4600 Series IP Telephone

Release 2.2

LAN Administrator Guide

555-233-507
Issue 2.2
April 2005

Copyright 2005, Avaya Inc.
All Rights Reserved

Notice

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

Warranty

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

Trademarks

All trademarks identified by the ® or ™ are registered trademarks or trademarks, respectively, of Avaya, Inc. All other trademarks are the property of their respective owners.

Preventing Toll Fraud

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

Avaya Fraud Intervention

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

Disclaimer

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

How to Get Help

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

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

Providing Telecommunications Security

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

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

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

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

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

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

Responsibility for Your Company's Telecommunications Security

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

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

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

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

TCP/IP Facilities

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

Standards Compliance

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

To order copies of this and other documents:

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

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

E-mail: totalware@gwsmail.com

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

Contents

Chapter 1: Introduction 9
About This Guide 9
Intended Audience 9
Document Organization 10
Change History 11
What's New in Release 2.2 12
Terms Used in This Guide 12
Conventions Used in This Guide 14
Symbolic Conventions 14
Typographic Conventions 14
Online Documentation 15
Related Documents 15
IETF Documents 18
ITU Documents 19
ISO/IEC, ANSI/IEEE Documents 20
Customer Support 20

Chapter 2: Overview of Voice over IP (VoIP) and Network Protocols . . 21
Introduction 21
Overview of Voice over IP (VoIP) 21
Data and Voice Network Similarities 21
Delay and Jitter 22
Tandem Coding 22
Voice Coding Standards 23
H.323 Standard 23
DHCP 23
TFTP 23
HTTP 24
DNS 24
NAT 24
QoS 25
SNMP 25
Network Assessment 26
TCP/UDP Port Utilization 27
Suggestions for Installation and Configuration 31
Reliability and Performance 31
IP Address Lists and Station Number Portability 32
Security 33

4600 Series IP Telephones 34
Dual Connection Architecture 34
Single Connection Architecture 34
Registration and Authentication 34
Software 34
WAN Considerations 35
DHCP and File Servers 35
Initialization Process 36
Step 1: Telephone to Network 36
Step 2: DHCP Server to Telephone 36
Step 3: Telephone and File Server 36
Step 4: Telephone and the Avaya Media Server 37

Chapter 3: Requirements 39
Introduction 39
Hardware Requirements 39
Additional Hardware Requirements 40
Software Requirements 41

Chapter 4: Server Administration 43
Introduction 43
Administering 4600 Series IP Telephones on Avaya Media Servers 46
DEFINITY Releases 9, 9.5, 10, and Avaya Communication Manager Software Release 1.1+ 46
DEFINITY Release 8.4 47
DHCP and File Servers 47
Software Checklist 47
Required Network Information 48
DHCP 49
Choosing a DHCP Configuration 49
DHCP Software Alternatives 49
DHCP Generic Setup 50
Windows NT 4.0 DHCP Server 53
Verifying the Installation of the DHCP Server 53
Initial Configuration 54
Creating a DHCP Scope for the IP Telephones 54
Editing Custom Options 55
Adding the DHCP Option 56

Activating the Leases 56
Verifying Your Configuration 57
Windows 2000 DHCP Server 58
Verifying the Installation of the DHCP Server 58
Adding DHCP Options 60
Activating the New Scope 61
TFTP 62
TFTP Generic Setup 62
Avaya TFTP (Suite Pro) 63
TFTP Server on S8300 Media Server 63
HTTP 66
HTTP Generic Setup 66
4600 Series IP Telephone Scripts and Application Files 67
Choosing the Right Application File and Upgrade Script File 69
Contents of the Upgrade Script 71
Contents of the Settings File 73
The GROUP System Value 73
QoS 74
IEEE 802.1D and 802.1Q 74
DIFFSERV 75
UDP Port Selection 76
Network Audio Quality Display on 4600 Series IP Telephones 77
RSVP and RTCP 78
VLAN Considerations 79
Administering Options for the 4600 Series IP Telephones 80
DNS Addressing 84
Customizing the Site-Specific Option Number (SSON) 84
Entering Options Using the Telephone Dialpad 84
Enhanced Local Dialing 85
Customizing the 4630/4630SW IP Telephone 87
4630/4630SW Backup/Restore 90
Call Log Archive 91
Customizing 4610SW, 4620/4620SW, 4621SW, 4622SW, and 4625SW IP Telephones 92
The Application Status Flag (APPSTAT) 95
Backup/Restore for 4610SW, 4620/4620SW, 4621SW, 4622SW and 4625SW IP Telephones 97

Chapter 5: Troubleshooting Guidelines 99
Introduction 99
Error Conditions 99
The Clear Administrative Option 106
The Reset Administrative Option 108
Reset System Values 108
Restart the Telephone 110
The View Administration Option 111
Error Messages 113
Troubleshooting the 4601 IP Telephone 118

Appendix A: Avaya - 46xx IP Telephone MIB 123
Downloading the Avaya - 46xx IP Telephone MIB 123

Appendix B: Creating Web Sites for the 4630/4630SW IP Telephone 125
Introduction 125
General Background. 126
Browser Features and Behavior 126
Document Skeleton 127
Content-Based Style. 127
Logical Style 128
Physical Style 129
Physical Spacing and Layout 129
Lists and Tables 130
Lists. 130
Tables. 130
Images 131
Links 132
Frames 132
Forms. 133
Character Entities 134
Colors. 134
Fonts 134
Cookies. 135
Design Guidelines 135
Fixed-Width Objects 135
Images 136
Frames 136

Fonts 137
Maintaining Context 137
User Interaction 138
Click-to-Dial Functionality. 138

Appendix C: Creating Web Sites for Other 4600 Series IP Telephones 141
Introduction 141

Appendix D: Administering Thin Client Directories. 143
Introduction 143

Appendix E: The Push Feature 145
Introduction 145
Push Content. 145
Push Priorities 146
For More Information on Push 146

Index 147

Chapter 1: Introduction

About This Guide

This guide provides a description of Voice over IP and describes how to administer the DHCP and TFTP servers. This guide also covers how to troubleshoot operational problems with the 4600 Series IP Telephones and the servers.

The 4600 Series IP Telephone product line is a supplement to Avaya's IP Solutions platform.

Note:

Unless otherwise indicated, any reference to "the DEFINITY® server" in this document also refers to the Avaya Communication Manager media servers.

The 4602/4602SW (non-SIP) IP Telephones *are* covered in this guide.

Administration of Avaya SIP Telephone software, such as the 4602/4602SW SIP Telephones *is not* covered in this guide. See the *4602 SIP Telephone Administrator's Guide* (Document Number 16-300037) for information on administering 4602/4602SW SIP Telephones.

Intended Audience

This document is intended for personnel who administer the DHCP and TFTP servers to support the 4600 Series IP Telephone. This guide is also intended for those who administer the Local Area Network (LAN) itself.

CAUTION:

Avaya does not support many of the products mentioned in this document. Take care to ensure that there is adequate technical support available for these types of servers:

- TFTP servers,
- HTTP servers,
- DHCP servers,
- FTP servers,
- LDAP servers, and
- Web servers.

Note: If the servers are not functioning correctly, the 4600 Series IP Telephones may not operate correctly.

Document Organization

The guide contains the following sections:

Chapter 1: Introduction	Provides an overview of the 4600 Series IP Telephone LAN Administrator document.
Chapter 2: Overview of Voice over IP (VoIP) and Network Protocols	Describes VoIP and factors influencing its performance that must be considered when implementing this feature.
Chapter 3: Requirements	Describes the hardware and software requirements for Avaya's VoIP offering.
Chapter 4: Server Administration	Describes DHCP, TFTP, and HTTP administration for the 4600 Series IP Telephones.
Chapter 5: Troubleshooting Guidelines	Describes messages that might occur during the operation of the 4600 Series IP Telephones.
Appendix A: Avaya - 46xx IP Telephone MIB	Provides a link to the MIB specification for the 46xx IP Telephones: 4601, 4602/4602SW, 4606, 4610SW, 4612, 4620/4620SW, 4621SW, 4622SW, 4624, 4625SW, and 4630/4630SW.
Appendix B: Creating Web Sites for the 4630/4630SW IP Telephone	Provides information on creating and customizing Web sites for viewing on the 4630/4630SW IP Telephone. Also describes the current capabilities and limitations of the 4630/4630SW's Web Browser.
Appendix C: Creating Web Sites for Other 4600 Series IP Telephones	Provides information on creating and customizing Web sites for viewing on the 4610SW, 4620/4620SW, 4621SW, 4622SW, and 4625SW IP Telephones.
Appendix D: Administering Thin Client Directories	Provides information on administering an LDAP directory for the 4610SW, 4620/4620SW, 4621SW, 4622SW, and 4625SW IP Telephones.
Appendix E: The Push Feature	Provides information about the Push feature available as of Release 2.1.

Change History

Issue 1.0	This document was issued for the first time in November 2000.
Issue 1.1	This version of the document, revised and issued in April 2001, supports through DEFINITY® Release 9.
Issue 1.5	This version of the document was revised in June, 2001 to support DEFINITY® Release 9.5.
Issue 1.6	This version of the document was revised to support DEFINITY® Release 10 and the 4630 IP Telephone.
Issue 1.7	This version of the document was revised in July, 2002 to support Avaya Communication Manager Release 1.1 and the 4602 and 4620 IP Telephones.
I**ssue 1.8**	This version of this document was revised in June, 2003 to support Avaya Communication Manager Releases 1.2 and 1.3. This version also supported the 4602SW and 4630SW IP Telephones.
Issue 2.0	This version of this document was revised in December, 2003 to add support for Avaya Communication Manager Release 2.0. This version also supported the 4610SW and 4620SW IP Telephones, and the 4690 IP Conference Telephone.
Issue 2.1	This version of this document was revised in July, 2004 to add support for Avaya Communication Manager Release 2.1. This version also added support for the TFTP server on the Avaya S8300 Media Server, and support for the 4601 IP Telephone.
Issue 2.2	This is the current version of this document, revised and issued in April, 2005. This version supports through Avaya Communication Manager Release 2.2. This version also introduces the 4621SW, 4622SW, and 4625SW IP Telephones.

What's New in Release 2.2

New material in this release includes:

- Support for Avaya Communication Manager Release 2.2.
- Support for the 4621SW, 4622SW, and 4625SW IP Telephones.
- Support for HTTP, HTTPS, and TLS (Transport Layer Security) for upgrade and settings files.
- Support for Avaya's Converged Network Analyzer (CNA).
- Additional information about setting VLANTEST to "0" in the 46xxsettings file.
- New general system parameters: CNAPORT, CNASRVR, L2Q, TLSSRVR.
- New 4625SW system parameter: BAKLIGHT.

Terms Used in This Guide

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.
ARP	Address Resolution Protocol, used, for example, to verify that the IP Address provided by the DHCP server is not in use by another IP telephone.
CELP	Code-excited linear-predictive. Voice compression requiring only 16 kbps of bandwidth.
CLAN	Control LAN, type of Gatekeeper circuit pack.
CNA	Converged Network Analyzer, an Avaya product to test and analyze network performance.
DHCP	Dynamic Host Configuration Protocol, an IETF protocol used to automate IP Address allocation and management.
DiffServ	Differentiated Services, an IP-based QoS mechanism.
DNS	Domain Name System, an IETF standard for ASCII strings to represent IP Addresses.
Gate-keeper	H.323 application that performs essential control, administrative, and managerial functions in the media server. Sometimes called CLAN in Avaya documents.
HTTP	Hypertext Transfer Protocol, used to request and transmit pages on the World Wide Web.
HTTPS	A secure version of HTTP.

1 of 2

IETF	Internet Engineering Task Force, the organization that produces standards for communications on the internet.
LAN	Local Area Network.
LDAP	Lightweight Directory Access Protocol, an IETF standard for database organization and query exchange.
MAC	Media Access Control, ID of an endpoint.
NAPT	Network Address Port Translation.
NAT	Network Address Translation.
PHP	Hypertext Preprocessor, software used to assist in the format and display of Web pages.
PSTN	Public Switched Telephone Network, the network used for traditional telephony.
QoS	Quality of Service, used to refer to several mechanisms intended to improve audio quality over packet-based networks.
RSVP	Resource ReSerVation Protocol, used by hosts to request resource reservations throughout a network.
RTCP	RTP Control Protocol, monitors quality of the RTP services and can provide real-time information to users of an RTP service.
RTP	Real-time Transport Protocol. Provides end-to-end services for real-time data such as voice over IP.
SIP	Session Initiation Protocol. An alternative to H.323 for VoIP signaling.
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 the IP telephones.
TLS	Transport Layer Security, an enhancement of Secure Sockets Layer (SSL). TLS is compatible with SSL 3.0 and allows for privacy and data integrity between two communicating applications.
UDP	User Datagram Protocol, a connectionless transport-layer protocol.
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 4620 Web Browser to communicate with WML servers.

2 of 2

Conventions Used in This Guide

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

Symbolic Conventions

Note:

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

CAUTION:

This symbol emphasizes possible harm to software, possible loss of data, or possible service interruptions.

Typographic Conventions

This guide uses the following typographic conventions:

`command`	Words printed in this type are commands that you enter into your system.
`message`	Words printed in this type are system messages.
device	Words printed in this type indicate parameters associated with a command for which you must substitute the appropriate value. For example, when entering the **`mount`** command, ***device*** must be replaced with the name of the drive that contains the installation disk.
Administrative	Words printed in bold type are menu or screen titles and labels. Words printed in bold type can also be items on menus and screens that you select or enter to perform a task, i.e., fields, buttons, or icons. Bold type also provides general emphasis for words or concepts.
italics	Italic type indicates a document that contains additional information about a topic.

Online Documentation

The online documentation for the 4600 Series IP Telephones is located at the following URL:

http://www.avaya.com/support

Related Documents

- *DEFINITY® Documentation Release 8.4*

  This CD contains documentation that describes, among other things, how to administer a DEFINITY switch with Release 8.4 software. This document is provided with the DEFINITY Release 8.4 product.

- *DEFINITY® Documentation Release 9*

  This CD contains documentation that describes, among other things, how to administer a DEFINITY switch with Release 9 software. This document is provided with the DEFINITY Release 9 product.

- *DEFINITY® Documentation Release 10*

  This CD contains documentation that describes, among other things, how to administer a DEFINITY switch with Release 10 software. This document is provided with the DEFINITY Release 10 product.

- *Avaya Communication Manager Software Documentation Release 1.1*

  This document describes how to administer a switch with Avaya Communication Manager software. This document is provided with the Avaya Communication Manager Release 1.1 product.

- *Avaya Communication Manager Software Documentation Release 1.2*

  This document describes how to administer a switch with Avaya Communication Manager software. This document is provided with the Avaya Communication Manager Release 1.2 product.

- *Avaya Communication Manager Documentation Release 1.3*

  This document describes how to administer a switch with Avaya Communication Manager software. This document is provided with the Avaya Communication Manager Release 1.3 product.

- *Avaya Communication Manager Documentation Release 2.0*

  This document describes how to administer a switch with Avaya Communication Manager software. This document is provided with the Avaya Communication Manager Release 2.0 product.

- *Avaya Communication Manager Documentation Release 2.1*

  This document describes how to administer a switch with Avaya Communication Manager software. This document is provided with the Avaya Communication Manager Release 2.1 product.

- *Avaya Communication Manager Documentation Release 2.2*

  This document describes how to administer a switch with Avaya Communication Manager software. This document is provided with the Avaya Communication Manager Release 2.2 product.

- *Administration for Network Connectivity for Avaya Communication Manager Software*

  This document describes how to administer Avaya Communication Manager software to implement Voice over IP (VoIP) applications for TCP/IP for DCS signaling, H.323 trunks, and private networks.

- *Administrator Guide for Avaya Communication Manager Software*

  This document provides an overall reference for planning, operating, and administering your Avaya Communication Manager solution.

- *Installation and Upgrades for Avaya G700 Media Gateway and Avaya S8300 Media Server*

  This document describes procedures for installing, upgrading, and performing initial configuration tasks for the Avaya G700 Media Gateway and the Avaya S8300 Media Server.

The following documents are available on the Web site listed under Online Documentation:

- *4600 Series IP Telephones Safety Instructions*

  This document contains important user safety instructions for the 4600 Series IP Telephones.

- *30A Switched Hub Set Up Quick Reference, Issue 2, July 2002 (Comcode 700234750)*

  This document contains important safety and installation information for the 30A Switched Hub.

- *4600 Series IP Telephone Installation Guide*

  This document describes how to install 4600 Series IP Telephones. It also provides troubleshooting guidelines for the 4600 Series IP Telephones.

- *4600 Series IP Telephones Application Programmer Interface (API) Guide*

  This document provides information on developing Web applications for 4610SW, 4620/4620SW, 4621SW, 4622SW, and 4625SW IP Telephones. This document also covers Push feature administration.

- *4601/4602/4602SW IP Telephone Stand Instructions*

  This document provides information on how to desk- or wall-mount a 4601 or 4602/4602SW IP Telephone.

- *4601 IP Telephone User Guide*

  This document provides detailed information about using the 4601 IP Telephone.

- *4602/4602SW IP Telephone User Guide*

  This document provides detailed information about using the 4602/4602SW IP Telephones.

- *4606 IP Telephone User Guide*

  This document provides detailed information about using the 4606 IP Telephone.

- *4610SW IP Telephone User Guide*

  This document provides detailed information about using the 4610SW IP Telephone.

- *4612 IP Telephone User Guide*

  This document provides detailed information about using the 4612 IP Telephone.

- *4620/4620SW/4621SW IP Telephone User Guide*

  This document provides detailed information about using the 4620/4620SW and 4621SW IP Telephones.

- *4622SW IP Telephone User Guide*

  This document provides detailed information about using the 4622SW IP Telephone.

- *4624 IP Telephone User Guide*

  This document provides detailed information about using the 4624 IP Telephone.

- *4625SW IP Telephone User Guide*

  This document provides detailed information about using the 4625SW IP Telephone.

- *4630/4630SW IP Telephone User Guide*

  This document provides detailed information about using the 4630/4630SW IP Telephones.

- *Avaya 4690 IP Conference Telephone User Guide*

  This document provides detailed information about using the 4690 IP Conference Telephones.

IETF Documents

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

Requirements for Internet Hosts - Communication Layers, October 1989, by R. Braden (STD 3: RFC 1122)

Requirements for Internet Hosts - Application and Support, October 1989, by R. Braden (STD 3: RFC 1123)

Internet Protocol (IP), September 1981, by Information Sciences Institute (STD 5: RFC 791), as amended by *Internet Standard Subnetting Procedure*, August 1985, by J. Mogul and J. Postel (STD 5: RFC 950)

Broadcasting Internet Datagrams, October 1984, by J. Mogul (STD 5: RFC 919)

Broadcasting Internet Datagrams in the Presence of Subnets, October 1984, by J. Mogul (STD 5: RFC 922)

User Datagram Protocol (UDP), August 28, 1980, by J. Postel (STD 6: RFC 768)

Transmission Control Protocol (TCP), September 1981, by Information Sciences Institute (STD 7: RFC 793)

Domain Names - Concepts and Facilities (DNS), November, 1987, by P. Mockapetris (STD 13: RFC 1034)

Domain Names - Implementation and Specification (DNS), November 1987, by P. Mockapetris (STD 13: RFC 1035)

The TFTP Protocol (Revision 2), (TFTP), July 1992, by K. Sollins, (STD 33: RFC 1350:) as updated by *TFTP Option Extension*, May 1998, by G. Malkin and A. Harkin (RFC 2347)

An Ethernet Address Resolution Protocol (ARP), November 1982, by David C. Plummer (STD 37: RFC 826)

Dynamic Host Configuration Protocol (DHCP), March 1997, by R. Droms (RFC 2131)

DHCP Options and BOOTP Vendor Extensions, March 1997, by S. Alexander and R. Droms (RFC 2132)

RTP: A Transport Protocol for Real-Time Applications (RTP/RTCP), January 1996, by H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson (RFC 1889)

Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, *(DIFFSRV)*, December 1998, by K. Nichols, S. Blake, F. Baker and D. Black (RFC 2474)

Introduction to version 2 of the Internet-standard Network Management Framework (SNMPv2), April 1993, by J. Case, K. McCloghrie, M. Rose, and S. Waldbusser (RFC 1441)

Management Information Base for Network Management of TCP/IP Internets: MIB-II, March 1991, edited by K. McCloghrie and M. Rose (RFC 1213)

SNMPv2 Management Information Base for the Internet Protocol using SMIv2, November 1996, edited by K. McCloghrie (RFC 2011)

Structure of Management Information Version 2 (SMIv2), April 1999, edited by K. McCloghrie, D. Perkins, and J. Schoenwaelder (RFC 2578)

Resource ReSerVation Protocol VI, September 1997, by R. Braden, L. Zhang, S. Berson, S. Herzog, and S. Jamin (RFC 2205)

Lightweight Directory Access Protocol, March 1995, by M. Wahl, T. Howes, and S. Kille (RFC 1777)

Lightweight Directory Access Protocol (v3), December 1997, by M. Wahl, T. Howes, and S. Kille (RFC 2251)

Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions, December 1997, by M. Wahl, Coulbeck, T. Howes, and S. Kitte (RFC 2252)

Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names, December 1997, by M. Wahl, S. Kille, and T. Howes (RFC 2253)

The TLS Protocol Version 1.0, January 1999, by T. Dierks and C. Allen (RFC 2246)

ITU Documents

The following documents are available for a fee from the ITU Web site: http://www.itu.int**.**

Recommendation G.711, Pulse Code Modulation (PCM) of Voice Frequencies, November 1988

Recommendation G.729, Coding of speech at 8 kbit/s using Conjugate-Structure Algebraic-Code-Excited Linear-Prediction (CS-ACELP), March 1996

Annex A to Recommendation G.729: Reduced complexity 8 kbit/s CS-ACELP speech codec, November 1996

Annex B to Recommendation G.729: A silence compression scheme for G.729 optimized for terminals conforming to Recommendation V.70, November 1996

Recommendation H.225.0, Call signalling protocols and media stream packetization for packet-based multimedia communications systems, February 1998

Recommendation H.245, Control protocol for multimedia communication, February 1998

Recommendation H.323, Packet-based multimedia communications systems, February 1998

ISO/IEC, ANSI/IEEE Documents

The following documents are available for a fee from the ISO/IEC standards Web site: http://www.iec.ch.

International Standard ISO/IEC 8802-2:1998 ANSI/IEEE Std 802.2, 1998 Edition, Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks- Specific requirements- Part 2: Logical Link Control

ISO/IEC 15802-3: 1998 ANSI/IEEE Std 802.1D, 1998 Edition, Information technology- Telecommunications and information exchange between systems- Local and metropolitan area networks- Common specifications- Part 3: Media Access Control (MAC) Bridges

IEEE Std 802.1Q-1998, IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks

IEEE Std 802.3af-2003, IEEE Standard for Information technology- Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific requirements- Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications- Amendment: Data Terminal Equipment (DTE) Power via Media Dependent Interface (MDI)

Customer Support

Call the Avaya support number provided to you by your Avaya representative or Avaya reseller for 4600 Series IP Telephone support.

Information about Avaya products can be obtained at the following URL:

http://www.avaya.com/support

Chapter 2: Overview of Voice over IP (VoIP) and Network Protocols

Introduction

This chapter describes the differences between data and voice networks, and the factors that influence the performance of VoIP. The installation and administration of 4600 Series IP Telephones on Avaya media servers, and the installation and configuration of DHCP and TFTP are addressed.

Overview of Voice over IP (VoIP)

The 4600 Series IP Telephones allow enterprises to use Voice over IP (VoIP). VoIP uses packet-switched networks over the Public Switched Telephone Network (PSTN) instead of telephony. However, using data networks to transmit voice packets poses a problem. Data networks were not designed for the specific qualities required by voice traffic.

Data and Voice Network Similarities

Data and voice networks share similar functions because of the nature of networking.

- **Signaling:** establishes a connection between two endpoints.

  In a voice network, signaling helps identify who the calling party is trying to call and where the called party is on the network. Traditional telephony uses terminals with fixed addresses. Traditional telephony establishes a fixed connection for the communication session between two such terminals, allocating fixed bandwidth resources for the duration of the call.

  IP communications constitute a connectionless network, having neither fixed addresses nor fixed connections.

- **Addressing:** a unique address that must identify each terminal on a network.

  In a voice network, the unique address is a permanent attribute, based on any combination of:

  - international numbering plans,
  - national numbering plans,

  - local telephone company practices,
  - internal customer-specific codes.

  In IP communications, dial plans track extension numbers assigned to terminals. No fixed connection path is needed.

- **Routing** is related to addressing and allows connections to be established between endpoints.

Although these functions are common to data and voice networks, the implementations differ.

Delay and Jitter

Data traffic is usually short and comes in bursts. Data networks like the Internet are designed to manage these bursts of traffic from many sources on a first-come, first-served basis. Data packets are sent to multiple destinations, often without any attempt to keep them in a particular order.

Voice networks are designed for continuous transmission during a call. The traffic is not bursty, and the conversation uses a specific amount of bandwidth between the two ends during the call.

Several features of data networks are unsuitable for voice telephony:

- Data network design delivers data at the destination, but not necessarily within a certain time, producing delay (latency). In data networks, delay tends to be variable. For voice messages, variable delay results in jitter, an audible choppiness in conversations.
- Variable routing also can result in loss of timing synchronization, so packets are not received at the destination in the proper order.
- Data networks have a strong emphasis on error correction, resulting in repeated transmissions.

Data network concepts include prioritization of traffic types to provide some form of greater traffic reliability, for example, for interactive transactions. However, data requirements tend to not be as strict as most voice requirements.

Starting with Release 1.1, the 4600 Series IP Telephones include a dynamic jitter buffer. This feature automatically smooths jitter to improve audio quality.

Tandem Coding

Tandem coding, also called transcoding, refers to converting a voice signal from analog to digital and back again. When calls are routed over multiple IP facilities, they can be subject to multiple transcodings. The multiple conversions between analog and digital coding result in a deterioration in the voice quality. Avoid tandem coding wherever possible in any compressed voice system, for example, by minimizing analog trunking on the PBX.

Voice Coding Standards

There are several voice coding standards. Avaya 4600 Series IP Telephones offer these options:

- G.711, which describes the 64 kbps PCM voice coding technique. G.711-encoded voice is already in the correct format for digital voice delivery in the public phone network or through PBXs.
- G.729A and G.729B, both of which describe adaptive code-excited, linear-predictive (CELP) compression that allows voice to be coded into 8 kbps streams.

