Avaya one-X™ Deskphone Edition for 9600 Series SIP IP Telephones Administrator Guide Release 2.0

16-601944
Issue 2
December 2007

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

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

About This Guide

This guide is for personnel who administer Avaya Communication Manager, DHCP, HTTP/HTTPS servers for 9600 Series SIP IP Telephones, a Local Area Network (LAN), SIP Enablement Services (SES) or a Network Time server.

The 9600 Series IP Telephones use Internet Protocol (IP) technology with Ethernet line interfaces and support both SIP and H.323 protocols. The 9600 Series IP Telephones provide support for DHCP, HTTP, and HTTPS over IPv4/UDP, which enhance the administration and servicing of the telephones. These telephones use DHCP to obtain dynamic IP Addresses, and HTTPS or HTTP to download new versions of software or customized settings for the telephones.

Important:

This document covers administration for 9600 Series SIP IP Telephones only. For administration for 9600 Series IP Telephones using the H.323 protocol, see the *Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Administrator Guide* (Document Number 16-300698), available at: www.avaya.com/support.

This document does not cover administration for Avaya Distributed Office. Full documentation for Avaya Distributed Office is available on the Avaya support Web site, www.avaya.com/support.

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 9600 Series IP and/or SIP IP Telephone system. If the servers are not functioning correctly, the 9600 Series IP Telephones might not operate correctly.

Major Differences Between 9600 Series SIP IP and 9600 Series H.323 IP Telephones

Review this section if your administrative environment includes both SIP and H.323 signaling protocols for 9600 Series IP Telephones.

General IP Telephony - Two major protocols handle Voice over IP (VoIP) signaling, Session Initiation Protocol (SIP) and H.323. The two protocols provide connection control and call progress signaling, but in very different ways. These protocols can be used simultaneously over the same network, but in general, no endpoint supports both protocols at the same time. Neither protocol is necessarily superior, but each offers some unique advantages. SIP telephones, for example, do not require centralized call servers, and can route telephone calls when a URL identifies the destination. H.323 telephones leverage the call server's presence into the potential availability of hundreds of telephone-related features that a standalone SIP telephone cannot provide.

Signaling - 96xx Series IP Telephones ship from the factory with H.323 signaling. To use the SIP protocol, applicable H.323 96xx Series IP Telephones must be appropriately converted and configured. See the *Avaya one-X™ Deskphone Edition for 9600 Series SIP IP Telephones Installation and Maintenance Guide* for detailed conversion/configuration information.

Avaya Communication Manager Release - 9600 Series SIP IP Telephones are supported only by Communication Manager Release 4.0 and greater. SIP telephones use Avaya OPS (Outbound SIP Proxy) features on the "trunk" side of Avaya Communication Manager whereas the H.323 (IP) telephones are supported on the "line" side of the Communication Manager. When a 9600 Series SIP IP Telephone is running under Communication Manager Release 5.0, an additional feature, Extend Call, is available.

Required Servers - SIP 9600 Series IP Telephones use two [additional] servers that H.323 telephones do not:

- SIP Proxy server - provided by SIP Enablement Services (SES) software, and
- Network Time server - which controls time-related parameters.

These servers are not necessarily separate hardware units.

Features & Functions supported by H.323 9600 Series IP Telephones, <u>Not</u> **Supported by SIP** - Button modules are not currently supported by 9600 SIP IP Telephones.

Backup/Restore - 9600 Series (H.323) IP Telephones use HTTP to store backup files. 9600 Series SIP IP Telephones use the Personal Profile Manager (PPM) functionality within SIP Enablement Services (SES) for backup and restore functions.

Settings File & System Parameters - Both SIP and H.323 9600 Series IP Telephones (and 4600 Series IP Telephones) use the same settings file. Some of the same system parameters are used, however, numerous SIP-specific parameters support SIP operation only. In H.323 9600 Series IP Telephones, the parameters OPSTAT and APPSTAT control all user interface functions, whereas 9600 Series SIP IP Telephones use a separate parameter (for example ENABLE_CONTACTS, ENABLE_CALLLOG) for each user interface function.

Language Support - SIP telephones support the same languages as H.323 telephones, with the exception of Hebrew. SIP does not support Hebrew or the English Large Text Font for any language. Further, all SIP language files have **.xml** file extensions whereas H.323 language files have **.txt** file extensions.

SNMP & MIBs - Although both SIP and H.323 telephones support SNMP v2c and have custom Management Information Bases (MIBs), the MIBs are formatted somewhat differently.

RSVP & VMON (VMM) - 9600 Series SIP IP Telephones do not use RSVP (Resource ReSerVation Protocol) software to provide real-time monitoring and historical data of audio quality for VoIP calls. 9600 Series SIP IP Telephones do support Avaya Voice over IP (VoIP) Monitoring Manager (VMON, now called VMM). 9600 Series IP Telephones use both RSVP and VMON.

QoS - Unlike H.323 telephones, 9600 Series SIP IP Telephones do not use Avaya Communication Manager to set Quality of Service (QoS). The SIP IP telephones use the parameters L2QAUD, L2QSIG, DSCPAUD, and DSCPSIG (described in Table 11: 9600 Series SIP IP Telephones Customizeable System Parameters).

NAT - 9600 Series SIP IP Telephones do not support Network Address Translation (NAT); 9600 Series IP (H.323) Telephones do support NAT.

Features & Functions Supported by H.323 and Not Supported by SIP:

SIP Software Release 2.0	SIP Software Release 1.0
• Calltype Digit Conversion • RSVP • Remote Ping & Trace Route • SBM24 Button Modules • Push (Top Line, web page, and/or audio)	• Link Layer Discovery Protocol (LLDP) • GigE (Gigabit Ethernet) • Calltype Digit Conversion • IEEE 802.1X • RSVP • VMON • Remote Ping & Trace Route • Web browser • SBM24 Button Modules • Push (Top Line, web page, and/or audio) • Autodial feature buttons

Change History

Issue 1	This document was issued for the first time in May 2007 to support the first release of 9600 Series SIP IP Telephones.
Issue 2	This is the current version of the document, revised and issued in December, 2007 to support SIP IP Software Release 2.0. This release provides the 9600 SIP IP Telephones with similar functionality to their H323 9600 IP Telephone counterparts, despite their signaling protocol differences. Release 2.0 introduces several new functions, new configuration parameters, and adds telephone models 9630G and 9640G. What's New in SIP Software Release 2.0 describes this release in more detail.

What's New in SIP Software Release 2.0

New material in this issue to support SIP Release 2.0 software includes:

New GigE Models Support SIP - This release extends SIP capability to two additional telephones, the 9630G and 9640G. Both models provide built-in Gigabyte Ethernet (GigE) support, but are otherwise identical to their 9630 and 9640 SIP IP telephone counterparts.

Language Support - 9600 Series SIP IP Telephones now support 13 languages. See Language Selection on page 107 for more information.

Emergency Button - Administrators can now program an "Emergency" number using the new PHNEMERGNUM parameter. Users can dial the Emergency Number whether or not they are logged into the telephone from which they are calling for assistance. For more information, see Emergency Number Administration.

Administration Enhancements - SIP Software Release 2.0 supports functionality introduced on Avaya Communication Manager Release 5.0 and SIP Enablement Services (SES) Release 5.0.

Visiting User Support - Visiting user support allows users to easily move between geographic locations while retaining their telephone extension and settings. 9600 Series SIP IP Telephones can be provisioned through the settings file VU_MODE configuration parameter to one of three modes:

- No Visiting User - the telephone operates "normally" and has no user interface impact for normal operation. The telephone can be forced to a "registered Inactive" state when a visiting user registers elsewhere.
- Optional Visiting User - the telephone prompts the user at registration time if they are visiting or not.
- Forced Visiting User - the telephone allows only visiting user registrations.

For more information, see Visiting User Administration.

Link Layer Discovery Protocol (LLDP) - 9600 Series SIP IP Telephones now support link layer discovery protocol. See Link Layer Discovery Protocol (LLDP) for information.

802.1X - 9600 Series SIP IP Telephones now support IEEE standard 802.1X for increased security. The new configuration parameter DOT1X defines the 802.1X operational mode. The new parameter DOT1XSTAT enables/disables 802.1X. The new parameter DOT1XEAPS specifies the authentication method to use with 802.1X. These parameters can be set through the settings file or on a per-phone basis using a local Craft procedure.

Support for Non-Avaya (Third Party) Environments - Several parameters, most notably ENABLE_AVAYA_ENVIRONMENT, have been added to cover operation for either:

- an Avaya environment, which provisions SIP/AST features and uses Personal Profile Manager (PPM) for download and backup/restore, or
- a non-Avaya mode, which complies with 3rd party standard SIP proxy with provision for SIPPING 19 feature.

WML Applications/Browser - 9600 Series SIP IP Telephones now provide access to WML applications via a WML Browser, as described in Chapter 9: Administering Applications and Options.

New, Revised, and Deleted Configuration Parameters - The following configuration parameters have been added for this release and are linked to the table that describes them in detail:

- CALL_TRANSFER_MODE
- CALLFWDADDR
- CALLFWDDELAY
- CALLFWDSTAT
- CNAPORT
- CNASRVR
- CONFIG_SERVER_SECURE_MODE
- COVERAGEADDR
- DIALPLAN
- DOT1X
- DOT1XEAPS
- DOT1XSTAT
- ENABLE_AVAYA_ENVIRONMENT
- INTER_DIGIT_TIMEOUT (replaces INTER_DIGIT_DIALING_TIMEOUT_DURATION)
- LAST_LOGIN_STATUS (system-set only)
- LLDP_ENABLED
- MWISRVR
- NO_DIGITS_TIMEOUT
- PHNEMERGNUM
- PHNNUMOFSA
- POE_CONS_SUPPORT
- PRESENCE_SERVER
- PROVIDE_EDITED_DIALING
- PROVIDE_EXCHANGE_CALENDAR
- PROVIDE_EXCHANGE_CONTACTS
- QKLOGINSTAT
- RTCPCONT

- RTCPMON
- RTCPMONPORT
- SIP_MODE
- SIPCONFERENCECONTINUE
- TLSSRVRID
- VU_MODE
- VU_TIMER
- WMLEXCEPT
- WMLHOME
- WMLIDLETIME
- WMLIDLEURI
- WMLPORT
- WMLPROXY

The following parameters have been modified or renamed:

- Parameters PHYxDUPLEX and PHYxSPEED were combined. PHY1SPEED has been renamed to PHY1_OPERATIONAL_MODE. This parameter now includes the current duplex mode. PHY2SPEED has been renamed to PHY2_OPERATIONAL_MODE. This parameter now includes the current duplex mode.
- The OUTBOUND_SUBSCRIPTION_REQUEST_DURATION default value has been changed from 17280000 to 86400 seconds. This parameter can now be set through the settings file.
- The dimensions for SNTP_SYNC_INTERVAL and SNTP_SYNC_RANDOMIZATION_INTERVAL have changed from seconds to minutes.
- EXCHANGE_CONTACTS_ENABLED has been renamed to USE_EXCHANGE_CONTACTS.
- EXCHANGE_CALENDAR_ENABLED has been renamed to USE_EXCHANGE_CALENDAR.
- The default value definition of ENABLE_G726 has changed from 0 to 1.
- The default values and sidetone definitions of the audio parameters AUDIOSTHD and AUDIOSTHS have been modified.
- WAIT_FOR_REGISTRATION_TIMER can now be set through the settings file.

The following configuration parameters are no longer valid and have been removed:

- PHY1DUPLEX
- PHY2DUPLEX
- INTER_DIGIT_DIALING_TIMEOUT_DURATION

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: Communication Manager Administration	Describes how to administer Avaya Communication Manager to operate with 9600 Series SIP IP Telephones.
Chapter 5: SIP Enablement Services (SES) Administration	Covers SIP Enablement Services (SES) configuration for 9600 Series SIP IP Telephones.
Chapter 6: Server Administration	Describes DHCP and HTTP/HTTPS administration for the 9600 Series IP Telephones.
Chapter 7: Telephone Software and Binary Files	Describes telephone 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 9600 Series SIP IP Telephones. Covers backup and restoration of telephone data. Also describes how to use local procedures to customize a single telephone from the dialpad.
Chapter 9: Administering Applications and Options	Describes customizeable application-specific parameters, to provide administrative control of telephone functions and options.
Appendix A: Glossary of Terms	Provides a glossary of terms used in this document or which can be applicable to 9600 Series SIP IP Telephones.
Appendix B: Related Documentation	Provides references to Web sites with external documents that relate to telephony in general, and can provide additional information about specific aspects of the telephones.
Appendix C: Sample Station Forms	Provides examples of Avaya Communication Manager forms related to system wide and individual telephone administration.

Other Documentation

See the Avaya support site at http://www.avaya.com/support for 9600 Series SIP IP Telephone technical and end user documentation.

See Appendix B: Related Documentation for Web sites that list related, 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

9600 Series IP Telephones

The 9600 Series IP Telephones 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 Secure Real Time Transfer Protocol (SRTP)
- Real Time Control Protocol (RTCP) and Secure Real Time Control Protocol (SRTCP)

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 9600 Series SIP IP Telephones support Media Encryption (SRTP) and use built-in Avaya SIP Certificates for trust management. Trust management involves downloading certificates for additional trusted Certificate Authorities (CA) and the policy management of those CAs. Identity management is handled by Simple Certificate Enrollment Protocol (SCEP) with phone certificates and private keys.

The 9600 Series IP Telephones are loaded with either H.323 or SIP software as part of initial script file administration and initialization during installation. Post-installation, software upgrades automatically download using the proper signaling protocol.

The parameters under which the 9600 Series SIP IP Telephones need to operate are summarized as follows:

- Telephone Administration on the Communication Manager (CM) call server, as covered in Chapter 4: Communication Manager Administration.
- Administration on SIP Enablement Services (SES), as covered in Chapter 5: 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 Edition for 9600 Series SIP IP Telephones 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 29 and QoS on page 40.
- 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 Edition for 9600 Series SIP IP Telephones 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 Web-specific information required for the optional Web browser application.

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

- Maintaining the information on the call server.
- Manually entering the information by means of the telephone dialpad.
- 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.

Table 1: Administration Alternatives and Options for 9600 Series SIP IP Telephones

Parameter(s)	Administrative Mechanisms	For More Information See:
Telephone Administration	Avaya Communication Manager and SES	Chapter 4: Communication Manager Administration, Chapter 6: Server Administration, and Appendix B: Related Documentation.
IP Addresses	DHCP (strongly recommended)	DHCP and File Servers on page 53, and especially DHCP Server Administration on page 54.
	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 Edition for 9600 SIP IP Telephones Installation and Maintenance Guide.*
	LLDP	Link Layer Discovery Protocol (LLDP) on page 101.
Tagging and VLAN	LLDP	Link Layer Discovery Protocol (LLDP) on page 101.
	DHCP	DHCP Server Administration on page 54, and Chapter 8: Administering Telephone Options.
	Settings file	DHCP and File Servers on page 53 and Chapter 8: Administering Telephone Options.
	Manual administration at the telephone	"Static Addressing Installation" in the *Avaya one-X™ Deskphone Edition for 9600 SIP IP Telephones Installation and Maintenance Guide*.
Network Time Server (NTS)	DHCP Settings file	DHCP Server Administration on page 54 and Network Time Protocol (NTP) Server on page 27.
Quality of Service	Settings file	Chapter 8: Administering Telephone Options.
Interface	DHCP	DHCP and File Servers on page 53, and Chapter 7: Telephone Software and Binary Files.
	Settings file (strongly recommended)	DHCP and File Servers on page 53, and Chapter 7: Telephone Software and Binary Files.
	LLDP	Link Layer Discovery Protocol (LLDP) on page 101.
	Manual administration at the telephone	"Secondary Ethernet Interface Enable/Disable" in the *Avaya one-X™ Deskphone Edition for 9600 SIP IP Telephones Installation and Maintenance Guide*.
Application - specific parameters	DHCP	DHCP and File Servers on page 53, and especially DHCP Server Administration on page 54. Also, Chapter 8: Administering Telephone Options.
	Settings file (strongly recommended)	DHCP and File Servers on page 53, and especially HTTP Generic Setup on page 66. Also, Chapter 8: Administering Telephone Options.

General information about administering DHCP servers is covered in DHCP and File Servers on page 53, and more specifically, DHCP Server Administration on page 54. 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 9600 Series SIP IP Telephones, you can administer a given parameter in a number of ways. If a given parameter is administered through different mechanisms, the last server to provide the parameter has precedence. The precedence, from lowest to highest, is:

1. LLDP
2. DHCP
3. Settings file
4. Personal Profile Manager (PPM),

   Note:

   Exception: In the case of the parameter SIPDOMAIN, the settings file has a higher precedence than PPM.

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 Craft 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 at all. 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 101.

