SIP Support

in

Avaya Communication Manager 2.1.1

running on the

Avaya S8300, S8500, or S8700 Media Server

555-245-206
Issue 2
September 2004

Notice

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

Warranty

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

Preventing Toll Fraud

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

Avaya Fraud Intervention

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

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 via this Avaya product (that is, "networked equipment").

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

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

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

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

Responsibility for Your Company's Telecommunications Security

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

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

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

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

TCP/IP Facilities

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

Standards Compliance

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

Product Safety Standards

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

Safety of Information Technology Equipment, IEC 60950, 3rd Edition 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

Safety Requirements for Customer Equipment, ACA Technical Standard (TS) 001 - 1997

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 operate within the following parameters:

- Maximum power output: -5 dBm to -8 dBm
- Center Wavelength: 1310 nm to 1360 nm

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 and EN55022:1998.

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
- Powerline Harmonics IEC 61000-3-2
- Voltage Fluctuations and Flicker IEC 61000-3-3

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.

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

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

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

Japan

This is a Class 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

SIP Support in Communication Manager

This chapter describes the support for SIP (Session Initiated Protocol) incorporated into Avaya Communication Manager 2.1.1 or later running an Avaya S8300, S8500 or S8700 Media Server.

Introduction to SIP

What is SIP?

SIP is the Session Initiation Protocol, an endpoint-oriented messaging standard 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), and it can support any type of communication session, whether the session's content is voice, video, or instant messaging (text).

As implemented by Avaya in Communication Manager, SIP "trunking" functionality will be available on any of the Linux-based media servers (S8300, S8500 or S8700). By means of having SIP-enabled endpoints managed by Communication Manager, many features can be extended to these endpoints. The media servers will function as Plain Old Telephone Service (POTS) gateways, and they will also support name/number delivery between and among the various non-SIP endpoints supported by Communication Manager (analog, DCP or H.323 stations and analog, digital or IP trunks) and new SIP-enabled endpoints, such as the Avaya 4602 SIP Telephone. In addition to its calling capabilities, the SIP-enabled version of IP Softphone R5 and later also includes Instant Messaging (IM) client software, while continuing its full support of the existing H.323 standard for call control.

How does SIP fit into Your System?

The support for SIP which is built into Avaya Communication Manager has the following attributes which help it fit easily into your system:

- It is built around published standards. These include both IETF Requests for Comments (RFCs) and Internet-Drafts. Some standards implemented in the Avaya SIP solution include (but are not limited to) the following:
  - 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)
  - Internet-Drafts of *The SIP 'Replaces' Header* and *Session Timers in the SIP*

- It integrates with traditional circuit-switched interfaces and IP-switched interfaces. This integration allows the user to evolve easily from the current 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, like 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.

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

SIP-Related Support

The additions made to support SIP in Avaya Communication Manager 2.x running on S8300, S8500 or S8700 media servers include what is described in the following section.

Trunking

Support for SIP trunks allows an enterprise to connect its media server(s) to the SIP-enabled proxy server, the Avaya Converged Communications Server (CCS), and through this proxy, optionally to an external SIP service provider, if desired. The trunk support in Communication Manager complies with SIP standards (e.g., IETF RFC 3261) and thereby will interoperate with any SIP-enabled endpoint/station which also complies with the standard.

In complex configurations with Avaya S8700 Media Server(s), the signaling-group properties in Communication Manager must be administered to match in certain ways. See SIP Trunk Engineering Notes on page 13.

Stations

Support for SIP stations using SIP trunks allows any fully compliant SIP phone to interoperate with Avaya phones. This means any SIP phone, from Avaya or a third party, that complies with the appropriate RFC or Internet-Draft standards will be able to:

- Dial and be dialed as an extension in the enterprise dial plan.
- Put calls on hold and participate in transfers and conference calls.
- Additionally, SIP stations administered in Communication Manager as Off-Premises station (OPS) stations support most Extended Access features, such as call park, call pick-up and priority calls. These features are activated by using station buttons which have been set up to dial special extensions (Feature Name Extensions). For more details, refer to the *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

Support is provided, if desired, for complete call detail records for all SIP calls based on their URIs.