H.323 Standard

Internal signaling provides connection control and call progress (status) information. The H.323 standard is used for IP packet voice networks' internal signaling. H.323 defines more than just voice. H.323 defines a complete multimedia network, for example, voice, video, and data, with everything from devices to protocols. The H.245 standard links all the entities within H.323 by negotiating facilities among participants and H.323 network elements.

The H.323 standard makes G.711 PCM compression the default form of compression. All other compression formats are optional.

DHCP

Dynamic Host Configuration Protocol (DHCP) allows a server to assign IP Addresses and other parameters to devices like the 4600 Series IP Telephones on an as-needed basis. DHCP eliminates the need to configure each end station with a static IP Address. The DHCP application also passes information to the 4600 Series IP Telephone. The DHCP application identifies the PBX and the file server's IP Addresses. The application also identifies the paths to the upgrade script and the application file on the file server.

For further information, see DHCP and File Servers on page 47 and DHCP on page 49.

TFTP

The Avaya 4600 IP Telephones can get useful application information from the TFTP server. The telephones also can upgrade themselves using files stored on the TFTP server. After downloading software, the Avaya 4600 Series IP Telephones can operate without a file server. However, some functionality can be lost if the file server is not available for a telephone reset. For further information, see DHCP and File Servers on page 47 and TFTP on page 62.

HTTP

HTTP is potentially a more secure alternative to TFTP, particularly when Transport Layer Security (TLS) is used to create HTTPS (Secure HTTP). You can store the same application software, script file, and settings file on an HTTP server as you can on the TFTP server. With proper administration, the telephone seeks out and uses that material appropriately. However, the 4600 Series IP Telephone must already be running Release 2.2 software to be able to access and use HTTP servers. As with TFTP, some functionality might be lost by a reset if the HTTP server is not available. For more information, see DHCP and File Servers on page 47 and HTTP on page 66.

DNS

The Domain Name System (DNS) is a distributed Internet directory service. DNS is used mostly to translate between domain names and IP Addresses. Release 1.5 and later Avaya 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. See DNS Addressing on page 84.

NAT

A Network Address Translation (NAT) is an application that can be administered between your network and the Internet. The NAT translates network layer IP Addresses so your local intranet IP Addresses can duplicate global, Internet addresses. A detailed discussion of NAT is beyond the scope of this document. Note that NAT use can lead to problems that affect the consistency of addressing throughout your network. In Release 1.6 and earlier releases of the 4600 Series IP Telephones, NAT is **not** recommended for networks handling IP-based telephony traffic. As of Release 1.7, all 4600 Series IP Telephones support NAT interworking. Therefore, no problems exist with NAT and Release 1.7 of the 4600 Series IP Telephones. Note that support for NAT does not imply support for Network Address Port Translation (NAPT). Specifically, the 4600 Series IP Telephones do not support communication to the PBX through any NAPT device.

NAT requires specific administration on the media server. The capability to have a direct Avaya IP Telephone-to-Avaya IP Telephone call with NAT, also called “NAT shuffling,” requires Avaya Communication Manager Release 1.3 software. See the *Administration for Network Connectivity* document listed in Related Documents on page 15.

QoS

Quality of Service (QoS) is a term covering several initiatives to maximize the voice quality heard at both ends of a call that originates or terminates on an IP-based telephone. These initiatives include various prioritization schemes to offer voice packets a larger or prioritized share of network resources. These schemes include standards such as:

- IEEE's 802.1D and 802.1Q,
- the Internet Engineering Task Force's (IETF's) "Differentiated Services,"
- RTP Control Protocol (RTCP),
- Resource ReSerVation Protocol (RSVP), and
- port-based priority schemes such as UDP port selection.

Documentation for your LAN equipment details the extent to which your network can support any or all of these initiatives. See Server Administration on page 43, for some implications of QoS for the 4600 Series IP Telephones.

As of Release 1.7, both the 4620 and 4630 families of IP Telephones provided network audio quality information to the end user. This network audio quality information might be useful to the LAN Administrator. As of Release 1.8, all 4600 Series IP Telephones provide some level of detail about network audio quality. For specific information, see Network Audio Quality Display on 4600 Series IP Telephones on page 77.

SNMP

Simple Network Management Protocol (SNMP) is a family of standards-based protocols and procedures to allow vendor-independent data network management. Using a simple set of protocol commands, an SNMP-compliant device stores information in standard format in one or more Management Information Bases (MIBs). Usually, devices support the standards-specific MIB termed MIB-II. In addition, devices can define one or more "custom MIBs" that contain information about the device's specifics.

As of Release 1.1, the 4600 Series IP Telephones are fully compatible with SNMPv2c, a later version of SNMP, 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 Custom MIB. The 4600 Series IP Telephone Custom MIB is read-only. 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 SNMPSTAT, respectively, as indicated in Chapter 4: Server Administration, Table 6: 4600 Series IP Telephone Customizable System Parameters.

To find more information about SNMP and MIBs, see the IETF references listed in Related Documents on page 15. The Avaya Custom MIB for the 4600 Series IP Telephones is available for download in *.txt format on the Avaya support Web site.

Network Assessment

The current technology allows optimum network configurations to deliver VoIP with perceived voice quality close to that of the Public Switched Telephone Network (PSTN). Not all networks can take advantage of packet voice transmissions. Some data networks have insufficient residual capacity for even compressed voice traffic. In addition, the usual approach to developing data networks by integrating products from many vendors requires testing the components for Voice over IP traffic compatibility.

Avaya assumes that your organization has performed a network assessment with or without Avaya's assistance before attempting to install Voice over IP. The network assessment provides a high degree of confidence that the existing data network has the capacity to carry voice packet traffic. The network assessment assures that the existing data network is compatible with the required technology.

A network assessment should include:

- A network audit to review existing equipment and evaluate its capabilities, including its ability to meet planned voice and data needs.
- A determination of network objectives, including the dominant traffic type, selection of technologies, and setting voice quality objectives.

The assessment should leave you confident that the implemented network will have the capacity for the foreseen data and voice traffic, and can support H.323, DHCP, TFTP, and jitter buffers in H.323 applications.

It is important to distinguish between compliance with the minimal VoIP standards and QoS support, the latter being a requirement to run VoIP on your configuration.

TCP/UDP Port Utilization

Like most network equipment, the 4600 Series IP Telephones use a variety of protocols, particularly TCP and UDP, to communicate with other equipment in that network—numerous different types of servers, routers, other telephones, etc. Part of this communication identifies which TCP and/or UDP ports each piece of equipment uses to support each protocol and each task within the protocol.

Depending on your network, you might need to know what ports or ranges are used in the 4600 Series IP Telephones' operation. Knowing these ports or ranges allows you to appropriately administer your networking infrastructure. In this case, you will find the following material useful.

In Figure 1, Figure 2, and Figure 3:

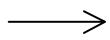
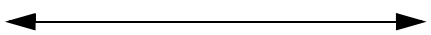
- The box on the left always represents the 4600 Series IP Telephone.
- Depending on the diagram, the boxes on the right refer to various pieces of network equipment with which the phone can (or will) communicate.
- Open-headed arrows (for example, ) represent the direction(s) of socket initialization.
- Closed-headed arrows (for example, ) represent the direction(s) of data transfer.
- The text the arrows point to identifies the port or ports that the 4600 Series IP Telephones support for the specific situation. Brackets identify ranges when more than one port applies. In addition, the text indicates any additional qualifications or clarifications. In many cases, the ports used are the ones called for by IETF or other standards bodies.
- Many of the diagrams' explanations refer to system parameters or options settings, for example, IRSTAT or DIRSRVR. See Administering Options for the 4600 Series IP Telephones in Chapter 4: Server Administration for more information on parameters and settings.

Figure 1: Signaling, Audio and Management Diagram

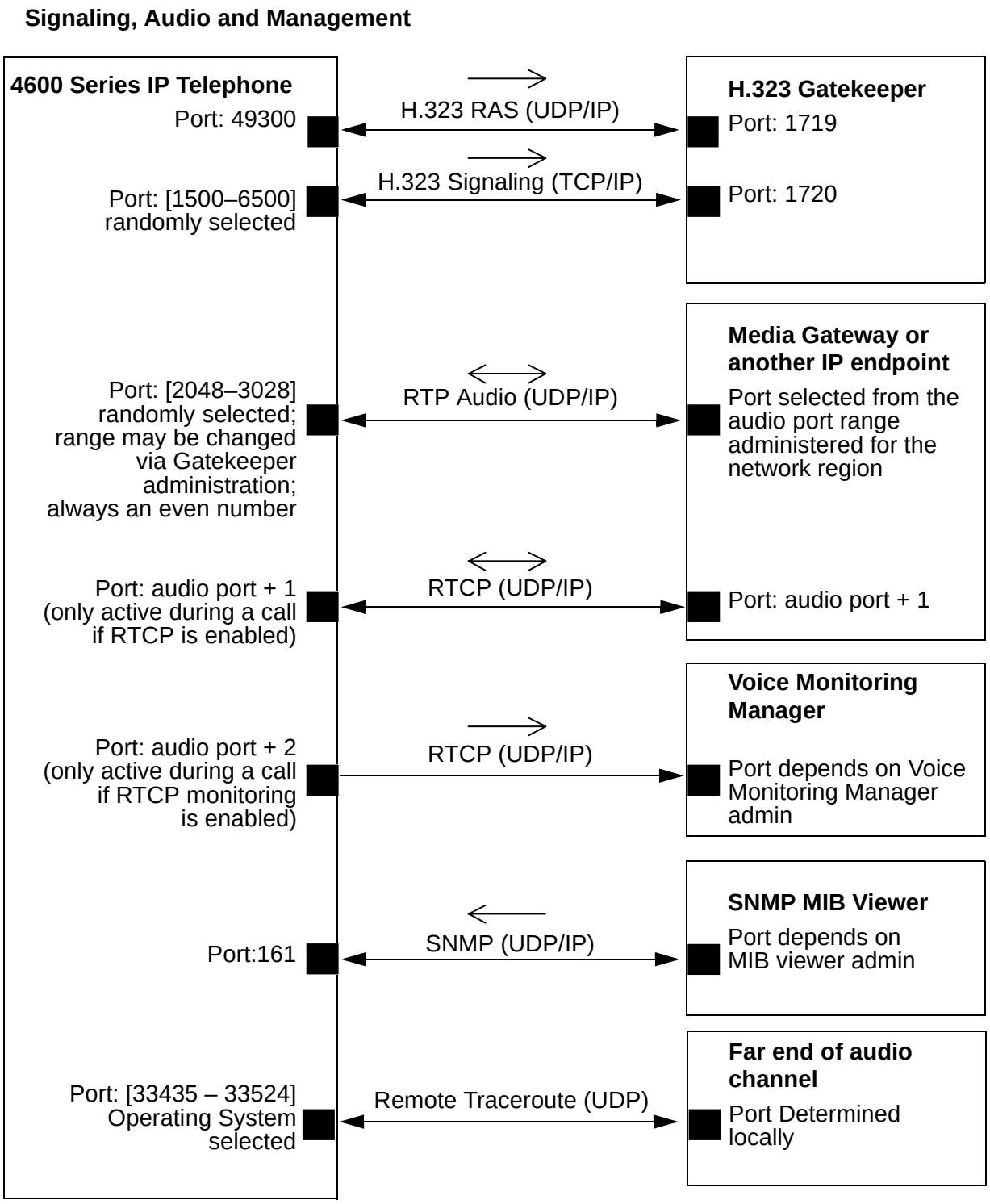


Figure 2: Initialization and Address Resolution Diagram

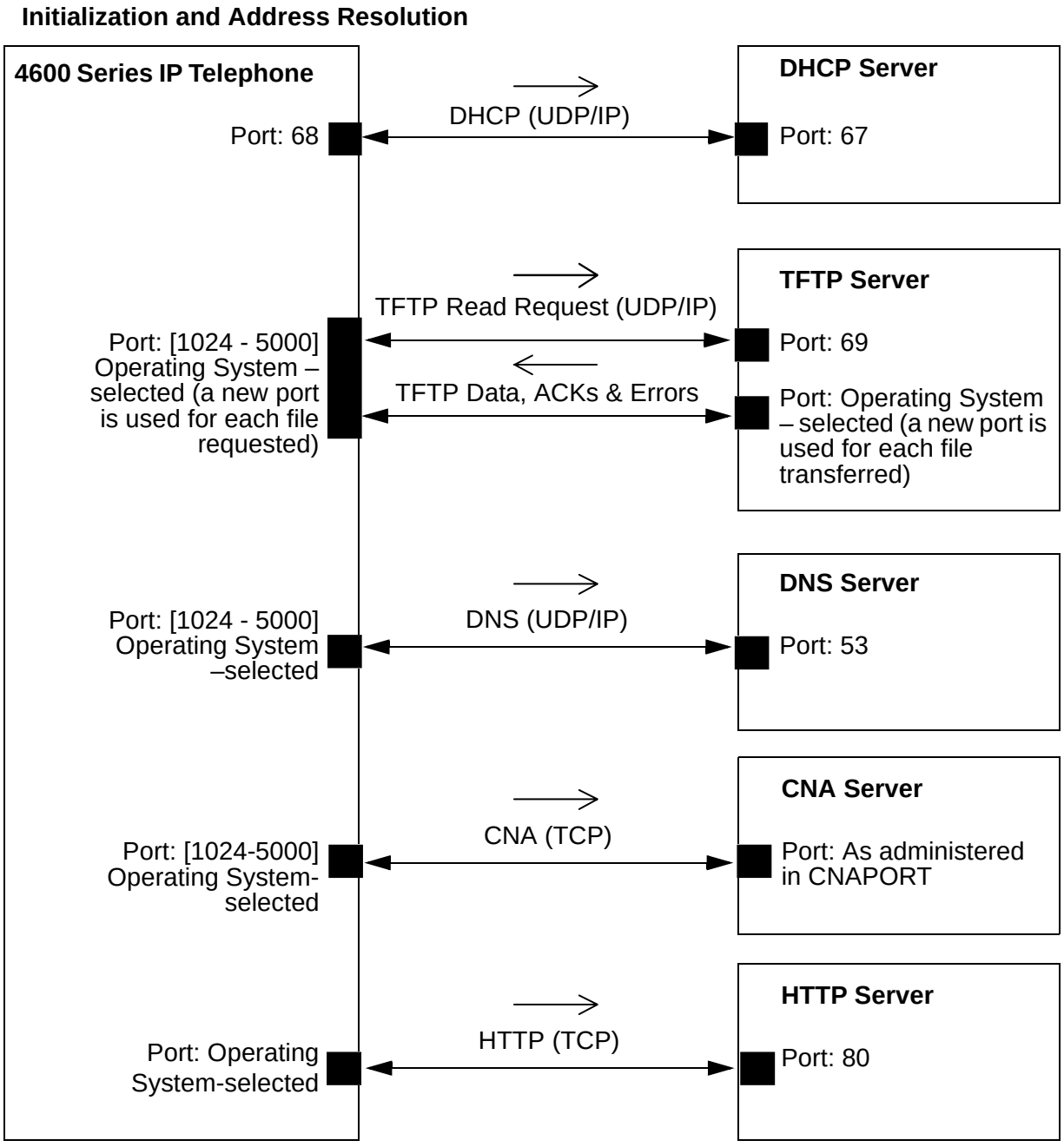
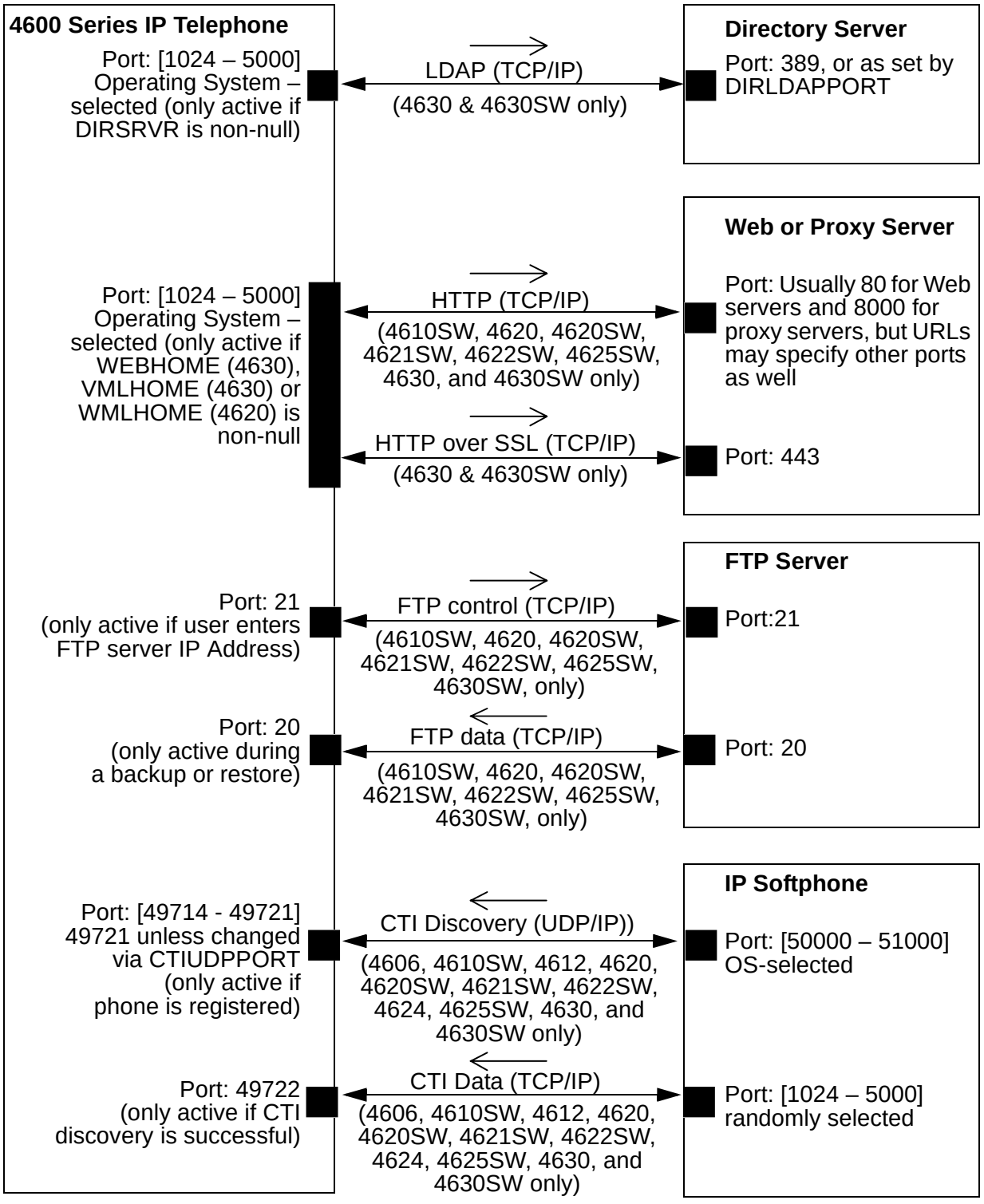
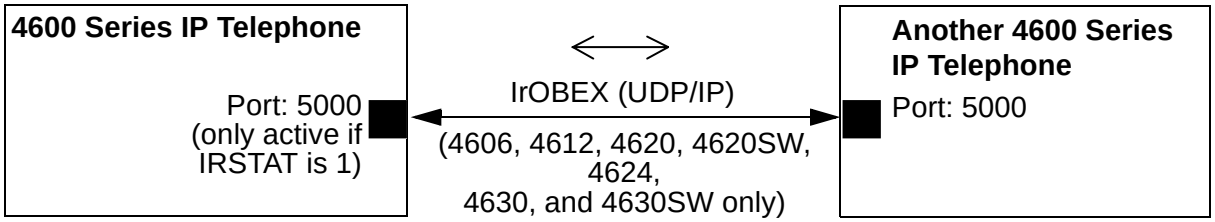


Figure 3: Applications Diagram



Applications, continued



Suggestions for Installation and Configuration

Reliability and Performance

There is a cost/performance trade-off associated with Voice over IP. Greater reliability and improved performance can be obtained through server redundancy and components with higher bandwidth capabilities.

The reliability and performance of the traditional PBX systems are very high to date. Much of the LAN is outside the PBX's control. However, consider the points in the next paragraph to enhance the reliability and performance of the IP telephone network.

All 4600 Series IP Telephones support the tools "ping" and "traceroute." These are standard LAN/WAN tools to identify:

- whether two points on a network can communicate with each other, and
- what path a sample communication takes as it traverses the network from one point to the other.

All 4600 Series IP Telephones respond appropriately to a ping or a traceroute message sent from the DEFINITY® or MultiVantage™ switch or any other source on your network. These telephones will not, in general, initiate a ping or traceroute. Release 1.6 of the 4600 Series IP Telephones introduced "remote ping" and "remote traceroute" support. The switch can instruct such a 4600 Series IP Telephone to initiate 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. See your DEFINITY® or MultiVantage™ Administration documentation for more details.

As of Release 1.8, if applicable, 4600 Series IP Telephones test whether the network Ethernet switch port supports IEEE 802.1D/q tagged frames by ARPing the router with a tagged frame. See VLAN Considerations on page 79. If your LAN environment includes Virtual LANs (VLANs), your router must respond to ARPs for VLAN tagging to work properly.

IP Address Lists and Station Number Portability

Release 1.5 of the 4600 Series IP Telephones provided the capability to specify IP Address lists in either dotted decimal or DNS format. Release 1.5 allowed key network elements to have multiple IP Addresses, rather than being restricted to just one address for each element. You can specify up to 127 total characters in each list of the following devices:

- router/gateways,
- DHCP/TFTP/HTTP servers, and
- the media server.

Upon startup or a reboot, the 4600 Telephone attempts to establish communication with these various network elements in turn. The telephone starts with the first address on the respective list. If the communication is denied or times out, the telephone proceeds to the next address on the appropriate list and tries that one. The telephone does not report failure unless all the addresses on a given list fail.

Obviously, this capability significantly improves the reliability of IP telephony. Multiple IP Addresses maximize the telephone's likelihood to communicate with backup equipment if the primary equipment is not operating or is not accessible. For example, alternate communication would be needed during a limited network outage.

However, this capability also has the advantage of making station number portability easier. 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 telephones from their offices in London and bring them to New York. When users start up their telephones in the new location, the local DHCP server will generally route them to the local switch. But the local switch denies service because it knows nothing about these new users. With proper administration of the local DHCP server, the telephone knows to try a second media server IP Address, this one in London. The user can then be automatically registered with the London switch.

Chapter 4: Server Administration contains details on administration of DHCP servers for lists of alternate media servers, router/gateways, and TFTP servers. For specific information, see DNS Addressing on page 84.

Security

In VoIP, physical wire is replaced with an IP connection. The connection is more mobile. Unauthorized relocation of the IP telephone allows unauthorized users to send and receive calls as the valid owner. For further details on toll fraud, see the DEFINITY® or Avaya Communication Manager documents mentioned in Related Documents on page 15.

Any equipment on a data network, including a 4600 Series IP Telephone, can be the target of a Denial of Service attack. Usually, such an attack consists of flooding the network with so many messages that the equipment either:

- spends so much time processing the messages that legitimate tasks are not processed, or
- the equipment overloads and fails.

The 4600 Series IP Telephones cannot guarantee resistance to all Denial of Service attacks. However, each Release has increasing checks and protections to resist such attacks while maintaining appropriate service to legitimate users.

All 4600 Series IP Telephones that have WML Web applications and run R2.2 software support Transport Layer Security (TLS). This standard allows the phone to establish a secure connection to a HTTPS server, in which the phone's upgrade and settings file can reside. This setup adds security over the TFTP alternative.

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 4: Server Administration, and include:

- As of Release 2.0, restricting the 4600 Series IP Telephone's response to SNMP queries to only IP Addresses on a list you specify.
- As of Release 2.0, specifying an SNMP community string for all SNMP messages sent by the telephone.
- As of Release 1.8, restricting dialpad access to Local Administration Procedures, such as specifying IP Addresses, with a password.
- Removing dialpad access to most Local Administration Procedures.
- Restricting the end user's ability to use a telephone Options application to view network data.

4600 Series IP Telephones

Dual Connection Architecture

Releases 1.0 and 1.1 of the 4600 Series IP Telephones use dual connection architecture to communicate with the DEFINITY® switch. In the dual connection architecture, two station extensions must be administered for each telephone.

Single Connection Architecture

Release 1.5 and subsequent releases of the 4600 Series IP Telephones use single connection architecture to communicate with the Avaya media server switch. In the single connection architecture, only one station extension must be administered for each telephone.

Registration and Authentication

The Avaya media server switch supports using the extension and password to register and authenticate 4600 Series IP Telephones. For further information, see Related Documents on page 15.

Software

As shipped from the factory, the 4600 Series IP Telephones may not contain sufficient software for registration and operation. When the phone is first plugged in, a software download from a TFTP or HTTP server starts to give the phone its proper functionality.

For downloads of software upgrades, the PBX provides the capability for a remote restart of the 4600 Series IP Telephone. As a consequence of restarting, the phone automatically restarts reboot procedures. If new software is available on the server, the telephone downloads it as part of the reboot process.

WAN Considerations

QoS is harder on a WAN than a LAN. A LAN assumes no bandwidth concerns. A WAN assumes a finite amount of bandwidth. Therefore, QoS considerations are more significant when the IP telephony environment includes a WAN. In addition, there are administrative and hardware compatibility issues unique to WANs. WAN administration is beyond the scope of this document.

DHCP and File Servers

The DHCP server provides the following information to the 4600 Series IP Telephone:

- IP Address of the 4600 Series IP Telephone
- IP Address of the Gatekeeper board on the Avaya media server
- IP Address of the TFTP server if applicable, otherwise the HTTP server
- The subnet mask
- IP Address of the router
- DNS Server IP Address

Administer the LAN so each IP telephone can access a DHCP server containing the IP Addresses and subnet mask listed.

The IP telephone cannot function without an IP Address. The failure of a DHCP server at boot time leaves all the affected voice terminals unusable. A user can manually assign an IP Address to an IP telephone. This can cause a problem when the DHCP server finally returns because 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. We therefore **strongly recommend** that a DHCP server be available when the IP telephone reboots. If a DHCP server is not available at remote sites during WAN failures, the IP telephone is not available after a reboot.

