Avaya one-X™ Deskphone Value Edition SIP for 1603SW-I IP Deskphones

Administrator Guide
Release 1.0

16-603608
Issue 1
June 2010

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

For full legal page information, please see the complete document, Avaya Legal Page for Hardware Documentation, Document number 03-600759.

To locate this document on our Web site, simply go to http://www.avaya.com/support and search for the document number in the search box.

Documentation disclaimer

Avaya Inc. 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.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

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

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Avaya support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site:

http://www.avaya.com/support

Software License

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE AT http://support.avaya.com/LicenseInfo/ ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

License Type(s):

Designated System(s) License (DS). End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Third-party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them is available on Avaya's Web site at:

http://support.avaya.com/ThirdPartyLicense/

Interference

Using a cell, mobile, or GSM telephone, or a two-way radio in close proximity to an Avaya IP Telephone might cause interference.

Security

See http://support.avaya.com/security to locate and/or report known vulnerabilities in Avaya products. See http://support.avaya.com to locate the latest software patches and upgrades. For information about secure configuration of equipment and mitigation of toll fraud threats, see the Avaya Toll Fraud and Security Handbook at http://support.avaya.com.

Contents

Chapter 1: Introduction 7

About This Guide 7

Document Organization 8

Other Documentation 9

Chapter 2: Administration Overview and Requirements 11

1600 Series IP Telephones 11

Parameter Data Precedence 14

The Administrative Process. 15

Administrative Checklist 16

Telephone Initialization Process 18

Step 1: Deskphone to Network 18

Step 2: Deskphone to LLDP-Enabled Network 18

Step 3: Deskphone to DHCP Server 18

Step 4: Deskphone and File Server. 18

Step 5: Deskphone and SIP Proxy Server 19

Error Conditions 19

Chapter 3: Network Requirements 21

Network Assessment 21

Hardware Requirements. 21

Server Requirements 22

DHCP Server 23

HTTP/HTTPS Server 23

Simple Network Time Protocol (SNTP) Server. 23

Required Network Information 23

Other Network Considerations 24

SNMP 24

Registration and Authentication 25

QoS 25

IEEE 802.1P and 802.1Q 25

SIP Station Number Portability 26

TCP/UDP Port Utilization 26

IP Address Reuse 29

Security. 30

Chapter 4: Avaya Aura Communication Manager Administration 31
Call Server Requirements 31
Supported SIP Environments 31
Switch Compatibility. 31
Communication Manager Administrative Requirements for Session Manager or SES 32
System-Level Preparation Tasks 32
SIP Trunk Administration 33
Call Routing Administration 33
IP Interface and Addresses 34
UDP Port Selection 34
RSVP and RTCP/SRTCP. 34
QoS 34
IEEE 802.1D and 802.1Q. 34
NAT 35
DIFFSERV 35
Auto Hold. 35
Call Transfer Considerations 35
Conferencing Call Considerations 36
Telephone Administration. 36
CM/SIP IP Deskphone Configuration Requirements 37
Administering Stations 42
Administering Features 42
Printing Button Labels 42

Chapter 5: Session Manager (SM) and SIP Enablement Services (SES) Administration 43
Introduction 43
Administering Avaya Session Manager 43
Administering Avaya SES. 44

Chapter 6: Server Administration 47
Software Checklist. 47
DHCP and File Servers 47
DHCP Server Administration 48
Configuring DHCP for 1603SW-I SIP IP Deskphones 48
DHCP Generic Setup 50
Windows NT 4.0 DHCP Server 54
Verifying the Installation of the DHCP Server 54

Creating a DHCP Scope for the IP Telephones 54
Editing Custom Options. 55
Adding the DHCP Option 55
Activating the Leases 56
Verifying Your Configuration 56
Windows 2000 DHCP Server 57
Verifying the Installation of the DHCP Server 57
Adding DHCP Options. 59
Activating the New Scope. 60
HTTP Generic Setup. 60

Chapter 7: Telephone Software and Binary Files 63
General Download Process. 63
Software 63
1603SW-I SIP IP Deskphone Upgrade and Binary Files. 64
Choosing the Right Binary File and Upgrade File. 64
Upgrade File (16xxupgrade.txt). 65
Settings File 65
Contents of the Settings File 67
The GROUP System Value 70

Chapter 8: Administering Telephone Options. 73
Administering Options for the 1603SW-I SIP IP Deskphones 73
VLAN Considerations. 83
VLAN Tagging 84
VLAN Detection 84
VLAN Default Value and Priority Tagging 85
VLAN Separation. 86
DNS Addressing. 88
IEEE 802.1X 88
802.1X Pass-Through and Proxy Logoff 90
802.1X Supplicant Operation 90
Link Layer Discovery Protocol (LLDP). 91
Local Administrative Options Using the Telephone Dialpad 96
Clear Procedure 96
Group Identifier 97
Reset System Values 98
Restart the Telephone. 99
Interface Control. 100

The View Administrative Option 102
Static Addressing Installation 105
Disable/Enable Event Logging 108
Logoff. 109
Self-Test Procedure 110
Language Selection 111
Setting the Dial Plan on SIP IP Telephones 113
Setting the Date and Time on SIP IP Telephones 114
Failover/Failback Behavior 114
Appendix A: Glossary of Terms 115
Appendix B: Related Documentation 117
IETF Documents 117
ITU Documents. 117
ISO/IEC, ANSI/IEEE Documents 117
Appendix C: Countries With Specific Network Progress Tones 119
Overview 119
Country List 119
Index 121

Chapter 1: Introduction

About This Guide

This guide is for personnel who administer Avaya Aura™ Communication Manager or Avaya Midsize Business Template 5.2.1, HTTP/HTTPS servers for Avaya 1603SW-I IP Deskphones using Session Initiation Protocol (SIP), a Local Area Network (LAN), Avaya Aura Session Manager, Avaya SIP Enablement Services (SES), or a Network Time server.

The 1603SW-I IP Deskphones use Internet Protocol (IP) technology with Ethernet line interfaces and support both SIP and H.323 protocol only. The 1603SW-I IP Deskphones provide support for DHCP, HTTP, and HTTPS, which enhance the administration and servicing of the deskphones. These deskphones use DHCP to obtain dynamic IP Addresses, and HTTPS or HTTP to download new versions of software or customized settings for the deskphones.

Note:

This document covers SIP administration for 1603SW-I SIP Deskphones only. For administration for 1603SW-I IP Deskphones using the H.323 protocol, see the *Avaya 1600 Series IP Deskphones Administrator Guide.*

This document does not cover installation or administration for Avaya Aura™ Session Manager. Find full documentation for Avaya Aura™ Session Manager on the Avaya support Web site, www.avaya.com/support, specifically *Installing and Upgrading Avaya Aura™ Session Manager* (Document Number 03-603473) and *Administering Avaya Aura™ Session Manager* (Document Number 03-603324).

For more information about administering Avaya Midsize Business Template Release 5.2.1 and Avaya SES R5.2.1, go to www.avaya.com/support.

⚠ **Important:**

Avaya does not provide product support for many of the products mentioned in this document. Take care to ensure that there is adequate technical support available for servers used with any 1603SW-I IP and/or SIP Deskphone system. If the servers are not functioning correctly, the 1603SW-I IP Deskphones might not operate correctly.

Document Organization

The guide contains the following sections:

Chapter 1: Introduction	Provides an overview of this document.
Chapter 2: Administration Overview and Requirements	Provides an overview of the administrative process and describes general hardware, software, and operational requirements.
Chapter 3: Network Requirements	Describes administrative requirements for your Local Area Network.
Chapter 4: Avaya Aura Communication Manager Administration	Describes how to administer Avaya Aura Communication Manager to operate with 1603SW-I SIP Deskphones.
Chapter 5: Session Manager (SM) and SIP Enablement Services (SES) Administration	Covers Avaya Session Manager configuration and Avaya SIP Enablement Services (SES) configuration for 1603SW-I SIP Deskphones.
Chapter 6: Server Administration	Describes DHCP, HTTP, and HTTPS administration for the 1603SW-I SIP Deskphones.
Chapter 7: Telephone Software and Binary Files	Describes deskphone software, covers software downloads, and provides information about the configuration file.
Chapter 8: Administering Telephone Options	Describes how to use file parameters and options to administer the 1603SW-I SIP Deskphones. Also describes how to use local procedures to customize a single telephone from the dialpad and provides detailed information about survivability, including configuration and parameter setup.
Appendix A: Glossary of Terms	Provides a glossary of terms used in this document or which can be applicable to 1603SW-I SIP Deskphones.
Appendix B: Related Documentation	Provides references to external documents that relate to telephony in general, which can provide additional information about specific aspects of the telephones.
Appendix C: Countries With Specific Network Progress Tones	Provides lists of network progress tones for each country.

Other Documentation

See the Avaya support site at http://www.avaya.com/support for 1603SW-I IP Deskphone technical and end user documentation.

See Appendix B: Related Documentation for a list of non-Avaya documents, such as those published by the Internet Engineering Task Force (IETF) and the International Telecommunication Union (ITU).

Chapter 2: Administration Overview and Requirements

1600 Series IP Telephones

The 1603SW-I IP Deskphones currently support the H.323 signaling protocol and the SIP signaling protocol.

The H.323 standard provides for real time audio, video, and data communications transmission over a packet network. An H.323 telephone protocol stack comprises several protocols:

- H.225 for registration, admission, status (RAS), and call signaling,
- H.245 for control signaling,
- Real Time Transfer Protocol (RTP), and
- Real Time Control Protocol (RTCP)

SIP was developed by the IETF. Like H.323, SIP provides for real time audio, video, and data communications transmission over a packet network. SIP uses various messages, or methods, to provide:

- Registration (REGISTER),
- Call signaling (INVITE, BYE)
- Control signaling (SUBSCRIBE, NOTIFY)

The 1603SW-I SIP Deskphones use built-in Avaya SIP Certificates for trust management.

The 1603SW-I SIP Deskphones do not support Media Encryption (SRTP).

The 1603SW-I IP Deskphones are loaded with either H.323 or SIP software as part of initial 16xxupgrade.txt file administration and initialization during installation. Post-installation, software upgrades automatically download using the proper signaling protocol.

The conditions under which the 1603SW-I SIP IP Deskphones need to operate are summarized as follows:

- Telephone Administration on the Communication Manager (CM) call server, as covered in Chapter 4: Avaya Aura Communication Manager Administration.
- Administration on Avaya Session Manager (SM), as covered in *Administering Avaya Aura™ Session Manager* (Document Number 03-603324), or administration on Avaya SES, as covered in Session Manager (SM) and SIP Enablement Services (SES) Administration.
- IP Address management for the telephone, as covered in Chapter 6: Server Administration for dynamic addressing. For static addressing, see the *Avaya one-X™ Deskphone Value Edition SIP for 1603SW-I IP Deskphones Installation and Maintenance Guide*.
- Tagging Control and VLAN administration for the telephone, if appropriate, as covered in Chapter 8: Administering Telephone Options.
- Quality of Service (QoS) administration for the telephone, if appropriate. QoS is covered in QoS on page 25 and QoS on page 34.
- Protocol administration, for example, Simple Network Management Control (SNMP) and Link Layer Discovery Protocol (LLDP).
- Interface administration for the telephone, as appropriate. Administer the telephone to LAN interface using the PHY1 parameter described in Chapter 3: Network Requirements. Administer the telephone to PC interface using the PHY2 parameter described in "Interface Control" in the *Avaya one-X™ Deskphone Value Edition SIP for 1603SW-I IP Deskphones Installation and Maintenance Guide.*
- Application-specific telephone administration, if appropriate, as described in Chapter 8: Administering Telephone Options. An example of application-specific data is specifying the extent to which users can add/edit/delete data for Contacts entries.

Table 1 indicates that you can administer system configuration parameters in a variety of ways and use the following administrative mechanisms:

- Administering the information on the call server.
- Manually entering the information by means of the telephone dialpad using local administrative (Craft) procedures. Local administrative procedures are described in "Chapter 3: Local Administrative Options" in the *Avaya one-X™ Deskphone Value Edition SIP for 1603SW-I IP Deskphones Installation and Maintenance Guide.*
- Administering the DHCP server.
- Editing the configuration file on the applicable HTTP or HTTPS file server.
- User modification of certain parameters, when given administrative permission to do so.

Note:

Not all parameters can be administered on all administrative mechanisms. See the applicable chapters in this guide for specific information.

Table 1: Administration Alternatives and Options for 1603SW-I SIP IP Deskphones

Parameter(s)	Administrative Mechanisms	For More Information See:
Telephone Administration	Avaya Communication Manager and SM/ SES	Chapter 4: Avaya Aura Communication Manager Administration, Chapter 6: Server Administration, and Appendix B: Related Documentation. For Session Manager administration, see *Administering Avaya Aura™ Session Manager* (Document Number 03-603324), available on the Avaya support site.
IP Addresses	DHCP (strongly recommended)	DHCP and File Servers on page 47, and especially DHCP Server Administration on page 48.
	Settings file	Chapter 7: Telephone Software and Binary Files and Chapter 8: Administering Telephone Options.
	Manual administration at the telephone	"Static Addressing Installation" in the *Avaya one-X™ Deskphone Value Edition SIP for 1603SW-I IP Deskphones Installation and Maintenance Guide.*
	LLDP	Link Layer Discovery Protocol (LLDP) on page 91.
Tagging and VLAN	LLDP	Link Layer Discovery Protocol (LLDP) on page 91.
	DHCP	DHCP Server Administration on page 48, and Chapter 8: Administering Telephone Options.
	Settings file	DHCP and File Servers on page 47 and Chapter 8: Administering Telephone Options.
	Manual administration at the telephone	"Static Addressing Installation" in the *Avaya one-X™ Deskphone Value Edition SIP for 1603SW-I IP Deskphones Installation and Maintenance Guide*.
Network Time Server (NTS)	DHCP Settings file	DHCP Server Administration on page 48 and Simple Network Time Protocol (SNTP) Server on page 23.
Quality of Service	Settings file	Chapter 8: Administering Telephone Options.
Interface	DHCP	DHCP and File Servers on page 47, and Chapter 7: Telephone Software and Binary Files.
	Settings file (strongly recommended)	DHCP and File Servers on page 47, and Chapter 7: Telephone Software and Binary Files.
	LLDP	Link Layer Discovery Protocol (LLDP) on page 91.
	Manual administration at the telephone	"Secondary Ethernet Interface Enable/Disable" in the *Avaya one-X™ Deskphone Value Edition SIP for 1603SW-I IP Deskphones Installation and Maintenance Guide*.
Application - specific parameters	DHCP	DHCP and File Servers on page 47, and especially DHCP Server Administration on page 48. Also, Chapter 8: Administering Telephone Options.

Table 1: Administration Alternatives and Options for 1603SW-I SIP IP Deskphones (continued)

Parameter(s)	Administrative Mechanisms	For More Information See:
	Settings file (strongly recommended)	DHCP and File Servers on page 47, and especially HTTP Generic Setup on page 60. Also, Chapter 8: Administering Telephone Options.

General information about administering DHCP servers is covered in DHCP and File Servers on page 47, and more specifically, DHCP Server Administration on page 48. General information about administering HTTP servers is covered in DHCP and File Servers, and more specifically, HTTP Generic Setup. Once you are familiar with that material, you can administer telephone options as described in Chapter 8: Administering Telephone Options.

Parameter Data Precedence

As shown in Table 1: Administration Alternatives and Options for 1603SW-I SIP IP Deskphones, you can administer a given parameter in a number of ways. The precedence, from lowest to highest, is:

1. LLDP
2. DHCP
3. Settings file

   ⚠ **Important:**
   Set failover parameters in the settings file and not in SM or SES.

4. Personal Profile Manager (PPM) through SM
5. Manual administration, unless the system parameter USE_DHCP is set to 1 (Get IP Address automatically by DHCP), or backup file data obtained through PPM.

For example, if the SIP outbound proxy server address is defined to have the precedence information so that the value retrieved from DHCP server has a lower precedence than the value retrieved from the settings file, and the value retrieved from the settings file is higher than the value retrieved from PPM, then the following determination occurs:

- If the most recent value the telephone has is from DHCP and new server address information is retrieved from the settings file, the telephone will use the new value from the settings file.
- If later on, the telephone receives a new server address value from PPM, it will not use this value because PPM’s precedence as a data source for the server address is lower than the current value (which came from the settings file).

- If the server to which a specific telephone points is changed manually using the local administrative ADDR procedure, that value now takes precedence over the previous value.

  Note:

  The only exception to this sequence is in the case of VLAN IDs. In the case of VLAN IDs, LLDP settings of VLAN IDs are the absolute authority. Then the usual sequence applies. For the L2QVLAN and L2Q system values, LLDP settings of VLAN IDs are the absolute authority only if the LLDP task receives the VLAN IDs before DHCP, and the DHCP client of the telephone is activated. If the LLDP task receives the VLAN IDs after DHCP negotiation, several criteria must be successful before the telephone accepts VLAN IDs from LLDP. For more information, see Link Layer Discovery Protocol (LLDP) on page 91.

The Administrative Process

The following list depicts administration for a typical 1603SW-I SIP IP Deskphone network. Your own configuration might differ depending on the servers and system you have in place.

1. Avaya Communication Manager 6.0 or greater or Avaya Midsize Business Template 5.2.1 administered for 1603SW-I IP Deskphones. Administer 1603SW-I SIP Deskphones aliased as the 9620SIP station type.
2. Avaya Session Manager 6.0 or greater or Avaya SES 5.2.1 administered.

   Note:

   Avaya SES 5.2.1 is supported only with Avaya Midsize Business Template 5.2.1.
3. LAN and applicable servers (file servers, Network Time server) administered to accept the telephones.
4. Telephone software downloaded from the Avaya support site.
5. 46xxsettings file updated with site-specific and SIP-specific information, as applicable.
6. 1603SW-I IP Deskphones installed. For more information, see the *Avaya one-X™ Deskphone Value Edition SIP for 1603SW-I IP Deskphones Installation and Maintenance Guide*.
7. Individual 1603SW-I IP phones updated using local administrative procedures, as applicable. For more information, see “Local Administrative Procedures” in the *Avaya one-X™ Deskphone Value Edition SIP for 1603SW-I IP Deskphones Installation and Maintenance Guide*.
8. Survivability administration to set up the local SIP gateway and administer additional controllers in the settings file as applicable.

Administrative Checklist

Use the following checklist as a guide to system and LAN administrator responsibilities. This high-level list helps ensure that all telephone system prerequisites and requirements are met prior to telephone installation.

Note:

One person might function as both the system administrator and the LAN administrator in some environments.

Table 2: Administrative Checklist

Task	Description	For More Information See:
Network Requirements Assessment	Determine that network hardware is in place and can handle telephone system requirements.	Chapter 3: Network Requirements.
Administer Avaya Communication Manager	Verify that the call server has a valid license file and is administered for Voice over IP (VoIP).	Chapter 4: Avaya Aura Communication Manager Administration.
	Verify the individual telephones are administered as desired on the CM station form(s).	Chapter 4: Avaya Aura Communication Manager Administration.
Administer the Proxy Server	Administer for Avaya Aura Session Manager (SM) or Avaya SES.	*Administering Avaya Aura™ Session Manager* (Document Number 03-603324) or *Installing, Administering, Maintaining, and Troubleshooting SIP Enablement Services* (Document Number 03-600768), available on the Avaya support Web site, http://www.avaya.com/support.
DHCP server installation	Install a DHCP application on at least one new or existing PC on the LAN.	Vendor-provided instructions.
Administer DHCP application	Add IP telephone administration to the DHCP application.	DHCP Server Administration in Chapter 6: Server Administration.
Administer Network Time Server	Set value(s) for Simple Network Time Protocol (SNTP)	Option 42 under HTTP Generic Setup.
HTTP/HTTPS server installation	Install an HTTP/HTTPS application on at least one new or existing PC on the LAN.	Vendor-provided instructions.
		1 of 2

Table 2: Administrative Checklist (continued)

Task	Description	For More Information See:
Binary file(s), 16xxupgrade.txt file, and settings file installation on HTTP/ HTTPS server	Download the files from the Avaya support site.	http://www.avaya.com/support Chapter 7: Telephone Software and Binary Files.
Modify settings file as needed	Edit the settings file as necessary for your environment, using your own tools.	Chapter 7: Telephone Software and Binary Files.
Administer telephones locally as applicable	As a Group:	The GROUP System Value on page 70 and the *Avaya one-X™ Deskphone Value Edition SIP for 1603SW-I IP Deskphones Installation and Maintenance Guide.*
	Individually:	The applicable Local Procedures in the *Avaya one-X™ Deskphone Value Edition SIP for 1603SW-I IP Deskphones Installation and Maintenance Guide.*
Installation of telephones in the network		*Avaya one-X™ Deskphone Value Edition SIP for 1603SW-I IP Deskphones Installation and Maintenance Guide*.
		2 of 2

Telephone Initialization Process

These steps offer a high-level description of the information exchanged when the telephone initializes and registers. This description assumes that all equipment is properly administered ahead of time. This description can help you understand how the 1603SW-I SIP Deskphones relate to the routers and servers in your network.

Step 1: Deskphone to Network

The deskphone is appropriately installed and powered. After a short initialization process, the deskphone identifies the LAN speed and sends a message out into the network, identifying itself and requesting further information. A router on the network receives and relays this message to the appropriate DHCP server.

Step 2: Deskphone to LLDP-Enabled Network

An LLDP-enabled network provides information to the deskphone, as described in Link Layer Discovery Protocol (LLDP) on page 91. Among other data passed to the telephone is the IP Address of the HTTP or HTTPS server.

Step 3: Deskphone to DHCP Server

The DHCP server provides information to the telephone, as described in DHCP and File Servers on page 47. Among other data passed to the telephone is the IP Address of the HTTP or HTTPS server.

Step 4: Deskphone and File Server

The 1603SW-I IP Deskphones can download upgrade files, binary files, language files, and settings files from either an HTTP or HTTPS server. The deskphone queries the file server, which transmits an upgrade file to the telephone. At a minimum, this 16xxupgrade.txt file tells the telephone which binary file the telephone must use. The binary file is the software that has the telephony functionality.

