character	Call waiting indication: 0 = No indication to user 1= Beep heard by user	0	CFG, WEBA, WEBU
ConfigHttpSrvr	Up to 64 ASCII characters	IP address of the HTTP server on which configuration files are located. All configuration files must be in the root directory. Examples: 192.168.0.100	“”	SSON, MAN, WEBA

2 of 8

Table 1: 4602 SIP Telephone Parameters (continued)

Parameter	Value Type	Value	Default	Source(s)
DialDelay	Up to 2 ASCII characters	The number of seconds (1-99) to wait before en bloc sending digits dialed in an invite message. The time after which a phone automatically attempts to dial a non-null DialPlan sequence. See Appendix B: Configuring a Dial Plan for more information.	10	CFG, WEBA
DialPlan	Up to 255 ASCII characters	This string of characters specifies one or more dialplans for the phone. More than one DialPlan parameter may be specified and parameters should be logically OR'd together. See Appendix B: Configuring a Dial Plan for more information.	""	CFG, WEBA
DisableWebAdmin	1 ASCII character	0 = Web Administration Interface Enabled 1 = Web Administration Interface Disabled	0	CFG
DisplayName	Up to 32 ASCII characters	Name to be sent in the SIP display name field. This value displays during caller id.	""	CFG, WEBA, WEBU
DnsAddress	Up to 255 ASCII characters	IP address of the DNS server.	0.0.0.0	DHCP, CFG, WEBA
DoNotDisturb	1 ASCII character	Specifies if the user wants the phone to ring for incoming calls. When set to 1, the phone will not ring. 0 = DND Disabled 1 = DND Enabled	0	CFG, WEBA, WEBU
DscpAudio	Up to 2 ASCII characters	Differentiated services code point for audio packets. Valid values are 0 to 63.	46	CFG, WEBA
DscpSignaling	Up to 2 ASCII characters	Differentiated services code point for signaling packets. Valid values are 0 to 63.	34	CFG, WEBA
DstEnable	1 ASCII character	Daylight Savings Time (DST). 0 = Disable DST 1 = Enable DST	0	CFG, WEBA
DstEnd	Up to 3 ASCII characters	Start date of Daylight Savings Time in MMDDHH.	""	CFG, WEBA
DstStart	Up to 3 ASCII characters	End date of Daylight Savings Time in MMDDHH.	""	CFG, WEBA

3 of 8

Table 1: 4602 SIP Telephone Parameters (continued)

Parameter	Value Type	Value	Default	Source(s)
DTFormat	1 ASCII character	Date and time format for LCD: 0 = mm/dd/yy hh:mm(a/p) 1 = dd/mm/yy hh:mm(a/p) 2 = mm/dd/yy hh:mm(24-hour time) 3 = dd/mm/yy hh:mm(24-hour time)	0	CFG, WEBA, WEBU
DtmfMethod	1 ASCII character	0 = Always use in-band signaling (never send 2833) 1 = 2833 by negotiation in SDP (Session Description Protocol) 2 = 2833 always (ignore SDP)	1	CFG, WEBA
Ethernet2	1 ASCII character	Status of the second Ethernet Interface. 0 = disabled 1 = Auto negotiate	1	CFG, WEBA
ForcedLogin	1 ASCII character	Forces the user to enter a numeric extension and password to log in to the phone. The numeric login and password are used as the user name and password with the SIP registrar. The password automatically has the string “elite” appended because many registrars require a non-numeric character in the password. If ForcedLogin is disabled, the SipName and SipPwd must be provided via the Web interface or a Configuration file for the phone to properly register. Only numeric extensions and passwords are allowed. 0 = No Login Required (disabled) 1 = Login Required In addition, the set keeps the last valid login and password in non-volatile memory so that it can be automatically submitted on a reboot. If the user logs off the phone, the non-volatile values are cleared.	0	CFG, WEBA
GatewayAddress	Dotted Decimal ASCII	Gateway address for the telephone.	0.0.0.0	DHCP, MAN, WEBA
HoldRemind	1 ASCII character	If enabled, the Hold reminder tone sounds every minute while any call is in the hold state. 0 = Disabled 1 = Enabled	0	CFG, WEBA, WEBU

4 of 8

Table 1: 4602 SIP Telephone Parameters (continued)