The Administrative Process

The following list depicts administration for a typical 9600 Series SIP IP Telephone network. Your own configuration might differ depending on the servers and system you have in place.

1. Avaya Communication Manager (4.0 or greater) administered for 9600 Series IP Telephones. All 9600 Series SIP IP Telephones must be administered with the 4620SIP station type.
2. SES (SIP Enablement Services) administered.
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. 9600 Series Telephones installed. For more information, see the *Avaya one-X™ Deskphone Edition for 9600 SIP IP Telephones Installation and Maintenance Guide*.
7. Individual 9600 Series IP Telephones updated using Craft procedures, as applicable. For more information, see “Local Administrative Procedures” in the *Avaya one-X™ Deskphone Edition for 9600 SIP P Telephones Installation and Maintenance Guide*.

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 is licensed and is administered for Voice over IP (VoIP).	Chapter 4: Communication Manager Administration.
	Verify the individual telephones are administered as desired.	Chapter 4: Communication Manager Administration.
Administer the Proxy Server	Administer for SIP Enablement Services (SES).	*Installing and Administering SIP Enablement Services* (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 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 DHCP 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.
Binary file(s), script 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 72 and the *Avaya one-X™ Deskphone Edition for 9600 SIP IP Telephones Installation and Maintenance Guide.*
	Individually:	The applicable Craft Local Procedures in the *Avaya one-X™ Deskphone Edition for 9600 SIP IP Telephones Installation and Maintenance Guide.*

1 of 2

Table 2: Administrative Checklist (continued)

Task	Description	For More Information See:
Installation of telephones in the network		*Avaya one-X™ Deskphone Edition for 9600 SIP IP Telephones Installation and Maintenance Guide*.
Allow user to modify Options, if applicable	Set the following parameters in the settings file: ENABLE_CALL_LOG ENABLE_CONTACTS ENABLE_MODIFY_CONTACTS ENABLE_PRESENCE PROVIDE_OPTIONS_SCREEN PROVIDE_NETWORKINFO_SCREEN PROVIDE_LOGOUT	9600 Series SIP IP Telephones Customizeable System Parameters.

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 9600 Series SIP IP Telephones relate to the routers and servers in your network.

Step 1: Telephone to Network

The telephone is appropriately installed and powered. After a short initialization process, the telephone 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: Telephone to LLDP-Enabled Network

An LLDP-enabled network provides information to the telephone, as described in Link Layer Discovery Protocol (LLDP) on page 101. Among other data passed to the telephone is the IP Address of the HTTP or HTTPS server.

Step 3: Telephone to DHCP Server

The DHCP server provides information to the telephone, as described in DHCP and File Servers on page 53. Among other data passed to the telephone is the IP Address of the HTTP or HTTPS server.

Step 4: Telephone and File Server

The 9600 Series IP Telephones can download script files, binary files, certificates, language files, and settings files from either an HTTP or HTTPS server. The telephone queries the file server, which transmits a script file to the telephone. This script file, at a minimum, 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 script file to determine if it has the proper binary file. If the telephone determines the proper binary file is missing, the telephone 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 telephone determines it already has the proper file, the telephone proceeds as described in the next paragraph without downloading the binary file again.

The telephone checks and loads the binary file, then uses the script 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 9600 Series SIP IP Telephones in your network. For more information about this download process and settings file, see Chapter 7: Telephone Software and Binary Files.

Step 5: Telephone and the SES Server

In this step, the telephone might prompt the user for an extension and password. The telephone uses that information to exchange a series of messages with 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 SES password. For a restart of an existing installation, this information is already stored on the telephone, but the user might have to confirm the information. The telephone and SES and SES and CM exchange more messaging. The expected result is that the telephone is appropriately registered and CM call server data such as feature button assignments are downloaded.

For more information about the installation process, see the *Avaya one-X™ Deskphone Edition for 9600 SIP IP Telephones 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 telephone performance.

The *Avaya one-X™ Deskphone Edition for 9600 SIP IP Telephones Installation and Maintenance Guide* covers possible operational problems that might be encountered after successful 9600 Series SIP IP Telephone installation. The User Guides for a specific telephone model also contain guidance for users having problems with specific IP telephone 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
- Jitter buffers

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: 9600 Series SIP IP Telephones Customizeable System Parameters.

Hardware Requirements

To operate properly, you need:

- Category 5e cables designed to the IEEE 802.3af-2003 standard, for LAN powering,
- 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.
- TN799C or D Control-LAN (C-LAN) circuit pack.

Important:

IP telephone firmware Release 1.0 or greater 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.

To ensure that the appropriate circuit pack(s) are administered on your Communication Manager call server, see Chapter 4: Communication Manager Administration. For more information about hardware requirements in general, see the *Avaya one-X™ Deskphone Edition for 9600 SIP IP Telephones Installation and Maintenance Guide*.

Server Requirements

Four server types can be configured for the 9600 Series IP Telephones:

- DHCP server
- HTTP or HTTPS server
- SIP Proxy or Registration server
- Network Time Protocol server for SNTP

Note:

9600 Series SIP IP Telephones need SIP Enablement Services (SES) to work properly. The SIP Proxy and Registration servers reside on the SES server. Avaya Communication Manager (CM) is considered a “feature server” behind SES that provides Outboard Proxy SIP (OPS) features. SIP software Release 2.0 supports both SES 4.X and 5.X, but when the corresponding server is running SES 4.X, the telephones assume only those features compatible with SES 4.X.

While the servers listed provide different functions that relate to the 9600 Series IP Telephones, 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: Communication Manager Administration. For parameters related to DHCP and file servers, see Chapter 6: Server Administration.

Important:

The telephones obtain important information from the script files on the server(s) and depend on the binary file for software upgrades. If these servers are unavailable when the telephones reset, the telephones 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 53.

HTTP/HTTPS Server

Administer the HTTP or HTTPS file server and application as described in HTTP Generic Setup on page 66.

Network Time Protocol (NTP) Server

SIP IP telephones require NTP server support to set the time and date, used in system log time stamps and other time/date functions. The NTP server is typically needed by one or more servers within the enterprise. Administration of the NTP 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 9600 Series SIP IP Telephones 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”) or DNS names. 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 56 and DNS Addressing on page 98.

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)	
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 script 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 9600 Series SIP IP Telephone Scripts and Binary Files.

Other Network Considerations

SNMP

The 9600 Series SIP IP Telephones are fully compatible with SNMPv2c and with Structure of Management Information Version 2 (SMIv2). The telephones respond correctly to queries from entities that comply with earlier versions of SNMP, such as SNMPv1. “Fully compatible” means that the telephones 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: 9600 Series SIP IP Telephones 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 9600 Series SIP IP Telephones is available for download in *.txt format on the Avaya support Web site at http://www.avaya.com/support.

Registration and Authentication

A 9600 Series SIP IP Telephone requires an outboard proxy SIP (OPS) extension on Avaya Communication Manager and a login and password on the SES Server to register and authenticate it. Registration is described in the Initialization process, in Step 5: Telephone and the SES Server on page 22. For further information, see *Installing and Administering SIP Enablement Services R 4.0* (03-600766), available on the Avaya support Web site, http://www.avaya.com/support.

Reliability and Performance

All 9600 Series SIP IP Telephones respond to a ping or traceroute message sent from Avaya Communication Manager or any other network source. The telephones do not originate a ping or traceroute. The 9600 Series SIP IP Telephones offer and support “remote ping” and “remote traceroute.” The switch can instruct the telephone to originate a ping or a traceroute to a specified IP Address. The telephone carries out that instruction and sends a message to the switch indicating the results. For more information, see your switch administration documentation.

If applicable, the telephones test whether the network Ethernet switch port supports IEEE 802.1D/q tagged frames by ARPing the router with a tagged frame. For more information, see VLAN Considerations on page 94. If your LAN environment includes Virtual LANs (VLANs), your router must respond to ARPs for VLAN tagging to work properly.

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 40 for QoS implications for the 9600 Series SIP IP Telephones.

All 9600 Series SIP IP Telephones provide some detail about network audio quality. For more information see, Network Audio Quality Display on 9600 Series SIP IP Telephones on page 30.

IEEE 802.1D and 802.1Q

For more information about IEEE 802.1D and IEEE 802.1Q and the 9600 Series SIP IP Telephones, see IEEE 802.1D and 802.1Q on page 40 and VLAN Considerations on page 94. 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.

Network Audio Quality Display on 9600 Series SIP IP Telephones

All 9600 Series SIP IP Telephones give the user an opportunity to monitor network audio performance while on a call. For more information, see the telephone user guide.

While on a call, the telephones display network audio quality parameters in real-time, as shown in Table 4:

Table 4: Parameters in Real-Time

Parameter	Possible Values
Received Audio Coding	***G.711***, ***G.722***, ***G.726A***, or ***G.729***.
Packet Loss	No data or a percentage. Late and out-of-sequence packets are counted as lost if they are discarded. Packets are not counted as lost until a subsequent packet is received and the loss confirmed by the RTP sequence number.
Packetization Delay	No data or an integer number of milliseconds. The number reflects the amount of audio data in each RTP packet.
One-way Network Delay	No data or an integer number of milliseconds. The number is one-half the value RTCP or SRTCP computes for the round-trip delay.
Network Jitter Compensation Delay	No data or an integer number of milliseconds reporting the average delay introduced by the jitter buffer of the telephone.

The implication for LAN administration depends on the values the user reports and the specific nature of your LAN, like topology, loading, and QoS administration. This information gives the user an idea of how network conditions affect the audio quality of the current call. Avaya assumes you have more detailed tools available for LAN troubleshooting.

SIP Station Number Portability

The 9600 Series SIP IP Telephones provide station number portability. On startup or a reboot, the telephone attempts to establish communication with its home Personal Profile Manager (PPM)/SIP Enablement Services (SES) server based on the User Name and Password.

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 SES/PPM server usually routes them to the local call server. With proper administration of the local SES/PPM server, the telephone knows to try its home SES/PPM server, the one in London. The user can then be automatically registered with the London SES/PPM server.

TCP/UDP Port Utilization

The 9600 Series SIP IP Telephones 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 39.

Depending on your network, you might need to know what ports or ranges are used in the operation of 9600 Series IP Telephones. 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.
Many of the explanations in Table and Table refer to configuration parameters or options settings. For more information about parameters and settings, see Administering Options for the 9600 Series SIP IP Telephones.

Table 5: 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 telephone	Any	Received DNS messages	UDP
The number used in the Source Port field of the packets sent by the telephone'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 telephone's HTTP client	Any	TLS/SSL packets received by the telephone'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 telephone	Any	Received SNTP messages	UDP
161	Any	Received SNMP messages	UDP
50000	Any	Received CNA test request messages	UDP

1 of 2

Table 5: Received Packets (Destination = SIP IP Telephone) (continued)

Destination Port	Source Port	Use	UDP or TCP?
The number used in the Source Port field of registration messages sent by the telephone's CNA Agent	Any	Received CNA registration messages	TCP
PORTAUD or the port number reserved for CNA RTP tests	Any	Received RTP and SRTP packets	UDP
PORTAUD + 1 (if PORTAUD is even) or PORTAUD – 1 (if PORTAUD is odd) or the port number reserved for CNA RTP tests plus or minus one, as for PORTAUD, above	Any	Received RTCP and SRTCP packets	UDP
If signaling is initiated by the telephone = the number used in the Source Port field of the signaling packets sent by the telephone If signaling is initiated by the server = System-Specific	Any	Received signaling protocol packets	UDP/TCP
			2 of 2

Table 6: 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 telephone	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 telephone's HTTP client	TCP
			1 of 3

Table 6: Transmitted Packets (Source = SIP IP Telephone) (continued)

Destination Port	Source Port	Use	UDP or TCP?
514	Any unused port number	Transmitted Syslog messages	UDP
CNAPORT	Any otherwise unused port number	Transmitted CNA registration messages	TCP
The port number specified in the test request message	50000	Transmitted CNA test results messages	UDP
System-specific	Any unused port number	Transmitted signaling protocol packets	TCP
FEPORT or the port number specified in a CNA RTP test request	PORTAUD, which must be in the range specified by the RTP_PORT_LOW and RTP_PORT_RANGE parameters or the port number reserved for CNA RTP tests	Transmitted RTP and SRTP packets	UDP
FEPORT + 1 (if FEPORT is even) or FEPORT -1 (if FEPORT is odd) or the port number specified in a CNA RTP test request plus or minus one, as with FEPORT above	PORTAUD + 1 (if PORTAUD is even) or PORTAUD – 1 (if PORTAUD is odd) or the port number reserved for CNA RTP tests plus or minus one, as for PORTAUD, above	RTCP and SRTCP packets transmitted to the far-end of the audio connection	UDP

2 of 3

Table 6: Transmitted Packets (Source = SIP IP Telephone) (continued)

Destination Port	Source Port	Use	UDP or 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
			3 of 3

Security

For information about toll fraud, see the respective call server documents on the Avaya support Web site. The 9600 Series SIP IP Telephones 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.

9600 Series SIP IP Telephones support Transport Layer Security (TLS) for signaling and for secure communications (SRTP). This standard allows the telephone to establish a secure connection to a HTTPS server, in which the upgrade and settings file can reside. This setup adds security over another alternative.

Communications between the 9600 Series SIP IP telephone and the Personal Profile Manager (PPM) can also be secured by setting the CONFIG_SERVER_SECURE_MODE parameter.

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 SIGSIGNAL parameter, supporting signaling channel encryption while registering, and when registered, with appropriately administered Avaya Communication Manager.
- Restricting the response of the 9600 Series SIP IP Telephones to SNMP queries to only IP Addresses on a list you specify.
- Specifying an SNMP community string for all SNMP messages the telephone sends.
- Restricting dialpad access to Craft Local 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.

Registration and Authentication

A 9600 Series SIP IP Telephone requires an off-PBX station (OPS) extension on Avaya Communication Manager and a login and password on the SES Server to register and authenticate it. For more information, see the current version of your call server administration manual.

Chapter 4: 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 9600 Series SIP IP Telephones. Avaya recommends the latest CM software and the latest SIP IP telephone firmware.

Switch Compatibility

As of SIP Release S1.0, 9600 Series IP Telephones are supported by Avaya Communication Manager (CM) Release 4.0 and later. Be sure to administer 9600 Series SIP IP Telephones as 4620SIP telephones on Avaya Communication Manager.

Note:

The 9620 only supports a total of 12 call appearances and administered feature buttons. The 9630/9630G and 9640/9640G can be administered for a total of 24 call appearances and feature buttons.

For specific administration instructions about the 9600 Series SIP IP Telephones, see Administering Stations on page 48.

Communication Manager Administrative Requirements

There are several initial CM provisioning tasks that must be performed before administering SIP users. These tasks are described in *SIP Support in Avaya Communication Manager Running on Avaya S8XXX Server* s (Document Number 555-245-206), the latest release of which is Issue 8, January 2008. The tasks to administer Communication Manager for SIP Enablement Services (SES) and fall into three categories:

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

The sections that follow describe each of these tasks.

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 that uses 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 9600 Series SIP IP Telephones use an even-numbered port, selected from the interval 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 SIP IP Telephones support the RTP/SRTP Control Protocol (RTCP/SRTCP). The 9600 Series SIP IP Telephones do not support RSVP (Resource ReSerVation Protocol).

QoS

The 9600 Series SIP IP Telephones 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 9600 Series IP Telephones can simultaneously support receipt of packets using, or not using, 802.1Q parameters. To support IEEE 802.1D/Q, you can administer 9600 Series SIP IP Telephones by the value of the following configuration parameters:

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

NAT

9600 Series SIP IP Telephones 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.

Voice Mail Integration

9600 Series SIP IP Telephones use the settings file to configure the **Messages** button by setting the system parameter MSGNUM to any dialable string. MSGNUM examples are:

- a standard telephone number the telephone should dial to access your voice mail system, such as AUDIX or Octel.
- a Feature Access Code (FAC) that allows users to transfer an active call directly to voice mail. FACs are supported only for QSIG-integrated voice mail systems like AUDIX or Octel. QSIG is an enhanced signaling system that allows the voice mail system and Avaya Communication Manager Automated Call Processing (ACP) to exchange information.

When the user presses the **Messages** button on the telephone, that number or FAC is automatically dialed, giving the user one-touch access to voice mail.

The settings file specifies the telephone number to be dialed automatically when the user presses this button. The command is:

SET MSGNUM ***1234***

where ***1234*** is the Voice Mail extension (CM hunt group or VDN). For more information, see Table 11.

Auto Hold

9600 Series SIP IP Telephones always provide auto hold, regardless of whether or not the Auto Hold parameter is administered on the IP Network System Parameters form.

Call Transfer Considerations

Unlike 9600 H.323 IP Telephones, the 9600 Series SIP IP Telephones 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 9600 H.323 IP Telephones, the 9600 Series SIP IP Telephones 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 7 summarizes the calling features available on 9600 Series SIP IP Telephones. Some features are supported locally at the telephone, while others are only available with Avaya SIP Enablement Services and Communication Manager with OPS.