The telephone uses the 16xxupgrade.txt file to determine if it has the proper binary file. If the deskphone determines the proper binary file is missing, the deskphone requests an binary file download from the file server. The file server then downloads the file and conducts some checks to ensure that the file was downloaded properly. If the deskphone determines it already has the proper file, the deskphone proceeds as described in the next paragraph without downloading the binary file again.

The deskphone checks and loads the binary file, then uses the 16xxupgrade.txt file to look for a settings file, if appropriate. The optional settings file can contain settings you have administered for any or all of the 1603SW-I SIP IP Deskphones in your network. For more information about this download process and settings file, see Chapter 7: Telephone Software and Binary Files.

Step 5: Deskphone and SIP Proxy Server

In this step, the deskphone might prompt the user for an extension and password. The deskphone uses that information to exchange a series of messages with SM/SES, which in turn communicates with Avaya Communication Manager (CM). For a new installation and for full service, the user can enter the telephone extension and the SM/SES password. For a restart of an existing installation, this information is already stored on the deskphone. The deskphone and SM/SES, and SM/SES and CM exchange more messaging. The expected result is that the telephone is appropriately registered and call server data such as dial plan and feature button assignments are downloaded.

For more information about the installation process, see the *Avaya one-X™ Deskphone Value Edition SIP for 1603SW-I IP Deskphones Installation and Maintenance Guide*.

Error Conditions

Assuming proper administration, most of the problems reported by telephone users are likely to be LAN-based. Quality of Service, server administration, and other issues can impact user perception of IP deskphone performance.

The *Avaya one-X™ Deskphone Value Edition SIP for 1603SW-I IP Deskphones Installation and Maintenance Guide* covers possible operational problems that might be encountered after successful installation. The User Guide also contains guidance for users having problems with specific IP deskphone applications.

Chapter 3: Network Requirements

Network Assessment

Perform a network assessment to ensure that the network will have the capacity for the expected data and voice traffic, and that it can support for all applications:

- SIP,
- DHCP,
- HTTP/HTTPS, and

Also, QoS support is required to run VoIP on your configuration. For more information, see Appendix B: Related Documentation and the QoS parameters L2QAUD, L2QSIG, DSCPAUD, and DSCPSIG in Table 11: 1603SW-I SIP IP Deskphones Customizeable System Parameters.

Hardware Requirements

To operate properly, you need:

- Category 5e cables designed to the IEEE 802.3af-2003 standard, for LAN powering,
- Avaya Communication Manager 6.0 with Avaya Session Manager or Avaya Midsize Business Template 5.2.1 with Avaya SES 5.2.1,
- A cabinet with a TN799C V3 or greater circuit pack or a TN2602 IP Media Processor circuit pack. Sites with a TN2302 IP Media Processor circuit pack are strongly encouraged to install a TN2602 circuit pack to benefit from the increased capacity.

  ⚠ **Important:**

  IP telephone firmware requires TN799C V3 or greater C-LAN circuit pack(s). For more information, see the *Communication Manager Software and Firmware Compatibility Matrix* on the Avaya support Web site http://www.avaya.com/support.

  Later versions of the Communication Manager S87XX or S85XX can use Processor Ethernet in place of the C-LAN.

  Sites with H.248 gateways will use the Processor Ethernet (procr) on the S8300 in place of the C-LAN. The media processor resources are embedded on the gateway. See the gateway documentation for media processor capacity.

  To ensure that the appropriate circuit pack(s) are administered on your Communication Manager call server, see Chapter 4: Avaya Aura Communication Manager Administration.

For more information about hardware requirements in general, see the *Avaya one-X™ Deskphone Value Edition SIP for 1603SW-I IP Deskphones Installation and Maintenance Guide*.

Server Requirements

The following server types can be configured for the 1603SW-I IP Deskphones:

- DHCP server
- HTTP or HTTPS server
- SIP Proxy (controller) or Registration server
- Network Time Protocol server for SNTP
- Avaya Session Manager SIP Proxy Server (controller) or Avaya SES SIP Proxy Server to be used as a gateway for survivability

Note:

1603SW-I SIP IP Deskphones require one of the following configurations:

- Avaya Aura Session Manager (SM) to work properly with Avaya Communication Manager (CM) Release 6.0
- Avaya SES 5.2.1 to work properly with Avaya Midsize Business Template 5.2.1.

The SIP Proxy and Registration servers reside on the Session Manager or SES server. Avaya Communication Manager is considered a “feature server” behind Session Manager or SES that provides Outboard Proxy SIP (OPS) features.

While the servers listed provide different functions that relate to the 1603SW-I IP Deskphones, they are not necessarily different boxes. For example, DHCP provides network information whereas HTTP provides configuration and application file management, yet both functions can co-exist on one hardware unit. Any standards-based server is recommended.

For parameters related to Avaya Communication Manager information, see Chapter 4: Avaya Aura Communication Manager Administration. For parameters related to DHCP and file servers, see Chapter 6: Server Administration.

Important:

The deskphones obtain important information from the 16xxupgrade.txt files on the server(s) and depend on the binary file for software upgrades. If these servers are unavailable when the deskphones reset, the deskphones will not operate properly. Some features might not be available. To restore them, you need to reset the telephone(s) when the file server is available.

DHCP Server

Avaya recommends that a DHCP server and application be installed and that static addressing be avoided. Install the DHCP server and application as described in DHCP and File Servers on page 47.

HTTP/HTTPS Server

Administer the HTTP or HTTPS file server and application as described in HTTP Generic Setup on page 60.

Simple Network Time Protocol (SNTP) Server

SIP IP deskphones require SNTP server support to set the time and date, used in system log time stamps and other time/date functions. The SNTP server is typically needed by one or more servers within the enterprise. Administration of the SNTP server is beyond the scope of this document.

Required Network Information

Before you administer DHCP and HTTP/HTTPS, as applicable, complete the information in Table 3. If you have more than one router, HTTP/TLS server and subnetwork mask in your configuration, complete Table 3 for each DHCP server.

The 1603SW-I SIP IP Deskphones support specifying a list of IP Addresses for a gateway/ router and the HTTP/HTTPS server. Each list can contain up to 255 total ASCII characters, with IP Addresses separated by commas with no intervening spaces. Depending on the specific DHCP application, only 127 characters might be supported.

When specifying IP Addresses for the file server, use either dotted decimal format (“xxx.xxx.xxx.xxx”), DNS names, or FQDN. If you use DNS, the system value DOMAIN is appended to the IP Addresses you specify. If DOMAIN is null, the DNS names must be fully qualified, in accordance with IETF RFCs 1034 and 1035. For more information about DNS, see DHCP Generic Setup on page 50 and DNS Addressing on page 88.

Table 3: Required Network Information Before Installation - Per DHCP Server

1. Gateway (router) IP Address(es)
2. HTTP server IP Address(es)
3. Subnetwork mask
4. HTTP server file path (HTTPDIR)

Table 3: Required Network Information Before Installation - Per DHCP Server (continued)

5. Telephone IP Address range *From*: *To*:	
6. DNS server address(es)	If applicable.
7. HTTPS server address(es)	If applicable.

The default file server file path is the “root” directory used for all transfers by the server. All files are uploaded to or downloaded from this default directory. In configurations where the upgrade (16xxupgrade.txt) and binary files are in the default directory, do not use item 4 in Table 3.

As the LAN or System Administrator, you are also responsible for:

- Administering the DHCP server as described in Chapter 6: Server Administration.

Editing the configuration file on the applicable HTTP or HTTPS file server, as covered in 1603SW-I SIP IP Deskphone Upgrade and Binary Files.

Other Network Considerations

SNMP

The 1603SW-I SIP IP Deskphones are fully compatible with SNMPv2c and with Structure of Management Information Version 2 (SMIv2). The deskphones respond correctly to queries from entities that comply with earlier versions of SNMP, such as SNMPv1. “Fully compatible” means that the deskphones respond to queries directed either at the MIB-II or the read-only Custom MIB. Read-only means that the values therein cannot be changed externally by means of network management tools.

You can restrict which IP Addresses the telephone accepts SNMP queries from. You can also customize your community string with system values SNMPADD and SNMPSTRING, respectively. For more information, see Chapter 6: Server Administration and Table 11: 1603SW-I SIP IP Deskphones Customizeable System Parameters.

Note:

SNMP is disabled by default. Administrators must initiate SNMP by setting the SNMPADD and SNMPSTRING system values appropriately.

For more information about SNMP and MIBs, see the IETF Web site listed in Appendix B: Related Documentation. The Avaya Custom MIB for the 1603SW-I SIP IP Deskphones is available for download in *.txt format on the Avaya support Web site at http://www.avaya.com/support.

Registration and Authentication

A 1603SW-I SIP IP Deskphone requires an outboard proxy SIP (OPS) extension on Avaya Communication Manager and a login and password on the SM Server to register and authenticate it. Registration is described in the Initialization process, in Step 5: Deskphone and SIP Proxy Server on page 19. For further information, see *Maintaining and Troubleshooting Avaya Aura™ Session Manager* (03-603325), available on the Avaya support Web site, http://www.avaya.com/support and your call server administration manual.

QoS

For more information about the extent to which your network can support any or all of the QoS initiatives, see your LAN equipment documentation. See QoS on page 34 about QoS implications for the 1603SW-I SIP IP Deskphones.

IEEE 802.1P and 802.1Q

For more information about IEEE 802.1P and IEEE 802.1Q and the 1603SW-I SIP IP Deskphones, see IEEE 802.1D and 802.1Q on page 34. Three bits of the 802.1Q tag are reserved for identifying packet priority to allow any one of eight priorities to be assigned to a specific packet.

- **7:** Network management traffic
- **6:** Voice traffic with less than 10ms latency
- **5:** Voice traffic with less than 100ms latency
- **4:** “Controlled-load” traffic for critical data applications
- **3:** Traffic meriting “extra-effort” by the network for prompt delivery, for example, executive e-mail
- **2:** Reserved for future use
- **0:** The default priority for traffic meriting the “best-effort” for prompt delivery of the network.
- **1:** Background traffic such as bulk data transfers and backups

Note:

Priority 0 is a higher priority than Priority 1.

SIP Station Number Portability

The 1603SW-I SIP IP Deskphones provide station number portability. On startup or a reboot, the telephone attempts to establish communication with its home Personal Profile Manager (PPM) server.

Assume a situation where the company has multiple locations in London and New York, all sharing a corporate IP network. Users want to take their telephone functionality from their offices in London to their New York office. When users start up their telephones in the new location and enter their credentials, the local PPM server usually routes them to the local call server. With proper administration of the local PPM server, the deskphone knows to try its home PPM server, the one in London. The user can then be automatically registered with the London PPM server.

TCP/UDP Port Utilization

The 1603SW-I SIP IP Deskphones use a variety of protocols, particularly TCP (Transmission Control Protocol), UDP (User Datagram Protocol), and TLS (Transport Layer Security) to communicate with other equipment in the network. Part of this communication identifies which TCP or UDP ports each piece of equipment uses to support each protocol and each task within the protocol. For additional TCP/UDP port utilization information as it applies to Avaya Communication Manager, see UDP Port Selection on page 34.

Depending on your network, you might need to know what ports or ranges are used in the operation of 1603SW-I SIP IP Deskphones. Knowing these ports or ranges helps you administer your networking infrastructure.

Note:

In many cases, the ports used are the ones called for by IETF or other standards bodies.
Some of the explanations in Table 4 and Table 5 refer to configuration parameters or options settings. For more information about parameters and settings, see Administering Options for the 1603SW-I SIP IP Deskphones.

Table 4: Received Packets (Destination = SIP IP Telephone)

Destination Port	Source Port	Use	UDP or TCP?
The number used in the Source Port field of the DNS query sent by the deskphone	Any	Received DNS messages	UDP
The number used in the Source Port field of the packets sent by the deskphone's HTTP client	Any	Packets received by the telephone's HTTP client	TCP
The number used in the Source Port field of the TLS/ SSL packets sent by the deskphone's HTTP client	Any	TLS/SSL packets received by the deskphone's HTTP client	TCP
68	Any	Received DHCP messages	UDP
The number used in the Source Port field of the SNTP query sent by the deskphone	Any	Received SNTP messages	UDP
161	Any	Received SNMP messages	UDP
PORTAUD or the port number reserved for RTP tests	Any	Received RTP packets	UDP
If signaling is initiated by the deskphone = the number used in the Source Port field of the signaling packets sent by the deskphone If signaling is initiated by the server = System-Specific	Any	Received signaling protocol packets	UDP/TCP

Table 5: Transmitted Packets (Source = SIP IP Telephone)

Destination Port	Source Port	Use	UDP or TCP?
53	Any unused port number	Transmitted DNS messages	UDP
67	68	Transmitted DHCP messages	UDP
80 unless explicitly specified otherwise (i.e. in a URL)	Any unused port number	Packets transmitted by the telephone’s HTTP client	TCP
123	Any unused port number	Transmitted SNTP messages	UDP
The number used in the Source Port field of the SNMP query packet received by the deskphone	161	Transmitted SNMP messages	UDP
443 unless explicitly specified otherwise (i.e. in a URL)	Any unused port number	TLS/SSL packets transmitted by the deskphone’s HTTP client	TCP
514	Any unused port number	Transmitted Syslog messages	UDP
System-specific	Any unused port number	Transmitted signaling protocol packets	TCP
RTCPMONPORT	PORTAUD + 1 (if PORTAUD is even) or PORTAUD – 1 (if PORTAUD is odd)	RTCP packets transmitted to an RTCP monitor	UDP
System-specific	Any unused port number	Transmitted signaling protocol packets	UDP

IP Address Reuse

The SIP software has processing functionality to reuse IP Addresses during the DHCP process. IP Address reuse prevents infinite looping when separate VLAN servers are used for voice and data VLANs, and response is received from the DHCP server on the data VLAN, but not on the voice VLAN.

Unless otherwise indicated, the values described here during IP address reuse are internally provisioned or set by the process itself and not by manual administration.

Router(s) in Use:

if no responses are received from the router(s) indicated in the configuration parameter ROUTER (set using DHCP Option 3 or by a local administrative procedure), and if REUSE = 1, then ROUTER_IN_USE will be set to REUSE_ROUTER_IN_USE. With the exception of the ROUTER configuration parameter, the other router-related parameters are internally set system values.

VLAN Check:

During the VLAN check, if a reset is to be done and VLAN_IN_USE is not zero, VLAN_IN_USE will be added to VLANLIST if it is not already on VLANLIST.

The VLAN detection process described in VLAN Detection on page 84 is followed If tagging is off or if tagging is on and L2QVLAN is > 0, and if REUSETIME > 0, and if REUSE_IPADD is not “0.0.0.0”. If VLANTEST expires, the value of VLAN_IN_USE is added to VLANLIST if it is not already on VLANLIST.

If a DHCPOFFER is not received within REUSETIME seconds, or if a DHCPOFFER is received that contains a value of L2QVLAN that is on VLANLIST, REUSE will be set to 1, IPADD will be set to the value of REUSE_IPADD, NETMASK will be set to the value of REUSE_NETMASK, ROUTER will be set to the value of REUSE_ROUTERS, and if the value of REUSE_TAGGING is 1, 802.1Q tagging will be turned on with a VLAN ID equal to the value of L2QVLAN_INIT,

DHCP will then enter the “extended” REBINDING state, and operation will proceed as normal.

After a successful registration, the following system values are set:

REUSE_IPADD will be set to the value of IPADD,

REUSE_NETMASK will be set to the value of NETMASK,

REUSE_ROUTERS will be set to the value of ROUTER,

REUSE_ROUTER_IN_USE will be set to the value of ROUTER_IN_USE,

REUSE_TAGGING will be set to the value of TAGGING,

L2QVLAN_INIT will be set to the value of VLAN_IN_USE,

the MIB object endptVLANLIST will be set to the value of VLANLIST and then the value of VLANLIST will be set to null.

Security

For information about toll fraud, see the respective call server documents on the Avaya support Web site. The 1603SW-I SIP IP Deskphones cannot guarantee resistance to all Denial of Service attacks. However, there are checks and protections to resist such attacks while maintaining appropriate service to legitimate users.

You also have a variety of optional capabilities to restrict or remove how crucial network information is displayed or used. These capabilities are covered in more detail in Chapter 6: Server Administration and include:

- Depending on the protocol indicated by the SIP_CONTROLLER_LIST parameter, supporting signaling channel encryption while registering, and when registered, with appropriately administered Avaya Communication Manager.
- Restricting the response of the 1603SW-I SIP IP Deskphones to SNMP queries to only IP Addresses on a list you specify.
- Specifying an SNMP community string for all SNMP messages the deskphone sends.
- Restricting dialpad access to Local Administration Procedures to experienced installers and technicians and requiring password entry to access Craft procedures.
- Restricting the end user’s ability to use a telephone Options application to view network data.
- Restricting the reception of incoming calls only from configured controllers.

Chapter 4: Avaya Aura Communication Manager Administration

Call Server Requirements

Avaya Communication Manager (CM) extends advanced telephony features to SIP telephones via Outboard Proxy SIP (OPS) support. This feature set offers enhanced calling features in advance of SIP protocol definitions and telephone implementations.

Before you perform administration tasks, ensure that the proper hardware is in place, and your call server software is compatible with the 1603SW-I SIP IP Deskphones. Avaya recommends the latest CM software and the latest SIP IP deskphone firmware.

Supported SIP Environments

1603SW-I SIP IP Deskphones can be deployed in non-survivability mode in the following enterprise environments:

- Avaya Session Manager with Avaya Aura Communication Manager Release 6.0
- Avaya Midsize Business Template 5.2.1 with Avaya SES Release 5.2.1

Switch Compatibility

You must administer 1603SW-I SIP IP Deskphones as 9620SIP telephones on Avaya Communication Manager Release 6.0.

For specific administration instructions about the 1603SW-I SIP IP Deskphones, see Administering Stations on page 42.

Communication Manager Administrative Requirements for Session Manager or SES

There are several initial CM provisioning tasks that must be performed before administering SIP users. For information about CM administrative requirements with Avaya Aura Session Manager, see the Avaya Aura™ document library on the Avaya support site. For information about Avaya Midsize Business Template administrative requirements with Avaya SES, see the Avaya Midsize Business Template 5.2.1 document library on the Avaya support site.

The tasks to administer Communication Manager for SIP Enablement Services (SES) fall into three categories:

- system-level preparation,
- SIP trunk administration, and
- call routing administration

System-Level Preparation Tasks

The system-level preparation tasks include:

- Setting the SIP Trunk capacity on the System Capacity screen.
- Verifying that the IP Trunks field is set to **y** on the System-Parameters Customer-Options screen page 4.
- Verifying that the Maximum Administered SIP Trunks are set correctly on the System Parameters Customer-Options screen page 2.
- Setting the OPS SIP station capacity on the System Parameters Customer Options screen page 1.
- Setting the IP Node name for SES on the IP Node Names screen.
- Entering the IP Address and host name for the administered SES server on the IP Address Mapping screen.
- Setting the Authoritative Domain on the IP Network Region screen.
- Setting the intra- and inter-region IP-IP Direct Audio to yes on the IP Network Region screen.
- Setting the Signaling Group on the Signaling Group screen page 1.

SIP Trunk Administration

SIP trunk administration tasks include:

- Setting the SIP Intercept Treatment and Trunk-to-Trunk Transfer on the System Parameters Features screen page 1.
- Administering Trunk Groups on the Trunk Group screens (pages 1 through 4).
- Assigning public unknown numbering data on the Numbering - Public/Unknown Numbering screen.
- Assigning a SIP phone Set description on Configuration Set screen.

Call Routing Administration

Call routing administration includes:

- Administering Feature Access Codes (FACs) on the Feature Access Code screen.
- Administering the ARS Digit Analysis Table on the ARS Digit Analysis Table screen.
- Administering the Route Pattern on the Route Pattern screen.
- Adding the Route Pattern to the Numbering - Public/Unknown Numbering screen.
- Administering the Proxy Selection Route Pattern on the Locations screen.
- Allowing the system to identify the location of a caller who dials a 911 emergency call from a SIP endpoint on the IP Network Map screen.

The *Administrator Guide for Avaya Communication Manager* (Document Number 03-300509) provides detailed instructions for administering an IP telephone system on Avaya Communication Manager. See Chapter 3 “Managing Telephones,” which describes the process of adding new telephones. Also, you can locate pertinent screen illustrations and field descriptions in Chapter 19 “Screen References” of that guide. You can find this document on the Avaya support Web site.

IP Interface and Addresses

Follow these general guidelines:

- Define the IP interfaces for each C-LAN and Media processor circuit pack on the switch using the IP Interfaces screen. For more information, see *Administration for Network Connectivity for Avaya Communication Manager* (Document 555-233-504).
- On the Customer Options form, verify that the **IP Stations** field is set to “**y**” (Yes). If it is not, contact your Avaya sales representative.

UDP Port Selection

The 1603SW-I SIP IP Deskphones use an even-numbered port, selected from the range 4000 to 10000. The telephones **cannot** be administered from the Avaya Communication Manager Network Region form to support UDP port selection.

RSVP and RTCP/SRTCP

Avaya 1603SW-I SIP IP Deskphones support the RTP Control Protocol. The 1603SW-I SIP IP Deskphones do not support SRTP and RSVP (Resource ReSerVation Protocol).

QoS

The 1603SW-I SIP IP Deskphones support both IEEE 802.1D/Q and DiffServ. Other network-based QoS initiatives such as UDP port selection do not require support by the telephones. However, the initiatives contribute to improved QoS for the entire network.

IEEE 802.1D and 802.1Q

The 1603SW-I SIP IP Deskphones can simultaneously support receipt of packets using, or not using, 802.1Q parameters. To support IEEE 802.1D/Q, you can administer 1603SW-I SIP IP Deskphones by the value of the following configuration parameters:

- L2Q,
- L2QVLAN,
- L2QAUD, and
- L2QSIG.

NAT

The 1603SW-I SIP IP Deskphones do not support Network Address Translation (NAT) interworking.