Parameter	Value Type	Value	Default	Source(s)
HotDial	1 ASCII character	When HotDialing is enabled, the user can dial calls without first going off hook on the handset or speaker. HotDialing automatically turns the speaker on. Note that HotDialing is automatically disabled if HotLine is enabled. 0 = Disabled 1 = Enabled	0	CFG, WEBA, WEBU
HotLine	Up to 1 ASCII character	Enables or disables hotline operation. 0 = disable 1 = enable. When HotLine is active, hotdialing and speed dialing from the phone's dialpad are automatically disabled. Note: The Avaya SIP Solution does not support this feature.	0	CFG, WEBA
HotLineAddress	Up to 64 ASCII characters	Specifies the URI dialed when the set goes offhook and HotLine is enabled. Note: The Avaya SIP Solution does not support the Hotline feature.	“”	CFG, WEBA
Include	Up to 64 ASCII characters	The file name specified is read and its contents processed as another configuration file. Configuration files can have more than one Include parameter.	“”	CFG
IPAddress	Dotted Decimal ASCII	IP address to be used by the telephone.	0.0.0.0	DHCP, MAN, WEBA
IPDialing	1 ASCII character	This lets the user enter a numeric IP address to dial as a dial string. Mainly useful during debugging. 0 = IP address dialing off 1 = IP address dialing on	0	CFG, WEBA
Layer2Audio	1 ASCII character	Layer 2 audio priority values, from 0 to 7.	6	CFG, WEBA
Layer2Signaling	1 ASCII character	Layer 2 signaling priority values, from 0 to 7.	6	CFG, WEBA
Layer2Tagging	1 ASCII character	802.1Q tagging enabled on Port 1. 0 = Disable 1 = Enable	0	CFG, MAN, WEBA

5 of 8

Table 1: 4602 SIP Telephone Parameters (continued)

Parameter	Value Type	Value	Default	Source(s)
MsgButtonUrl	Up to 255 ASCII characters	When the user presses the **Messages** button, a call is initiated to this URL. If the handset is on-hook, the speaker is turned on and the call is placed. Note that if Hotline is enabled, this parameter holds the extension to dial to reach voice mail instead of a SIP URI. In this case, the digits are sent using RFC 2833. Examples: voicemail@comm.elite.com 77777	“”	CFG, WEBA
MsgWaitSubscribe	Up to 255 ASCII characters	URL of the voice mail server to subscribe to for message waiting notification. Example: voicemail@comm.elite.com	“”	CFG, WEBA
OverrideWeb	1 ASCII character	Select if configuration data in the Configuration file download overwrites data saved from the Web interface. Useful when the HTTP server is not found. 0 = No 1 = Yes	0	CFG, WEBA
ProxyPort	Up to 4 ASCII characters	Port number to contact the proxy server. If a domain is specified for proxy servers this value must be 0. If a numeric IP address is specified, for proxy servers, this value must be 5060.	5060	CFG, WEBA, MAN
ProxyServers	Up to 255 ASCII characters	Proxy server IP address or domain. 192.168.0.9 example.com	0.0.0.0	CFG, WEBA, MAN
RegisterExpires	Up to 5 ASCII characters	Number of seconds before the phone re-registers with the registration server. A value of 0 turns off automatic registration. Values of 0 to 65,000 are permitted.	360	CFG, WEBA
RegistrarServers	Up to 255 ASCII characters	Proxy server IP address or domain. For example: 192.168.0.9 example.com	0.0.0.0	CFG, WEBA, MAN

6 of 8

Table 1: 4602 SIP Telephone Parameters (continued)

Parameter	Value Type	Value	Default	Source(s)
RegistrarPort	Up to 4 ASCII characters	Port number to contact the Registrar server. If a domain is specified for Registrar servers, this value must be 0. If an IP address is specified for Registrar servers, this value must be 5060.	5060	CFG, WEBA, MAN
RegistrationDomain	Up to 255 ASCII characters	SIP Domain, for example: example.com		CFG, WEBA
RingType	Up to 2 ASCII characters	Telephone ring type. Permitted values are 1 to 16.	1	CFG, WEBA, WEBU
RtpBase	Up to 5 ASCII characters	The base port from which the phone increments upward to specify where it will receive media streams.	16384	CFG, WEBA
SipName	Up to 32 ASCII characters	SIP user name or extension used with the set’s IP address to uniquely identify the user. SipName is used to login to the Registrar, but is only used if **ForcedLogin** is disabled.	“”	CFG, WEBA, WEBU
SipProtocol	1 ASCII character	Transport protocol: 1 = UDP 2 = TCP	1	CFG, WEBA
SipPwd	Up to 16 ASCII characters	Password that is passed on to the Registar for user authorization. The value is only used if **ForcedLogin** is disabled.	“”	CFG, WEBA, WEBU
SiteOption	Up to 3 ASCII characters	Site-specific option number between 130 and 254 used by DHCP.	172	CFG, WEBA
SntpServers	Up to 255 ASCII characters	SNTP server’s IP address.	0.0.0.0	CFG, WEBA
SpeedDial	Up to 255 ASCII characters	Specifies the data assigned to a **Speed Dial** button in the format: Name, Number. The name field is restricted to 14 characters. More than one SpeedDial parameter may be specified. Examples: Bob Day, 6715 Dave R, sip:dbr@home.com	“”	CFG, WEBU