The features shown in Table 7 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 via OPS 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 *Avaya Extension to Cellular and OPS Installation and Administration Guide* (Document Number 210-100-500). The Avaya SIP solution configures all SIP telephones in Communication Manager as OPS.

Table 7: 9600 Series SIP IP Telephone Release S2.0 Feature Support

Feature	Delivered by Telephone	CM Feature Button/FNU	Avaya Communication Manager
3-Way Conferencing	X (non-Avaya environment)		
6-way Conference Bridge			X
Automatic Call Back/ Cancel		FNU	
Call Forward All Calls		FNU	
Call Forward Busy/ Don’t Answer	X (non-Avaya environment)	FNU	

1 of 3

Table 7: 9600 Series SIP IP Telephone Release S2.0 Feature Support (continued)

Feature	Delivered by Telephone	CM Feature Button/FNU	Avaya Communication Manager
Call Forward Deactivation		FNU	
Call Forward Unconditional	X (non-Avaya environment)		
Call Hold	X		
Call Management - incoming, outgoing call screening			X
Call Park and Unpark		FNU	
Call Pick-Up Group		FNU	
Call Pickup Directed		FNU	
Call Pickup Extended Group		FNU	
Calling Party Number Block/Unblock		FNU	
Consultation Hold	X		
Directed Call Pick-Up	X	FNU	
Distinctive Alerting	X		
EC500 Enable		FNU	
EC500 Disable		FNU	
Extend Call for EC500		FNU	Available with CM Release 5.0
Extended Group Call Pickup			
Find Me			X
Group Call Pickup		FNU	

2 of 3

Table 7: 9600 Series SIP IP Telephone Release S2.0 Feature Support (continued)

Feature	Delivered by Telephone	CM Feature Button/FNU	Avaya Communication Manager
Last Number Dialed (Redial)	X		
Malicious Call Trace	No	FNU	
Message Waiting Indication	X		
Music on Hold			X
One Touch Recording	X		
Priority Call		FNU	
Send All Calls Enable/ Disable		FNU	
Transfer - attended (non-Avaya environment)	X		
Transfer - unattended (one-button transfer) (non-Avaya environment	X		
Transfer to Voice Mail		FNU	
Whisper Page	X		

3 of 3

CM/SIP IP Telephone 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 telephone user interface. CM 4.0 or greater is required. For sample Station and other pertinent forms, see Appendix C: Sample Station Forms.

Table 8: 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.” In CM Release 5.0, default is “none.”
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.
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	

1 of 4

Table 8: CM/SIP Configuration Requirements (continued)

Task/Form	Command	Field(s)	Value(s)
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)
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 SIP Enablement Services. See Chapter 5: SIP Enablement Services (SES) Administration for SES configuration information.
		(Station) Type	Use 9620 or 9630.
		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 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.)

2 of 4

Table 8: 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.

3 of 4

Table 8: 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 SIP Enablement Services 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.

4 of 4

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, sample screens of which are provided in Figure 1 through Figure 4. Avaya recommends setting the features covered in this section because they optimize the user interface.

Administering Features

The following buttons can be administered for a 9600 Series SIP IP Telephone, unless otherwise noted:

Administrable Station Features

Feature	Administration Notes
Audix One-Touch Recording	
Auto Callback	
Autodial	
Bridged Call Appearances	
Busy Indicator	
Call Appearances	
Call Forward (all)	Leave the Ext: field blank, as the telephone does not support 3rd party call forwarding.
Call Forwarding (busy/ don't answer)	Leave the Ext: field blank, as the telephone does not support 3rd party call forwarding.
Call Park	
Call Unpark	This (SES) feature will show up automatically without administration. Regardless of CM Station screen administration, these features will show on the Features menu automatically, but not on a telephone button.
Call Pickup	
CPN Block	
CPN Unblock	
Directed Call Pickup	
EC500	
EC500 Extend Call	
Extended Call Pickup	This (SES) feature will show up automatically without administration. Regardless of CM Station screen administration, these features will show on the Features menu automatically, but not on a telephone button.
MCT Activation	This (SES) feature will show up automatically without administration. Regardless of CM Station screen administration, these features will show on the Features menu automatically, but not on a telephone button.
Priority Call	
Send All Calls	Leave the Ext: field blank, as the telephone does not support 3rd party send all calls.
Transfer-to-Voicemail	This (SES) feature will show up automatically without administration. Regardless of CM Station screen administration, these features will show on the Features menu automatically, but not on a telephone button.
Whisper Page	

For additional information about administering Avaya Communication Manager for 9600 Series SIP IP Telephones, 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 555-245-770).

Chapter 5: SIP Enablement Services (SES) Administration

Introduction

SIP Enablement Services (SES) software resides on the SIP Proxy server and provides most of the features and functionality to SIP telephones.This chapter describes using the SES Web browser to configure SES for use with 9600 Series SIP IP Telephones.

Avaya provides a Web browser to simplify SES administration.

Using the Web Browser to Configure SES

Follow this configuration procedure.

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.

   Note:
   This example administers station 34071 as a SIP endpoint using a 9630 telephone.
3. Click on **Launch Administration Web Interface**.

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

   The Add User screen displays.
5. Complete all required fields, indicated by asterisks *.
6. Enter a handle in the **Primary Handle** field. The Primary Handle must be all numeric.
7. 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.
8. Check the **Add Media Server Extension** checkbox and click **Add**.

   The confirmation screen displays.

9. Click **Continue**.

   The Add Media Server Extension page displays.

10. In the **Extension** field, enter the same extension you entered on page 1 of the Communication Manager Station form. 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).

11. Click **Add**.

    Since the user is being added to Avaya SES Home, the Communication Manager (CM) call server corresponding to the SIP trunk between the CM server and SES Home is selected. The confirmation page displays.

12. Click **Continue**.

13. Repeat Steps 4 - 11 for each SIP telephone.

14. 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.

Important:

The firmware in the 9600 Series SIP IP Telephones reserves IP Addresses of the form **192.168.2.x** for internal communications. The telephone(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 9600 Series SIP IP Telephone network by removing the need to individually assign and maintain IP Addresses and other parameters for each telephone on the network.

The DHCP server provides the following information to the 9600 Series SIP IP Telephones:

- IP Address of the 9600 Series SIP IP Telephone(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 IP telephone can access a DHCP server that contains the IP Addresses and subnet mask.

Important:

An IP telephone cannot function without an IP Address. The failure of a DHCP server at boot time leaves all the affected telephones unusable. A user can manually assign an IP Address to an IP telephone. When the DHCP server finally returns, the telephone 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 telephone reboots.
- A DHCP server be available at remote sites if WAN failures isolate IP telephones from the central site DHCP server(s).

The file server provides the 9600 Series SIP IP Telephone with a script file and, if appropriate, new or updated binary software. See Step 4: Telephone and File Server on page 22 under Telephone Initialization Process. In addition, you can edit an associated settings file to customize telephone parameters for your specific environment. For more information, see Chapter 8: Administering Telephone Options.

DHCP Server Administration

This document concentrates on the simplest case of the 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 9600 Series SIP IP Telephones

To administer DHCP option 242, make a copy of an existing option 176 for your 46xx IP Telephones. You can then either:

- leave any parameters the 9600 Series SIP IP Telephones do not support for setting via DHCP in option 242 to be ignored, or
- delete unused or unsupported 9600 IP Series Telephone parameters to shorten the DHCP message length.

Only the following parameters can be set in the DHCP site-specific option for 96xx telephones, although most of them can be set in a 46xxsettings.txt file as well.

Table 9: Parameters Set by DHCP

Parameter	Description
HTTPDIR	Specifies the path name to prepend to all file names used in HTTP GET operations during startup. (0 to 127 ASCII characters, no spaces.) The command is "**`SET HTTPDIR myhttpdir`**". The path (relative to the root of the HTTP file server) where 96xx telephone files are stored. If an Avaya file server is used to download configuration files over TLS, 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 **except** for BRURI.
HTTPPORT	Destination port for HTTP requests (0-65535, 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).
SIPPROXYSRVR	SIP proxy/registrar server IP or DNS address. (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.
SNTPSRVR	List of SNTP server IP or DNS address(es) u.sed to retrieve date and time via SNTP
TLSDIR	Used as path name that is prepended to all file names used in HTTPS get operations during initialization (0-127 character string).
TLSPORT	Destination TCP port used for requests to https server (0-65535). The default is 443.
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 document is limited to describing a generic administration that works with the 9600 Series SIP IP Telephones. 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 9600 Series SIP IP Telephones.
   - 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 9600 IP Telephone 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 98.

- **Option 42 - SNTP Server**.
  This option specifies a list of IP Addresses indicating NTP servers available to the telephone. 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: 9600 Series SIP IP Telephones 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.

- **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.
- **Option 53 - DHCP message type**.
  Value is 1 (DHCPDISCOVER) or 3 (DHCPREQUEST).
- **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**.
- **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 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 9600 Series IP Telephones do not support Regular Expression Matching, and therefore, do not use wildcards. For more information, see Administering Options for the 9600 Series SIP IP Telephones on page 73.

In configurations where the upgrade script and binary files are in the default directory on the HTTP server, do not use the HTTPDIR=<path>.

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

The SIP Proxy server name and HTTP server name must each be no more than 32 characters in length.

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 10, the 9600 Series IP Telephone sets the system values to the DHCPACK message field values shown.

Table 10: 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 telephones.

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 9600 Series IP Telephones with sequential IP Addresses. Also do not mix 9600 Series IP Telephones 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, “9600OPTION.”
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 **96XXOPTIONs** are correctly configured for the Windows NT® 4.0 DHCP server.

Verify the Default Option, 242 96XXOPTION

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 96XXOPTION**.
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 96XXOPTION

1. Select **Scope** under **DHCP OPTIONS**.
2. In the **Active Options:** scroll list, click **242 96XXOPTION**.
3. Click the **Value** button.
4. Verify that the **Value String** box contains the correct string from DHCP Generic Setup on page 56.

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

Verify the Global Option, 242 96XXOPTION

1. Select **Global** under **DHCP OPTIONS**.
2. In the **Active Options:** scroll list, click **242 96XXOPTION**.
3. Click the **Value** button.
4. Verify that the **Value String** box contains the correct value from DHCP Generic Setup on page 56. 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 9600 Series IP Telephones 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 56.

    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 same binary file, script file, and settings file on an HTTP server as you can on a TFTP server. TFTP is not supported for 9600 Series SIP IP Telephones. 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 53.

Important:

The files defined by HTTP server configuration must be accessible from all IP telephones invoking 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 upgrade script file and binary file(s) from the Avaya Web site http://www.avaya.com/support to the HTTP server. For more information, see Contents of the Settings File on page 70.

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.

Chapter 7: Telephone Software and Binary Files

General Download Process

The 9600 Series SIP IP Telephones download script files, binary files, and settings files from either an HTTP or HTTPS server. The HTTPS server applies only if the server supports Transport Layer Security (TLS) encryption.

Note:

The script files, binary files, and settings files discussed in this chapter are identical for HTTP and HTTPS servers. The generic term “file server” refers to both “HTTP server” and “HTTPS server.”

The file downloading process is the same for both servers, except that when you use an HTTPS server, a TLS server is contacted first. The telephone queries the file server, which transmits a script file to the telephone. The script file tells the telephone which binary file the telephone must use. The binary file is the software that has the telephony functionality, and is easily updated for future enhancements. In a newly installed telephone, the binary file might be missing. In a previously installed telephone, the binary file might not be the proper one. In both cases, the telephone requests a download of the proper binary file from the file server. The file server downloads the file and conducts some checks to ensure that the file was downloaded properly. If the telephone determines it already has the proper file, the telephone proceeds to the next step without downloading the binary file again.

After checking and loading the binary file, the 9600 Series SIP IP Telephone, if appropriate, uses the script 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 70.

Software

As part of installation, a conversion from H.323 to SIP signaling protocol is done as described in "Converting Software on 9600 Series IP Telephones" of the *Avaya one-X™ Deskphone Edition for 9600 Series SIP IP Telephones Installation and Maintenance Guide.* When the telephone is first plugged in, a software download from an HTTP or HTTPS server starts to give the phone its proper functionality.

For software upgrades, SIP Enablement Services (SES) provides the capability for a remote reboot of the 9600 Series SIP IP Telephones. As a result, the telephone automatically starts reboot procedures. If new software is available on the server, the telephone downloads it as part of the reboot process. The *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide* covers upgrades to a previously installed telephone and related information.

9600 Series SIP IP Telephone Scripts and Binary Files

Choosing the Right Binary File and Upgrade Script File

The software releases containing the files needed to operate the 9600 Series IP Telephones are bundled together. You download this self-extracting executable file to your file server from the Avaya support Web site at: http://www.avaya.com/support. The file is available in both zipped and unzipped format. You must select one of two software “bundles" to download the latest software, depending on whether your telephone environment is primarily SIP-centric or H.323-centric.

Each bundle contains:

- An upgrade script file, **96xxupgrade.txt**, which allows you to upgrade to new software releases and new functionality without having to replace SIP IP telephones. The upgrade script tells the telephone whether a software upgrade is needed. All Avaya IP Telephones attempt to read this file whenever they reset. The upgrade script file is also used to point to the settings file. An alternate file may be included, depending on which software bundle you download.
- Binary files for all current 9600 Series SIP IP Telephones.
- Other useful information such as a ReadMe file and the latest binary code.

In addition to the upgrade script, binary files and Read Me file you need the latest binary code the Avaya SIP IP Telephones use, which is part of the software bundle you choose for your site. All these files are in self-extracting executable file comes in both zipped and unzipped format.

When the majority of your IP telephones are SIP-based, select the software bundle identified as “SIP” from the Avaya Support Web site. The binary files in this SIP software bundle are the same as in the H.323 bundle. The difference is a modified upgrade script file that assumes SIP is the default protocol for your 9600 Series IP Telephones, and that H.323 is the exception. For more information on SIP-centric environments, see "Converting Software on 9600 Series IP Telephones" in the *Avaya one-X™ Deskphone Edition for 9600 Series SIP IP Telephones Installation and Maintenance Guide*.

Upgrade Script File

An upgrade script file named **96xxupgrade.txt**, tells the IP telephone whether the telephone needs to upgrade software. The 9600 Series SIP IP Telephones attempt to read this file whenever they reset. The upgrade script file also points to the settings file.

You download the upgrade script file, sometimes called the “script file,” from http://www.avaya.com/support. This file allows the telephone to use default settings for customer-definable options. All files must reside in the same directory.

An "alternate" upgrade script is also included, 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 each software bundle. Once these changes are made, the alternate file should be renamed to “96xxupgrade.txt” and placed in the HTTP download directory. The HTTP download directory holds the telephone backup and application binaries the telephone will download. Renaming the alternate file causes any “96xxupgrade.txt” files residing in that directory to be overwritten.

Note:

Avaya recommends that the settings file have the extension ***.txt**. The Avaya IP Telephones can operate without this file. You can also change these settings with DHCP or, in some cases, from the dialpad of the telephone.

Settings File

The settings file contains the option settings you need to customize the Avaya IP Telephones for your enterprise.

Note:

Use one settings file for all your Avaya IP Telephones. The settings file includes the 9600 Series SIP IP Telephones covered in this document. The settings file also includes 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 any of five types of statements, one per line:

- Comments, which are statements with a “**#**” character in the first column.
- Tags, which are comments that have exactly one space character after the initial **#**, followed by a text string with no spaces.
- **`Goto`** commands, of the form **GOTO *tag.*** **`Goto`** commands cause the telephone to continue interpreting the configuration file at the next line after a **# *tag*** statement. If no such statement exists, the rest of the configuration file is ignored.

- Conditionals, of the form **IF *$name* SEQ *string* GOTO *tag***. Conditionals cause the **`Goto`** command to be processed if the value of ***name*** is a case-insensitive equivalent to ***string***. If no such ***name*** exists, the entire conditional is ignored. The only system values that can be used in a conditional statement are: BOOTNAME, GROUP, and SIG.
- **`SET`** commands, of the form **SET *parameter_name value***. Invalid values cause the specified value to be ignored for the associated ***parameter_name*** so the default or previously administered value is retained. All values must be text strings, even if the value itself is numeric, a dotted decimal IP Address, and so on.

  Note:

  Enclose all data in quotation marks for proper interpretation.

The upgrade script file Avaya provides includes a line that tell the telephone to **GET *46xxsettings.txt***. This lines causes the telephone to use HTTP to attempt to download the file specified in the **`GET`** command. If the file is obtained, its contents are interpreted as an additional script file. That is how your settings are changed from the default settings. If the file cannot be obtained, the telephone continues processing the upgrade script file.