Access Control

Support is provided for full access control to external trunks from any phone. Both SIP trunks and SIP endpoints require network access to a CCS. Note that some other means of access control, such as a firewall, typically would be required to control network access from outside of the enterprise (e.g., to the CCS and through it, to SIP trunks or SIP endpoints inside the enterprise).

Requirements for SIP

Software

Support for SIP can be enabled in Avaya Communication Manager 2.1.1 running on any Linux-based media server. The appropriate Avaya RFA licensing files are also required.

Hardware

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

- Avaya S8300 Media Server
- Avaya S8500 Media Server
- Avaya S8700 Media Server.
- NOTE: Any of these media servers also may control one or more Avaya media gateways.

All CLAN or processor CLAN IP interfaces must be configured correctly. For more details, refer to "*Administration for Network Connectivity for Avaya Communication Manager, 555-233-504"*.

Refer to the *Converged Communications Server Installation and Administration* document, Issue 2, DocID 555-245-705, for details on Avaya's SIP proxy, endpoint registration and instant-messaging (IM) server, which connects to media server(s) running Communication Manager and provides SIP-enabled applications such as enterprise IM using the client in Avaya IP SoftPhone R5 or later software.

Firmware

It is important to note that SIP standards dictate that Dual-Tone Multifrequency (DTMF) tones be supported within the Real-Time Transfer Protocol (RTP) data stream. Interoperability with certain third-party SIP-enabled devices may depend on this. This requirement further demands, for example, that the newest versions of Avaya's VoIP engine be installed throughout your system to support "rtp-payload."

NOTE:
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.

TN2302AP hardware/ firmware version	Circuit Pack w/1-digit HW vintage	Circuit Pack w/2-digit HW vintage
Minimum for SIP	V71 or V72	V71 or V72
Highly Recommended	V93	V93
In G700/G350 media gateways	V21 (or V22, with full support for facsimile in G.729 mode)	

SIP Trunk Engineering Notes

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

There is no physical "trunk" when using SIP. Therefore, there is no physical limit on how many calls (trunk members) can be set up using a particular signaling connection. (It is limited only by the total bandwidth available).

However, using the signaling group and trunk group administrative screens in Communication Manager also for SIP is useful, because doing so helps extend several Communication Manager features to SIP easily. Although Communication Manager normally limits signaling groups to 255 trunk members, thereby limiting each signaling connection 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. In other words, 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 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 2.1.1 compares the caller’s domain, as specified in the header of the SIP INVITE message, with the far-end domain(s) specified for the administered SIP signaling group(s). 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. Therefore, it is ***recommended*** that at least one SIP signaling group per signaling connection be administered with a blank domain in order to terminate 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 which have identical node names/ports, as well as the SIP trunks groups using each of these signaling groups, should be administered with identical properties (i.e., matching entries in the fields on administrative screens). Of course, different SIP signaling connections will differ with respect to their near-end and/or far-end node name(s)/port number(s), and they should therefore 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 three. You may administer more than three, but the run-time limit of simultaneous signaling connections is three. 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

Refer to the *Converged Communications Server Installation and Administration* document, Issue 2, DocID 555-245-705, for details on the SIP proxy server. Refer to online help for Avaya IP SoftPhone R5 for details on setting up and using it for SIP Instant Messaging. Refer to the following documentation for details on setting up and using for your Avaya 4602 SIP Telephone as a station for SIP voice calling:

- *4602 SIP Telephone User's Guide* (16-300035, Issue 2, September 2004)
- *4602 SIP Telephone Administrator's Guide* (16-300037, Issue 2, September 2004)
- *4602 SIP Telephone Quick Setup Guide* (16-300158, Issue 2, September 2004).

