SIP Support in Release 3.0 of Avaya Communication Manager

Running on the
Avaya S8300, S8500, S8500B, S8700, and
8710 Media Server

555-245-206
Issue 5.1
July 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. See your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language as well as information regarding support for this product, while under warranty, is available through the following Web site: http://www.avaya.com/support.

Preventing Toll Fraud

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

Avaya Fraud Intervention

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

Disclaimer

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

How to Get Help

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

- Within the United States, click the *Escalation Management* link. Then click the appropriate link for the type of support you need.
- Outside the United States, click the *Escalation Management* link. 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 by this Avaya product (that is, "networked equipment").

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

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

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

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

Responsibility for Your Company's Telecommunications Security

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

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

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

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

TCP/IP Facilities

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

Standards Compliance

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

Product Safety Standards

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

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

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

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

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

The equipment described in this document may contain Class 1 LASER Device(s). These devices comply with the following standards:

- EN 60825-1, Edition 1.1, 1998-01
- 21 CFR 1040.10 and CFR 1040.11.

The LASER devices used in Avaya equipment typically operate within the following parameters:

Typical Center Wavelength	Maximum Output Power
830 nm - 860 nm	-1.5 dBm
1270 nm - 1360 nm	-3.0 dBm
1540 nm - 1570 nm	5.0 dBm

Luokan 1 Laserlaite

Klass 1 Laser Apparat

Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposures. Contact your Avaya representative for more laser product information.

Electromagnetic Compatibility (EMC) Standards

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

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

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

- Electrostatic Discharge (ESD) IEC 61000-4-2
- Radiated Immunity IEC 61000-4-3
- Electrical Fast Transient IEC 61000-4-4
- Lightning Effects IEC 61000-4-5
- Conducted Immunity IEC 61000-4-6
- Mains Frequency Magnetic Field IEC 61000-4-8
- Voltage Dips and Variations IEC 61000-4-11

Power Line Emissions, IEC 61000-3-2: Electromagnetic compatibility (EMC) - Part 3-2: Limits - Limits for harmonic current emissions.

Power Line Emissions, IEC 61000-3-3: Electromagnetic compatibility (EMC) - Part 3-3: Limits - Limitation of voltage changes, voltage fluctuations and flicker in public low-voltage supply systems.

Federal Communications Commission Statement

Part 15:

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

Part 68: Answer-Supervision Signaling

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

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

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

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

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

REN Number

For MCC1, SCC1, CMC1, G600, and G650 Media Gateways:

This equipment complies with Part 68 of the FCC rules. On either the rear or inside the front cover of this equipment is a label that contains, among other information, the FCC registration number, and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.

For G350 and G700 Media Gateways:

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the rear of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXXX. The digits represented by ## are the ringer equivalence number (REN) without a decimal point (for example, 03 is a REN of 0.3). If requested, this number must be provided to the telephone company.

For all media gateways:

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed 5.0. To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company.

REN is not required for some types of analog or digital facilities.

Means of Connection

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

For MCC1, SCC1, CMC1, G600, and G650 Media Gateways:

Manufacturer's Port Identifier	FIC Code	SOC/ REN/ A.S. Code	Network Jacks
Off premises station	OL13C	9.0F	RJ2GX, RJ21X, RJ11C
DID trunk	02RV2-T	0.0B	RJ2GX, RJ21X
CO trunk	02GS2	0.3A	RJ21X
	02LS2	0.3A	RJ21X
Tie trunk	TL31M	9.0F	RJ2GX
Basic Rate Interface	02IS5	6.0F, 6.0Y	RJ49C
1.544 digital interface	04DU9-BN	6.0F	RJ48C, RJ48M
	04DU9-IKN	6.0F	RJ48C, RJ48M
	04DU9-ISN	6.0F	RJ48C, RJ48M
120A4 channel service unit	04DU9-DN	6.0Y	RJ48C

For G350 and G700 Media Gateways:

Manufacturer's Port Identifier	FIC Code	SOC/ REN/ A.S. Code	Network Jacks
Ground Start CO trunk	02GS2	1.0A	RJ11C
DID trunk	02RV2-T	AS.0	RJ11C
Loop Start CO trunk	02LS2	0.5A	RJ11C
1.544 digital interface	04DU9-BN	6.0Y	RJ48C
	04DU9-DN	6.0Y	RJ48C
	04DU9-IKN	6.0Y	RJ48C
	04DU9-ISN	6.0Y	RJ48C
Basic Rate Interface	02IS5	6.0F	RJ49C

For all media gateways:

If the terminal equipment (for example, the media server or media gateway) causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment, for repair or warranty information, please contact the Technical Service Center at 1-800-242- 2121 or contact your local Avaya representative. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. It is recommended that repairs be performed by Avaya certified technicians.

The equipment cannot be used on public coin phone service provided by the telephone company. Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

This equipment, if it uses a telephone receiver, is hearing aid compatible.

Canadian Department of Communications (DOC) Interference Information

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

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

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

Installation and Repairs

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Declarations of Conformity

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

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

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

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

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

European Union Declarations of Conformity

CE

Avaya Inc. declares that the equipment specified in this document bearing the "CE" (*Conformité Europeénne*) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (89/336/EEC) and Low Voltage Directive (73/23/EEC).

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

Japan

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

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

To order copies of this and other documents:

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

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

E-mail: totalware@gwsmail.com

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

Contents

About this Document

This document, *SIP Support in Avaya Communication Manager 3.0 Running on the Avaya S8300, S8500, S8500B, S8700, and S8710 Media Server*:

- Is a revision of the 2.1.x document of the same name
- Includes corrections and newly developed information
- Contains new SIP (Session Initiated Protocol) information as well as 2.1.x SIP information
- Presents additional information about SIP for the 3.0 ACM system only. See Avaya Communication Manager documentation for non-SIP issues.

This document is available in online in paper format. For your convenience, consider using the embedded cross-references to locate information in addition to the table of contents and the index. Online readers may also use the search facility of the software.

Audience

This document is for field technicians, remote service personnel, and user-assigned administrative personnel, as a reference to configure and administer Avaya media servers using Communication Manager systems with SIP. We recommend having three to five years experience, and experience with working on media servers and the Communication Manager system.

This document assumes that the engineer has a working knowledge of telecommunication fundamentals and PBX maintenance practices. This document also assumes that the system was initially installed and tested properly and brought into service with every fault cleared. Adjuncts and other devices external to the switch are covered by their own service documentation.

If you do not have these experiences and qualifications, please make arrangements for a mentor.

Document set

Although this book is published separately, it is part of a set. Use this document as an adjunct to the following references:

- *Avaya Converged Communication Server v3.0 Installation and Administration,* DocID 555-245-705
- *Avaya Communication Manager Administrator Guide*, 03-300509
- *Administration for Network Connectivity for Avaya Communication Manager*, Doc ID 555-233-504

Equipment

The contents of this document discuss the equipment used as CM media servers:

- Avaya S8300
- Avaya S8500
- Avaya S8700
- Avaya S8710

Organization

- About this Document —What you are reading now gives general information on a SIP implementation, how to use this document, and others.
- Chapter 1: Overview of Changes —This section has high-level information about SIP at the general level that you can read quickly.
- Chapter 2: SIP Support in Avaya Communication Manager—This section describes in detail the SIP-related features, screens and fields for SIP support in Communication Manager version 3.0.
- Glossary —The glossary provides explanations of abbreviations, acronyms, and terms.
- Index

Conventions

Table 1: Explanation of typography

To represent...	This typeface and syntax are shown as...	For example...
commands	• Bold for **`commands`** • Bold italic for ***`variables`*** • Square brackets **[ ]** around optional parameters • "**|**" between exclusive choices	**`refresh ip-route [all |`** ***`location`*****`]`**
screen input and output	• Bold for **input** • Constant width for `output (screens and messages)`	Set the `Save Translation` field to **daily**. The message `Command successfully completed` should appear.
Web interface	• Bold for **menu selections, tabs, buttons,** and **field names** • Right arrow **>** to separate a sequence of menu selections	Select **Alarms and Notification,** the appropriate alarm, and then select **Clear**. Select **Diagnostics > View System Logs**, then select **Watchdog Logs**.
Keys	Special font for **keyboard keys** and SAT screen **clickable buttons**	Press **Tab**. Select **Next Page**.

Other conventions used in this book:

- Physical dimensions are in English units [Foot Pound Second (FPS)], followed by metric units [Centimeter Gram Second (CGS)] in parentheses.

  Wire-gauge measurements are in AWG, followed by the diameter in millimeters in parentheses.

- Circuit-pack codes (such as TN790B or TN2182B) are shown with the minimum acceptable alphabetic suffix (like the "B" in the code TN2182B).

  Generally, an alphabetic suffix higher than that shown is also acceptable. However, not every vintage of either the minimum suffix or a higher suffix code is acceptable. The *Hardware Guide for Avaya Communication Manager,* DocID 555-245-207, contains current information on circuit pack codes and functionality.

Safety labels and security alert labels

Observe all caution, warning, and danger statements to help prevent loss of service, equipment damage, personal injury, and security problems. This book uses the following safety labels and security alert labels:

CAUTION:
A caution statement denotes a situation that can result in harm to software, loss of data, or an interruption in service.

WARNING:
A warning statement indicates a situation that can result in harm to hardware or equipment.

DANGER:
A danger statement alerts you to a situation that can result in harm to personnel.

SECURITY ALERT:
A security alert points to a situation that can increase the potential for unauthorized use of a telecommunications system.

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.

Related resources

Table 2: Additional document resources lists additional documentation, some of which is referenced within this document.

Table 2: Additional document resources

Document	DocID
4600 Series IP Telephone R2.2 LAN Administrator's Guide, Issue 2.2.1, May 2005	555-233-507
4600 Series IP Telephone R2.2 Installation Guide, Issue 2.2.1, May 2005	555-233-128
4602/4602SW SIP Telephone R2.2 Userís Guide, Issue 2.2, May 2005	16-300470
4602/4602SW SIP Telephone Quick Reference, Issue 1, May 2005	16-300471
4610SW SIP Telephone R2.2 User's Guide, Issue 2.2, May 2005	16-300472
4620SW/4621SW SIP Telephone R2.2 User's Guide, Issue 2.2, May 2005	16-300474
4620SW/4621SW SIP Telephone Quick Reference, Issue 1, May 2005	16-300475
4600 Series IP Telephone Documentation Library, Issue 2.2.1, May 2005	16-300091
4602 SIP Telephone Administrator's Guide	16-300037
4602 SIP Telephone Quick Setup Guide	16-300158
4602 SIP Telephone User's Guide	16-300035
Avaya Communication Manager main ten ace documentation set	---
Avaya Communication Manager Capacities Table	555-245-601
Online help for Avaya IP SoftPhone R5	---
Online help for Avaya SIP SoftPhone R2	---
SIP Personal Information Manager release 3.0	03-300441
Understanding SIP, a course offered by Avaya University	---
Administration for Network Connectivity for Avaya Communication Manager	*555-233-504*
Avaya Communication Manager Administrator Guide	03-300509
	1 of 2

Table 2: Additional document resources (continued)

Document	DocID
Avaya Extension to Cellular and OPS Installation and Administration Guide	210-100-500
Avaya Extension to Cellular User's Guide, Issue 6	210-100-700
Avaya Toll Fraud and Security Handbook	555-025-600
Converged Communications Server Installation and Administration document	555-245-705
Hardware Guide for Avaya Communication Manager	555-245-207
Installation and Upgrades for the Avaya G700 Media Gateway and Avaya S8300 Media Server	555-234-100
Maintenance Alarms Reference	03-300190
Maintenance Commands Reference	03-300191
Maintenance Procedures	03-300192
	2 of 2

Technical assistance

Avaya provides the following resources for technical assistance.

- Within the U.S.
- International

Within the U.S.

For help with:

- Feature administration and system applications, call the Technical Consultants System Support group at
  1-800-225-7585
- Maintenance and repair, call the Avaya Remote Technical Services at
  1-800-242-2121
- Toll fraud, call Avaya Technical Services Organization at
  1-800-643-2353

International

For all international resources, contact your local Avaya authorized dealer for additional help.

Downloading this book from the Web

You can download the latest version of this book from the Avaya Web site. You must have access to the Internet, and a copy of Acrobat Reader must be installed on your personal computer.

Avaya makes every effort to ensure that the information in this book is complete and accurate. However, information can change after we publish this book. Therefore, the Avaya Web site might also contain new product information and updates to the information in this book. You can also download these updates from the Avaya web site.

Downloading this book

To download the latest version of this book:

1. Access the Avaya web site at http://support.avaya.com.
2. At the top center of the page, select **Product Documentation**.

   The system displays the **Welcome to Product Documentation** page.
3. In the upper-left corner type the 8- or 9-digit book number in the Search Support field, and then select **Go**.

   The system displays the **Product Documentation Search Results** page.
4. Scroll down to find the latest issue number, and then select the book title to the right of the latest issue number.
5. On the next page, scroll down and select one of the following options:
   - **PDF Format** to download the book in regular PDF format
   - **ZIP Format** to download the book in zipped PDF format

Sending us comments

Avaya welcomes your comments about this book. To reach us by:

- Mail, send your comments to:

  Avaya Inc.

  Product Documentation Group

  Room B3-H13

  1300 W. 120 Ave.

  Westminster, CO 80234 USA

- E-mail, send your comments to:

  document@avaya.com

- Fax, send your comments to:

  1-303-538-1741

Mention the name and number of this book, *SIP Support in Avaya Communication Manager 3.0 Running on the Avaya S8300, S8500, S8500B, or S8700/S8710 Media Server,* (555-245-206, Issue 3).

Chapter 1: Overview of Changes

New and changed SIP features

This section provides an overview of the new and changed Session Initiated Protocol (SIP) features as they affect Communication Manager release 3.0. SIP improvements are grouped into these areas:

- Internal feature changes
- VIP priority calling
- 80k bridged appearances
- SIP-related changes to the System-Parameters Features screen
- New UNICODE Name field
- SIP-related changes to the ICHT table

Internal feature changes

This release of SIP with respect to Communication Manager provides these features that may be transparent to the user:

- OATS call flow (Origination and terminating signaling)
- Transfer recall
- Hold recall
- PSTN fallback enabled for problematic calls

VIP priority calling

This release introduces a new class of service (COS), VIP Caller. The designation VIP Caller means a call from a VIP telephone is always a priority call without having to use the feature button or feature access code (FAC).

For more information see Class of Service screen on page 88.

80k bridged appearances

The maximum number of bridged appearances on the Avaya S8700/S8710 and S8500 Media Servers is increased to 80,000. The number of bridged appearances on the Avaya S8300 Media Server remains 2,400.

The ICHT table screen supports change and display commands. The command remains **inc-call-handling-trmt**. The key is an administered ISDN or SIP trunk group.

SIP-related changes to the System-Parameters Features screen

The field **Invalid Number Dialed Intercept Treatment** on page 5 of the System-Parameters Features screen was moved to the new page in the System-Parameters Features screen.

The field **Intercept Treatment on Failed Trunk Transfer** on page 9 of the System-Parameters Features screen was moved to the new page 15 in the System-Parameters Features screen. In this field, **y** means play a tone, and **n** means to drop the call immediately.

The valid selections for the field **Restricted Number Dialed Intercept Treatment** are now either **tone** or **announcement**.

For more information see System Parameters screen for SIP features on page 60.

New UNICODE Name field

The new field **UNICODE Name** is added to the SIP Trunk screen. A value of **y** means you want to use the NAME2 value of an Avaya Communication Manager field. NAME2 values support Unicode and can be used for most of the world's writing scripts. For more information on which fields support Name2 values, refer to the Unicode Native Name support in the *Avaya Communication Manager Administrator Guide*, 03-300509.

For more information see UNICODE Name on page 46.

SIP-related changes to the ICHT table

The ICHT table is no longer available on the **Trunk Group** screen.

A new ICHT screen was created that supports 30 pages with 18 entries per page, or 540 ICHT entries per trunk group.

For more information see ICHT Table screen on page 67.

Chapter 2: SIP Support in Avaya Communication Manager

This chapter describes the support for SIP (Session Initiated Protocol) that is incorporated into Avaya Communication Manager release 5, running an Avaya S8300, S8500 or S8700/S8710 Media Server.

This section contains these major topics:

Introduction to SIP

This section introduces SIP for release 3.0 Communication Manager and is divided into two sections:

What is SIP?

SIP is an endpoint-oriented signalling standard that is defined by the Internet Engineering Task Force (IETF). SIP is a text-based protocol based on elements of Hypertext Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP). SIP supports several types of communication sessions that include voice, video, or instant text messaging.

As implemented by Avaya in Communication Manager, SIP trunking functionality is available on the Linux-based S8300, S8500 and S8700/S8710 media servers.

SIP uses an OATS call flow model, in addition to others, and a URI-based feature access extension (Uniform Resource Indicator).

Because SIP-enabled endpoints are managed by Communication Manager, many features can be extended to these endpoints.

The media servers function in three ways:

- As Plain Old Telephone Service (POTS) gateways.
- As support for name and number delivery between and among the various non-SIP endpoints that Communication Manager supports. These endpoints can be, for example, analog, Digital Communications Protocol (DCP), or H.323 stations, and analog, digital or Internet Protocol (IP) trunks.
- As support for new SIP-enabled endpoints, such as the Avaya 4602 SIP telephone.

In addition to its calling capabilities, the SIP-enabled release of IP SoftPhone R5 and later, and SIP Softphone R2 and later, includes Instant Messaging (IM) client software, and provides full support for f the existing H.323 standard for call control.

How does SIP integrate into your system?