DIFFSERV

Type of Service bits 0-5 (also called the Differentiated Services Code Point) are set to the binary equivalent of the decimal number represented by the value of the following configuration parameters:

- DSCPAUD for transmitted audio (RTP, RTCP, SRTP and SRTCP) packets;
- DSCPSIG for transmitted system-specific signaling packets;
- Zero for all other transmitted packets (e.g., DHCP, DNS, HTTP, SNMP, etc.).

Received DSCP information will be ignored.

Auto Hold

1603SW-I SIP IP Deskphones always provide auto hold, regardless of whether or not the Auto Hold parameter is administered on the Avaya Communication Manager IP Network System Parameters form.

Call Transfer Considerations

Unlike 1603SW-I H.323 IP Deskphones, the 1603SW-I SIP IP Deskphones transfer operation is controlled locally by the telephone and is not affected by the settings Abort Transfer, Transfer Upon Hang-up, and Toggle Swap, on page 7 of the system-parameters features screen.

Conferencing Call Considerations

Unlike 1603SW-I H.323 IP Deskphones, the 1603SW-I SIP IP Deskphones conference operation is controlled locally by the phone and is not affected by the settings Abort Conference Upon Hang-up, No Dial Tone Conferencing, Select Line Conferencing and Toggle Swap, on page 7 of the system-parameters features screen.

Telephone Administration

Table 6 summarizes the calling features available on 1603SW-I SIP IP Deskphones. Some features are supported locally at the deskphone, while others are only available with Avaya Session Manager/SES and Communication Manager with OPS.

The features shown in Table 6 can be invoked at the phone either directly or by selecting a CM-provisioned feature button. Communication Manager automatically handles many other standard calling features such as call coverage, trunk selection using Automatic Alternate Routing (AAR), or Automatic Route Selection (ARS), Class Of Service/Class Of Restriction (COS/COR), and voice messaging. Details on feature operation and administration can be found in the *Feature Description and Implementation for Avaya Communication Manager* (Document Number 555-245-205) and any of the CM administration documents available on the Avaya support site. The Avaya SIP solution configures all SIP telephones in Communication Manager as OPS.

Note:

Features activated in CM can only be deactivated via CM; features activated during failover can only be deactivated during the failover period.

Table 6: Avaya SIP Feature Support

Feature	Normal Operation with CM/SM
3-Way Conferencing	Yes
Auto Dial	Yes
Call Hold	Yes
Message Waiting Indication	Yes
Music on Hold	Yes
	1 of 2

Table 6: Avaya SIP Feature Support (continued)

Feature	Normal Operation with CM/SM
Redial	Yes
Transfer - attended	Yes
Transfer - unattended	No
	2 of 2

CM/SIP IP Deskphone Configuration Requirements

This section refers to Communication Manager (CM) administration on the Switch Administration Terminal (SAT) or by Avaya Site Administration. The system-wide CM form and the particular page that needs to be administered for each feature are provided. These features, which already exist, are not required but are recommended because they optimize the deskphone user interface. For deskphone configuration requirements for Avaya Aura™ Session Manager, see *Administering Avaya Aura Communication Manager as a Feature Server* (Document Number 03-603479) and related Avaya Aura Session Manager documents, all available on the Avaya support site.

Table 7: CM/SIP Configuration Requirements

Task/Form	Command	Field(s)	Value(s)
IP Network Region		RTCP Report Period (secs)	SIP telephones have a fixed reporting period. Note that this parameter is only displayed if "Use Default Server Parameters?" is set to "n".
IP Network Region		Authoritative Domain	Make sure that the Authoritative Domain is set to the same value as SIP Domain for Solution.
Off-PBX Telephones Station Mapping	change off-pbx-station mapping xxxx		Bridged call items on this form MUST be “none” or “orig.”
Feature - Related System Parameters (page 1)	change system-parameters features	Music/Tone on Hold	This CM setting controls the music on hold capability for all endpoints, including SIP telephones.
			1 of 5

Table 7: CM/SIP Configuration Requirements (continued)

Task/Form	Command	Field(s)	Value(s)
Feature - Related System Parameters (page 4)	change system-parameters features	Directed Call Pickup	This CM setting controls the availability of directed call pickup.
Feature - Related System Parameters (page 4)	change system-parameters features	Extended Group Call Pickup	This CM setting allows a user to answer calls that were directed to another call pickup group.
Feature - Related System Parameters (page 17)	change system-parameters features	Whisper Page Tone Given To	This CM setting controls who hears the whisper page.
Define the dial plan formats on the Dialplan Analysis Table form	change dialplan analysis	Call Type	Includes all telephone extensions and OPS Feature Name Extensions (FNEs). To define the FNEs for the OPS features listed in Table , a FAC must also be specified for the corresponding feature. In a sample configuration, telephone extensions are five digits in length and begin with 3 or 4, FNEs are five digits beginning with 7, and the access codes have various formats as indicated with the Call Type of “fac.”
Define the access codes corresponding to the OPS FNEs on the Feature Access Code form	change feature-access-codes	Various fields on pages 1-5 of the form	
After defining the FACs, define the FNEs not provisioned by CM feature buttons using the command	change off-pbx-telephone feature-name-extensions		Used to support both OPS and Extension to Cellular.
Set the appropriate service permissions to support OPS features on the Class of Service form	change cos	Varied	y (Yes) or n (No)
			2 of 5

Table 7: CM/SIP Configuration Requirements (continued)

Task/Form	Command	Field(s)	Value(s)
Enable applicable calling features on the Class of Restriction form	change cor	Varied	To use the Call Pickup feature, the Can Use Directed Call Pickup and Can Be Picked Up By Call Pickup fields must be set to "y" for the affected stations. Note that Page 3 can be used to implement a form of centralized call screening for groups of stations and trunks
Add a station for each SIP phone to be supported using the Station form (page 1)	add station ***xxxxxx*** (where ***xxxxxx*** represents the extension number)	Extension	Assign the same extension as the CM call server extension administered in Session Manager or SES See Chapter 5: Session Manager (SM) and SIP Enablement Services (SES) Administration.
		(Station) Type	Use 9620SIP.
		Port	System-populated.
		Coverage Path	For voice messaging or other hunt group, if available.
		COS and COR	Same values as administered in the previous COS & COR section(s).
		Name	The person associated with the telephone. This name should match what is entered for name in the Avaya Session Manager or Avaya SES proxy configuration.
		Message Lamp Ext	Enter the extension of the station you want to track with the message waiting lamp. (Usually the same extension initially entered on the Station form.)
			3 of 5

Table 7: CM/SIP Configuration Requirements (continued)

Task/Form	Command	Field(s)	Value(s)
Continue adding station information for the SIP phone using the Station form (page 2)	add station ***xxxxxx*** (where ***xxxxxx*** represents the extension number)	Bridged Call Alerting	Set to "y" if the extension for this SIP telephone will have a "bridged" appearance defined on another non-SIP telephone. Note that no other attributes of the bridged appearance feature apply to SIP telephones (e.g. off-hook indication, bridge-on, etc.).
		Restrict Last Appearance	By default, the last call appearance is reserved for outgoing calls from a phone. On stations with only three (3) call appearances, set the field to "n" for proper SIP conference and transfer operation. In this mode, all call appearances are available for making or receiving calls.
		AUDIX Name	Enter the name of the voice messaging system administered for this system.
		Coverage After Forwarding	This field, with a default of "s" for system, governs whether an unanswered forwarded call is given CM coverage treatment.
		Per Station CPN Send Calling Number?	If CM is configured to always send Caller ID, you can individually block certain stations by setting this field to "n". This field also needs to be set to "n" if you want to use the "Calling Number nblock" FNE.
Continue adding station button assignments for the SIP telephone using the Station form (page 4)		BUTTON ASSIGNMENTS 1. call-appr 2. call-appr etc.	Fill in the number of call appearances ("call-appr" buttons) to be supported for this telephone. Use the following guidelines to determine the correct number: To support certain transfer and conference scenarios, the minimum number of "call-appr" buttons should be 3.

4 of 5

Table 7: CM/SIP Configuration Requirements (continued)

Task/Form	Command	Field(s)	Value(s)
Stations With Off-PBX Telephone Integration form (page 1)	change off-pbx-telephone station-mapping ***xxxxxx*** where ***xxxxxx*** represents the extension number of the station being configured	Station Extension Application Dial Prefix Phone Number Trunk Selection Configuration Set	Use to map the Communication Manager extension to the same Session Manager or SES call server extension. The Application is "OPS." Enter the other appropriate field values, for example, the Trunk Selection value indicates the SIP trunk group. The Configuration Set value can reference a set that has the default settings in Communication Manager.
Stations With Off-PBX Telephone Integration form (page 2)	change off-pbx-telephone station-mapping ***xxxxxx*** where ***xxxxxx*** represents the extension number of the station being configured	Call Limit	Change the call limit to match the number of "call-appr" entries in the Add Station form.
			5 of 5

Administering Stations

This section refers to Communication Manager (CM) administration on the Switch Administration Terminal (SAT) or by Avaya Site Administration. Administer the following items on the Station form. Avaya recommends setting the features covered in this section because they optimize the user interface.

Note:

> You can use Avaya Aura™ System Manager as an alternative to the SAT to administer the features described in the section that follows, Administering Features.

Administering Features

You can administer the Autodial feature for a 1603SW-I SIP IP Deskphone.

For additional information about administering Avaya Communication Manager for 1603SW-I SIP IP Deskphones, see the following Avaya documents, available on the Avaya Support Web site:

- *Administrator Guide for Avaya Communication Manager* (Document 03-300509).
- *Feature Description and Implementation for Avaya Communication Manager* (Document 555-245-205).
- *Administering Avaya Aura™ Communication Manager as a Feature Server* (Document Number 03-603479) and related Avaya Aura Session Manager documents.

Printing Button Labels

You can download software from www.desi.com that enables you to print button labels for the 1603SW-I SIP IP Deskphones. To download this software, perform the following steps:

1. Using your web browser, go to **www.desi.com**.
2. Click **DESI downloads**.
3. Download the appropriate application.

Chapter 5: Session Manager (SM) and SIP Enablement Services (SES) Administration

Introduction

Avaya Session Manager and Avaya SES can provide most of the features and functionality to SIP telephones. This chapter provides references to Session Manager documents on administration and configuration and describes using the SES web browser to configure SES for use with 1603SW-I SIP Deskphones on Avaya Midsize Business Template 5.2.1.

Administering Avaya Session Manager

For an administrative overview of Session Manager and details for administrative requirements and procedures, see the following documents available on the Avaya support Web site www.avaya.com/support:

- *Avaya Aura™ Session Manager Overview* (Document Number 03-603323)
- *Installing and Upgrading Avaya Aura™ Session Manager* (Document Number 03-603473)
- *Administering Avaya Aura™ Session Manager* (Document Number 03-603324)
- *Maintaining and Troubleshooting Avaya Aura™ Session Manager* (Document Number 03-603325)
- *Network Case Study for Avaya Aura™ Session Manager* (Document Number 03-603478)

Administering Avaya SES

Avaya provides a Web server to simplify SES administration. Follow these steps to access the SES administration pages.

1. Set the browser URL to http://IP-address/admin, where IP-address is the IP Address of the Avaya SIP Enablement Services Edge or Edge/Home Server.
2. Log in as the administrator “admin” and when prompted, enter the password.

   The main administration screen displays after login.

Once you have administered one or more outboard proxy SIP (OPS) stations on CM, you must administer each of these stations as a SIP endpoint on SES by performing the following steps.

1. Click on **Launch Administration Web Interface**.

   The SIP Enablement Services Web interface screen displays.
2. Click **Add** under the **Users** heading on the left side menu.

   The Add User screen displays.
3. Complete all required fields, indicated by asterisks *.
4. Enter a handle in the **Primary Handle** field. The Primary Handle must be all numeric.
5. Set the **Host** field to the DNS host name of the Avaya SIP Enablement Services Home or Home/Edge server to which the telephone will register.
6. Check the **Add Media Server Extension** checkbox and click **Add**.

   The confirmation screen displays.
7. Click **Continue**.

   The Add Media Server Extension page displays.
8. In the **Extension** field, enter the same extension you entered on page 1 of the Communication Manager Station form for one of the stations you administered on CM. This step links the extension recorded in Avaya Communication Manager to the extension recorded in SES. (See *Feature Description and Implementation for Avaya Communication Manager* Document Number 555-245-205 for information about Station form entries if necessary).
9. Click **Add**.

   The CM server corresponding to the station is automatically selected and displayed on a confirmation page.
10. Click **Continue**.
11. Repeat Steps 4 - 10 for each SIP telephone.

12. When you finish configuring all applicable telephones, click **Update** on the left side menu. This link appears on the current page whenever updates are outstanding, and can be selected at any time to save the administration performed to that point.

Chapter 6: Server Administration

Software Checklist

Ensure that you own licenses to use the DHCP, HTTP, and HTTPS server software.

Note:

You can install the DHCP and HTTP server software on the same machine.

⚠ **CAUTION:**

The firmware in the 1603SW-I IP Deskphones reserves IP addresses of the form **192.168.0.24** and **192.168.1.x** for internal communications. The deskphone(s) improperly use addresses you specify if they are of that form.

DHCP and File Servers

Dynamic Host Configuration Protocol (DHCP) minimizes maintenance for a 1603SW-I SIP IP Deskphone network by removing the need to individually assign and maintain IP addresses and other parameters for each IP telephone on the network.

The DHCP server provides the following information to the 1603SW-I SIP IP Deskphones:

- IP address of the 1603SW-I SIP IP Deskphone(s)
- IP address of the HTTP or HTTPS server
- IP address of the NTP (Network Time Protocol) server (using Option 42)
- The subnet mask
- IP address of the router
- DNS Server IP address

Administer the LAN so each SIP deskphone can access a DHCP server that contains the IP addresses and subnet mask.

⚠ **Important:**

An IP deskphone cannot function without an IP address. The failure of a DHCP server at boot time leaves all the affected deskphones unusable. A user can manually assign an IP address to an IP deskphone. When the DHCP server finally returns, the deskphone never looks for a DHCP server unless the static IP data is unassigned manually. In addition, manual entry of IP data is an error-prone process.

Avaya recommends that:

- A minimum of two DHCP servers be available for reliability.
- A DHCP server be available when the IP deskphone reboots.
- A DHCP server be available at remote sites if WAN failures isolate IP deskphones from the central site DHCP server(s).

A (HTTP or HTTPS) file server, which may run on the same physical computer as Avaya Aura Communication Manager, provides the 1603SW-I SIP IP Deskphone with a 16xxupgrade.txt file and, if appropriate, new or updated binary software. See Step 4: Deskphone and File Server on page 18. In addition, you can edit the settings file (46xxupgrade.txt) to customize deskphone parameters for your specific environment. For more information, see Chapter 7: Telephone Software and Binary Files.

DHCP Server Administration

This section concentrates on the simplest case of a single LAN segment. Information provided here can be used for more complex LAN configurations.

⚠ **Important:**

Before you start, understand your current network configuration. An improper installation will cause network failures or reduce the reliability and performance of your network.

Configuring DHCP for 1603SW-I SIP IP Deskphones

1603SW-I SIP IP Deskphones allow you to specify the value of some configuration parameters using DHCP option 242. If you have 46xx phones that use option 176, you can make a copy of an existing option 176. Then, using that copy to administer DHCP option 242, you can either:

- leave any (46xx) parameters the 1603SW-I SIP IP Deskphones do not support in Option 242 to be ignored, or
- delete unused or unsupported 1603SW-I SIP IP Deskphone parameters to shorten the DHCP message length.

The following parameters for 1603SW-I SIP IP Deskphones can be set in DHCP Option 242. Most of the same parameters can be set in a 46xxsettings.txt file as well.

Table 8: Parameters Set by DHCP

Parameter	Description
HTTPDIR	Specifies the path to prepend to all configurations and data files the phone might request when starting up, i.e., the path, relative to the root of the HTTP file server, to the directory in which the telephone configuration and date files are stored. The path may contain no more than 127 characters and may contain no spaces. If an Avaya file server is used to download configuration files over HTTPS, but a different server is used to download software files via HTTP, set the path of the Avaya server in the DHCP site-specific option, and set HTTPDIR again in the 46xxsettings.txt file with the appropriate path for the second server. HTTPDIR is the path for all HTTP operations. The command is "SET HTTPDIR=<path>". In configurations where the upgrade (16xxupgrade.txt) and binary files are in the default directory on the HTTP server, do not use the HTTPDIR=<path>.
HTTPPORT	Destination port for HTTP requests (default is 80).
HTTPSRVR	IP Address(es) or DNS name(s) of HTTP file server(s) used for file download (settings file, language files, code) during startup. The files are digitally signed, so TLS is not required for security.
ICMPDU	Controls the extent to which ICMP Destination Unreachable messages are sent in response to messages sent to closed ports so as not to reveal information to potential hackers. The default is 1 (sends Destination Unreachable messages for closed ports used by traceroute).
ICMPRED	Controls whether ICMP Redirect messages are processed. The default is 0 (redirect messages are not processed).
L2Q	802.1Q tagging mode. The default is 0 (automatic).
L2QVLAN	VLAN ID of the voice VLAN. The default is 0.
LOGSRVR	Syslog server IP or DNS address.
MTU_SIZE	Maximum transmission unit size. Used to accommodate older Ethernet switches that cannot support the longer maximum frame length of tagged frames (since 802.1Q adds 4 octets to the frame).
PHY1STAT	Controls the Ethernet line interface speed. The default is 1 (auto-negotiate).
PHY2STAT	Controls the secondary Ethernet interface speed. The default is 1 (auto-negotiate).
PROCPSWD	Security string used to access local procedures. The default is 27238.
PROCSTAT	Controls whether local procedures are enabled. The default is 0 (enabled).
SIP_CONTROLLER_LIST	SIP proxy/registrar server IP or DNS address(es). (0 to 255 characters; zero or one IP Address in dotted decimal or DNS name format, separated by commas without any intervening spaces.) The default is null.
TLSDIR	Used as path name that is prepended to all file names used in HTTPS GET operations during initialization (0-127 character string).

Table 8: Parameters Set by DHCP (continued)

Parameter	Description
TLSSRVR	IP Address(es) or DNS name(s) of Avaya file server(s) used to download configuration files. **Note:** Transport Layer Security is used to authenticate the server.
VLANTEST	Number of seconds to wait for a DHCPOFFER on a non-zero VLAN. The default is 60 seconds.

DHCP Generic Setup

This section is limited to describing a generic administration that works with the 1603SW-I SIP IP Deskphones. Three DHCP software alternatives are common to Windows operating systems:

- Windows NT® 4.0 DHCP Server
- Windows 2000® DHCP Server
- Windows 2003® DHCP Server

Any other DHCP application might work. It is the responsibility of the customer to install and configure the DHCP server correctly.

DHCP server setup involves:

1. Installing the DHCP server software according to vendor instructions.
2. Configuring the DHCP server with:
   - IP Addresses available for the 1603SW-I SIP IP Deskphones.
   - The following DHCP options:
     - **Option 1 - Subnet mask**.
       As described in Table 3, item 3.
     - **Option 3 - Gateway (router) IP Address(es)**.
       As described in Table 3, item 1. If using more than one address, the total list can contain up to 127 total ASCII characters. You must separate IP Addresses with commas with no intervening spaces.
     - **Option 6 - DNS server(s) address list**.
       If using more than one address, the total list can contain up to 255 total ASCII characters. You must separate IP Addresses with commas with no intervening spaces. At least one address in Option 6 must be a valid, non zero, dotted decimal address.
     - **Option 12 - Host Name**.
       Value is **AV*ohhhhhh***, where: o has one of the following values based on the OID (first three octets) of the telephone's MAC address: "A" if the OID is 00-04-0D, "B" if the OID is 00-1B-4F, (SIP software Release 2.0+), "E" if the OID is 00-09-6E, "L" if the OID is 00-60-1D, "T" if the OID is 00-07-3B, (SIP software Release R2.0+) and "X" if the OID

is anything else, and where hhhhhh are ASCII characters for the hexadecimal representation of the last three octets of the telephone’s MAC address.

- **Option 15 - DNS Domain Name**.
  This string contains the domain name to be used when DNS names in system parameters are resolved into IP Addresses. This domain name is appended to the DNS name before the 1603SW-I SIP IP Deskphone attempts to resolve the DNS address. Option 15 is necessary if you want to use a DNS name for the HTTP server. Otherwise, you can specify a DOMAIN as part of customizing HTTP as indicated in DNS Addressing on page 88.
- **Option 42 - SNTP Server**.
  This option specifies a list of IP or DNS addresses indicating SNTP servers available to retrieve date and time via SNTP. List servers in the order of preference.The minimum length is 4, and the length must be a multiple of 4.
- **Option 51 - DHCP lease time**.
  If this option is not received, the DHCPOFFER is not be accepted. Avaya recommends a lease time of six weeks or greater. If this option has a value of FFFFFFFF hex, the IP Address lease is assumed to be infinite as per RFC 2131, Section 3.3, so that renewal and rebinding procedures are not necessary even if Options 58 and 59 are received. Expired leases cause Avaya IP Telephones to reboot. Avaya recommends providing enough leases so an IP Address for an IP telephone does not change if it is briefly taken offline.

Note:

Regarding Option 51: The DHCP standard states that when a DHCP lease expires, the device should immediately cease using its assigned IP Address. If the network has problems and the only DHCP server is centralized, the server is not accessible to the given telephone. In this case the telephone is not usable until the server can be reached. Avaya recommends that once assigned an IP Address, the telephone continues using that address after the DHCP lease expires, until a conflict with another device is detected. As Table 11: 1603SW-I SIP IP Deskphones Customizeable System Parameters indicates, the system parameter DHCPSTD allows an administrator to specify that the telephone will either: a). Comply with the DHCP standard by setting DHCPSTD to “1”, or b). Continue to use its IP Address after the DHCP lease expires by setting DHCPSTD to “0.” The latter case is the default. If the default is invoked, after the DHCP lease expires the telephone sends an ARP Request for its own IP Address every five seconds. The request continues either forever, or until the telephone receives an ARP Reply. After receiving an ARP Reply, the telephone displays an error message, sets its IP Address to 0.0.0.0, and attempts to contact the DHCP server again. Log events are generated for either case.