For an overview of the different components and their associated tasks supporting Avaya's SIP solution, refer to the *SIP Implementation Guide* (16-300140, Issue 1, September 2004).

Setup and Configuration

Administration

To administer SIP trunks in Avaya Communication Manager 2.1.1, perform the following tasks:

1. Verify that your system supports and is correctly configured for IP connectivity. Refer to *Administration for Network Connectivity for Avaya Communication Manager,* 555-233-504
2. On the ***System-Parameters Customer-Options screen on page 38***:
   a. Verify that the "IP Trunks?" field on page 4 is set to **y** (controlled by the license file).
   b. Verify the license-authorized value from **0-100** (for S8300) or **0-800** (for S8500) or **0-1000** (for S8700) in the "Maximum Administered SIP Trunks:" field on page 2.
3. Enter the valid hostname and IP Address for any Converged Communications Server (CCS) on your network in the corresponding fields on the ***IP Node Names*** screen.
4. Enter the fully qualified name or IP address of the domain for which this network region applies in the "Home Domain:" field on the ***IP Network Region screen on page 34***. A valid entry in this field is required for SIP endpoints on Communication Manager to call the public network. Note that this Home Domain must exactly match the Domain on the Edit System Properties screen set via the Master Administration Web Interface on CCS. In a single-CCS (combined Home/Edge server) configuration, exactly one Home Domain is set (e.g., company.com). In a multiple-CCS configuration (i.e., an Edge and one or more Home servers), each Home CCS may have its own Home Domain (e.g., east.company.com and west.company.com).
5. On the ***Feature-Related System Parameters screen on page 33***, select **all** in the "Trunk-to-Trunk Transfer?" field to enable the transfer and conference features to operate correctly with SIP.
6. On the ***Signaling Group screen on page 17***:
   a. Enter **sip** in the "Group Type:" field . A new screen for SIP groups will be displayed.
   b. Verify that the "Transport Method:" field displays the default value of **tls** (TLS).
   c. The "Trunk Group for Channel Selection:" field may be set to the default of blank.
   d. 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 S8300 media servers, the value of this entry is typically **procr**. For the S8700, it is the node name for the selected CLAN interface.
   e. Ensure the recommended TLS port value **5061** is set in the "Near-End Listen Port:" field.
   f. Enter the name of the node you administered for the SIP proxy server in step 3 in the "Far-end Node Name:" field.
   g. Enter the recommended TLS port value of **5061** in the "Far-End Listen Port:" field.
   h. 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.
   i. Enter the domain name or IP address of a server to which calls should be routed in the "Far-End Domain:" field. For example, one group could be set to route SIP calls within your enterprise to an Avaya Converged Communications Server on your LAN, and another group set to route calls through your SIP service provider's far-end domain.
   j. 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.

7 On the ***Trunk Group*** screen, illustrated on pages 18-32:

- **a** Enter **sip** in the "Group Type:" field . A new screen for SIP groups will be displayed.
- **b** Depending on your needs related to call-detail recording, enter **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** Enter the number of the SIP signaling group you previously administered in the "Signaling Group:" field.
- **d** Enter a value of 0-255 for the number of SIP trunks belonging to this group in the "Number of Members:" field. NOTE: The sum total number of all SIP trunks specified for all groups must be less than or equal to the value entered in the "Maximum Administered SIP Trunks:" field on the ***System-Parameters Customer-Options screen on page 38***.
- **e** On the ***Trunk Group screen, page 2***, you should set both the "Send Name:" and "Send Calling Number:" fields to **y** (to allow SIP users on Communication Manager to call the public network) and verify the entries in the "Numbering Format:" and (optionally) "Send Connected Number:" fields.
- **f** Group Member Assignments are automatically completed and displayed on the ***Trunk Group screen, page 6***, and any subsequent pages necessary, based on the values that you entered on the ***Trunk Group screen, page 1***. Members cannot be administered individually; all members of each administered group will share the same characteristics.
- **g** Repeat the preceding Step a through Step f for each SIP trunk group you wish to assign, up to your media server's trunk- number limit.