The support for SIP that is built into Avaya Communication Manager is designed to help SIP supplement your present system:

- It is built around published standards. These standards include both IETF Requests for comments (RFCs) and Internet-Drafts. The standards that the Avaya SIP solution implements include, but are not limited to, these standards:
  - RFC 3261 (SIP), 3265 (SIP Event Notification), 3515 (SIP REFER Method), and 3842 (SIP Message Summary and Message Waiting Indication Event Package)
  - RFC 2327 (Session Description Protocol) and 3264 (SDP Offer/Answer Model)
  - RFC 2617 (HTTP Digest Authentication)
  - RFC 3325, "*Network Asserted Identity*" is complied with on the SES proxy servers
  - Internet-Draft of "*The SIP 'Replaces' Header*"
  - Internet-Draft of "*Session Timers in the SIP*"
- It integrates with traditional circuit-switched interfaces and IP-switched interfaces. With this integration, the telecommunication system can evolve easily from a circuit-switched telephony infrastructures to next-generation IP infrastructures, including SIP.
- It positions customers to leverage, as needed, the increasing number and power of SIP-enabled applications, such as instant messaging and presence.

Note:

Building SIP support into Avaya MultiVantage Software adds another element to the modular family of Avaya components, which seamlessly delivers a business's voice and messaging capabilities over an IP network. Avaya continues enhancing the value it provides to customers in a standards-based, IP communications infrastructure.

Avaya uses a modular and extensible system architecture to implement SIP support. This architecture has a unique benefit for Avaya customers: the set of features SIP supports is augmented by those features that Communication Manager supports. Any media server that runs a SIP-enabled release of Communication Manager becomes, in effect, a telephony feature server. The Communication Manager media server is accessible from any SIP endpoint and provides access transparently to many telephony features that published SIP standards currently do not address.

SIP-related support

The following sections describe additions made to support SIP in release 3.0 Communication Manager running on the S8300, the S8500, or S8700/S8710 media servers:

- Trunking on page 23
- Stations on page 24
- CDR on page 24
- Access control on page 24

Trunking

With support for SIP trunks, an enterprise can connect media servers to a SIP-enabled proxy server, specifically, an Avaya Converged Communications Server (CCS) or through a third-party SIP service provider. The trunk support in Communication Manager complies with SIP standards, specifically IETF RFC 3261, and so interoperates with any SIP-enabled endpoint/ station that also complies with the standard.

In complex configurations with Avaya S8700/S8710 Media Servers, the signaling-group properties in Communication Manager must be administered to match in certain ways. For more information see SIP trunk engineering notes on page 26.

Stations

Support for SIP stations that use SIP trunks allows any fully compliant SIP telephone to interoperate with Avaya telephones. This means that any SIP telephone, from Avaya or a third party, that complies with the appropriate RFC or Internet-Draft standards can:

- Dial and be dialed as an extension in the enterprise dial plan.
- Put calls on hold and participate in transfers and conference calls.

SIP stations that are administered in Communication Manager as off-PBX station (OPS) stations support most Extended Access features, such as call park, call pick-up, and priority calls. To activate these features, use station buttons set up to dial special extensions, that is, Feature Name Extensions.

For more details, see *Avaya Extension to Cellular User's Guide*, Issue 6, DocID 210-100-700, and the *Avaya Extension to Cellular and OPS Installation and Administration Guide*, Issue 7, DocID 210-100-500.

CDR

Avaya provides support for complete call detail records (CDR) for all SIP calls based on the URIs of the calls.

Access control

Avaya provides support for full access control to external trunks from any telephone. Both SIP trunks and SIP endpoints require network access to an Avaya Converged Communications Server (CCS). Note that some other means of access control, such as a firewall, is usually required to control network access from outside the enterprise, that is, to the SES system and through it, to SIP trunks or SIP endpoints inside the enterprise.

Requirements for SIP

The minimum requirements for SIP added to a Communication Manager installation are described in these sections:

- Software on page 25
- Hardware on page 25
- Firmware on page 26
- SIP trunk engineering notes on page 26
- Related systems on page 28

Software

Support for SIP can be enabled in Communication Manager 5 running on any Linux-based media server. The appropriate Avaya remote feature activation (RFA) licensing files are also required.

Hardware

The SIP-enabled release of Communication Manager runs on the following Avaya media servers:

- S8300
- S8500 and S8500B
- S8700 and S8710

Note:

Any of these media servers may also control one or more Avaya media gateways.

All controlled LAN (CLAN) interfaces or processor CLAN IP interfaces must be configured correctly. For more information, see *Administration for Network Connectivity for Avaya Communication Manager*, DocID 555-233-504.

For more information see the *Converged Communications Server Installation and Administration* document, Issue 2, DocID 555-245-705, Avaya's SIP proxy, endpoint registration and instant messaging server. This product connects to one or several Avaya Communication Manager media servers, and provides SIP-enabled applications such as enterprise instant messaging (IM) that uses the client in Avaya IP SoftPhone R5 or later, or the Avaya SIP SoftPhone R2 or later.

Firmware

Note that SIP standards dictate that dual-tone multi frequency (DTMF) tones be supported within the RTP (Real Time Protocol) data stream. Interoperability with certain third-party, SIP-enabled devices may depend on this. This requirement further demands, for example, that the newest releases of Avaya's voice over IP (VoIP) engine be installed throughout your system to support RTP-payload.

For example, any TN2302AP circuit packs that are present in your system must have the correct firmware version to support DTMF tones within the RTP data stream. Table 3 shows what circuit pack you need for various versions of firmware and hardware.

Table 3: TN2302AP hardware and firmware combinations

	Media Processor	VoIP
Minimum for SIP	V72	V22 or greater
Highly recommended	V93	V93
In G700/G350 media gateways	V22	V22

SIP trunk engineering notes

The SIP signaling group administered on Communication Manager defines the characteristics of a signaling connection.

The total number of calls that can be carried over a single signaling connection is limited by the bandwidth available. There is no true physical trunk when using SIP. Because of this, there is no physical limit on how many calls or trunk members you can set up with a particular signaling connection.

However, using the signaling group and trunk group administrative screens in Communication Manager is also useful for SIP. Doing so extends several Communication Manager features to SIP. Communication Manager normally limits signaling groups to 255 trunk members, limiting each signaling group to 255 calls. For SIP groups, Avaya has removed the restriction that each combination of far-end and near-end IP address/port must be unique for each signaling group. For SIP groups, multiple signaling groups can use the same signaling connections.

More than one signaling group may be administered to share a signaling connection with exactly the same properties of:

- far-end node-name (fe-nn)
- far-end port (fe-pt)
- near-end node-name (ne-nn)
- near-end port (ne-pt).

This kind of administration supports more than 255 calls on the same SIP-based signaling connection, where a signaling connection is defined as <near-end node-name, near-end port, far-end node-name, far-end port>.

For an incoming call, Communication Manager 5 compares the caller's domain, as specified in the header of the SIP INVITE message, with the far-end domains specified for the administered SIP signaling groups. If there is a signaling group with a matching far-end domain, that signaling group and its associated trunking resources will be used to handle the incoming SIP call. If there is not a match, then a signaling group with a blank entry for far-end domain will be used. Avaya recommends that at least one SIP signaling group per signaling connection be administered with a blank domain. This blank domain terminates calls from any far-end domains not specifically assigned to other groups. Otherwise, if no matching or blank groups exist, then any SIP signaling group that has trunks available may be used.

All signaling groups that have identical node names/ports, as well as the SIP trunks groups using each of these signaling groups, should be administered with identical properties. That is, fields on this screen should match the analogous fields on the administrative screens.
Of course, different SIP signaling connections will differ with respect to their near-end and/or far-end node names/port numbers, and they *should* have their SIP trunk's signaling groups administered accordingly. It is not appropriate to administer them identically.

In Communication Manager, the number of simultaneous SIP signaling connections is limited to 10. You may administer more than 10, but the run-time limit of simultaneous signaling connections is 10. Remember that a signaling connection is not the same as a signaling group, and that more than one SIP signaling group can and should share the same signaling connection.

Related systems

See the *Converged Communications Server Installation and Administration* document, Issue 2, DocID 555-245-705, for details on the SIP proxy server.

See the following documentation for details on setting up and using for your Avaya 4602 SIP telephone as a station for SIP voice calling:

- *46xx SIP Telephone User's Guide*, DocID 16-300035
- *46xx SIP Telephone Administrator's Guide*, DocID 16-300037
- *46xx SIP Telephone Quick Setup Guide*, DocID 16-300158
- 4600 Series IP Telephone R2.2 LAN Administrator's Guide, DocID 555-233-507
- 4600 Series IP Telephone R2.2 Installation Guide, DocID 555-233-128
- 4602/4602SW SIP Telephone R2.2 User's Guide, DocID 16-300470
- 4602/4602SW SIP Telephone Quick Reference, DocID 16-3004715
- 4610SW SIP Telephone R2.2 User's Guide, DocID 16-300472
- 4610SW SIP Telephone Quick Reference, DocID 16-300473
- 4620SW/4621SW SIP Telephone R2.2 User's Guide, DocID 16-300474
- 4620SW/4621SW SIP Telephone Quick Reference, DocID 16-300475
- 4600 Series IP Telephone Documentation Library, DocID 16-300091

For an overview of the different components and the associated tasks that support Avaya's SIP solution, see the *SIP Implementation Guide*, DocID 16-300140.

Administering Communication Manager for SIP

This section describes how to administer and configure SIP on a Communication Manager system so that Communication Manager can support SIP endpoints. You administer and configure the system with Communication Manager screens, some of which are specific to SIP.

Most likely, you have been directed to this point from the section in the SES 3.0 installation procedures, from the section, *Administering Communication Manager and endpoints*. All installation work discussed prior to this point should be correctly completed by you.

Communication Manager must be functioning properly before you begin SIP administration. If your CM installation uses the Enhanced Meet Me conferencing feature, install that feature before beginning the following administration steps.

To administer SIP trunks in Communication Manager 5, complete the eight steps below. As you work through each step, you will find links to examples of your screens if you need them.

1. Verify that your system supports and is correctly configured for IP connectivity.

   See *Administration for Network Connectivity for Avaya Communication Manager*, DocID 555-233-504

2. On the **System-Parameters Customer-Options** screen (Figure 22: Optional Features screen **on page 85**), check the following two values:

   a. Verify that the **IP Trunks** field on page 4 is set to **y**, meaning controlled by the license file.

   b. Verify that the **Maximum Administered SIP Trunks** field, on page 2 of the Optional Features screen, has a value within these ranges:

      - 0 through 400 for S8300 servers
      - 0 through 800 for S8500 servers
      - 0 through 2000 for S8700/S8710 servers

3. Enter an IP address and host name for any SES server on your network in the corresponding fields on the **IP Node Names** screen. See Figure 11: IP Node Names screen **on page 69**.

   See the Communication Manager administration guide for information on this screen.

4. Enter the domain name or IP address for which this network region applies in the **Authoritative Domain** field on the **IP Network Region** screen, Figure 15: IP Network Region screen **on page 76**. A valid entry in this field is required for SIP endpoints on Communication Manager to call the public network.

   Note that the value for this **Authoritative Domain** field must match the content of the **Domain** field on the **Edit System Properties** screen, which is set with the Master Administration web interface in the SES system. In a single-server configuration, a home authoritative server combined on an Edge server, exactly one authoritative domain is set, for example, *company.com*.

   In a duplex configuration, each home is subject to the domain to which it is connected. Each Edge can have a separate domain, and a single CM can support multiple domains.

   Subdomains are not supported. You may not use domain structures such as east_company. com or west_company.com.

5. On the **Feature-Related System Parameters** screen,Figure 5: Feature-Related System-Parameters screen **on page 55**, select **all** in the **Trunk-to-Trunk Transfer** field to allow the transfer and conference features to operate correctly with SIP.

6. On the **Signaling Group Page 1** screen, Figure 1: Signaling Group screen, Page 1 **on page 34**:

   a. Type **sip** in the **Group Type** field. The system displays a screen for SIP groups.

   b. Verify that the **Transport Method** field contains the default value of **tls** (Transport Layer Security).

   c. Enter the name of the IP interface at the near (local) end of the SIP trunk signaling group in the **Near-end Node Name** field.

      For the S8300 media server, the value of this entry is typically **procr**.

      For the S8700/S8710 media server, the entry is the **node name** for the selected CLAN interface.

      The S8500 media server has IP capability as an internal process.

   d. Ensure the recommended TLS port value **5061** is set in the **Near-End Listen Port** field.

   e. Enter the name of the node you administered as the SIP proxy server in Step 3 in the **Far-end Node Name** field.

   f. Type the recommended TLS port value of **5061** in the **Far-end Listen Port** field.

   g. If you want the SIP proxy server you administered in Step 3 to use the codec set and/or parameters specified for an IP network region different from that of the LAN IP interface, then enter the SIP proxy's region in the **Far-end Network Region** field.

h. Enter the domain name or IP address of a server to which calls should be routed in the **Far-end Domain** field.

   For example, set one group to route SIP calls within your enterprise to an Avaya Converged Communications Server on your LAN, and set another group to route calls through your SIP service provider's far-end domain.

i. Ensure that the **DTMF over IP** field is set to the default value of **rtp-payload**.

Note:

This requires the support found in specific firmware versions on media-processing boards. For more information see Table 3: TN2302AP hardware and firmware combinations on page 26.

7. On the **Trunk Group** screen, illustrated in section **Trunk Group** screens, Figure 2: Trunk Group screen, page 1 on page 39:

a. Type **sip** in the **Group Type** field. The screen displays fields pertinent for SIP groups. An entry of **sip** also affects the fields presented on other administrative screens discussed later.

b. Depending on your need for call detail recording, type **y** for yes or **n** for no in the **CDR Reports** field. Note that very large numbers of CDR reports may be generated by SIP calling.

c. Type the number of the SIP signaling group you previously administered in the **Signaling Group** field.

d. Enter a value of 0 through 255 for the number of SIP trunks belonging to this group in the **Number of Members** field.

Note:

The total number of all SIP trunks specified for all groups must be less than or equal to the value in the **Maximum Administered SIP Trunks** field on the **System-Parameters Customer Options** screen. For more information see Figure 20: System Capacity screen on page 84.

e. Verify that the value in the **Numbering Format** field on page 2 is what you want.

   Group Member Assignments are automatically completed and populated on the Trunk Group screens **on page 39**, and on any subsequent pages necessary, based on the values that you entered on the Trunk Group screens. Group members cannot be administered individually. All members of each administered group share the same characteristics.

f. Repeat the preceding Steps a. through e. for each SIP trunk group you want to assign, up to your media server's trunk-number limit.

8. The final task before you can make SIP calls from endpoints connected to Communication Manager is to administer call routing properly in Communication Manager.

   On the **Route Pattern** screen, as shown in Figure 18: Numbering - Public/Unknown screen **on page 80**, verify that the **Secure SIP** field is set to the default value of **n** for routing through a public network.

   You can set **secure sip** to **y** only if you have a secure connection between the public SIP network and the SES home server you are routing to.

   Optionally on that screen, you may type a value of **p** at the beginning of the **Inserted Digits** field to insert a + (plus sign) into a digit string.

   Example

   Using AAR as an example, first be sure that the **Auto Alternate Routing (AAR) Access Code** field is set to the proper value on the **Feature Access Code** screen. Then administer both the **AAR Digit Analysis Table** and the **Numbering—Private screen** Figure 16: Locations screen **on page 77** and the **Numbering—Public/Unknown screen**, Figure 17: Numbering - Private Format screen **on page 78**, if applicable, to ensure that dialed strings of digits will be interpreted correctly and the resulting calls routed appropriately using the SIP trunks that you administered in Step 7. (Note that you may not access a SIP trunk with a dialed TAC.)

   For more details on all the screens that may be used to administer routing, see the *Avaya Communication Manager Administrator Guide*, 03-300509

   As shown in the Figure 16: Locations screen **on page 77**, type the appropriate **Proxy Selection Route Pattern** in the field corresponding to each location employing a SIP proxy server in routing SIP traffic.

9. (Optional) With Communication Manager 5, manage the resources supporting your SIP endpoints. Use the Figure 13: IP Address Mapping screen **on page 74** (using the **`ip-network-map`** command). This step is important in distributed Communication Manager environments in which network bandwidth may be consumed unnecessarily for calls among SIP and other endpoints.

   Also, use the **IP Address Mapping** screen to allow the system to identify the location of a caller who dials a 911 emergency call from a SIP endpoint. For more information on this topic, see the *Screen Reference* chapter in the *Avaya Communication Manager Administrator Guide*, 03-300509.

Chapter 3: Communication Manager administered for SIP—screen examples

This section contains properly populated screens that you might need to check as you administer Communication Manager for SIP trunking.

- SIP administrative screens on page 33
- Other Administrative screens on page 53

SIP administrative screens

These Communication Manager screens for SIP must be administered to support SIP trunking:

- Signaling Group Page 1 screen **on page 34**, when **sip** is entered in the **Group Type** field
- Trunk Group screens **on page 39**, when **sip** is entered in the **Group Type** field
- Trunk Group screen, Page 2 on page 48
- Trunk Group screen, Page 3 on page 51

Only SIP-related screens are described in this document. In all instances of screens and table descriptions, see the *Administration for Network Connectivity for Avaya Communication Manager* and the *Avaya Communication Manager Administrator Guide*, 03-300509, for more details about all Avaya Communication Manager screens and fields, including the SIP ones presented here.

These screens deal heavily with SIP administration. Look at them carefully.

Signaling Group Page 1 screen

The system displays the **Signaling Group** screen shown in Figure 1: Signaling Group screen, Page 1 **on page 34** when **sip** is the **Group Type** field on this page.

Figure 1: Signaling Group screen, Page 1

```
                                                              Page 1 of 6
                               SIGNALING GROUP

Group Number ___            Group Type: sip
                      Transport Method: tls




  Near-end Node Name:                  Far-end Node Name:
Near-end Listen Port: 5061           Far-end Listen Port: ____
                                  Far-end Network Region: __
      Far-end Domain: __________________________________

                                    Bypass If IP Threshold Exceeded? n

       DTMF over IP: rtp-payload             Direct IP-IP Audio Connections? y
Session Establishment Timer (min): 120       IP Audio Hairpinning? y
```

Signaling Group screen field descriptions

Group Number

A display-only field showing the signaling group.