7 of 8

Table 1: 4602 SIP Telephone Parameters (continued)

Parameter	Value Type	Value	Default	Source(s)
SubNetMask	Dotted Decimal ASCII	Network Mask for the phone.	0.0.0.0	DHCP, MAN, WEBA
SysLogInfo	Up to 16 ASCII characters	IP address to which syslog output is sent.	0.0.0.0	CFG, WEBA
SysLogPort	Up to 5 ASCII characters	Port to which syslog output is sent.	514	CFG, WEBA
TimeZone	Up to 2 ASCII characters	Time Zone in hours after GMT. (Greenwich Mean Time). See Appendix C: Time Zone Determination. Local time = GMT + Time Zone, if Time Zone <=12 Local time = GMT + 25 minus Time Zone, if Time Zone is >12.	8	CFG, WEBA
VlanId	Up to 9 ASCII characters	Comma-separated pair of VLAN IDs for Ethernet Port 1. Allowed values are 0 to 4094. Example: 1234	0	CFG, WEBA, MAN

8 of 8

Appendix B: Configuring a Dial Plan

Introduction

This appendix describes how to configure the **DialPlan** parameter.

Note:

If the **HotLine** feature is enabled, you cannot configure a dial plan. The DialPlan feature is automatically disabled whenever the HotLine feature is active. Since Avaya does not support the HotLine feature, be sure you have not inadvertently enabled this parameter.

Dial Plan Setup

The 4602 SIP Telephone uses custom dial plans to assist in routing telephone calls and to minimize dialing delays experienced by users. In addition, the phone automatically attempts to dial a non-null dial sequence after a period of **DialDelay** seconds have passed.

The following table shows the syntax for dial plan entries.

Table 2: Dial Plan Syntax

To Specify	Enter	Result
Digit	**`0 1 2 3 4 5 6 7 8 9 0`**	Identifies a specific digit.
Range of Digits	**`[Digit-Digit] OR`**	Specifies a range that will match a digit.
Wildcard	**`x OR`** **`x+`**	Match any single digit that is dialed. Matches any arbitrary number of digits or range of digits including none.
Multiple Dial Plans	**`|`**	Use the | symbol to separate multiple dial plans. For example: 911|9xxxxxxx|

Example

To use 4-digit extension dialing in combination with dialing 9 to dial an outside number this dial plan would work.

Note:
Note that the plan below does not use 0xxx or 9xxx numbers as extensions.

[1-8]xxx|9xxxxxxx|911|90|91xxxxxxxxxx	
[1-8]xxx	Causes extensions 1000-8999 to be dialed immediately
9xxxxxxx	Causes 7 digit local numbers to be dialed
911	Causes 911 to be dialed immediately after it is entered
90	Causes the outside operator to be dialed immediately
91xxxxxxxxxx	Causes long distance calls to be dialed after the 10th digit is entered

Setting Up an International Dial Plan

Each customer's dialing plan needs differ, so there is no specific Avaya-recommended dial plan setup. Table 2 shows that the SIP Dial Plan allows you to specify lengths of phone numbers (useful for extensions or local calls) or arbitrary digit string lengths (useful for international numbers, which can vary in length from country to country).

When dialing International numbers, the 4602 does not know in advance how many digits a given number requires, so some indication is needed to terminate the dialing process and send out the digits.

If you set up your SIP Dial Plan to include arbitrary length International numbers with the **+** character (for example, 9011x+), instruct your users to press **#** upon completion of dialing an International number. The user's terminating # is therefore part of the arbitrary length string. If you set up your SIP Dial Plan to include only fixed-length International numbers (for example, 901144xxxxxxx to allow only calls to England), the phone dials the number automatically when the proper length is reached. In this case, a terminating # is not necessary.

Appendix C: Time Zone Determination

Introduction

This appendix describes how to determine the **TimeZone** parameter setting.

Time Zone Setting

Time zones are based on the distance from Greenwich Mean Time (GMT), which is zero. Time zones east of Greenwich, UK, go from +1 to +12. Time zones west of Greenwich, UK go from -1 to -12.

The 4602 SIP Telephone uses the **TimeZone** parameter to set the Date and Time display. The TimeZone parameter can be up to two ASCII characters. Because the phone does not accept a plus (+) or negative (-) sign, you have to use a formula to obtain a numerical time zone value to use.

Time Zone Calculation:

1. Use the Time Zone Chart to determine the time zone in which the phone is located.
2. If the time zone is -1 to -12 (i.e., West of Greenwich, UK), eliminate the minus sign and use the number as the **TimeZone** parameter value. For example, a phone site located in the Eastern United States has an actual time zone of -5. Therefore the TimeZone parameter value for that site is **5**.
3. If the time zone is +1 to +12 (i.e., East of Greenwich, UK), subtract that number from 25 and use the result as the **TimeZone** parameter value. For example, a phone site located in Japan has an actual time zone of +9. Therefore, the TimeZone parameter value for that site is 25 minus 9, or **16**.