A minimum of two DHCP servers are recommended for reliability. We **strongly recommend** that 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 4600 Series IP Telephone with a script file and, if appropriate, new or updated application software. See Step 3: Telephone and File Server on page 36 under Initialization Process. In addition, you can edit an associated settings file to customize telephone parameters for your specific environment. See Administering Options for the 4600 Series IP Telephones on page 80.

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 4600 Series 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 this message and relays it to the appropriate DHCP server.

Step 2: DHCP Server to Telephone

The DHCP file server provides information to the telephone, as described in DHCP and File Servers on page 47. Among other data passed to the telephone is the IP Address of the TFTP or HTTP server, which is crucial for the next step.

Step 3: Telephone and File Server

Beginning with Release 2.2, 4600 Series IP Telephones can download script files, application files, and settings files from either a TFTP, HTTP, or HTTPS server. The HTTPS server applies only if the server supports Transport Layer Security (TLS) encryption. If you have a mixture of Release 2.2 and pre-Release 2.2 telephones, you can use either:

- TFTP servers only.
- Both TFTP and HTTP servers, with TFTP running phones with older releases and HTTP for telephones running Release 2.2 and later software.

A telephone that supports HTTP will attempt to access the HTTP server (if administered), and, if successful, will not attempt to access the TFTP server (if administered).

The script files, application files, and settings files discussed in this section are identical for HTTP and TFTP servers. The general downloading process for those files is essentially the same. One exception is that when you use an HTTPS server, a TLS server is contacted first. Therefore, we use the generic term “file server” here to mean both “TFTP server” and “HTTP 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 application file the telephone must use. The application file is the software that has the telephony functionality, and can be easily updated for future enhancements.

The telephone uses the script file to determine if it has the proper application file. A newly installed telephone may have no application file, and therefore would not have the proper one. A previously installed telephone might not have the proper application file. If the telephone determines the application file indicated in the script file is missing, the telephone requests a download of the proper application file 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 phone proceeds to the next step without downloading the application file again.

After checking and loading the application file, the 4600 Series IP Telephone, if appropriate, uses the script file to look for a settings file. The settings file can contain options you have administered for any or all of the 4600 Series IP Telephones in your network. For more information about this settings file, see Administering Options for the 4600 Series IP Telephones on page 80.

Step 4: Telephone and the Avaya Media Server

In this step, the telephone and the PBX exchange a series of messages which cause the display on the telephone to prompt the user. For a new installation, the user must enter the telephone's extension and the media server 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 the switch exchange more messaging, with the expected result that the telephone is appropriately registered on the switch.

More details about the installation process are available in the *4600 Series IP Telephone Installation Guide* and in Chapter 3: Requirements of this document.

Chapter 3: Requirements

Introduction

The 4600 Series IP Telephones use Internet Protocol (IP) technology with Ethernet line interfaces. The IP telephones supplement the existing Avaya IP Solutions platform. This feature provides the user with the capability to natively administer and maintain the new 4600 Series IP Telephones.

The 4600 Series IP Telephones provide support for DHCP, TFTP, and HTTP over IPv4/UDP, which enhance the administration and servicing of the phones. These phones use DHCP to obtain dynamic IP Addresses and TFTP or HTTP to download new versions of software for the phones.

Using the telephone's built-in hub, the 4600 Series IP Telephones offer one desktop connection for both the telephone set and the PC.

Hardware Requirements

Before plugging in the 4600 Series IP Telephone, verify that all the hardware requirements are met. Failure to do so prevents the telephone from working and might have a negative impact on your network.

The following hardware is required for 4600 Series IP Telephones to work properly.

Note:

The recommended configuration is the latest PBX software and the latest IP telephone firmware. In the event your site does not have the latest PBX software, follow the recommendations in the table immediately below.

Media Server Release	Avaya IP Telephone	IP Telephone Release	Notes
Avaya Communication Manager 1.3+	All telephones	R1.8+	Use the latest release.
Avaya Communication Manager 1.1, Avaya Communication Manager 1.2	All telephones *except* 4630	R1.8+	Use the latest release.
R10, Avaya Communication Manager 1.1, Avaya Communication Manager 1.2	4630	R1.74	Upgrade to Avaya Communication Manager Release 1.3 or later before installing R1.8 on 4630 telephones.
R10	4606, 4612, 4624	R1.8+	The 4602 and 4620 are not supported.
R9.5	4606, 4612, 4624	R1.8+	The 4620, 4602, and 4630 are not supported. R1.5 is the minimum 4600 IP Telephone vintage.
R9	4612, 4624	R1.1	R1.1 is the only supported 4600 IP Telephone vintage.
R8.4	4612, 4624	R1.0	R1.0 is the only supported 4600 IP Telephone vintage.

Additional Hardware Requirements

- Ensure that the appropriate circuit pack(s) are administered on your media server. See the media server's hardware guide for more detail.
- A Category 5e LAN. If the telephones are to be powered from the LAN, the power supply must be designed to the IEEE 802.3af-2003 standard for LAN powering.
- Electrical power provided to each phone by one of the following two sources:
  - A Telephone Power Module, also called the DC power jack. You must order this module separately, except for the 4630 and the 4690 phones. The 4630 comes with its own power brick and the 4690 has its own power interface module. The 4630SW does not come with a power brick. For the 4630SW, you must order the power brick separately if LAN powering will not be used for that particular telephone model.
  - IEEE 802.3af-2003, if the LAN supports this powering scheme. Note that the 4630 and 4690 **cannot** be powered this way, but the 4630SW **can** be powered this way.

- Verify that the 4600 Series IP Telephone package includes the following components:
  - 1 telephone set.
  - 1 telephone handset. Note that the 4622SW and the 4690 IP Conference Telephones do not come with handsets.
  - 1 H4DU 4-conductor coiled handset cord that is 9-foot long when extended, plugged into the telephone and the handset. Not applicable for the 4622SW and 4690 IP Conference Telephones.
  - 1 Category 5 modular line cord for the connection from the IP telephone to the Ethernet wall jack.
  - *4600 Series IP Telephone Safety Instructions* (555-233-779).
  - Power Interface Module for the 4690 IP Conference Telephone only.
  - Power Brick for 4630 IP Telephones only.
  - Stylus for 4630/4630SW IP Telephones only.
- You might need a Category 5e modular line cord for the connection from the 4600 Series IP Telephone to the PC.

Note:

See the *4600 Series IP Telephone Installation Guide*.

Software Requirements

The following software is required for 4600 Series IP Telephones to work properly:

- The DHCP server and application must be installed and properly administered, as described in DHCP on page 49.

CAUTION:

A DHCP server is not mandatory, but static addressing is necessary when a DHCP server is unavailable. Because of difficulties associated with static addressing, we **very strongly recommend** that a DHCP server be installed and that static addressing be avoided.

- The TFTP and/or HTTP file server and application must be properly administered, as described in TFTP on page 62 and HTTP on page 66.

  CAUTION:

  A file server does not need to be available for the Avaya IP Telephones to operate. The Avaya IP Telephones obtain important information from the script files on the file server and depend on the application file for software upgrades. If the file server is not available when the Avaya IP Telephones reset, the telephones will register with the media server and operate. Some features may not be available, and restoring those features requires resetting the Avaya IP Telephone(s) when the file server is available.

- For 4630 and 4630SW IP Telephone environments, if users are to have access to LDAP directories or corporate Web sites, the appropriate servers must be in place. The 4630/4630SW Telephones must be appropriately administered in accordance with Server Administration on page 43.

  CAUTION:

  4630 IP Telephone Release 1.72 introduced significant software architecture changes. Thus, unlike most 4600 Series IP Telephones software releases, 4630 IP Telephone Release 1.72 and later **cannot** be downgraded to a release earlier than 1.72. Attempting to do so renders the 4630 (and 4630SW, if Release 1.8 or greater) set inoperable. In addition, if you are upgrading a 4630 from a release prior to Release 1.61, you must first upgrade to Release 1.61. Then you must upgrade to the newer Release. You **cannot** upgrade directly from a pre-1.61 Release to a post-1.61 Release for the 4630.

- For 4610SW/4620/4620SW/4621SW/4622SW/4625SW IP Telephone environments, if users are to have access to LDAP directories or corporate WML Web sites, the appropriate servers must be in place. You must download the LDAP Directory Application software from the Avaya support Web site. You must appropriately administer the telephones in accordance with Server Administration on page 43.

  Note:

  Ensure that all required parameters are configured correctly. For Avaya media server information, see your administration documentation. For the DHCP and file servers, see Chapter 4: Server Administration.

Chapter 4: Server Administration

Introduction

When a 4600 Series IP Telephone is plugged in and powered, it automatically negotiates with its associated LAN to determine the Ethernet speed. From that point on, the telephone's actions depend largely on network administration prior to phone installation, and on any actions the installer takes. This chapter details the parameters and other data the telephone needs to operate, and the alternatives to deliver that information to the telephone, where appropriate. Recommendations and specifications for alternatives to certain parameters are also provided.

The parameters under which the phone needs to operate are summarized as follows:

- Telephone Administration on the media server.
- IP Address management for the telephone.
- Tagging Control and VLAN administration for the telephone, if appropriate.
- Quality of Service (QoS) administration for the telephone, if appropriate.
- Site-specific Option Number (SSON) setting of DHCP servers, if appropriate.
- Interface administration for the telephone, if appropriate.
- Application-specific telephone administration, if appropriate. For example, Directory- or Web-specific information required for these optional applications.

The delivery mechanisms are:

- Maintaining the information on the Avaya media server.
- Manually entering the information using the telephone dialpad.
- Administering the DHCP server.
- Editing the settings file on the applicable TFTP or HTTP file server.

These parameters can be administered in a variety of ways, as indicated in Table 1. Note that not all parameters can be administered on all delivery mechanisms.

Table 1: Administration Alternatives and Options for 4600 Series IP Telephones

Parameter(s)	Administrative Mechanisms	For More Information See:
Telephone Administration	Media server	Administering 4600 Series IP Telephones on Avaya Media Servers on page 46 and Related Documents on page 15.
IP Addresses	DHCP (strongly recommended)	DHCP and File Servers on page 47, and especially DHCP on page 49.
	Settings file	DHCP and File Servers on page 47 and Administering Options for the 4600 Series IP Telephones on page 80.
	Manual administration at the phone	See “Static Addressing Installation” in Chapter 3 of the *4600 IP Telephone Installation Guide.*
Tagging and VLAN	DHCP	DHCP and File Servers on page 47, and Administering Options for the 4600 Series IP Telephones on page 80.
	Settings file (strongly recommended)	DHCP and File Servers on page 47 and Administering Options for the 4600 Series IP Telephones on page 80.
	Manual administration at the phone	See “Static Addressing Installation” in Chapter 3 of the *4600 IP Telephone Installation Guide*.
Quality of Service	Media server	Administering 4600 Series IP Telephones on Avaya Media Servers on page 46 and Related Documents on page 15.
	DHCP	DHCP and File Servers on page 47, and Administering Options for the 4600 Series IP Telephones on page 80.
	Settings file (strongly recommended)	DHCP and File Servers on page 47, and Administering Options for the 4600 Series IP Telephones on page 80.
	Manual administration at the phone	See “QoS Option Setting” in Chapter 3 of the *4600 IP Telephone Installation Guide*.

1 of 2

Table 1: Administration Alternatives and Options for 4600 Series IP Telephones (continued)

Parameter(s)	Administrative Mechanisms	For More Information See:
Interface	DHCP	DHCP and File Servers on page 47, and Administering Options for the 4600 Series IP Telephones on page 80.
	Settings file (strongly recommended)	DHCP and File Servers on page 47, and Administering Options for the 4600 Series IP Telephones on page 80.
	Manual administration at the phone	See “Secondary Ethernet (Hub) Interface Enable/Disable” in Chapter 3 of the *4600 IP Telephone Installation Guide*.
SSON	DHCP	Customizing the Site-Specific Option Number (SSON) on page 84. DHCP and File Servers on page 47, and especially DHCP on page 49.
	Settings file (strongly recommended)	Customizing the Site-Specific Option Number (SSON) on page 84. DHCP and File Servers on page 47, and especially TFTP Generic Setup on page 62 and HTTP Generic Setup on page 66.
	Manual administration at the phone	See “Site-Specific Option Number Setting” in Chapter 3 of the *4600 IP Telephone Installation Guide*.
Application - specific parameters	DHCP	DHCP and File Servers on page 47, and especially DHCP on page 49. Also, Customizing the 4630/4630SW IP Telephone on page 87 and Customizing 4610SW, 4620/4620SW, 4621SW, 4622SW, and 4625SW IP Telephones on page 92.
	Settings file (strongly recommended)	DHCP and File Servers on page 47, especially TFTP on page 62. Also, Customizing the 4630/4630SW IP Telephone on page 87 and Customizing 4610SW, 4620/4620SW, 4621SW, 4622SW, and 4625SW IP Telephones on page 92.

2 of 2

General information about administering DHCP servers is covered in DHCP and File Servers on page 47, and more specifically, DHCP on page 49. General information about administering TFTP servers is covered in DHCP and File Servers, and more specifically, TFTP on page 62. General information about administering HTTP servers is covered in DHCP and File Servers, and more specifically, HTTP. Once you are familiar with that material, you can administer telephone options as described in Administering Options for the 4600 Series IP Telephones on page 80.

Note:

If a given parameter is administered in multiple places, the last server to provide the parameter has precedence. The precedence is:

- manual administration,
- DHCP,
- TFTP/HTTP,
- the media server, and finally,
- FTP backup files (if administered and if permitted).

Any settings the IP telephone receives from FTP backup files, or in their absence, the media server, overwrite any previous settings, including manual settings. The only exception to this sequence is in the case of VLAN IDs. In the case of VLAN IDs, the usual sequence applies through TFTP or HTTP as appropriate. If the VLAN ID after TFTP or HTTP is not zero, any VLAN ID from the media server is ignored.

Administering 4600 Series IP Telephones on Avaya Media Servers

DEFINITY Releases 9, 9.5, 10, and Avaya Communication Manager Software Release 1.1+

DEFINITY® Releases 9 and 9.5 provide support for the 4606, 4612, and 4624 IP Telephones. DEFINITY® Release 10 adds support for the 4630 and 4630SW IP Telephones. Avaya Communication Manager Software Release 1.1 adds support for the 4602/4602SW and 4620/4620SW IP Telephones. Administration of a 4612 and 4624 IP Telephone is identical to a 6424 IP softphone. The 4610SW and 4690 are not natively supported, but can be aliased as 4620 IP Telephones. See Related Documents on page 15, particularly the *Administration for Network Connectivity* and the *Administrator Guides*. Follow these guidelines:

- 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.
- The **IP Softphone** field does not have to be set to "**y**" (Yes).

DEFINITY Release 8.4

Note:

DEFINITY® Release 8.4 is very old. We do not recommend using this release.

DEFINITY® Release 8.4 supports the 4612 and 4624 IP Telephones. The 4612 and 4624 IP Telephones are aliased as 6424 Telephones, administered as IP Softphones. The administrative forms for the 6424 IP Softphone are used for the two IP telephones. See Related Documents on page 15, particularly the *Administration for Network Connectivity* and the *Administrator Guides*. Follow these guidelines:

- Alias the IP telephone as a 6424D+ DCP set, with the **IP Softphone** field set to "**y**" (Yes).
- Administer a **Media Complex Ext** for the audio channel.

DHCP and File Servers

Dynamic Host Configuration Protocol (DHCP) provides a means by which configuration parameters can be automatically assigned to clients on a TCP/IP network. DHCP minimizes a 4600 Series IP Telephone network's maintenance by removing the need to individually assign and maintain IP Addresses and other parameters for each IP telephone on the network.

Software Checklist

Ensure that you have purchased and/or own licenses to install and use any or all of the DHCP, TFTP, and HTTP server software.

Note:

It is possible to install the DHCP, TFTP, and HTTP server software on the same machine.

CAUTION:

The circuitry in the 4600 Series IP Telephones reserves IP Addresses of the form **192.168.2.x** for internal communications. The telephone(s) will not properly use addresses you specify if they are of that form.

Required Network Information

DHCP is the control point where an enterprise controls its IP telephones. Before administering DHCP and TFTP, HTTP, and TLS, as applicable, complete the information in Table 2: Required Network Information Before Installation - Per DHCP Server on page 48. Completing the pre-installation steps ensures that you have the necessary information regarding your network. If you have more than one Gateway, TFTP/HTTP/TLS server, subnet mask, and Gatekeeper in your configuration, you need to complete Table 2 for each DHCP server.

Release 1.5 of the 4600 Series Telephones supported specifying a list of IP Addresses for a gateway/router, TFTP server, and Avaya media server Gatekeeper(s). We explain this specification in Overview of Voice over IP (VoIP) on page 21. Each list can contain up to 255 total ASCII characters, with IP Addresses separated by commas with no intervening spaces. Note that depending on the specific DHCP application, only 127 characters might be supported.

When specifying IP Addresses for the file server or media server, use either dotted decimal format (“xxx.xxx.xxx.xxx”) or DNS names. If you use DNS, note that 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 specific information about DNS, see DHCP Generic Setup on page 50 and DNS Addressing on page 84.

Table 2: Required Network Information Before Installation - Per DHCP Server

1. Gateway (router) IP Address(es)	
2. TFTP server IP Address(es)	If applicable.
3. Subnet mask	
4. Avaya Media Server Gatekeeper IP Address(es)	
5. Avaya Media Server Gatekeeper port	Although this can be a value between 0 and 65535, the default value is **1719**. Do not change the default value unless that value conflicts with an existing port assignment.
6. TFTP server file path	If applicable.
7. Telephone IP Address range *From*: *To*:	
8. DNS server address(es)	If applicable.
9. HTTP server address(es)	If applicable.
10. HTTPS/TLS server address(es)	If applicable

The file server’s file path is the “root” directory used for all transfers by the server. This is the default directory all files will be uploaded to or downloaded from. In configurations where the upgrade script and application files are in the default directory, item 6 in Table 2: Required Network Information Before Installation - Per DHCP Server on page 48 should not be used.

DHCP

This section provides basic information on DHCP servers and generic information on DHCP server administration.

Choosing a DHCP Configuration

A discussion on how to best set up your network to work with the 4600 Series IP Telephones is beyond the scope of this document. See Network Assessment on page 26. This document concentrates on the simplest case of the single LAN segment. Information provided here can be extrapolated for more complex LAN configurations.

CAUTION:

Before you start, it is important that you understand your current network configuration. An improper installation can cause network failures or reduce the reliability and performance of your network.

DHCP Software Alternatives

Two 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 customer's responsibility to install and configure the DHCP server correctly. This document is limited to describing a generic administration that works with the 4600 Series IP Telephones.

DHCP Generic Setup

DHCP server setup involves the following phases:

1. Installing the DHCP server software according to vendor instructions.
2. Configuring the DHCP server with the following information:
   - IP Addresses available for the 4600 Series IP Telephones.
   - The following DHCP options:
     - Option 1- Subnet mask, as described in Table 2, item 3.
     - Option 3 - Gateway (router) IP Address(es), as described in Table 2, item 1. 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.
     - Option 6 - DNS server(s) address list. 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. At least one address in Option 6 must be a valid, non zero, dotted decimal address. Otherwise, DNS will fail.
     - 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 4600 IP Telephone attempts to resolve the DNS address. Option 15 is necessary if you want to use a DNS name for the TFTP server. Otherwise, you can specify a DOMAIN as part of customizing TFTP as indicated in DNS Addressing on page 84.
     - Option 51 - DHCP lease time, if desired. We recommend six weeks or greater. Expired leases cause Avaya IP Telephones to reboot. It is highly desirable to provide enough leases so an IP telephone's IP Address does not change if it is briefly taken offline.

Note:

The DHCP standard states that when a DHCP lease expires, the device should immediately cease using its assigned IP Address. This is not necessarily the desired behavior for telephones, especially if a user is on a call. 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.

Preferably, 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 6: 4600 Series IP Telephone Customizable System Parameters on page 80 indicates, the system parameter DHCPSTD allows an administrator to specify that the telephone will either:

- Comply with the DHCP standard by setting DHCPSTD to “1”, or
- 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 phone 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 RFC 2132, Section 9.3.
- Option 58 - DHCP lease renew time, if desired.
- Option 59 - DHCP lease rebind time, if desired.
- Option 66 - TFTP Server Name.

Note:

Microsoft DHCP servers support only dotted-decimal format for file server addresses, not symbolic names. Option 66 need not be used if the TFTP server is identified in the Site Specific Option Number string (Option 176), or if HTTP is to be used exclusively instead of TFTP. However, to simplify configuration, we recommend that you use Option 66 if you are using TFTP. If you use both Option 66 and Option 176 to identify TFTP servers, the value(s) in Option 176 overrides the value(s) in Option 66.

- A 4600 Series IP Telephone-specific DHCP option specifying information such as TFTP server and Avaya Media Server Gatekeeper IP Addresses. Use the Site-Specific Option Number (SSON) at #176. You can set this option’s value, for example, to either of the following strings:

  MCIPADD=*xxx.xxx.xxx.xxx*,MCPORT=*yyyy*,TFTPDIR=<*path*>,TFTPSRVR=*zzz.zzz.zzz.zzz*

  OR

  MCIPADD=*{list of DNS names}*, MCPORT=*yyyy*, TFTPDIR=<*path*>, TFTPSRVR= *{list of DNS names}*

Note:

List the TFTPDIR value before the TFTPSRVR value, if the latter is specified in the SSON.

Note:

Some DHCP applications limit the length of Option 176 to 247 characters.

The 4600 Series IP Telephones do not support Regular Expression Matching, and therefore, do not use wildcards. See Administering Options for the 4600 Series IP Telephones on page 80.

In configurations where the upgrade script and application files are in the default directory, do not use the TFTPDIR=<path>.

You do not have to use Option 176. If you do not use this option, you must ensure that the key information, especially TFTPSRVR, MCIPADD, and MCPORT, is administered appropriately elsewhere. For example, when you specify the DNS server in Option 6, and the Domain Name in Option 15, you can use the configured names “AvayaTFTPServer” and “AvayaCallServer” for TFTPSRVR and MCIPADD, respectively. Upgrading from IP telephone Releases prior to R1.60 requires Option 176 to be minimally administered with MCIPADD.

Administer DHCP servers to deliver only the options specified in this document. Administering additional, unexpected options might have unexpected consequences, including possibly causing the IP telephone to ignore the DHCP server.

The media server name and TFTP server name must each be no more than 32 characters in length.

Note:

Examples of good DNS administration include:

- Option 6: “***aaa.aaa.aaa.aaa***”
- Option 15: “***dnsexample.yourco.com***”
- Option 66: “***tftpserver.yourco.com,zzz.zzz.zzz.zzz***”
- Option 176: “**MCIPADD=*xxxx.xxx.xxx.xxx***”

Depending on the DHCP application you choose, be aware that the application most likely will not immediately recycle expired DHCP leases. An expired lease might remain reserved for the original client for a day or more. For example, Windows NT® DHCP reserves expired leases for about one day. This reservation period protects a client’s lease for a short time. If the client and the DHCP server are in two different time zones, the computers’ clocks are not in synch, 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 first two telephones’ lease 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 phone remains without a lease until the reservation period expires.

In Table 3, the 4600 Series IP Telephone sets the system values to the DHCPACK message field values shown.

Table 3: DHCPACK Setting of System Values

System Value	Set to
IPADD	The **yiaddr** field.
NETMASK	Option #1 (if received).
GIPADD	The first four octets of Option #3 (if received).
TFTPSRVR	The first four octets of the **siaddr** field.

The rest of this section describes some common DHCP servers.

Windows NT 4.0 DHCP Server

This section contains details on how to verify and configure the DHCP server included in the Windows NT® 4.0 server operating system.

Use Verifying the Installation of the DHCP Server to verify whether the DHCP server is installed. If it is not, install the DHCP server. If it is installed, go to the section Initial Configuration on page 54 and the subsequent sections.

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, go to the following section, Initial Configuration. If it is not listed, then install the DHCP server.

Initial Configuration

The Windows NT® 4.0 DHCP server configuration involves setting up a scope for the IP telephone. A DHCP scope is essentially a grouping of IP devices, in this case IP telephones, running the DHCP client service in a subnet. The scope defines parameters for each subnet. Each scope has the following properties:

- A unique subnet mask used to determine the subnet related to a given IP Address.
- A scope name assigned by the administrator when the scope is created.
- Lease duration values to be assigned to DHCP clients with dynamic addresses.

In addition, the DHCP server can assign configuration parameters to a client, and these can be specified for each DHCP scope.

Setting up the Windows NT® 4.0 DHCP server requires the following steps:

1. Creating a DHCP scope for the IP telephones.
2. Editing custom options.
3. Adding the DHCP options.
4. Activating the new scope.

Each step is detailed in the next four sub-sections.

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. Define the range of IP Addresses used by the IP telephones listed in Table 2: Required Network Information Before Installation - Per DHCP Server.

   The **Start Address** is the first IP Address to be used for the IP telephones.

   The **End Address** is the last IP Address to be used for the IP telephones.

   Set the **Subnet Mask** to the value recorded in Table 2: Required Network Information Before Installation - Per DHCP Server.

   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.

Example:

Suppose the range of IP Addresses available for your IP telephone network are:

- 135.254.76.7 to 135.254.76.80
- 135.254.76.90 to 135.254.76.200
- 135.254.76.225 to 135.254.76.230

Your start address and end address are 135.254.76.7 and 135.254.76.230 respectively.

Exclude the ranges 135.254.76.81 to 135.254.76.89 and 135.254.76.201 to 135.254.76.224.

Note:

We recommend that you provision the 4600 Series IP Telephones with sequential IP Addresses.
We recommend not mixing 4600 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 “DEFINITY IP Telephones.”
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, “46XXOPTION”.
5. Change the **Data Type Byte** value to **String**.
6. Enter **176** in the **Identifier** field.

7. Click the **OK** button.

   The **DHCP Options** menu displays.
8. Select the **Option Name** for 176 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 2: 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 **176 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 **176 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.

1. 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 **46XXOPTIONs** are correctly configured for the Windows NT® 4.0 DHCP server.

Verify the Default Option, 176 46XXOPTION

Use the following procedure to verify the default option.

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 **176 46XXOPTION**.
6. Verify that the **Value String** box contains the correct string from DHCP Software Alternatives on page 49.

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

Verify the Scope Option, 176 46XXOPTION

Use the following procedure to verify the scope option:

1. Select **Scope** under **DHCP OPTIONS**.
2. In the **Active Options:** scroll list, click **176 46XXOPTION**.
3. Click the **Value** button.
4. Verify that the **Value String** box contains the correct string from DHCP Generic Setup on page 50.