Group Type

This field describes the type of protocol to be used with the signaling group. Select **SIP** in this field and the screen changes to show only SIP-applicable fields.

Valid entries	Usage
sip	Use for SIP on the Avaya S8300, S8500, S8700/S8710 IP-Connect, or S8700/S8710 Multi-Connect media servers only.

Transport Method

The screen displays this field only when the value of the entry in the **Group Type** field is **sip**. Make sure that the default **tls** is selected in this field. No other value is supported.

Valid entries	Usage
tls	Default (secure) transport method is TLS. This is the only method supported.

Near-end Node Name

The screen displays this field when the value of the entry in the **Group Type** field is either **h.323** or **sip**. Type the node name for the CLAN IP interface in this media server. The node name must be administered on the **IP Node Names** screen and the **IP Interfaces** screen.

Valid entries	Usage
Name of an administered IP node	Uniquely identifies the near-end node.

Far-end Node Name

The screen displays this field when the value of the entry in the **Group Type** field is either **h.323** or **sip**. Type the node name for the SIP proxy server used for trunks assigned to this signaling group. The node name must be administered on the **IP Node Names** screen.

Valid entries	Usage
Name of an administered IP node.	Describes the far-end node.

Tip:

If either the node name or port differs for each SIP signaling group, you have different SIP signaling connections, and you should administer a maximum of 10 using TLS. If you administer more than 10 TLS signaling connections, and they are all in use at the same time, the results may be unpredictable. Note that if the node names and ports match, you may administer as many identical SIP signaling groups using TLS as desired.

Near-end Listen Port

The screen displays this field when the **Group Type** field is either **h.323** or **sip**. The **Near-end Listen Port** field defaults to 5061 for SIP over TLS.

Valid entries	Usage
1719, **1720**, or **5000** through **5999**	Type an unused port number. The recommended port for SIP over TLS is 5061.

Far-end Listen Port

The screen displays this field when the **Group Type** field is either **h.323** or **sip**.

Valid entries	Usage
1-65535	Type the same number as entered in the **Near-end Listen Port** field, that is, port entry 5061 for SIP over TLS.

Far-end Network Region

The screen displays this field when the **Group Type** field is either **h.323** or **sip**. This field shows the number of the network region that is assigned to the far-end of the trunk group.

Valid entries	Usage
1-250 or blank	Type the network region number that is assigned to the far end of the trunk group. The region number is used to obtain the codec set used for negotiation of trunk bearer capability. Leave blank to select the region of the near-end node by default.

Far-end Domain

The screen displays this field only when the value of the entry in the **Group Type** field is **sip**.

Valid entries	Usage
Maximum of 40-character string, or blank	Enter the fully qualified domain name or IP address for the destination proxy server. For example, to route SIP calls within your enterprise, enter the domain assigned to your proxy server. For external SIP calling, the domain name could be that of your SIP service provider. If blank, the far-end IP address is used.

Bypass If IP Threshold Exceeded

The screen displays this field when the **Group Type** field is either **h.323** or **sip**.

Valid entries	Usage
y/n	Type **y** to automatically remove from service the trunks assigned to this signaling group when IP transport performance falls below limits. These limits are set on the **Maintenance-Related System Parameters** screen.

DTMF over IP

The screen displays this field when the value of the entry in the **Group Type** field is either **h.323** or **sip**.

Valid entries	Usage
rtp-payload	SIP trunks require **rtp-payload**.

Session Establishment Timer

This field determines how long the system waits before tearing down a ring no answer call. The default is 120 minutes.

Valid entries	Usage
3 to 120	The time in minutes Communication Manager waits before tearing down a ring no answer call.

Direct IP-IP Audio Connections

The screen displays this field when the value of the entry in the **Group Type** field is either **h.323** or **sip**. For SIP trunk groups, this is the value that allows direct audio connections between SIP endpoints.

Valid entries	Usage
y/n	Type **y** to save bandwidth resources and improve sound quality of VoIP transmissions for H.323 or SIP trunk groups.

IP Audio Hairpinning

The screen displays this field when the **Group Type** field is either **h.323** or **sip**. The **IP Audio Hairpinning** field entry allows the option for H.323 and SIP-enabled endpoints to be connected through the IP circuit pack in the media server or switch, without going through the time division multiplexing (TDM) bus.

Valid entries	Usage
y/n	Type **y** to enable hairpinning for H.323 or SIP trunk groups.

Trunk Group screens

This section describes each page of the Trunk Group screens. Valid data entry for each screen follows the screen example.

Trunk Group screen, Page 1

The system displays the **Trunk Group** screen shown in Figure 2, when **sip** is the **Group Type** on page 1.

Figure 2: Trunk Group screen, page 1

```
add trunk-group next                                                   Page 1 of x
                                   TRUNK GROUP

 Group Number: 1                     Group Type: sip_____      CDR Reports: _
   Group Name: OUTSIDE CALL_____________ COR: _1_       TN: _1__      TAC: ____
    Direction: two-way           Outgoing Display?__n__
  Dial Access? n                   Busy Threshold: 255      Night Service: ________
 Queue Length: __0_
 Service Type: _____                 Auth Code? n
                                           Signaling Group: ___
                                         Number of Members: __0__
 TRUNK PARAMETERS




   UNICODE Name? __y__
                                  Redirect on OPTIM failure: 5000
       SCCAN? n                   Digital Loss Group: 18
```

Trunk Group screen, Page 1 field descriptions

Group Number

This field contains the group number assigned to this group when the trunk group was added.

Group Type

Type **sip** to specify the trunk group as SIP.

Tip:

Busy-out the trunk group before you change the group type. Release the trunk group after you make the change. For more information about busying out and releasing trunk groups, see your system's maintenance documentation.

Valid entries	Usage
sip	Use SIP trunks to connect a media server running Communication Manager to a SIP proxy server (Avaya Converged Communications Server).

CDR Reports

Set this field according to the kind of call detail records (CDR) you want to generate.

Valid entries	Usage
y	All outgoing calls on this trunk group generate call detail records. To generate CDRs on incoming trunks, type **n** in the **Record Outgoing Calls Only** field on the **CDR System Parameters** screen.

Valid entries	Usage
n	Calls over this trunk group will not generate call detail records.
r (ring-intvl)	Generate CDR records for both incoming and outgoing calls. In addition, the following ringing interval CDR records are generated: ● Abandoned calls: The system creates a record with a condition code of **H**, indicating the time until the call was abandoned. ● Answered calls: The system creates a record with a condition code of **G**, indicating the interval from start of ring to answer. ● Calls to busy stations: The system creates a record with a condition code of **I** indicating a recorded interval of 0.

Group Name

Set this field to uniquely identify a trunk group.

Valid entries	Usage
1 to **27** characters	Enter a unique name that provides information about the trunk group. Do not use the default entry or the group type (DID, WATS) here. For example, you might use names that identify the vendor and function of the trunk group: USWest Local, Sprint Toll, Level(3) SIP.

COR

Decisions regarding the use of Class of Restriction (COR) and Facility Restriction Levels (FRLs) should be made with an understanding of their implications for allowing or denying calls when AAR/ARS/WCR route patterns are accessed. See Chapter 5 of the *Avaya Toll Fraud and Security Handbook*, DocID 555-025-600, for details on using COR and FRLs.

Valid entries	Usage
0 to **95**	Enter a class of restriction (COR). Classes of restriction control access to trunk groups, including trunk-to-trunk transfers.

Tip:

Remember that facility restriction levels are assigned to *classes* of restriction. Even if two trunk groups have classes of restriction that allow a connection, different facility restriction levels may prevent operations such as off-net call forwarding or outgoing calls by remote access users.

TN

Set this field to assign a trunk to a partition.

In the Customer Options screen, if Tenant Partitioning is set to **n**, this field is present on the Trunk Screen but does not function. Go the Customer Options screen if you suspect incorrect operation.

Valid entries	Usage
1 to **100**	Type a tenant partition number to assign this trunk group to the partition. Enter the digit 1 in this field to assign the trunk to the universal group which can be called by any other TN group.

Tip:

Double-check your entry. If you accidentally type an unassigned tenant partition number, the system accepts the entry but no calls go to the trunk group.

TAC

Type the trunk access code (TAC) for each trunk group. Assign a different TAC to each trunk group. CDR reports use the TAC to identify each trunk group. Each trunk must have a different TAC.

Valid entries	Usage
1- to 4-digit number	Type any number that fits the format for trunk access codes or dial access codes defined in your dial plan. NOTE: Although this field is required, trunk groups of type SIP cannot be dialed by using TAC. The TAC you type here only identifies them on CDR reports.
asterisk (*) and pound sign (#)	* and # may be used as the first character in a TAC.

Outgoing Display

This field allows display telephones to show the name and number of the trunk group used for an outgoing call before the call is connected. This information may be useful to you when you are trying to diagnose trunking problems.

Valid entries	Usage
y	Displays the trunk group name and number.
n	Displays the digits the caller dials.

Dial Access

This field controls whether users can route outgoing calls through an outgoing or two-way trunk group by dialing its trunk access code. Allowing dial access does not interfere with the operation of AAR/ARS. Dial access to SIP trunks is not allowed.

Valid entries	Usage
n	The entry **n** is used for SIP trunks, no others. Prevents users from accessing the trunk group by dialing its access code. Attendants can still select this trunk group with a Trunk Group Select button. This is the default entry.

Busy Threshold

This field specifies the threshold limit for the number of trunks that could be simultaneously active. Once the threshold is reached, any additional calls that *would* result in accessing that trunk group get redirected to the attendant. The attendant takes control of that trunk group and the access to the trunk members.

Use this field if you want attendants to control access to outgoing and two-way trunk groups during periods of high use. When the threshold is reached and the warning lamp for that trunk group lights, the attendant can activate trunk group control: internal callers who dial out using a trunk access code will be connected to the attendant, and the attendant can prioritize outgoing calls for the last remaining trunks. Calls handled by AAR and ARS route patterns go out normally.

Valid entries	Usage
0 to **255**	Type the number of trunks that must be busy in order to light the warning lamp on the Attendant Console. For example, if there are 30 trunks in the group and you want to alert the attendant whenever 25 or more are in use, type **25**.

The S8700/S8710 supports a maximum of 30000 busy hour call completions (BHCC).

The S8300 remains at a maximum of 3600 BHCC.

Night Service

This field sets the destination for incoming calls when Night Service is in operation. If a **Night** field on the **Group Member Assignments** page is administered with a different destination, that entry overrides the group destination for that trunk. CPE, DID, and DIOD trunk groups do not support night service.

Tip:

Whenever possible, use a night service destination on your switch to prevent incorrect behavior of some features, even on a DCS network.

Valid entries	Usage
blank	Leave this field blank if the **Trunk Type (in/out)** field is not **auto**.
An extension number (can be a VDN)	Type the extension of your night service destination.
attd	Calls go to the attendant and are recorded as Listed Directory Number (LDN) calls on call detail records.

Queue Length

Outgoing calls can wait in a queue, in the order in which they were made, when all trunks in a trunk group are busy. If you type **0** in this field, callers receive a busy signal when no trunks are available. If you type a higher number, a caller hears a confirmation tone when no trunk is available for the outgoing call. The caller can then hang up and wait. When a trunk becomes available, Communication Manager calls the extension that placed the original call. The caller hears three short, quick rings. The caller does not need to do anything but pick up the handset and wait. Communication Manager remembers the number the caller dialed and automatically completes the call.

The screen displays this field when the **Direction** field on the screen is set to **outgoing** or **two-way**.

Valid entries	Usage
0	Type **0** for DCS trunks.
1 through **100**	Type the number of outgoing calls that you want to be held waiting when all trunks are busy.

Service Type

The **Service Type** field indicates the service to which this trunk group is dedicated. A listing of predefined entries is shown below. In addition to the Services/Features listed in this table, any user-defined Facility Type of **0** (feature) or `1` (service) on the **Network Facilities** screen is allowed. For SIP trunks, only **public-ntwrk** and **tie** are valid.

Valid entries	Usage
public-ntwrk	Public network calls. It is the equivalent of CO (outgoing), DID, or DIOD trunk groups. If **Service Type** is **public-ntwrk** and the trunk is not a SIP trunk, then **Dial Access** can be set to `y`.
tie	Tie trunks. General purpose.

Auth Code

This field affects the level of security for incoming and outgoing calls on the Communication Manager server. The system displays this field if the **Direction** field is **incoming** or **two-way**. The **Auth Code** field can only be **y** if the **Authorization Codes** field is **y** on the System-Parameters Customer-Options screen ***on page 85***.

Valid entries	Usage
y or **n**	Type **y** to require callers to enter an authorization code in order to tandem a call through an AAR or ARS route pattern. The code will be required even if the facility restriction level of the incoming trunk group is normally sufficient to send the call out over the route pattern.

Signaling Group

The screen displays this field only when the value of the entry in the **Group Type** field is **sip**.

Valid entries	Usage
1 through **650**	Type the number of the SIP signaling group associated with this trunk group on the Signaling Group Page 1 screen **on page 34**, **Group Number** field.

This field restricts calling, and requires a code for users below the FRL level for incoming and outgoing calls.

Number of Members

The screen displays this field only when the value of the entry in the **Group Type** field is **sip**.

Valid entries	Usage
1 through **255**	Type the number of SIP trunks that are members of the trunk group. All members of a SIP trunk group will have the same characteristics. NOTE: Member pages for SIP trunk groups are completed automatically based on this entry and are not individually administrable.

UNICODE Name

This field determines which table of names to use to display the name, the legacy or the UTF-8 character table.

Valid entries	Usage
y or **n**	Type **y** to use the table with legacy names. Type **n** to use the table with UTF-8 format and so may contain Asian language names. Note that fifteen UTF-8 characters can take up to 45 bytes. Also, legacy names support Roman, Cyrillic, Ukrainian, and Katakana characters.

SCCAN

The system displays this field when the **Group Type** field is **sip** and **Enhanced EC500** on the **System Parameters - Customer Options** screen is set to **y**.

When the **SCCAN** field is set to **y**, the non-SCCAN-associated fields are hidden.

When set to **n**, the system displays all fields.

Valid entries	Usage
y	Type **y** to indicate that this trunk group supports incoming SCCAN calls.
n	Type **n** to indicate that the trunk does not support incoming SCAAN calls.

Redirect on OPTIM failure

This field is a timer that determines how long to wait for OPTIM to intercede before the call is redirected. Redirect on OPTIM failure is sometimes known as ROOF.

Valid entries	Usage
250 to **32000 milliseconds**	See OPTIM documentation for details on this field

Digital Loss Group

This field determines which administered 2-party row in the loss plan applies to this trunk group if the call is carried over a digital signaling port in the trunk group.

Valid entries	Usage
1 to **19**	Shows the index into the loss plan and tone plan.

Trunk Group screen, Page 2

The system displays page 2 of the Trunk Group screen, the **Trunk Features** screen, shown in Figure 3 when **sip** is the **Group Type** on page 1 of the trunk group screens.

Figure 3: Trunk Features screen

```
add trunk-group next                                                 Page 2 of 19
                                    TRUNK FEATURES
          ACA Assignment? _          Measured: none
                                                        Maintenance Tests? y




                     Numbering Format: public_




                                              Replace Unavailable Numbers? n
```

Trunk Group, Page 2 field descriptions

ACA Assignment

Valid entries	Usage
y/n	Type **y** if you want Automatic Circuit Assurance (**ACA**) measurements to be taken for this trunk group. If you set this field to **y**, complete the **Service Type** field.The default entry for SIP is **n**.

Measured

This field determines if the system will transmit data for this trunk group to the Call Management System (CMS).

You cannot use **internal** and **both** unless either the BCMS (Basic Call Management System) or the **Service Type** field is **y** on the **System-Parameters Customer-Options** screen. If the **ATM** field is set to **y** on the **System-Parameters Customer-Options** screen, this field accepts only **internal** or **none** as values. If this field contains a value other than **internal** or **none** when **ATM** is **y**, the screen displays **none** for the field value.

Valid entries	Usage
internal	Type **internal** if the data can be sent to the BCMS, the VuStats data display, or both.
external	Type **external** to send the data to the CMS.
both	Type **both** to collect data internally and to send it to the Communication Manager.
none	Type **none** if trunk group measurement reports are not required. NOTE: This is the default for SIP trunk groups.

Maintenance Tests

The screen displays this field only when the value of the **Group Type** field is **aplt**, **isdn**, **sip**, or **tie**.

Valid entries	Usage
y/n	Type **y** (the default) to run maintenance tests hourly on this trunk group. One or more trunk members must be administered for this entry to be saved.

Numbering Format

The screen displays this field if the **Send Calling Number** field is either **y** or **r**, or the **Send Connected Number** field is either **y** or **r**. The **Numbering Format** field specifies the encoding of Numbering Plan Indicator for identification purposes in the Calling Number, the Connected Number IEs or both, and in the QSIG Party Number. Valid entries are **public**, **unknown**, **private**, and **unk-pvt**.

Valid entries	Usage
Public	Indicates that the number plan according to CCITT Recommendation E.164 is used and that the **Type of Number** is **national**. This is the default entry for SIP trunks.
Unknown	Indicates that the **Numbering Plan Indicator** is **unknown** and that the **Type of Number** is **unknown**.
Private	Indicates the **Numbering Plan Indicator** is **PNP** and the **Type of Number** is determined from the **Private-Numbering** screen.
unk-pvt	Also determines the **Type of Number** from the **Private-Numbering** screen, but the **Numbering Plan Indicator** is **unknown**.

Replace Unavailable Numbers

The screen displays this field only when the **Group Type** field is **isdn** or **sip**. The **Replace Unavailable Numbers** field dictates whether to replace unavailable numbers with administrable strings for incoming and outgoing calls assigned to the specified trunk group. Administrable strings are located in the System Parameters Features screen.