If the configuration file is successfully obtained but does not include any setting changes the telephone stops using HTTP. This happens when you initially download the script file template from the Avaya support Web site, before you make any changes. When the configuration file contains no setting changes, the telephone does not go back to the upgrade script file.

Avaya recommends that you do **not** alter the upgrade script file. If Avaya changes the upgrade script 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 upgrade script file.

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

Contents of the Settings File

After checking the software, the 9600 Series IP Telephone looks for a 46xxsettings file. This file is where you identify non-default option settings, application-specific parameters, and so on. You can download a template for this file from the Avaya support Web site. An example of what the file might look like follows.

Note:

The following is intended only as a simple example. 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.

SET DNSSRVR ”dnsexample.yourco.com”

SET SIPPROXYSRVR 192.168.1.110

SET SIPSIGNAL “1” (TCP)

SET ENABLE_PRESENCE “1” (show presence icons)

SET SIPDOMAIN ”domain name”

SET SNTPSRVR 192.168.1.111

SET GMTOFFSET “-5:00”

SET DSTOFFSET “1”

SET DSTSTART “2SunMar2L” (second Sunday in March at 2 am Local time)

SET DSTSTOP “1SunNov2L” (first Sunday in November at 2 am Local time)

Note that the DSTSTART and DSTSTOP parameters reflect the new 2007 Daylight Savings Time values for North America

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 example assumes the data VLAN ID is “yyy” and the data traffic priority is “z”:

SET VLANSEP 1
SET PHY2VLAN yyy
SET PHY2PRIO z

Note:

Also 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 Edition for 9600 SIP IP Telephones 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 associates in different groups at the same location:

```
IF $GROUP SEQ 1 goto GROUP1
IF $GROUP SEQ 2 goto GROUP2
```

{specify settings unique to Group 0}

```
goto END
# GROUP1
```

{specify settings unique to Group 1}

```
goto END
# GROUP2
```

{specify settings unique to Group 2}

```
# END
```

{specify settings common to all Groups}

Chapter 8: Administering Telephone Options

Administering Options for the 9600 Series SIP IP Telephones

This chapter explains how to change parameters by means of the DHCP or HTTP servers. 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.

Table 11 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 telephones use the default values for the remaining ones. At a minimum, be sure to set these important SIP-related parameters: SIPPROXYSRVR, SIPDOMAIN, SNTPSRVR, SIPSIGNAL, ENABLE_PRESENCE, GMTOFFSET, DSTOFFSET, DSTSTART, and DSTSTOP.

For DHCP, the DHCP Option sets these parameters to the desired values as discussed in DHCP and File Servers on page 53. For HTTP, the parameters in Table 11 are set to desired values in the script file. For more information, see Contents of the Settings File on page 70.

Avaya recommends that you administer options on the 9600 Series SIP IP Telephones using script files. Some DHCP applications have limits on the amount of user-specified information. The administration required can exceed those limits for the more full-featured telephone models.

You might choose to completely disable the capability to enter or change option settings from the dialpad. 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 entering the PROCPSWD value on the Craft Access Code Entry screen. For more information on craft options, see the *Avaya one-X™ Deskphone Edition for 9600 Series SIP IP Telephones Installation and Maintenance Guide*.

Important:

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 PROCPSWD limits access to all local procedures, including VIEW. VIEW is a read-only Craft option that allows review of the current telephone settings.

Table 11: 9600 Series SIP IP Telephones 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.
AGCHEAD	1	Automatic Gain Control status for headset. Values are 0=disabled, 1=enabled.
AGCSPKR	1	Automatic Gain Control status for speaker. Values are 0=disabled, 1=enabled.
AUDASYS	3	Globally controls audible alerting. Values range from 0 through 3. Value 0 or 2=audible alerting off. Value 1 or 3=audible alerting on.
AUDIOENV	0	Audio environment selection index. Values range from 0 through 191.
AUDIOSTHD	0	Headset sidetone setting. Values are: 0 = Nominal 1 = -3dB below nominal 2 = -9dB below nominal 3 = -15dB below nominal 4 = -30dB below nominal (essentially no sidetone) 5 = 10dB above nominal.
AUDIOSTHS	0	Handset sidetone setting. Values are: 0 = Nominal 1 = -3dB below nominal 2 = -9dB below nominal 3 = -15dB below nominal 4 = -30dB below nominal (essentially no sidetone) 5 = 10dB above nominal.
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).

1 of 21

Table 11: 9600 Series SIP IP Telephones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
CALL_TRANSFER_ MODE	0	When ENABLE_AVAYA_ENVIRONMENT=0, this parameter indicates how transfers are performed: 0 = attended transfer 1 = unattended transfer
CALLFWDADDR	" " (Null)	The URI to which calls are forwarded in 3rd party (non-Avaya) environments only.
CALLFWDDELAY	1	Third-party (non-Avaya) environments only. Specifies the number of ring cycles generated at the phone before the call is forwarded to the Call Forwarding Address, if call forwarding on "No answer" is selected in 3rd party environments. Valid number of ringing cycles are 0-20.
CALLFWDSTAT	0	Third-party (non-Avaya) environments only. Specifies the sum of the allowed Call Forwarding permissions. This parameter controls which of the Call Forwarding Feature Buttons are made visible and active for the user in 3rd party environments. Valid values are: 0 = no Call Forwarding permitted. 1 = Call Forward Unconditional only permitted. 2 = Call Forward Busy only permitted. 4 = Call Forward No Answer only permitted. Others = sum of Call Forward types permitted.
CNAPORT	50002	Transport-layer port number to be used for registration to CNA server for network analysis. Valid range is 0-65535.
CNASRVR	" " (Null)	List of CNA server IP or DNS address(es). Used to connect to CNA server for network analysis (in case of several entries first address always first, etc.). Format is 0 to 255 characters: zero or more IP addresses in dotted decimal or DNS name format, separated by commas without any intervening spaces. Currently set to a maximum of 5 servers.
CNGLABEL	1	Indicates whether end user can personalize button labels. Valid values are: 0=User cannot change button labels 1=User has ability to change button labels
CONFIG_ SERVER	“” (Null)	Address of Avaya configuration server (currently, this parameter, when used, is set to the PPM server address). Format is dotted decimal or DNS format, separated by commas, with no spaces (0-255 ASCII characters, including commas, optionally followed by colon and port number).
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. 2 = Use HTTPS if the SIP transport type is TLS, otherwise use HTTP.

2 of 21

Table 11: 9600 Series SIP IP Telephones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
COUNTRY	USA	Country of operation for specific dial tone generation.
COVERAGEADDR	" " (Null)	The URI to which call coverage is sent to in 3rd party (non-Avaya) environments only.
CURRENT_SKIN	" " (Null)	Defines if a custom skin is currently selected (non-empty string) or built-in default skin is used (empty string or not set). If a custom skin is selected (non-empty string), this value points to the corresponding skin resource definition (i.e. contains a label as defined in "SKINS" configuration parameter). Can also be set by the end user via Avaya Menu Screen & Sounds option.
DATEFORMAT	%m/%d/%y	Formatting string defining how to display the date in the top line and the call log.
DAYLIGHT_SAVING_ SETTING_MODE	2	Controls daylight saving setting. Values are: 0=daylight saving time is deactivated (no offset to local time) 1=daylight saving time is activated (offset to local time as configured in "DSTOFFSET") 2=the device switches automatically to daylight saving time and back according to the contents of "DSTSTART" and "DSTSTOP"
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 (in "non-PPM" format) Used to identify the end of dialing information to accelerate dialing. Valid value is 0 to 1023 characters that define the dial plan.
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.

3 of 21

Table 11: 9600 Series SIP IP Telephones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
DOT1XEAPS	MD5	Specifies the EAP authentication method(s) to be used with IEEE 802.1X. Comma-separated list of key words defining EAP methods. In SIP Release 2.0, this value is restricted to a single EAP method. Valid values are either "MD5" or "TLS".
DOT1XSTAT	1	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.
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)

4 of 21

Table 11: 9600 Series SIP IP Telephones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
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_AVAYA_ ENVIRONMENT	1	Determines whether the phone operates in a mode to comply with 3rd party standard SIP proxy (provision of SIPPING 19 feature) or the Avaya environment mode (provision of SIP/AST features and use of PPM for download and backup/restore). Valid values are: 0=Non-Avaya environment; 1=Avaya environment.
ENABLE_CALL_LOG	1	Enable or disable complete Call Log application. If disabled no calls are logged, screens related to Call Log are not displayed to user, and menu items of User Interface to set Call Log options are not displayed. Values are 0=disabled; 1=enabled.
ENABLE_CONTACTS	1	Enable or disable complete Contact application. If disabled no contacts are downloaded during initialization from PPM, screens related to Contacts application are not displayed to user, and menu items of the User Interface to set Contacts options are hidden. Values are 0=disabled; 1=enabled.
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.
ENABLE_G711A	1	Enable or disable G711A codec capability of the phone. If the parameter is set to 1, the phone includes G711A capability in an outbound INVITE request, and accepts G711A when received in an incoming INVITE request. Values are 0=disabled; 1=enabled.

5 of 21

Table 11: 9600 Series SIP IP Telephones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
ENABLE_G711U	1	Enable or disable G711U codec capability of the phone. If the parameter is set to 1, the phone includes G711U capability in an outbound INVITE request, and accepts G711U when received in an incoming INVITE request. Values are 0=disabled; 1=enabled.
ENABLE_G722	0	Enable or disable G722 capability of the telephone. If the parameter is set to 1, the phone includes G722 capability in an outbound INVITE request, and accepts G722 when received in an incoming INVITE request. If set to 0, processing of G722 as a capability is disabled. Values are 0=disabled, off; 1=enabled, on.
ENABLE_G726	1	Enable or disable G726 capability of the telephone. If the parameter is set to 1, the telephone includes G726 capability in an outbound INVITE request, and accepts G726 when received in an incoming INVITE request. Values are 0=disabled, off; 1=enabled, on.
ENABLE_G729	1	Enable or disable G729A codec capability of the phone. Values are: 0=G729A disabled 1=The phone includes G729(A) without Annex B support capability in an outbound INVITE request, and accepts G729 when received in an incoming INVITE request. 2=The phone includes G729(A) with Annex B support capability in an outbound INVITE request, and accepts G729 when received in an incoming INVITE request.
ENABLE_MODIFY_ CONTACTS	1	Enable or disable the ability to modify contacts if the Contact application is enabled. Values are 0=disabled; 1=enabled.
ENABLE_MULTIPLE_ CONTACTS_WARNING	1	Activate/deactivate multiple contacts warning. Depending on current value, a warning message is displayed explaining to the user there are multiple devices registered on user's behalf and that this can cause service disruption. Values: 0 = warning disabled, 1 = warning enabled.
ENABLE_PRESENCE	0	Enable or disable complete Presence functionality. If disabled, Presence icons do not show in Contacts or Call History Lists, Presence is not displayed to the user, incoming Presence updates are ignored, and menu items of User Interface to set Presence options are not displayed (if available). Values are 0=disabled, off; 1=enabled, on.
ENABLE_REDIAL	1	Enable or disable complete Redial functionality. If disabled pressing the redial button has no effect and the redial softkeys and menu items are not displayed. Values are 0=disabled; 1=enabled.

6 of 21

Table 11: 9600 Series SIP IP Telephones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
ENABLE_REDIAL_LIST	1	Enables or disables the capability to redial out of a list of recently dialed numbers instead of performing last number redial. Values are 0=disabled (last number redial only is offered to the user); 1=enabled (user can select either last number redial or redial from a list).
ENHDIALSTAT	1	Enhanced Dialing Status. Valid range is 0 to 2. If set to “0” the feature is turned off. If set to “1” it is partially enabled (dialing rules do not apply for dialing from Contacts). If set to “2”, the Enhanced Local Dialing feature is fully enabled (dialing rules also apply for dialing from Contacts). Note that If CTDC_SUPPORT is enabled, Enhanced Local Dialing is automatically disabled, independent of the actual setting of ENHDIALSTAT. If CTDC_SUPPORT is disabled, Enhanced Local Dialing is processed as defined by ENHDIALSTAT.
EXCHANGE_SERVER_ LIST	" " (Null)	Used to connect to Microsoft Exchange™ server to access calendar data. Zero to 255 characters: zero or more IP Addresses in dotted decimal or DNS name format, separated by commas without any intervening spaces.
EXCHANGE_USER_ DOMAIN	" " (Null)	String of 0 to 255 characters representing user domain for Microsoft Exchange™ Server.
FAILED_SESSION_ REMOVAL_TIMER	30	Timer to automatically remove a failed call session. Range in seconds is 5 to 999.
G726_PAYLOAD_TYPE	110	RTP dynamic payload used for G.726. Range is 96 to 127.
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.
GROUP	0	Specific user group as tested in configuration files. Valid values are 0 to 999.
HEADSYS	1	Headset operational mode. One ASCII numeric digit. Valid values are: 0 or 2=General Operation, where a disconnect message returns the telephone to an idle state. 1 or 3=Call Center Operation, where a disconnect message does not change the state of the telephone.
HTTPDIR	" " (Null)	HTTP server directory path. The path name prepended to all file names used in HTTP and HTTPS get operations during initialization. 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.

7 of 21

Table 11: 9600 Series SIP IP Telephones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
HTTPEXCEPTION DOMAINS	" " (Null)	Domains to be excluded for SCEP. String representing zero or one domains in a URL of 0 to 255 characters in dotted decimal or DNS name format with multiple domains delimited by commas.
HTTPPORT	80	Destination TCP port used for requests to the HTTP server during initialization. Range is 0 - 65535. **Note:** For SIP Release 1.0, there should be no need to set this parameter to values other than default value.
HTTPPROXY	" " (Null)	Zero or one IP or DNS address of the HTTP server for SCEP. 0 to 255 characters in dotted decimal or DNS name format followed by a colon and port number. The colon and port number are optional. If this parameter is not null, this (proxy) transport address is used to set up the HTTP connection as the transport protocol for SCEP.
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
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.
IPADD	0.0.0.0	IP Address of the telephone. Range is 7 to 15 ASCII characters (less than the default string length) defining one IP Address in dotted-decimal format.
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.

8 of 21

Table 11: 9600 Series SIP IP Telephones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
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.
LANGUAGES	" " (Null)	List of links to language files to be downloaded. Substrings are delimited by commas. Maximum length is 1023 characters. Each substring shall follow one of the these naming rules: A substring is identical to a file name without any prefix specifying the path or server: The files are downloaded from the same source as the setting file(s). A substring can provide a prefix to the file name, which specifies the relative path ("./" for next higher directory level) from the directory the settings file(s) has been downloaded to the directory the language file shall be download. A substring specifies the completed URL to the language file including protocol identifier ("http://" or "https://"), server and path.
LLDP_ENABLED	2	Flag to enable/disable LLDP (Link Layer Discovery Protocol). Valid values are: 0 = disabled; the telephone will not support LLDP. 1 = enabled; the telephone will support LLDP. 2 = auto; the telephone will support LLDP, but the transmission of LLDP frames will not begin until or unless an LLDP frame is received.
LOCAL_LOG_LEVEL	3	Numerical code of severity level. Store entries to the local event log, if event occurs with a severity level whose numerical code is equal to or less than the LOCAL_LOG_LEVEL value. Values are: 0 (emergencies), 1 (alerts), 2 (critical), 3 (errors), 4 (warning), 5 (notice), 6 (informational), 7 (debug).

9 of 21

Table 11: 9600 Series SIP IP Telephones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
LOG_CATEGORY		Comma-separated list of keywords in standard string format representing logging categories (SW modules or functions to be included in lower level logging). Logging implementation blocks all traces at level "Warning" or lower, unless the category corresponding to a given trace is enabled. If the LOCAL_LOG_LEVEL is set to "Warning" or lower, this parameter would enable low-level traces from the adaptors or manager as indicated. Applies to all logging mechanisms (syslog and local log). Example: "ALSIP, SESSION" enables debug level traces from the ALSIP adaptor and Session manager.
LOGOS	" " (Null)	List of custom logo definitions used as background on display. Each logo tuple is delimited by commas. Each logo tuple contains logo label (verbatim label displayed on the screen) and logo URL. Logo label and URL are separated from one another by a '='. String maximum of 1023 characters.
LOGSRVR	" " (Null)	Syslog server IP or DNS address. 0 to 255 characters: zero or one IP Addresses in dotted decimal or DNS name format.
MEDIAENCRYPTION	9	This parameter sets the cryptosuite and session parameters for SRTP. The parameter can have one or two of the following nine values (separated by commas without any intervening spaces): 1=aescm128-hmac80 2=aescm128-hmac32 3=aescm128-hmac80-unauth 4=aescm128-hmac32-unauth 5=aescm128-hmac80-unenc 6=aescm128-hmac32-unenc 7=aescm128-hmac80-unenc-unauth 8=aescm128-hmac32-unenc-unauth 9=none
MSGNUM	" " (Null)	Voice mail system telephone/extension number. Specifies the number to be dialed automatically when the telephone user presses the **Message** button.
MTU_SIZE	1500	Maximum Transmission Unit size. Range is 1496 or 1500 only octets.