- **Option 52 - Overload Option, if desired**.
  If this option is received in a message, the telephone interprets the **sname** and **file** fields in accordance with IETF RFC 2132,
  Section 9.3, listed in Appendix B: Related Documentation.

Note:

Option 53 - DHCP message type.
Value is 1 (DHCPDISCOVER) or 3 (DHCPREQUEST). As of Release 2.5, if a DHCPACK is received in response to a DHCPREQUEST sent to renew the telephone's IP address lease, a log event record is generated with a Log Category of "DHCP". If a DHCPNAK is received in response to a DHCPREQUEST sent to renew the telephone's IP address lease, the telephone will immediately cease use of the IP address, a log event record will be generated, IPADD will be set to "0.0.0.0", and the telephone will enter the DHCP INIT state.

-

- **Option 55 - Parameter Request List**.
  Acceptable values are:
  1 (subnet mask),
  3 (router IP Address[es])
  6 (domain name server IP Address[es])
  7 (log server)
  15 (domain name)
  26 (Interface MTU)
  42 (NTP servers)
  SSON (site-specific option number)
- **Option 57 - Maximum DHCP message size**.
  Release 2.5+ value is 1000; prior to R2.5, value was 576.
- **Option 58 - DHCP lease renew time**.
  If not received or if this value is greater than that for Option 51, the default value of T1 (renewal timer) is used as per IETF RFC 2131, Section 4.5, listed in Appendix B: Related Documentation.
- **Option 59 - DHCP lease rebind time**.
  If not received or if this value is greater than that for Option 51, the default value of T2 (rebinding timer) is used as per RFC 2131, Section 4.5

The 1603SW-I SIP IP Deskphones do not support Regular Expression Matching, and therefore, do not use wildcards. For more information, see Administering Options for the 1603SW-I SIP IP Deskphones on page 73.

Avaya recommends that you administer DHCP servers to deliver only the options specified in this section and Table 8. Administering additional, unexpected options might have unexpected results, including causing the IP telephone to ignore the DHCP server.

Examples of good DNS administration include:

- Option 6: “***aaa.aaa.aaa.aaa***”
- Option 15: “***dnsexample.yourco.com,zzz.zzz.zzz.zzz***”
- Option 42: "***aaa.aaa.aaa.aaa***"

Depending on the DHCP application you choose, be aware that the application most likely does not immediately recycle expired DHCP leases. An expired lease might remain reserved for the original client a day or more. For example, Windows NT® DHCP reserves expired leases for about one day. This reservation period protects a lease for a short time. If the client and the DHCP server are in two different time zones, the clocks of the computers are not in sync, or the client is not on the network when the lease expires, there is time to correct the situation.

The following example shows the implication of having a reservation period: Assume two IP Addresses, therefore two possible DHCP leases. Assume three IP telephones, two of which are using the two available IP Addresses. When the lease for the first two telephones expires, the third telephone cannot get a lease until the reservation period expires. Even if the other two telephones are removed from the network, the third telephone remains without a lease until the reservation period expires.

In Table 9, the 1603SW-I SIP IP Deskphone sets the system values to the DHCPACK message field values shown.

Table 9: DHCPACK Setting of System Values

System Value	Set to
DHCP lease time	Option #51 (if received).
DHCP lease renew time	Option #58 (if received).
DHCP lease rebind time	Option #59 (if received).
DOMAIN	Option #15 (if received).
DNSSRVR	Option #6 (if received, which might be a list of IP Addresses).
HTTPSRVR	The **siaddr** field, if that field is non-zero.
IPADD	The **yiaddr** field.
LOGSRVR	Option #7 (if received).
MTU_SIZE	Option #26.
NETMASK	Option #1 (if received).
ROUTER	Option #3 (if received, which might be a list of IP Addresses).
SNTPSRVR	Option #42.

Windows NT 4.0 DHCP Server

Verifying the Installation of the DHCP Server

Use the following procedure to verify whether the DHCP server is installed.

1. Select **Start**-->**Settings**-->**Control Panel**.
2. Double-click the **Network** icon.
3. Verify that **Microsoft DHCP Server** is listed as one of the Network Services on the **Services** tab.
4. If it is listed, continue with the next section. If it is not listed, install the DHCP server.

Creating a DHCP Scope for the IP Telephones

Use the following procedure to create a DHCP scope for the IP deskphones.

1. Select **Start**-->**Programs**-->**Admin Tools**-->**DHCP Manager**.
2. Expand **Local Machine** in the DHCP Servers window by double clicking it until the **+** sign changes to a **-** sign.
3. Select **Scope**-->**Create**.
4. Using information recorded in Table 3: Required Network Information Before Installation - Per DHCP Server:

   Define the **Telephone IP Address Range**.

   Set the **Subnet Mask**.

   To ***exclude*** any IP Addresses you do not want assigned to IP telephones within the **Start** and **End** addresses range:

   a. In the **Exclusion Range Start Address** field, enter the ***first IP Address*** in the range that you want to exclude.

   b. In the **Exclusion Range End Address** field, enter the ***last IP Address*** in the range that you want to exclude.

   c. Click the **Add** button.

   d. Repeat steps a. through c. for each IP Address range to be excluded.

   Note:

   > Avaya recommends that you provision the 1603SW-I SIP IP Deskphones with sequential IP Addresses. Also do not mix 1603SW-I SIP IP Deskphones and PCs in the same scope.

5. Under **Lease Duration**, select the **Limited To** option and set the ***lease duration*** to the maximum.

6. Enter a ***sensible name*** for the **Name** field, such as “CM IP Telephones," where CM would represent Avaya Communication Manager.
7. Click **OK**.

   A dialog box prompts you: `Activate the new scope now?`
8. Click **No**.

   Note:

   Activate the scope only after setting all options.

Editing Custom Options

Use the following procedure to edit custom options.

1. Highlight the newly created scope.
2. Select **DHCP Options**-->**Defaults** in the menu.
3. Click the **New** button.
4. In the **Add Option Type** dialog box, enter an appropriate custom option name, for example, “16xxOPTION.”
5. Change the **Data Type Byte** value to **String**.
6. Enter **242** in the **Identifier** field.
7. Click the **OK** button.

   The **DHCP Options** menu displays.
8. Select the **Option Name** for 242 and set the *value string*.
9. Click the **OK** button.
10. For the **Option Name** field, select **003 Router** from the drop-down list.
11. Click **Edit Array**.
12. Enter the ***Gateway IP Address*** recorded in Table 3: Required Network Information Before Installation - Per DHCP Server for the **New IP Address** field.
13. Select **Add** and then **OK**.

Adding the DHCP Option

Use the following procedure to add the DHCP option.

1. Highlight the scope you just created.
2. Select **Scope** under **DHCP Options**.
3. Select the **242** option that you created from the **Unused Options** list.
4. Click the **Add** button.

5. Select option **003** from the **Unused Options** list.
6. Click the **Add** button.
7. Click the **OK** button.
8. Select the **Global parameter** under **DHCP Options**.
9. Select the **242** option that you created from the **Unused Options** list.
10. Click the **Add** button.
11. Click the **OK** button.

Activating the Leases

Use the following procedure to activate the leases.

- Click **Activate** under the **Scope** menu.

  The light-bulb icon for the scope lights.

Verifying Your Configuration

This section describes how to verify that the **16XXOPTIONs** are correctly configured for the Windows NT® 4.0 DHCP server.

Verify the Default Option, 242 16XXOPTION

1. Select **Start**-->**Programs**-->**Admin Tools**-->**DHCP Manager**.
2. Expand **Local Machine** in the DHCP servers window by double clicking until the **+** sign changes to a **-** sign.
3. In the DHCP servers frame, click the *scope* for the IP telephone.
4. Select **Defaults** from the **DHCP_Options** menu.
5. In the **Option Name** pull-down list, select **242 16XXOPTION**.
6. Verify that the **Value String** box contains the correct string from DHCP Server Administration.

   If not, update the string and click the **OK** button twice.

Verify the Scope Option, 242 16XXOPTION

1. Select **Scope** under **DHCP OPTIONS**.
2. In the **Active Options:** scroll list, click **242 16XXOPTION**.
3. Click the **Value** button.

4. Verify that the **Value String** box contains the correct string from DHCP Generic Setup on page 50.

   If not, update the string and click the **OK** button.

Verify the Global Option, 242 16XXOPTION

1. Select **Global** under **DHCP OPTIONS**.
2. In the **Active Options:** scroll list, click **242 16XXOPTION**.
3. Click the **Value** button.
4. Verify that the **Value String** box contains the correct value from DHCP Generic Setup on page 50. If not, update the string and click the **OK** button.

Windows 2000 DHCP Server

Verifying the Installation of the DHCP Server

Use the following procedure to verify whether the DHCP server is installed.

1. Select **Start**-->**Program**-->**Administrative Tools**-->**Computer Management**.
2. Under **Services and Applications** in the Computer Management tree, find **DHCP**.
3. If DHCP is not installed, install the DHCP server. Otherwise, proceed directly to Creating and Configuring a DHCP Scope for instructions on server configuration.

Creating and Configuring a DHCP Scope

Use the following procedure to create and configure a DHCP scope.

1. Select **Start**-->**Programs**-->**Administrative Tools**-->**DHCP**.
2. In the console tree, click the *DHCP server* to which you want to add the DHCP scope for the IP telephones. This is usually the name of your DHCP server machine.
3. Select **Action**-->**New Scope** from the menu.

   Windows displays the **New Scope Wizard** to guide you through rest of the setup.
4. Click the **Next** button.

   The **Scope Name** dialog box displays.
5. In the **Name** field, enter a name for the scope such as “CM IP Telephones” (where CM would represent Avaya Communication Manager), then enter a brief comment in the **Description** field.
6. When you finish Steps 1 - 5, click the **Next** button.

   The **IP Address Range** dialog box displays.
7. Define the range of IP Addresses used by the IP telephones listed in Table 3: Required Network Information Before Installation - Per DHCP Server. The **Start IP Address** is the first IP Address available to the IP telephones. The **End IP Address** is the last IP Address available to the IP telephones.

Note:

Avaya recommends not mixing 1603SW-I SIP IP Deskphones and PCs in the same scope.

8. Define the **subnet mask** in one of two ways:
   - The number of bits of an IP Address to use for the network/subnet IDs.
   - The subnet mask IP Address.

   Enter only one of these values. When you finish, click the **Next** button.

   The **Add Exclusions** dialog box displays.

9. Exclude any IP Addresses in the range specified in the previous step that you do not want assigned to an IP telephone.
   a. In the **Start Address** field under **Exclusion Range**, enter the ***first IP Address*** in the range you want to exclude.
   b. In the **End Address** field under **Exclusion Range**, enter the ***last IP Address*** in the range you want to exclude.
   c. Click the **Add** button.
   d. Repeat steps a through c for each IP Address range that you want to exclude.

   Note:

   You can add additional exclusion ranges later by right clicking the **Address Pool** under the newly created scope and selecting the **New Exclusion Range** option.

   Click the **Next** button after you enter all the exclusions.

   The **Lease Duration** dialog box displays.

10. For all telephones that obtain their IP Addresses from the server, enter **30 days** in the **Lease Duration** field. This is the duration after which the IP Address for the device expires and which the device needs to renew.
11. Click the **Next** button.

    The **Configure DHCP Options** dialog box displays.

12. Click the **No, I will activate this scope later** button.

    The **Router** (Default Gateway) dialog box displays.

13. For each router or default gateway, enter the ***IP Address*** and click the **Add** button.

    When you are done, click the **Next** button.

    The **Completing the New Scope Wizard** dialog box displays.

14. Click the **Finish** button.

    The new scope appears under your server in the DHCP tree. The scope is not yet active and does not assign IP Addresses.

15. Highlight the newly created scope and select **Action**-->**Properties** from the menu.

16. Under **Lease duration for DHCP clients**, select **Unlimited** and then click the **OK** button.

> ⚠ **CAUTION:**
>
> IP Address leases are kept active for varying periods of time. To avoid having calls terminated suddenly, make the lease duration unlimited.

Adding DHCP Options

Use the following procedure to add DHCP options to the scope you created in the previous procedure.

1. On the DHCP window, right-click the **Scope Options** folder under the scope you created in the last procedure.

   A drop-down menu displays.

2. In the left pane of the DHCP window, right click the **DHCP Server name**, then click **Set Predefined Options...**.
3. Under **Predefined Options and Values**, click **Add**.
4. In the **Option Type Name** field, enter ***any appropriate name***, for example, “Avaya IP Telephones.”
5. Change the **Data Type** to **String**.
6. In the **Code** field, enter **242**, then click the **OK** button twice.

   The **Predefined Options and Values** dialog box closes, leaving the DHCP dialog box enabled.

7. Expand the newly created scope to reveal its **Scope Options**.
8. Click **Scope Options** and select **Action-->Configure Options** from the menu.
9. In the **General** tab page, under the **Available Options**, check the **Option 242** checkbox.
10. In the **Data Entry** box, enter the ***DHCP IP telephone option string*** as described in DHCP Generic Setup on page 50.

    Note:

    You can enter the text string directly on the right side of the **Data Entry** box under the ASCII label.

11. From the list in **Available Options**, check option **003 Router**.
12. Enter the ***gateway (router) IP Address*** from the IP Address field of Table 3: Required Network Information Before Installation - Per DHCP Server.
13. Click the **Add** button.
14. Click the **OK** button.

Activating the New Scope

Use the following procedure to activate the new scope.

1. In the DHCP console tree, click the **IP Telephone Scope** you just created.
2. From the **Action** menu, select **Activate**.

   The small red down arrow over the scope icon disappears, indicating that the scope was activated.

HTTP Generic Setup

You can store the binary file, 16xxupgrade.txt file, and settings file on an HTTP server. With proper administration, the telephone seeks out and uses that material. Some functionality might be lost by a reset if the HTTP server is unavailable. For more information, see DHCP and File Servers on page 47.

Note:

If you used TFTP to provide the binary, upgrade, and settings files to older Avaya IP telephones, note that 1603SW-I IP Deskphones do not support TFTP; you must use HTTP or HTTPS instead.

⚠ **Important:**

The files defined by HTTP server configuration must be accessible from all IP telephones that might request those files. Ensure that the file names match the names in the upgrade script, including case, since UNIX systems are case-sensitive.

Note:

Use any HTTP application you want. Commonly used HTTP applications include Apache® and Microsoft® IIS™.

⚠ **Important:**

To set up an HTTP server:

- Install the HTTP server application.
- Administer the system parameter HTTPSRVR to the address of the HTTP server. Include this parameter in DHCP Option 242 or the appropriate SSON Option.

- Download the 16xxupgrade.txt file and binary file(s) from the Avaya Web site http://www.avaya.com/support to the HTTP server. For more information, see Chapter 7: Telephone Software and Binary Files.

Note:

Many LINUX servers distinguish between upper and lower case names. Ensure that you specify the settings file name accurately, as well as the names and values of the data within the file.

If you choose to enhance the security of your HTTP environment by using Transport Layer Security (TLS), you also need to:

- Install the TLS server application.
- Administer the system parameter TLSSRVR to the address(es) of the Avaya HTTP server.

Note:

The HTTPS server's certificate must be an Avaya-signed certificate.

Chapter 7: Telephone Software and Binary Files

General Download Process

The 1603SW-I SIP IP Deskphones download upgrade files, settings files, language files, and software files from a file server. All of the file types can be downloaded either via HTTP or HTTPS except the software files, which can only be downloaded via HTTP. Avaya recommends HTTPS for downloading the file types because it ensures the integrity of the downloaded file by preventing "man in the middle" attacks. HTTPS is not used for software file downloads because 1603SW-I IP Deskphone software files are already digitally signed, so there is no need to incur additional processing overhead while downloading these relatively large files. The HTTPS protocol applies only if the server supports Transport Layer Security (TLS) encryption.

Note:

The 16xxupgrade.txt file, binary files, and settings files discussed in this chapter are identical for file servers running HTTP and HTTPS. The generic term “file server” refers to a server running either HTTP or HTTPS.

When shipped from the factory, 1603SW-I IP Deskphones might not contain the latest software. When the telephone is first plugged in, it will attempt to contact a file server, and will download new software if the software version available on the file server is different than the version on the phone. For subsequent software upgrades, the call server provides the capability to remotely reset the telephone, which then initiates the same process for contacting a file server.

The telephone queries the file server, which transmits a 16xxupgrade.txt file to the deskphone. The 16xxupgrade.txt file tells the telephone which binary file the deskphone must use. The binary file is the software that has the telephony functionality, and is easily updated for future enhancements. In a newly installed deskphone, the binary file might be missing. In a previously installed deskphone, the binary file might not be the proper one. In both cases, the deskphone requests a download of the proper binary file from the file server. The deskphone downloads the file and conducts some checks to ensure that the file was downloaded properly. If the deskphone determines it already has the proper file, the deskphone proceeds to the next step without downloading the binary file again.

After checking and loading the binary file, the 1603SW-I SIP IP Deskphone, if appropriate, uses the 16xxupgrade.txt file to look for a settings file. The settings file contains options you have administered for any or all of the IP telephones in your network. For more information about the settings file, see Contents of the Settings File on page 67.

Software

As part of installation, a conversion from H.323 to SIP signaling protocol is done as described in "Converting Software on 1603SW-I IP Deskphones" of the *Avaya one-X™ Deskphone Value*

Edition SIP for 1603SW-I IP Deskphones Installation and Maintenance Guide. When the deskphone is first plugged in, a software download from an HTTP or HTTPS server starts to give the phone its proper functionality.

For software upgrades, Session Manager and SES provide the capability for a remote reboot of the 1603SW-I SIP IP Deskphones. As a result of a message from SM, the deskphone automatically starts reboot procedures. If new software is available on the file server, the deskphone downloads it as part of the reboot process. The *Avaya one-X™ Deskphone Value Edition SIP for 1603SW-I IP Deskphones Installation and Maintenance Guide* covers upgrades of a previously installed deskphone and related information.

1603SW-I SIP IP Deskphone Upgrade and Binary Files

Choosing the Right Binary File and Upgrade File

Every software release contains the files needed to operate the 1603SW-I IP Deskphones. Two software download "bundles" of files are available for use with 1603SW-I IP Deskphones. Which bundle you select depends on whether your telephone environment is primarily SIP-centric or H.323-centric. When all or the majority of your IP telephones are SIP-based, select the software download bundle for "1603SW-I SIP Telephones" from the Avaya Support Web site. The SIP bundle contains a unique version of the 16xxupgrade.txt file that assumes SIP is the default protocol for your 1603SW-I IP Deskphones and that H.323 is the exception. For more information on SIP-centric environments, see "Converting Software on 1603SW-I IP Deskphones" in the *Avaya one-X™ Deskphone Value Edition SIP for 1603SW-I IP Deskphones Installation and Maintenance Guide*.

Each SIP software bundle contains:

- An upgrade file, **16xxupgrade.txt**, which allows you to upgrade to the new software release. The 16xxupgrade.txt file tells the telephone whether a software upgrade is needed. All Avaya IP deskphones attempt to read this file whenever they reset. The upgrade file also causes the telephone to download the 46xxsettings.txt file.
- A second upgrade file, **Alternate_16xxupgrade.txt**, which allows you to use both SIP and H.323 IP telephones in the same environment. You only need this file if you also want some of your 1603SW-I IP Deskphones to run H.323 software. If so, use an ASCII text editor to read the directions in the file and to add the file names of the H.323 software files that you want to use. This file must then be saved as "16xxupgrade.txt" and will overwrite the 16xxupgrade.txt file originally provided in the bundle.
- Binary files with the latest SIP binary code for all current 1603SW-I SIP IP Deskphones.
- Language files that can be downloaded to the telephones containing the language name (as it should be presented to a user for selection), an indication of the preferred character

input method, text string replacements for the built-in English text strings, where each replacement string may contain up to 120 characters, and each has a unique index that associates it with the corresponding built-in English string, an indication as to whether Chinese, Japanese or Korean glyphs should be displayed for the Unicode “Unified Han” character codes, and a Language Identification Tag for the language of the text contained in the file. A downloadable language file may also contain a translation of the language name into any or all of the languages for which a language file is included in the software distribution package.

- Extended Korean ring tones xml files.
- Other useful information such as a ReadMe file.

Each software bundle comes in one or more formats. Download the appropriate software bundle to your file server from the Avaya support Web site at: http://www.avaya.com/support. Note that all files must reside in the same directory on your file server.

Upgrade File (16xxupgrade.txt)

The **16xxupgrade.txt** file tells the IP deskphone whether the deskphone needs to upgrade its software. The 1603SW-I SIP IP Deskphones attempt to read this file on the file server whenever they reset. This file allows the telephone to use default settings for customer-definable options. The 16xxupgrade.txt file also points to the Settings File, where you can set provide values to override the default values for any settings you want to customize for your specific environment.

The 16xxupgrade.txt file is part of the software bundle you download from http://www.avaya.com/support.

An "alternate" upgrade file (Alternate_16xxupgrade.txt) is included in the SIP software bundle, designed for environments that will support both the H323 and SIP modes of operation. For such environments, the file needs to be edited in those sections having headings of “H.323 EDIT INSTRUCTIONS.” Specific instructions are provided in the Readme file that accompanies the software bundle. Once these changes are made, the alternate file should be renamed to “16xxupgrade.txt” and placed in the HTTP download directory. The HTTP download directory holds the telephone backup and application software binaries the telephone will download. Renaming the alternate file causes any “16xxupgrade.txt” files residing in that directory to be overwritten.

Settings File

The settings file contains the parameters that you can use to customize the Avaya IP Deskphones for your enterprise.

Note:

Avaya recommends that the settings file have the extension ***.txt**. The Avaya IP Deskphones can use Avaya-provided default values and operate without this file if you have no settings you want to customize. Note that you can also change these settings with DHCP (for information see Configuring DHCP for 1603SW-I SIP IP Deskphones) or, in some cases, from the dialpad of the telephone using local administrative (Craft) procedures described in the *Avaya one-X™ Deskphone Value Edition SIP for 1603SW-I IP Deskphones Installation and Maintenance Guide*.