See Table 3 for an easy to use reference to TimeZone parameter values.

Figure 2: Time Zone Chart

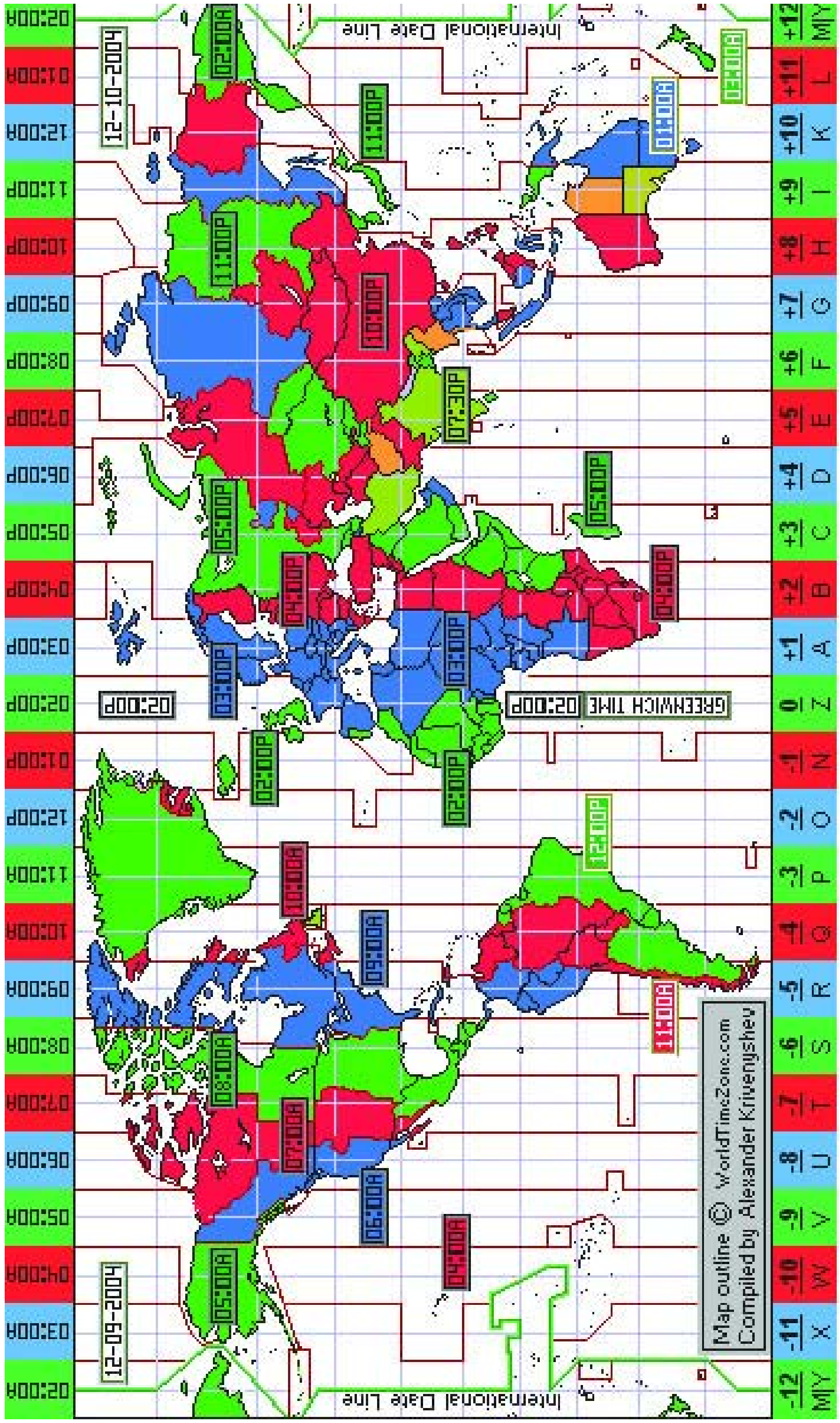

Table 3: Actual Time Zones and Corresponding Time Zone Parameter Values

If Actual Time Zone is:	Use this Parameter Value:
-1	1
-2	2
-3	3
-4	4
-5	5
-6	6
-7	7
-8	8
-9	9
-10	10
-11	11
-12	12
0	0
+1	24
+2	23
+3	22
+4	21
+5	20
+6	19
+7	18
+8	17
+9	16
+10	15
+11	14
+12	13

Index

Numerical

A

B

C

D

F

H

I

M

N

O

P

Q

R

S

T

U

W