This field applies to BRI/PRI and SIP trunks.

Valid entries	Usage
y/n	Type **y** to replace the display of an unavailable number with a phrase, for example, **Private Caller**. The system replaces unavailable numbers regardless of the service type of the trunk. The default for SIP trunks is **n**.

Trunk Group screen, Page 3

The system displays the **Trunk Group** screen, shown in Figure 4, when **sip** is the **Group Type** field on Trunk Group, Page 1.

Figure 4: Trunk Group screen, page 3

```
add trunk-group next                                       Page 3 of 22
                               TRUNK GROUP
                                   Administered Members(min/max): xxx/yyy
                                          Total Administered Members: xxx
GROUP MEMBER ASSIGNMENTS
       Port                    Name
    1: _______                 ___________  _____
    2: _______                 ___________  _____
    3: _______                 ___________  _____
    4: _______                 ___________  _____
    5: _______                 ___________  _____
    6: _______                 ___________  _____
    7: _______                 ___________  _____
    8: _______                 ___________  _____
    9: _______                 ___________  _____
   10: _______                 ___________  _____
   11: _______                 ___________  _____
   12: _______                 ___________  _____
   13: _______                 ___________  _____
   14: _______                 ___________  _____
   15: _______                 ___________  _____
```

Note:

For SIP trunks, the group member-assignment pages are *not* individually administrable. The system automatically populates and displays these fields based on the number of members of SIP trunk groups specified on page 1. Note that these display-only group member-assignment pages of the **Trunk Group** screen are repeated, as needed, to support all the trunk group's members.

For more information see SIP trunk engineering notes on page 26 for more details.

Trunk Group, Page 3 field descriptions

Administered Members (min/max)

Note:

This field shows the minimum and maximum member numbers that have been administered for this trunk group. For SIP trunks, this field is for display only.

For more information see SIP trunk engineering notes on page 26 for more details.

Total Administered Members

This field shows the total number of members administered in the trunk group. For SIP trunks, this field is display only.

Port

The **Port** field shows the port number assigned to each of the members administered in the trunk group. For SIP trunks, this field is display only.

Other Administrative screens

In addition to the SIP administrative screens on page 33, which must be administered to support SIP trunking, other fields in Communication Manager screens are also related to SIP. Check these screens and administer them correctly as well:

- Class of Service screen on page 88
- Coverage Path screen on page 58
- System Parameters screen for SIP features on page 60
- Feature-Related System Parameters screen, page 1 on page 55
- Locations screen on page 77
- ICHT Table screen on page 67
- IP Address Mapping screen on page 74 (now supports SIP endpoints, as well as H.323)
- IP Network Region screen on page 76
- IP Node Names screen on page 69
- Numbering—Private Format screen on page 78
- Numbering—Public/Unknown screen on page 79
- Route Pattern screen on page 82
- SCCAN-Related System Parameters screen on page 57
- Station screen on page 66
- System Capacity screen on page 84
- System Parameters screen for SIP features on page 60
- System Parameters—Call Coverage/Call Forwarding screen on page 85
- System-Parameters Customer-Options screen ***on page 85***
- Trunk Group screen, Pages 3-5 on page 71

This section discusses only SIP-related fields in the examples. Find information about non-SIP related fields on these screens in *Avaya Communication Manager Administrator Guide*, 03-300509.

SIP device as an OPTIM extension

If a SIP telephone is configured as an OPTIM extension, then the number of call appearances must be configured in all of these following areas:

1. **PHNNUMOFSA** must be set to the number of call appearances (in `46xxsettings.txt` file or in DHCP scope option).
2. Station screen - page 2: **restrict last appearance = n** (default = y)
3. Station for on CM, page 3: must add additional button assignments as 'call appearances' to match the value of PHNNUMOFSA
4. Off-station pbx mapping, page 2: **call limit** must equal the number of call appearances set in **PHNNUMOFSA**.

Feature-Related System Parameters screen, page 1

The Feature-Related System Parameters screen in Figure 5 shows the SIP-related information in bold.

Figure 5: Feature-Related System-Parameters screen

```
change system-parameters features                                              page 1
                         1-FEATURE-RELATED SYSTEM PARAMETERS
                            Self Station Display Enabled? n
                                 Trunk-to-Trunk Transfer? all
 Automatic Callback - No Answer Timeout Interval (rings): 4_
                    Call Park Timeout Interval (minutes): 10
     Off-Premises Tone Detect Timeout Interval (seconds): 20_
                              AAR/ARS Dial Tone Required? y
                                      Music/Tone On Hold: music    Port: _______
           Music (or Silence) On Transferred Trunk Calls: all
                    DID/Tie/ISDN/SIP Intercept Treatment: attd

 Internal Auto-Answer of Attd-Extended/Transferred Calls? y
               Automatic Circuit Assurance (ACA) Enabled? y
                                      ACA Referral Calls: local
                                ACA Referral Destination: ________
            ACA Short Holding Time Originating Extension: ______
             ACA Long Holding Time Originating Extension: ______
          Abbreviated Dial Programming by Assigned Lists:
    Auto Abbreviated/Delayed Transition Interval(rings):
                Protocol for Caller ID Analog Terminals: Bellcore
 Display Calling Number for Room to Room Caller ID Calls?
```

Note:

The **Trunk-to-Trunk Transfer** field on the screen above must be set to **all** to support the SIP transfer feature.

Trunk-to-Trunk Transfer

Regulations in some countries control the settings for this field. See your Avaya technical support representative for assistance.

Transfer between SUSHI SIP phones operates correctly even if Trunk-to-Trunk Transfer parameter is set to none. Trunks to OPS stations are not counted as trunks in OPTIM.

But, if one SIP telephone makes a call to a CO/ISDN trunk and then tries to transfer it to another CO/ISDN trunk, transfer is incorrect if **Trunk-to-Trunk Transfer** parameter is set to **none**.

Valid entries	Usage
all	Enter **all** to enable all trunk-to-trunk transfers. This allows telephone users to set up trunk-to-trunk transfer, go on-hook without disconnecting the call, and forward the call to a remote location.
restricted	Enter **restricted** (restricted public) to restrict all public trunks (CO, WATS, FX, CPE, DID, and DIOD).
none	Enter **none** to restrict all trunks (except CAS and DCS) from being transferred

DID/Tie/ISDN/SIP Intercept Treatment

Valid entries	Usage
Extension of a recorded announcement	Toll charges do not apply to DID and private network calls routed to an announcement. **NOTE:** If entering a Multi-Location Dial Plan shortened extension, note the following: When entering a Multi-Location Dial Plan shortened extension in a field designed for announcement extensions, certain administration end validations that are normally performed on announcement extensions are not done, and resultant warnings or submittal denials do not occur. The shortened extensions also do not appear in any display or list that shows announcement extensions. Extra care should be taken to administer the correct type of announcement for the application when assigning shortened extensions.
attd	For system security, Avaya recommends entering **attd** in this field. This routes intercept calls to the attendant and, if the attendant receives several of these, indicates a problem.

SCCAN-Related System Parameters screen

Figure 6: SCCAN-Related System Parameters screen

```
change system-parameters sccan
                      SCCAN - RELATED SYSTEM PARAMETERS

                MM(WSM) Route Pattern: ________
                          H1 Handover: ________
                          H2 Handover: ________
                         Announcement: ________
             Special Digit Conversion? ________
```

MM (WSM) Route Pattern

Enter a route pattern number that is SCCAN-enabled. Partition route pattern indexes, RHNPA indexes, deny, or nodes are not allowed.

Valid entries	Usage
blank	Default value. If this field is left blank, the feature is turned off. To enable this feature, you must enter an acceptable value.
digits	Right-click on the field on the SAT screen to see valid entries for your system.

Coverage Path screen

Coverage path processing has a new field, **Holiday Coverage**, to support a vectoring holiday coverage table as an input. The table determines use of a coverage path point or an announcement, or ring back.

Figure 7: Coverage Path screen

```
change coverage path 2                                              Page 1 of x
                                  COVERAGE PATH
            Coverage Path Number: 2
                                             Hunt After Coverage: n
                Next Path Number: ___        Linkage: ___ ___
COVERAGE CRITERIA

  Station/Group Status    Inside Call      Outside Call
            Active?             n                  n
              Busy?             y                  y
       Don't Answer?            y                  y    Number of Rings:7
               All?             n                  n
DND/SAC/Goto Cover?             y                  y
  Holiday Coverage?             n                  y    Holiday Table: 1

COVERAGE POINTS

  Terminate to Coverage Pts. with Bridged Appearance? n
Point1: _________ Point2: _________ Point3: _________
Point4: _________ Point5: _________ Point6: _________
```

Holiday Coverage

This field determines when to redirect call to coverage for an inside or outside call. This field is on the **Coverage Path** screen.

Set **Holiday coverage** to **y** to send an announcement.

Set **Holiday coverage** to **n** to send it to the next point in the coverage path.

For an incoming trunk call routed to a station extension using an Avaya switch DNIS-to-extension number call routing table, set these two fields as follows to get coverage:

- The station is administered with a coverage path that has the **Don't Answer** coverage external criteria set to **y**, and the **Number Of Rings** set to 7 (30 seconds)

and

- The station is administered with a coverage path that has a **Holiday Announcement** coverage path set to **y**. A VDN extension may be specified for a **y** coverage point.

If the incoming call is made on a holiday specified by the Holiday Table, after 30 seconds of ringing the incoming caller hears a holiday announcement with no tone, after which the call is dropped.

If the incoming call is made on a day not specified in the Holiday Table, the switch's call-coverage coverage-point processing does not take any action. The call rings indefinitely until answered by the routed-to station user or until the caller hangs up.

Holiday Table

The **Holiday Table** field on this screen refers to an existing holiday table. Use Communication Manager's Holiday Table screen to define a holiday table.

If the **Holiday Table** field is set to **y** for either inside or outside calls, the system uses a Holiday Table to route the call. Type the number of the holiday table to use.

System Parameters screen for SIP features

If the LED operation is changed for any of these new fields, then IP Agent and IP Softphone using a station type of 84xx or 64xx will not work. Only the 64xx and 84xx telephones have LEDs. A change to these LEDs for these fields should not affect either IP Agent or IP Softphone when these applications use a station type *other* then 84xx and 64xx.

All fields on this screen are SIP-related, but not bolded.

Figure 8: New Feature-Related System Parameters screen, page 15

```
change system-parameters features                                  page 15 of 15
                         FEATURE-RELATED SYSTEM PARAMETERS

INTERCEPT TREATMENT PARAMETERS

   Invalid Number Dialed Intercept Treatment: announcement 7700

          Invalid Number Dialed Display: Invalid Number

   Restricted Number Dialed Intercept Treatment: announcement 7701

         Restricted Number Dialed Display: Restricted No

   Intercept Treatment On Failed Trunk Transfers? n



WHISPER PAGE
   Whisper Page Tone Given To: all

DIGITAL STATION LINE APPEARANCE LED SETTINGS
                    Station Putting Call On Hold: green wink
                     Station When Call Is Active: steady
         Other Stations When Call Is Put On Hold: green wink
              Other Stations When Call Is Active: green
                                         Ringing: green flash
                                            Idle: steady


           Display Information With Bridged Call? n
                                  Pickup On Transfer? n
```

Invalid Number Dialed Intercept Treatment

This field is not new, but it has moved from page 5 of the Communication Manager's System-Parameters screen. That information is repeated here for your convenience.

For the **Invalid Number Dialed Intercept Treatment** field, type the kind of intercept treatment the end-user hears after dialing an invalid number.

Valid entries	Usage
announcement	Provides a recorded announcement when the end-user dials an invalid number. You select and record the message. Type the extension number for the announcement in the associated field.
tone	Default. Provides intercept tone when the end-user dials an invalid number.

Invalid Number Dialed Display

This field shows a name in either Latin or Asian characters for an invalid number calling in.

This field supports both a NAME1 and a NAME2 value. A NAME1 value directs the system to use the table of names that contains Latin characters, which can be displayed. Type a value of NAME2 to direct the system to use the UTF-8 table of names, which contains non-ASCII characters suitable for Asian language names.

The maximum length for both values is 15 characters. The NAME2 value is hidden on the SAT screen. It cannot be displayed there.

Restricted Number Dialed Intercept Treatment

This field controls whether an announcement or an intercept tone is played when an end-user dials an number restricted from them due to COS, COR, or FRL restrictions.

The valid selections for the **Restricted Number Dialed Intercept Treatment** field are now either **tone** or an **announcement**. The default is **tone**.

If set to **announcement**, the end-user must also type an extension number for the announcement.

- The end-user records and selects the announcement.
- The end-user must type, in the associated field, the extension number for the announcement.
- Communication Manager sends the text value in the **Restricted Number Dialed Display** field:
- If text is entered in that field
- If the **Restricted Number Dialed Intercept Treatment** is set to **announcement**

If set to **announcement**, the end-user hears a recorded announcement. If set to **tone**, the end-user hears an intercept tone.

Restricted Number Dialed Display

This field controls whether the system displays any string of alphanumeric characters assigned for calls that are denied because of COS, COR, or FRL restrictions.

This field supports both a NAME1 and a NAME2 value. A NAME1 value directs the system to use the table of names that contains Latin characters, which can be displayed. Type a value of NAME2 to direct the system to use the UTF-8 table of names, which contains non-ASCII characters suitable for Asian language names.

The maximum length for both values is 15 characters. The NAME2 value is hidden on the SAT screen. It cannot be displayed there.

Intercept Treatment On Failed Trunk Transfers

This field has moved from page 9 of **System-Parameters** screens. The information about this field is repeated here for your convenience.

Valid entries	Usage
y	Type **y** to provide intercept treatment to calls failing trunk transfers.
n	Type **n** to drop these calls.

Whisper Page Tone Given To

This field determines who hears a whisper page.

Valid entries	Usage
paged	The whisper page tone sends a beep to the paging party and the paged party
all	All parties hear the whisper tone. This is the default.
blank	No tone is sent to any party.

Digital Station Line Appearance LED Settings

All the fields in this section control the LED operation on 84xx and 64xx stations and only these stations. Changes to this group of fields has the following consequences.

- If you change the LED operation with fields in this screen, then IP Agent and IP Softphone using a station type of 84xx or 64xx will not work.
- A change to these LEDs using these fields does not affect either IP Agent or IP Softphone when these applications use a station type other then 84xx and 64xx.

Station Putting Call On Hold

This field is for a DCP bridged appearance LED color and flash when a call on a bridged appearance is put on hold by the party on the DCP bridged appearance.

This field controls the options for the station of a person who pushes the hold button. This field has choices of green or red and a flash option with the choices of off, wink, inverse-wink, flash, flutter, broken, flutter, and steady. Default values are green and wink.

This field applies only to 8400 and 6400 series telephones.

Correct Japanese-style operation requires the values **green flash** for this field.

Station When Call Is Active

This field controls the flash of the telephone when it is actively handling a call. This field has a flash option with the choices of **off** or **steady**. The default value is **steady**. When set to steady, Communication Manager controls the red LED.

This field applies only to 8400 and 6400 series telephones.

Correct Japanese-style operation requires the value **OFF** for this field.

Other Stations When Call Is Put On Hold

This field has LED options for the other stations with a bridged appearance that has been placed on hold, that is, the user of this station has not pushed the hold button. This field has choices of green or red, and flash options of off, wink, inverse-ink, flash, flutter, broken-flutter, and steady.

The default values are green and wink.

This field applies only to 8400 and 6400 series telephones.

The LED color and flash rate on 8400 telephones and 6400 telephones, for a call held by another party on a bridged appearance, is determined by the value set in this field. The LED for the color *not* selected for is turned OFF.

This field is for all users who share a bridged appearance. None of these users have pushed the hold button. The following list shows the codes for the flash rate:

Code	Rate Name
0	off
2	wink
3	Inverse wink (not supported on 8400 telephones, 8400 telephones use 8-flash)
8	flash

Code	Rate Name
A	flutter
D	broken flutter
F	steady

Correct Japanese-style operation requires the values **red flash** for this field.

Other Stations When Call Is Active

The value for color in this field controls a DCP bridged appearance LED for those inactive parties with a bridged appearance that is active.

This field applies only to 8400 and 6400 series telephones.

Correct Japanese-style operation requires the value of **red** for this field.

In release 5, a bridged appearance is unable to pick up a call that is being transferred.

This field applies only to 8400 and 6400 series telephones.

Station When Call Is Active

This field controls the red LED for the station selected when a user goes off hook. If set to **steady**, Communication Manager controls the red LED according to current Communication Manager rules. If set to **off**, the red LED is always OFF.

This field applies only to 8400 and 6400 series telephones.

The telephone should be set as red LED OFF on a station active on a call.

Ringing

This field controls the flash and LED color when a call is ringing in.

This field has LED color options with the choices of green or red, and a flashing option with the choices of off, wink, inverse-wink, flash, flutter, broken-flutter, and steady. The default is **green flash**. When set to steady, Communication Manager controls the red LED.

This field applies only to 8400 and 6400 series telephones.

Correct Japanese-style operation requires the values of **red wink** for this field.

Idle

This field controls the flash rate and LED color when a station is idle. This field has a flash option with the choices of **off** and **steady**. The default is **steady**. When set to **steady**, Communication Manager controls the red LED.

This field applies only to 8400 and 6400 series telephones.

Correct Japanese-style operation requires the value of **off** for this field.

Display Information With Bridged Call

This field determines whether name and number information is displayed for bridged calls on the called telephone.

If set to **y** to display the name and number for a bridged appearance. The display on the station shows the incoming call to the bridged appearance whether it is ringing audibly or not. There are currently cases where the display is not updated, even for an audibly ringing appearance.

If set to **n** to use the current Communication Manager behavior for the display, which is no display.

The default is **n**.