10 of 21

Table 11: 9600 Series SIP IP Telephones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
MUSICSRVR		List of Music-on-Hold Server IP or DNS address(es). Used to retrieve "Music on hold" for audio streams of sessions put on hold (in case of several entries first address always first, etc.). In some third-party proxy environments the SIP proxy/registrar might be different from the Music-on-Hold server. In this case, the Music-on-Hold server is set via this parameter. If both functions are provided by the same server, it is not necessary to set MUSICSRVR and the SIP proxy server is used for Music-on-Hold. Zero to 255 characters: zero or more IP addresses in dotted decimal or DNS name format, separated by commas without any intervening spaces. if operating in a non-Avaya environment, this value is set via a SET command in the settings file, otherwise the address of SIP Proxy server is used.
MWISRVR	" " (Null)	List of Message Waiting Indicator Event Server IP or DNS address(es). Used to register for MWI event notifications (in case of several entries first address always first, etc.). In some third-party proxy environments the SIP proxy/registrar may be different than the MWI server. In this case, the MWI server is set via this parameter. If both functions are provided by the same server, it is not necessary to set MWISRVR. The SIP proxy server is then used for MWI indications. Zero to 255 characters: zero or more IP addresses in dotted decimal or DNS name format, separated by commas without any intervening spaces. if operating in a non-Avaya environment, this value is set via a SET command in the settings file, otherwise the address of SIP Proxy server is used.
MYCERTCAID	CAIdentifier	Certificate Authority Identifier. String identifying whether the endpoints can work with another certificate authority.
MYCERTCN	$SERIALNO	Common name (CN) for SUBJECT in SCEP certificate request. Values are: $SERIALNO = the phone's serial number is included as CN parameter in the SUBJECT of a certificate request. $MACADDR = the phone's MAC address is included as CN parameter in the SUBJECT in the certificate request.
MYCERTDN	" " (Null)	Common part of SUBJECT in SCEP certificate request. String which defines the part of SUBJECT in a certificate request (including Organizational Unit, Organization, Location, State, Country), of 0 to 255 characters, starting with / and separating items with /.
MYCERTKEYLEN	1024	Private Key length in range of 1024 to 2048.
MYCERTRENEW	90	Threshold to renew certificate (given as percentage of device certificate's Validity Object). Range is 1 to 99.
MYCERTURL	" " (Null)	URL of SCEP server. String representing zero or one URI starting with "http://", 0 to 255 characters.

11 of 21

Table 11: 9600 Series SIP IP Telephones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
MYCERTWAIT	1	Flag defining phone's behavior when performing certificate enrollment. Values are: 0=wait until a certificate or a denial is received or a pending notification is received 1=periodical check in the background
NETMASK	0.0.0.0	IP subnet mask. Range is 7 to 15 ASCII characters defining one IP Address in dotted-decimal format.
NO_DIGITS_TIMEOUT	20	Number of seconds of delay after going "off-hook" or getting secondary dial tone before phone automatically plays a warning tone and does not accept dial input any longer. Range in seconds is 1 to 60.
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)	The number dialed when the Emerg softkey is pressed, or when a pop-up screen for making an emergency call is confirmed.
PHNCC	1	Telephone country code. The administered international country code for the location by the algorithm that dials calls from the incoming Call Log or from Web pages. Range: 1-3 digits, from “1” to “999.”
PHNDPLENGTH	5	Internal extension telephone number length. Specifies the number of digits associated with internal extension numbers by the algorithm that dials calls from the incoming Call Log or from Web pages. Range: 1 or 2 digits, from “3” to “13.”
PHNIC	011	Telephone international access code. The maximum number of digits, if any, dialed to access public network international trunks by the algorithm that dials calls from the incoming Call Log or from Web pages. Range: 0-4 digits.
PHNLD	1	Telephone long distance access code. The digit, if any, dialed to access public network long distance trunks. Range: 1 digit (0 to 9) or " " (Null). Needed to for "Enhanced Local Dialing Algorithm".
PHNLDLENGTH	10	Length of national telephone number. The number of digits in the longest possible national telephone number. Range: 5 to 15. Needed to for "Enhanced Local Dialing Algorithm".
PHNOL	9	Outside line access code. The character(s) dialed, including # and *, if any, to access public network local trunks. Range: 0-2 dialable numeric digits, including " " (Null).

12 of 21

Table 11: 9600 Series SIP IP Telephones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
PHNNUMOFSA	" " (Null)	When ENABLE_AVAYA_ENVIRONMENT=0, this value sets the number of Session Appearances.
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).
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.
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).
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.
POE_CONS_SUPPORT	1	Flag to activate Power over Ethernet conservation mode. Valid values are: 0 = the telephone does not support power conservation mode. 1 = the telephone indicates support of power conservation mode by transmission of LLDP frames with appropriate indication in Avaya/Extreme proprietary PoE Conservation Support Level TLV. The telephone supports power conservation mode, if requested by reception of an LLDP frame with Avaya/Extreme proprietary PoE Conservation Level Request.
		13 of 21

Table 11: 9600 Series SIP IP Telephones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
PRESENCE_SERVER	" " (Null)	List of Presence Server IP or DNS address(es). This value is used to access the server for presence indications (in case of several entries first address always first, etc.). In some environments the SIP proxy/ registrar may be different than the presence server. In this case, the presence server is set via this parameter. If both functions are provided by the same server, it is not necessary to set PRESENCE_SERVER - the SIP proxy server is accessed for server-based presence indications. Zero 0 to 255 characters: zero or more IP addresses in dotted decimal or DNS name format, separated by commas without any intervening spaces. When operating in a non-Avaya environment, this value is "set via a SET command in the settings file. If this value is not set, the SIP Proxy server address is used. When not set via settings file, this value is retrieved via PPM.
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 Access Code Entry screen, either during initialization or when Mute (or Contacts for the 9610) 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 local (dialpad) administrative procedures. Values are: 0 = Full access to craft local procedures 1 = restricted access to craft local procedures
PROVIDE_EDITED_ DIALING	2	Controls whether edited dialing is allowed and whether on-hook dialing is disabled. Valid values are: 0 = Disable edit dialing. "Dialing Options" is not displayed to the user so the user cannot change edit dialing; the telephone defaults to on-hook dialing. 1 = Disable on-hook dialing and do not display "Dialing Options" to the user so the user cannot change edit dialing; the telephone defaults to edit dialing. 2 = Display "Dialing Options" to allow user to change from on-hook to edit dialing. This is the default. 3 = Display "Dialing Options" to allow user to change from edit dialing to on-hook dialing; the telephone defaults to edit dialing.

14 of 21

Table 11: 9600 Series SIP IP Telephones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
PROVIDE_EXCHANGE_ CALENDAR	1	Flag to define whether or not menu item(s) for MS Exchange® Calendar integration are provided to the user. Values are 0=off, 1=on. If disabled, the menu item in Options&Settings sub-menu to select access to MS Exchange® Calendar is hidden to the user. If PROVIDE_EXCHANGE_CONTACTS is also disabled the complete sub-branch for MS Exchange® integration is hidden. Values are: 0=Off; 1=On.
PROVIDE_EXCHANGE_ CONTACTS	0	Flag to define whether or not menu item(s) for MS Exchange® Contacts integration are provided to user. If disabled, the menu item in “Options & Settings” sub-menu to select access to MS Exchange® Contacts is hidden. If PROVIDE_EXCHANGE_CALENDAR is also disabled the complete subbranch for MS Exchange® integration is hidden. Values are: 0=Off; 1=On.
PROVIDE_ LOGOUT	1	Flag to define whether or not logout function is provided to user. If disabled and phone is operating in user mode, hide "Logout" item in option menu. Values are: 0=off; 1=on
PROVIDE_ NETWORKINFO_ SCREEN	1	Flag to define whether or not "Network Information" menu is provided to user. If disabled and phone is operating in user mode, hide complete "Network Information". Values are: 0=off; 1=on
PROVIDE_OPTIONS_ SCREEN	1	Flag to define whether or not "Options & Settings" menu is provided to user. If disabled and phone is operating in user mode, hide complete "Option & Settings" menu tree. Values are: 0=off; 1=on
PROVIDE_TRANSFER_ TYPE	0	Flag to determine whether user can select a Transfer Type (Attended/Unattended) via the Avaya A Menu Call Settings options. Applies to 3rd party environments only. Values are: 0=user cannot select a transfer type, transfer type not shown; 1=user can select a transfer type, transfer type shown.
QKLOGINSTAT	0	Quick login status indicator. Specifies whether a password must always be entered manually, when the telephone is in a "registered and inactive" state (another telephone is used to take over a primary extension e.g. SIP visiting User). Valid values are: 0 = manual password entry is mandatory. 1 = quick-login is enabled; a "quick-login" is possible by pressing the Continue softkey on the login screen to accept the current password value.
REGISTERWAIT	3600	Number of seconds for next re-registration to SIP server. Range in second 10 - 1 000 000 000.
ROUTER	0.0.0.0	Address(es) of default router(s) / gateway(s) in the IP network. Range is 7-127 characters defining one or more IP Addresses in dotted decimal format, separated by commas without any intervening spaces.

15 of 21

Table 11: 9600 Series SIP IP Telephones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
RTCPCONT	1	Enables/disables the RTCP in parallel to RTP audio streams. Values are 0=RTCP disabled, 1=RTCP enabled.
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.
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.
SCREENSAVERON	240	Number of idle time minutes after which the screen saver is turned on. Valid values range from zero (disabled) to 999 minutes (16.65 hours).
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	0	Parameter to allow to download during start-up the specific configuration sets for H323 or SIP endpoints. Valid values are: 0=Default 1=H323 2=SIP
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.
SIP_MODE	0	Determines whether the telephone uses a proxy to receive incoming calls or can receive calls directly from another telephone. Values are: 0=proxy mode, 1=peer-to-peer mode.

16 of 21

Table 11: 9600 Series SIP IP Telephones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
SIP_PORT_SECURE	5061	Default SIP port (for secure message transfer via TLS). Values range from 1024 - 65535.
SIPCONFERENCECONTINUE	0	When the ENABLE_AVAYA_ENVIRONMENT parameter is 0 (non-Avaya environment) and the telephone initiating the conference ends the call, the other parties will be dropped unless SIPCONFERENCECONTINUE is set to 1 (continue conference call without initiator). If this parameter is set to 0, the capability is turned off and the phone ends the conference when the initiator hangs up.
SIPDOMAIN	" " (Null)	SIP domain name for registration. 0 to 255 characters: string representing domain name.
SIPPORT	5060	Default SIP port (for non-secure message transfer only). Values range from 1024 - 65535.
SIPREGISTRAR	" " (Null)	List of SIP registrar server IP or DNS address(es). Server(s) used to address SIP registrations, if operating in proxy mode. In case of several entries, the first address always first, etc. In some third-party environments the SIP proxy and SIP registrar may be different servers. In this case, the SIP registrar will be set using SIPREGISTRAR. If both functions are provided by the same server, it is not necessary to set the SIPREGISTRAR (i.e., this value will remain null). Zero to 255 characters: zero or more IP addresses in dotted decimal or DNS name format, separated by commas without any intervening spaces. Only set via SET command in settings file if you are operating in a non-Avaya environment. In an Avaya environment, this value is not applicable, because this is always identical to SIPPROXYSRVR.
SIPROXYSRVR	" " (Null)	SIP proxy/registrar server IP or DNS address. Zero or one IP Address. Format is dotted decimal or DNS format, separated by commas, with no spaces (0-255 ASCII characters, including commas).
SIPSIGNAL	2	SIP signaling transport protocol. Values are: 0=UDP 1=TCP 2=TLS over TCP

17 of 21

Table 11: 9600 Series SIP IP Telephones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
SKINS	" " (Null)	Applicable to the SIP 9640 IP Telephone only. Represents a list of skin information tuples. Each skin information is a pair of {skin label, skin URL} data. Each skin tuple is delimited by commas. Each skin tuple contains skin label (verbatim label displayed on the screen) and skin URL. Skin label and URL are separated by a ' ='. The URL may be specified in an absolute or relative path format ("./" for next higher directory level in relative path format; origin is the directory specified by HTTPDIR or TLSDIR depending on download via http or https). String maximum is 1023 characters. Example: Yankees (Color)=http://svn.avaya.com/drop/skins/ yankees_color/boohisscolor.xml
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.
SPEAKERSTAT	2	Limits the hands-free audio operation mode. Valid values are: 0=no speakerphone allowed 1=one-way speakerphone operation allowed (monitor) 2=two-way speakerphone operation allowed
SUBSCRIBE_SECURITY	2	Controls the use of SIP and SIPS subscriptions. Valid values are 0 - 2.
SUPPORT_GIGABIT	0	Flag indicating whether the telephone supports GigE (Gigabit Ethernet). Valid values are: 0=Telephone does not support GigE 1=Telephone supports GigE
SYSTEM_ LANGUAGE	" " (Null)	System Default Language definition. String representing a file name (shall be identical to one of the file names received via LANGUAGES parameter or null).
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.
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.

18 of 21

Table 11: 9600 Series SIP IP Telephones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
TCP_KEEP_ALIVE_TIME	60	This time interval is the time 9600 Series SIP IP Telephones 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.
TLSPORT	443	Destination TCP port used for requests to https server during initialization. Values: 0-65535.
TLSSRVRID	1	Flag to indicate if TLS server identification is required. Valid values are: 0 = no certificate match necessary; TLS/SSL connection will be established anyway. 1 = certificate match required; TLS/SSL connection will only be established if the server's identity matches the server's certificate.
TRUSTCERTS	" " (Null)	File names of certificates to be used for authentication. List of file names separated by commas (0 to 1024 characters).
USE_EXCHANGE_ CALENDAR	0	Activate/deactivate usage of calendar on Microsoft Exchange™ Server. Values are: 0=disabled, 1=enabled.
USE_QUAD_ZEROS_ FOR_HOLD	0	Flag that indicates whether a= directional attributes or 0.0.0.0 IP Address is used in the SDP to signal hold operation. 0=use “a= directional attributes”, 1=use quad zeros.
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 96.
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”).

19 of 21

Table 11: 9600 Series SIP IP Telephones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
VU_MODE	0	Visiting User mode. Determines, if and how the telephone supports Visiting User capabilities: 0 = Off; the telephone operates "normally" and "Visiting User" has no essential impact for normal operation. 1 = Optional; the telephone prompts the user at registration time if they are Visiting or Not. 2 = Forced; the telephone only allows Visiting User registrations.
VU_TIMER	36000	To Be Determined
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 1-60 (seconds).
WMLEXCEPT	" " (Null)	Exceptions domains for the WML browser proxy server. If WMLPROXY is resolved and WMLEXCEPT is null, the HTTP proxy server defined by WMLPROXY is used for all transactions of the WML browser application. If WMLEXCEPT is not null, the HTTP proxy server is only used for the URLs whose domains are not on the WMLEXCEPT list. Format is zero or more strings in DNS format, separated by commas without any intervening spaces.
WMLHOME	" " (Null)	Home page for WML browser. If this parameter is null, the telephone will not display the browser option under the "A" Avaya Menu. If non-null the URL specified is retrieved via HTTP and rendered in the Web page display area, when the WML browser application is initially accessed. Value is zero or one URL.
WMLIDLETIME	10	Number of minutes of inactivity until the Web browser will display the idle URL. When the Web idle timer reaches the number of minutes equal to this parameter, the telephone sends an HTTP GET for the URI specified by WMLIDLEURI. Valid value is 1-999. Note that the web idle timer starts only when access to the WML browser is provided by an application line under the "A" Avaya Menu and the parameter WMLIDLEURI is non-null.
WMLIDLEURI	" " (Null)	URL of web page displayed after idle timer expires. Note that the web idle timer will only be started when access to the WML browser is provided by an application line under the "A" Avaya Menu and the parameter WMLIDLEURI is non-null. Value is zero or one URL.
WMLPORT	8080	TCP port number to be used to access the HTTP proxy server by the WML browser application (if defined by WMLPROXY). Valid value is 0 - 65535.

20 of 21

Table 11: 9600 Series SIP IP Telephones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
WMLPROXY	" " (Null)	Address of WML proxy server. WMLPROXY is used as the HTTP proxy server by the WML browser application. If WMLPROXY is null, or if WMLPROXY cannot be resolved into a valid IP address, an HTTP proxy server is not used. Value is zero or one IP address in dotted decimal or DNS name format. Note that WMLPROXY defines the HTTP proxy server for WML browser application and HTTPPROXY to perform SCEP certificate enrollment.