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

Verify the Global Option, 176 46XXOPTION

Use the following procedure to verify the global option:

1. Select **Global** under **DHCP OPTIONS**.
2. In the **Active Options:** scroll list, click **176 46XXOPTION**.
3. Click the **Value** button.
4. Verify that the **Value String** box contains the correct value from DHCP Generic Setup on page 50. If not, update the string and click the **OK** button.

Windows 2000 DHCP Server

This section describes the configuration of the DHCP server in Windows 2000®.

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 “DEFINITY IP Telephones,” 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 2: 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:

   We recommend not mixing 4600 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.

   Example:

   Suppose the ranges of IP Addresses available for your IP telephone network are:
   - 135.254.76.7 to 135.254.76.80
   - 135.254.76.90 to 135.254.76.200
   - 135.254.76.225 to 135.254.76.230

   The Start IP Address and End IP Address you enter in the **IP Address Range** dialog box are 135.254.76.7 and 135.254.76.230 respectively.

   In the Add Exclusions dialog box, exclude the following ranges:
   - 135.254.76.81 to 135.254.76.89
   - 135.254.76.201 to 135.254.76.224

   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 a device's IP Address 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 will 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. Click the **Configure Options...** option.

   The **Scope Options** dialog box displays.

3. In the General tab page, under the **Available Options**, check the **066'Boot Server Host Name' Options** checkbox.

   The **String Value** dialog box displays.

4. Enter the ***TFTP Server address(es)*** in the **String Value**. Use the same TFTPSRVR value format as discussed in TFTP Generic Setup on page 62. For example, if you had a TFTP server at IP Address "*zzz.zzz.zzz.zzz*" and a second TFTP server at address "tftpserver.yourco.com," in the string value enter:

   "zzz.zzz.zzz.zzz,tftpserver.yourco.com"

5. In the left pane of the DHCP, right click the **DHCP Server name**, then click **Set Predefined Options...**.

6. Under **Predefined Options and Values**, click **Add**.

7. In the **Option Type Name** field, enter ***any appropriate name***, for example, "Avaya IP Telephones".

8. Change the **Data Type** to **String**.
9. In the **Code** field, enter **176**, then click the **OK** button twice.

   The **Predefined Options and Values** dialog box closes, leaving the DHCP dialog box enabled.
10. Expand the newly created scope to reveal its **Scope Options**.
11. Click **Scope Options** and select **Action**- ->**Configure Options** from the menu.
12. In the **General** tab page, under the **Available Options**, check the **Option 176** checkbox.
13. In the **Data Entry** box, enter the ***DHCP IP telephone option string*** as described in DHCP Generic Setup on page 50.

    Note:

    You can enter the text string directly on the right side of the **Data Entry** box under the ASCII label.
14. From the list in **Available Options**, check option **003 Router**.
15. Enter the ***gateway (router) IP Address*** from the IP Address field of Table 2: Required Network Information Before Installation - Per DHCP Server.
16. Click the **Add** button.
17. 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.

TFTP

This section describes how to set up a TFTP server for downloading software updates to the 4600 Series IP Telephones.

CAUTION:

The files defined by the TFTP server configuration have to be accessible from all IP telephones. Ensure that the filenames match the names in the upgrade script, including case, since UNIX systems are case-sensitive.

Note:

You can use any TFTP application you want. However, we strongly recommend using the TFTP application available for free download at http://www.avaya.com/support or the TFTP server capability on the S8300's media server. The Avaya support site also contains instructions for installing and configuring the Avaya TFTP server.

TFTP Generic Setup

The following phases are involved in setting up a TFTP server.

- Install the TFTP server software. The two sections that follow describe how to install and configure Avaya's TFTP application.
- Configure the file path parameter to the directory where the files are to be stored. This is the file path in Table 2: Required Network Information Before Installation - Per DHCP Server on page 48. For increased security, we also recommend that you disable the ability to upload to the server. Note that this option might not be available to all TFTP servers.
- Download the upgrade script file and application file from the Avaya Web site (http://www.avaya.com/support) to the directory as specified by the file path.

  Note:

  Many LINUX servers distinguish between uppercase and lowercase names. Ensure that you accurately specify the 46xxsettings filename, and the names and values of the data therein.

Avaya TFTP (Suite Pro)

Configuration

Use the following procedure to configure the Avaya TFTP server:

1. Run the TFTP Suite Pro Server by selecting:
   Start- ->**Programs**- ->**Avaya TFTP Server**- ->**TFTPServer32**.

   The TFTP server starts.

   CAUTION:

   You must restart Avaya TFTP manually whenever you reboot your TFTP server machine.

2. Select **System**- ->**Setup**.

3. Enter the following values:

   On the **Outbound** tab page: **1**.
   The **Outbound path** is the TFTP file path as recorded in Table 2: Required Network Information Before Installation - Per DHCP Server on page 48.

   Check the **Enable Path** options.
   Under the **Options** tab page: turn on the **No Incoming** option. Under the **Client Limits** tab page: Drag the slide bar all the way to the right to set the **Maximum Simultaneous Clients** to **infinite**.

4. Place the ***46xxupgrade.scr*** file in the file path directory. The filename “46xxupgrade.scr” is an example only. Use the filename obtained from the material downloaded from the Avaya Support Web site. See Contents of the Upgrade Script on page 71.

TFTP Server on S8300 Media Server

The S8300 Media Server provides all the TFTP support required for the 4600 Series IP Telephones. In addition, the media server has an easy to use, PC-based interface for creating script files. Thus, you do not need to manually create the text files discussed in 4600 Series IP Telephone Scripts and Application Files. The media server creates the files for you. For more information about the media server, see *Installation and Upgrades for Avaya G700 Media Gateway and Avaya S8300 Media Server*, mentioned in Related Documents.

Table 6, Table 7, and Table 8 list the parameters you can administer when manually creating the TFTP script file. Manual administration is discussed in 4600 Series IP Telephone Scripts and Application Files. When using the media server, you do not need to worry about the specific parameter names, since the media server handles that for you. For information, Table 4 lists the parameter names from 4600 Series IP Telephone Scripts and Application Files. Table 4 also indicates the corresponding field name from the media server’s TFTP/HTTP server application. Any limits, restrictions, etc. on the parameters are built into the media server.

Table 4: Media Server Field Names & Corresponding Script File Parameter Names

Media Server Field Name	Script File Parameter Name
Domain Name	DOMAIN
Domain Name Server	DNSSRVR
HTTP Server IP Address	HTTPSRVR
HTTP Directory	HTTPDIR
HTTP Port	HTTPPORT
Source IP Addresses for SNMP Queries	SNMPADD
SNMP Community String	SNMPSTRING
Telephone Country Code	PHNCC
Telephone Dial Plan Length	PHNDPLENGTH
International Access Code	PHNIC
Long Distance Access Code	PHNLD
National Telephone # Length	PHNLDLENGTH
Outside Line Access Code	PHNOL
Handset Audio Gain Control Status	AGCHAND
Headset Audio Gain Control Status	AGCHEAD
Speaker Audio Gain Control Status	AGCSPKR
Application Status	APPSTAT
CTI Status	CTISTAT
CTI UDP Port	CTIUDPPORT
Infrared Interface Status	IRSTAT
Layer 2 Audio Priority Value	L2QAUD
Layer 2 Signaling Priority Value	L2QSIG
802.1A VLAN Identifier	L2QVLAN
Management Complex IP Addresses	MCIPADD
Management Complex Transport Layer Port	MCPORT
Network Audio Quality Assessment Display	NTWKAUDIO
Wait Time for DHCP Offer	VLANTEST
Ethernet Line Interface Status	PHY1STAT

1 of 2

Table 4: Media Server Field Names & Corresponding Script File Parameter Names (continued)

Media Server Field Name	Script File Parameter Name
Secondary Ethernet Line Interface Status	PHY2STAT
Local (dial pad) Procedure Password	PROCPSWD
RTCP Monitor IP Address	RTCPMON
Voicemail Home Page	VMLHOME
LDAP Directory Server	DIRSRVR
LDAP Directory Server TCP Port	DIRLDAPPORT
LDAP Directory's Topmost Distinguished Name	DIRTOPDN
Default Search Value	DIRFULLNAME
Telephone Number Field Name in LDAP	DIRTELNUM
Maximum Seconds for Directory Search	DIRSRCHTIME
4630 Home Page	WEBHOME
4630 HTTP Proxy Server	WEBPROXY
4630 HTTP Proxy Server Port	WEBPORT
4630 HTTP Proxy Server Exception Domains	WEBEXCEPT
Emergency Contact Number	PHNEMERGNUM
Stock Ticker	STKSTAT
System Language	SYSLANG
4610SW/4620 Home Page	WMLHOME
4610SW/4620 HTTP Proxy Server	WMLPROXY
4610SW/4620 HTTP Proxy Server Port	WMLPORT
4610SW/4620 HTTP Proxy Server Exception Domains	WMLEXCEPT
FTP Server	FTPSRVR
FTP Directory	FTPDIR
User Options Access	OPSTAT

2 of 2

HTTP

This section gives general guidance to set up an HTTP server for downloading software updates to 4600 Series IP Telephones.

CAUTION:

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. In addition to the HTTP application on the Avaya S8300 Media Server, other commonly used HTTP applications include Apache and Microsoft IIS.

HTTP Generic Setup

These are the phases involved in setting up an HTTP server:

- Install the HTTP server application.
- Administer the system parameters HTTPSRVR and CODESRVR to the address(es) of the HTTP server. Include these parameters in DHCP Option 176, or the appropriate SSON Option.
- Download the upgrade script file and application file(s) from the Avaya Web site http://www.avaya.com/support to the HTTP server.

  Note:

  Many LINUX servers distinguish between upper and lower case names. Ensure that you specify the 46xxsettings filename 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.

4600 Series IP Telephone Scripts and Application Files

The files necessary to operate the 4600 Series IP Telephones are available on the Avaya Web site at: http://www.avaya.com/support.

Two files on the file server are essential. Other files are needed when the Avaya IP Telephones need an upgrade. The essential files are:

Note:

The 4630 Telephones have a different upgrade process than the other telephones. This is because the 4630 touch screen operation is significantly more complex than any of the other Avaya IP Telephones. There are some common elements between the 4630 and other IP telephones. Any differences are highlighted as appropriate in this section.

- An upgrade script file, which tells the IP telephone whether the phone needs to upgrade software. The Avaya IP Telephones attempt to read this file whenever they reset. The upgrade script file is also used to point to the settings file. There are separate upgrade script files for the 4630 Telephones.
- The settings file contains the option settings that enable many of the options you will need to customize the Avaya IP Telephones for your enterprise. You can use one settings file for all your Avaya IP Telephones.

In addition to the upgrade script and settings files you need the latest binary code used in the Avaya IP Telephones.

The upgrade script file and settings file are available from the Avaya Web site. The files allow you to upgrade to new software releases and new functionality without having to replace IP telephones. These two files, plus other useful information such as a ReadMe file, information about infrared capabilities, and a settings file template, are contained in a self-extracting executable file you download to your file server. Application files for all current 4600 Series IP Telephones except the 4630/4630SW, and an upgrade script file, are bundled together in that self-extracting executable file. The self-extracting executable file comes in both zipped and unzipped format. See Choosing the Right Application File and Upgrade Script File on page 69 for more information.

The Avaya-provided upgrade script files, and the binaries included in the zip files, upgrade the Avaya IP Telephones. You should not need to modify them. It is essential that all the binary files be together on the file server. When downloading a new release onto a file server with an existing release already on it, we recommend that you:

- Stop the file server.
- Back up all the current file server directories as applicable.
- Copy your ***46xxsettings.txt*** file to a backup location.
- Remove all the files in the download directory. This ensures that you do not have an inappropriate binary or configuration file on the server.

- Download the self-extracting executable file, or the corresponding zip file.
- Extract all the files. When extracting the 4630 files, ensure that you allow the directories to be created.
- Copy your ***46xxsettings.txt*** file back into the download directory.
- Check the Readme files for release-specific information.
- Modify the ***46xxsettings.txt*** file as desired.
- Restart the TFTP/HTTP Server.
- Reset your Avaya IP Telephones.

You can download a default upgrade script file, sometimes called merely the "script file," from http://www.avaya.com/support. This file allows the telephone to use default settings for customer-definable options. Of course, these settings can also be changed with DHCP or in some cases, from the telephone's dialpad itself. However, you might want to open the default file and administer the options to add useful functionality to your Avaya IP Telephones. This file must reside in the same directory as the upgrade script file, and must be called ***46xxsettings.scr*** or ***46xxsettings.txt***. The Avaya IP Telephones can operate without this file.

Note:

Most Windows systems interpret the file extension *.scr as a screen saver. The 4600 IP Telephones originally used *.scr to indicate a script file. Starting with Release 1.7, the settings file can also have the extension *.txt.

The settings file can include any of the 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 settings file at the next line after a ***# tag*** statement. If no such statement exists, the rest of the settings 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.
- **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, etc.

Note:

Enclose all data in quotation marks for proper interpretation.

The Avaya-provided upgrade script file includes lines that tell the telephone to **GET *46xxsettings.scr*** and ***46xxsettings.txt***. These lines cause the telephone to use TFTP/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. The upgrade script file is processed so that if there is no 46xxsettings.scr file, the telephone looks for a 46xxsettings.txt file. If the settings file is successfully obtained but does not include any setting changes the telephone stops using TFTP or HTTP. This happens when you initially download the script file template from the Avaya support Web site, before you make any changes. When the settings file contains no setting changes, the telephone does not go back to the upgrade script file.

You can change the settings file name, if desired, as long as you also edit the corresponding **GET** command in the upgrade script file. However, we encourage you **not** to alter the Avaya-provided upgrade script file. If Avaya changes the upgrade script file in the future, any changes you have made will be lost. We strongly encourage you to use the ***46xxsettings*** file to customize your settings instead.

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

Choosing the Right Application File and Upgrade Script File

The 4600 IP Telephone software Releases are bundled together in ***exe** and ***zip** files on the Avaya support Web site. See 4600 Series IP Telephone Scripts and Application Files for a detailed description. As of Release 2.0, you have four “bundles” from which to choose. Only one bundle is likely to be optimal for any one environment.

Which bundle to choose depends on the answer to two questions:

- Which version of 4610SW/4620SW software do you need in that environment?
- Are the majority of your 4602/4602SW, 4610SW, 4620, 4620SW, and 4621SW Telephones in that environment H.323-based or SIP-based?

The 4610SW, 4620SW, 4621SW, and 4622SW IP Telephones support multi-byte characters, so the software bundles come in one of three versions:

- a default version which only supports single-byte characters like those used in English, French, Japanese Katakana, etc.,
- a multi-byte version for 4610SW, 4620SW, 4621SW, and 4622SWs that support Chinese and Russian, and
- a separate multi-byte version for 4610SW, 4620SW, 4621SW, and 4622SWs that support Japanese and Russian.

If multi-byte support is not relevant to you, select the default bundle, even if you do not have any 4610SW, 4620SW, 4621SW, and 4622SW phones. Otherwise, select the software bundle that includes Chinese or Japanese, as appropriate.

Note:

All bundles include the complete software for the other, non-4610SW/4620SW/4621SW/4622SW Telephones. The software includes the 4620 IP Telephone, but not the 4630/4630SW, which remains separate. The only differences between the three bundles are the software for the 4610SW, 4620SW, 4621SW, and 4622SWs, and a slight change in the associated upgrade script file.

The 4602, 4610SW, 4620SW, and 4621SW IP Telephones can support either H.323 or SIP signaling protocols. If a majority of your 4600 Series IP Telephones are H.323-based, which is the most common situation, you can use any or all of the software bundles identified in this section. If a majority are SIP-based, select the fourth software bundle, identified as the “SIP” software bundle on the Web site. The application files in this SIP software bundle are the same as in the default bundle. The difference is a modified upgrade script file that assumes SIP is the default protocol for 4602, 4610SW, 4620SW, and 4621SW IP Telephones, and that H.323 is the exception.

When you have a mixture of H.323 and SIP telephones, use the **SIG** system value to ensure that each telephone type has appropriate software downloaded. The **SIG** system value has three legal values:

- the default value “**0**” which indicates “use the default protocol,”
- “**1**” meaning “use H.323”, and
- “**2**” meaning “use SIP.”

You decide the meaning of “the default protocol.” If the majority of your IP telephones are H.323-based, that should be the default. Otherwise, SIP is the default.

The SIG system value cannot be set in the 46xxsettings file or in the upgrade script file. SIG can only be set on a phone-by-phone basis. Instead of manually setting SIG yourself, first instruct the installers of the non-default phones to perform the SIGnaling Protocol Identifier procedure in Chapter 3 of the *4600 Series IP Telephone Installation Guide*. For example, if yours is a largely H.323 environment, when SIP phones are installed the SIG system value should be set to “**2**”. If yours is a largely SIP environment, when H.323 phones are installed the SIG system value should be set to “**1**”.

Detailed information about SIP is available in the SIP-related documentation, provided elsewhere on the Avaya support Web site.

Note:

As indicated above, although the SIG system value is a Release 2.0 feature, the 4601 IP Telephone supports SIG functionality, even though the 4601 currently supports only Release 1.8 software.

Contents of the Upgrade Script

This is a sample upgrade script file:

Note:

The filenames following the **SET APPNAME** command in this sample are examples only and may not match those used in production.

```
####################################
#Copyright Avaya 2005              #
#All rights reserved               #
####################################
#check bootApp version             #
####################################
IF $MODEL4 SEQ 4602 goto BOOTAPP4602
IF $MODEL4 SEQ 4606 goto BOOTAPP46XX
IF $MODEL4 SEQ 4612 goto BOOTAPP46XX
IF $MODEL4 SEQ 4620 goto BOOTAPP4620
IF $MODEL4 SEQ 4624 goto BOOTAPP46XX
goto END

# BOOTAPP4602
IF $BOOTNAME SEQ bb4602r1_61.bin goto DEF46XX
SET APPNAME bb4602r1_61.bin
goto END

# BOOTAPP4620
IF $BOOTNAME SEQ 4620COMMON.V1719 goto DEF46XX
SET APPNAME bbla20_1719.bin
goto END

# BOOTAPP46XX
IF $BOOTNAME SEQ 46XXCOMMON.V36 goto DEF46XX
IF $BOOTNAME SEQ 46XXCOMMON.V52 goto DEF46XX
IF $BOOTNAME SEQ 46XXCOMMON.V69 goto DEF46XX
SET APPNAME bbla0_69.bin
goto END

################################
#download definity bigApp      #
################################

# DEF46xx
IF $MODEL4 SEQ 4602 goto DEF4602
IF $MODEL4 SEQ 4606 goto DEF4606
```

```
IF $MODEL4 SEQ 4612 goto DEF4624
IF $MODEL4 SEQ 4620 goto DEF4620

IF $MODEL4 SEQ 4624 goto DEF4624
goto END

#definity bigApp for 4602 model
# DEF4602
SET APPNAME ap4602r1_61.bin
goto END

#definity bigApp for 4606 model
# DEF4606
SET APPNAME def06r1_73.bin
goto END

#definity bigApp for 4620 model
# DEF4620
SET APPNAME def20r1_73.bin
goto END

#definity bigApp for 4612 & 4624 model
# DEF4624
SET APPNAME def24r1_73.bin
goto END

# END

#####################################

#download the 46xx Settings script #

#####################################

GET 46xxsettings.scr
GET 46xxsettings.txt
```

Contents of the Settings File

Check the last lines of the Upgrade Script file example in the previous section. They show that after checking the application software, the 4600 Series IP Telephone looks for a 46xx settings file. This optional file is under your control and is where you can identify non-default option settings, application-specific parameters, etc. The Avaya support Web site has a template for this file for downloading. An example of what the file could look like follows.

Note:

The following is intended only as an example. Your settings will vary from the settings shown. This sample assumes specification of a DNS Server, parameters for the 4630/4630SW Directory application, and a 4620 Web Browser. See Administering Options for the 4600 Series IP Telephones on page 80, for details about specific values. You need only specify settings that vary from defaults, although specifying defaults is harmless.

DNSSRVR=”dnsexample.yourco.com”

DIRSRVR=”123,123,123,123”
DIRTOPDN=”yourco”

WMLHOME=”http://support.avaya.com/elmodocs2/avayaip/4620/home.wml”
WEBPROXY=”11.11.11.11”

The GROUP System Value

You might have different communities of end users, all of which have the same model telephone, but which require different administered settings. For example, you might want to restrict Call Center agents from being able to Logoff, which might be an essential capability for “hot-desking” associates.

As of Release 2.0, the simplest way to separate groups of users is to associate each of them with a number. You then edit the 46xxsettings file so each group is assigned the appropriate settings. Use the GROUP system value for this purpose. The GROUP system value **cannot** be set in the 46xxsettings file. The GROUP System value can only be set on a phone-by-phone basis. To do so, first identify which phones 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 would be assigned as Group 0.

Then, at each non-default phone, instruct the installer or end-user to invoke the GROUP Local (dialpad) Administrative procedure as specified in the *4600 Series IP Telephone Installation Guide* and specify which GROUP number to use. Once the GROUP assignments are in place, edit the settings file to allow each telephone of the appropriate group to download its proper settings.

For example, the settings file might look like:

```
IF $GROUP SEQ 1 goto CALLCENTER
IF $GROUP SEQ 2 goto HOTDESK
{specify settings unique to Group 0}
goto END

# CALLCENTER
{specify settings unique to Group 1}
goto END

# HOTDESK
{specify settings unique to Group 2}

# END
{specify settings common to all Groups}
```

QoS

The 4600 Series IP Telephones support both IEEE 802.1D/Q and DiffServ. In the future, the 4600 Series IP Telephones might support other, possibly proprietary, procedures for implementing Quality of Service. In addition, other network-based QoS initiatives such as UDP port selection do not require support by the telephones. Those initiatives nonetheless can contribute to improved QoS for the entire network.

IEEE 802.1D and 802.1Q

IEEE's 802.1Q standard defines a tag that can be added to voice and data packets. Most of the information associated with this tag deals with Virtual LAN (VLAN) management, but 3 bits are reserved for identifying packet priority. These 3 bits allow any one of 8 priorities to be assigned to a specific packet. As defined in the standard, the 8 priorities are, from highest to lowest:

- 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 mission-critical data applications
- 3: Traffic meriting "extra-effort" by the network for prompt delivery, for example, executives' e-mail
- 2: Reserved for future use
- 0: Traffic meriting the network's "best-effort" for prompt delivery. This is the default priority.
- 1: Background traffic such as bulk data transfers and backups

Note:

Priority 0 is a higher priority than Priority 1.

To support IEEE 802.1D/Q, the 4600 Series IP Telephones can be administered either of two ways:

- from the network by appropriate administration of the DHCP or TFTP/HTTP servers, or
- at the telephone itself using dialpad input.

Specific implementation details for local administration are in the *Installation Guide.* This chapter covers remote administration in 4600 Series IP Telephone Scripts and Application Files on page 67. In summary, five IEEE 802.ID/Q QoS parameters in the telephones can be administered. These parameters are:

- **L2Q:** setting the 802.1Q framing parameter (1=ON, 2=OFF, or 0=AUTO. The default is 0.) You can manually set a specific 4600 IP Telephone's L2Q value to any value other than AUTO, for example to ON or OFF. However, the telephone uses that manual value rather than any value administered via the DHCP or TFTP/HTTP settings file. To use the **QoS** Local Administrative Option to set L2Q manually see the *4600 Series IP Telephone Installation Guide.*
- **L2QVLAN:** setting the VLAN ID on which the telephone should operate. For example, what VLAN ID to use for DHCP Discovery, etc. (up to 4 digits, from 0 to 4094, default is 0).
- **VLANTEST:** setting the number of seconds to wait for a DHCPOFFER when using a non--zero VLAN ID (up to 3 digits, from 0 to 999, default is 60).
- **L2QAUD:** setting the 802.1Q audio priority value (between 0 and 7, default is 6)
- **L2QSIG:** setting the 802.1Q signaling priority value (between 0 and 7, default is 6)

In the *4600 Series IP Telephone Installation Guide*, the Local Administrative Option for specifying ADDResses also allows you to specify VLAN IDs and VLANTEST values. See also VLAN Considerations on page 79. The Local Administrative Option to specify QoS values allows you to specify values for L2Q, L2QAUD, and L2QSIG.

The 4600 Series IP Telephones can simultaneously support receipt of packets using, or not using, 802.1Q parameters.

DIFFSERV

IETF RFCs 2474 and 2475 define "services" basically as different ways to treat a network's different traffic subsets at the Internet Protocol (IP) layer, Layer 3. For example, some packets might be routed to expedite delivery and minimize delay, with other packets routed to minimize loss or cost. Redefining an octet in the Layer 3 headers for IP versions 4, or IPv4 and 6, or IPv6 provides the differentiation between these services (Differentiated Services). IPv4 calls this octet a Type of Service (TOS) octet while IPv6 calls this octet a Traffic Class. In both cases, the octet is interpreted differently than it was originally defined. With Differentiated Services, bits 0 through 5 of the octet identify a Differentiated Services Code Point (DSCP). The DSCP identifies a procedure to be used to handle that packet on a per-hop basis. Bits 6 and 7 of the octet are currently unused, and DSCP-compliant routers ignore them.

With DiffServ, the default DSCP is all zeroes, and represents “no special handling.” RFC 2474 also defines eight “Class Selector Codepoints,” which are the eight DSCP encodings that can be represented by ***xxx*000,** where “***x***” represents one bit. These Code Selector Codepoints are considered prioritized, with the larger numeric values having a higher relative order. DSCP-compliant routers should give the associated packets of larger-valued DSCPs a “probability of timely forwarding” greater than a packet with a lower-valued DSCP. In addition to the eight Class Selector Codepoints, a network can define its own DSCPs by defining encodings that do not terminate in 000. The specific treatment intended by these custom DSCPs will not necessarily be carried out by routers outside the customer’s own network.

The *4600 Series IP Telephone Installation Guide* describes the Local Administrative Option for QoS. This option allows you to specify Diffserv values for Layer 3 audio (“L3QAUD”) and signaling traffic (“L3QSIG”) on a phone-by-phone basis.

The Avaya IP Telephones’ DiffServ values change to the values administered on the media server as soon as the phone registers. For more information, see the document titled *Administration for Network Connectivity* (555-233-504). Unless there is a specific need in your enterprise LAN, we do not recommend you change the default values.

UDP Port Selection

Some data networks include equipment that can perform UDP port selection. This is a mechanism that gives packets with port numbers in a given range priority over packets with port numbers outside that range.