Note:

Use one settings file for all your Avaya IP Deskphones. The settings file includes the 1603SW-I SIP IP Deskphones covered in this document. The settings file also includes parameters for 9600 Series (H.323) IP Telephones, 4600 Series IP Telephones, and 1600 Series IP Telephones as covered in their respective administrator guides.

The settings file can include five types of statements, one per line. Any invalid statement is ignored. The statement types are:

- SET statements of the form **SET *parameter_name value***. If the desired value contains a blank or a comma, the entire value must by placed within double quotes.
- GET statements of the form **GET *filename***, which cause the phone to get the named file from the same file server and directory from which it got the current file. If the file is not available, the phone continues to execute the current file.
- GOTO statements, of the form **GOTO *tag***. GOTO statements cause the telephone to continue interpreting the configuration file after a line that begins with a “**# tag**” statement. If no such line exists in the upgrade or settings file after the GOTO, the phone ignores anything in the file after the GOTO.
- Tags are lines that begin with a # tag; tag is an unquoted string and cannot contain a space or comma.
- IF statements, of the form **IF $*name SEQ string* GOTO *tag***, where name is one of the system parameters shown in table #A#. Conditionals cause the GOTO command to be processed if the (string equivalent) value of name is equal to string. Note that the string comparison ignores case, so “Abc” matches “ABC” or “abc”. If no such name exists, the entire conditional is ignored. As for SET statements, the string must be included in double quotes if it includes spaces or commas. Any string may be double quotes, so 1 and “1” are equivalent as are “abc” and abc.

Any line which does not match one of the previous statement types is ignored and, therefore, can be treated as a comment. By convention, in the upgrade and settings files distributed by Avaya, any line intended to be ignored by the phone or read as a comment starts with “##”.

Table 10: Settings File System Parameters That Can Be Tested in an IF Statement

Parameter	Description
BOOTNAME	The name of the boot code file in the telephone.
MACADDR	MAC address of the phone (hh:hh:hh:hh:hh:hh; automatically supplied by a phone).
MODEL	Telephone Model identifier (8 ASCII characters; automatically supplied by a phone).
MODEL4	The first four digits of the model identifier (automatically supplied by a phone).
PWBCC	Avaya identification number for the printed circuit board (automatically supplied by a phone).
GROUP	Group identifier (must be manually set on a phone)
SIG	Signalling protocol identifier (2=SIP, 1=H.323, 0=default; must be manually changed on a phone).

The ***16xxupgrade.txt*** files distributed by Avaya start with a ***GOTO GETSET*** command based on the value of the SIG parameter to preclude loading SIP software into a phone that has been manually designated to run H.323 software (indicated by a SIG value of 1), and to preclude loading H.323 software into a phone that has been manually designated to run SIP software (indicated by a SIG value of 2). The default SIG value of zero indicates that the telephone should download whatever software is available.

The ***16xxupgrade.txt*** files distributed by Avaya end with the statement ***GET 46xxsettings.txt.*** If you need to redefine the values of any parameters for your installation, do so in the ***46xxsettings.txt*** file and not in the ***16xxupgrade.txt*** file. The reason for using the 46xxsettings.txt file is because each new Avaya release you download will include a new version of ***16xxupgrade.txt***, which will overwrite any changes you have made to your previous copy of that file.

Avaya recommends that you do **not** alter the 16xxupgrade.txt file. If Avaya changes the 16xxupgrade.txt file in the future, any changes you have made will be lost. Avaya recommends that you use the ***46xxsettings*** file to customize your settings instead. However, you can change the settings file name, if desired, as long as you also edit the corresponding **GET** command in the 16xxupgrade.txt file.

For more information on customizing your settings file, see Contents of the Settings File.

Contents of the Settings File

The final step in processing the 16xxupgrade.txt file is to GET the 46xxsettings.txt file. The default 46xxsettings.txt file contains explanatory material and default values on lines that start with ##. A parameter value can be changed and actioned by changing its value and removing the two ##'s at the beginning of the line.

The following are example settings only. Your settings will vary from the settings shown. This sample assumes specification of a DNS Server, identifying SIP-specific settings, and setting the time/date.

```
##
##
## Define the Domain Name Server to be "dns.example.yourco.com"
## Note that quotes are only needed for parameters that contain
  spaces.
##
SET DNSSRVER dnsexample.yourco.com
##
##
## SIP Proxy/Registrar servers list
##  SIP_CONTROLLER_LIST provides ability to configure SIP Proxy/
  Registrar list.
##  The format is host[:port];[transport:xxx]. A comma seperated
  list in this
##  format can be provided. Host can be DNS name or IP address. Port
  is optional.
##  If port is not specified then default value of 5060 for TCP and
  UDP and 5061 for
##  TLS will be used. Transport type is optional. It can be tcp or
  udp or tls.
##  Default value of tls will be used if it is not provided.
SET SIP_CONTROLLER_LIST proxy1,proxy2:5070;transport=udp
##
##
##  SIPDOMAIN sets the domain name to be used during
##  registration.  The default is null ("") but valid values
##  are 0 to 255 ASCII characters with no spaces.
SET SIPDOMAIN   example.com
##
##
##  SNTPSRVR sets the IP address or Fully-Qualified
##  Domain Name (FQDN) of the SNTP server(s) to be used.
##  The default is null ("") but valid values are zero or
##  more IP addresses in dotted-decimal or DNS format,
##  separated by commas without intervening spaces, to a
##  maximum of 255 ASCII characters.
##  You may also want to use the ntp pool of servers.
##  See http://www.pool.ntp.org/use.html
##
SET SNTPSRVR  192.168.0.5
##
##
##  GMTOFFSET sets the time zone the phone should use. The
##  default is -5:00; see the 1603SW-I SIP Telephone LAN
##  Admin Guide for format and setting alternatives.
SET GMTOFFSET "-6:00"
##
##
##  DSTOFFSET sets the daylight savings time adjustment
##  value. The default is 1 but valid values are 0, 1, or 2.
## SET DSTOFFSET "1"
##
##
##  DSTSTART sets the beginning day for daylight savings
##  time. See the 1603SW-I
##  SIP Telephone LAN Admin Guide for format and setting
##  alternatives.
## SET DSTSTART  "2SunMar2L"
##
##  NOTE:
##  The default DSTSTART and DSTSTOP parameters reflect the
##  new 2007 Daylight Savings Time values for North America
##
##  DSTSTOP sets the ending day for daylight savings time.
##   See 1603SW-I SIP IP Deskphones Customizeable System Parameters
  for format and setting alternatives.

## SET DSTSTOP   "1SunNov2L"

##

------------------------------
```

See Chapter 8: Administering Telephone Options for details about specific values. You need only specify settings that vary from defaults, although specifying defaults is harmless.

VLAN separation controls whether or not traffic received on the secondary Ethernet interface is forwarded on the voice VLAN and whether network traffic received on the data VLAN is forwarded to the telephone. Add commands to the 46xxsettings.txt file to enable VLAN separation. The following three lines will enable VLAN separation when the data VLAN ID is "yyy" and the data traffic priority is "z":

- Enable VLAN separation by setting the parameter to 1: `SET VLANSEP "1"`
- Define the data VLAN ID (for any computer connected to the second ethernet port on the phone) to be 'yyy': `SET PHY2VLAN "yyy"`
- Define the priority of the data traffic to be 'z': `SET PHY2PRIO "z"`

Note:

When the configuration parameter VLANSEP is set to "1" you should configure the network switch so that 802.1Q tags are not removed from frames forwarded to the telephone.

The GROUP System Value

You might have different communities of users, all of which have the same telephone model, but which require different administered settings. For example, you might want to group users by time zones or work activities.

Use the GROUP system value for this purpose:

1. identify which telephones are associated with which group, and designate a number for each group. The number can be any integer from 0 to 999, with 0 as the default, meaning your largest group is assigned as Group 0.
2. At each non-default telephone, instruct the installer or user to invoke the GROUP Craft Local procedure as specified in the *Avaya one-X™ Deskphone Value Edition SIP for 1603SW-I IP Deskphones Installation and Maintenance Guide* and specify which GROUP number to use. The GROUP System value can only be set on a phone-by-phone basis.

3. Once the GROUP assignments are in place, edit the configuration file to allow each telephone of the appropriate group to download its proper settings.

Here is an example of a settings file with telephones in three different groups - group "0" (the default), group "1", and group "2":

```
## First check if this phone is in group 1. If it is, jump to the
  tag GROUP1

##

IF $GROUP SEQ 1 goto GROUP1

##

## Now check if this phone is in group 2. If it is, jump to the tag
  GROUP2
  IF $GROUP SEQ 2 goto GROUP2

##

## The phone is not in either GROUP 1 or 2 so it is in GROUP 0
  {specify settings unique to Group 0}
  goto END

# GROUP1

## GROUP 1-only settings go here
  {specify settings unique to Group 1}
  goto END

# GROUP2

## GROUP 2-only settings go here
  {specify settings unique to Group 2}
  # END

## The settings here apply to all three groups
  {specify settings common to all Groups}
```

Chapter 8:   Administering Telephone Options

Administering Options for the 1603SW-I SIP IP Deskphones

This chapter explains how to change parameters to customize them for your operating environment. In all cases, you are setting a system parameter in the telephone to a desired value. Table 11 lists:

- the parameter names,
- their default values,
- the valid ranges for those values, and
- a description of each one.

Figure 8 is a comprehensive list of all the parameters you can configure. However, you do not have to set every parameter. In most cases, you will include only those parameters in the settings file that are specific to your own environment and let the deskphones use the default values for the remaining ones.

Note:

At a minimum, be sure to set these important SIP-related parameters: SIP_CONTROLLER_LIST, SIPDOMAIN, SNTPSRVR, GMTOFFSET, DSTOFFSET, DSTSTART, and DSTSTOP.

For DHCP, the DHCP Option sets certain parameters to the desired values as discussed in DHCP and File Servers on page 47. For HTTP, the parameters in Table 11 are set to desired values in the script (46xxsettings) file. For more information on working with the settings files, see Contents of the Settings File on page 67.

Avaya recommends that you administer options on the 1603SW-I SIP IP Deskphones using script files. This is because some DHCP applications have limits on the amount of user-specified information. The administration required can exceed those limits for the more full-featured deskphone models.

Some parameters can be changed using the deskphone dialpad. For example, you might choose to completely disable the capability to enter or change option settings from the dialpad using local administrative (Craft) procedures. You can set the system value, PROCPSWD, as part of standard DHCP/HTTP administration. If PROCPSWD is non-null and consists of 1 to 7 digits, a user cannot invoke any local options without first pressing **Mute** and entering the PROCPSWD value. For more information on dialpad options, see the *Avaya one-X™ Deskphone Value Edition SIP for 1603SW-I IP Deskphones Installation and Maintenance Guide*.

⚠ **CAUTION:**

PROCPSWD is likely stored on the server “in the clear” and is sent to the telephone in the clear. Therefore, do not consider PROCPSWD as a high-security technique to inhibit a sophisticated user from obtaining access to local procedures.

Administering this password can limit access to all local procedures, including V I E W. VIEW is a read-only option that allows review of the current telephone settings.

Note:

There are several ways to change configuration parameters, for example, using DHCP options, the 46xxsettings file, or using local administrative (manual) procedures, and a specific procedure exists to determine which value the telephone should use. Parameter Data Precedence on page 14 describes the order in which parameter values are determined.

Table 11: 1603SW-I SIP IP Deskphones Customizeable System Parameters

Parameter Name	Default Value	Description and Value Range
AGCHAND	1	Automatic Gain Control status for handset. Values are 0=disabled, 1=enabled.
AGCSPKR	1	Automatic Gain Control status for speaker. Values are 0=disabled, 1=enabled.
AUTH	0	Authentication flag for settings file download. Values are: 0=secure setting file download is not required 1=secure setting file download is required
BAKLIGHTOFF	120	Number of minutes without display activity to wait before turning off the backlight. Values range from zero (never turn off) through 999 minutes (16.65 hours).
CONFIG_SERVER_ SECURE_MODE	0	Indicates whether or not secure communication via HTTPS is required to access the configuration server. 0 = Use HTTP. 1 = Use HTTPS.
COUNTRY	USA	Country of operation for specific dial tone generation. This is a specific text string specifying the country in which the device operates (e.g. "USA", "France", Germany"). See Appendix C: Countries With Specific Network Progress Tones for a list of applicable countries.
DATEFORMAT	%m/%d/%y	Formatting string defining how to display the date in the top line and the call log.
		1 of 10

Table 11: 1603SW-I SIP IP Deskphones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
DHCPSTD	0	DHCP Standard lease violation flag. Indicates whether to keep the IP Address if there is no response to lease renewal. If set to “1” (No) the telephone strictly follows the DHCP standard with respect to giving up IP Addresses when the DHCP lease expires. If set to “0” (Yes) the telephone continues using the IP Address until it detects reset or a conflict (see DHCP Generic Setup).
DIALPLAN	" " (Null)	Dial plan for operation with a secondary controller. The DIALPLAN parameter is used to determine one or more valid dialstrings. Valid value is 0 to 1023 characters that define the dial plan. See Setting the Dial Plan on SIP IP Telephones for more information.
DNSSRVR	0.0.0.0	Text string containing the IP Address of zero or more DNS servers, in dotted-decimal format, separated by commas with no intervening spaces (0-255 ASCII characters, including commas).
DOMAIN	" " (Null)	Text string containing the domain name to be used when DNS names in system values are resolved into IP Addresses. Valid values are 0-255 ASCII characters.
DOT1X	0	Defines the telephone's operational mode for IEEE 802.1X.Valid values are: 0 = Unicast Supplicant operation only, with PAE multicast pass-through, but without proxy Logoff. 1= Unicast Supplicant operation only, with PAE multicast pass-through and proxy Logoff. 2= Unicast or multicast Supplicant operation, without PAE multicast pass-through or proxy Logoff.
DOT1XSTAT	0	IEEE 802.1X status. Enables/disables IEEE 802.1X function and, if enabled, additionally defines reaction on received multicast or unicast EAPOL messages. Valid values are: 0 = Supplicant operation disabled. 1 = Supplicant operation enabled, but responds only to received unicast EAPOL messages. 2 = Supplicant operation enabled, responds to received unicast and multicast EAPOL messages.
DSCPAUD	46	Differentiated Services Code Point for audio. Values range from 0 to 63.
DSCPSIG	34	Differentiated Services Code Point for signaling. Values range from 0 to 63.
DSTOFFSET	1	Used for daylight saving time calculation in hours. Values range from 0 to 2.

2 of 10

Table 11: 1603SW-I SIP IP Deskphones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
DSTSTART	2Sun Mar2L	Used to identify start date for automatic change to Daylight Saving Time. Default string length with a format of either *odddmmmht* or *Dmmmht*, where: *o* = one character representing an ordinal adjective of "1" (first), "2" (second), "3" (third), "4" (fourth) or "L" (last) *ddd* = 3 characters containing the English abbreviation for the day of the week *mmm* = 3 characters containing the English abbreviation for the month *h* = one numeric digit representing the time to make the adjustment, exactly on the hour at hAM (0h00 in military format), where valid values of h are "0" through "9" *t* = one character representing the time zone relative to the adjustment where "L" is local time and U is universal time *D* = one or two ASCII digits representing the date of the month from "1" or "01" to "31", or the character "L", which means the last day of the month)
DSTSTOP	1SunNov2L	Used to identify stop date for automatic change to Daylight Saving Time. Default string length with a format of either *odddmmmht* or *Dmmmht*, where: *o* = one character representing an ordinal adjective of "1" (first), "2" (second), "3" (third), "4" (fourth) or "L" (last) *ddd* = 3 characters containing the English abbreviation for the day of the week *mmm* = 3 characters containing the English abbreviation for the month *h* = one numeric digit representing the time to make the adjustment, exactly on the hour at hAM (0h00 in military format), where valid values of h are "0" through "9" *t* = one character representing the time zone relative to the adjustment where "L" is local time and U is universal time *D* = one or two ASCII digits representing the date of the month from "1" or "01" to "31", or the character "L", which means the last day of the month)
DTMF_PAYLOAD_TYPE	120	RTP dynamic payload used for RFC 2833 signaling. Range is 96 to 127.
ENABLE_EARLY_MEDIA	1	Flag that indicates if SIP early is enabled. If enabled and 18x progress message includes early SDP, Spark uses that information to open a VoIP channel to the far-end before the call is answered. Values are 0=disabled; 1=enabled.

3 of 10

Table 11: 1603SW-I SIP IP Deskphones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
ENABLE_PPM_ SOURCED_ SIPPROXYSRVR	1	Enables PPM as a source of SIP proxy server information. Valid values are: 0 = Do not use PPM as a source for SIP proxy server information. 1 = Use PPM for SIP proxy server information.
FAILED_SESSION_ REMOVAL_TIMER	30	Timer to automatically remove a failed call session. Range in seconds is 5 to 999.
FONTFILE	" " (Null)	Name of the font file for a language for a 1603SW-I SIP IP Deskphone.
GMTOFFSET	0:00	Offset used to calculate time from GMT reference time. Default string length positive or negative number of hours and minutes less than 13 hours. Consists of 1 to 6 characters, optionally beginning with "+" or "-", followed by one or two number digits whose combined value is from "0" to "12" optionally followed by a ":" and two numeric digits whose combined value is from "00" to "59".
HTTPDIR	" " (Null)	HTTP server directory path. The path name prepended to all file names used in HTTP and HTTPS get operations during initialization/HTTP downloads. Value: 0-127 ASCII characters, no spaces. Null is a valid value. Leading or trailing slashes are not required. The command syntax is “GET HTTPDIR *myhttpdir*” where “myhttpdir” is your HTTP server path. HTTPDIR is the path for all HTTP operations.
HTTPPORT	80	Destination TCP port used for requests to the HTTP server during initialization. Range is 0 - 65535.
HTTPSRVR	0.0.0.0	List of IP Address(es) or DNS Name(s) of HTTP file server(s) used to download telephone files. HTTP server addresses can be in dotted decimal or DNS format, and must be separated by commas (0-255 ASCII characters, including commas).
ICMPDU	1	Controls whether ICMP Destination Unreachable messages will be processed. Values are: 0=DU messages not transmitted 1= DU messages not transmitted in response to specific events 2= DU message with code 2 will be transmitted in case of specific events
ICMPRED	0	Controls whether ICMP Redirect messages will be processed. Values are: 0 = Redirect messages will neither be transmitted nor received Redirect messages will be supported 1 = Redirect messages will not be transmitted, but received Redirect messages will be supported per RFC 1122

4 of 10

Table 11: 1603SW-I SIP IP Deskphones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
INGRESS_DTMF_VOL_ LEVEL	-12	RFC 2833 Digit event "volume" level. The power level of the tone, expressed in dBm0 after dropping the sign. (from RFC 2833 section 3.5 "Payload Format." Values are: -20 to -7.
INTER_DIGIT_TIMEOUT	5	This is the timeout that takes place when user stops inputting digits. The timeout is treated as digit collection completion, and when it occurs, the application sends out an invite. Range in seconds of 1 to 10.
L2Q	0	Requests 802.1Q tagging mode (auto/on/off). Values are: 0 = auto 1 = on 2 = off
L2QAUD	6	Layer 2 audio priority value. Range from 0 to 7.
L2QSIG	6	Layer 2 signaling priority value. Range from 0 to 7.
L2QVLAN	n/a	802.1Q VLAN Identifier (0 to 4094). Null (" ") is not a valid value and the value cannot contain spaces. This parameter is preserved in RAM which survives reset and stored to flash (as L2QVLAN_INIT) only upon successful registration. This value is initialized from L2QVLAN_INIT after power-up. This value will not be initialized from L2QVLAN_INIT after reset, but can be modified using the ADDR craft procedure.
LANG0STAT	1	This flag defines, whether or not the built-in English is offered to the user as selectable item in the language selection UI menu. At least one other language file must be downloaded, before "not offering" built-in English. Values are 0=not offered; 1=selectable.
LANGSYS	" " (Null)	0 to 32 ASCII characters. The file name of the system default language file, if any.
LOGSRVR	" " (Null)	Syslog server IP or DNS address. 0 to 255 characters: zero or one IP Addresses in dotted decimal or DNS name format.
		5 of 10

Table 11: 1603SW-I SIP IP Deskphones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
OPSTAT	111	Options status flag(s) (1 or 3 ASCII numeric digits) indicate which options are user-selectable. The default of 111 grants access to all options and related applications. Single digit valid values are: 1=user can access all options, including Logout, 2= user can access only view-oriented applications. Three-digit valid values are a concatenation of binary values, in the form *abc*, where each letter represents a 0 (disabled/off) or 1 (enabled/on), interpreted as: *a* = base settings for all user options and related applications, except as noted in *b* or *c*. *b* = setting for view-oriented applications (for example, the Network Information application), as applicable. *c* = setting for Logout application, if applicable. The binary "0" does not allow an end user to see or invoke options and related applications. The binary "1" allows full display and access to all options and related applications.
OUTBOUND_ SUBSCRIPTION_ REQUEST_DURATION	86400	Number of seconds used in initial SUBSCRIBE messages. This is the suggested duration value of the telephone, which might be lowered by the server, depending on the server configuration. Range is 60-31536000. Note that the default value is equal to one day and the maximum value represents one year.
PHNEMERGNUM	" " (Null)	Emergency Number. 0 to 30 dialable characters (0-9, * , and/or #). This number is dialed when the Emergency softkey is pressed, or when a pop-up screen for making an emergency calls is confirmed.
PHY1STAT	1	Ethernet line interface setting (1=auto-negotiate, 2=10Mbps half-duplex, 3=10Mbps full-duplex, 4=100Mbps half-duplex, 5=100Mbps full-duplex, and 6=1000Mbps full-duplex if supported by the hardware). Speed and duplex issues are summarized and the best practice is provided in the *Avaya Application Solutions: IP Telephony Deployment Guide*, Document Number 555-245-600 Issue 6, January 2008 on page 290. This document is available from the Avaya support website.
PHY2PRIO	0	Layer 2 priority value for frames received on or forwarded to the secondary Ethernet interface. Set this parameter only when VLAN separation is "1" (enabled). Values are from 0-7 and correspond to the drop-down menu selection.