8 The final step before you can make SIP calls from endpoints connected to Avaya Communication Manager is to administer call routing properly in Communication Manager 2.x.

On the ***Route Pattern screen on page 36***, verify that the "Secure SIP?" field is set to the default value of **n** for routing through a public network; an entry of **y** for yes is not supported. Most SIP endpoints do not support end-to-end secure traffic yet. Optionally on that screen, you may enter a value of **p** in the "Insert Digits" field to insert a + (plus sign) into a digit string.

Example Using AAR as an example, first ensure that the "Auto Alternate Routing (AAR) Access Code:" field is set to the proper value on the ***Feature Access Code*** screen. Then you would administer both the ***AAR Digit Analysis Table*** and the ***Numbering -- Private screen on page 35*** and/or ***Numbering -- Public/Unknown screen on page 35*** to ensure that dialed strings of digits will be interpreted correctly and the resulting calls routed appropriately using the SIP trunks which you administered in Step 7. (Note that you may not access a SIP trunk via a dialed TAC.)

For more details on all the screens that may be used in the administration of routing, refer to the *"Administrator's Guide for Avaya Communication Manager*," Issue 8, DocID 555-233-506.

9 On the ***Locations screen on page 34***, enter the appropriate "Proxy Selection Route Pattern" in the field corresponding to each location employing a SIP proxy server in routing SIP traffic.

10 (Optional) In Avaya Communication Manager 2.1.1, you can manage the resources supporting your SIP endpoints on the ***IP Address Mapping screen*** (using the ip-network-map command). This is important in distributed Communication Manager environments in which network bandwidth may be consumed unnecessarily for calls among SIP and other endpoints. This screen can also be used to allow the system to properly identify the location of a caller who dials a 911 emergency call from a SIP endpoint. For more information, see the Screen Reference chapter in the "*Admininstrator's Guide for Avaya Communication Manager*," Issue 8, Doc ID 555-233-506.

SIP Administrative Screens

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

- *Signaling Group screen* (when the new value of **sip** is entered in the "Group Type:" field)
- Trunk Group screens (when the new value of **sip** is entered in the "Group Type:" field).

In addition, SIP-related fields on Other Administrative Screens may also need to be administered.

Signaling Group screen

The following screen is displayed when **sip** is entered in the "Group Type:" field on page 1:

```
                                                                Page 1 of 5
                              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
                                                       IP Audio Hairpinning? y
```

Signaling Group field descriptions

The following fields are displayed when **sip** is entered in the "Group Type:" field on page 1:

Group Number

A display-only field identifying the signaling group.

Group Type

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

Valid entries	Usage
sip	Use for SIP on the Avaya S8300, S8500, S8700 IP-Connect, or S8700 Multi-Connect Media Servers only.

Transport Method

Appears only when the value of the entry in the "Group Type:" field is **sip**. Ensure that the default of TLS is selected in this field. If not, results will be unpredictable.

Valid entries	Usage
tls	Default and recommended (secure) transport method is TLS.
tcp	***WARNING:*** TCP may be used only for debugging purposes.

Near-end Node Name

Appears when the value of the entry in the "Group Type:" field is **h.323** or **sip**. Enter 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.	Describe the near-end node.

Far-end Node Name

Appears when the value of the entry in the "Group Type:" field is **h.323** or **sip**. Enter 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.	Describe 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 three using TLS. If you administer more than three 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 do match, you may administer as many identical SIP signaling groups using TLS as desired.

Near-end Listen Port

Appears when "Group Type:" is **h.323** or **sip**. Defaults to 5061 for SIP over TLS.

Valid entries	Usage
5000-9999	Enter an unused port number. The recommended port for SIP over TLS is 5061.

Far-end Listen Port

Appears when the Group Type field is **h.323** or **sip**.

Valid entries	Usage
1-65535	Enter the same number as entered in the Near-end Listen Port field. The recommended port entry is 5061 for SIP over TLS.