Note:

This new field in release 5 is needed because the maximum number of bridged appearances on the S8700/S8710 and S8500 media servers is to 80,000. The number of bridged appearances on the S8300 server remains at 2,400.

Pickup On Transfer

In release 5, the system restricts pickup on transfer. A bridged appearance is unable to pick up a call that is being transferred.

The default is **y**.

For correct Japanese-style operation, set this field to **n**.

Station screen

Figure 9: Station screen

```
change station 75001                                            Page 2 of X
                                    STATION
FEATURE OPTIONS
           LWC Reception? spe           Auto Select Any Idle Appearance? n
          LWC Activation? y                      Coverage Msg Retrieval? y
   LWC Log External Calls? n                                Auto Answer: none
             CDR Privacy? n                            Data Restriction? n
     Redirect Notification? y                 Idle Appearance Preference? n
   Per Button Ring Control? n              Bridged Idle Line Preference? Y
     Bridged Call Alerting? n                   Restrict Last Appearance? y
    Active Station Ringing: single       Conf/Trans On Primary Appearance? n

         H.320 Conversion? n        Per Station CPN - Send Calling Number? _
         Service Link Mode: as-needed      Busy Auto Callback without Flash? y
           Multimedia Mode: basic
    MWI Served User Type: ______                Display Client Redirection? n
              AUDIX Name:                      Select Last Used Appearance? n
                                               _ Coverage After Forwarding? _

                                           Direct IP-IP Audio Connections? n
Emergency Location Ext: 75001                        IP Audio Hairpinning? n
```

Bridged Idle Line Preference

This field controls whether the user must push a button to answer an incoming call to a bridge, or whether the user can take the telephone off hook or push a button. In this section, consider a 46xx station to include any station administered as a 46xx station.

If set to **y**, any incoming calls to a bridged appearance on a DCP or 46xx station require the bridged appearance button to be pushed to answer the call.

If set to **n**, this allows an incoming call on a bridged appearance to be answered with either an off hook or a button push.

The desired operation for DCP and 46xx stations with bridged appearances is comparable to the operation on prime line appearances when the existing **Idle Appearance Preference** field is set to **y**.

The 46xx H.323 telephones support bridged lines as well. For a call to a SIP telephone, the H.323 telephone sees it as a bridged call and can pick it up like a bridged appearance.

Conf/Trans On Primary Appearance

This field controls whether a DCP station permits transfer and conference.

For 46xx SIP telephones, the telephone, not this field, controls conference and transfer.

If set to **y**, the primary call appearance is activated for a transfer or conference.

If set to **n**, an idle bridge appearance is used for a transfer or conference.

ICHT Table screen

The ICHT Table screen has moved from the Trunk Group screen. The new ICHT Table screen supports 30 pages, 18 entries per page, for a total of 540 entries for each trunk group supported.

The system maximum for ICHT entries is 9,999, an increase from 576. The ICHT Table screen still supports **`change`** and **`display`** commands as before.

A new command available for the ICHT Table screen is **`inc-call-handling-trmt`**.

In Communication Manager release 5, the ICHT Table screen is administrable under the following conditions:

- **Trunk-group Type** is either ISDN or SIP
- The trunk-group is not **Outgoing_Only**
- The **Digit Handling** field is administered as either **enbloc/enbloc**, incoming and outgoing, or **enbloc/overlap**, one digit at a time. This field does not display for SIP trunk-groups, and always has a default value of **enbloc/enbloc**.
- If the link group's service type is *not* **cbc,** then that **Service Type** value populates the Service/Feature column and the administrator cannot change it.

  If the trunk group's service type *is* **cbc**, then the Service/Feature column is not populated. You must type a valid value for each entry.

ICHT pages 2 and 3 are only administrable on G3/LINUX and only if the Usage Allocation Enhancements feature is enabled.

The system displays a new message, Group not assigned when the command **`inc-call-handling-trmt`** is invoked on an unassigned trunk group

The system displays a new message, `The trunk group must be either an ISDN or SIP trunk group`, when the command **`inc-call-handling-trmt`** is invoked on an invalid trunk group type.

The system displays a new message, "This trunk group does not support incoming calls. Please select another." when the command **`inc-call-handling-trmt`** is invoked on an outgoing only trunk group type.

The system displays a new error message, "Trunk group does not support enbloc/enbloc or enbloc/overlap digit handling" when the command **`inc-call-handling-trmt`** is invoked on a trunk group type with incorrect digit handling.

Figure 10 is an example of the expanded **ICHT Table** screen.

Figure 10: New ICHT Table screen, page 1

```
change inc-call-handling-trmt trunk-group 2                      Page  1 of  30

                        INCOMING CALL HANDLING TREATMENT
Service/       Called      Called     Del      Insert          Per Call    Night
Feature         Len        Number                              CPN/BN      Serv
______________  ____  ______________  ____  _______________  ________  ________
______________  ____  ______________  ____  _______________  ________  ________
______________  ____  ______________  ____  _______________  ________  ________
______________  ____  ______________  ____  _______________  ________  ________
______________  ____  ______________  ____  _______________  ________  ________
______________  ____  ______________  ____  _______________  ________  ________
______________  ____  ______________  ____  _______________  ________  ________
______________  ____  ______________  ____  _______________  ________  ________
______________  ____  ______________  ____  _______________  ________  ________
______________  ____  ______________  ____  _______________  ________  ________
______________  ____  ______________  ____  _______________  ________  ________
______________  ____  ______________  ____  _______________  ________  ________
______________  ____  ______________  ____  _______________  ________  ________
______________  ____  ______________  ____  _______________  ________  ________
______________  ____  ______________  ____  _______________  ________  ________
______________  ____  ______________  ____  _______________  ________  ________
______________  ____  ______________  ____  _______________  ________  ________
______________  ____  ______________  ____  _______________  ________  ________
```

IP Node Names screen

Figure 11: IP Node Names screen

```
change node-names ip                                          Page 1 of X
IP NODE NAMES
Name            IP Address     Name           IP Address
1.   _______________ ___.___.___.___ 17. _______________ ___.___.___.___
2.   _______________ ___.___.___.___ 18. _______________ ___.___.___.___
3.   _______________ ___.___.___.___ 19. _______________ ___.___.___.___
4.   _______________ ___.___.___.___ 20. _______________ ___.___.___.___
5.   _______________ ___.___.___.___ 21. _______________ ___.___.___.___
6.   _______________ ___.___.___.___ 22. _______________ ___.___.___.___
7.   _______________ ___.___.___.___ 23. _______________ ___.___.___.___
8.   _______________ ___.___.___.___ 24. _______________ ___.___.___.___
9.   _______________ ___.___.___.___ 25. _______________ ___.___.___.___
10.  _______________ ___.___.___.___ 26. _______________ ___.___.___.___
11.  _______________ ___.___.___.___ 27. _______________ ___.___.___.___
12.  _______________ ___.___.___.___ 28. _______________ ___.___.___.___
13.  _______________ ___.___.___.___ 29. _______________ ___.___.___.___
14.  _______________ ___.___.___.___ 30. _______________ ___.___.___.___
15.  _______________ ___.___.___.___ 31. _______________ ___.___.___.___
16.  _______________ ___.___.___.___ 32. _______________ ___.___.___.___
```

Note:

If you are using an SES system for SIP Instant Messaging, enter the IP address for the SIP Proxy Server for your network in the corresponding fields on the **IP Node Names** screen.

Name

Identifies the name of the adjunct or server/switch node.

Valid entries	Usage
1 to 15 alphanumeric characters	Used as a label for the associated IP address. The node names must be unique for each server and switch.

IP Address

The IP address for the node named in the previous field.

Valid entries	Usage
32-bit address (4 decimal numbers, each in the range 0 to 255)	A unique IP address is assigned to each port on any IP device that is used for a connection. See the *Administration for Network Connectivity for Avaya Communication Manager*, DocID 555-233-504 for more information.

Trunk Group screen, Pages 3-5

The system displays the **Incoming Call Handling Treatment** (ICHT) screen shown in Figure 12, when **sip** is the **Group Type** on page 1 of the trunk group screens.

Figure 12: Incoming Call Handling Treatment screen

```
add trunk-group next                                          Page  3  of  22
                        INCOMING CALL HANDLING TREATMENT
     Service/   Called     Called         Del     Insert
     Feature     Len       Number

   _____________  ___   _______________   ___   ______________
   _____________  ___   _______________   ___   ______________
   _____________  ___   _______________   ___   ______________
   _____________  ___   _______________   ___   ______________
   _____________  ___   _______________   ___   ______________
   _____________  ___   _______________   ___   ______________
   _____________  ___   _______________   ___   ______________
   _____________  ___   _______________   ___   ______________
   _____________  ___   _______________   ___   ______________
   _____________  ___   _______________   ___   ______________
   _____________  ___   _______________   ___   ______________
   _____________  ___   _______________   ___   ______________
   _____________  ___   _______________   ___   ______________
   _____________  ___   _______________   ___   ______________
   _____________  ___   _______________   ___   ______________
   _____________  ___   _______________   ___   ______________
   _____________  ___   _______________   ___   ______________
   _____________  ___   _______________   ___   ______________
```

Trunk Group, Pages 3-5 field descriptions

Service/Feature

This field specifies the services and features for an incoming call type. For more information see the field description for Service Type on page 45 for a list of predefined services and features that can be received.

Valid entries	Usage
other	Use for any service or feature not explicitly named, for example, for SIP trunk groups.
Type 0, **Type 1** or **Type 2**	Indicates what user-defined services to use.

Called Len

The field **Called Len** specifies the number of digits received for an incoming call.

Valid entries	Usage
blank	A wild card entry meaning that any length of digits associated with the specified Service/Feature can match in this field.
0 through **21**	The number of digits received for an incoming call.

Called Number

This field value specifies the leading digits received for an incoming call. A blank entry is a “wild card” entry. Valid entries are up to 16 digits, or blank.

Valid entries	Usage
blank	A wild card entry meaning that any number of leading digits can be received for an incoming call.
0 through **16**	The number of leading digits received for an incoming call.

Del

Set the value of the **Del** field to specify the number of leading digits to be deleted from the incoming Called Party Number. Calls of a particular type may be administered to be routed to a single destination by deleting all incoming digits and then administering the **Insert** field with the desired extension.

Valid entries	Usage
blank	A wild card entry meaning that any number of leading digits can be received for an incoming call.
all	Specify all of the leading digits to be deleted from the incoming Called Party Number.
0 through **21**	The number of leading digits to delete from the incoming Called Party Number.

Insert

The **Insert** field specifies the digits to be added to the front of the incoming called party's number. Prepending these numbers occurs after any (optional) digit deletion has been performed. The number formed from digit deletion and insertion is used to route the call if night service is not in effect.

Valid entries are up to 16 characters consisting of a combination from the following: **0** to **9**, *****, **#**, or leave blank.

Valid entries	Usage
blank	A wild card entry meaning that no number of leading digits can be inserted for an incoming call.
0 through **9**, *****, **#**	You can specify up to 16 characters of these types.

IP Address Mapping screen

The **IP Address Mapping** screen in Figure 13 shows the SIP-related information.

Figure 13: IP Address Mapping screen

```
change ip-network-map                                                Page 1 of x
                         IP ADDRESS MAPPING
                                                        Emergency
                                  Subnet           802.1Q Location
From IP Address  (To IP Address)  or Mask)  Region   VLAN Extension
__1.__2.__3.__0  __1.__2.__3.255   24        _1_     __3  ________
__1.__2.__4.__4  __1.__2.__4.__4   32        _2_     __0  ________
__1.__2.__4.__5  __1.__2.__4.__5   __        _3_     __0  ________
__1.__2.__4.__6  __1.__2.__4.__9   __        _4_     __4  ________
___.___.___.__   ___.___.___.__    __        ___     __   ________
___.___.___.__   ___.___.___.__    __        ___     __   ________
___.___.___.__   ___.___.___.__    __        ___     __   ________
___.___.___.__   ___.___.___.__    __        ___     __   ________
___.___.___.__   ___.___.___.__    __        ___     __   ________
___.___.___.__   ___.___.___.__    __        ___     __   ________
___.___.___.__   ___.___.___.__    __        ___     __   ________
___.___.___.__   ___.___.___.__    __        ___     __   ________
___.___.___.__   ___.___.___.__    __        ___     __   ________
___.___.___.__   ___.___.___.__    __        ___     __   ________
___.___.___.__   ___.___.___.__    __        ___     __   ________
___.___.___.__   ___.___.___.__    __        ___     __   ________
```

Note:

In release 3.0 of Communication Manager, use this screen to allocate resources for both H.323 and SIP endpoints.

Figure 14: Feature Related System Parameters Screen

```
change system-parameters features                                        page 1
                         FEATURE-RELATED SYSTEM PARAMETERS
                            Self Station Display Enabled? n
                                 Trunk-to-Trunk Transfer? all
 Automatic Callback - No Answer Timeout Interval (rings): 4_
                    Call Park Timeout Interval (minutes): 10
     Off-Premises Tone Detect Timeout Interval (seconds): 20_
                              AAR/ARS Dial Tone Required? y
                                      Music/Tone On Hold: music    Port: _______
           Music (or Silence) On Transferred Trunk Calls: all
                    DID/Tie/ISDN/SIP Intercept Treatment: attd

 Internal Auto-Answer of Attd-Extended/Transferred Calls? y
               Automatic Circuit Assurance (ACA) Enabled? y
                                      ACA Referral Calls: local
                                ACA Referral Destination: ________
            ACA Short Holding Time Originating Extension: ______
             ACA Long Holding Time Originating Extension: ______
           Abbreviated Dial Programming by Assigned Lists:
     Auto Abbreviated/Delayed Transition Interval(rings):
                Protocol for Caller ID Analog Terminals: Bellcore
 Display Calling Number for Room to Room Caller ID Calls?
```

IP Network Region screen

The SIP-related fields are in bold in Figure 15:

Figure 15: IP Network Region screen

```
change ip-network-region 1                                     Page 1 of 19
                              IP NETWORK REGION
  Region: 1
Location:                  Home Domain:
    Name:
                                Intra-region IP-IP Direct Audio: no
MEDIA PARAMETERS                Inter-region IP-IP Direct Audio: no
   Codec Set: 1                           IP Audio Hairpinning? y
UDP Port Min: 2048
UDP Port Max: 3028                      RTCP Reporting Enabled? y
                                  RTCP MONITOR SERVER PARAMETERS
DIFFSERV/TOS PARAMETERS           Use Default Server Parameters? y
 Call Control PHB Value:                      Server IP Address:   .   .   .
        Audio PHB Value:                            Server Port: 5005
        Video PHB Value:
802.1P/Q PARAMETERS                    RTCP Report Period(secs): 5
 Call Control 802.1p Priority: 7
        Audio 802.1p Priority: 6      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                   RSVP Enabled? y
  H.323 Link Bounce Recovery? y               RSVP Refresh Rate(secs): 15
 Idle Traffice Interval (sec): 20     Retry upon RSVP Failure Enabled? y
     Keep-Alive Interval (sec): 6                RSVP Profile: guaranteed-service
             Keep-Alive Count: 5      RSVP unreserved (BBE) PHB Value: 40
```

Home Domain

The **Home Domain** field must be set to the same value as the domain administered, the home domain, or a third-party proxy for the signaling group associated with this network region.

This field designates the name or IP address of the domain for which this network region is responsible or authoritative.

Valid entries	Usage
Up to 20 characters or blank.	Enter the name or IP address of the domain for which this network region is responsible. Note that this will appear in the From header of any SIP messages.

Locations screen

The SIP-related fields are in bold in Figure 16:

Figure 16: Locations screen

```
change locations                                               Page   1 of   1
                                  LOCATIONS

                ARS Prefix 1 Required For 10-Digit NANP Calls? y

 Loc. Name                 Timezone  Rule      NPA    ARS Attd Loc.   Pre- Proxy Sel.
 No                         Offset                    FAC FAC  Parms. fix  Rte. Pat.
 1.  Main                 + 00:00    1         312
 2.  Denver-01______      - 01:00    1         303    ____ ____ __    ____ _______
 3.  Lincroft-01____      + 01:00    1         953    ____ ____ __    ____ _______
 xxx _______________ _ __:__    __        ___    ____ ____ __    ____ _______
 xxx _______________ _ __:__    __        ___    ____ ____ __    ____ _______
```

Note:

This screen allows for each location to point to the route pattern that is routing to its outbound SIP proxy server. This correlation is required by features and services such as Transfer and URI Dialing.

Proxy Selection Route Pattern

The **Proxy Selection Route Pattern** field identifies the routing pattern that leads to the proxy server. This is the route pattern assigned on the **Route Pattern** screen.

Valid entries	Usage
1 to **999** or blank	Type the number of the routing pattern to be used to get to the proxy server.

Numbering—Private Format screen

This screen supports Private Numbering Plans (PNP) and now applies to both ISDN and SIP.

This screen is for AAR private trunking. The numbers entered here precede the station number in the display.

This screen allows you to specify the digits to be put in the Calling Number information element (IE), the Connected Number IE, and the QSIG Party Number for extensions in the Private Numbering Plan.

Communication Manager supports private-network numbers as long as 15 digits. If the complete number, including the level 1 and 2 prefixes, the PBX identifier, and the extension, is more than 15 digits long, then Communication Manager neither creates nor sends the QSIG Party Numbers or information elements. Figure 17 shows an example of the **Numbering - Private Format** screen.

Figure 17: Numbering - Private Format screen

```
change private-numbering                                              Page 1 of 1

                          NUMBERING - PRIVATE FORMAT


          Network Level: _                      PBX Identifier: ____
           Level 2 Code: _____                  Deleted Digits: _
           Level 1 Code: _____
```

Numbering—Public/Unknown screen

This screen is used for ARS public trunks.

In Communication Manager 5, the Public-Unknown Numbering screens support 9,999 entries.