21 of 21

Note:

Table 11 applies to all 9600 Series SIP IP Telephones. Certain 9600 SIP IP Telephones might have additional, optional information that you can administer. For more information, see Chapter 8: Administering Telephone Options.

VLAN Considerations

This section contains information on how to administer 9600 Series SIP IP Telephones 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* VLAN, set L2QVLAN to that VLAN, and provide voice traffic with priority over other traffic. You can set VLAN tagging manually, by DHCP, or in the 46xxsettings.txt file.

If VLAN tagging is enabled (L2Q= 0 or 1), the 9600 Series SIP IP Telephones set the VLAN ID to L2QVLAN, and the 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 9600 Series SIP IP Telephone will always transmit packets from the telephone at absolute priority over packets from secondary Ethernet. The priority settings are useful only if the downstream equipment is administered to give the *voice* VLAN priority.

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 9600 Series SIP IP Telephone 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 9600 Series SIP IP Telephone 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 Edition for 9600 Series SIP IP Telephones 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 802.1D 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 9600 Series SIP IP Telephone 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 9600 IP Series Telephone waits for a DHCPOFFER message when using a non-zero VLAN ID. The VLANTEST default is “60” seconds. Using VLANTEST ensures that the telephone 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 telephone restarts for any reason and the VLANTEST time limit expires, the telephone assumes the administered VLAN ID is invalid. The telephone 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 telephone 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 telephone. See the Reset procedure in the *Avaya one-X™ Deskphone Edition for 9600 Series SIP IP Telephones Installation and Maintenance Guide*.

VLAN Separation

VLAN separation is available to control priority tagging from the device on the secondary Ethernet, typically PC data. The following system parameters control VLAN separation:

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

Table 12 provides several VLAN separation guidelines.

Table 12: VLAN Separation Rules

If		Then
VLANSEP is “0”,	**OR** the telephone is not tagging frames, **OR** the telephone is tagging frames with a VLAN ID equal to PHY2VLAN.	Frames received on the secondary Ethernet interface will not be changed before forwarding. For example, tagging is not added or removed and the VLAN ID and tagged frames priority are not changed. The Ethernet switch forwarding logic determines that frames received on the Ethernet line interface are forwarded to the secondary Ethernet interface or to the telephone without regard to specific VLAN IDs or the existence of tags.
VLANSEP is “1” (On/Enabled)		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. Tagged frames with a VLAN ID of zero (priority-tagged frames) will either be: - forwarded without being changed (preferred), or - changed before they are forwarded such that the VLAN ID of the forwarded frame is equal to the PHY2VLAN value and the priority value is equal to the PHY2PRIO value.
VLANSEP is “1” (On/Enabled)	**AND** the telephone is not tagging frames, **OR** if the telephone is tagging frames with a VLAN ID equal to PHY2VLAN, **OR** if the PHY2VLAN value is zero.	The Ethernet switch forwarding logic determines that frames received on the Ethernet line interface are forwarded to the secondary Ethernet interface or to the telephone without regard to specific VLAN IDs or the existence of tags. Frames received on the secondary Ethernet interface will not be changed before forwarding. In other words, tagging is not added or removed, and the VLAN ID and priority of tagged frames is not changed.
VLANSEP is “1” (On/Enabled)	**AND** the telephone is tagging frames with a VLAN ID not equal to PHY2VLAN, **AND** the PHY2VLAN value is not zero.	Tagged frames received on the Ethernet line interface will only be forwarded to the secondary Ethernet interface if the VLAN ID equals PHY2VLAN. Tagged frames received on the Ethernet line interface will only be forwarded to the telephone if the VLAN ID equals the VLAN ID used by the telephone. Untagged frames 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 the telephone as determined by the forwarding logic of the Ethernet switch (preferred), or - dropped.

DNS Addressing

The 9600 Series SIP IP Telephones support DNS addresses and dotted decimal addresses. The telephone 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 56 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 telephone 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

Certain 9600 Series SIP IP Telephones 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 telephone forwards 802.1X multicast packets from the Authenticator to the PC attached to the telephone and forwards multicast packets from the attached PC to the Authenticator (multicast pass-through). Proxy Logoff is not supported.
- When DOT1X = 1, the telephone supports the same multicast pass-through as when DOT1X=0. Proxy Logoff is supported.
- When DOT1X = 2, the telephone forwards multicast packets from the Authenticator only to the telephone, ignoring multicast packets from the attached PC (no multicast pass-through). Proxy Logoff is not supported.

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

802.1X Pass-Through and Proxy Logoff

9600 Series SIP IP Telephones 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 Telephones 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 on the Ethernet line interface to the data switch on behalf of the attached PC. The message alerts the switch that the device is no longer present. Proxy logoff occurs only after at least one EAPOL frame with the Port Access Entity (PAE) group multicast address as the destination MAC address was received on the secondary Ethernet interface. The destination MAC address of the proxy EAPOL-Logoff frame is the PAE group multicast address. The source MAC address of the proxy EAPOL-Logoff frame is the same as the source MAC address of the last frame received on the secondary Ethernet interface that had the PAE group multicast address as the destination MAC address.

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

802.1X Supplicant Operation

9600 SIP IP Telephones 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] or with TLS.

If an EAP method in the configuration parameter DOT1XEAPS requires the authentication of a digital certificate, the standard authentication requirements apply, including matching the TLSSRVRID with that on the certificate.

If an EAP response requires an identity or a password, the values of the DOT1XID and DOT1XPSWD parameters will be used unless a new identity and/or password has been entered by the user via an 802.1X User Input interrupt screen, in which case the new values entered by the user will be used instead. The ID and password are not overwritten by telephone software downloads. For all EAP methods, if the Supplicant is unauthenticated, an 802.1X Waiting interrupt screen is displayed when a response is transmitted, unless an 802.1X User Input interrupt screen is already being displayed.

If an EAP-Failure frame is received after transmitting a response that contains an identity or a password, an 802.1X User Input interrupt screen is displayed, unless an 802.1X User Input interrupt screen is already being displayed. If an EAP-Failure frame is received after transmitting a response that did not contain an identity or a password, an 802.1X Failure interrupt screen is displayed.

When a telephone 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 IP telephone does not accept null value passwords. See “Dynamic Addressing Process” in the *Avaya one-X™ Deskphone Edition for 9600 Series SIP IP Telephones Installation and Maintenance Guide*. The telephone 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.

An IP telephone 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 telephone is configured for Supplicant Mode (DOT1X=2), the telephone can support authentication from the switch.
- **Telephone with attached PC (Telephone Only Authenticates)** - When the telephone is configured for Supplicant Mode (DOT1X=2), the telephone 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 telephone is configured for Pass-Through Mode or Pass-Through Mode with Logoff (DOT1X=0 or 1), 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 telephone (Telephone Only Authenticates)** - When the telephone is configured for Supplicant Mode (DOT1X=2), the telephone can support authentication from the switch. When DOT1X is "0" or "1" the telephone is unable to authenticate with the switch.
- **Telephone and PC Dual Authentication** - Both the telephone and the connected PC can support 802.1X authentication from the switch. The telephone may be configured for Pass-Through Mode or Pass-Through Mode with Logoff (DOT1X=0 or 1). 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 Telephones 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 9600 Series IP Telephones 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).

9600 Series IP Telephones running SIP Release 2.0 software support IEEE 802.1AB if the value of the configuration parameter LLDP_ENABLED is "1" (On) or "2" (Auto). If the value of LLDP_ENABLED is “0” (off), the transmission and reception of Link Layer Discovery Protocol (LLDP) is not supported. When the value of LLDP_ENABLED is “2”, the transmission of LLDP frames will not begin until or unless an LLDP frame is received, and the first LLDP frame will be transmitted within 2 seconds after the first LLDP frame is received. Once transmission begins, an LLDPDU will be transmitted every 30 seconds.

Note:

There could be a delay of up to 30 seconds in telephone initialization if the file server address is delivered by LLDP and not by DHCP.

These telephones:

- 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 9600 Series IP Telephone 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 9600 Series SIP IP Telephones

Category	TLV Name (Type)	TLV Info String (Value)
Basic Mandatory	Chassis ID	IPADD of telephone, IANA Address Family Numbers enumeration value for IPv4, or subtype 5:Network address.
Basic Mandatory	Port ID	MAC address of the telephone.
Basic Mandatory	Time-To-Live	120 seconds.

1 of 3

Table 13: LLDPDU Transmitted by 9600 Series SIP IP Telephones (continued)

Category	TLV Name (Type)	TLV Info String (Value)
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 capabilities = 00-33 (Inventory, Power-via-MDI, Network Policy, MED Caps).
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	Telephone serial number.
TIA LLDP MED	Inventory – Manufacturer Name	Avaya.
TIA LLDP MED	Inventory – Model Name	MODEL with the final D***xxx*** characters removed.
		2 of 3

Table 13: LLDPDU Transmitted by 9600 Series SIP IP Telephones (continued)

Category	TLV Name (Type)	TLV Info String (Value)
Avaya Proprietary	PoE Conservation Level Support	Provides Power Conservation abilities/settings, Typical and Maximum Power values. OUI = 00-40-0D (hex), Subtype = 1. Current conservation level=POE_CONS_MODE.
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	CNA Server IP Address	CNA Server IP Address = in-use value from CNASRVR. Subtype = 5.
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.

3 of 3

On receipt of a LLDPDU message the Avaya IP Telephones will act on these TLV elements.

Table 14: Impact of TLVs 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 is set to 1 (ON). 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. VLAN Name TLV is ignored if: ● the value of USE_DHCP is “0” and the value of IPADD is not “0.0.0.0”, or ● the current value of L2QVLAN was set by a TIA LLDP MED Network Policy TLV, or ● the VLAN name in the TLV does not contain the substring “voice” in lower-case, upper-case or mixed-case ASCII characters anywhere in the VLAN Name.
L2Q, L2QVLANID, L2QAUD, L2QSIG, DSCPAUD, DSCPSIG	TIA LLDP 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), or ● the Unknown Policy Flag (U) is set to 1.
SIPPROXYSRVR	Proprietary Call Server TLV	SIPPROXYSRVR will be set to the IP Address(es) in this TLV value.
TLSSRVR and HTTPSRVR	Proprietary File Server TLV	TLSSRVR and HTTPSRVR will be set to the IP Address(es) in this TLV value.

Table 14: Impact of TLVs on System Parameter Values (continued)

System Parameter Name	TLV Name	Impact
L2Q	Proprietary 802.1 Q Framing	If TLV = 1, L2Q set to "1" (On). If TLV = 2, L2Q set to "2" (Off). If TLV = 3, L2Q set to "0" (Auto). 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 current L2QVLAN value was set by an IEEE 802.1 VLAN Name, or ● the current L2QVLAN value was set by a TIA LLDP MED Network Policy TLV.
POE_CONS_ SUPPORT	Proprietary - PoE Conservation Level Request TLV	If the value of POE_CONS_SUPPORT is “1”, POE_CONS_MODE is set to the level requested in the TLV.

Visiting User Administration

A "visiting user" is anyone who logs into a 9600 Series SIP IP Telephone that is not his or her primary phone at the user’s home location. This could mean that the visiting user can log into a telephone that is across the country from the home location or one in the office adjacent to the home office. When registered as a visiting user:

- An inactivity timer is used to trigger inactivity and thereby un-register a user.The Visiting User Inactivity Timer value is communicated to the telephone via Personal Profile Manager (PPM). The Visiting User Inactivity Timer is a local timer (VUTIMER) in the telephone that has the same value as the EMU timer value that is set in Avaya Communication Manager (CM). The inactivity timer is relevant when users are served through a SIP Enablement Services (SES) that is not their home SES.
- Registration Events with "Q value" of 0 result in a logout. When a new registration is sent from a visiting roaming or non-roaming telephone, the visiting telephone takes priority over the user's home or primary telephone. Outbound calls can be made from either the visiting telephone or the primary telephone. The home SES lowers the q-value of previous registrations to zero and promotes the new registration to ensure that inbound calls will be routed to the most recent telephone registered.

- The telephone will un-register if it is a visiting user telephone. But that telephone will become registered inactive if it is the primary telephone.

Set the VU_MODE configuration parameter value in the settings file to determine the visiting user login routine. VU_MODE determines whether the phone will support Visiting User capabilities as follows:

- If the VU_MODE value is zero (Off) the telephone is considered a non-VU phone. This is the default value and the value associated with the user's "home" phone. The inactivity timer is not applied when VU_MODE is 0.
- If the VU_MODE value is 1 (Optional), the telephone presents the user with the Login Screen with a Primary Phone yes/no toggle field, for the user to designate whether the telephone is that user's primary phone. If the user selects "yes", then the phone operates as a non-visiting user telephone and the inactivity timer is not applied. If the user selects "no", then the telephone operates in the visiting user mode where an inactivity timer will log the user off after a predetermined time.
- If the value is 2 (Forced), the telephone is always in the visiting user mode and the inactivity timer is always applied.

Emergency Number Administration

Set the PHNEMERGNUM configuration parameter in the settings file to assign an emergency telephone number. This telephone number will be automatically dialed whenever the **Emerg** softkey is selected on the Login screen, or the Phone screen, or when the user chooses the **Yes** softkey on an Emergency pop-up screen.

The local proxy routes emergency calls from a user at a visited phone so that the local emergency number is called. When PHNEMERGNUM is administered, using the **Emerg** softkey overrides the SPEAKERSTAT parameter setting or a user-selected referred audio path. This means that the even if the Speakerphone is disabled it is the default transducer when the user presses the **Emerg** softkey.

Local Administrative (Craft) Options Using the Telephone Dialpad

The *Avaya one-X™ Deskphone Edition for 9600 Series SIP IP Telephones Installation and Maintenance Guide* details how to use Craft local procedures at the telephone for administration. The local procedures you might use most often as an administrator are:

- **ADDR** - Static address programming.
- **CLEAR** - Remove all administered values, user-specified data, option settings, etc. and return a telephone to its initial “out of the box” default values.
- **DEBUG** - Enable or disable debug mode for the button module serial port.
- **GROUP** - Set the group identifier on a per-phone basis.
- **INT** - Locally enable or disable the secondary Ethernet hub.
- **RESET** - Reset the telephone to default values including the registration extension and password, any values administered through local procedures, and values previously downloaded using DHCP or a settings file.
- **RESTART** - Restart the telephone in response to an error condition, including the option to reset system values.
- **SIG -** Change the default signaling value to/from SIP, or change SIG to/from H.323. Chapter 2 of the *Avaya one-X™ Deskphone Edition for 9600 Series SIP IP Telephones Installation and Maintenance Guide* also describes how to determine which SIG value is appropriate for your environment.
- **SIP** - Configure SIP call settings.
- **VIEW** - Review the system parameters for the telephone to verify current values and file versions.

Language Selection

9600 Series IP Telephones are factory-set to display information in the English language. In addition to English, SIP software bundle downloads include the following language files:

- Canadian French
- Parisian French
- Latin American Spanish
- German
- Brazilian Portuguese
- Italian
- Dutch
- Castilian Spanish
- Russian
- Simplified Chinese
- Japanese
- Korean

Administrators can specify from one to four languages per telephone to replace English. End users can then select which of those languages they want their telephone to display.

All downloadable language files contain all the information needed for the telephone to present the language as part of the user interface.

Use the configuration file (46xxsettings.txt) and these parameters to customize the settings for up to four languages:

- **LANGUAGES** - the list of languages to be downloaded from which the end user can select a desired display language. Each language is listed in the following format: Mls_Spark_German.xml, Mls_Spark_English.xml, Mls_Spark_CastilianSpanish.xml, and so on.
- **SYSTEM_LANGUAGE** - a string indicating the filename of the default system language. The string indicates which of the available languages to use for display purposes. If this parameter is not set, or if no other language has been set by the user, or if a user language choice cannot be satisfied, the built-in English strings are used.
- **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 default) the user can select the built-in English language text strings.

For more information, see 9600 Series SIP IP Telephones Customizeable System Parameters. To view multiple language strings, see the MLS local procedure in the *Avaya one-X™ Deskphone Edition for 9600 Series SIP IP Telephones Installation and Maintenance Guide*. To download a language file or review pertinent information, go to http://support.avaya.com/unicode.

Note:

Specifying a language other than English in the configuration file has no impact on Avaya Communication Manager settings, values, or text strings.

Enhanced Local Dialing

The 9600 Series SIP IP Telephones have a variety of telephony-related applications that might obtain a telephone number during operation. For example, the Call Log saves a number of an incoming caller, but does not consider that the user has to then prepend the saved number with a digit to dial an outside line, and possibly a digit to dial long distance.

9600 Series SIP IP Telephones can evaluate a raw telephone number, based on administered parameters. The telephone can automatically prepend the correct digits, saving the user time and effort. This is the Enhanced Local Dialing feature. The key to the success of this feature is accurate administration of several important values, summarized below.