Far-end Network Region

Appears when the Group Type field is **h.323** or **sip**. The number of the network region that is assigned to the far-end of the trunk group.

Valid entries	Usage
1-250 or blank	Enter the network region number that is assigned to the far end of the trunk group. The region 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

Appears only when the value of the entry in the "Group Type:" field is **sip**.

Valid entries	Usage
Max. 40-character string, or leave 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, it could be that of your SIP service provider. If blank, the far-end IP address is used.

Bypass If IP Threshold Exceeded

Appears when the Group Type field is **h.323** or **sip**.

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

DTMF over IP

Appears when the value of the entry in the "Group Type:" field is **h.323** or **sip**.

Valid entries	Usage
rtp-payload	SIP Trunks require the entry of **rtp-payload**.

Direct IP-IP Audio Connections

Appears when the value of the entry in the "Group Type:" field is **h.323** or **sip**. For SIP trunk groups, this allows direct audio connections between SIP endpoints.

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

IP Audio Hairpinning

Appears when the Group Type field is **h.323** or **sip**. 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 TDM bus.

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

Trunk Group screen, page 1

The following screen is displayed when **sip** is entered in the "Group Type:" field on page 1:

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

 Group Number: ___                  Group Type: sip_____      CDR Reports: _
   Group Name: ___________________________ COR: __       TN: ___      TAC: ____
    Direction: ________        Outgoing Display? _
  Dial Access? _                 Busy Threshold: ___        Night Service: ________
 Queue Length: ___
 Service Type: _____       Auth Code? _
                                            Signaling Group: ___
                                          Number of Members: ____
 TRUNK PARAMETERS







                                        Digital Loss Group: ___
```

Trunk Group field descriptions

The following fields are displayed when **sip** is entered in the "Group Type:" field on page 1:

Group Number

This field displays the group number assigned when the trunk group was added..

Group Type

Enter the type of trunk group.

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

Valid entries	Usage
y	All outgoing calls on this trunk group will generate call detail records. If the "Record Outgoing Calls Only?" field on the ***CDR System Parameters*** screen is **n**, then incoming calls on this trunk group will also generate call detail records.
n	Calls over this trunk group will not generate call detail records.
r (ring-intvl)	CDR records will be generated 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

Valid entries	Usage
1 to 27 characters	Enter a unique name that provides information about the trunk group. Don’t 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, Level3 SIP, etc.

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. Refer to Chapter 5 of the "*Avaya Toll Fraud and Security Handbook*," 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 (FRL) are assigned to classes of restriction. Even if 2 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

Valid entries	Usage
1 to **100**	Enter a Tenant Partition number to assign this trunk group to the partition.

Tip:

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

TAC

Enter the trunk access code (TAC) for each trunk group. A different TAC must be assigned to each trunk group. CDR reports use the TAC to identify each trunk group.

Valid entries	Usage
1- to 4-digit number	Enter 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 via TAC; the TAC you enter here is used only to identify them on CDR reports.
***, #**	* and # may be used as the first character in a TAC.

Outgoing Display

This field allows display phones 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're 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
y	Allows users to access the trunk group by dialing its access code. NOTE: This entry is not available for SIP trunks.
n (Display only for SIP trunks)	Does not allow users to access 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

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
1 to **255**	Enter 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, enter **25**.

Night Service

This field sets the destination to which incoming calls go when Night Service is in operation. If a Night field on the Group Member Assignments page is administered with a different destination, that entry will override 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: otherwise some features won't work correctly, even over 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)	Enter 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 enter 0, callers receive a busy signal when no trunks are available. If you enter a higher number, a caller hears 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 will call the extension that placed the original call. The caller will hear 3 short, quick rings. The caller doesn't need to do anything but pick up the handset and wait: Communication Manager remembers the number the caller dialed and automatically completes the call.

This field appears when the Direction field is **outgoing** or **two-way**.

Valid entries	Usage
0	Enter 0 for DCS trunks. This entry is not applicable for SIP.
1 to **100**	Enter the number of outgoing calls that you want to be held waiting when all trunks are busy.

Service Type

Indicates the service for which this trunk group is dedicated. The following table provides a listing of predefined entries. 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 tandemed outgoing calls at your server running Communication Manager. This field appears if the Direction field is incoming or two-way, and it can only be **y** if the Authorization Codes field is **y** on the *System-Parameters Customer-Options screen on page 38*.

Valid entries	Usage
y/n	Enter **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

Appears only when the value of the entry in the "Group Type:" field is **sip**.

Valid entries	Usage
1-650	Enter the number of the SIP signaling group associated with this trunk group on the ***Signaling Group screen on page 17***.

Number of Members

Appears only when the value of the entry in the "Group Type:" field is **sip**.

Valid entries	Usage
1-255	Enter 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 adminstrable.

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 **17**	Shows the index into the loss plan and tone plan.

Trunk Group screen, page 2

The following screen is displayed when **sip** is entered in the "Group Type:" field on page 1:

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

                                Send Name: n     Send Calling Number: y

                     Numbering Format: public_



                                         Replace Unavailable Numbers? n
                                               Send Connected Number: n
```