The ANI table, which this screen uses, is increased from 240 to 9,999 entries. This increase is for S8500 and S8700/S8710 media servers only.

The **public-unknown-numbering forms** use a window of 2 pages. The first page is filled in starting at the key (Ext Len) specified on the command line. The second page is blank. The secondary key is Ext Code.

New command: **`list public-unknown-numbering`**. This command has one argument, **`Ext Len`**, and two options, **`Ext digits`** and **`count`**, both of which are optional.

- **`Ext Len`** determines how many digits to display. If you specify **0** as the **Ext Len**, attendant information displays.
- **`Ext digits`** lets you specify a starting point for the extension digits you want to see. Only assigned extensions are available to view.
- **`count`** lets you specify how many lines of output to display.

Examples

`display public-unknown-numbering 0`

shows the attendant entry first, followed by the subsequent entries.

`display public-unknown-numbering 4`

shows the first **`Ext Code`** of length 4 followed by the subsequent entries.

`display public-unknown-numbering 5 ext-digits 10010`

shows the first entry of **`Ext Code 10010`** followed by the subsequent entries.

`display public-unknown-numbering 5 ext digits 10020`

Extension 10020 has not been assigned. The screen shows the next entry following 10020 and all subsequent entries.

This screen supports the Call Identification Display feature for ISDN and SIP. The feature presents a name and number for display-equipped stations within an ISDN or SIP network. The system uses the caller's name and number, and presents it on the called party's telephone display. Conversely, the called party's name and number can be displayed on the caller's telephone display as well.

The screen allows you to specify the desired digits for the Calling Number IE and the Connected Number IE (in addition to the QSIG Party Number) for any extension in the Public and/or Unknown Number Plans.

Administer these screens if the value entered in either the **Send Calling Number** or the **Send Connected Number** field is **y**, or the value entered in the **Supplementary Service Protocol** field is **b**, on the **Trunk Group** screen.   See Figure 18.

Figure 18: Numbering - Public/Unknown screen

```
change public-unknown-numbering                                     Page 1 of x
                         NUMBERING - PUBLIC/UNKNOWN FORMAT

                                 Total                                     Total
Ext Ext        Trk       CPN         CPN Ext Ext       Trk       CPN           CPN
Len Code       Grp(s)    Prefix      Len Len Code      Grp(s)    Prefix        Len

 5  4_______   _____     73283_______ 10  _  _______  _____     _____________  __
 7  3646180    _____     210_________ 10  _  _______  _____     _____________  __
 _  ______     _____     _____________ __ _  _______  _____     _____________  __
 _  _______    _____     _____________ __ _  _______  _____     _____________  __
 _  _______    _____     _____________ __ _  _______  _____     _____________  __
 _  _______    _____     _____________ __ _  _______  _____     _____________  __
 _  _______    _____     _____________ __ _  _______  _____     _____________  __
 _  _______    _____     _____________ __ _  _______  _____     _____________  __
 _  _______    _____     _____________ __ _  _______  _____     _____________  __
 _  _______    _____     _____________ __ _  _______  _____     _____________  __
 _  _______    _____     _____________ __ _  _______  _____     _____________  __
 _  _______    _____     _____________ __ _  _______  _____     _____________  __
 _  _______    _____     _____________ __ _  _______  _____     _____________  __
```

Note:

If the table is not properly administered, but the **Send Calling Number** or the **Send Connected Number** field is **public** or **unknown**, the Identification Number (PartyNumber data type) is not sent for QSIG Party Numbers. In this case, the ASN.1 data type containing the PartyNumber (PresentedAddressScreened, PresentedAddressUnscreened, PresentedNumberScreened, or PresentedNumberUnscreened) will be sent marked as **PresentationRestricted** with **NULL** for the associated digits.

Examples

The command **`list public-unknown-numbering`** operates as follows:

- **`list public-unknown-numbering start 4`** displays the entries starting with Ext Len of 4.
- **`list public-unknown-numbering start 4 count 50`** displays the first 50 entries starting with Ext Len 4.
- **`list public-unknown-numbering`**—displays all entries. The system only displays the first two pages of them.

The command **`change/display public-unknown-numbering`** operates as follows:

- **`change/display public-unknown-numbering 0`**—the screen displays the attendant entry first, followed by the subsequent entries.
- **`change/display public-unknown-numbering 4`**—the screen displays the first Ext Code of length 4 followed bay the subsequent entries.
- **`change/display public-unknown-numbering 5 ext-digits 10010`**—the screen displays the first entry of Ext Code 10010 followed by the subsequent entries
- **`change/display public-unknown-numbering 5 ext-digits 10020`**—If 10020 has not been assigned, the screen displays the next entry following 10020 and subsequent entries.

Route Pattern screen

The **Route Pattern** screen defines the route patterns used by Communication Manager. Each route pattern contains a list of trunk groups that can be used to route the call. The maximum number of route patterns and trunk groups depends on the configuration and memory available in your system.

AAR analysis and ARS analysis determine which trunks calls use. You can convert an AAR number into an international number, and insert an area code in an AAR number to convert an on-network number to a public network number. Also, when a call directly accesses a local central office (CO), if the long-distance carrier provided by your CO is not available, then Communication Manager can insert the dial access code for an alternative carrier into the digit string.

The SIP-related fields are in bold on the screen shown in Figure 19.

Figure 19: Route Pattern screen

```
change route-pattern 1                                          Page  1 of  X
                              Pattern Number: 1_
             SCCAN y/n                                 Secure SIP? n
                              No.                                      DCS/
   Grp. FRL NPA Pfx Hop Toll Del  Inserted                             QSIG  IXC
   No.          Mrk Lmt List Dgts Digits                               Intw
 1: ___   _ ___  _  __   __   __  _____________________________________  n   user
 2: ___   _ ___  _  __   __   __  _____________________________________  n   user
 3: ___   _ ___  _  __   __   __  _____________________________________  n   user
 4: ___   _ ___  _  __   __   __  _____________________________________  n   user
 5: ___   _ ___  _  __   __   __  _____________________________________  n   user
 6: ___   _ ___  _  __   __   __  _____________________________________  n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature BAND  No.   Numbering LAR
    0 1 2 3 4 W     Request                                Dgts   Format
                                                       Subaddress
  1: y y y y y n  y  none   ___ both ept outwats-bnd____ ____  _   ________  none
  2: y y y y y n  y             rest     _______________       _   ________  next
  3: y y y y y n  y             rest     _______________       _   ________  rehu
  4: y y y y y n  y             rest     _______________       _   ________  none
  5: y y y y y n  y             rest     _______________       _   ________  none
  6: y y y y y n  y             rest     _______________       _   ________  none
```

SCCAN

When the **SCCAN** field is set to **y**, the non-SCCAN-associated fields are hidden.

When set to **n**, the system displays all fields.

Secure SIP

Valid entries	Usage
y/n	Specify whether the SIP or SIPS prefix will be used, if the call is routed to a SIP trunk preference. If SIP trunks are not specified on the **Route Pattern** screen, the call will be routed over whatever trunk is specified. Therefore, to ensure a SIP TLS connection when such a route-pattern is invoked, only SIP trunks should be specified. Default is **n**.

System Capacity screen

The SIP-related fields are in bold on this screen, as shown in Figure 20:

Figure 20: System Capacity screen

```
display capacity                                                  Page 7 of 12
                              SYSTEM CAPACITY
                                                                      System
                                                         Used  Available  Limit
                                                      - - - - - - - - - - - - -
                     TRUNKS
                               DS1 Circuit Packs:         10       390      400
                      DS1 With Echo Cancellation:          0       400      400
                            ICHT For ISDN Trunks:          0       576      576
                ISDN CBC Service Selection Trunks:         1       199      200
                                    Trunk Groups:         34      1966     2000
                                     Trunk Ports:        608      7392     8000
        H.323 Trunks (included in 'Trunk ports'):        604      3396     4000
Remote Office Trunks (included in 'Trunk ports'):          0      4000     4000
          SBS Trunks (included in 'Trunk ports'):          0      1000     1000
          SIP Trunks (included in 'Trunk ports'):        764       236     1000
```

Note that system trunking capacity varies, based on media server. See the document *Capacities Table* for more information. This capacities table document is for Avaya use only and not available to customers. Customers should consult their Avaya representative.

System Parameters—Call Coverage/Call Forwarding screen

The SIP-related fields are in bold on Figure 21:

Figure 21: System Parameters—Call Coverage/Call Forwarding screen

```
change system-parameters coverage-forwarding                           page 2

           SYSTEM PARAMETERS -- CALL COVERAGE / CALL FORWARDING

COVERAGE OF CALLS REDIRECTED OFF-NET (CCRON)
                            Coverage Of Calls Redirected Off-Net Enabled? y
      Activate Answer Detection (Preserves SBA) On Final CCRON Cvg Point? y
                                       Ignore Network Answer Supervision? y
                      Disable call classifier for CCRON over ISDN trunks? n
                       Disable call classifier for CCRON over SIP trunks? n
```

For more details on completing the fields on this screen, see the *Avaya Communication Manager Administrator Guide*, 03-300509.

System-Parameters Customer-Options screen

The SIP-related fields are in bold on this screen, as shown in Figure 22:

Figure 22: Optional Features screen

```
display system-parameters customer-options                            page 1 of 10
                              OPTIONAL FEATURES
                                                                           Used
        G3 Version: V12
         Location: 1                                RFA System ID (SID): 1
         Platform: 2                                RFA Module ID (MID): 1


                                                            USED
                              Platform Maximum Ports: 44000 597
                                    Maximum Stations: 36000 552
                             Maximum XMOBILE Stations: 1000 0
                   Maximum Off-PBX Telephones - EC500: 0    0
                   Maximum Off-PBX Telephones -   OPS: 600  545
                   Maximum Off-PBX Telephones - SCCAN: 0    0




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

The Avaya license file controls many fields on this screen. The web-based RFA process generates these license files for customers. For more detailed descriptions of the fields on this screen, see *Avaya Communication Manager Administrator Guide*, 03-300509.

Figure 23: Optional Features screen, page 2

```
display system-parameters customer-options                          page 2 of 10
                              OPTIONAL FEATURES
IP PORT CAPACTIES
                                                                       USED
                             Maximum Administrered H.323 Trunks: 200   20
                    Maximum Concurrently Registered IP Stations: 50    0
                        Maximum Administered Remote Office Trunks: 0     0
         Maximum Concurrently Registered Remote Office Stations: 0     0
                         Maximum Concurrently Registered IP eCons: 0     0
                             Maximum Video Capable H.323 Stations: 0     0
                              Maximum Video Capable IP Softphones: 0     0
                                  Maximum Administered SIP Trunks: 500   25

            Maximum Number of DS1 Boards with Echo Cancellation: 0     0
                                        Maximum TN2501 VAL Boards: 10    0
                              Maximum G250/G350/G700 CAL Sources: 10    0
                                   Maximum TN2602 VoIP Channels: 10000 96

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




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

Maximum Concurrently Registered IP Stations

This field now accepts 6,000 concurrently registered IP stations for the S8700/S8710 and 3,000 for the S8500. The maximum in previous releases of Communication Manager was 450.

Maximum Administered SIP Trunks

Defines limits of the number of SIP trunks administered.

Figure 24: System Parameters Customer Options screen, page 4

```
display system-parameters customer-options                       Page 4 of 10
                              OPTIONAL FEATURES
  Emergency Access to Attendant? y                               IP Stations? y
          Enable 'dadmin' Login? y                 Internet Protocol (IP) PNC? y
          Enhanced Conferencing? y                          ISDN Feature Plus? y
                 Enhanced EC500? y             ISDN Network Call Redirection? y
   Enterprise Survivable Server? n
      Enterprise Wide Licensing? y                           ISDN-BRI Trunks? y
             ESS Administration? n
         Extended Cvg/Fwd Admin? y                                  ISDN-PRI? y
    External Device Alarm Admin? y                 Local Survivable Processor? y
                                 y                        Malicious Call Trace? y
                                                      Media Encryption Over IP? y
    External Device Alarm Admin? y      Mode Code for Centralized Voice Mail? y
  Five Port Networks Max per MCC? y
               Flexible Billing? y                     Multifrequency Signaling? y
  Forced Entry of Account Codes? y   Multimedia Appl.Server Interface (MASI)? y
     Global Call Classification? y          Multimedia Call Handling (Basic)? y
            Hospitality (Basic)? y       Multimedia Call Handling (Enhanced)? y
Hospitality (G3V3 Enhancements)? y
                      IP Trunks? y

          IP Attendant Consoles? y

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

To enable SIP telephones to display dual language Caller ID, administer page 4 of this screen this way:

- **ISDN-PRI** field is set to **y**, *or* set **ISDN BRI trunks** is set to **y** *or* the **IP Trunks** field is set to **y**.
- **Basic Supplementary Service?** field is set to **y** *and* the **Value-Added** field is set to **y**.

Figure 25: System Parameters Customer Options, page 8

```
display system-parameters customer-options              Page 8 of x

                            QSIG OPTIONAL FEATURES
                                         Basic Call Setup? y
                             Basic Supplementary Services? y
                                    Centralized Attendant? n
                                    Interworking with DCS? y
                     Supplementary Services with Rerouting? y
                             Transfer into QSIG Voice Mail? n
                                       Value-Added (VALU)? y
```

Class of Service screen

A new class of service is VIP Caller. This class of service identifies a station as VIP-enabled. The value **y** means the station is VIP-enabled and **n** means that it is not.

When an internal call is made form a station administered as a VIP station, the ring cadence is automatically priority. To activate this, administer each COS to **y** for VIP caller on the Class of Service screen.

```
change COS                                                      Page 1 of 2

                                Class of Service
                                0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
Trk-to-Trk Restriction Override:n n n n n n n n n n  n  n  n  n  n  n
QSIG Call Offer Origination:    n n n n n n n n n n  n  n  n  n  n  n
```