6 of 10

Table 11: 1603SW-I SIP IP Deskphones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
PHY2STAT	1	Secondary Ethernet interface setting (0=Secondary Ethernet interface off/disabled, 1=auto-negotiate, 2=10Mbps half-duplex, 3=10Mbps full-duplex, 4=100Mbps half-duplex, 5=100Mbps full-duplex), and, for post-Release S1.0 use, 6=1000Mbps full-duplex (if supported by the hardware). Speed and duplex issues are summarized and the best practice is provided in the *Avaya Application Solutions: IP Telephony Deployment Guide*, Document Number 555-245-600 Issue 6, January 2008 on page 290. This document is available from the Avaya support website.
PHY2VLAN	0	VLAN identifier used by frames received on or forwarded to the secondary Ethernet interface. Set this parameter only when VLAN separation is "1" (enabled). Value is 1-4 ASCII numeric digits from "0" to "4094." Null is not a valid value, nor can the value contain spaces.
PROCPSWD	27238	Text string containing the local (dialpad) procedure password (Null or 1-7 ASCII digits). If set, password must be entered immediately after accessing the craft interface, either during initialization or when Mute is pressed to access a craft procedure. Intended to facilitate restricted access to local procedures even when command sequences are known. Password is viewable, not hidden.
PROCSTAT	0	Controls access to Craft local (dialpad) administrative procedures. Values are: 0 = Full access to craft local procedures 1 = restricted access to craft local procedures
RDS_INITIAL_RETRY_ATTEMPTS	15	Indicates how many times the PPM adaptor should try to download from PPM before giving up on connecting to the PPM server. Values are: 1-30.
RDS_INITIAL_RETRY_TIME	2	Remote Data Source initial retry time in seconds; indicates the initial delay for a retry to connect to the PPM server. Valid range is 2-60 (seconds).
RECOVERYREGISTER WAIT	60	Reactive monitoring interval in seconds for Failover. Valid values are: 10 - 36000
REGISTERWAIT	900	Number of seconds for next re-registration to SIP server. The default value for software Release 2.4+ was originally set to 300 to accommodate UDP, however, TCP/TLS is the recommended arrangement and is the most typical configuration; the default was changed from 300 to 900 seconds for software Release 2.5+. UDP arrangements can be handled by setting the value of the parameter to a lower value in the settings file. Range in seconds: 30 to 86400
RTCPCONT	1	Enables/disables the RTCP in parallel to RTP audio streams. Values are 0=RTCP disabled, 1=RTCP enabled.

7 of 10

Table 11: 1603SW-I SIP IP Deskphones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
RTCPMON	" " (Null)	RTCP Monitor IP or DNS address to be used as destination for RTCP monitoring. Zero to 255 characters: zero or one IP addresses in dotted decimal or DNS name format. Note that this value is only set via SET command in settings file if operating in a NON-Avaya environment, otherwise this value is retrieved via PPM.
RTCPMONPERIOD	5	RTCP Monitor report period. Valid range = 5 - 30 Interval in seconds for sending out RTCP monitoring reports.
RTCPMONPORT	5005	RTCP monitor port number. TCP/UDP port to be used as destination port for RTCP monitoring. Valid range is 0-65535. Note that this value is only set via SET command in settings file if operating in a NON-Avaya environment, otherwise this value is retrieved via PPM.
RTP_PORT_LOW	5004	Specifies lower limit of a port range to be used by RTP/ RTCP or SRTP/SRTCP connections, for example, to adapt to firewall traversal policies. Values: 1024-65503.
RTP_PORT_RANGE	40	Specifies the width of the port range to be used by RTP/ RTCP or SRTP/SRTCP connections, for example, to adapt to firewall traversal policies. The upper limit is calculated by the value of RTP_PORT_LOW plus the value of RTP_PORT_RANGE, taking into consideration the overall limit of 65535. Values: 32-64511.
SEND_DTMF_ TYPE	2	Defines whether DTMF tones are send in-band (regular audio) or out-band (negotiation and transmission of DTMF according to RFC 2833, with fallback to send in-band DTMF tones, if far end does not support RFC2833). Values are 1=in-band DTMF; 2=RFC2833 procedure.
SIG_PORT_LOW	1024	Lower limit of port range for signaling to support by the phone. Values range from 1024 to 65503.
SIG_PORT_RANGE	64511	Port range for signaling to support by the phone. Values range from 32 to 64511.

8 of 10

Table 11: 1603SW-I SIP IP Deskphones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
SIP_CONTROLLER_LIST	" " (Null)	List of SIP proxy/registrar server IP or DNS address(es). Server(s) used to address SIP registrations and signaling, if operating in proxy mode (in case of several entries first address always first, etc.). When operating in an Avaya Environment SIP_CONTROLLER_LIST is also used to access Personal Profile Manager (PPM). This parameter is considered the list of "Configured Controllers" for Failover logic. When this parameter has multiple IP Addresses, the ordering of the list defines the priority of the controllers for selection during Failover; the first element of the list is the highest priority, the last element is the lowest priority. Format: host[:port][;transport=xxx] where *host* is an IP address in dotted decimal format or DNS name, *port* is the optional port number (if not specified, the default port value of 5060 for UDP and TCP or 5061 for TLS is used), *transport* is the optional transport type (where *xxx* is tls, tcp, or udp) and if not specified, the default value of TLS is used. The first element of this parameter (if applicable) has the highest precedence within the parameter. This parameter can have 0 to 255 characters indicating zero or more IP addresses in dotted decimal or DNS name format, separated by commas without any intervening spaces.
SIPDOMAIN	" " (Null)	SIP domain name for registration. 0 to 255 characters: string representing domain name.
SNMPADD	" " (Null)	Text string containing zero or more allowable source IP Addresses for SNMP queries, in dotted decimal or DNS format, separated by commas, with up to 255 total ASCII characters including commas and no intervening spaces.
SNMPSTRING	" " (Null)	Text string containing the SNMP community name string (up to 32 ASCII characters, no spaces).
SNTPSRVR	" " (Null)	Used to retrieve date and time via SNTP (in case of several entries first address always first, etc.). Zero to 255 characters: zero or more IP Addresses in dotted decimal or DNS name format, separated by commas without any intervening spaces.
TCP_KEEP_ALIVE_ INTERVAL	10	Time interval (number of seconds) after which TCP keep-alive packets are re-transmitted. The interval is started by the system TCP/IP stack (when TCP keep-alive is enabled with specified time intervals). Values are 5-60 seconds.

9 of 10

Table 11: 1603SW-I SIP IP Deskphones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
TCP_KEEP_ALIVE_STATUS	1	Indicates whether TCP/IP keep-alive should be enabled at the system. Values are 0=TCP keep alive disabled, 1=TCP keep alive enabled.
TCP_KEEP_ALIVE_TIME	60	This time interval is the time 1603SW-I SIP IP Deskphones will wait before sending out a TCP keep-alive message (TCP ACK message) to the far-end. The time is controlled by the system's TCP/IP stack. The timer is restarted after application level data (for example, a SIP message) is sent over the socket. When the system is idle, this keep-alive time expires and results in sending a TCP ACK (keep-alive) packet. Valid values are 10-3600 (seconds).
TIMEFORMAT	0	Display time according to defined format in the top line and in the call log. Values are: 0=am/pm format 1=24h format
TLSDIR	" " (Null)	Path name for https downloads. Character string of 0 to 127 characters representing a directory name or path to directory.
VLANSEP	1	Enables or disables VLAN separation. Controls whether frames to/from the secondary Ethernet interface receive IEEE 802.1Q tagging treatment. The tagging treatment enables frames to be forwarded based on their tags in a manner separate from telephone frames. If tags are not changed, no tag-based forwarding is employed. Values are: 1=On/Enabled, 2= Off/Disabled. This parameter is used with several related parameters. For more information, see VLAN Separation on page 86.
VLANTEST	60	Number of seconds to wait for a DHCPOFFER when using a non-zero VLAN ID (1-3 ASCII digits, from “0” to “999”).
WAIT_FOR_REGISTRATION_TIMER	32	Time in seconds the SIP application will wait for a register response message. If no message is received, registration is retried. Range is 4-3600 (seconds).

10 of 10

VLAN Considerations

This section contains information on how to administer 1603SW-I SIP IP Deskphones to minimize registration time and maximize performance in a Virtual LAN (VLAN) environment. If your LAN environment does not include VLANs, set the system parameter L2Q to 2 (off) to ensure correct operation.

VLAN Tagging

IEEE 802.1Q tagging (VLAN) is a useful method of managing VoIP traffic in your LAN. Avaya recommends that you establish a *voice* LAN, set L2QVLAN to that VLAN, and provide voice traffic with priority over other traffic. If LLDP was used to set the telephones' VLAN, that setting has absolute authority. Otherwise, you can set VLAN tagging manually, by DHCP, or in the 46xxsettings.txt file.

If VLAN tagging is enabled (L2Q=0 or 1), the 1603SW-I SIP IP Deskphones set the VLAN ID to L2QVLAN, and VLAN priority for packets from the telephone to L2QAUD for audio packets and L2QSIG for signalling packets. The default value (6) for these parameters is the recommended value for voice traffic in IEEE 802.1D.

Regardless of the tagging setting, a 1603SW-I SIP IP Deskphone will always transmit packets from the deskphone at absolute priority over packets from secondary Ethernet. The priority settings are useful only if the downstream equipment is administered to give the *voice* LAN priority.

⚠ **Important:**

VLAN tags are always removed from frames that egress (go out of) the secondary Ethernet interface.

VLAN Detection

The Avaya IP Telephones support automatic detection of the condition where the L2QVLAN setting is incorrect. When VLAN tagging is enabled (L2Q= 0 or 1) initially the 1603SW-I SIP IP Deskphone transmits DHCP messages with IEEE 802.1Q tagging and the VLAN set to L2QVLAN. The telephones will continue to do this for VLANTEST seconds.

- If the VLANTEST timer expires and L2Q=1, the telephone sets L2QVLAN=0 and transmits DHCP messages with the default VLAN (0).
- If the VLANTEST timer expires and L2Q=0, the telephone sets L2QVLAN=0 and transmits DHCP messages without tagging.
- If VLANTEST is 0, the timer will never expire.

Note:

Regardless of the setting of L2Q, VLANTEST, or L2QVLAN, you must have DHCP administered so that the telephone will get a response to a DHCPDISCOVER when it makes that request on the default (0) VLAN.

After VLANTEST expires, if a 1603SW-I SIP IP Deskphone receives a non-zero L2QVLAN value, the telephone will release the IP Address and send DHCPDISCOVER on that VLAN. Any other release will require a manual reset before the telephone will attempt to use a VLAN on which VLANTEST has expired. See the Reset procedure in Chapter 3 of the *Avaya one-X™ Deskphone Value Edition SIP for 1603SW-I Deskphones Installation and Maintenance Guide*.

The telephone ignores any VLAN ID administered on the Communication Manager call server.

VLAN Default Value and Priority Tagging

The system value **L2QVLAN** is initially set to “0” and identifies the 802.1Q VLAN Identifier. This default value indicates “priority tagging” as defined in IEEE 802.IQ Section 9.3.2.3. Priority tagging specifies that your network closet Ethernet switch automatically insert the switch port default VLAN without changing the user priority of the frame (cf. IEEE 802.1P and 802.1Q).

The VLAN ID = 0 (zero) is used to associate priority-tagged frames to the port/native VLAN of the ingress port of the switch. But some switches do not understand a VLAN ID of zero and require frames tagged with a non-zero VLAN ID.

If you do not want the default VLAN to be used for voice traffic:

- Ensure that the switch configuration lets frames tagged by the 1603SW-I SIP IP Deskphone through without overwriting or removing them.
- Set the system value **L2QVLAN** to the ***VLAN ID*** appropriate for your voice LAN.

Another system value you can administer is **VLANTEST**. VLANTEST defines the number of seconds the 1603SW-I SIP IP Deskphone waits for a DHCPOFFER message when using a non-zero VLAN ID. The VLANTEST default is “60” seconds. Using VLANTEST ensures that the deskphone returns to the default VLAN if an invalid VLAN ID is administered or if the phone moves to a port where the L2QVLAN value is invalid. The default value is long, allowing for the scenario that a major power interruption is causing the phones to restart. Always allow time for network routers, the DHCP servers, etc. to be returned to service. If the deskphone restarts for any reason and the VLANTEST time limit expires, the telephone assumes the administered VLAN ID is invalid. The deskphone then initiates registration with the default VLAN ID.

Setting **VLANTEST** to “**0**” has the special meaning of telling the phone to use a non-zero VLAN indefinitely to attempt DHCP. In other words, the deskphone does not return to the default VLAN.

Note:

If the telephone returns to the default VLAN but must be put back on the L2QVLAN VLAN ID, you must Reset the deskphone. See the Reset procedure in the *Avaya one-X™ Deskphone Value Edition SIP for 1603SW-I IP Deskphones Installation and Maintenance Guide*.

VLAN Separation

VLAN separation is available to control access to the voice VLAN from the secondary Ethernet interface, and to control whether broadcast traffic from the data VLAN is forwarded to the deskphone. The following system parameters control VLAN separation:

- **VLANSEP** - enables (1) or disables (0) VLAN separation.
- **PHY2VLAN** - specifies the VLAN ID to be used for frames forwarded to the network from the secondary Ethernet interface.
- **PHY2PRIO** - the layer 2 priority value to be used for tagged frames forwarded to the network from the secondary Ethernet interface.

Table 12 provides several VLAN separation guidelines.

Table 12: VLAN Separation Rules

If		Then
VLANSEP is “1” (On/Enabled)	**AND** the deskphone is tagging frames with a VLAN ID not equal to PHY2VLAN, **AND** the PHY2VLAN value is not zero.	**Tagged frames received on the secondary Ethernet interface:** All tagged frames received on the secondary Ethernet interface are changed before forwarding to make the VLAN ID equal to the PHY2VLAN value and the priority value equal to the PHY2PRIO value. Untagged frames received on the secondary Ethernet interface are not changed before forwarding to the network. Tagged frames with a VLAN ID of zero (priority-tagged frames) will be changed before they are forwarded such that the VLAN ID of the forwarded frame is equal to the PHY2LAN value and the priority value is equal to the PHY2PRIO value. **Tagged frames received on the line interface:** Tagged frames received on the Ethernet line interface will only be forwarded to the secondary Ethernet interface if the VLAN ID equals PHY2LAN. Tagged frames received on the Ethernet line interface will only be forwarded to the deskphone if the VLAN ID equals the VLAN ID used by the deskphone. Untagged frames are not changed and will continue to be forwarded or not forwarded as determined by the Ethernet switch forwarding logic. Tagged frames with a VLAN ID of zero (priority-tagged frames) will either be forwarded to the secondary Ethernet interface or to the deskphone as determined by the forwarding logic of the Ethernet switch, but the tag will still be removed from frames that egress from the secondary Ethernet interface.
VLANSEP is “1” (On/Enabled)	**AND** the deskphone is not tagging frames, **OR** if the deskphone is tagging frames with a VLAN ID equal to PHY2VLAN, **OR** if the PHY2VLAN value is zero.	Frames forwarded to the network from the secondary Ethernet interface will not be changed before forwarding. Tagging is not added or removed and the VLAN ID and priority does not change for frames received on the secondary interface. Tags are still removed for frames that egress from the secondary interface. The Ethernet switch forwarding logic determines whether frames received on the Ethernet line interface are forwarded to the secondary Ethernet interface or to the deskphone without regard to specific VLAN IDs or the existence of tags.

1 of 2

Table 12: VLAN Separation Rules (continued)

If		Then
VLANSEP is "0",	**OR** the deskphone is not tagging frames, **OR** the deskphone is tagging frames with a VLAN ID equal to PHY2VLAN.	Frames forwarded to the network from the secondary Ethernet interface will not be changed before forwarding. Tagging is not added or removed and the VLAN ID and priority does not change for frames received on the secondary interface. Tags are still removed for frames that egress from the secondary interface. The Ethernet switch forwarding logic determines whether frames received on the Ethernet line interface are forwarded to the secondary Ethernet interface or to the deskphone without regard to specific VLAN IDs or the existence of tags.
		2 of 2

DNS Addressing

The 1603SW-I SIP IP Deskphones support DNS addresses and dotted decimal addresses. The deskphone attempts to resolve a non-ASCII-encoded dotted decimal IP address by checking the contents of DHCP Option 6. See DHCP Generic Setup on page 50 for information. At least one address in Option 6 must be a valid, non-zero, dotted decimal address, otherwise, DNS fails. The text string for the **DOMAIN** system parameter (Option 15, Table 11) is appended to the address(es) in Option 6 before the deskphone attempts DNS address resolution. If Option 6 contains a list of DNS addresses, those addresses are queried in the order given if no response is received from previous addresses on the list. As an alternative to administering DNS by DHCP, you can specify the DNS server and/or Domain name in the HTTP script file. But first **SET** the **DNSSRVR** and **DOMAIN** values so you can use those names later in the script.

Note:

Administer Options 6 and 15 appropriately with DNS servers and Domain names respectively.

IEEE 802.1X

1603SW-I SIP IP Deskphones support the IEEE 802.1X standard for pass-through and Supplicant operation but only if the value of the configuration parameter DOT1XSTAT is "1" (the default, meaning supplicant operation is enabled, and the telephone responds only to received unicast EAPOL messages) or "2" (supplicant operation enabled, and telephone responds to received unicast and multicast EAPOL messages). If DOT1XSTAT has any other value, supplicant operation will not be supported. The system parameter DOT1X determines how the telephones handle 802.1X multicast packets and proxy logoff, as follows:

- When DOT1X = 0 (the default) the deskphone forwards 802.1X multicast packets from the Authenticator to the PC attached to the deskphone and forwards multicast packets from the attached PC to the Authenticator (multicast pass-through). Proxy Logoff is not supported.
- When DOT1X = 1, the deskphone supports the same multicast pass-through as when DOT1X=0. Proxy Logoff is supported.
- When DOT1X = 2, the deskphone forwards multicast packets from the Authenticator only to the deskphone, ignoring multicast packets from the attached PC (no multicast pass-through). Proxy Logoff is not supported.

Regardless of the DOT1X setting, the deskphone always properly directs unicast packets from the Authenticator to the deskphone or its attached PC, as dictated by the MAC address in the packet.

1603SW-I SIP IP Deskphones will respond to unicast EAPOL frames (frames with the deskphone’s MAC address as the destination MAC address, and a protocol type of 88-8E hex) received on the Ethernet line interface if the value of DOT1XSTAT is "1" or "2", but will only respond to EAPOL frames that have the PAE group multicast address as the destination MAC address if the value of DOT1XSTAT is "2". If the value of DOT1XSTAT is changed to "0" from any other value after the Supplicant has been authenticated, an EAPOL-Logoff will be transmitted before the Supplicant is disabled.

The system parameter DOT1XSTAT determines how the deskphone handles Supplicants as follows:

- When DOT1XSTAT=0, Supplicant operation is completely disabled. This is the default value.
- When DOT1XSTAT=1, Supplicant operation is enabled, but responds only to received unicast EAPOL messages.
- When DOT1XSTAT=2, Supplicant operation is enabled and responds to received unicast and multicast EAPOL messages.

Note:

If the Ethernet line interface link fails, the 802.1X Supplicant, if enabled, enters the Disconnected state. The 802.1X Supplicant variable userLogoff normally has a value of FALSE. This variable will be set to TRUE before the telephone drops the link on the Ethernet line interface (and back to FALSE after the link has been restored). The userLogoff variable may also be briefly set to TRUE to force the Supplicant into the LOGOFF state when new credentials are entered.

802.1X Pass-Through and Proxy Logoff

1603SW-I SIP IP Deskphones with a secondary Ethernet interface support pass-through of 802.1X packets to and from an attached PC. This enables an attached PC running 802.1X supplicant software to be authenticated by an Ethernet data switch.

The SIP IP Deskphones support two pass-through modes:

- pass-through and
- pass-through with proxy logoff.

The DOT1X parameter setting controls the pass-through mode. In Proxy Logoff mode (DOT1X=1), when the secondary Ethernet interface loses link integrity, the telephone sends an 802.1X EAPOL-Logoff message to the data switch on behalf of the attached PC. The message alerts the switch that the device is no longer present. For example, a message would be sent when the attached PC is physically disconnected from the IP telephone.

Note:

When DOT1X = 0 or 2, the Proxy Logoff function is not supported.

802.1X Supplicant Operation

1603SW-I SIP IP Deskphones that support Supplicant operation also support Extensible Authentication Protocol (EAP), but only with the MD5-Challenge authentication method as specified in IETF RFC 3748 [8.5-33a].

A Supplicant identity (ID) and password of no more than 12 numeric characters are stored in reprogrammable non-volatile memory. The ID and password are not overwritten by deskphone software downloads. The default ID is the MAC address of the telephone, converted to ASCII format without colon separators, and the default password is null. Both the ID and password are set to defaults at manufacture. EAP-Response/Identity frames use the ID in the Type-Data field. EAP-Response/MD5-Challenge frames use the password to compute the digest for the Value field, leaving the Name field blank.

When a deskphone is installed for the first time and 802.1x is in effect, the dynamic address process prompts the installer to enter the Supplicant identity and password. The deskphone does not accept null value passwords. See “Dynamic Addressing Process” in the *Avaya one-X™ Deskphone Value Edition SIP for 1603SW-I IP Deskphones Installation and Maintenance Guide*. The deskphone stores 802.1X credentials when successful authentication is achieved. Post-installation authentication attempts occur using the stored 802.1X credentials, without prompting the user for ID and password entry.

A deskphone can support several different 802.1X authentication scenarios, depending on the capabilities of the Ethernet data switch to which it is connected. Some switches may authenticate only a single device per switch port. This is known as single-supplicant or port-based operation. These switches typically send multicast 802.1X packets to authenticating devices.

These switches support the following three scenarios:

- **Standalone telephone (Telephone Only Authenticates) -** When the deskphone is configured for Supplicant Mode (DOT1XSTAT=2), the deskphone can support authentication from the switch.
- **Telephone with attached PC (Telephone Only Authenticates) -** When the deskphone is configured for Supplicant Mode (DOT1X=2 and DOT1XSTAT=2), the deskphone can support authentication from the switch. The attached PC in this scenario gains access to the network without being authenticated.
- **Telephone with attached PC (PC Only Authenticates) -** When the deskphone is configured for Pass-Through Mode or Pass-Through Mode with Logoff (DOT1X=0 or 1 and DOT1XSTAT=0), an attached PC running 802.1X supplicant software can be authenticated by the data switch. The telephone in this scenario gains access to the network without being authenticated.