To support UDP port selection, the 4600 Series IP Telephones can be administered from the Avaya Communication Manager Network Region form. Locate specific implementation details for local administration of MCPORT in the *4600 Series IP Telephone Installation Guide*. For Avaya Communication Manager administration, find implementation details in *Administration for Network Connectivity for Avaya Communication Manager Software*. In summary, the system value MCPORT represents the port on the TN2302AP board. Use this port number to administer routers, etc. supporting UDP port selection, to maximize priority of voice packets being exchanged between the PBX and the telephone.

The default value for **MCPORT** is 1719. Administer the switch to use a port within the proper range for the specific LAN, and the IP telephone(s) will copy that port. A related parameter is **PORTAUD**, which is the RTP port used by the switch. If no UDP port range is administered on the switch, the IP telephone uses an even-numbered port, randomly selected from the interval 4000 to 10000.

Network Audio Quality Display on 4600 Series IP Telephones

With the exceptions of the 4601, 4606, 4612, 4624, and 4690 IP Telephones, all Series 4600 IP Telephones are by default administered to allow the end user an opportunity to monitor network audio performance while on a call. The user guides for each phone provide specific detail on getting to the appropriate screen, what the end user sees, and what the information means.

For 4610SW/4620/4620SW/4621SW/4622SW/4625SW/4630/4630SW IP Telephones, these parameters display in real-time to users on the appropriate screens, while on a call:

Table 5: Parameters in Real-Time

Parameter	Possible Values
Audio Connection Present?	***Yes*** if a receive RTP stream was established. ***No*** if a receive RTP stream was **not** established.
Received Audio Coding	***G.711***, ***G.726A***, or ***G.729***.
Silence Suppression	***Yes*** if the telephone knows the far-end has silence suppression Enabled. ***No*** if the telephone knows the far-end has silence suppression Disabled, or the telephone does not know either way.
Packet Loss	No data or a decimal 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 delay in received audio packets, and includes any look-ahead delay associated with the codec.
One-way Network Delay	No data or an integer number of milliseconds. The number is one-half the value RTCP 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 telephone's jitter buffer.

For 4602/4602SW IP Telephones, the Network Audio Quality Screen gives the user a qualitative assessment of the current overall audio quality. This assessment is based on separate evaluations of:

- the Packet Loss, and
- the total Network Delay, which is the sum of Packetization Delay, One-way Network Delay, and Network Jitter Compensation Delay, and
- consideration of the codec in use.

You can disable the Network Audio Quality data and assessment display for all sets by setting the system value **NTWKAUDIO** to a value of “0.” Administering Options for the 4600 Series IP Telephones on page 80 explains how to do so.

This information’s implication for LAN administration depends, of course, on the values the user reports and the specific nature of your LAN, like topology, loading, QoS administration, etc. This information’s major use is to give the user an idea of how network conditions affect the current call’s audio quality. It is assumed you have more detailed tools available for troubleshooting the LAN.

RSVP and RTCP

Avaya IP Telephones implement the Resource ReSerVation Protocol (RSVP) to support WAN bandwidth management. RSVP is administered from the media server. Avaya IP Telephones implement the RTP Control Protocol (RTCP) so Avaya’s Voice over IP (VoIP) Monitoring Manager (VMON) software can provide real-time monitoring and historical data of audio quality for VoIP calls.

Resource ReSerVation Protocol (RSVP) is an IETF-standard protocol hosts use to request resource reservations throughout a network. RSVP-compliant hosts send messages through a network to receivers. Receivers respond with messages requesting a type of service and an amount of resources, for example, bandwidth, to carry out that service. The host is responsible for *admitting* (approving) or *rejecting* (denying) the request. In a QoS context, RSVP tries to reserve bandwidth on the network for voice calls on a call-by-call basis. If insufficient bandwidth is available for the target voice quality, a request to use network bandwidth for a voice call is rejected.

RTP Control Protocol (RTCP), as its name implies, is a protocol that provides control functions for Real-time Transport Protocol (RTP). RTP provides end-to-end network services for real-time data such as Voice over IP. But RTP does not provide a reservation function, nor does it guarantee any level of QoS. RTCP supplements RTP by monitoring the quality of the RTP services and can provide real-time information to users of an RTP service. In a QoS context, RTCP is valuable to identify information such as:

- packet loss,
- 1-way delay or how long a packet has to go from source A to destination B,
- jitter, etc.

RTCP itself does not improve QoS, but provides information to help identify where problem areas might be.

You cannot change the telephone’s RSVP or RTCP parameters directly on the telephone or by TFTP or DHCP administration. The only way to change these parameters is by appropriate switch administration. See your Avaya media server administration material for more detail.

VLAN Considerations

If your LAN environment does not include Virtual LANs (VLANs), ignore this section. Otherwise, this section contains information on how to administer 4600 Series IP Telephones to minimize registration time and maximize performance in a VLAN environment.

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’s Ethernet switch automatically insert the switch port’s default VLAN without changing the frame’s user priority (cf. IEEE 802.1D and 802.1Q).

However, you might not want the default VLAN to be used for voice traffic. For example, you might have administered a VLAN specifically for IP telephony. You need to ensure that the switch configuration allows frames tagged by the 4600 Series IP Telephone through without overwriting or removing them. In addition, you want to set the system value **L2QVLAN** to the ***VLAN ID appropriate for your voice LAN***.

Another system value you can administer as of Release 1.8 software, is **VLANTEST**. VLANTEST defines the number of seconds the 4600 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 fairly long, allowing for the scenario that a major power interruption is causing the phones to restart. Always allow time for network routers, the DHCP/TFTP 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 re-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 Chapter 3 of the *4600 Series IP Telephone Installation Guide*.

The telephone ignores any VLAN ID administered on the media server if a non-zero VLAN ID is administered either:

- manually,
- through DHCP, and/or
- through TFTP or HTTP.

Administering Options for the 4600 Series IP Telephones

This chapter's Introduction indicates that there are many parameters you can administer for the 4600 Series IP Telephones. This section explains how to change parameters by means of the DHCP or TFTP/HTTP servers. In all cases, you are setting a system parameter in the telephone to a desired value. Table 6 lists the parameter names, their default values, the valid ranges for those values, and a description of each one. For DHCP, the DHCP Option sets these parameters to the desired values as discussed in DHCP Generic Setup on page 50. For TFTP and HTTP, the parameters in Table 6 are set to desired values in the Script File, as discussed in Contents of the Upgrade Script on page 71.

We recommend that you administer options on the 4600 Series 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 example, for a 4630 with all applications administered.

You might choose to completely disable the capability to enter or change option settings from the dialpad, as of Release 1.8. As of that Release, a new system value, PROCPSWD, can be set as part of standard DHCP/TFTP administration. If PROCPSWD is non-null and consists of 1 to 7 digits, the user cannot invoke any "dialpad options" without first pressing **Mute** or **Hold** and entering the PROCPSWD value. See "Chapter 3" of the *4600 Series IP Telephone Installation Guide* for more information.

CAUTION:

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

Administering this password can limit access to all local procedures, including V I E W, which is read-only and would not change any settings in any case.

Table 6: 4600 Series IP Telephone Customizable System Parameters

Parameter Name	Default Value	Description and Value Range
AGCHAND	1	Automatic Gain Control status for handset (0=disabled, 1=enabled).
AGCHEAD	1	Automatic Gain Control status for headset (0=disabled, 1=enabled).
AGCSPKR	1	Automatic Gain Control status for Speaker (0=disabled, 1=enabled).

1 of 4

Table 6: 4600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
AUTH	0	Script file authentication value (0=HTTP is acceptable, 1=HTTPS is required).
CNAPORT	8888	Avaya Converged Network Analyzer (CNA) server registration transport-layer port number (0-65535).
CNASRVR	“AvayaCNAserver”	Text string containing the IP Addresses of one or more Avaya Converged Network Analyzer (CNA) servers, in dotted decimal or DNS format.
CTISTAT	1	Computer-Telephony Integration (CTI) Status (1=enabled, 0=disabled).
CTIUDPPORT	49721	CTI UDP listener port (49714 through 49721, inclusive).
DHCPSTD	0	DHCP Standard flag. If set to “1” the telephone strictly follows the DHCP standard with respect to giving up IP Addresses when the DHCP lease expires. If set to “0” the telephone continues using the IP Address until it detects reset or a conflict (see DHCP Generic Setup).
DNSSRVR	" " (Null)	Text string containing the IP Address of one or more DNS servers, at least one of which must be a valid, non-zero, dotted decimal address.
DOMAIN	" " (Null)	Text string containing the domain name to be used when DNS names in system values are resolved into IP Addresses.
ENHDIALSTAT	1	Enhanced Dialing Status. If set to “1” the Enhanced Local Dialing feature is turned on for all associated applications. If set to “0” the feature is turned off.
IRSTAT	1	Text string containing status of Infrared interface (0=off/disabled, 1=on/enabled).
L2Q	0	802.1Q framing value (0=auto, 1=on, 2=off).
L2QAUD	6	Layer 2 audio priority value (0 to 7).
L2QSIG	6	Layer 2 audio priority value (0 to 7).
L2QVLAN	" " (Null)	802.1Q VLAN IDentifier (1 to 4094).
MCPORT	1719	Media server transport-layer port number (0-65535).
NTWKAUDIO	0	Network Audio Quality Assessment Display (1=on, 0=off).

2 of 4

Table 6: 4600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
OPSTAT	111	Options status flags. Consists of 3 “bits” of the form *abc*, where each letter represents a 0 (disabled/off) or 1 (enabled/on). The first bit, *a*, controls the setting for all options not controlled by the second or third bits. The second bit, *b*, controls the setting for view-oriented options (for example, the 4620’s *View IP Settings* option), if applicable. The third bit, *c*, controls the setting for the LOGOFF option, if applicable.
PHNCC	1	Telephone country code. The administered international country code for the location of the serving MultiVantage™ server. Range: 1-3 digits, from “1” to “999”.
PHNDPLENGTH	5	Telephone dial plan length. The length of the administered dial plan for the serving MultiVantage™ server. Range: 1 or 2 digits, from “3” to “10”.
PHNIC	011	Telephone international access code. The digits dialed to access public network international trunks from the serving Multi-Vantage™ server. Range: 1-4 digits.
PHNLD	1	Telephone long distance access code. The digit dialed to access public network long distance trunks from the serving MultiVantage™ server. Range: 1 digit or " " (Null).
PHNLDLENGTH	10	Length of national telephone number. The number of digits in the longest possible national telephone number for the serving Avaya media server’s location. Range: 1 or 2 digits, from “5” to “15”.
PHNOL	9	Outside line access code. The character(s) dialed to access public network local trunks from the serving Avaya media server. Range: 0-2 dialable characters, including " " (Null).
PHY1STAT	1	Ethernet line interface setting (1=auto, 2=10Mbps half-duplex, 3=10Mbps full-duplex, 4=100Mbps half-duplex, 5=100Mbps full-duplex).
PHY2STAT	1	Secondary Ethernet interface setting (0=Secondary Ethernet interface off/disabled, 1=auto, 2=10Mbps half-duplex, 3=10Mbps full-duplex, 4=100Mbps half-duplex, 5=100Mbps full-duplex).

3 of 4

Table 6: 4600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
PROCPSWD	" " (Null)	Text string containing the local (dialpad) procedure password (Null or 1-7 ASCII digits).
PROCSTAT	0	Local (dialpad) Administrative Options status (0=all Administrative Options are allowed, 1=only VIEW is allowed).
RTCPMON	" " (Null)	Text string containing the 4-octet IP Address of the RTCP monitor currently in use.
SNMPADD	" " (Null)	Text string containing one or more allowable source IP Addresses for SNMP queries, in dotted decimal or DNS format, separated by commas, with up to 127 total ASCII characters
SNMPSTRING	public	Text string containing the SNMP community string (up to 32 ASCII characters).
STATIC	0	Static programming override flag. If set to “0” static programming never overrides file server- (DHCP or TFTP) or call server-administered data. If set to “1” static programming overrides only file server-administered data. If set to “2” static programming overrides only call server-administered data. If set to “3” static programming overrides both file server- and call server -administered data.
TLSSRVR	" " (Null)	Text string containing the IP Addresses of one of more Avaya HTTPS servers, in dotted decimal or DNS format.
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”).

4 of 4

Note:

Table 6 applies to all 4600 Series IP Telephones. The 4630/4630SW and 4620/4620SW/4621SW/4622SW/4625SW IP Telephones have additional, optional administration. See Customizing the 4630/4630SW IP Telephone on page 87 and Customizing 4610SW, 4620/4620SW, 4621SW, 4622SW, and 4625SW IP Telephones on page 92 for more information.

DNS Addressing

As of Release 1.5, the 4600 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 50 for information. At least one address in Option 6 must be a valid, non-zero, dotted decimal address, otherwise, DNS fails. The system parameter **DOMAIN's** (Option 15, Table 6) text string is appended to the address(es) in Option 6 before the telephone attempts to resolve the DNS address. 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 TFTP or HTTP script file. But first **SET** the **DNSSRVR** and **DOMAIN** values so you can use those names later in the script.

Note:

If you administer Options 6 and 15 appropriately with DNS servers and Domain names respectively, you do not need to specify **MCIPADD** and **TFTPSRVR** settings in the Site Specific Option string.

Customizing the Site-Specific Option Number (SSON)

DHCP Generic Setup on page 50, discusses that the SSON can be set to a string. For each system parameter listed in Table 6 that you want to include, append the SSON string with:

a comma followed by ***name=value***
where ***name*** is a parameter name and ***value*** is its associated value. Invalid values cause the data to be ignored for that name. Customizing the SSON affects all telephones associated with that DHCP server.

Entering Options Using the Telephone Dialpad

The *4600 Series IP Telephone Installation Guide's* Chapter 3 details how to use the local administrative options.

To customize any or all of the QoS parameters locally, follow the "QoS Option Setting" procedure. You can find that procedure in Chapter 3 of the *4600 Series IP Telephone Installation Guide*.

To enable or disable the secondary Ethernet hub locally, follow the "Secondary Ethernet (Hub) Interface Enable/Disable" procedure. That procedure also appears in Chapter 3 of the *4600 Series IP Telephone Installation Guide*.

To view the 4600 IP Telephone system parameters, see The View Administration Option on page 111.

Enhanced Local Dialing

The 4610SW, 4620/4620SW, 4621SW, 4622SW, 4625SW, and 4630/4630SW have a variety of telephony-related applications (e.g., Speed Dial, Call Log, Web Browser, etc.). These applications might obtain a telephone number during operation. For example, the Call Log saves an incoming caller's number, while the Web browser might obtain a dialable link from a corporate Web site. Before Release 1.8 software, when the user indicated a desire to call one of these incoming numbers, the 4610SW/4620/4620SW/4630/4630SW would first require the user to edit the number, generally by prepending digits to account for dial access codes, country codes if applicable, etc.

As of Release 1.8, the 4610SW/4620/4620SW/4630/4630SW can evaluate a raw telephone number. This is also true of the 4621SW, 4622SW, and 4625SW as of Release 2.2. Based on administered parameters, the phone can automatically prepend the correct digits, saving the user time and effort. This is the "Enhanced Dialing" feature. The key to this feature's success is accurate administration of several important values. Table 8 summarizes these values and their meanings. That information is expanded upon in this section.

Note:

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

In all cases, the digits the phones insert and dial are subject to standard Avaya media server features and administration. This includes Class of Service (COS), Class of Restriction (COR), Automatic Route Selection (ARS), etc.

As indicated in Table 6, you can administer the system parameter **ENHDIALSTAT** to turn off the Enhanced Local Dialing feature.

The system values relevant to the Enhanced Dialing Feature are:

- **PHNCC -** the media server's international country code.
  For example, "1" for the United States, "44" for the United Kingdom, etc.
- **PHNDPLENGTH -** the length of the dial plan on the media server.
- **PHNIC -** the digits the media 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 media server.
- **PHNLDLENGTH -** the maximum length, in digits, of the national telephone number for the country in which the Avaya media server is located.
- **PHNOL -** the character(s) dialed to access public network local trunks on the media server.

Example: A corporate voice network has a 4-digit dialing plan. The corporate WML Web site lists a 4-digit phone number as a link on the Human Resources page. A 4620 user selects that link. The 4620 deduces the phone number is part of the corporate network because the phone number's length is the same as the corporate dialing plan. The phone dials the number without further processing.

Example: A user notes a Web site contains an international phone number that needs to be called, and presses "Call." The 4630/4630SW determines the number to be called is from another country code. The phone then prepends the rest of the phone number with PHNOL to get an outside line + PHNIC to get an international trunk. The 4630/4630SW then dials normally, with the Avaya media server routing the call appropriately.

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 8. The algorithm also assumes that international telephone numbers are identified as such in, for example, WML Web sites. This is indicated by preceding that type of number with a plus (+) sign, and a space or some non-digit character following the country code.

Customizing the 4630/4630SW IP Telephone

The 4630/4630SW IP Telephone has some unique and powerful capabilities that take advantage of its large display and access to LAN facilities. If your LAN has an LDAP-compliant directory, or if you have a corporate Web site suitable for the 4630's/4630SW's 1/4-VGA display, the telephone needs key information about the servers providing those facilities. Specifically, to administer the 4630/4630SW Telephone for the LDAP Directory application or the Web Access application, you must provide the information Table 7 calls for. You must provide this information in a customized script file, in accordance with 4600 Series IP Telephone Scripts and Application Files on page 67.

CAUTION:

For the 4630/4630SW to work properly, you must have a 46xxsettings.scr or 46xxsettings.txt file in the same directory as the 4630/4630SW application file. If you do not edit the 46xxsettings file, the 4630/4630SW uses default settings only. The 46xxsettings file is no longer part of the *.zip file on the Avaya software download Web site, but is available as a stand-alone download. If you already have such a file because you downloaded it for a previous 4630 release, installing the stand-alone file overwrites the original file.

Note:

The 4620 and the 4630/4630SW IP Telephones use the same ***46xxsettings*** file.

In Table 7, parameters shown with a *Mandatory* status must be accurate and non-null for the application to work. The Avaya Help Web site, however, is always available. Parameters with an **Optional** status may be changed to suit your environment. If you do not change the parameters, their defaults are used.

Table 7: 4630/4630SW IP Telephone Customizable System Parameters by Application

Parameter Name	Default Value	Status	Description and Value Range
Phone Application Parameters:			
PHNEMERGNUM	" " (Null)	Optional	Text string of a phone number to be dialed in case of an emergency (e.g., 911)
Directory Application Parameters:			
DIRSRVR	" " (Null)	Mandatory	Text string of dotted decimal IP Address, or DNS name, of the server containing the LDAP directory.
DIRTOPDN	" " (Null)	Mandatory	“Directory Topmost Distinguished Name.” Text string of the LDAP directory’s root entry. Note that spaces and other special characters might need to be treated as specified in RFC 2253, *Lightweight Directory Access Protocol (v3); UTF-8 String Representation of Distinguished Names.*
DIRFULLNAME	cn	Optional	Text string for the database field’s customer-specific label.
DIRTELNUM	telephoneNumber	Optional	Text string for the customer-specific label for the database field containing telephone numbers. The default is the standard LDAP value.
DIRSRCHTIME	0	Optional	Text string for an integer number of seconds. This is the maximum duration the LDAP directory spends searching before reporting completion or failure of the search. The default is LDAP-standard for “unlimited duration.”
DIRLDAPPORT	389	Optional	Directory LDAP Port. The port that exchanges LDAP messages with the server.

1 of 2

Table 7: 4630/4630SW IP Telephone Customizable System Parameters by Application (continued)

Parameter Name	Default Value	Status	Description and Value Range
Stock Ticker Application Parameters:			
STKSTAT	1	Optional	Text string identifying whether the phones are allowed to have the Stock Ticker Application. “1” is the default and “0” disables the Stock Ticker Application.
Voice Mail Application Parameters:			
VMLHOME	" " (Null)	Mandatory	Text string containing the URL of the home page for the Voice Mail Application.
Web Access Application Parameters:			
WEBHOME	" " (Null)	Mandatory	Text string containing the URL of the home page for the Web Access application.
WEBPROXY	" " (Null)	Optional	Text string containing the IP Address, in dotted decimal or DNS format, of an HTTP proxy server. This parameter is optional if the all the Web pages the user accesses are on your organization’s intranet.
WEBEXCEPT	" " (Null)	Optional	Text string containing a list of one or more HTTP proxy server exception domains. Separate each exception with commas, and use up to a total of 127 ASCII characters. This parameter is optional if all the Web pages the user accesses are on your organization’s intranet. If WEBPROXY is null, the value of this parameter is ignored.
WEBPORT	80	Optional	Text string containing the TCP port number for the HTTP proxy server. The default is the TCP default for HTTP. This parameter is optional if all the Web pages the user accesses are on your organization’s intranet. If WEBPROXY is null, the value of this parameter is ignored.

2 of 2

Note:

For assistance in developing local Web sites tailored to the 4630 IP Telephone’s display, see Appendix B: Creating Web Sites for the 4630/4630SW IP Telephone.

4630/4630SW Backup/Restore

4630/4630SW users can create an FTP backup file for Speed Dial button labels and unique option or parameter settings. The associated Option is covered in Chapter 8 of the *4630/4630SW IP Telephone User Guide*. Data is saved in a file called **4630data.txt** on a user-specified server and in a user-specified directory. Unlike the 4620/4620SW settings indicated in Table 8, the 4630/4630SW FTP settings cannot be centrally administered.

In addition to Speed Dial labels and associated phone numbers, a backup saves these options and non-password parameters:

Setting/Parameter Name	Type
Idle Timeout	Option
Keyboard Layout	Option
Click Feedback	Option
Edit Dialing	Option
Personalized Ring	Option
Redial	Option
Go to Phone on Incoming Calls	Option
Go to Phone on Originate	Option
Call Timer	Option
Alphabetize Entries?	Option
Call Log Active?	Option
Call Log Automatic Archive	Option
Directory User ID	Parameter
Automatic Backup	Option
FTP Server IP Address	Parameter
FTP Directory Path	Parameter
FTP User ID	Parameter
Stock Ticker Active?	Option
STK.*mm*	Parameter
Stock Index DJIA	Option
Stock Index S&P 500	Option
Stock Index Nasdaq	Option
Stock Change	Option
Stock Volume	Option

If the Automatic Backup option is set to **No**, Speed Dial data, Options and Parameter settings are not saved. However, the user can force a one-time backup via the appropriate option. See Chapter 8 of the *4630 IP Telephone User Guide* for information. Restoring backed-up data is a separate user option, also covered in Chapter 8 of the *4630 IP Telephone User Guide.*

Note:

For specific error messages relating to Backup/Restore, see Table 13: Possible Error Messages During 4610SW, 4620/4620SW, 4621SW, 4622SW, 4625SW, and 4630/4630SW Backup/Restore on page 118.

Call Log Archive

Automatic archiving of the Call Log occurs when:

- The Call Log Automatic Archive option setting is **Yes,** and
- The Call Log is more than 50% filled with unarchived entries. Or, when a new (unarchived) log entry occurs within two hours of the last archive (whichever occurs first).

Call Log Archive automatically saves applicable Call Log entries. When the Call Log Automatic Archive option on a 4630/4630SW IP Telephone is set to **Yes** and the FTPSRVR is specified, the **FTP APPE** command attempts to save all call log contents to the FTP server. The FTP Server is the FTPSRVR value in the FTPDIR directory path. The file **4630calllog.txt** saves the data. The System Administrator can optionally specify **FTPSRVR** and/or **FTPDIR** by network administration. However, the phone's user can also specify these values. Chapter 8 of the *4630/4630SW IP Telephone User Guide* covers user specification. Automatic backup occurs whenever the user executes a **Save** command on a Speed Dial or Options/Parameter screen.

Note:

For specific error messages relating to Archiving, see Table 13: Possible Error Messages During 4610SW, 4620/4620SW, 4621SW, 4622SW, 4625SW, and 4630/4630SW Backup/Restore on page 118.

Customizing 4610SW, 4620/4620SW, 4621SW, 4622SW, and 4625SW IP Telephones

The 4610SW/4620/4620SW/4621SW/4622SW/4625SW IP Telephones have some unique and powerful capabilities that take advantage of their display and access to LAN facilities. If your LAN has an LDAP-compliant directory or a WML Web site, the telephone needs key information about the servers providing those facilities. Specifically, you need to provide the information relevant sections of Table 8 call for. You must provide this information in a customized script file, in accordance with 4600 Series IP Telephone Scripts and Application Files on page 67.

CAUTION:

For a 4610SW, 4620/4620SW, 4621SW, 4622SW, or 4625SW to work properly, you must have a 46xxsettings.txt file in the same directory as the 4610SW/4620/4620SW/4621SW/4622SW/4625SW application file. If you do not edit the 46xxsettings.txt file, those telephones use default settings only. The 46xxsettings file is no longer part of the *zip file on the Avaya software download Web site, but is available as a stand-alone download. If you already have such a file because you downloaded it for a previous 4610SW, 4620/4620SW, 4621SW, 4622SW, or 4625SW IP Telephone release, installing the stand-alone file overwrites the original file.

Note:

The 4610SW/4620/4620SW and the 4630/4630SW IP Telephones use the same ***46xxsettings.txt*** file.

In Table 8, parameters shown with a **Mandatory** status must be accurate and non-null for the application to work. You can change parameters with an **Optional** status to suit your environment. If you do not change parameters, their defaults are used.

Table 8: 4610SW, 4620/4620SW, 4621SW, 4622SW, and 4625SW IP Telephone Customizable System Parameters

Parameter Name	Default Value	Status	Description and Value Range
General User Parameters:			
APPSTAT	1	Optional	Applications status flag. See The Application Status Flag (APPSTAT) on page 95 for a description. See Table 9 for the range of values.
FTPDIR	" " (Null)	Optional	FTP Server Directory. The path on the FTP server to the directory in which an FTP backup/restore is saved.
FTPUSERSTAT	1	Optional	FTP User Permission. If set to “0” the user **cannot** specify alternatives to the FTP servers and FTP directories DHCP and/or TFTP/HTTP administration specify. If set to “1” the user **can** specify alternatives to the FTP servers and FTP directories that DHCP and/or TFTP/HTTP administration specify. If set to “2” the user **cannot** specify alternatives to the FTP servers that DHCP and/or TFTP/HTTP administration specify, but **can** specify alternatives to FTP Directories.
SYSLANG	English	Optional, and can be user-specified	Language of the 4610SW/4620/4620SW user interface, in ASCII, independent of the MultiVantage™ message language. Options are English, Deutsche, Espanol, Francais, Italiano, Nederlands, Portugues and Katakana (Japanese). In addition to these languages, the 4610SW/4620SW also support Chinese, Japanese, and Russian.