The system values relevant to the Enhanced Dialing Feature are:

- **ENHDIALSTAT** - Enhanced dialing status. If set to “1” the enhanced local dialing feature is partially enabled, meaning dialing rules do not apply to dialing from the Contacts list. If set to "2" the enhanced local dialing feature is fully enabled and does apply to dialing from the Contacts list. If set to “0” enhanced local dialing is off.
- **PHNCC** - the international country code of the Communication Manager (CM) call server. For example, “1” for the United States, “44” for the United Kingdom, and so on.
- **PHNDPLENGTH** - the length of the dial plan on the CM call server.
- **PHNIC** - the digits the CM call server dials to access public network international trunks. For example, “011” for the United States.
- **PHNLD** - the digit dialed to access public network long distance trunks on the CM call server.
- **PHNLDLENGTH** - the maximum length, in digits, of the national telephone number for the country in which the CM call server is located.
- **PHNOL** - the character(s) dialed to access public network local trunks on the CM call server.

Note:

In all cases, the values you administer are the values relevant to the location of the CM call server at which the IP telephones are registered. If a telephone is in Japan, but its CM call server is in the United States, set the **PHNCC** value to “1" for the United States.

In all cases, the digits the telephones insert and dial are subject to standard CM call server features and administration. This includes Class of Service (COS), Class of Restriction (COR), Automatic Route Selection (ARS), and so on.

As indicated in Table 11, you can administer the system parameter **ENHDIALSTAT** to turn off the Enhanced Local Dialing feature.

Example: A corporate voice network has a 4-digit dialing plan. The corporate WML Web site lists a 4-digit telephone number as a link on the Human Resources page. A 9620 user selects that link. The 9620 deduces the telephone number is part of the corporate network because the length of the telephone number is the same as the corporate dialing plan. The telephone dials the number without further processing.

Example: A user notes a Web site contains an international telephone number that needs to be called and initiates the call. The telephone determines the number to be called is from another country code. The telephone then prepends the rest of the telephone number with PHNOL to get an outside line and PHNIC to get an international trunk. The telephone then dials normally, with the CM call server routing the call appropriately.

Enhanced Local Dialing Requirements

The enhanced local dialing feature is invoked when all the following conditions are met:

- An application on a 9600 Series IP Telephone obtains or otherwise identifies a character string as containing a telephone number the user wants to dial, and
- The Phone application determines a call appearance is available for an outgoing call, and
- The originating application passes the character string to the Phone application, and
- The originating application specifies a Source Flag set to **No**, and
- The current value of ENHDIALSTAT is “1” (partially enabled) or “2” (fully enabled).

The Phone application takes the incoming character string, applies an algorithm, and determines the string of digits to be sent to Avaya Communication Manager (CM) for dialing. At this point the Phone application goes off-hook and sends the digits to CM.

The Source Flag has two possible values:

- Yes - the Called Party Number has been administered or otherwise identified as a valid outgoing phone number, such as a Speed Dial button, Redial number, or Outgoing Call Log number, or
- No - the Called Party Number comes from a source that is likely to require enhanced local dialing processing, for example, the Incoming Call Log application.

Note:

The Enhanced Local Dialing algorithm requires that telephone numbers be presented in a standard format. The standard format depends on how you administer the parameters indicated in Table 11. The algorithm also assumes that international telephone numbers are identified as such in, for example, the Contacts application. Precede international numbers with a plus (+) sign, and a space or some non-digit character following the country code.

Chapter 9: Administering Applications and Options

Customizing Telephone Applications and Options

This chapter covers configuration options for activating/deactivating options and applications. The 9600 Series SIP IP Telephones offer the user numerous applications like Contacts, Call Log, Redial, and so on. Each of these applications allows the user to add, delete, or in some cases, edit entries. As the administrator, you might not want the user to have that level of functionality.

This chapter also contains information related to administering the Avaya A Menu to include the WML browser, and other browser setup information.

In 4600 and 9600 Series H.323 IP Telephones, the parameters APPSTAT (meaning Application permission status) and OPSTAT (meaning Options permission status) control application access and functionality. However, 9600 Series SIP IP Telephones have a more granular way of assigning functionality, with a specific parameter for each permission, as follows:

- **ENABLE_CALL_LOG** - Allows end user access to the list of unanswered and answered calls. If disabled, the Call Log application is not displayed to the user and calls are not logged.
- **ENABLE_REDIAL** - Allows the end user to redial one to three previously called numbers. If disabled, redialing is not available to the end user.
- **ENABLE_REDIAL_LIST** - Allows the end user to select a number to redial from a list. If disabled, only the previously-dialed number can be redialed.
- **ENABLE_CONTACTS** - Allows end user access to a list of numbers and to make calls by selecting a Contact Name/Number. If disabled, the Contacts application is not displayed to the user and a Contact list cannot be set up or maintained.
- **ENABLE_MODIFY_CONTACTS** - If the Contacts application is enabled (ENABLE_CONTACTS=1), this option allows or prevents the end user from changing or updating the Contact list.
- **PROVIDE_OPTIONS_SCREEN** - If disabled, the Options & Settings menu is not displayed on the Avaya menu. The user cannot change any of the features and options associated with the Options & Settings menu.
- **PROVIDE_NETWORKINFO_SCREEN** - If disabled, the Network Information menu is not displayed on the Avaya menu.
- **PROVIDE_LOGOUT** - If disabled, Logout is not displayed to the user as an option on the Avaya menu.

These parameters have On (1=enabled)/Off (0=disabled) settings, and are described in detail in Table 11: 9600 Series SIP IP Telephones Customizeable System Parameters.

Note:

To facilitate administration of application-related parameters, the 9600 Series (both SIP and H.323) and 4600 Series IP Telephones use the same ***46xxsettings.txt*** file.

Avaya “A” Menu Administration

The A (Avaya) Menu is a list of sub-applications the user can select to invoke the corresponding functionality. The Avaya Menu contains these entries in this order:

- Options & Settings
- Browser (only if WMLHOME administered in settings file)
- Network Information
- Log Out
- About Avaya one-X

Each individual sub-application is listed left justified on an individual Application Line.

Administering Standard Avaya Menu Entries

Options & Settings is listed if and only if the PROVIDE_OPTIONS_SCREEN configuration parameter value is 1.

Network Information is listed if and only if the PROVIDE_NETWORKINFO_SCREEN configuration parameter value is 1.

Logout is listed if and only if the PROVIDE_LOGOUT configuration parameter value is 1.

Administering the WML Browser

SIP software Release 2.0 provides a WML Browser which, if administered, follows the Options and Settings listing on the Avaya (A) Menu.

Note:

WML applications are accessed from the Browser.

Set the configuration parameter WMLHOME in the settings file to link the Browser Home page to the Avaya (A) Menu and to include the Browser option on the Avaya (A) Menu. The Browser application is listed if and only if it is properly administered as specified in *Avaya one-X*™

Deskphone Edition for 9600 IP Telephones Application Programmer Interface (API) Guide (Document Number 16-600888).

In addition to WMLHOME, other browser-related configuration parameters which can be set using the 46xxsettings.txt file (as applicable to your environment) are:

- WMLEXCEPT - Exception domain for the WML browser proxy server.
- WMLIDLETIME - Number of minutes of inactivity until the Web browser will display the idle URL specified in WMLIDLEURI.
- WMLIDLEURI - URL of web page to be displayed after idle timer (WMLIDLETIME) expires.
- WMLPORT - TCP port number the WML browser application should use to access the HTTP proxy server (if defined by WMLPROXY).
- WMLPROXY - Proxy server address to be used by the WML browser application.

For detailed information about WML Browser configuration parameters, see Table 11: 9600 Series SIP IP Telephones Customizeable System Parameters.

Appendix A: Glossary of Terms

802.1D **802.1Q**	802.1Q defines a layer 2 frame structure that supports VLAN identification and a QoS mechanism usually referred to as 802.1D.
802.1X	Authentication method for a protocol requiring a network device to authenticate with a back-end Authentication Server before gaining network access. Applicable 9600 Series IP telephones support IEEE 802.1X for pass-through and for Supplicant operation with the EAP-MD5 authentication method. SIP Software Release 2.0 and up supports 802.1X.
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, a type of 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 9600 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.
EAP	Extensible Authentication Protocol, or EAP, a universal authentication framework frequently used in wireless networks and Point-to-Point connections defined by RFC 3748. EAP provides some common functions and a negotiation of the desired authentication methods, two of which are EAP-MD5 and EAP-TLS. When EAP is invoked by an 802.1X enabled NAS (Network Access Server) device such as an 802.11 a/b/g Wireless Access Point, modern EAP methods provide a secure authentication mechanism and negotiate a secure PMK (Pair-wise Master Key) between the client and the NAS.
H.323	A TCP/IP-based protocol for VoIP signaling. An alternative to SIP for VoIP signaling. One of the two protocols 9600 Series IP Telephones support.
HTTP	Hypertext Transfer Protocol, used to request and transmit pages on the World Wide Web.

1 of 3

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. SIP Software Release 2.0 and up supports LLDP.
MAC	Media Access Control, ID of an endpoint.
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.
PPM	Personal Profile Manager, part of the SIP Enablement Services (SES) platform. PPM is responsible for maintaining and managing end users' personal information in the system.
Proxy Server	An intermediary entity that acts as both a server and a client for the purpose of making requests on behalf of other clients. A proxy server primarily plays the role of routing, meaning its job is to ensure that a request is sent to another entity "closer" to the targeted user. Proxies are also useful for enforcing policy, for example, making sure a user is allowed to make a call. A proxy interprets, and if necessary, rewrites specific parts of a request message before forwarding it.
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.
SCEP	Simple Certificate Enrollment Protocol, used to obtain a digital certificate.
SDP	Session Description Protocol. A well-defined format for conveying sufficient information to discover and participate in a multi session.

2 of 3

SES	SIP Enablement Services, the Avaya solution for SIP telephony with Avaya Communication Manager.
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 channel encryption.
SIP	Session Initiation Protocol, an open standard defined initially by IETF RFC 3261. SIP is an alternative to H.323 for VoIP signaling, both of which 9600 Series IP Telephones support.
SNTP	Simple Network Time Protocol. An adaptation of the Network Time Protocol used to synchronize computer clocks in the internet.
SRTCP	Secure Real-time Transport Control Protocol.
SRTP	Secure Real-time Transport Protocol.
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. SIP IP telephones use HTTP or HTTPS instead of TFTP.
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.
TLV	Type-Length-Value elements transmitted and received as part of Link Layer Discovery Protocol (LLDP).
UDP	User Datagram Protocol, a connectionless transport-layer protocol.
Unnamed Registration	Registration with Avaya Communication Manager by an IP telephone with no extension. Allows limited outgoing calling.
URI & URL	Uniform Resource Identifier and Uniform Resource Locator. Names for the strings used to reference resources on the Internet (for example, HTTP://....). URI is the newer term.
VLAN	Virtual LAN.
VoIP	Voice over IP, a class of technology for sending audio data and signaling over LANs.
WML	Wireless Markup Language, used by the 9600 Series IP Telephone Web Browser to communicate with WML servers.

3 of 3

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: Sample Station Forms

Use the sample screens that follow as guidelines for telephone setup.

Figure 1: Station Form - Basic Telephone Information

```
add station next                                              Page 1 of X
                              STATION

Extension:                    Lock Messages? n                        BCC: 0
     Type:                    Security Code:                           TN: 1
     Port:                  Coverage Path 1:                          COR: 1
     Name:                  Coverage Path 2:                          COS: 1
                            Hunt-to Station:

STATION OPTIONS
      XOIP Endpoint type: auto                Time of Day Lock Table:
              Loss Group: 2         Personalized Ringing Pattern: 3
             Data Module? n                     Message Lamp Ext: 1014
            Speakerphone: 2-way              Mute button enabled? y
        Display Language? English
                   Model:                       Expansion Module?

 Survivable GK Node Name:                      Media Complex Ext:
          Survivable COR:                           IP Softphone? y
   Survivable Trunk Dest?                    Remote Office Phone? y
                                              IP Video Softphone?
                                                        IP Video?

                                             Customizable Labels?
```

Figure 2: Station Form - Feature Options

```
change station nnnn                                            Page 2 of X
                                    STATION

FEATURE OPTIONS
           LWC Reception? spe           Auto Select Any Idle Appearance? n
          LWC Activation? y                      Coverage Msg Retrieval? y
  LWC Log External Calls? n                                 Auto Answer: none
             CDR Privacy? n                             Data Restriction? n
   Redirect Notification? y                      Call Waiting Indication:
 Per Button Ring Control? n                Attd. Call Waiting Indication:
   Bridged Call Alerting? n                  Idle Appearance Preference? n
        Switchhook Flash? n             Bridged Idle Line Preference? y
    Ignore Rotary Digits? n                   Restrict Last Appearance? y
  Active Station Ringing: single        Conf/Trans On Primary Appearance? n
                                                       EMU Login Allowed?
        H.320 Conversion? n        Per Station CPN - Send Calling Number? _
       Service Link Mode: as-needed      Busy Auto Callback without Flash? y
         Multimedia Mode: basic
    MWI Served User Type: ______              Display Client Redirection? n
         Automatic Moves:
              AUDIX Name:                    Select Last Used Appearance? n
                               _               Coverage After Forwarding? _
     Recall Rotary Digit? n                      Multimedia Early Answer? n

Remote Softphone Emergency Calls: as-on-local Direct IP-IP Audio Connections? n
Emergency Location Ext: 75001      Always use? n       IP Audio Hairpinning? n
Precedence Call Waiting? y
```

Figure 3: Station Form - Call Appearance Info & Enhanced Call Forwarding

```
add station next                                                 Page 3 of x
                                    STATION


          Conf/Trans on Primary Appearance? y
Bridged Appearance Origination Restriction? y
            Call Appearance Display Format: loc-param-default

                             ENHANCED CALL FORWARDING
                                      Forwarded Destination        Active
Unconditional For Internal Calls To:                                  n
                  External Calls To:                                  n
         Busy For Internal Calls To:                                  n
                  External Calls To:                                  n
     No Reply For Internal Calls To:                                  n
                  External Calls To:                                  n

           SAC/CF Override? n
```

Figure 4: Station Form -Site Data, Feature Button Assignments, Voice Mail #

```
add station nnnn                                                 Page 4 of X
                                    STATION

     SITE DATA
          Room: _______                                     Headset? n
          Jack: ___                                         Speaker? n
         Cable: ___                                        Mounting: d
         Floor: _______                                 Cord Length: 0_
      Building: _______                                   Set Color: _____


ABBREVIATED DIALING
     List1: ________          List2: _________          List3: _________

BUTTON ASSIGNMENTS
 1: call-appr                 6:limit-call
 2: call-appr                 7:team     Ext: 5381231         Rg:
 3: call-appr                 8:cfwd-enh Ext:
 4: audix-rec  Ext: 4000      9:cfwd-enh Ext: 5502
 5: release                  10:aux-work RC: 1 Group:

voice-mail Number:
```

Figure 5: Station Form - Additional Feature Button Assignments

```
change station nnnn                                              Page 5 of x
                                      STATION

FEATURE BUTTON ASSIGNMENTS

 9:
10:
11:
12:
13:
14:
15:
16:
17:
18:
19:
20:
21:
22:
23:
24:
```

Figure 6: SIP Feature Options

```
change station nnnn                                              Page 5 of x
                                    STATION

SIP Feature Options
         Type of 3PCC Enabled: none
```

Figure 7: Feature-Related System Parameters Form

```
change system-parameters features                              page 11 of x
                        FEATURE-RELATED SYSTEM PARAMETERS

CALL CENTER SYSTEM PARAMETERS
  EAS
        Expert Agent Selection (EAS) Enabled? n
       Minimum Agent-LoginID Password Length:
         Direct Agent Announcement Extension: ________           Delay: ___
   Message Waiting Lamp Indicates Status For: station
VECTORING
                   Converse First Data Delay: 0       Second Data Delay: 2
              Converse Signaling Tone (msec): 100          Pause (msec): 70_
                    Prompting Timeout (secs): 10
                Interflow-qpos EWT Threshold: 2
   Reverse Star/Pound Digit For Collect Step? n
         Available Agent Adjustments for BSR? n
                           BSR Tie Strategy? 1st_found
  Store VDN Name in Station’s Local Call Log? n

SERVICE OBSERVING
             Service Observing: Warning Tone? n      or Conference Tone? n
    Service Observing Allowed with Exclusion? n
            Allow Two Observers in Same Call? n
```