Some switches support authentication of multiple devices connected through a single switch port. This is known as multi-supplicant or MAC-based operation. These switches typically send unicast 802.1X packets to authenticating devices. These switches support the following two scenarios:

- **Standalone deskphone (Deskphone Only Authenticates) -** When the deskphone is configured for Supplicant Mode (DOT1XSTAT=2), the deskphone can support authentication from the switch. When DOT1X is "0" or "1", the deskphone is unable to authenticate with the switch.
- **Deskphone and PC Dual Authentication -** Both the deskphone and the connected PC can support 802.1X authentication from the switch. The deskphone may be configured for Pass-Through Mode or Pass-Through Mode with Logoff (DOT1X=0 or 1 and DOT1XSTAT=1 or 2). The attached PC must be running 802.1X supplicant software.

Link Layer Discovery Protocol (LLDP)

Link Layer Discovery Protocol (LLDP) is an open standards layer 2 protocol IP deskphones use to advertise their identity and capabilities and to receive administration from an LLDP server. LAN equipment can use LLDP to manage power, administer VLANs, and provide some administration.

The transmission and reception of LLDP is specified in IEEE 802.1AB-2005. The 1603SW-I SIP IP Deskphones use Type-Length-Value (TLV) elements specified in IEEE 802.1AB-2005, TIA TR-41 Committee - Media Endpoint Discovery (LLDP-MED, ANSI/TIA-1057), and Proprietary elements. LLDP Data Units (LLDPDUs) are sent to the LLDP Multicast MAC address (01:80:c2:00:00:0e).

These deskphones:

- do not support LLDP on the secondary Ethernet interface.

- will not forward frames received with the 802.1AB LLDP group multicast address as the destination MAC address between the Ethernet line interface and the secondary Ethernet interface.

A 1603SW-I SIP IP Deskphone initiates LLDP after receiving an LLDPDU message from an appropriate system. Once initiated, the telephones send an LLDPDU every 30 seconds with the following contents:

Table 13: LLDPDU Transmitted by the 1603SW-I SIP IP Deskphones

Category	TLV Name (Type)	TLV Info String (Value)
Basic Mandatory	Chassis ID	IPv4 IP Address of telephone.
Basic Mandatory	Port ID	MAC address of the telephone.
Basic Mandatory	Time-To-Live	120 seconds.
Basic Optional	System Name	The Host Name sent to the DHCP server in DHCP option 12.
Basic Optional	System Capabilities	Bit 2 (Bridge) will be set in the System Capabilities if the telephone has an internal Ethernet switch. If Bit 2 is set in Enabled Capabilities then the secondary port is enabled. Bit 5 (Telephone) will be set in the System Capabilities. If Bit 5 is set in the Enabled Capabilities than the telephone is registered.
Basic Optional	Management Address	Mgmt IPv4 IP Address of telephone. Interface number subtype = 3 (system port). Interface number = 1. OID = SNMP MIB-II sysObjectID of the telephone.
IEEE 802.3 Organization Specific	MAC / PHY Configuration / Status	Reports autonegotiation status and speed of the uplink port on the telephone.
TIA LLDP MED	LLDP-MED Capabilities	Media Endpoint Discovery - Class III - IP Telephone.
TIA LLDP MED	Extended Power-Via-MDI	Power Value = 0 if the deskphone is not currently powered via PoE, else the maximum power usage of the deskphone plus all modules and adjuncts powered by the telephone in tenths of a watt.

1 of 2

Table 13: LLDPDU Transmitted by the 1603SW-I SIP IP Deskphones (continued)

Category	TLV Name (Type)	TLV Info String (Value)
TIA LLDP MED	Network Policy	Tagging Yes/No, VLAN ID for voice, L2 Priority, DSCP Value.
TIA LLDP MED	Inventory – Hardware Revision	MODEL - Full Model Name.
TIA LLDP MED	Inventory – Firmware Revision	BOOTNAME.
TIA LLDP MED	Inventory – Software Revision	APPNAME.
TIA LLDP MED	Inventory – Serial Number	Deskphone serial number.
TIA LLDP MED	Inventory – Manufacturer Name	Avaya.
TIA LLDP MED	Inventory – Model Name	MODEL with the final D***xxx*** characters removed.
Avaya Proprietary	PoE Conservation Level Support	Provides Power Conservation abilities/settings, Typical and Maximum Power values. OUI = 00-40-0D (hex), Subtype = 1.
Avaya Proprietary	Call Server IP Address	Call Server IP Address. Subtype = 3.
Avaya Proprietary	IP Phone Addresses	Phone IP Address, Phone Address Mask, Gateway IP Address. Subtype = 4.
Avaya Proprietary	File Server	File Server IP Address. Subtype = 6.
Avaya Proprietary	802.1Q Framing	802.1Q Framing = 1 if tagging or 2 if not. Subtype = 7.
Basic Mandatory	End-of-LLDPDU	Not applicable.
		2 of 2

On receipt of a LLDPDU message, the Avaya IP Deskphones will act on the TLV elements described in Table 14:

Table 14: Impact of TLVs Received by 1603SW-I SIP IP Deskphones on System Parameter Values

System Parameter Name	TLV Name	Impact
PHY2VLAN	IEEE 802.1 Port VLAN ID	System value changed to the Port VLAN identifier in the TLV.
L2QVLAN and L2Q	IEEE 802.1 VLAN Name	The system value is changed to the TLV VLAN Identifier. L2Q will be set to 1 (ON). VLAN Name TLV is only effective if: ● The telephone is not registered with the Call Server. ● Name begins with VOICE (case does not matter). ● The VLAN is not zero. ● DHCP Client is activated. ● The telephone is registered but is not tagging layer 2 frames with a non-zero VLAN ID. If VLAN Name causes the telephone to change VLAN and the telephone already has an IP Address the telephone will release the IP Address and reset. If the TLV VLAN ID matches the VLAN ID the telephone is using, the VLAN ID is marked as set by LLDP. Otherwise, if already registered, the telephone waits until there are no active calls, releases its IP Address, turns on tagging with the TLV VLAN ID, sets L2Q to "on," changes the default L2Q to "on," and resets. If there is no valid IP Address, the telephone immediately starts tagging with the new VLAN ID without resetting.

Table 14: Impact of TLVs Received by 1603SW-I SIP IP Deskphones on System Parameter Values (continued)

System Parameter Name	TLV Name	Impact
L2Q, L2QVLAN, L2QAUD, L2QSIG, DSCPAUD, DSCPSIG	MED Network Policy TLV	L2Q - set to “2” (off) If T (the Tagged Flag) is set to 0; set to “1” (on) if T is set to 1. L2QVLAN - set to the VLAN ID in the TLV. L2QAUD and L2QSIG - set to the Layer 2 Priority value in the TLV. DSCPAUD and DSCPSIG - set to the DSCP value in the TLV. A check is made as to whether a reset is necessary to obtain a new IP address due to a change in the values of the parameters L2Q or L2QVLAN. This TLV is ignored if: ● the value of USE_DHCP is “0” and the value of IPADD is not “0.0.0.0”, or ● the Application Type is not 1 (Voice) and is not 2 (Voice Signaling), or ● the Unknown Policy Flag (U) is set to 1.
TLSSRVR and HTTPSRVR	Proprietary File Server TLV	TLSSRVR and HTTPSRVR will be set to this value if neither of them have already been set.
L2Q	Proprietary 802.1 Q Framing	The default L2Q is set to the value of this TLV. No change is made to the current L2 tagging, but the new default value is used on the next reboot. If TLV = 1, L2Q set to "1" (On). If TLV = 2, L2Q set to "2" (Off). If TLV = 3, L2Q set to "0" (Auto).
	Proprietary - PoE Conservation TLV	This proprietary TLV can initiate a power conservation mode. The telephones that support this will turn on/off the telephone backlight and the backlight of an attached Button Module in response to this TLV.
	Extended Power-Via-MDI	Power conservation mode will be enabled if the received binary Power Source value is 10, and power conservation mode will be disabled if the received binary Power Source value is not 10. Power conservation mode is enabled even if the telephone is not powered over Ethernet because the telephone sends information about the power source that it is using in a TIA LLDP MED Extended Power-Via-MDI TLV; it is assumed that the power management system intends to conserve local power as well.

Local Administrative Options Using the Telephone Dialpad

The local procedures you use most often as an administrator are:

- **CLEAR** - Remove all administered values, user-specified data, option settings, etc. and return a telephone to its initial “out of the box” default values.
- **GROUP** - Set the group identifier on a per-phone basis.
- **RESET** - Reset all system values and system initialization values except AUTH, NVAUTH, registration extension, and password to the default values. Also resets the 802.1X identity and password to the default values.
- **VIEW** - Review the 1603SW-I SIP IP Deskphone system parameters to verify current values and file versions.
- **Ethernet (Hub) Interface Enable/Disable** - Enable or disable the Ethernet hub locally.

Clear Procedure

Sometimes, you might want to remove *all* administered values, user-specified data, and option settings. Essentially, you want to return a telephone to its initial “clean slate” or out of the box condition. This is usually done when passing a telephone to a new, dedicated user when the user’s **L O G O F F** option is not sufficient. For example, a new user is assigned the same extension, but requires different permissions than the previous user.

The **C L E A R** option erases all administered data—static programming, file server and call server programming, and user settings including Contact button labels and locally programmed Feature button labels, and restores all such data to default values. The **C L E A R** option does not affect the software load itself. If you have upgraded the telephone, the telephone retains the latest software. Once you have cleared a telephone, you can administer it normally.

⚠ **CAUTION:**

This procedure erases all administered data, without any possibility of recovering the data.

Use the following procedure to clear the telephone of its administrative, user-assigned and options values.

1. While the telephone is on-hook and idle, press the following sequence of keys on the faceplate of the telephone:

   Mute 2 5 3 2 7 # (Mute C L E A R #)

Note:

Press the **Mute** button momentarily. Do not press this button while pressing other keys/buttons.

The following text displays left-justified at the top of the display:

```
Clear all values?
*=no        #=yes
```

2. If you do not want to clear all values, press * (no) to terminate the procedure and retain the current values.

   A screen displays the following prompt on the top line:

```
Are you sure?
*=no    #=yes
```

3. Press the * button to terminate the procedure without clearing the values. Press the # button to clear all values to their initial default values.

   A confirmation tone sounds and the following text displays left-justified at the top of the display:

```
Clearing values.
```

The telephone is cleared to its “out of the box” state.

Group Identifier

Use the following procedure to set or change the Group Identifier.

Note:

Perform this procedure only if the LAN Administrator instructs you to do so.
For more information about groups, see The GROUP System Value on page 70.

While the telephone is on-hook and idle, press the following sequence of keys on the faceplate of the telephone:

Mute 4 7 6 8 7 (Mute G R O U P)

Note:

Press the **Mute** button momentarily. Do not press this button while pressing other keys/buttons.

The following text displays left-justified at the top of the display:

```
Group=ddd
New=_
```

where ***ddd*** is the Group value.

1. Enter a valid **Group** value (0-999).

   If a value different from the current Group value is entered, the following text displays left-justified at the top of the display:

   ```
   Save new value?
   *=no     #=yes
   ```

2. Press the ***** button to terminate the procedure, or the **#** button to save the new value.

   If you press the **#** button, the following text displays:

   ```
   New value
   being saved
   ```

   The new value is saved and the user interface is restored to its previous state.

Reset System Values

Use the following procedure to reset all system values and system initialization values except AUTH, NVAUTH, registration extension, and password to the default values. Also resets the 802.1X identity and password to the default values.

CAUTION:

This procedure erases all static information except the extension number and password, without any possibility of recovering the data.

1. While the telephone is on-hook and idle, press the following sequence of keys on the faceplate of the telephone:

   Mute 7 3 7 3 8 # (Mute R E S E T #)

Note:

Press the **Mute** button momentarily. Do not press this button while pressing other keys/buttons.

The IP telephones display the following text left-justified at the top of the display:

```
Reset values?
*=no    #=yes
```

CAUTION:

As soon as you press the # button, all static information except the extension number and password will be erased, without any possibility of recovering the data.

2. Press the # button to reset values to their defaults.

   All telephones display the following text left-justified at the top of the display while the system values are reset to defaults:

```
Resetting
values.
```

The telephone resets from the beginning of registration, which takes a few minutes.

Restart the Telephone

Use the following procedure to restart the telephone.

1. While the telephone is on-hook and idle, press the following sequence of keys on the faceplate of the telephone:

   Mute 7 3 7 3 8 # (Mute R E S E T #)

Note:

Press the **Mute** button momentarily. Do not press this button while pressing other keys/buttons.

The IP telephones display the following text left-justified at the top of the display:

```
Reset values?
*=no    #=yes
```

2. Press the **#** button to reset values to their defaults, or ***** to continue a restart without resetting the values to their defaults.

   The telephones display the following text left-justified at the top of the display while the system values are reset to defaults:

   ```
   Resetting
   values.
   ```

   Once the system values are reset, the following prompt displays on all IP telephones:

   ```
   Restart phone?
   *=no    #=yes
   ```

3. Press the ***** key to terminate the procedure without restarting the telephone.

   Press the **#** key to restart the telephone.

   The remainder of the procedure depends on the status of the boot and application files.

Interface Control

Use the following procedure to set or change the interface control value.

1. While the telephone is on-hook and idle, press the following sequence of keys on the faceplate of the telephone:

   Mute 4 6 8 # (Mute I N T #)

   Note:

   Press the **Mute** button momentarily. Do not press this button while pressing other keys/buttons.

2. After entry of the command sequence, telephones with an internal Ethernet switch display the following text, depending on the current interface control value:

   ```
   PHY1=status
   *=change #=OK
   ```

   where ***status*** is the value of PHY1STAT, defined as:

   - Status is **auto** when PHY1STAT = 1
   - Status is **10Mbps HDX** when PHY1STAT = 2
   - Status is **10Mbps FDX** when PHY1STAT = 3
   - Status is **100Mbps HDX** when PHY1STAT = 4

- Status is **100Mbps FDX** when PHY1STAT = 5

3. To change the PHY1 value, press *****.

   Depending on the current value, the next sequential valid PHY1 value is selected and displayed as the status. For example, if the current value is 10Mbps HDX (2), pressing ***** changes the value to 3 (10Mbps FDX).

4. Press the ***** button to terminate the procedure, or the # button to save the new value. If you press the # button, the following text displays:

   ```
   PHY2=status
   *=change #=OK
   ```

   where ***status*** is the value of PHY2STAT, defined as:

   - Status is **disabled** when PHY2STAT = 0
   - Status is **auto** when PHY2STAT = 1
   - Status is **10Mbps HDX** when PHY2STAT = 2
   - Status is **10Mbps FDX** when PHY2STAT = 3

- Status is **100Mbps HDX** when PHY2STAT = 4
- Status is **100Mbps FDX** when PHY2STAT = 5

5. To change the PHY2 value, press *****.

   Depending on the current value, the next sequential valid PHY2 value is selected and displayed as the status. For example, if the current value is 10Mbps HDX (2), pressing ***** changes the value to 3 (10Mbps FDX).

   The following text displays left-justified at the top of the display:

   ```
   Save new value?
   *=no      #=yes
   ```

6. Press the ***** button to terminate the procedure, or the # button to save the new values. If you press the # button, the following text displays.

   ```
   New value
   being saved
   ```

   The new values are saved and a restart occurs automatically. The user interface is restored to its previous state.

The View Administrative Option

If you are using static addressing and encounter problems, use the following procedure to verify the current values of system parameters and file versions.

Note:

Unless otherwise prevented using administration, the user can view but not change most of the parameters associated with Local Administrative Procedures. For more information about this option, see the applicable user guide(s).

Note:

If the View Network Information option is not available due to being disabled by administration, use the **ADDR** option to view IP addresses. See Static Addressing Installation on page 105. The IP addresses might have been entered incorrectly. Verify whether you were provided with correct IP addresses.

1. While the telephone is on-hook and idle, press the following sequence of keys on the faceplate of the telephone:

   Mute 8 4 3 9 # (Mute V I E W #)

   Note:

   > Press the **Mute** button momentarily. Do not press this key while pressing other keys.

   The following text displays left-justified at the top of the display:

   ```
   View settings
   *=next   #=exit
   ```

2. Press the ***** button at any time during viewing to display the next name and system value pair or filename from Table 15. The first pair returns after the last pair displays. Values that cannot display on one line wrap to the next line.

   Press the # button at any time during viewing to terminate the procedure and restore the user interface to its previous state. The names and values display in the following order:

Table 15: Parameter Values

Name	System Value	Format
Model	***16ccDccc***	Up to 8 ASCII characters: MODEL value.
Phone SN	***cccccccccccccccccc***	Telephone Serial Number, up to 18 ASCII characters.
PWB SN	***cccccccccccccccccc***	Printed Wiring Board (circuit board) Serial Number, up to 18 ASCII characters. Applies only to 16xx IP Telephones that have a software-readable PWB serial number and comcode.
PWB comcode	***nnnnnnnnn***	9 ASCII numeric characters. Applies only to 16xx IP Telephones that have a software-readable PWB serial number and comcode.
MAC address	***hh:hh:hh:hh:hh:hh***	Each octet of the MAC address displays as a pair of hexadecimal numbers.
		1 of 3

Table 15: Parameter Values (continued)

Name	System Value	Format
L2 tagging	***ccccccccc***	Up to 9 ASCII characters: “on” if NVL2Q = 1 “off” if NVL2Q = 2 “auto: on” if NVL2Q = 0 and 802.1Q tagging is on “auto: off” if NVL2Q = 0 and 802.1Q tagging is off
VLAN ID	***cccc***	Up to 4 ASCII characters. Value is L2QVLAN if 802.1Q tagging is on or “none” of 802.1Q tagging is off.
IP address	***nnn.nnn.nnn.nnn***	Up to 15 ASCII characters: IPADD value.
Subnet mask	***nnn.nnn.nnn.nnn***	Up to 15 ASCII characters: NETMASK value.
Router	***nnn.nnn.nnn.nnn***	Up to 15 ASCII characters: the IP address of the router in use.
File server	***nnn.nnn.nnn.nnn.nnnnn***	Up to 21 ASCII characters: IP address and port of last file server used successfully during initialization or “0.0.0.0” if no file server was used successfully.
Call server	***nnn.nnn.nnn.nnn.nnnnn***	Up to 21 ASCII characters: IP address and port of the call server currently in use, otherwise “0.0.0.0.”
802.1X	If DOT1X = 0 If DOT1X = 1 If DOT1X = 2	Pass-thru mode. Pass-thru with Logoff. Supplicant mode.
Group	***nnn***	Up to 3 ASCII numeric characters: GROUP value.
		2 of 3

Table 15: Parameter Values (continued)

Name	System Value	Format
Protocol:	***cccccccc***	Up to 8 ASCII characters.
	filename.ext	4 to 32 ASCII characters. The name of the primary ("big app") image file currently stored in the telephone (endptAPPINUSE).
	***cccccccc* Ethernet**	2 to 7 ASCII characters, either “100Mbps”, “10Mbps”, or “No” depending on the current speed of the Ethernet line interface.
	bootcodename	1 to 32 ASCII characters. The name of the backup ("little app") image file currently stored in the telephone (endptBOOTNAME).
		3 of 3

Static Addressing Installation

The usual way to assign IP addresses to IP telephones is the automatic method. There might be times, however, when manual assignment of IP addresses is desired.

⚠ **CAUTION:**

Static addressing is necessary when a DHCP server is unavailable.

Because of the increased opportunities for text entry errors associated with static addressing, we very strongly recommend that a DHCP server be installed and static addressing avoided.

Use the following procedure to invoke manual address information programming.

1. Start manual address programming by performing one of the following steps:

   a. During normal DHCP processing, press the ***** key while “`* to program`“ displays during the DHCP process.

   or

   b. While the telephone is on-hook and idle, press the following sequence of keys on the faceplate of the telephone:

   Mute 2 3 3 7 # (Mute A D D R #)

Note:

> Press the **Mute** button momentarily. Do not press this button while pressing other keys/buttons.

The telephone displays:

```
Phone=nnn.nnn.nnn.nnn
New=_
```

where ***nnn.nnn.nnn.nnn*** is the current IP address system value of the telephone.

2. Enter the **telephone's IP address** followed by the # button.

   The telephone displays:

   ```
   CallSv=nnn.nnn.nnn.nnn
   New=_
   ```

   where ***nnn.nnn.nnn.nnn*** is the current system value of the media server/gatekeeper IP address.

3. Enter the **call controller IP address** followed by the # button.

   Note:

   > The default transport and port settings when locally configuring the call controller are **TLS** and **5061**.

   The telephone displays:

   ```
   Router=nnn.nnn.nnn.nnn
   New=_
   ```

   where ***nnn.nnn.nnn.nnn*** is the current system value of the gateway/router IP address.

4. Enter the **Gateway router IP address** followed by the # button.

   The telephone displays:

   ```
   Mask=nnn.nnn.nnn.nnn
   New=_
   ```

   where ***nnn.nnn.nnn.nnn*** is the current system value of the IP netmask.

5. Enter the **IP netmask** followed by the # button.

   The telephone displays:

   ```
   FileSv=nnn.nnn.nnn.nnn
   New=_
   ```

   where ***nnn.nnn.nnn.nnn*** is the current system value of the HTTP/HTTPS server IP address.

6. Enter the **File server** followed by the # button.

   The telephone displays one of the following texts, depending on the current setting of the system parameter NVL2Q (802.1Q):

   If NVL2Q is 0:

   ```
   802.1Q=auto
   *=change #=OK
   ```

   If NVL2Q is 1:

   ```
   802.1Q=on
   *=change #=OK
   ```

   If NVL2Q is 2:

   ```
   802.1Q=off
   *=change #=OK
   ```

7. Press ***** to change **802.1Q** to the next sequential value. For example, if the current value is 0 (auto) pressing * changes it to 1 (on) and if the current value is 2 (off), pressing * changes it to 0 (auto).