1 of 3

Table 8: 4610SW, 4620/4620SW, 4621SW, 4622SW, and 4625SW IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Status	Description and Value Range
Web Access Application Parameters:			
SUBSCRIBELIST	" " (Null)	Optional	Subscription list for potential pushed content. List of zero or more fully qualified URLs, separated by commas without intervening spaces, with up to 255 total characters. See, Appendix E: The Push Feature.
TPSLIST	" " (Null)	Optional	List of Trusted Push Servers. List of zero or more fully qualified domain/ path strings, separated by commas without intervening spaces, with up to 255 total characters. See Appendix E: The Push Feature.
WMLHOME	" " (Null)	Mandatory	Text string containing the URL of the home page for the Web Access application.
WMLPROXY	" " (Null)	Optional	Text string containing the IP Address, in dotted decimal or DNS format, of an HTTP proxy server. This parameter is optional if the Web pages a user accesses are all on your organization's intranet.
WMLEXCEPT	" " (Null)	Optional	Text string containing a list of one or more HTTP proxy server exception domains, separated by commas, up to a total of 127 ASCII characters. This parameter is optional if the Web pages to be accessed by the user are all on your organization's intranet. If WMLPROXY is null, the value of this parameter is ignored.
WMLPORT	80	Optional	Text string containing the TCP port number for the HTTP proxy server. The default is the TCP default for HTTP. This parameter is optional if the Web pages to be accessed by the user are all on your organization's intranet. If WMLPROXY is null, the value of this parameter is ignored.

2 of 3

Table 8: 4610SW, 4620/4620SW, 4621SW, 4622SW, and 4625SW IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Status	Description and Value Range
Backup/Restore Parameters			
FTPSRVR	" " (Null)	Mandatory but can be user-specified	Text string containing the 4-octet IP Address for the FTP server that stores and retrieves 4610SW/4620/4620SW/ 4621SW/4622SW/4625SW user information. See The Application Status Flag (APPSTAT) on page 95.
Backlight Parameters - 4621SW, 4622SW, and 4625SW only			
BAKLIGHTOFF	120	Optional	Number of idle minutes after which the backlight turns off (1-3 ASCII digits, from 0-999).

Note:

Appendix C: Creating Web Sites for Other 4600 Series IP Telephones provides assistance in developing local Web sites tailored to the 4610SW/4620/4620SW IP Telephone's display.

The Application Status Flag (APPSTAT)

The 4610SW, 4620/4620SW, 4621SW, 4622SW, and 4625SW IP Telephones offer the user numerous applications like Speed Dial, Call Log, Redial, etc. Each of these applications allows the user to add, delete, or in some cases, edit entries. However, you as the administrator may not want the user to have that level of functionality. For example, a hotel lobby telephone probably should not allow a user to delete the concierge's Speed Dial number. Further, for privacy reasons, that same telephone should not allow a Call Log display. You can use the Application Status Flag, APPSTAT, to administer specific application functionality permission levels for one or more telephones.

APPSTAT consists of one number, specifying a certain level of allowed functionality. A Zero ("0") value is the most limiting setting. Values "2" and "3" allow increasing levels of functionality, and "1" allows the user complete application functionality.

Table 9: Application Status Flags and Their Meaning

APPSTAT Value	Meaning
0	Redial and Call Log are suppressed. Speed Dial changes are not allowed.
1	***All administered applications are displayed, with full functionality. This is the default value.***
2	Call Log is suppressed. Speed Dial changes are not allowed. Only one-number Redial is allowed.
3	Speed Dial changes are not allowed.

In Table 9, “suppressed” applications are not displayed to the user. Softkey labels, application tabs, etc. that would usually be labeled or displayed to indicate the presence of that application are not labeled or displayed. Options associated with suppressed applications can continue to display unless overridden by appropriate OPSTAT parameter administration. However, displayed options have no effect while the application is suppressed.

In Table 9, “Speed Dial changes are not allowed” means the Speed Dial application displays and the user can make calls as normal. However, any controls that allow the user to change any aspect of the Speed Dial application do not display. This restriction includes the ability to add, delete, or edit any Speed Dial name or number.

In Table 9, “Only one-number Redial is allowed” means the user Option that allows a choice between displaying one, three, or six of the last numbers dialed, depending on the telephone, is suppressed. The Redial buffer stores only one number. The Redial application does not display since the user can redial only one number. This restriction allows a certain measure of privacy once a given user has left the telephone.

Note that you can:

- set **APPSTAT** to **1**, for example, in a staging area,
- administer a given telephone with Speed Dial entries of your choice, like the **Concierge Speed Dial** button in an earlier example,
- then move the telephone to where it will be used, where you have administered APPSTAT to be, say, 0 (zero).

When the relocated telephone resets, it retains its Speed Dial entries, like Concierge, but does not allow the user to create new entries.

When you set APPSTAT to any valid value other than 1, the telephone does not accept any Speed Dial button label changes that might have been made directly on an FTP backup file. Only the telephone’s existing labels are used. This restriction prevents circumvention of the APPSTAT restrictions.

APPSTAT has no effect on telephones having no user-selectable applications such as the 4602. Also, to “suppress” the WML applications, all you have to do is not administer the appropriate parameters. In essence, these applications are suppressed by default.

Backup/Restore for 4610SW, 4620/4620SW, 4621SW, 4622SW and 4625SW IP Telephones

Backup/Restore automatically saves a phone's Speed Dial button labels and options/parameter settings, including local Feature button labels. When the Automatic Backup option on a 4610SW, 4620/4620SW, 4621SW, 4622SW, or 4625SW IP Telephone is set to **Yes** and **FTPSRVR** is specified, the **FTPST0R** command attempts to save all Speed Dial contents, all system options, and non-password parameters to the FTP server specified by **FTPSRVR**.

Data is saved in a text file called ***ext*_4610data.txt** or ***ext*_4620data.txt**, as appropriate to the telephone type, where ***ext*** stands for the telephone extension. The 4621SW, 4622SW, and 4625SW all use "4620" as the telephone type for purposes of the Backup/Restore filename, to allow seamless upgrades from 4620s if applicable.

The system administrator can optionally set the backup option and specify **FTPSRVR** through network administration. A phone user can also specify these values, as covered in Chapter 6 of the appropriate User Guide for the telephone type. Automatic backup occurs whenever the user executes a **Save** command on a Speed Dial or Options/Parameter screen.

Note:

Users can specify alternate servers and directories, for example, their own PCs, for backups and retrievals.

The 4610SW/4620/4620SW/4621SW/4622SW/4625SW backup/restore file can contain ASCII, Extended ASCII, and non-ASCII characters. However, if the file contains non-ASCII characters, specifically Cyrillic, Hebrew, Katakana, Han, or Hiragana characters, the file must be stored in UTF-8 form. The 4610SW/4620/4620SW/4621SW/4622SW/4625SW creates a file in this form automatically. But if you opt to create a backup/restore file yourself or edit this file, you must do both of the following:

1. Insert a blank line at the beginning of the file, and
2. Save the file in UTF-8 format.

These precautions ensure that regardless of how your editor stores the data file, the telephone can read the contents. If you fail to insert the blank line, the first line of data might be ignored. The 4620 and 4625SW do not support display of Cyrillic, Hebrew, Han, or Hiragana characters. Even the 4610SW/4620SW/4621SW/4622SW cannot support all Han or Hiragana characters. If you insert a character that the 4610SW/4620SW/4621SW/4622SW does not support, the display shows that character as a rectangle.

In addition to Speed Dial labels and associated phone numbers, the following options, settings and non-password parameters are saved during a backup:

Setting/Parameter Name	Type
Personalized Ring	Option
Redial	Option
Phone Screen on Answer	Option
Phone Screen on Calling	Option
Call Timer	Option
Message Display Rate	Option
Call Appearance Width	Option (4620/4620SW only)
Visual Alerting	Option
Call Log Enable	Option
Contrast	Option
Display Language	Option
Automatic Backup	Option
FTP Server IP Address	Parameter
FTP Directory Path	Parameter
FTP User Name	Parameter

Note:

When the Options Status Flag, **OPSTAT**, is set to **0,** retrieving backed up data has no effect. This prevents a user from bypassing the administration of OPSTAT and changing options settings in the backup file. Table 8 includes OPSTAT values.

Chapter 5: Troubleshooting Guidelines

Introduction

This chapter describes problems that might occur during 4600 Series IP Telephone operation and possible ways of resolving these problems.

Error Conditions

Table 10: Some Error Conditions in Operation of 4600 Series IP Telephones identifies some of the possible operational problems that might be encountered after successful 4600 Series IP Telephone installation. Possible installation problems and how to conduct a telephone self-test are discussed in the *4600 Series IP Telephone Installation Guide's* "Troubleshooting" chapter. The following User Guides also contain guidance for users having problems with specific IP telephone applications:

- *4601 IP Telephone User Guide*,
- *4602/4602SW IP Telephone User Guide*,
- *4610SW IP Telephone User Guide,*
- *4620/4620SW/4621SW IP Telephone User Guide,*
- *4622SW IP Telephone User Guide*,
- *4625SW IP Telephone User Guide*, and
- *4630/4630SW IP Telephone User Guide*

Note:

Most of the problems reported by 4600 Series IP Telephone users are not likely to be problems with the telephone itself. Problems are more likely LAN-based, where Quality of Service, server administration, and other issues can impact end-user perception of IP telephone performance.

Table 10: Some Error Conditions in Operation of 4600 Series IP Telephones

Condition		Cause/Resolution
The telephone continually reboots, or reboots continuously about every 15 minutes.		**CAUSE:** The telephone cannot find the call server. **RESOLUTION:** Ensure that MCIPADD is administered either manually or through DHCP, TFTP, or HTTP, as appropriate. **CAUSE:** This might be a firmware fault because the MAC address in memory is corrupted. **RESOLUTION:** Return the telephone to Avaya for repair.
The message light on the telephone turns on and off intermittently, but the telephone never registers.		**CAUSE:** This is a hardware fault. **RESOLUTION:** The telephone must be returned to Avaya for repair.
The telephone stops working in the middle of a call,	**AND** no lights are lit on the phone and the display is not lit.	**CAUSE:** Loss of power. **RESOLUTION:** Check the connections between the telephone, the power supply, and the power jack. For example, verify that either static addressing was not used or that any changes to static addresses were entered correctly.
	AND power to the telephone is fine (and the telephone might have gone through the restarting sequence).	**CAUSE:** Loss of path to Avaya media server, DHCP Lease expired, or DHCP server not available when telephone attempts to renegotiate DHCP lease. **RESOLUTION:** As above. Note that if the telephone is attached to a 30A switched hub, upon loss of Ethernet connectivity, the usual `No Ethernet` message is not displayed.

1 of 6

Table 10: Some Error Conditions in Operation of 4600 Series IP Telephones (continued)

Condition		Cause/Resolution
The telephone was working, but does not work now,	**AND** no lights are lit on the phone and the display is not lit.	**CAUSE:** Loss of power. **RESOLUTION:** Check the connections between the telephone, the power supply, and the power jack.
	AND power to the telephone is fine, but there is no dial tone. The display might show "System Busy."	**CAUSE:** Loss of communication with the PBX switch. **RESOLUTION:** Check LAN continuity from the PBX to the telephone using ARP or trace-route and from the telephone to the PBX by invoking a Feature button. Verify that LAN administration has not changed for the Gatekeeper, TN 2302AP boards, or the LAN equipment (routers, servers, etc.) between the switch and the telephone. Verify no one changed the telephone settings locally using the **VIEW** and **ADDR** codes, as described in the *4600 Series IP Telephone Installation Guide*. Verify the telephone volume is set high enough. Finally, conduct a self-test.
	AND the telephone was recently moved.	**CAUSE:** Loss of communication with the PBX. **RESOLUTION:** As above, but pay particular attention to the possibility that the telephone is being routed to a different DHCP server, or even a different PBX switch. If so, the new server or switch might need to be administered to support the telephone.
	AND the network was recently changed to upgrade or replace servers, re-administer the Avaya media server, add or change NAT, etc.	**CAUSE:** Loss of communication with the PBX. **RESOLUTION:** As above.

2 of 6

Table 10: Some Error Conditions in Operation of 4600 Series IP Telephones (continued)

Condition		Cause/Resolution
The telephone works, but the audio quality is poor, specifically:		
	the user hears echo when speaking on a handset.	**CAUSE:** Echo from digital-to-analog conversion on your Avaya media server trunk. **RESOLUTION:** Verify which trunk is causing the echo, and swap the trunk's Trunk Termination parameter on the PBX.
	the user hears echo on a headset, but not on a handset.	**CAUSE:** Improper headset adapter. **RESOLUTION:** Replace adapter with Avaya's M12LU or 3412-HIC adapters. We recommend the M12LU, since it supports Automatic Gain Control.
	the user is on Speaker and hears no echo, but the far-end hears echo.	**CAUSE:** Room acoustics. **RESOLUTION:** Ensure that there are six inches or so of blank space to the right of the telephone. If that is insufficient, use the handset.
	the user experiences sudden silences such as gaps in speech, or static, clipped or garbled speech, etc.	**CAUSE:** Jitter, delay, dropped packets, etc. **RESOLUTION:** One or more Quality of Service (QoS) features should be implemented in the network. See Chapter 3 of the *4600 Series IP Telephone Installation Guide*. **CAUSE:** Improper non-Category 5 wiring. **RESOLUTION:** Replace non-Category 5 wiring with Category 5 wiring.
The 4612 or 4624 IP Telephone works properly except the phone does not ring.		**CAUSE:** The Ringer Off (**RngOF**) softkey feature has been activated. **RESOLUTION:** Use the softkey **Menu** option to access the **RngOF** feature. A downward-pointing triangle means the Ringer is off. Ensure that the triangle points up. Also, check the Volume setting on the telephone. Finally, do a self-test on the telephone.

3 of 6

Table 10: Some Error Conditions in Operation of 4600 Series IP Telephones (continued)

Condition	Cause/Resolution
The telephone works properly except for the Speaker.	**CAUSE:** The Speaker was turned off on the PBX. **RESOLUTION:** Administer the PBX to allow that station's Speaker to operate. If that does not work, do a Self-test on the telephone.
The telephone works properly, except incoming DTMF tones are not received.	**CAUSE:** The TN2302AP board does not pass in-band DTMF tones. **RESOLUTION:** None; the board is operating as designed.
The telephone works properly, except sidetone DTMF is not heard.	**CAUSE:** PBX suppresses sidetone DTMF. **RESOLUTION:** On PBX administration, on the Change-System-Parameters screen, enable On-Hook Dialing. If the user has Hands-Free Answer (HFA), answers a call using the Speaker and switches to the handset, pressing dialpad buttons does not send DTMF tones. This is a known bug, and the only current resolution is to disable HFA.
Hands-Free Answer (HFA) is administered but the telephone did not automatically answer a call.	**CAUSE:** HFA only works if the telephone is idle. A second call is ignored if it comes in while a call is in progress, including ringing before the first call is answered. **RESOLUTION:** None.
The TFTP application terminates and asks for registration.	**CAUSE:** Non-Avaya shareware or freeware TFTP applications often cease operating to request registration. **RESOLUTION:** *Short-term:* Restart the application. *Long-term:* Register the product or replace it with an application that does not behave this way, for example, Avaya's TFTP application.
The TFTP or HTTP script file and settings file are ignored (not being used by the telephone)	**CAUSE:** The system value AUTH is set to 1 (HTTPS required) but no valid address is specified in TLSSRVR. **RESOLUTION:** Change AUTH to 0 (zero), or enter a valid address for TLSSRVR.

Table 10: Some Error Conditions in Operation of 4600 Series IP Telephones (continued)

Condition		Cause/Resolution
The TFTP or HTTP script file is ignored or not used by the telephone	**AND** the TFTP or HTTP server is a LINUX or UNIX system.	**CAUSE:** The telephone expects lines of the script file to terminate with a **<Carriage Return> <Line Feed>**. Some UNIX applications only terminate lines with **<Line Feed>**. Editing the script file with a UNIX-based editor can strip **<Carriage Return>**s from the file. Doing so causes the entire file to be treated as a comment, and thus be ignored. **RESOLUTION:** Edit the script file with a Windows®-based editor, or another editor that does not strip out the **<Carriage Return>**. **CAUSE:** UNIX and LINUX systems use case-sensitive addressing and file labels. **RESOLUTION:** Verify the file names and path in the script file are accurately specified.
	AND telephone administration recently changed.	**CAUSE:** The ***46xxupgrade.scr*** file was mis-edited, renamed, etc. **RESOLUTION:** Download a clean copy of the ***46xxupgrade.scr*** file from the Avaya support Web site, and do not edit or rename it. Customize or change *only* the ***46xxsettings*** file, as discussed in Chapter 4: Server Administration.
Telephone power is interrupted while the telephone is saving the application file **and** the TFTP or HTTP application stops responding.		**CAUSE:** The TFTP or HTTP server stops responding if power is interrupted while a telephone is saving the application file. **RESOLUTION:** Restart the TFTP or HTTP server, as applicable.
The DHCP server indicates the 4600 Series IP Telephone reports itself as a Token Ring device, and refuses to provide the telephone an address.		**CAUSE:** Early versions of the 4600 Series IP Telephones erroneously report being a Token Ring device. With most DHCP servers, this does not matter. Some LINUX servers, however, refuse to issue addresses to Ethernet devices reporting to be Token Ring devices. **RESOLUTION:** Administer the DHCP server to delete all MAC and IP Addresses associated with Lucent Technologies or Avaya, or allow the associated DHCP leases to expire.

5 of 6

Table 10: Some Error Conditions in Operation of 4600 Series IP Telephones (continued)

Condition		Cause/Resolution
The user indicates a 4610SW/4620/4620SW/ 4621SW/4622SW/4625SW-specific or 4630/4630SW-specific application is not accessible.		**CAUSE:** The ***46xxsettings*** script file is not pointed to accurately, or is not properly administered to allow the application. **RESOLUTION:** Assuming the user is meant to have that application, verify the 46xxsettings script file is properly specified for your system, including case if your file server is UNIX or LINUX, and extension. Then, verify all the relevant parameters indicated in Table 7 and Table 8, are accurately specified in the 46xxsettings file.
PHY2STAT was set using the INT local procedure as specified in the *4600 Series IP Telephone Installation Guide*.	**BUT** the 4610SW, 4620/4620SW, 4621SW, 4622SW, 4625SW uses the original setting instead of using the new setting following a reboot.	**CAUSE:** The telephone's FTP Backup/ Restore feature is enabled. The user specified a setting file for the **PC Ethernet Interface** setting through the Options menu. The user-specified setting is overriding the Local Procedure PHY2STAT setting. **RESOLUTION:** Use the Options menu to change the setting to the value you want, so the INT local procedure is not necessary. Alternatively, use the Options menu to change the **PC Ethernet Interface** setting to **Auto-negotiation**. Then make all future changes using the INT local procedure.

6 of 6

There are three areas where installers can troubleshoot problems before seeking assistance from the system or LAN administrator:

1. Check the power and Ethernet wiring to ensure that:
   - all components are plugged in correctly.
   - there is LAN connectivity in both directions to all servers - DHCP, TFTP, HTTP, media server. Note that if the telephone is attached to a 30A switched hub, upon loss of Ethernet connectivity the usual `No Ethernet` message is not displayed.
   - If the telephone is supposed to be powered from the LAN, ensure that the LAN is properly administered and is compliant with IEEE 802.3af-2003.
2. If you are using static addressing:
   - Use the **`VIEW`** command to find the names of the files being used and verify that these filenames match those on the TFTP server. Check on the Avaya Web site to verify whether the correct files are being used. Note that the 4601 IP Telephone does not support static addressing and therefore, does not support the **`VIEW`** command.
   - Use the **`ADDR`** option to verify IP Addresses.
   - Use the **`QoS`** option to verify QoS parameters.

     See Chapter 3 of the *4600 Series IP Telephone Installation Guide*.
3. If the 4600 Series IP Telephone is not communicating with the DHCP, TFTP, HTTP, or media server, make a note of the last message displayed. Consult the system administrator.

The Clear Administrative Option

Sometimes, you might want to remove *all* administered values, user-specified data, and option settings, etc. Essentially, you want to return a telephone to its initial “clean slate” condition. Usually, this is done to pass a telephone to a new, dedicated user when the user’s L O G O F F option is not sufficient. For example, if the new user has the same extension, but has different permissions than the previous user. The C L E A R option erases all administered data such as:

- static programming,
- file server and call server programming, and
- user settings, including Speed Dial button labels and locally programmed Feature button labels.

C L E A R then restores all such data to default values. The C L E A R option does not affect the software load itself, so if you have upgraded the telephone, the phone retains the latest software. Once a telephone is Cleared, you can administer it normally.

CAUTION:

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

Note:

Only telephones with Release 2.1 or later software support the CLEAR Administrative Option.

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

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

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

   Note:

   Press the **Mute** button momentarily. Do not press this button while pressing other keys/buttons. The 4630/4630SW IP Telephones and the 4690 IP Conference Telephone do not have a dedicated **Hold** button. For all other 4600 Series IP Telephones, pressing the **Hold** button instead of the **Mute** button also works.

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

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

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

   A screen displays the following prompt on the top line:

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

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

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

   ```
   Clearing values.
   ```

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

The Reset Administrative Option

As indicated in some troubleshooting procedures, sometimes it is appropriate to reset the 4600 Series IP Telephone. Procedures on how to do so are printed in this section. You can also find reset procedures in Chapter 3 of the *4600 Series IP Telephone Installation Guide*. These parameters and settings are reset to default values, including “null” as applicable, when the Reset procedure finishes:

- Registration extension and password.
- All values administered by local procedures, in accordance with Chapter 3 of the *4600 Series IP Telephone Installation Guide*.
- All values previously downloaded using DHCP or from a TFTP settings file. These values, of course, are usually restored when the telephone re-registers after the reset.

Note:

If **PROCSTAT** was administered to **1**, as described in Chapter 4: Server Administration, you cannot invoke the **R E S E T** option. In addition, if **PROCPSWD** was administered as non null, you must enter that value after you press **Mute** and before you press **R E S E T**.

Reset System Values

Use the following procedure to reset all system initialization values to the application software default values.

CAUTION:

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

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

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

   Note:

   Press the **Mute** button momentarily. Do not press this button while pressing other keys/buttons. The 4630/4630SW IP Telephones and the 4690 IP Conference Telephone do not have a dedicated **Hold** button. For all other 4600 Series IP Telephones, pressing the **Hold** button instead of the **Mute** button also works.

The 4601 IP Telephone flashes both Message Waiting indicators 500 milliseconds on, 500 milliseconds off to indicate user input is expected. All other IP telephones display the following text left-justified at the top of the display:

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

CAUTION:

All static information is erased without any possibility of recovering the data as soon as you press the # button.

2. If you do not want to reset the system values, press ***** (no) and proceed to Step 4.

   Pressing the pound sign (#) to reset the system values on a 4601 IP Telephone produces a confirmation tone. The 4601's Message Waiting indicators illuminate but do not flash to indicate no entry is allowed while the system values are being reset. All other phones display a screen with the following prompt on the top line:

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

3. Press the ***** button to continue without resetting the values and proceed to Step 4. Or, press the # button to reset values to their defaults.

   All phones except the 4601 display the following text left-justified at the top of the display while the system values are reset to defaults:

```
Resetting
values.
```

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

4. If you do not reset the phone, all IP telephones except the 4601 display the following prompt:

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

5. Press the ***** key to terminate the procedure without restarting the telephone. Otherwise, press # and follow the next procedure to restart the telephone.

Restart the Telephone

Use the following procedure to restart the telephone.

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

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

   Note:

   Press the **Mute** button momentarily. Do not press this button while pressing other keys/buttons. The 4630/4630SW IP Telephones and the 4690 IP Conference Telephone do not have a dedicated **Hold** button. For all other 4600 Series IP Telephones, pressing the **Hold** button instead of the **Mute** button also works.

   The 4601 IP Telephone flashes both Message Waiting Indicators 500 milliseconds on, 500 milliseconds off to indicate user input is expected. All other IP telephones display the following text left-justified at the top of the display:

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

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

   Pressing the pound sign (#) to reset the system values on a 4601 IP Telephone produces a confirmation tone. The 4601's Message Waiting indicators illuminate but do not flash to indicate no entry is allowed while the system values are being reset. All other phones display the following text left-justified at the top of the display while the system values are reset to defaults:

   ```
   Resetting
   values.
   ```

   Once the system values are reset, the following prompt displays on all IP telephones, except the 4601:

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

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

   Press the # key to restart the telephone.

   The remainder of the procedure depends on the status of the boot and application files. See Appendix A of the *4600 Series IP Telephone Installation Guide*.

The View Administration Option

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

Note:

Also use the **ADDR** option to view IP Addresses covered in “Static Addressing Installation” in Chapter 3 of *4600 Series IP Telephone Installation Guide*. IP Addresses might have been entered incorrectly*. Verify whether you were provided with correct IP Addresses.*

If **PROCPSWD** is administered as indicated in Chapter 4: Server Administration, you must type the Local Procedure password after pressing **Mute**, and before pressing **V I E W**.

The 4601 IP Telephone does not support static addressing, and therefore does not support the V I E W command.

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

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

   Note:

   Press the **Mute** button momentarily. Do not press this key while pressing other keys. The 4630 IP Telephone does not have a dedicated **Hold** button. For all other 4600 Series IP Telephones, pressing the **Hold** button instead of the **Mute** button also works.

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

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

2. Press the ***** button at any time during viewing to display the next name and system value pair from Table 11. The first pair displays again after the last pair displays.

   Press the # button at any time during viewing to terminate the procedure and restore the user interface to its previous state.

   The names and values display in the order shown in Table 11.