Figure 8: IP Address Mapping Form

```
change ip-network-map                                          Page 1 of X

                     IP ADDRESS MAPPING
                                                                 Emergency
                                   Subnet             802.1Q     Location
FROM IP Address   (TO IP Address or Mask)   Region     VLAN      Extension
  1.__2.__3.__0    1.__2.__3.255    24       __1        ___3     ________
  1.__2.__4.__4    1.__2.__4.__4    32       __2        ___0     ________
  1.__2.__4.__5    1.__2.__4.__5    __       __3        ___0     ________
  1.__2.__4.__6    1.__2.__4.__9    __       __4        ___4     ________
___.___.___.___  ___.___.___.___    __       ___        ____     ________
___.___.___.___  ___.___.___.___    __       ___        ____     ________
___.___.___.___  ___.___.___.___    __       ___        ____     ________
___.___.___.___  ___.___.___.___    __       ___        ____     ________
___.___.___.___  ___.___.___.___    __       ___        ____     ________
___.___.___.___  ___.___.___.___    __       ___        ____     ________
___.___.___.___  ___.___.___.___    __       ___        ____     ________
___.___.___.___  ___.___.___.___    __       ___        ____     ________
___.___.___.___  ___.___.___.___    __       ___        ____     ________
```

Figure 9: IP Network Region Form

```
change ip-network-region n                                         Page 1 of x
                             IP NETWORK REGION
  Region: n
Location:                  Authoritative Domain:
    Name:
                                Intra-region IP-IP Direct Audio: n
MEDIA PARAMETERS                Inter-region IP-IP Direct Audio: n
   Codec Set: 1                            IP Audio Hairpinning? n
UDP Port Min: 2048
UDP Port Max: 3028                       RTCP Reporting Enabled? y
                                  RTCP MONITOR SERVER PARAMETERS
DIFFSERV/TOS PARAMETERS           Use Default Server Parameters? y
 Call Control PHB Value:                       Server IP Address:   .   .   .
        Audio PHB Value:                             Server Port: 5005
        Video PHB Value:

802.1P/Q PARAMETERS                      RTCP Report Period(secs): 5
 Call Control 802.1p Priority: 7
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 7
                                       AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? y
  H.323 Link Bounce Recovery? y              RSVP Refresh Rate(secs): 15
 Idle Traffic Interval (sec): 20      Retry upon RSVP Failure Enabled? y
   Keep-Alive Interval (sec): 6                          RSVP Profile:
            Keep-Alive Count: 5       RSVP unreserved (BBE) PHB Value: 40
```

Figure 10: IP Network Region (page 2)

```
change ip-network-region n                                      Page 2 of x

                                 IP NETWORK REGION

INTER-GATEWAY ALTERNATE ROUTING/DIAL PLAN TRANSPARENCY
Incoming LDN Extension:
Conversion to Full Public Number - Delete: ___Insert: ___
 Maximum Number of Trunks to Use for IGAR:
Dial Plan Transparency in Survivable Mode? n

BACKUP SERVERS IN PRIORITY ORDER            H.323 SECURITY PROCEDURES
1                                           1
2                                           2
3                                           3
4                                           4
5
6                                          Allow SIP URI Conversion? y

TCP SIGNALING LINK ESTABLISHMENT FOR AVAYA H.323 ENDPOINTS
   Near End Establishes TCP Signaling Socket? y
                       Near End TCP Port Min: 61440
                       Near End TCP Port Max: 61444
```

Figure 11: Stations with Off-PBX Telephone Integration Form

```
add off-pbx-telephone station-mapping                                    Page 1 of 2
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

Station     Application   Dial     CC     Phone Number          Trunk       Config
Extension                 Prefix                                Selection   Set
43001         EC500       ____ -   1      9736831204            ars         1
43001         OPS         ____ -          12345                 ars         5
43009         EMU         ____ -          67890                 aar         2
43011         CSP         ____ -   998    6095343211            ars         3
_______       ______      ____ -          _______________       ____        __
_______       ______      ____ -          _______________       ____        __
_______       ______      ____ -          _______________       ____        __
```

Figure 12: IP Codec Set Form

```
change ip-codec-set n                                           Page 1 of x

                              IP Codec Set

      Codec Set: 1

     Audio         Silence        Frames    Packet
     Codec         Suppression    Per Pkt   Size (ms)
1: G.711MU            y              3         30
2:_______________    _              _
3:_______________    _              _
4:_______________    _              _
5:_______________    _              _
6:_______________    _              _
7:_______________    _              _

Media Encryption:
1: aes
2: aea
3: srtp-aescm128-hmac80
```

Figure 13: IP Codec Set screen page 2

```
change ip-codec-set n                                    Page   2 of   x

                             IP Codec Set

                                 Allow Direct-IP Multimedia? y
        Maximum Bandwidth Per Call for Direct-IP Multimedia: 256:Kbits

                    Mode        Redundancy

            FAX     relay          0

          Modem     off            0

        TDD/TTY     us             0

  Clear-channel     n              0
```

Figure 14: Inter Network Region Connection Management screen

```
change ip-network-region n                                        Page   3 of x

                   Inter Network Region Connection Management

 src dst codec direct   Total          Video                          Dyn
 rgn rgn  set  WAN   WAN-BW limits Norm Prio Shr Intervening-regions   CAC IGAR
 3   1    1       y    256:Kbits             y                              n
 3   2    1       n       :NoLimit           n                              n
 3   3    1               :NoLimit                                          n
 3   4    1       n       :NoLimit           n                              n
 3   5    1       n       :NoLimit           n                              n
 3   6    1       y       :NoLimit           y                              n
 3   7    1       y     10:Calls             y                              n
 3   8
 3   9
 3   10
 3   11
 3   12
 3   13
 3   14
 3   15
```

The entries on the IP Address network map shown in Figure 8 might redirect endpoints into a particular network region. That region could be different from what is administered on the previous forms.

Figure 15: Numbering - Public/Unknown Format Form

```
change public-unknown-numbering 5                                   Page 1 of X
                       NUMBERING - PUBLIC/UNKNOWN FORMAT
Total
Ext Extension       Trk       CPN            CPN
Len Code            Grp(s)    Prefix         Len
 12 1234567890123   123456789 123456789012345 12

 5 4                777777                    10
 5 4                250       30379           10
 5 4                253       30379           10
 5 41               40        303222          11
 5 41               45                        5
 5 41               87        30323           10
 5 43               538                       7
 5 45               222                       7
 5 47               2222                      9
 5 61               45                        5
 5 406              250       30379           10
 5 406              253       30379           10
 5 418                        303538          11
 5 419                        222222222222222 15
 5 770                        970             8
```

Figure 16: IP-Options System Parameters Form

```
display system-parameters ip-options                       Page 1 of x

                        IP-OPTIONS SYSTEM PARAMETERS

 IP MEDIA PACKET PERFORMANCE THRESHOLDS
    Roundtrip Propagation Delay (ms)    High: 800      Low: 400
                    Packet Loss (%)     High: 40       Low: 15
                    Ping Test Interval (sec): 20
    Number of Pings Per Measurement Interval: 10

 RTCP MONITOR SERVER
                   Default Server IP Address:
                         Default Server Port: 5005
            Default RTCP Report Period(secs): 5

AUTOMATIC TRACE ROUTE ON
            Link Failure? y


 H.248 MEDIA GATEWAY                H.323. IP ENDPOINT
 Link Loss Delay Timer (min):5     Link Loss Delay Timer (min):
                                     Primary Search Time (sec):
                             Periodic Registration Timer (min):
```

Figure 17: IP-Options System Parameters Form (page 2)

```
change system-parameters ip-options                        Page 2 of x

                        IP-OPTIONS SYSTEM PARAMETERS

Always use G.711 (30ms, no SS) for intra-switch Music-On-Hold?

IP DTMF TRANSMISSION MODE
     Intra-System IP DTMF Transmission Mode: in-band-g711
                       Inter-System IP DTMF: See Signaling Group Forms

HYPERACTIVE MEDIA GATEWAY REGISTRATIONS
  Enable Detection and Alarms?
```

Figure 18: Class of Restriction screen (page 1)

```
change cor n                                                    Page 1 of x
                             CLASS OF RESTRICTION
               COR Number: n
          COR Description: supervisor

                      FRL: 0                                    APLT? y
  Can Be Service Observed? n              Calling Party Restriction: none
Can Be A Service Observer? y               Called Party Restriction: none
 Partitioned Group Number: 1           Forced Entry of Account Codes? n
         Priority Queuing? n                     Direct Agent Calling? y
     Restriction Override: none            Facility Access Trunk Test? n
     Restricted Call List? n                      Can Change Coverage? n
   Unrestricted Call List? __ __ __ __ __ __ __ __ __ __
            Access to MCT? y                Fully Restricted Service? n
Group II Category For MFC: 7                Hear VDN of Origin Annc.? n
         Send ANI for MFE? n_                Add/Remove Agent Skills? y
            MF ANI Prefix: ______           Automatic Charge Display? n
Hear System Music on Hold? y     PASTE(Display PBX Data on telephone)? n
                             Can Be Picked Up By Directed Call Pickup? n
                                         Can Use Directed Call Pickup? n
                                         Group Controlled Restriction: inactive
```

Figure 19: Class of Restriction screen (page 2)

```
change cor nn                                                     Page 2 of x
                         CLASS OF RESTRICTION

                     MF Incoming Call Trace? n
               Brazil Collect Call Blocking? n
                     Block Transfer Display? n
Block Enhanced Conference/Transfer Displays? y
                     Remote Logout of Agent? n

                           Station Lock COR: 10
  Outgoing Trunk Disconnect Timer (minutes):
       Line Load Control:
 Maximum Precedence Level:        Preemptable?
 MLPP Service Domain:
      Station-Button Display of UUI IE Data?
      Service Observing by Recording Device?
                         ERASE 24xx USER DATA UPON
        Dissociate or unmerge at this phone: none
          EMU login or logoff at this phone: none
           Mask CPN/NAME for Internal Calls:
```

Figure 20: Class of Restriction screen (page 3)

```
hange cor nn                                                Page 3 of x
                      CLASS OF RESTRICTION

            SAC/CF Override by Team Btn? n
SAC/CF Override Protection for Team Btn? n



            (NOTE: Use pages 4 to 13 to assign up to 995 CORs.)
```

Figure 21: Class of Restriction screen (page 4)

```
change cor nn                                                Page 4 of x
                      CLASS OF RESTRICTION
CALLING PERMISSION (Enter y to grant permission to call specified COR)
  0? n     15? n     30? n     44? n     58? n     72? n    86? n
  1? n     16? n     31? n     45? n     59? n     73? n    87? n
  2? n     17? n     32? n     46? n     60? n     74? n    88? n
  3? n     18? n     33? n     47? n     61? n     75? n    89? n
  4? n     19? n     34? n     48? n     62? n     76? n    90? n
  5? n     20? n     35? n     49? n     63? n     77? n    91? n
  6? n     21? n     36? n     50? n     64? n     78? n    92? n
  7? n     22? n     37? n     51? n     65? n     79? n    93? n
  8? n     23? n     38? n     52? n     66? n     80? n    94? n
  9? n     24? n     39? n     53? n     67? n     81? n    95? n
 10? n     25? n     40? n     54? n     68? n     82? n    96? n
 11? n     26? n     41? n     55? n     69? n     83? n    97? n
 12? n     27? n     42? n     56? n     70? n     84? n    98? n
 13? n     28? n     43? n     57? n     71? n     85? n    99? n
 14? n     29? n
```

Figure 22: System Parameters Customer-Options (Optional Features) screen

```
display system-parameters customer-options                      Page   1 of  x
                                OPTIONAL FEATURES

G3 Version: V12  123456789012                      Software Package: Standard
  Location: 2                                   RFA System ID (SID):
  Platform: 2                                   RFA Module ID (MID): 123456

                                                                USED
                                Platform Maximum Ports: 300   174
                                      Maximum Stations: 300   174
                              Maximum XMOBILE Stations: 30    28
                    Maximum Off-PBX Telephones - EC500: 1200  0
                    Maximum Off-PBX Telephones -   OPS: 1200  0
                    Maximum Off-PBX Telephones - SCCAN: 0     0
                    Maximum Off-PBX Telephones - PBFMC: 0     0
                    Maximum Off-PBX Telephones - PVFMC: 0     0



        (NOTE: You must logoff & login to effect the permission changes.)
```

Figure 23: System Parameters Customer-Options (Optional Features) screen

```
display system-parameters customer-options                       page 2 of x

                              OPTIONAL FEATURES

IP PORT CAPACITIES                                                USED
                       Maximum Administered H.323 Trunks:
                          Maximum Administered IP Trunks: 100   96
             Maximum Concurrently Registered IP Stations: 10    10
               Maximum Administered Remote Office Trunks: 0     0
  Maximum Concurrently Registered Remote Office Stations: 0     0
                Maximum Concurrently Registered IP eCons: 0     0
                          Maximum Video Capable Stations: 0     0
                     Maximum Video Capable IP Softphones: 0     0
                         Maximum Administered SIP Trunks: 500   25
    Maximum Administered Ad-hoc Video Conferencing Ports: 0     0
     Maximum Number of DS1 Boards with Echo Cancellation: 0     0
                               Maximum TN2501 VAL Boards: 1     0
                      Maximum G250/G350/G700 VAL Sources: 0     0
             Maximum TN2602 Boards with 80 VoIP Channels: 20    12
            Maximum TN2602 Boards with 320 VoIP Channels: 4     3

     Maximum Number of Expanded Meet-me Conference Ports: 0      0

           (NOTE: You must logoff & login to effect the permission changes.)
```

Figure 24: System Parameters Customer-Options (Optional Features) screen

```
display system-parameters customer-options                         page 3 of x

                         OPTIONAL FEATURES

     Abbreviated Dialing Enhanced List?             Audible Message Waiting?
         Access Security Gateway (ASG)?                 Authorization Codes?
         Analog Trunk Incoming Call ID?                          CAS Branch?
   A/D Grp/Sys List Dialing Start at 01?                           CAS Main?
  Answer Supervision by Call Classifier?                  Change COR by FAC?
                                    ARS?    Computer Telephony Adjunct Links?
                  ARS/AAR Partitioning?     Cvg Of Calls Redirected Off-net?
           ARS/AAR Dialing without FAC?                         DCS (Basic)?
           ASAI Link Core Capabilities?                    DCS Call Coverage?
           ASAI Link Plus Capabilities?                   DCS with Rerouting?
          Async. Transfer Mode (ATM) PNC?
Async. Transfer Mode (ATM) Trunking?          Digital Loss Plan Modification?
               ATM WAN Spare Processor?                              DS1 MSP?
                                 ATMS?              DS1 Echo Cancellation?
                  Attendant Vectoring?
```

Figure 25: System Parameters Customer-Options (Optional Features) screen

```
display system-parameters customer-options                      Page   4 of  x
                                OPTIONAL FEATURES

  Emergency Access to Attendant? y                            IP Stations? y
          Enable 'dadmin' Login? y
          Enhanced Conferencing? y                      ISDN Feature Plus? y
                 Enhanced EC500? y      ISDN/SIP Network Call Redirection? y
   Enterprise Survivable Server? y
      Enterprise Wide Licensing? y                        ISDN-BRI Trunks? y
             ESS Administration? y                               ISDN-PRI? y
         Extended Cvg/Fwd Admin? y              Local Survivable Processor? y
    External Device Alarm Admin? y                    Malicious Call Trace? y
         Extended Cvg/Fwd Admin? y   Mode Code for Centralized Voice Mail? y
    External Device Alarm Admin? y
 Five Port Networks Max per MCC? y                Multifrequency Signaling? y
               Flexible Billing? y Multimedia Appl. Server Interface(MASI)? y
  Forced Entry of Account Codes? y        Multimedia Call Handling (Basic)? y
     Global Call Classification? y     Multimedia Call Handling (Enhanced)? y
            Hospitality (Basic)? y              Multimedia IP SIP Trunking? y
Hospitality (G3V3 Enhancements)? y
                      IP Trunks? y

          IP Attendant Consoles? y

           (NOTE: You must logoff & login to effect the permission changes.)
```

Figure 26: System Parameters Customer-Options (Optional Features) screen

```
display system-parameters customer-options                          page 5 of x

                               OPTIONAL FEATURES

                Multinational Locations?            Station and Trunk MSP? n
Multiple Level Precedence and Preemption?      Station as Virtual Extension? n
                     Multiple Locations?
                                            System Management Data Transfer? n

         Personal Station Access (PSA)? y
                      Posted Messages? n               Tenant Partitioning? n
                      PNC Duplication? n       Terminal Trans. Init. (TTI)? y
                 Port Network Support? y               Time of Day Routing? y
            Processor and System MSP? n              Uniform Dialing Plan? y
                  Private Networking? y      Usage Allocation Enhancements? y
                  Processor Ethernet? y       TN2501 VAL Maximum Capacity? y

                       Remote Office? n                Wideband Switching? y
        Restrict Call Forward Off Net? y                         Wireless? n
                Secondary Data Module? y
```

Index

Numerical

A

B

C

D

E

F

G

H

I

L

N

O

P

Q

R

S

T

U

V

W