   The display is updated to show the current status of 802.1Q.

8. Press the # button to continue the procedure without changing the displayed status of 802.1Q

   The telephone displays the following text:

   ```
   VLAN ID=dddd
   New=_
   ```

   where ***dddd*** is the current system value of the 802.1 VLAN ID.

9. Enter a valid value between 0 and 4094 for the new value of the 802.1 **VLAN ID**.

   The telephone displays the following message:

   ```
   VLAN test=ddd
   New=_
   ```

   where ***ddd*** is the number of seconds to wait for a **DHCPOFFER** on a non-zero VLAN.

10. Enter a valid value between 0 and 999 for the new value of the **DHCPOFFER** wait period.

    The telephone displays:

    ```
    Save new values?
    *=no #=yes
    ```

11. Press the # button to save the new values you entered.

    The telephone displays:

    ```
    New values
    being saved
    ```

    Once the new values are stored, the telephone is reset.

    If a new boot program is downloaded from the HTTP server after you enter static addressing information, you must reenter your static addressing information.

Disable/Enable Event Logging

Use the following procedure to enable or disable logging of system events.

Note:

To use event logging, you must configure a syslog server via a settings file.

1. While the telephone is on-hook and idle, press the following sequence of keys on the faceplate of the telephone:

   Mute 5 6 4 # (Mute L O G #)

   Note:

   Press the **Mute** button momentarily. Do not press this button while pressing other keys/buttons.

2. After entry of the command sequence, the telephone displays the following text, depending on the current value of the system parameter NVLOGSTAT:

   ```
   Log=status
   *=change #=OK
   ```

   where ***status*** is the type of logging indicated by the NVLOGSTAT value, defined as:

   - Status is **disabled** when NVLOGSTAT = 0
   - Status is **emergencies** when NVLOGSTAT = 1
   - Status is **alerts** when NVLOGSTAT = 2
   - Status is **critical** when NVLOGSTAT = 3

- Status is **errors** when NVLOGSTAT = 4
- Status is **warnings** when NVLOGSTAT = 5
- Status is **notices** when NVLOGSTAT = 6
- Status is **information** when NVLOGSTAT = 7
- Status is **debug** when NVLOGSTAT = 8

3. To change the logging status, press *.

   Depending on the current value, the next sequential valid NVLOGSTAT value is selected and displayed as the status. For example, if the current value is alerts (2), pressing ***** changes the value to 3 (critical). If the current value is debug (8), pressing ***** changes the value to 0 (disabled).

   If a value different from the current NVLOGSTAT value is entered, the following text displays left-justified at the top of the display:

   ```
   Save new value?
   *=no    #=yes
   ```

4. Press the * button to terminate the procedure, or the # button to save the new value. If you press the # button, the telephone displays the following text:

   ```
   New value being saved
   ```

   The telephone saves the new value.

Logoff

Use the following procedure to log off a telephone.

CAUTION:

Once a telephone is logged off, a password and extension might be needed to log back on.

1. While the telephone is on-hook and idle, press the following sequence of keys on the faceplate of the telephone:

   Mute 5 6 4 6 3 3 # (Mute L O G O F F #)

   Note:

   Press the **Mute** button momentarily. Do not press this button while pressing other keys/buttons.

2. After entry of the command sequence, the telephone unregisters from the call server. The telephone display clears and then displays the following prompt for subsequent login:

```
Enter Extension
EXT= #=OK
```

Self-Test Procedure

Note:

Replace variable w/ short product names store two software code images in reprogrammable non-volatile memory. The primary image, called the “big app” must be running to perform a self-test. The backup image, called the “little app” does not support the self-test.

For self-testing, use the following procedure:

1. To invoke Replace variable w/ short product name self-test procedures, press the following sequence of keys on the faceplate of the telephone:

   Mute 8 3 7 8 # (Mute T E S T #)

   Note:

   Press the **Mute** button momentarily. Do not press this button while pressing other keys/buttons.

   All telephones show the following text, left-justified at the top of the display, for 1 second after self-test is invoked:

   ```
   Self test
   #=end
   ```

   A block character with all pixels on then displays in all display character locations for 5 seconds. Display of the block character helps to find bad display pixels.

   The telephone displays one of the following:

   If self-test passes:

   ```
   Self test passed
   #=end
   ```

   If self-test fails:

   ```
   Self test failed
   #=end
   ```

2. To terminate the self-test, press the # button on the dial pad at any time. Doing so generates a confirmation tone, and returns the user interface to its previous state.

Language Selection

1603SW-I SIP IP Deskphones are factory-set to display information in the English language. All software downloads include language files for six additional languages. Administrators can specify one of those languages per telephone to replace English.

All downloadable language files contain:

- UTF-16 encoded Unicode characters (only)
- a file name ending in .txt. (This is the language file.)
- a file name ending in .lzma. (This is the font file.)
- the language name as it should be presented to the user for selection
- a translation of each available language name into all other languages
- an indication of the preferred character input method as shown in Table 16
- text string replacements for the built-in English text strings, for example, entry prompts and error messaged
- an indication of the font corresponding to the language

Note:

> The 1603SW-I SIP IP Deskphones also require a font file (*.lzma) that must be paired with the language file. Both the language file and corresponding font file must reside on the HTTP server.

Table 16: Language Files Available with Software Downloads for 1603SW-I SIP IP Deskphones

Language	Character Input Method to be specified in each respective language file	Font
Arabic	Latin-1	Arabic/Hebrew
Chinese - Simplified	Latin-1	Simplified Chinese
Chinese - Traditional	Latin-1	Traditional Chinese
Hebrew	Latin-1	Arabic/Hebrew
Japanese Katakana	Latin-1	Default
Korean	Latin-1	Korean

Note:

The 1603SW-I SIP IP Deskphones also support half-width Katakana.

There are no dependencies between the languages available from the software download and the actual character input method. If a character input method is not supported, ASCII is used instead. Acceptable input methods are as follows:

- ASCII
- Arabic
- Chinese - Simplified
- Chinese - Traditional
- Hebrew
- Korean

Use the configuration file and these parameters to customize the settings for one language:

- **FONTFILE** - The name of the selected font file for a language to be downloaded. You must specify this parameter for any language except Japanese Katakana. For example, to use Arabic, the setting is: **SET FONTFILE Arabic_b004i.rbm.lzma**.

  Note:

  Arabic and Hebrew share one font file.

- **LANGxFILE** - The name of a selected language file. In addition to providing the language name as this value, replace the "x" in this parameter with a "1" For example, to use Arabic, the setting is: **SET LANG1FILE=mlf_arabic_b004i.txt**.
- **LANG0STAT** - Allows the user to select the built-in English language when other languages are downloaded. If LANG0STAT is "0" and at least one language is downloaded, the user cannot select the built-in English language. If LANG0STAT is "1" the user can select the built-in English language text strings.
- **LANGSYS** = The file name of the system default language file, if any.

To view multiple language strings, see the MLS local procedure in the *Avaya one-X™ Deskphone Value Edition SIP for 1603SW-I IP Deskphones Installation and Maintenance Guide*.

Note:

Keep in mind the following information:

- Specifying a language other than English in the configuration file has no impact on Avaya Aura Communication Manager settings, values, or text strings.
- You can download only one language (with the corresponding font file and language file) at a time.
- The font files for the five languages also contain the font information for the languages supported on the 1600 Series Global Telephones.

- You can use the GROUP feature to logically separate the 1600 Series Global Telephones from the 1600 Series International Telephones in one enterprise network by specifying different language/font files in the 46xxsettings.txt file.

Setting the Dial Plan on SIP IP Telephones

Note:

This section only applies to operations with a secondary controller where SM/ PPM is not available.
In a failover situation, the dial plan is played locally even if a proxy connection is not available; the user may hear a dial tone but cannot make a call.

During manual dialing, a dial plan allows a call to be initiated without using a **Send** button and without waiting for the expiration of a timeout interval. The dial plan consists of one or more format strings. When the dialed digits match a format string in the DIALPLAN configuration parameter, the call is initiated. (In an SM environment, PPM retrieves the equivalent dial plan information in another format, thus the dial plan information from CM).

Valid characters in a format string, and their meanings, are as follows:

digits 0 through 9, inclusive = Specific dialpad digits
***** = the dialpad character *
= the dialpad character # (but only if it is the first character in the dialed string – see below)
x = any dialpad digit (i.e., 0-9)
Z or **z** = present dial tone to the user (for example, for Feature Access Code (FAC) entry)
[ ] = any one character within the brackets is a valid match for a dial plan string
- = any one digit between the bounds within the brackets, inclusive, is a match
+ = the character following the + can repeat 0 or more additional times, for a valid match

An individual valid dial plan is any combination of the above characters. If there are multiple valid dial plans, separate each one from the next using an OR symbol ("|"). If the dial plan text string begins or ends with an OR symbol, that symbol is ignored. Users cannot modify the dial plan.

Dial plan example:

“[2-4]xxx|[68]xxx|*xx|9Z1xxxxxxxxxx|9z011x+”

where:

[2-4]xxx: Four-digit dial extensions, with valid extensions starting with 2, 3, or 4;
[68]xxx: Four-digit dial extensions, with valid extensions starting with 6 or 8;
***xx**: Two-digit Feature Access Codes, preceded by a *;
9Z1xxxxxxxxxx: Network Access Code ("9 for an outside line"), followed by dial tone, followed by any string of 10 digits– typical instance of Automatic Route Selection (ARS) for standard US long distance number;
9z011x+: Network Access Code ("9 for an outside line"), followed by dial tone, followed by at least one digit – typical instance of Automatic Route Selection (ARS) for US access to international numbers of unknown, and variable, length.

An additional parameter that affects dialing is:

COUNTRY - Country of operation for specific dial tone generation.

Setting the Date and Time on SIP IP Telephones

SIP IP telephones need a source of date and time information. This typically comes from a network time server running the Simple Network Time Protocol (SNTP). The deskphones use several administrative parameters for this functionality. The parameter SNTPSRVR defines the server's IP Address(es). GMTOFFSET defines the offset from Greenwich Mean Time (GMT). DSTSTART and DSTSTOP define the start and end of Daylight Savings Time, respectively. DSTOFFSET defines the Daylight Savings Time offset from Standard Time. Finally, DATETIMEFORMAT defines the format of the date and time display. See Table 11 for definitions and valid values for SIP Date and Time parameters.

Failover/Failback Behavior

For survivability with the 1603SW-I SIP IP Deskphones, you can provision a list of controllers. If more than one controller has been provisioned, the deskphone will attempt to register with the highest-priority controller on the list. If there is a failure to register, the deskphone will then attempt to register with the next controller on the list. Note that the deskphone will not failback automatically. (The deskphone will continue to work with the failover controller.) If the higher-priority controller becomes available, the deskphone must be manually rebooted or the user must log out and log in again to attempt to register with the higher-priority controller.

Appendix A: Glossary of Terms

802.1P **802.1Q**	802.1Q defines a layer 2 frame structure that supports VLAN identification and a QoS mechanism usually referred to as 802.1P.
802.1X	Authentication method for a protocol requiring a network device to authenticate with a back-end Authentication Server before gaining network access. Applicable 1600 Series IP telephones support IEEE 802.1X for pass-through and for Supplicant operation with the EAP-MD5 authentication method.
ARP	Address Resolution Protocol, used, for example, to verify that the IP address provided by the DHCP server is not in use by another IP telephone.
CELP	Code-excited linear-predictive. Voice compression requiring only 16 kbps of bandwidth.
CLAN	Control LAN, type of Gatekeeper circuit pack.
CNA	Converged Network Analyzer, an Avaya product to test and analyze network performance.
DHCP	Dynamic Host Configuration Protocol, an IETF protocol used to automate IP address allocation and management.
DiffServ	Differentiated Services, an IP-based QoS mechanism.
DNS	Domain Name System, an IETF standard for ASCII strings to represent IP addresses. The Domain Name System (DNS) is a distributed Internet directory service. DNS is used mostly to translate between domain names and IP addresses. Avaya 1600 Series IP Telephones can use DNS to resolve names into IP addresses. In DHCP, TFTP, and HTTP files, DNS names can be used wherever IP addresses were available as long as a valid DNS server is identified first.
Gatekeeper	H.323 application that performs essential control, administrative, and managerial functions in the media server. Sometimes called CLAN in Avaya documents.
H.323	A TCP/IP-based protocol for VoIP signaling.
HTTP	Hypertext Transfer Protocol, used to request and transmit pages on the World Wide Web.
HTTPS	A secure version of HTTP.
IETF	Internet Engineering Task Force, the organization that produces standards for communications on the internet.
LAN	Local Area Network.
LLDP	Link Layer Discovery Protocol. All IP telephones with an Ethernet interface support the transmission and reception of LLDP frames on the Ethernet line interface in accordance with IEEE standard 802.1AB.
MAC	Media Access Control, ID of an endpoint.

1 of 2

Media Channel Encryption	Encryption of the audio information exchanged between the IP telephone and the call server or far end telephone.
NAPT	Network Address Port Translation.
NAT	Network Address Translation.
OPS	Off-PBX Station.
PHP	Hypertext Preprocessor, software used to assist in the format and display of Web pages.
PSTN	Public Switched Telephone Network, the network used for traditional telephony.
QoS	Quality of Service, used to refer to several mechanisms intended to improve audio quality over packet-based networks.
RSVP	Resource ReSerVation Protocol, used by hosts to request resource reservations throughout a network.
RTCP	RTP Control Protocol, monitors quality of the RTP services and can provide real-time information to users of an RTP service.
RTP	Real-time Transport Protocol. Provides end-to-end services for real-time data such as voice over IP.
SDP	Session Description Protocol. A well-defined format for conveying sufficient information to discover and participate in a multimedia session.
Signaling Channel Encryption	Encryption of the signaling protocol exchanged between the IP telephone and the call server. Signaling channel encryption provides additional security to the security provided by media channel encryption.
SIP	Session Initiation Protocol. An alternative to H.323 for VoIP signaling. This protocol is not applicable to 1600 Series IP Telephones.
SNTP	Simple Network Time Protocol. An adaptation of the Network Time Protocol used to synchronize computer clocks in the internet.
TCP/IP	Transmission Control Protocol/Internet Protocol, a network-layer protocol used on LANs and internets.
TFTP	Trivial File Transfer Protocol, used to provide downloading of upgrade scripts and application files to certain IP telephones.
TLS	Transport Layer Security, an enhancement of Secure Sockets Layer (SSL). TLS is compatible with SSL 3.0 and allows for privacy and data integrity between two communicating applications.
UDP	User Datagram Protocol, a connectionless transport-layer protocol.
Unnamed Registration	Registration with Avaya Aura Communication Manager by an IP telephone with no extension. Allows limited outgoing calling.
VLAN	Virtual LAN.
VoIP	Voice over IP, a class of technology for sending audio data and signaling over LANs.

2 of 2

Appendix B: Related Documentation

IETF Documents

IETF documents provide standards relevant to IP Telephony and are available for free from the IETF Web site: http://www.ietf.org/rfc.html.

ITU Documents

Access the ITU Web site for more information about ITU guidelines and documents, available for a fee from the ITU Web site: http://www.itu.int.

ISO/IEC, ANSI/IEEE Documents

Access the ISO/IEC standards Web site for more information about IP Telephony standards, guidelines, and published documents: http://www.iec.ch.

Appendix C: Countries With Specific Network Progress Tones

Overview

The 1603SW-I SIP IP Deskphones provide country-specific network progress tones which are presented to the user at appropriate times. The tones are controlled by administering the COUNTRY parameter for the country in which the telephone will operate. Each Network Progress Tone has six components, as follows:

- Dialtone
- Ringback
- Busy
- Congestion
- Intercept
- Public Dialtone

All countries listed in this appendix are applicable to the 1603SW-I SIP IP Deskphones. Some of the dialtone entries have changed from previous releases to be distinctively different than the Public dialtone entries.

Country List

The 1603SW-I SIP IP Deskphones support the following countries:

- United States (Use the keyword **USA**.)
- United Kingdom (Use the keyword **UK**.)
- Canada (Use the keyword **USA**.)
- Germany
- France
- Italy
- Japan
- Russia
- Brazil

- India
- Mexico
- South Africa

Index

Numerical

1600 Series IP Telephones
  Initialization Process 18
1603SW-I SIP IP Deskphones
  Administering Options for 73
  Administration Alternatives and Options 13
  Restart 99
  Upgrade and Application Files 64
1603SW-I SIP IP Deskphones Feature Support . . . 36
16xxupgrade.txt file 65
802.1X 88

A

About This Guide 7
ADDR Option 105
Administering Avaya Communication Manager. . . . 31
Administering Features 42
Administering Telephone Options 73
Administration Alternatives and Options for 1603SW-I SIP IP Deskphones 13
Administration, for Avaya Communication Manager . 31
Administration, for SES. 43
Administration, for Session Manager 43
Administration, for Telephones on server 36
Administrative Checklist 16
Administrative Options, Local 96
Administrative Process, The 15
Administrative Requirements, for Communication Manager 32
Alternatives, Administration 13
ANSI/IEEE Documents 117
Application Files and Telephone Software 63
Application-specific parameters, administering . . . 13
Assessment, of Network 21

B

Binary and Upgrade Files for 1603SW-I SIP IP Deskphones 64
Binary File and Upgrade File, Choosing 64
Binary Files 64
button labels. 42

C

Call Server Requirements 31
Call Transfer Considerations 35
Checklist, Administrative 16
Clear Procedure 96
CM/SIP Configuration Requirements. 37
Communication Manager Administration 31
Communication Manager Administrative Requirements. 32
Communication Manager/SIP IP Telephone Configuration Requirements 37
Conferencing Call Considerations 36
Configuration Requirements, CM/SIP 37
Contents of the Settings File 67
Countries With Network Progress Tones 119
Customizeable System Parameters 74

D

Date and Time, Setting on SIP IP Telephones 114
Date, Setting on SIP IP Telephones 114
Debug Procedure. 97
DHCP and File Servers 47
DHCP Generic Setup 50
DHCP options 50
DHCP Parameters Set by 49
DHCP Server 23
DHCP Server to Telephone initialization 18
DHCP Server, Windows 2000 Setup. 57
DHCP Server, Windows NT 4.0 Setup 54
DHCP, Configuring 48
Dial Plan, Setting on SIP IP Telephones 113
DIFFSERV. 35
Disable Event Logging 108
DNS Addressing 88
Document Organization 8
Documentation, Related 9, 117, 119

E

Enable Event Logging 108
Error Conditions 19
Event Logging 108

F

Failover 114
Failover/Failback Behavior 114
Features, Administering 42
File download
    Choosing the Right Binary and Upgrade Files . . 64
    Download File Content 65
from. 42

G

General Download Process. 63
Generic Setup, for DHCP. 50
Glossary of Terms 115
Group Identifier 97
GROUP System Value 70

H

Hardware Requirements 21
HTTP/HTTPS Server. 23

I

IEC/ISO Documents 117
IEEE 802.1D and 802.1Q. 25, 34
IEEE/ANSI Documents 117
IETF Documents. 117
Initialization Process, for 1603SW-I SIP Deskphones. 18
Installation, Network Information Required before
  installing 23
Interface Control 100
Interface, administering the 13
IP Addresses, administering 13
IP Interface and Addresses 34
ISO/IEC, ANSI/IEEE Documents 117
ITU Documents 117, 119

L

Language Selection 111
Link Layer Discovery Protocol (LLDP) 91
LLDP Data Units Transmitted 92
Local Administrative Options 96
LOG Procedure 108
Logoff Procedure 109

N

Network Assessment. 21
Network Considerations, Other 24
Network Information, Required 23
Network Progress Tones, Country List 119
Network Requirements 21
Network Time Protocol Server. 23
Network Time Server 13

O

Options, Administering 73
Options, entering using the Telephone Dialpad 96
Options, for 1603SW-I SIP IP Deskphones
  Administration 13
Other Network Considerations. 24

P

Parameter Values 103
Pass-Through and Proxy Logoff, 802.1X 90
Port Utilization
    Selection 34
    TCP/UDP 26
Proxy Logoff and Pass-Through, 802.1X 90

Q

QoS 25, 34
    Administrative Parameters 13
    IEEE 802.1D and 802.1Q 34

R

Related Documentation 117, 119
Requirements 11
    Call Server 31
    Hardware 21
    Network 21
    Server 22
Reset System Values 98
RSVP and RTCP 34
RTCP and RSVP 34

S

Security 30
Server Administration 47
Server Administration, DHCP 48
Server Requirements 22
SES Server 19
Settings File 65
Settings File, Contents 67
SIP Enablement Services (SES) Administration . . . 43
SNMP 24
SNTP Server. 23
Software 63
Software Checklist 47

Software, Telephone 63
SRTP 11, 81
Static Addressing
    Installation 105
Station Number Portability 26
Supplicant Operation, 802.1X 90
Switch Compatibility 31
System Parameter Values, Impact of Received TLVs. 94
System Parameter Values, troubleshooting 103
System Parameters, Customizeable 74
System Values, Reset 98

T

Tagging and VLAN, administering. 13
TCP/UDP Port Utilization 26
Telephone Administration 13, 36
Telephone and File Server initialization 18
Telephone and SES Server initialization 19
Telephone Initialization Process 18
Telephone Options, Administering 73
Telephone Software and Application Files 63
Telephone to Network initialization 18
Terms, Glossary of 115
TEST Procedure 110
Time and Date, Setting on SIP IP Telephones 114
Time, Setting on SIP IP Telephones. 114
TLS 26, 61
TLVs Received, Impact on System Parameter Values 94
Troubleshooting
    Parameter Values 103
    VIEW Administrative Option 102

U

UDP Port Selection 34
UDP/TCP Port Utilization 26
Upgrade and Binary Files, Choosing the Right 64
Upgrade and Binary Files, for 1603SW-I SIP IP Deskphones 64
Upgrade File (16xxupgrade.txt) 65

V

VIEW Administrative Option 102
VLAN Considerations 83
VLAN Default Value 85
VLAN Separation 86
VLAN Separation Rules 87
VLAN tagging 84