Table 11: Parameter Values

Name	System Value	Format
Model	***46ccDccc***	Up to 8 ASCII graphics characters.
Phone SN	***ccccccccccccc cccccccc***	Phone Serial Number, up to 18 ASCII graphic characters.
PWB SN	***ccccccccccccc cccccccc***	Printed Wiring Board (circuit board) Serial Number, up to 18 ASCII graphic characters.
PWB comcode	***ccccccccc***	9 ASCII numbered characters.
MAC address	***00:60:1D:hh:hh:hh***	Each octet of the MAC address displays as a pair of hexadecimal numbers.
L2 tagging	***ccccccccc***	Up to 9 ASCII characters.
VLAN ID	***cccc***	Up to 4 ASCII characters, ID number or “none.”
IP Address	***nnn.nnn.nnn.nnn***	Up to 15 ASCII characters.
Subnet mask	***nnn.nnn.nnn.nnn***	Up to 15 ASCII characters.
Router	***nnn.nnn.nnn.nnn***	Up to 15 ASCII characters.
File server	***nnn.nnn.nnn.nnn.nnnnn***	Up to 21 ASCII characters, IP Address and port of last file server successfully used.
Call server	***nnn.nnn.nnn.nnn.nnnnn***	Up to 21 ASCII characters, IP Address and port of media server currently in use.
Group	***nnn***	Up to 3 ASCII characters.
Protocol	***cccccccc*** ***filename1.exe*** ***filename2.exe***	Up to 8 ASCII characters. Up to 16 ASCII graphic characters.

Error Messages

The 4600 Series IP Telephones issue messages in English only. The IP telephones also display messages from the switch, which outside the United States might issue messages in the local language.

Note:

Because the 4601 IP Telephone does not have a display, it is limited in its ability to provide visual feedback and error messages. Nonetheless, some feedback is available and presented as applicable. For more information, see Table 14: Possible Error Messages During 4601 IP Telephone Installation or Operation on page 119.

Table 12: Possible Error Messages During Installation or Operation of 4600 Series IP Telephones

Error Message	Cause/Resolution
During Installation	
`Bad Router`	**CAUSE:** The telephone cannot find a router based on the information in the DHCP file for GIPADD. **RESOLUTION:** Change administration on DHCP, as indicated in DHCP in Chapter 4: Server Administration.
`Checksum error`	**CAUSE:** Downloaded application file was not downloaded or saved correctly. **RESOLUTION:** The telephone automatically resets and attempts to re-initialize.
`DHCP: CONFLICT * to program`	**CAUSE:** At least one of the IP Address offered by the DHCP server conflicts with another address. **RESOLUTION:** Review DHCP server administration to identify duplicate IP Address(es)
`Discover` ***`aaa.bbb.ccc.ddd`***	**CAUSE:** The 46xx telephone is attempting to discover (and register with) the Gatekeeper at IP Address *aaa.bbb.ccc.ddd*. **RESOLUTION:** If this message appears for more than a few seconds, especially if the IP Address keeps changing, the telephone is unable to contact the Gatekeeper. Verify network connectivity between the telephone and the Gatekeeper, or revise the Gatekeeper addresses in the DHCP/script files to point to different Gatekeepers. See Administering 4600 Series IP Telephones on Avaya Media Servers, DHCP, TFTP, and HTTP.

1 of 5

Table 12: Possible Error Messages During Installation or Operation of 4600 Series IP Telephones (continued)

Error Message	Cause/Resolution
`Discovering...`	**CAUSE:** The telephone is seeking a gatekeeper on the media server, using its administered gatekeeper list. **RESOLUTION:** Wait for a valid registration to occur, or press # to interrupt the search and re-initialize manual or DHCP/script files procedures.
`File too large` `Cannot save file`	**CAUSE:** The telephone does not have sufficient room to store the downloaded file. **RESOLUTION:** Verify the proper filename is administered in the script file, and that the proper application file is located in the appropriate location on the file server.
`Gateway Error`	**CAUSE:** DEFINITY Release 8.4 does not have an H.323 station extension for this telephone. **RESOLUTION:** On the station administration screen, ensure the DCP set being aliased for this IP telephone has an H.323 station extension administered, in accordance with switch administration instructions.
`Hardware failure`	**CAUSE:** Hardware failure prevented downloading of application file, **RESOLUTION:** Replace telephone.
`IP Address in use by another`	**CAUSE:** The telephone has detected an IP Address conflict. **RESOLUTION:** Verify administration to identify duplicate IP Address(es).
`NAPT Error`	**CAUSE:** A device between the telephone and the call server is invoking Network Address Port Translation, which the 4600 Series IP Telephones do not support. **RESOLUTION:** Remove or re-administer the NAPT device or move the telephone.
`No Ethernet`	**CAUSE:** When first plugged in, the IP telephone is unable to communicate with the Ethernet. **RESOLUTION:** Verify the connection to the Ethernet jack, verify the jack is Category 5, etc. Note that if the telephone is attached to a 30A switched hub, upon loss of Ethernet connectivity, the usual “No Ethernet” message is not displayed.

2 of 5

Table 12: Possible Error Messages During Installation or Operation of 4600 Series IP Telephones (continued)

Error Message	Cause/Resolution
`No file server address`	**CAUSE:** The file server IP Address in the IP telephone's memory is all zeroes. **RESOLUTION:** Depending on the specific requirements of your network, this may not be an error. If appropriate, either administer the DHCP server with the proper address of the file server, or administer the telephone locally using the ADDR option. The *4600 Series IP Telephone Installation Guide* explains the ADDR option.
`No Socket`	**CAUSE:** The telephone has registered with the call server, but network problems have prevented the telephone from opening a TCP socket. **Note:** This message only occurs on older software versions. Telephones with newer software automatically reset. **RESOLUTION:** Investigate the network problem normally.
`System busy`	**CAUSE:** Most likely, the number of IP endpoints on the Avaya media server is already at maximum, Less likely, network resource is unavailable. **RESOLUTION:** The telephone was attempting to access a network resource (DHCP server, TFTP server, or the Avaya media server) and was not successful. Check the resource being called upon for its availability. If the resource appears operational and properly linked to the network, verify addressing is accurate and a communication path exists in both directions between the telephone and the resource.
`System Error`	**CAUSE:** The Avaya media server has an unspecified problem. **RESOLUTION:** Consult your Avaya media server administration and troubleshooting documentation.
During Registration	
`Bad Router`	**CAUSE:** The telephone cannot find a router based on the information in the DHCP file for GIPADD. **RESOLUTION:** Change administration on DHCP, as indicated in DHCP in Chapter 4: Server Administration.
`Extension error`	**CAUSE:** An invalid Avaya media server Registration extension has been entered. **RESOLUTION:** Re-enter the extension if mis-entered initially. If appropriate, verify proper extension with respect to switch administration.

Table 12: Possible Error Messages During Installation or Operation of 4600 Series IP Telephones (continued)

Error Message	Cause/Resolution
`Extension in use`	**CAUSE:** The specified extension is already in use, according to the Avaya media server. **RESOLUTION:** Wait a few minutes, and try again. Waiting works when the extension is correctly administered, but a service interruption occurs of which the Avaya media server is not yet aware. Otherwise, verify the proper extension with respect to switch administration. Alternatively, if you are logging in from a remote location and want to log the other user off, press the # key twice, once at each prompt.
`Failed to set phone IP Address`	**CAUSE:** The 4600 Series Telephone was originally installed on one switch with Static Addressing, and has subsequently been installed on another switch with an active DHCP server assigning dynamic IP Addresses. **RESOLUTION:** Reset the telephone.
`Incompatible`	**CAUSE:** This release of the Avaya media server does not support the current version of the IP telephone. **RESOLUTION:** Upgrade to the current version of Avaya media server software.
`Message light blinks on and off, and the telephone did not complete registration.`	**CAUSE:** The telephone has a hardware fault. **RESOLUTION:** Replace the telephone.
`NAPT Error`	**CAUSE:** A device between the telephone and the call server is invoking Network Address Port Translation, which the 4600 Series IP Telephones do not support. **RESOLUTION:** Contact the System Administrator to remove or re-administer the NAPT device.
`No Socket`	**CAUSE:** The telephone has registered with the call server, but network problems have prevented the telephone from opening a TCP socket. **Note:** This message only occurs on older software versions. Telephones with newer software automatically reset. **RESOLUTION:** Press the # button to reset the telephone and contact the [Network] System Administrator to report the network problem.
`Password Error`	**CAUSE:** An invalid PBX Registration password has been entered. **RESOLUTION:** Re-enter the password if entered incorrectly. If appropriate, verify proper password with respect to switch administration.

Table 12: Possible Error Messages During Installation or Operation of 4600 Series IP Telephones (continued)

Error Message	Cause/Resolution
`Resource Error`	**CAUSE:** The Avaya media server rejects the registration request. **RESOLUTION:** Verify your Avaya media server administration to ensure the telephone's proper IP Address, extension, and password are being used.
`Timeout Error`	**CAUSE:** Protocol timeout error. **RESOLUTION:** Retry. If failure continues, check network congestion, addresses, etc. to identify cause of timeout.
`Undefined Error`	**CAUSE:** An error has occurred without an identifiable cause. **RESOLUTION:** Conduct self-test, restart the telephone, and if no other cause becomes evident, replace the telephone.
`Wrong Set Type`	**CAUSE:** The Avaya media server does not recognize the set type. **RESOLUTION:** Ensure that the Avaya media server is properly administered to expect the appropriate telephones for the IP Address and extension.
During Operation	
`Discover` ***`aaa.bbb.ccc.ddd`***	**CAUSE:** The 46xx telephone is attempting to discover (and register with) the Gatekeeper at IP Address *aaa.bbb.ccc.ddd*. **RESOLUTION:** If this message appears for more than a few seconds, especially if the IP Address keeps changing, the telephone is unable to contact the Gatekeeper. Verify network connectivity between the telephone and the Gatekeeper, or revise the Gatekeeper addresses in the DHCP/script files to point to different Gatekeepers. See Administering 4600 Series IP Telephones on Avaya Media Servers, DHCP, TFTP, and HTTP.
`Discovering...`	**CAUSE:** The user is on a call when the network connection between the telephone and call server is interrupted, but the call stays connected. The telephone automatically starts procedures to register with the call server again. However, until registration succeeds, the user has no access to Avaya Communication Manager features and functionality. This message alerts users to the lack of connection to the call server. **RESOLUTION:** This is the same message, with the same implications and Resolution as the Discovering... message on page 114.

5 of 5

Table 13: Possible Error Messages During 4610SW, 4620/4620SW, 4621SW, 4622SW, 4625SW, and 4630/4630SW Backup/Restore

Error Message	Cause/Resolution
`Current options and Speed Dial entries have not yet been backed up.`	**CAUSE:** An attempt to save the current options and Speed Dial entries on the FTP server has not yet been made or is in progress. **RESOLUTION:** Wait for a message stating that backup was successful.
`The FTP Server Name is not known. Please check the FTP Server IP Address.`	**CAUSE:** Invalid or missing server name. **RESOLUTION:** Verify the FTPSRVR address is the file server to which backup data should be saved. Verify that the FTPDIR value is the correct directory path for that file server.
`The FTP Server has not yet responded, so backup has not yet succeeded.`	**CAUSE:** The FTP server has not responded to the attempt to backup/restore. **RESOLUTION:** Try again, verify the FTP server address, verify the FTP server is online, and/or verify the network connectivity.
`The FTP Server has denied access. Please check FTP Setup parameters.`	**CAUSE:** The FTP server has reported that it did not store data. **RESOLUTION:** Verify the FTP server setup parameters, as indicated on the FTP Setup Parameters screen. See “FTP Setup” in Chapter 8 of the *4630/4630SW IP Telephone User Guide, or* see “Backup/Restore Options” in Chapter 6 of the appropriate User Guide for the telephone type.
`The FTP Server was unable to store the backup file.`	**CAUSE:** The FTP server has reported that it could not store the data. **RESOLUTION:** Verify administration and available capacity/ filespace on the FTP server.

Troubleshooting the 4601 IP Telephone

This section describes specific problems that can occur during 4601 IP Telephone installation, administration or normal operation, and possible ways of resolving these problems.

In Table 14, the Error Messages shown in the first column correspond to the equivalent conditions described in “Chapter 4" of the *4600 Series IP Telephone Installation Guide* and Table 12: Possible Error Messages During Installation or Operation of 4600 Series IP Telephones. However, rather than displaying messages, the 4601 turns its LEDs on and off to indicate an error condition, as described in Table 14’s second column. In addition, not all error conditions result in unique LED indications.

Table 14: Possible Error Messages During 4601 IP Telephone Installation or Operation

Error Message	4601 Visual Indication/Cause/Resolution
`Extension Error.`	**VISUAL INDICATION:** Message Waiting indicators at top of phone and the left middle of the faceplate display a broken flutter for a total of 5 cycles (with one cycle being alternating 50 milliseconds on, 50 milliseconds off for 500 milliseconds followed by 500 milliseconds off). **CAUSE:** The PBX does not recognize the extension entered or cannot find a valid gatekeeper. **RESOLUTION:** Confirm the extension is correct and is correctly administered on the switch. Then try registration again, taking particular care to enter the extension accurately.
`Extension in Use.`	**VISUAL INDICATION:** If the extension is being used, the 4601 attempts registration. The first attempt causes the Message Waiting indicators at the top of phone and left middle of the faceplate to display a broken flutter. The broken flutter alternates 50 milliseconds on, 50 milliseconds off for 500 milliseconds, followed by 500 milliseconds off five times. Then the indicators flash continuously, awaiting user entry. Then the 4601 makes a second registration attempt using the *same* extension. This attempt causes the Message Waiting indicators at the top of phone and left middle of the faceplate to display a continuous broken flutter. The broken flutter alternates 50 milliseconds on, 50 milliseconds off for 500 milliseconds followed by 500 milliseconds off. In addition, Call Appearance Line b's LED flashes continuously until either the "*" or "#" button is pressed. **CAUSE:** The PBX detects an extension conflict with an existing set or Softphone. **RESOLUTION:** You can force the current telephone to register, and thereby disconnect the other user, by pressing #. The 4600 Series IP Telephone prompts you again for the Extension and Password. If you enter the same Extension and Password, you must confirm that you want to unregister the original user. Press **#** to unregister the original user and register the current phone. Then press ***** to reset the phone and enter a different Extension and Password. If you take no action within 20 minutes, the phone attempts registration again, repeating the process until either you intervene or power is lost.
`IP Address in use by another.`	**VISUAL INDICATION:** All LEDs are steadily lit, except Call Appearance Line A, which is flashing. **CAUSE:** The telephone has detected an IP Address conflict. **RESOLUTION:** DHCP restart is automatically initiated. No user action required.
`No Ethernet.`	**VISUAL INDICATION:** No LEDs flash when phone is plugged in. **CAUSE:** Telephone is unable to communicate with the Ethernet. **RESOLUTION:** Verify the connection to the Ethernet jack, verify the jack is Category 5, verify power is applied on the LAN to that jack, etc.

1 of 3

Table 14: Possible Error Messages During 4601 IP Telephone Installation or Operation (continued)

Error Message	4601 Visual Indication/Cause/Resolution
`Password Error.`	**VISUAL INDICATION:** Message Waiting indicators at top of phone and left middle of faceplate display a broken flutter for a total of 5 cycles (with one cycle being alternating 50 milliseconds on, 50 milliseconds off for 500 milliseconds followed by 500 milliseconds off), then flash continuously, awaiting user entry. **CAUSE:** The PBX does not recognize the password entered. **RESOLUTION:** Confirm the password is correct, then try registration again, taking particular care to enter the password accurately.
`System busy.`	**VISUAL INDICATION:** Message Waiting indicators at top of phone and left middle of faceplate display a broken flutter continuously (alternating 50 milliseconds on, 50 milliseconds off for 500 milliseconds followed by 500 milliseconds off) until either the "*****" or "#" button is pressed. **CAUSE:** Most likely, the number of IP endpoints on the PBX is already at maximum, Less likely, network resource is unavailable. **RESOLUTION:** The telephone was attempting to access the PBX and was not successful. Check the resource being called upon for availability. If the resource appears operational and properly linked to the network, verify addressing is accurate and that a two-way telephone/resource communication path exists. Press ***** to retry the process with the same values, or # to restart and enter the Extension and Password again.
`System Error.`	**VISUAL INDICATION:** Message Waiting indicators at top of phone and left middle of faceplate display a broken flutter continuously (alternating 50 milliseconds on, 50 milliseconds off for 500 milliseconds followed by 500 milliseconds off) until either the "*****" or "#" button is pressed. **CAUSE:** The PBX has an unspecified problem. **RESOLUTION:** Press ***** to retry the process using the same values or # to restart and re-enter the Extension and Password. Consult your Avaya media server administration and troubleshooting documentation.
`Undefined Error.`	**VISUAL INDICATION:** Message Waiting indicators at top of phone and left middle of faceplate display a broken flutter continuously (alternating 50 milliseconds on, 50 milliseconds off for 500 milliseconds followed by 500 milliseconds off) until either the "*****" or "#" button is pressed. **CAUSE:** The PBX has rejected registration for an unspecified reason. **RESOLUTION:** Press ***** to retry the process using the same values or # to restart and re-enter the Extension and Password. Consult your Avaya media server administration and troubleshooting documentation.

2 of 3

Table 14: Possible Error Messages During 4601 IP Telephone Installation or Operation (continued)

Error Message	4601 Visual Indication/Cause/Resolution
`Wrong Set Type.`	**VISUAL INDICATION:** Message Waiting indicators at top of phone and left middle of faceplate display a broken flutter continuously (alternating 50 milliseconds on, 50 milliseconds off for 500 milliseconds followed by 500 milliseconds off) until either the "*****" or "**#**" button is pressed. **CAUSE:** The PBX does not recognize the set type. **RESOLUTION:** Ensure the PBX is properly administered to expect the appropriate telephone for the IP Address and extension. Press ***** to retry the process using the same values or # to restart and re-enter the Extension and Password.

3 of 3

Appendix A: Avaya - 46xx IP Telephone MIB

Downloading the Avaya - 46xx IP Telephone MIB

The custom Management Information Base (MIB) is available in ***.txt*** format for free download at http://www.avaya.com/support. Follow these links:

- Under **Technical Database**, select **Telephone Devices & User Agents**.
- Then under **IP Telephones and User Agents**, select **4600 IP Telephones**.
- Then select **Programming and Administration**.

Appendix B: Creating Web Sites for the 4630/4630SW IP Telephone

Introduction

This appendix describes the capabilities and limitations of the 4630/4630SW IP Telephone's Web Browser. We also provide suggestions to help you design Web sites for viewing on the 4630/4630SW. This appendix is intended for 4630/4630SW IP Telephone Web Browser [Web page] designers, and assumes readers are familiar with HTML, Style Sheets, and ECMAScript.

This appendix serves two primary functions:

- To present technologies implemented in the 4630/4630SW IP Telephone's Web Access application, including any limitations or non-standard implementations, and
- To provide a suggested model for developing effective Web pages for Web browser viewing.

This appendix is not intended to provide technical details on setting up a Web server, nor does it provide information on Web server technologies. Finally, this document is not intended to provide an introduction to Web browser protocols or technologies.

Note:

See the Avaya Web site for a link to sites where HTML templates are available for customizing.

Any subsequent reference to the 4630 IP Telephone in this appendix applies equally to the 4630SW IP Telephone.

General Background

The 4630 IP Telephone display is a 1/4-VGA (320 pixels wide by 240 pixels high, 256 colors supported) display.

The data types and other features supported in the browser include:

- HTML 4.01
- Cascading Style Sheets (CSS), Levels 1 and 2
- Document Object Model (DOM) Level 1
- Images: GIF and JPEG
- ECMAScript (JavaScript) 1.4
- HTTP 1.0 and 1.1
- Secure Sockets Layer (SSL) 2.0 and 3.0
- Cookies stored in non-volatile memory
- Click-to-Dial Functionality

Browser Features and Behavior

This section presents technologies implemented in the 4630 IP Telephone Web Access application, along with any limitations or non-standard implementations. Style sheets are now the preferred mechanism to control Web page appearance and have made most attribute specifications with tags obsolete. Therefore, the majority of tag attributes were not tried. The attributes that were tested were those of real interest to specific tags. The browser is HTML 4.0 compliant, with a few minor differences as noted where appropriate.

Note:

The sections in this appendix show comments specific to the 4630 IP Telephone and its browser in italics.

Document Skeleton

Certain tags define the basic framework of an HTML document. Most browsers are usually good at dealing with missing tags. However, when you apply style sheets it is essential that you follow the tag structures. Even ignoring style sheets, it is considered good style to follow the HTML rules. The following tags make up the basic skeleton of an HTML document:

- <html> indicates the start of an HTML document.
- <head> indicates the start of an HTML document's header. Title, meta definitions, ECMAScript function definition, document level style sheet definition, and external style sheet inclusion are all done in the header section.
- <title> sets the title of the document. This is usually shown in the frame of the browser window. *On the phone, the title is shown in the Top Line Information Display Area.*
- <body> indicates the start of the body of an HTML document. The rest of the document is embedded between the start and end <body> tags.
- <meta> adds additional information about an HTML page. *Web walking tools usually use this tag, which is of little use in browsers, and has no effect on the phone*.

Content-Based Style

Content-based tags deal with identifying words, phrases or chunks of text, or images as having a specific meaning or context. The intent of content-based tags is not to show physically marked text. However, it is not wrong for a browser to show content-based text in a distinct style, such as font style.

Each content-based tag is shown with a brief description, and any physical effects imposed by the browser.

- <abbr> indicates an abbreviation. *Using this tag has no effect*.
- <address> indicates an address. *Using this tag has no effect*.
- <acronym> indicates an acronym. *The enclosed text is shown in an italic font*.
- <cite> indicates a bibliographic citation or reference. *The enclosed text is shown in an italic font*.
- <code> indicates source code of a program. *The enclosed text is shown in a monospaced font*.
- <del> indicates deleted text. It shows editorial markup. *A line is drawn through enclosed text.*
- <dfn> indicates a definition for a term. This is usually used with the first appearance of a term in a document. *The enclosed text is shown in an italic font.*

- indicates emphasis on a string of text. This is the contextual equivalent of using the <i> (italic) tag. *The enclosed text is shown in an italic font*.
- <ins> indicates inserted text. It shows editorial markup. *The enclosed text is shown underlined.*
- <kbd> indicates keyboard input. This is similar to the <code> tag, but with a different contextual intent. *The enclosed text is shown in a monospaced font*.
- <samp> indicates literal text. *The enclosed text is shown in a monospaced font*.
- indicates emphasis on some text, but in a stronger contextual sense than the tag. This is the contextual equivalent of using the <b> (bold) tag. *The enclosed text is shown in a bold font.*
- <var> indicates source code variables. This is similar to the <code> tag, but with a different contextual intent. *The enclosed text is shown in an italic font*.

Logical Style

Tags that control logical style provide a similar functionality to those that control content-based style, but they have no implicit visual characteristics or contextual meaning. Instead, they only provide a means of invoking a style sheet. These tags, like all others, might have an ID and class attribute set. Using style sheet rules for these class names and IDs allows the designer to provide decoration, font, and color styles for each section. Thus, these tags can be considered to be designer-defined, content-based tags:

- indicates a division. A newline is inserted between the previous text and the text following the tag. No physical changes are noticeable, except those implemented in style sheets.
- indicates a spanned section of text is placed immediately after the text that precedes the tag with a newline. No physical changes are noticeable, except those implemented in style sheets.

Physical Style

Physical tags are effectively the opposite of content-based tags. The text in a physical tag might have no meaning whatsoever, outside what the designer intended. These tags show text in a distinct style. Physical tags usually affect font style.

Each physical style tag is shown with a brief description and any physical effects the browser imposes.

- <b> indicates that the text appears in a bold font weight.
- <big> indicates that the text appears one point size larger than the current text.
- <i> indicates that the text appears in an italic font.
- <small> indicates that the text appears one point size smaller than the current text.
- <sub> indicates that the text appears as a subscript to the current text. The text is shown one point size smaller.
- <sup> indicates that the text appears as a superscript to the current text. The text is shown one point size smaller.
- <tt> indicates that the text appears as teletype text. The text is shown in a monospaced typeface font.

Physical Spacing and Layout

Physical spacing and layout tags define the basic structure of a document. Headings, paragraphs, tables and lists all provide some basic physical and logical layout to a page.

Each spacing and layout tag is shown with a brief description, and any unusual behavior is described.

- <p> indicates the start of a new paragraph. A blank line is inserted between previous text and text following the <p> tag.
-
 indicates to insert a breakpoint. A newline is inserted between previous text and text following the <br> tag.
- <pre> indicates no formatting rules apply to the text that follows. This implies that no wrapping will be applied to this text, which can result in adding a horizontal scrollbar to view the text.
- <hr> indicates that a newline and a horizontal rule line should be inserted between the previous text and text following the <hr> tag.
- <blockquote> indicates that the following text is a quote, and should be offset in some way. The embedded text is shown with newlines before and after the text, with spacing to the left and right. Within that “block” of text, normal wrapping rules apply.

- <q> indicates that the following text is a short quote, and should be shown in double-quotes (according to documentation). This text appears as normal text, with no physical identifying indications.
- <h1> - <h6> indicate heading sections. Each level is one point smaller than the previous level, with <h1> being the largest.

The section titled Maintaining Context on page 137 contains design guidelines for maintaining user context.

Lists and Tables

For presentation of data in a logical format, lists and tables are two of the more important sets of tags. Since space is at a premium in the browser, tables should be used with discretion. While they provide sets of text, which are easy for the eye to process, they can quickly become cumbersome if misused in this browser. Both width and height are limited, so the data provided in the table cells should be short pieces of text. Beyond that, the page designer should come up with a different model for presenting the data, possibly using lists and divisions.

Lists

- starts an ordered list. Provides a list with some type of numbering: upper-case letters, lower-case letters, digits, upper-case roman numerals, lower-case roman numerals. Setting the type attribute is ignored in the browser.
- starts an unordered list. Provides a list with bullets to the left of each item.
- adds an item to an ordered or unordered list.
- <dl> starts a definition list. Provides a list with two fields per list item. The first is a term and the second is the term's definition.
- <dt> adds a new definition term to a definition list.
- <dd> adds a new term definition to a definition list.

Tables

The new HTML 4.0 table tags, <thead>, <tbody> and <tfoot> are all implemented. These tags allow printed pages to have headers and footers when the table is longer than a single page. Since the 4630 IP Telephone Web Browser has no print capability, we recommend that these tags not be used.

- <table> starts a table layout.
- <caption> adds a caption to a table. The align attribute allows a caption to be placed above or below the table. This attribute has no effect in the phone.
- <tr> adds a new table row to a table.