```
change COS                                                      Page 2of 2

                                Class of Service
                                0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
VIP Caller:                     y y y y y y y y y y  y  y  y  y  y  y
```

See the Communications Manager administrator guide for other information about this screen.

VIP class of service is available for both external and internal calls.

VIP calls get priority ringing when calling local stations as well as remote stations using QSIG.

- At the called party call is treated like a priority call:
    - Provides distinctive alerting, the ringing cadence you have provided above
    - Uses the last available call appearance even if it is restricted for originations
    - Does not cover unless calling party uses the go-to-cover feature, a feature button.
    - Can be forwarded as a priority call
    - Pickup group users can pickup a priority call
- - User gets alerted for the call even if SAC is activated.

Appendix A: Requirement specifications

These sections in this appendix explain how Converged Communications Server v3.0 rules are applied:

- Call processing software

Call processing software

Call processing software is explained in sections covering domains and routing:

- RFC 3325 compliance
- Origination/Capability-based routing

Avaya employees and business partners can find other information related to this appendix in SRAD 101014.

RFC 3325 compliance

The material in this book is based on regulatory compliance of RFC 3325 compliance.

Compliance with RFC 3325

The SES proxy complies with RFC 3325, *Network Asserted Identity*.

While RFC 3325 provides for a privacy header, this header does not provide complete anonymity to the user. The privacy header only requires that the p-asserted-identity header be removed from the request.

SES proxy trust domain

Trust domain definition

The SES proxy trust domain includes those SIP servers and gateways, but not endpoints, that have identities administered on the SES.

Entities not administered on SES as trusted hosts are considered outside the SES trust domain. If an edge proxy trusts an external proxy, asserted identity and privacy preferences are forwarded to the external proxy. Using TLS certificates to detect the trust domain is unsupported.

p-asserted-identity header

User identity is verified using Digest Authentication on all SIP requests. Upon receipt of a 407 Proxy Authentication challenge from the proxy, an endpoint re-sends the request with the user name and challenge response, as administered on the SES.

Forwarding unauthenticated requests

If a non-emergency request within the proxy's trust domain cannot be authenticated, the proxy does not forward it and replies with a 403 Forbidden message. If a request with a stale nonce is received, the proxy re-challenges, and indicates in the challenge that a stale nonce was received.

Responding with a 403 Forbidden message causes these actions:

- Prevents rogue users from sending requests
- Notifies the endpoint that an endpoint error has caused this
- Causes the endpoint to prompt for credentials

The re-challenge, indicating that a stale nonce was received, causes the endpoint to respond with stored credentials.

Emergency services and asserted identity

If the Request-URI of a request contains one of the administered emergency URIs, the proxy does not attempt to authenticate the request and does not assert identity.

These calls are logged on the proxy.

The request is not authenticated because some endpoints may respond by prompting a user for credentials, not an acceptable action in an emergency situation. Identity is not asserted and the Public Safety Access Point (PSAP) receives whatever identity is contained in the request.

p-asserted-identity header contents

The user identity, and SIP or SIPS URI resulting from authentication creates the p-asserted-identity header, which has the following format:

- If the user has a Communication Manager contact: "user identity"

  `<sip(s): nnnn@domain>`, where nnnn refers to the user's extension.
- Otherwise "user identity" `<sip(s): username@domain>`.

p-a-i header treatment—trusted source

The p-asserted-identity header is inserted into requests and 1xx and 2xx responses to requests that start a new dialog within the proxy's trust domain.

Requests arriving at the proxy from outside the proxy's authoritative domain only receive terminating processing.

p-a-i header treatment—untrusted source

Treatment of p-asserted-identity header for requests and 1xx and 2xx responses to requests to and from untrusted peers should be as explained in the discussions below.

Home proxy trusted peer case

If the request is from a trusted peer, a home proxy performs the following steps:

1. Examine the Route headers. Pop and remember the local Routes. If there are Route headers for other servers, perform normal SIP proxy.
2. If there is an originating phase indication in the local Route, and if there is a p-asserted-identity header, and the asserted user is local, Communication Manager does one of these two things:
   - If the user has a Communication Manager Contact, forward the request to the Communication Manager with the originating information requested in Route header.

     otherwise
   - Treat the call like the terminating case covered in step 4 below.

3. If there is an originating phase indication in the top Route header, but the identity is not local, or there is no asserted identity:
    a. The request is rejected with a 403 Forbidden response. This scenario would only arise if requests are hauled back to the home proxy for authentication in the visiting user case.
4. If there is a terminating phase indication in the local Route, and the user identified by the Request-URI is local (local user, alias or recognized by digit map):
    - If the user has a Communication Manager Contact, forward the request to the Communication Manager with terminating indication in Route header.

      otherwise
    - Treat the request as in the endpoint phase case described in step 6 below.
5. If there is a terminating phase indication in the local Route, and the user identified by the Request-URI is not local:
    - Insert Route header: `sip:terminatinguser@domain;phase=terminating`

      and
    - Send the request to the Edge proxy by pushing another Route header for the edge itself onto the request.
6. If there is an endpoint phase indication in the local Route:
    - If the user identified by the Request-URI is local, forward the request to the dynamically registered non-Communication Manager Contacts, parallel forking as per the Contacts.

      otherwise
    - Respond with an error (404).
7. If there is no phase indication in the local Route header, process as though the phase indication was terminating (this request came from outside but through the edge proxy).

Edge proxy trusted peer case

If the request is from a trusted peer, presumably a home proxy, an edge proxy performs the following steps:

1. Pop any Route headers that identify the edge proxy.
2. Route the call based on the Request-URI or remaining top Route header. If this identifies a user in a domain for which this edge is authoritative, route the call to the home of the user specified in the Route header by pushing a Route for the home proxy. If the top Route header identifies a known user, the edge should not pop the header (or it should push it back before routing onward).

The above changes can also be used to route REGISTER and other messages from a telephone through a visiting proxy to the home proxy of a user. This capability is deferred to a future release.

Since Communication Manager always tries to route the digits it received from SES, it returns a failure response if the numbers can not be routed. It is assumed that each Communication Manager knows how to route the calls to users on all the other Communication Managers, that is, a uniform dial plan. This can be either through non-SIP trunks or through SIP trunks. In other words, if a user cannot dial a number from the physical OPTIM set, that user cannot dial that number from OPS either.

p-preferred-identity header

Requests carrying the p-preferred-identity header

If the p-preferred-identity is present in a request, the proxy uses it to determine the user's domain for authentication, otherwise, it uses the From header.

The p-preferred-header indicates which identity the user prefers, and should contain the user's domain within its contents.

Privacy header

Behavior based on privacy header

If the privacy header has a value of **none**, or if there is no privacy header, the proxy should not remove the p-asserted-identity header from the request. If a request contains a privacy header with a value of **id**, the proxy must remove all p-asserted-identity headers from requests prior to forwarding to untrusted entities.

The privacy header indicates the privacy preferences of the user and is inserted by the endpoint or Communication Manager. If a user wishes to remain anonymous, his or her identity can still be authenticated and asserted, while maintaining anonymity. This is similar to caller-ID blocking. However, 100% anonymity is not granted since the proxy does not remove IP addresses in contact header or any other information from the request, only the p-asserted-identity header.

RFC 3325 recommends that the p-asserted-identity header remain in a request in order to prevent loss of services based on asserted identity. However, if explicitly required by the privacy header, anonymity should be granted.

Forwarding of requests

Remove p-preferred-header prior to forwarding

Upon receipt by the proxy of the p-preferred-identity header in a request, it should be removed from the request prior to forwarding.

The p-preferred-identity header is not necessary after the preferred identity has been authenticated and asserted.

Forwarding of request to trusted node

If the proxy is forwarding a request to a trusted node, the p-asserted-identity header must remain in the request.

The node is trusted to maintain the authenticity of the header contents.

Forwarding of request to untrusted node

If the proxy is forwarding a request to an untrusted node, the proxy must keep the p-asserted-identity header unless there is a privacy header with **id** token.

Sending the asserted identity to an untrusted node may result in misuse of the identity.

Origination/Capability-based routing

Re-write request URI

Prior to forwarding a request to Communication Manager, the proxy shall rewrite the Request URI in canonical form in all cases where it is able to do so.

Communication Manager cannot interpret user handles. In addition to providing this conversion for p-a-i, the conversion must also be applied to the Request URI.

FNU requirements

The following sections describe how feature notification unit (FNU) requirements are implemented:

- Directed Call Pickup FNU on page 95
- Extended Call Pickup FNU on page 95
- Calling Party Number Block FNU on page 96
- Calling Party Number Unblock FNU on page 97
- Dial Intercom FNU on page 97
- Drop FNU on page 98
- Exclusion FNU on page 98
- Off-PBX Call FNU on page 99
- Last Number Dialed FNU on page 100
- Malicious Call Trace FNU on page 100
- AUDIX One-Step Recording FNU on page 100

- Priority Call FNU on page 101
- Send All Calls FNU on page 102
- Transfer to Voice Mail FNU on page 103
- Whisper Page Activation on page 103

Directed Call Pickup FNU

Directed Call Pickup allows the user to answer a call ringing at another extension without having to be a member of a pickup group.

Directed Call Pickup FNU Structure:

```
INVITE sip:1111@example.com;avaya-cm-fnu=call-pickup-directed;avaya-cmextension=3333
SIP/2.0
```

```
INVITE sip:1111@example.com;avaya-cm-fnu=call-pickup-directed SIP/2.0
```

Parameters:

Name	Values	Req/Opt	PPM
avaya-cm-extension	The Communication Manager extension where the call is alerting.	O	No

Authorization: The endpoints need not be members of a group, but directed call pickup must be authorized by the class of restriction for both endpoints.

Communication Manager button: dir-pkup

Feature package: No

SDP required: Yes

Extended Call Pickup FNU

Extended Group Call Pickup allows a user to answer calls directed to another call pickup group.

Extended Group Call Pickup FNU structure:

```
INVITE sip:1111@example.com;avaya-cm-fnu=call-pickup-extended;avaya-cm-pickupnumber=3
SIP/2.0
```

```
INVITE sip:1111@example.com;avaya-cm-fnu=call-pickup-extended SIP/2.0
```

Parameters:

Name	Values	Req/Opt	PPM
avaya-cm-pickup-number	The pickup number from 1 to 24.	O	No

Authorization: The endpoint must be a member of a pickup group, and that pickup group must be a member of an extended pickup group, which must also include the group of the endpoint whose telephone is being picked up.

Communication Manager button: None. Accessed on the Communication Manager only via an FAC.

Feature package: No

SDP required: Yes

Calling Party Number Block FNU

Calling Party Number Block blocks the sending of the calling party number for one call.

Calling Party Number Block FNU structure:

```
INVITE
sip:1111@example.com;avaya-cm-fnu=calling-party-block;avaya-cmdestinat
ion=4444444 SIP/2.0
```

```
INVITE sip:1111@example.com;avaya-cm-fnu=calling-party-block SIP/2.0
```

Parameters:

Name	Values	Req/Opt	PPM
avaya-cm-destination	Any number within the Communication Manager dial plan to which this call is being directed.	O	No

Authorization: None

Communication Manager button: cpn-blk

Feature package: No

SDP required: Yes

Calling Party Number Unblock FNU

Calling Party Number Unblock deactivates calling party number (CPN) blocking and allows the CPN to be sent for a single call.

Calling Party Number Unblock FNU structure:

```
INVITE
sip:1111@example.com;avaya-cm-fnu=calling-party-unblock;avaya-cmdestin
ation=
```

```
4444444 SIP/2.0
```

```
INVITE sip:1111@example.com;avaya-cm-fnu=calling-party-unblock SIP/2.0
```

Parameters:

Name	Values	Req/Opt	PPM
avaya-cm-destination	Any number within the Communication Manager dial plan to which this call is being directed	O	No

Authorization: None

Communication Manager button: cpn-unblk

Feature package: No

SDP required: Yes

Dial Intercom FNU

Dial Intercom places a call to the station associated with the button. The called user receives a unique alerting indication. The endpoint extension and destination extension must be in the same intercom group. This feature is exactly like Automatic Intercom except for the way that the dial code is specified. PPM can provide the dial code for Automatic Intercom, but not for Dial Intercom.

Dial Intercom FNU structure:

```
INVITE sip:1111@example.com;avaya-cm-fnu=dial-intercom;avaya-cm-group=9;avayacm-
dial-code=12 SIP/2.0
INVITE sip:1111@example.com;avaya-cm-fnu=dial-intercom;avaya-cm-group=9 SIP/2.0
```

Parameters:

Name	Values	Req/Opt	PPM
avaya-cm-group	Any number within the Communication Manager dial Intercom group number from 1 to 32.	M	Yes
avaya-cm-dial-code	1- or 2-digit number	O	No

Authorization: An endpoint can use this FNU for a intercom group that matches an administered Communication Manager button for this extension.

Communication Manager button: dial-icom Grp: 9

Feature package: No

SDP required: Yes

Drop FNU

Drop FNU allows users to drop calls. Users can drop calls from automatic hold or drop the last party they added to a conference call.

Drop FNU structure:

```
INVITE sip:1111@example.com;avaya-cm-fnu=drop SIP/2.0
```

Parameters: None

Authorization: None

Communication Manager button: drop

Feature package: No

SDP required: No

Exclusion FNU

Exclusion allows multi-appearance telephone users to keep other users with appearances of the same extension from bridging onto an existing call. If the user activates the Exclusion button while other users are already bridged onto the call, the other users are dropped.

There are two ways to activate Exclusion.

- Manual Exclusion—when the user presses the exclusion button (either during dialing or during the call)
- Automatic Exclusion—as soon during a call, the user presses the exclusion button

Exclusion FNU structure:

```
INVITE sip:1111@example.com;avaya-cm-fnu=exclusion
       ;avaya-cm-action=on SIP/2.0
INVITE sip:1111@example.com;avaya-cm-fnu=exclusion
       ;avaya-cm-action=off SIP/2.0
```

Parameters:

Name	Values	Req/Opt	PPM
avaya-cm-action	on or off	O	No

Authorization: This request always applies to the endpoint's own extension. Automatic exclusion must be authorized by the extension's class of service.

Description:

Communication Manager button: exclusion

Feature package: No

SDP required: No

Off-PBX Call FNU

This FNU provides the capability to enable and disable the extending of an EC500 call.

Off-PBX Call FNU structure:

```
INVITE sip:1111@example.com;avaya-cm-fnu=off-pbx;avaya-cm-action=on SIP/2.0
INVITE sip:1111@example.com;avaya-cm-fnu=off-pbx;avaya-cm-action=off SIP/2.0
```

Parameters:

Name	Values	Req/Opt	PPM
avaya-cm-action	on or off	M	No

Authorization: This request always applies to the endpoint's own extension.

Communication Manager button: ec500

Feature package: Yes

SDP required: No

Last Number Dialed FNU

Last Number Dialed (redial) originates a call to the number last dialed by the station.

Last Number Dialed FNU structure:

```
INVITE sip:1111@example.com;avaya-cm-fnu=last-number-dialed SIP/2.0
```

Parameters: None

Authorization: None

Communication Manager button: last-numb

Feature package: No

SDP required: Yes

Malicious Call Trace FNU

Malicious Call Trace Activation sends a message to the MCT control extensions stating that the user wants to trace a malicious call. MCT activation also starts recording the call, if the system has a MCT voice recorder.

Malicious Call Trace FNU structure:

```
INVITE sip:1111@example.com;avaya-cm-fnu=mct SIP/2.0
```

```
INVITE sip:1111@example.com;avaya-cm-fnu=mct-cancel SIP/2.0
```

Parameters: None

Authorization: Must be authorized by the endpoint’s class of restriction

Communication Manager button: mct-act (to activate). Only an FAC to cancel.

Feature package: No

SDP required: No

AUDIX One-Step Recording FNU

This feature allows a station user to start and end the recording of an in-progress conversation using the AUDIX system recording facility. Note that avaya-cm-extension is optional when avaya-cm-action is "off" (because a station can only have one of these buttons).

AUDIX One-Step Recording

```
INVITE sip:1111@example.com; avaya-cm-fnu=one-touch-recording;
avaya-cmextension=3333;avaya-cm-action=on SIP/2.0
INVITE sip:1111@example.com;avaya-cm-fnu=one-touch-recording;avaya-cmaction=off SIP/
2.0
```

Parameters:

Name	Values	Req/Opt	PPM
avaya-cm-action	on or off	M	No
avaya-cm-extension	The Communication Manager extension of an AUDIX hunt group	M	Yes

Authorization: An endpoint can use this FNU on another extension only if the endpoint has a Communication Manager button audix-rec button with a matching extension.

Communication Manager button: audix-rec Ext: 3333

Feature package: No

SDP required: No

Priority Call FNU

Priority Calling allows a user to place priority calls or change an existing call to a priority call.

Priority Call FNU structure:

```
INVITE sip:1111@example.com;avaya-cm-fnu=priority-call;avaya-cm-destination=4444444
SIP/2.0
```

```
INVITE sip:1111@example.com;avaya-cm-fnu=priority-call SIP/2.0
```

Parameters:

Name	Values	Req/Opt	PPM
avaya-cm-destination	Any number within the Communication Manager dial plan, to which this call is being directed	O	No

Authorization: None

Communication Manager button: priority

Feature package: No

SDP required: Yes

Send All Calls FNU

Send All Calls allows users to temporarily direct all incoming calls to coverage regardless of the assigned call-coverage redirection criteria.

Send All Calls of the endpoint's own (1111) extension FNU structure

```
INVITE sip:1111@example.com;avaya-cm-fnu=sac;avaya-cm-action=on SIP/2.0
INVITE sip:1111@example.com;avaya-cm-fnu=sac;avaya-cm-action=off SIP/2.0
```

Parameters:

Name	Values	Req/Opt	PPM
avaya-cm-action	on or off	M	No

Authorization: This example shows the use of this FNU on the endpoint's own extension. No authorization is required. See the next case for how to apply this feature to another extension.

Communication Manager button: send-calls Ext: (left blank)

Feature package: Yes

SDP required: No

Send All Calls of another endpoint's (2222) extension FNU structure

```
INVITE sip:2222@example.com;avaya-cm-fnu=sac;avaya-cm-action=on SIP/2.0
INVITE sip:2222@example.com;avaya-cm-fnu=sac;avaya-cm-action=off SIP/2.0
```

Parameters:

Name	Values	Req/Opt	PPM
avaya-cm-action	on or off	M	No

Authorization: An endpoint can use this FNU on another extension only if the endpoint has a "send-calls Ext: 2222" button administered on Communication Manager.

Description: Applied to another extension.

Communication Manager button: send-calls Ext: 2222

Feature package: Yes

SDP required: No

Transfer to Voice Mail FNU

Transfer to Voice Mail FNU allows coverage to transfer the caller to the original call recipient's AUDIX mail where the caller can leave a message.

Transfer to Voice Mail FNU structure:

```
INVITE sip:1111@example.com;avaya-cm-fnu=transfer-to-voicemail SIP/2.0
```

Parameters: None

Authorization: None

Communication Manager button: None. Accessed on the Communication Manager only by an FAC.

Feature package: No

SDP required: No

Whisper Page Activation

Whisper Page Activation allows a user to make and receive whisper pages. A whisper page is an announcement sent to another extension that is active on a call where only the person on the extension hears the announcement. Other parties on the call cannot hear the announcement.

Whisper Page Activation FNU structure:

```
INVITE sip:1111@example.com;avaya-cm-fnu=whisper-page;avaya-cm-extension=3333 SIP/2.0
INVITE sip:1111@example.com;avaya-cm-fnu=whisper-page SIP/2.0
```

Parameters:

Name	Values	Req/Opt	PPM
avaya-cm-extension	The Communication Manager extension to which you want to whisper	O	No

Authorization: The user must have a class of restriction (COR) that allows intra-switch calling to use whisper paging, and the extension to which you are whispering must not have blocked whispers.

Communication Manager button: whisp-act

Feature package: No

SDP required: Yes

Appendix B: Terminal requirements and features

This appendix has two major sections that discuss Communication Manager's terminal requirements, features, and feature interactions with respect to SIP.

- Terminals
- Features and feature interactions

Terminals

Avaya CM OPTIM requirements for 3.0

Outgoing From header

OPTIM formats the outgoing **From: URI** field in the call that leaves the switch from a non-SIP telephone to a SIP telephone. The From header is as follows:

Display parameter followed administered digits at authoritative URI. The digits depend on the configuration set option calling number style. There are two choices: **network** and **PBX**. **PBX** is the station extension. **Network** is the network station modified by either the public or the private number table. The domain is taken from the Network Regions screen. If this is not administered the default is `anonymous.unknown.domain`. For an incoming ISDN call terminating to an OPTIM OPS station, the display information comes from the display IE and the handle is from the calling number. The domain is as above.

Features and feature interactions

- Hold and Soft Hold
- Message Waiting Indication
- SCCAN
- Restricted and invalid number procedures

Hold and Soft Hold

These are a method for signaling to Communication Manager to place a call on soft rather than hard hold so that downstream telephone interactions work correctly.

Proprietary soft hold header

When a re-INVITE is received with the "P-Avaya-CM-Soft-Hold" header, the call is placed on soft hold rather than hard hold.

This is not inserted in re-INVITEs created by CM for transfer/conference because CM does not currently give any indication to endpoints that a call is being placed on hold.

Message Waiting Indication

MWI event reporting enhancement for OPTIM

OPTIM MWI lamp status includes reporting lamp status for users assigned to the associated "aut-msg-wt" button. The *Message-Account* parameter indicates the specific user's lamp being reported.

SCCAN

p-asserted-identity header contents/Motorola proxy

CM inserts a p-asserted-identity header into requests based on the contents of the From header.

Although it does not perform digest authentication, Communication Manager trusts requests coming from the proxy and therefore trusts the From header.

Restricted and invalid number procedures

Restricted number

If a call is placed to a number that is denied due to COS/COR or FRL restrictions, and the field **Restricted Number Dialed Intercept Treatment:** is **announcement**, Communication Manager inserts either the Name1 or Name2 value from the field **Restricted Number Dialed Display** in the Contact Header (display parameter).

Invalid number

If a call is placed to an invalid number and the field **Invalid Number Dialed Intercept Treatment:** is **announcement**, Communication Manager inserts either the Name1 or Name2 value from the field **Invalid Number Dialed Display** in the Contact Header (display parameter).

Selective drop

The mechanism for providing selective drop is implemented for conference by supporting the REFER method with the "BYE" option encoded as follows:

Refer-To: <sip:xxx@domain;transport=tls;method=BYE>

Full selective drop procedures will be implemented in a later release.

The Refer-To URI validates it is the same as the Request-URI (the last party added).

Glossary

A

access code
A dial code of 1 to 3 digits that activates a feature, cancels a feature, or accesses an outgoing trunk.

Access Security Gateway (ASG)
A software module that secures Avaya Global Services log in accounts on many Avaya servers. Each login attempt on these accounts is met with a one-time challenge string that must be answered with the correct one-time response.

American National Standards Institute (ANSI)
A professional technical association that supports standards for transmission, protocol, and high-level languages, and that represents the U.S. in the International Organization for Standards. ANSI standards are for voluntary use in the U.S.

Avaya Communication Manager
An open, scalable, highly reliable, and secure telephony application. Communication Manager provides user functionality and system management functionality, intelligent call routing, application integration and extensibility, and enterprise communications networking.

B

bearer channel (B-channel)
A 64-kbps channel or a 56-kbps channel that carries a variety of digital information streams. A B-channel carries voice at 64 kbps, data at up to 64 kbps, WebLM voice encoded at 64 kbps, and voice at less than 64 kbps, alone or combined. See also data channel (D-channel).

bus
A multiconductor electrical path that transfers information over a common connection from any of several sources to any of several destinations. *See also* packet bus; time-division multiplex (TDM) bus.

C

Call Detail Recording (CDR)
A file that uses software and hardware to record call data. CDR was formerly called Station Message Detail Recording (SMDR). *See also* Call Detail Recording utility (CDRU).

Call Detail Recording utility (CDRU)
Software that collects, stores, filters, and provides output of call detail records. *See also* Call Detail Recording (CDR).

carrier
An enclosed shelf that contains vertical slots that hold circuit packs.

central office (CO)
Telephone switching equipment that provides local telephone service and access to toll facilities for long distance calling.

channel	(1) A circuit-switched call. (2) A communications path that transmits voice and data. (3) In WebLM transmission, all the contiguous time slots or noncontiguous time slots that are necessary to support a call. For example, an H0-channel uses six 64-kbps time slots. (4) A digital signal-0 (DS0) on a T1 facility or an E1 facility that is not specifically associated with a logical circuit-switched call. *See also* data channel (D-channel).
circuit	(1) An arrangement of electrical elements through which electric current flows. (2) A channel or a transmission path between two or more points.
circuit pack	A circuit card on which electrical circuits are printed, and integrated circuit (IC) chips and electrical components are installed. A circuit pack is installed in a SSH carrier. One example is the TN2302.
Class of Restriction (COR)	A feature that allows up to 96 classes of call-origination restrictions and call-termination restrictions for telephones, telephone groups, data modules, and trunk groups. *See also* Class of Service (COS).
Class of Service (COS)	A feature that uses a number to specify whether telephone users can activate the Automatic Callback (ACB), Call Forwarding All Calls, Data Privacy, or Priority Calling features. *See also* Class of Restriction (COR).
CCITT	Comitte Consultatif International Telephonique et Telegraphique. *See* International Telecommunications Union (ITU).
communications system	A software-controlled processor complex that interprets dial pulses, tones, and keyboard characters, and makes the proper connections within the system and externally. The communications system consists of a digital computer, software, storage devices, and carriers, with special hardware to perform the connections. A communications system provides communications services for the telephones on customer premises and the data terminals on customer premises, including access to public networks and Point-to-Point Protocol (PPP)s. *See also* SSH.
Controlled Local Area Network (CLAN) circuit pack	A circuit pack (TN799B) in an Avaya DEFINITY port network (PN) that provides TCP/IP connectivity to adjuncts over Ethernet or Point-to-Point Protocol (PPP). The CLAN circuit pack serves as the network interface for a DEFINITY server. The CLAN terminates IP (TCP and UDP), and relays those sockets and connections up to the Avaya DEFINITY server.
Converged Communications Server (CCS)	Avaya's proxy server for Session Initiated Protocol (SIP), initially supporting instant messaging.
CPN	called-party number
CPN/BN	calling-party number/billing number
customer-premises equipment (CPE)	Equipment that is connected to the telephone network, and that resides on a customer site. CPE can include telephones, modems, fax machines, video conferencing devices, switches, and so on.

D

data channel (D-channel)	A 16-kbps channel or a 64-kbps channel that carries signaling information or data on an Integrated Services Digital Network Basic Rate Interface (ISDN-BRI) or Integrated Services Digital Network Primary Rate Interface (ISDN-PRI). *See also* bearer channel (B-channel).
data communications equipment (DCE)	Equipment on the network side of a communications link that makes the binary serial data from the source or the transmitter compatible with the communications channel. DCE is usually a modem, a data module, or a packet assembly/disassembly (PAD).
data module	An interconnection device between a Basic Rate Interface (BRI) or a Digital Communications Protocol (DCP) interface of the SSH, and the data terminal equipment (DTE) or data channel (D-channel).
data terminal	An input/output (I/O) device that has either switched access or direct access to a host computer or to a processor interface.
data terminal equipment (DTE)	Equipment that comprises the endpoints in a connection over a data circuit. In a connection between a data terminal and a host, the terminal, the host, and the associated modems or data modules comprise the DTE.
digital	The representation of information by discrete steps. Compare with *analog*.
Digital Communications Protocol (DCP)	A proprietary protocol that transmits both digitized voice and digitized data over the same communications link. A DCP link consists of two 64-kbps information (I) channels, and one 8-kbps signaling (S) channel. The DCP protocol supports two information-bearing channels, and thus two telephones or data modules. The I1 channel is the DCP channel that is assigned on the first page of the 8411 Station screen. The I2 channel is the DCP channel that is assigned on the analog adjunct page of the 8411 Station screen, or on the data module page.
dual-tone multifrequency (DTMF)	The touchtone signals used for in-band telephone signaling.
Dynamic Host Configuration Protocol (DHCP)	An IETF protocol (RFCs 951, 1534, 1542, 2131, and 2132) that assigns IP addresses dynamically from a pool of addresses instead of statically.

E

extension	A number from 1 digit to 5 digits that routes calls through a communications system. With a Uniform Dial Plan (UDP) or a main-satellite dialing plan, extensions also route calls through a Point-to-Point Protocol (PPP).

F

FNU	Feature notification unit.
FTP	File Transfer Protocol.
feature	A specifically defined function or service that the system provides

H

H.323
An International Telecommunications Union (ITU) standard for switched multimedia communication between a LAN-based multimedia endpoint and a gatekeeper. *See also* Session Initiated Protocol (SIP).

host computer
A computer that is connected to a network, and that processes data from data-entry devices.

I

IE
See information element (IE).

IEEE
See Institute of Electrical and Electronics Engineers (IEEE).

IETF
See Internet Engineering Task Force (IETF).

IM
Instant Messaging. The instant-messaging client software required for the Avaya Communication Manager release 2.0 or later is a version of the Avaya IP Softphone R5 and later, and the SIP Softphone R2 and later.

information element (IE)
The name for the data fields within an Integrated Services Digital Network (ISDN) Layer 3 message.

Institute of Electrical and Electronics Engineers (IEEE)
An organization that produces standards for local area network (LAN) equipment.

Integrated Services Digital Network (ISDN)
A public network or a Point-to-Point Protocol (PPP) that provides end-to-end digital communications for all services to which users have access. An ISDN uses a limited set of standard multipurpose user-network interfaces that are defined by the CCITT. Through internationally accepted standard interfaces, an ISDN provides digital circuit switching communications or packet switching communications within the network. An ISDN provides links to other ISDNs to provide national digital communications and international digital communications. *See also* Integrated Services Digital Network Basic Rate Interface (ISDN-BRI); Integrated Services Digital Network Primary Rate Interface (ISDN-PRI).

Integrated Services Digital Network Basic Rate Interface (ISDN-BRI)
The interface between a communications system and terminal that includes two 64-kbps bearer channel (B-channel)s for transmitting voice or data, and one 16-kbps data channel (D-channel) for transmitting associated B-channel call control and out-of-band signaling information. ISDN-BRI also includes 48 kbps for transmitting framing and D-channel contention information, for a total interface speed of 192 kbps. ISDN-BRI serves ISDN terminals and digital terminals that are fitted with ISDN terminal adapters. *See also* Integrated Services Digital Network Primary Rate Interface (ISDN-PRI).

Integrated Services Digital Network Primary Rate Interface (ISDN-PRI)
The interface between multiple communications systems that in North America includes 24 64-kbps channels that correspond to the North American digital signal-level 1 (DS1) standard rate of 1.544 Mbps. The most common arrangement of channels in ISDN-PRI is 23 64-kbps bearer channel (B-channel)s for transmitting voice and data, and one 64-kbps data channel (D-channel) for transmitting associated B-channel call control and out-of-band signaling information. With nonfacility-associated signaling (NFAS), ISDN-PRI can include 24 B-channels and no D-channel. *See also* Integrated Services Digital Network (ISDN); Integrated Services Digital Network Basic Rate Interface (ISDN-BRI).

International Organization for Standards
A worldwide federation of standards bodies who issue International Standards for technological, scientific, intellectual, and economic activity. The federation is called *ISO*, and the US representative to the federation is the American National Standards Institute (ANSI).

International Telecommunications Union (ITU)
An international organization that sets universal standards for data communications, including Integrated Services Digital Network (ISDN). ITU was formerly known as International Telegraph and Telephone Consultative Committee (CCITT).

International Telegraph and Telephone Consultative Committee
See International Telecommunications Union (ITU).

Internet Engineering Task Force (IETF)
One of two technical working bodies of the Internet Activities Board. The IETF develops new Transmission Control Protocol (TCP)/Internet Protocol (IP) (for example, TCP/IP) standards for the Internet.

Internet Protocol (IP)
A connectionless protocol that operates at Layer 3 of the Open Systems Interconnect (OSI) model. IP protocol is used for Internet addressing and routing packets over multiple narrowbands to a final destination. IP protocol works in conjunction with Transmission Control Protocol (TCP), and is usually identified as TCP/IP.

L

local area network (LAN)
A networking arrangement that is designed for a limited geographical area. Generally, a LAN is limited in range to a maximum of 6.2 miles, and provides high-speed carrier service with low error rates. Common configurations include daisy chain, star (including circuit-switched), ring, and bus.

M

MAC address (or MAC name)
A 48-bit number, uniquely identifying and programmed into each network interface card or device.

media server interface	A CLAN card in a media server.
MWI	messaging waiting indication.

N

NAME1	Legacy name, Latin characters, usually displayable, for example Eurofont and Kanafont encoding.
NAME2	UTF-8 encoding. Used for multibyte character sets such as Chinese ideograms Hiragana, Katakana, and Hangul
narrowband	A circuit-switched call at a data rate of 64 kbps or less. All switch calls that are not WebLM are considered to be narrowband. *Compare with* wide band.
network	A series of points, nodes, or stations that are connected by communications channels.
network region	Network Region is a flexible administrative concept. A network region is an attribute associated with Communication Manager resources. It is used for among other things resource allocation and security. For example, when an H.323, or SIP, endpoint requires a Gateway Resource to set up a talk path with a non-IP endpoint like a DCP telephone, Communication Manager checks the network region parameter to attempt to get that gateway resource from the same Network Region, that is, as near to the endpoint as possible, to minimize trunk usage and delay.
node	A switching point or a control point for a network. Nodes are either tandem or terminal. Tandem nodes receive signals, and pass the signals on. Terminal nodes originate a transmission path, or terminate a transmission path.
nonce	Random value sent in a communications protocol exchange, often used to detect replay attacks. This specifically refers to the use of random information inserted in a challenge for SIP digest authentication. The algorithms are essentially the same as for HTTP, and are described in RFC2617.

O

OATS	Origination and terminating signaling. Formerly known as origination-based call flow or W call flow. In a call flow diagram, describes the direction, initiation, and termination of signaling
off-PBX station (OPS)	A telephone that Avaya Communication Manager does not control, such as a cellular telephone or the home telephone of a user. The features of Communication Manager can be extended to an OPS through switch administration by associating the extension of the office telephone with the off-site telephone. NOTE: Session Initiated Protocol (SIP) endpoints are administered on Communication Manager as OPS.

Open Systems Interconnect (OSI)	A system of seven independent communication protocols defined by the International Organization for Standards or ISO. Each of the seven layers enhances the communications services of the layer below, and shields the layer above from the implementation details of the lower layer. In theory, this structure can be used to build communications systems from independently developed layers.
origination-based call flow	See OATS.
O/S	Operating System.

P

packet	A group of bits that is used in packet switching and that is transmitted as a discrete unit. A packet includes a message element and a control information element (IE). The message element is the data. The control IE is the header. In each packet, the message element and the control IE are arranged in a specified format.
packet assembly/ disassembly (PAD)	The process of packetizing control data and user data from a transmitting device before the data is forwarded through the packet network.The receiving device disassembles the packets, removes the control data, and then reassembles the packets, thus reconstituting the user data in its original form.
packet bus	A bus with a wide bandwidth that transmits packets.
packet switching	A data-transmission technique that segments and routes user information in discrete data envelopes that are called *packets*. Control information for routing, sequencing, and error checking is appended to each packet. With packet switching, a channel is occupied only during the transmission of a packet. On completion of the transmission, the channel is made available for the transfer of other packets.
PBX	private branch exchange. *See* SSH.
Plain Old Telephone Service (POTS)	Basic voice communications with standard, single-line phones accessing the public switched telephone network (PSTN).
Point-to-Point Protocol (PPP)	A standard (largely replacing SLIP) allowing a computer to use TCP/IP with a regular telephone line.
port	A data-transmission access point or voice-transmission access point on a device that is used for communicating with other devices.
private network	A network that is used exclusively for the telecommunications needs of a particular customer.
protocol	A set of conventions or rules that governs the format and the timing of message exchanges. A protocol controls error correction and the movement of data.
proxy trust domain	Includes those SIP servers and gateways, but not endpoints with identities administered on the SES.

public network	A network to which all customers have open access for local calling and long distance calling.
public switched telephone network (PSTN)	The public worldwide voice telephone network.

R

RAS	Remote Access Server (or in Microsoft Windows operating systems, Remote Access Service).
Real Time Transfer Protocol (RTP)	An Internet Engineering Task Force (IETF) protocol (RFC 1889) that addresses the problems that occur when video and other exchanges with real-time properties are delivered over a local area network (LAN) that is designed for data. RTP gives higher priority to video and other real-time interactive exchanges than to connectionless data.
RFA	Remote Feature Activation is a web-based application which is used to obtain Avaya authentication and licensing files.
RFC	Request for Comments designates Internet Engineering Task Force (IETF) standards that are drafts.
RNIS	Remote Network Implementation Services is a contract installation services group within Avaya Inc.
RPM	RedHat Package Manager
RSA	Remote Supervisor Adapter
RTC	Real Time Communication
RTCP	Real Time Control Protocol

S

Session Initiated Protocol (SIP)	A signaling protocol for Internet conferencing, telephony, presence, events notification, and instant messaging. SIP initiates call setup, routing, authentication, and other feature messages to endpoints within an IP domain. *See also* H.323; Voice over IP (VoIP).
SSH	Secure SHell is a protocol for secure remote login and other secure network services over an insecure network. It provides for server authentication, and data integrity with perfect port-forwarding secrecy.
SSL	Secure Socket Layer.
subscriber	A Session Initiated Protocol (SIP) subscriber is one of the following: a Converged Communications Server (CCS) host or other SIP node, a SIP user (per Contact), or a Media Server (running Avaya Communication Manager 2.0 or later).
switch	Any kind of telephone switching system. *See also* communications system.

T

TAC trunk-access code

TCP *See* Transmission Control Protocol (TCP).

TCP/IP *See* Internet Protocol (IP). *See also* Transmission Control Protocol (TCP).

tie trunk A telecommunications channel that directly connects two private switching systems.

time-division multiplex (TDM) bus A bus that is time-shared regularly by pre allocating short time slots to each transmitter. In a SSH, all Plain Old Telephone Service (POTS) circuits are connected to the time-division multiplex (TDM) bus, and any port can send a signal to any other port. *See also* time-division multiplexing (TDM).

time-division multiplexing (TDM) A form of multiplexing that divides a transmission channel into successive time slots. *See also* time-division multiplex (TDM) bus.

time slot In the SSH, a time slot refers to either a digital signal level-0 (DS0) on a T1 facility or an E1 facility, or a 64-kbps unit on the time-division multiplex (TDM) bus or fiber connection between port networks (PNs) that is structured as 8 bits every 125 microseconds.

Transmission Control Protocol (TCP) A connection-oriented transport-layer protocol, IETF STD 7. RFC 793, that governs the exchange of sequential data. Whereas the Internet Protocol (IP) deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data, and also guarantees that packets are delivered in the same order in which the packets are sent.

Transport Layer Security (TLS) An IETF standard (RFC 2246) to supersede Netscapes' Secure Socket Layer (SSL) and provide host-to-host data connections with encryption and certification at the transport layer.

trunk A dedicated communications channel between two communications systems or central office (CO)s.

trunk access code (TAC) A dial access code used to access a specific trunk.

trunk group Telecommunications channels that are assigned as a group for certain functions, and that can be used interchangeably between two communications systems or central office (CO)s.

W

W call flow See OATS.

Index

E

F

S

T

U

V

W