- <th> adds a header for some column(s) of a table.
- <td> adds a piece of data for some row(s) and column(s) of a table.
- <thead> defines a set of table header rows. The intent of this tag is to provide a set of header rows for each printed page. While viewing the page in a browser, the header has no more effect than the <th> tag. What it provides for the designer is a more logical breakout of the data. The table's header area is easily recognizable, since it appears between the <thead> start and end tags.
- <tbody> defines the main body of a table, when used with the <thead> and <tfoot> tags.
- <tfoot> defines a footer for a table. This tag can contain multiple rows. Like the <thead> tag, the intent of this tag is to provide a set of footer rows for each printed page. Viewing the page in a browser has no additional effect. And like the <thead> tag, this tag provides a logical breakout of the data for the designer.
- <colgroup> defines a column group. It can be used as a single definition of identical columns or as a container for dissimilar columns. The span attribute defines what columns are parts of each group.
- <col> controls the appearance of one or more columns within a column group.

Images

The 4630 IP Telephone Web Browser handles both GIF and JPEG image formats. No other image formats, included animated GIFs, are supported. Note that images take up a large amount of memory compared to text and that updating the display can be an issue. For these reasons, we recommend keeping images to a minimum.

The image tags that can be used on the browser are:

- <img> displays an image.
- <map> display a client-side image. Client-side images have shaped regions called areas. These areas are tied to URLs or ECMAScript functions. Clicking on an area in a region executes the ECMAScript function.
- <area> defines an area in a <map> image. Each area uses the href attribute to define a URL to jump to, or an ECMAScript to execute when that area is clicked.

See the Design Guidelines on page 135 for information on displaying images.

Links

As of Release 1.8, the 4630/4630SW IP Telephones support dialing from hyperlinks. To dial from a link, a given link's href attribute value must of the form **tel:*nnnnn*** or javascript:dial('***nnnnn***'). Selecting that link passes the characters ***nnnnn*** to the 4630/4630SW Phone application for direct dialing.

Hyperlinks are the heart of the Web browser's power. The link allows the user to:

- click text or an image to jump to another Web site,
- click text or an image to jump to another page within this site, or
- click text or an image to jump to another area on a page.

Although URLs allow you to use various protocols, use only HTTP and HTTPS for the 4630 IP Telephone Web Browser.

- <a> specifies the full or relative URL for a hyperlink. When using the target attribute, never use the _blank name. With the exception of frames, the 4630 IP Telephone Web Browser is not intended to be a multi-window browser. Thus, if a page attempts to reference a new, non-frame window, the browser becomes confused and a reboot is necessary.
- <base> defines the default target to be used in all <a> tags. This is done by setting the target attribute of the <base> tag. If the target attribute is set in the <a> tag, the <base> tag value is ignored.

Using the target attribute with the Web Access Application is strongly discouraged because the application supports a single window for browsing. The use of the target attribute can cause the browser software to create a new window that is outside the Web Access Application's control.

Frames

Frames allow multiple windows to be created on the browser's base window. The browser is effectively split up into multiple areas. Each frame can be given a name or ID. Using the target attribute of the <a> tag, a Web page can be displayed in another frame.

Although frames behave as defined, the small size of the screen makes them impractical to use. Just like tables, frames take up too much room on the display. One can, though, take advantage of frames by having a small "table of contents" frame with images for links. In general, however, use of frames is strongly discouraged.

- <frameset> defines an area for a set of frames.
- <frame> defines a single frame in a frameset.
- <iframe> defines an in-line frame.

- <noframes> provides a fallback for browsers that don't handle frames. If the designer intends to use frames and make these pages available to the phone, this tag should certainly be employed.

See the Design Guidelines on page 135 for information on displaying frames.

Forms

HTML forms provide the user the ability to enter data into a Web browser. This data can then be passed to the Web server for processing. It is difficult to predict what Web designers might have in mind for the 4630 IP Telephone Web Browser. However, all forms-related tags have been verified, and the results are presented here.

- <form> defines the basic input form, and defines the action to be performed when the **Submit** button is selected, through the action attribute.
- <input> defines most user input. The type of attribute defines the type of input to use. The <button> tag was created to replace type values of button, reset and submit, in a cleaner, more flexible way. Other type values available are checkbox, hidden, image, password, radio, and text. The type value file is useless in this browser's context, since this control's intent is to allow the user to select a file on their local disk.
- <button> defines a button that the user can select. This tag behaves much like the <input type=button> tag, except the physical appearance is three-dimensional. Also, the button can display any text, image, or combination thereof.
- <fieldset> encapsulates a section of a form's contents to create a group of related form controls. The phone's browser puts a simple box around the fieldset.
- <label> associates a relationship between a form control and one or more text labels. Labels can be tied to form controls by the form attribute in the label and the id attribute in the form control. They can also be tied by embedding the form control inside the <label> tag, for example, <label>Name: <input type=text id=name></label>.
- <legend> gives a label to a <fieldset> tag. This label appears at the top of the fieldset section of the form, with a line separating the legend from the rest of the fieldset.
- <optgroup> provides nested, cascading menus to the user. This does not seem to work.
- <option> defines the values available in a <select> scrolling list or drop-down menu.
- <select> defines scrolling lists and drop-down menus.
- <textarea> provides free-form user input and display. This provides a scrolled text area for the user to read or type text.

Character Entities

As with any syntactic language, HTML has certain characters that have special meaning. The two most obvious characters are the < and > symbols, which surround all tags. These characters cannot be typed in directly if the designer's intent is to display these characters. Thus, all characters that a Web browser can display are assigned numeric values. In addition, many of these characters also are assigned names. The numeric values are entered into the source Web page as ***&#nnn;*** where ***nnn*** is some 3 digit value. For example, the < symbol is entered as '<'. Name values are entered into the source Web page as &name; where name is the name associated with this character. Again, using the < symbol, this would be entered as '<'. The browser fully supports the set of characters defined by the World Wide Web Consortium, in conformance with the standard.

Colors

The browser supports 256 colors. Colors can be specified by name, RGB percentages, or RGB raw numbers. The HTML and CSS specifications suggest 16 named colors.

The 4630 IP Telephone Web Browser recognizes these color names, which are:

- aqua
- black
- blue
- fuchsia
- gray
- green
- lime
- maroon
- navy
- purple
- red
- silver
- teal
- olive
- white
- yellow

Beyond these 16 well-known names, we recommend using RGB percentages or raw numbers to specify colors.

Fonts

Font specifications are one of the most important styles you can apply to a Web browser. Because of the 4630 IP Telephone's screen size, the browser has only a single font available for use. Font weights such as normal and bold are supported. Finer font values, such as lighter and bolder are not supported. Normal and Italic font styles are also supported. Font sizes are also supported, specified by either percentages or raw numbers. However, percentages below 50% all appear as the same size.

Although we found some problems with font specifications, fonts behave reasonably well given the screen's size and resolution. The only major problem found is the inability to specify font families.

See the Design Guidelines on page 135 for information on displaying images.

Cookies

Cookies can be a useful feature in maintaining the state of a user when interacting with a Web site. HTTP provides no state information, such as when or how often a user visits a site. Cookies allow Web sites to track this information by storing a simple set of values on the browser for the current session. Usually, browsers also provide the ability to save cookies to disk, to retain this information between sessions. However, the 4630 IP Telephone Web Browser has no such ability to save any data between sessions. Cookies do behave well within the realm of the current session, and can be used if desired. The 4630 IP Telephone has a maximum of 8Kilobytes of data available for cookie storage.

Design Guidelines

This section presents guidelines for developing a good model that effectively presents Web pages for 4630 IP Telephone Web Browser viewing. The biggest challenge in designing pages for this browser is the limited amount of space available for viewing the pages. The 4630 IP Telephone screen is a 1/4-VGA display. Part of that screen is lost to the browser by the 4630 IP Telephone's main controls. Page layout must be effective and efficient, to avoid causing more lost space through additional screen controls like scrollbars. Font sizing can make or break a page's usability. You must find a balance between fitting as much text as is possible, and allowing users to read the text without straining their eyes.

Fixed-Width Objects

One of a Web browser's primary functions is to present text wrapped at the browser window's right border. When dealing with internationalization, text would wrap at the left border. The browser always attempts to avoid adding a horizontal scrollbar. However, if you use fixed-width objects, like tables and pre-formatted (<pre> tag) text, wrapping becomes secondary to presenting the data exactly as HTML dictates.

Web browsers do not resize themselves larger when you add scrollbars. Thus, if there are more lines of text than can fit in the browser window's height, a vertical scrollbar is added. This now takes up some of the width of the browser, and less text displays on a single line. If text is wider than the browser's width, a horizontal scrollbar is added. This now takes up some of the browser's height, and fewer lines of text are displayed.

Given the small size of the browser, it is highly desirable to avoid causing scrollbars to appear. Unless the amount of text shown in a page is kept to a bare minimum, avoiding a vertical scrollbar is unlikely. However, avoiding fixed-width objects, or ensuring that the size of fixed-width is kept small, gains some viewable space. If scrolling is a requirement, vertical scrolling is usually better perceived by users than horizontal scrolling.

Images

Using images in a Web page is always a concern. For example, a page with many images can slow up downloading. While this is still a concern in the phone, an image's size has a much greater effect. Browser and phone memory is limited. Each image can use a sizable amount of memory, overwhelming the browser. Use an image only if it is essential to a page.

Images also fall into the realm of fixed-width objects. Check all images to verify that they do not cause a horizontal scrollbar to be added. Scale down a browser image by setting the width and height attributes of the <img> tag. Or instead, scale the images when setting up the Web site. Scaling images during Web site setup avoids forcing the browser to deal with the sizing. Using the width and height attributes scales the image after it is downloaded by the browser. Scaling images during setup also speeds up image downloading. Finally, reducing the size of the image reduces the amount of memory used.

Animated GIF images are a bad idea since they use up quite a bit of memory. Additionally, because of the persistence of the LCD screen, animated images tend to smear in the browser and lose their effectiveness. Therefore, animated GIFs are considered "not supported" with this phone.

Frames

While contents and document text frames provide a useful method to browse a series of pages, frames also use up real estate, just like scrollbars. Even if the frame decorations are all turned off, a frame containing the majority of the document text suffers the problems discussed in Images—the frame width is smaller, increasing the chances of adding a horizontal scrollbar. Additionally, a single text line has fewer viewable characters, and the page becomes even more difficult to read and comprehend. Using simple top and bottom page or section navigation buttons, can make up for the missing contents frame.

The interaction between frames and scrollbars is another important area of concern. While most browsers manage scrolling within each frame independently, the 4630 Web Access Application only scrolls the entire (single) window. Scrolling by window moves the user's view of the frames as a whole, but does not scroll any of the data in individual frames. Data is likely to be in frames that can never be seen.

Minimal screen real estate and scrolling issues make frames something to avoid.

Fonts

Font size is a major concern in the browser. Without designer intervention, the browser displays text as if it were running on a PC in a normal width and height display. This means that the fonts shown appear huge relative to the screen size. As a result, only seven lines of text can be viewed in the browser when no font sizing is applied. Additionally, only about 25 characters are viewable per line. From a practical point of view, this situation is not usable.

To make the browser usable, perform some form of font sizing to allow a reasonable amount of text to be viewed per screen. Ideally, put font sizing in a single external style sheet, and make all pages reference this style sheet. Do not set font sizes in document-level style sheets, or even worse, for in-line style sheets or <font> tags. Doing so makes it very difficult for the designer to update font changes, and runs the risk of failing to make a universal change. Use a single external style sheet to manage consistency in the pages.

Define fonts using a static external style sheet. You can also generate a style sheet dynamically using some form of server-side application, such as a CGI script or a Java servlet. Dynamic style sheet generation allows the server to decide, per user, what font size to use. This in turn allows the user to notify the server to change the font size. All HTML pages would have an external style sheet reference, another server-side executable. This executable dynamically generates font information based on the cookie, form component, or configuration value, relative to the phone's IP Address. Using a static external style sheet makes page development and testing much easier, since it appears the same way to both the designer and the reader. Allowing the user to choose a font size forces more work on the designer to verify that all fixed size items appear acceptably

Maintaining Context

Given the small screen area, a user can become easily lost. Headings are often not in view, and the user, if distracted by other work, can lose a sense of context. Style sheets can help maintain this sense of context through color. The and tags are intended to provide page designer-defined content-based style. By defining classes of tags with various colors and border styles, the designer provides additional information. However, a significant number of people suffer from some form of color blindness. Thus, it may be necessary to design pages both with and without using color styles.

User Interaction

As these Design Guidelines indicate, HTML forms work reasonably well in the Browser. However, due to the phone's limitations as an input device, keyboard input can be difficult. A complete keyboard is made available based on the context of mouse selection. When a text input control is on-screen, the user just clicks the input control. The keyboard appears, with the browser thrown into a small scrolling area. The input control is roughly centered in the scrolling area. The user can then press the software keys and the text is shown in the input control. Simply pressing the **Done** button dismisses the keyboard, and the input control shows the newly typed text. While this interaction technically works fine, it can be difficult to type a large amount of text from a user perspective. So avoid user input unless it is absolutely necessary. When necessary, keep user input to a minimum.

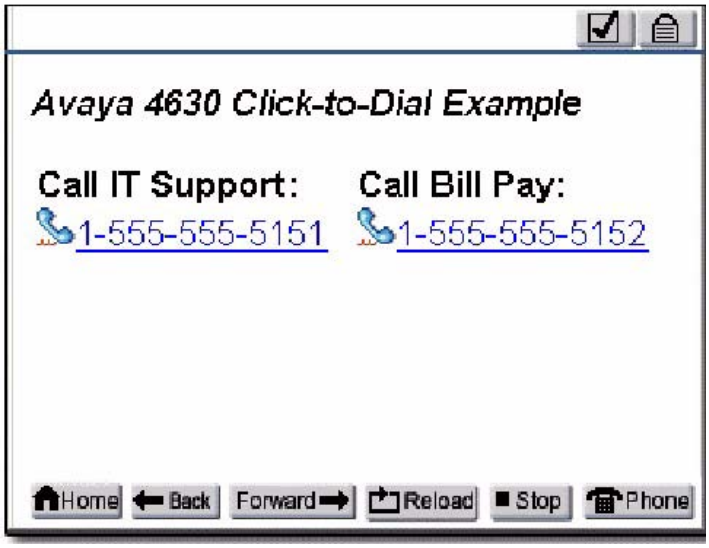
Click-to-Dial Functionality

Embedded as **`<a href="javascript:dial('nnnn')">`** ***nnnn*** is passed to the Phone application to initiate a phone call.

Example:

```
<html><head>
<body>
<table border="0" width="100%">
     <tr>
     <td>
          <b>Call IT Technical Support:</b><br>
          <a href="javascript:dial('1-555-555-5151')">
          <img border="0" src="call.gif">1-555-555-5151
          </a>
     </td>
     <tr>
     <td>
          <b>Call Bill Pay:</b><br>
          <a href="javascript:dial('1-555-555-5152')">
          <img border="0" src="call.gif">1-555-555-5152
          </a>
     <td>
     <tr>
</table>
</body></html>
```

The generated code is rendered as this Web page:



Appendix C: Creating Web Sites for Other 4600 Series IP Telephones

Introduction

A Web browser is available for Web application development in these 4600 Series IP Telephones:

- 4610SW
- 4620/4620SW
- 4621SW
- 4622SW
- 4625SW

See the *4600 Series IP Telephones Application Programmer Interface (API) Guide*, available on the Avaya support Web site (http://www.avaya.com/support) for detailed information about Web browser requirements, characteristics, and functionality. That guide also provides suggestions to help design Web sites for viewing on applicable IP telephones.

Appendix D: Administering Thin Client Directories

Introduction

If you have a corporate database that supports the Lightweight Directory Access Protocol (LDAP), Avaya's Thin Client Directory application can communicate with that database. IP telephone users can then use their phones to search for names, telephone numbers, or other information. Using search results, users can call a person directly, store a number on a Speed Dial button, and view more details about the person.

The Thin Client Directory application applies only to these IP telephone types:

- 4610SW
- 4620/4620SW
- 4621SW
- 4622SW
- 4625SW

See the *4600 Series IP Telephones Application Programmer Interface (API) Guide*, available on the Avaya support Web site (http://www.avaya.com/support) for detailed information about installing and administering Avaya's Thin Client Directory application.

Appendix E: The Push Feature

Introduction

Release 2.1 of the 4600 Series IP Telephones provides support for a feature called “Push,” which applies to the 4610SW, 4620, and 4620SW Telephones. Release 2.2 introduces additional IP telephones, the 4621SW, the 4622SW, and the 4625SW, to which the Push feature also applies. Push gives the System Administrator the capability to use WML protocol to:

- send *content* to a telephone without first receiving a user request, and
- potentially override what the user is otherwise experiencing.

You can send pushed content to a single phone, a group of phones, or the entire enterprise.

Push Content

Three types of content can be pushed, with one of two types of priorities, normal and barge-in. The content types are:

- **Text Messages** on the top display line. If a pushed text message has barge-in priority, the message overwrites whatever else is currently displayed. However, other subsequent messages can, in turn, overwrite the pushed message. If the pushed text message has normal priority, it is buffered in the telephone and displayed when no higher priority message is being displayed. Up to 56 characters can be pushed to the top line in a given message.
- **WML Web pages** can be pushed to the telephone’s WML browser. If a pushed Web page has barge-in priority, the content overwrites whatever else is currently displayed to the user.

  If the push of a Web page has normal priority, the Web page does not override what the user sees. If the user has the Web application displayed, normal-priority pushed content overrides what is otherwise displayed. If the Web application is not being displayed, normal-priority pushed content loads in the background. When the user invokes the Web application, the pushed content displays, subject to certain restrictions. For this reason, you might want to accompany a Web push with a corresponding pushed text message, alerting users there is Web content to view.

- **Audio Messages** (RTP) can be pushed. Pushed audio messages can drive the telephone off-hook, if necessary and play the pushed message through the telephone's Speaker. If the audio push has barge-in priority, the audio message is presented to the user, even if the user is on a call. In this latter case, the far-end is automatically placed on Hold and does not hear the pushed audio message.

A given push can include any or all of the three content forms, but can have only one priority. You can optionally accompany each push with notification tones to draw the user's attention to the phone and to the pushed content.

Push Priorities

Barge-in pushes, as the name implies, are meant for information important to get to the user. An example of a barge-in push might be an audio message alerting users that the building is closing because of inclement weather. You can accompany that message with a Web page detailing weather conditions. There are very few circumstances that can prevent barge-in pushes from being presented to the user. Of course, network conditions can prevent actual delivery of the pushed content.

Use normal pushes for less-essential or less time-critical information. An example might be "Mary has birthday cake in her office." A normal push might or might not be presented to the user. For example, a normal audio push is not presented to a user already on a call. Or, a normal text message would not display until a higher priority message completes.

For More Information on Push

The specifications and interactions of pushed content are beyond the scope of this document. The *4600 Series IP Telephones Application Programmer Interface (API) Guide* provides detailed information about developing Push content and administering the Push feature. Find the API on the Avaya support Web site, http://www.avaya.com/support. Further information, including sample applications, is also available in a Software Developer Toolkit on the Avaya support Web site.

For more detailed assistance in developing applications, also visit the Solutions Directory on Avaya's Developer Connect Web page (www.devconnectprogram.com) and follow the *Find a Solution* link. The Directory has a list of companies you can work with to develop applications. The Solutions Directory lists all current Developer Connection Program Members, with whom you can work to develop applications, and their innovative solutions. The members in this directory have all been approved in the program and are compliance-tested to assure customer satisfaction.

Index

Numerical

4600 Series IP Telephones . . . 34
- Administering on Avaya Media Servers . . . 46
- Administering Options for . . . 80
- Administration Alternatives and Options . . . 44
- Creating Web Sites for . . . 141
- DHCP and File Servers . . . 35
- DNS Addressing . . . 84
- Dual Connection Architecture . . . 34
- Initialization Process . . . 36
- Network Audio Quality Display . . . 77
- Registration and Authentication . . . 34
- Restart . . . 110
- Scripts and Application Files . . . 67
- Single Connection Architecture . . . 34
- Software . . . 34
- WAN Considerations . . . 35

4610SW, 4620/4620SW, 4621SW, 4622SW, and 4625SW IP Telephones
- Administering Thin Client Directories for . . . 143
- Application Status Flag (APPSTAT) . . . 95
- Backup/Restore . . . 97
- Customizable System Parameters . . . 93
- Customizing . . . 92

4630/4630SW IP Telephone
- Backup/Restore . . . 90
- Call Log Archive . . . 91
- Creating Web Sites for . . . 125
- Customizable System Parameters . . . 88
- customizing . . . 87

46xx IP Telephone MIB . . . 123

A

About This Guide . . . 9
Administering 4600 Series IP Telephones on Avaya Media Servers . . . 46
Administering DHCP and File Servers . . . 47
Administering Options for the 4600 Series IP Telephones . . . 80
Administering the Thin Client Directories . . . 143
Administration Alternatives and Options for 4600 Series IP Telephones . . . 44
Application File and Upgrade Script, Choosing . . . 69
Application Files, and Scripts for 4600 Series IP Telephones . . . 67
Application Status Flag (APPSTAT) . . . 95
Application Status Flag (APPSTAT) for 4610SW, 4620/4620SW, 4621SW, 4622SW and 4625SW IP Telephones . . . 95
Applications . . . 30
Architecture
- Dual Connection . . . 34
- Single Connection . . . 34

Avaya - 46xx IP Telephone MIB . . . 123
Avaya Communication Manager Software Release 1.1 . . . 46
Avaya TFTP (Suite Pro) . . . 63

B

Backup/Restore for 4610SW, 4620/4620SW, 4621SW, 4622SW and 4625SW IP Telephones . . . 97
Backup/Restore, for 4630/4630SW . . . 90

C

Call Log Archive, for 4630/4630SW . . . 91
Choosing the Right Application File and Upgrade Script File . . . 69
Clear Administrative Option . . . 106
Click-to-Dial Functionality . . . 138
Configuration and Installation, Suggestions for . . . 31
Conventions Used in This Guide . . . 14
Creating Web Sites for Other 4600 Series IP Telephones . . . 141
Creating Web Sites for the 4630/4630SW IP Telephone . . . 125
- Browser Features and Behavior . . . 126
- Click-to-Dial Functionality . . . 138
- Design Guidelines . . . 135
- General Background . . . 126

Customer Support . . . 20
Customizing
- 4610SW, 4620/4620SW, 4621SW, 4622SW and 4625SW IP Telephones . . . 92
- 4630/4630SW IP Telephone . . . 87
- Site-Specific Option Number (SSON) . . . 84
- System Parameters for 4610SW/4620/4620SW,4621SW, 4622SW, and 4625SW IP Telephones . . . 93
- System Parameters for 4630/4630SW IP Telephones . . . 88

D

DEFINITY Releases 9, 9.5, and 10 46
Delay and Jitter 22
DHCP and File Server Administration 47
DHCP and File Servers 35
DHCP and VoIP 23
DHCP Configuration, Choosing 49
DHCP Generic Setup 50
DHCP Server 35
DHCP Server Setup 49
DHCP Server, Windows 2000 Setup 58
DHCP Server, Windows NT 4.0 Setup. 53
DHCP Software Alternatives 49
DNS Addressing 84
Document Change History 11
Document Organization 10
Dual Connection Architecture 34

E

Enhanced Dialing Procedures 85
Enhanced Local Dialing 85
Error Conditions 99
Error Messages 113

F

File Servers 35
File Servers and DHCP Administration 47

G

GROUP System Value 73

H

H.323 Standard 23
Hardware Requirements 39
HTTP 24, 66
HTTP Generic Setup 66

I

IETF Documents 18
Initialization and Address Resolution 29
Initialization Process, for 4600 Series IP Telephones . 36
Installation and Configuration, Suggestions for 31
Installation, Network Information Required before installing 48
Intended Audience 9
IP Address Lists and Station Number Portability . . . 32
ISO/IEC, ANSI/IEEE Documents 20
ITU Documents. 19

M

Media Server Field Names and Corresponding Script File Parameter Names 64
MIB, for 46XX IP Telephones 123

N

NAT 24
Network Assessment and VoIP 26
Network Audio Quality Display, on 4600 Series IP Telephones 77
Network Information
Required 48
Required Before Installation 48
Network Protocols 21

O

Online Documentation 15
Options, entering using the Telephone Dialpad 84
Options, for 4600 Series IP Telephone Administration. 44

P

Port Utilization, TCP/UDP 27
Push Content 145
Push Priorities 146
Push, More Information on 146

Q

QoS 25, 74
DIFFSERV 75
IEEE 802.1D and 802.1Q 74
RSVP and RTCP 78
UDP Port Selection 76
QoS and VoIP 25
QoS, and 4600 Series IP Telephones 74

R

Registration and Authentication, of 4600 Series IP Telephones 34
Related Documents. 15
Release 2.2, What's New in 12
Reliability and Performance 31
Requirements 39
Hardware 39
Software 41

Reset Administrative Option 108
Restart the Telephone 110
RSVP and RTCP 78

S

S8300 Media Server, as TFTP Server 63
Script File Parameter Names and Corresponding Media Server Field Names 64
Scripts and Application Files, for 4600 Series IP Telephones 67
Security 33
Settings File, Contents of 73
SIGnaling Protocol Identifier procedure 70
Signaling, Audio and Management 28
Single Connection Architecture 34
Site-Specific Option Number, customizing 84
SNMP and VoIP 25
Software Alternatives, for DHCP 49
Software Checklist 47
Software Requirements 41
Software, for 4600 Series IP Telephones 34
System Values, Resetting 111

T

Tandem Coding 22
TCP/UDP Port Utilization 27
Terms Used in This Guide 12
TFTP 23, 62
TFTP (Suite Pro), Avaya 63
TFTP and VoIP 23
TFTP Generic Setup 62
TFTP Server on S8300 Media Server 63
TFTP Server Setup 62
Thin Client Directories, Administering the 143
Troubleshooting
  Parameter Values 112
  the 4601 IP Telephone 118
Troubleshooting Guidelines 99

U

UDP/TCP Port Utilization 27
Upgrade Script and Application File, Choosing the Right 69
Upgrade Script, contents of 71

V

View Administrative Option 111
VLAN Considerations 79
Voice over IP. See VoIP 21
VoIP 21
  Delay and Jitter 22
  DHCP 23
  H.323 Standard 23
  IP Address Lists and Station Number Portability . . 32
  NAT 24
  Network Assessment 26
  Overview, Voice over IP and Network Protocols . . 21
  QoS 25
  Reliability and Performance 31
  Security 33
  SNMP 25
  Tandem Coding 22

W

WAN Considerations, for 4600 Series IP Telephones . 35
Web Sites for Other 4600 Series IP Telephones . . 141
Web Sites, Creating for the 4630/4630SW IP Telephone 125
What's New in Release 2.2 12