Trunk Group field descriptions, cont.

The following fields are displayed on page 2 when **sip** is entered in the "Group Type:" field on page 1:

ACA Assignment

Valid entries	Usage
y/n	Enter **y** if you want Automatic Circuit Assurance (ACA) measurements to be taken for this trunk group. If **y** is entered, complete the Long Holding Time, Short Holding Time, and Short Holding Threshold fields.The default entry for SIP is **n**.

Measured

Indicates 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) or the VuStats 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**. If this field contains a value other than **internal** or **none** when ATM is **y**, **none** appears.

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

Maintenance Tests

Appears when the value of the Group Type field is **aplt**, **isdn**, **sip** or **tie**.

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

Send Name

Specifies whether the calling/connected/called/busy party's administered name is sent to the network on outgoing/incoming calls. In general, the valid entries are **y**, **n**, or **r** (restricted). For SIP, if the value in this field is set to the default of **n** or to **r**, then the calling/connected name of "anonymous" will be sent by Avaya Communication Manager for the display name.

NOTE:
If name information is not administered for the calling station or the connected/called/busy station, then the extension number is sent in place of the name.

Send Calling Number

Specifies whether the calling party's number is sent on outgoing or tandemed calls. Valid entries are **y**, **n**, or **r** (restricted).If the value is **r**, the calling number for display is "presentation restricted". For SIP trunks, entry of the default value of **n** or of **r** behave identically. If it has been set to **y**, then the ***Numbering - Public/Unknown Format*** screen is accessed to construct the actual number to be sent, or the ***Numbering-Private*** screen (based on the entry in the Numbering Format field) is used. The ***Numbering - Public/Unknown Format*** screen is used to manipulate only when Send Calling Number is set to **y** for any administrable block of extensions.

Numbering Format

This field appears if the Send Calling Number field is **y** or **r** or the Send Connected Number field is **y** or **r**. This specifies the encoding of Numbering Plan Indicator for identification purposes in the Calling Number and/or Connected Number IEs, and in the QSIG Party Number. Valid entries are **public**, **unknown**, **private**, and **unk-pvt**. **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 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. An entry of **unk-pvt** also determines the Type of Number from the Private-Numbering screen, but the Numbering Plan Indicator is unknown.

Replace Unavailable Numbers

Appears when the Group Type field is **isdn** or **sip**. Indicates whether to replace unavailable numbers with administrable strings for incoming and outgoing calls assigned to the specified trunk group. This field applies to BRI/PRI and SIP trunks.

Valid entries	Usage
y/n	Enter **y** for the display to be replaced regardless of the service type of the trunk. The default entry for SIP trunks is **n**.

Send Connected Number

Appears if the QSIG Value-Added field on the Trunk Group screen is **n**. Specifies if the connected party’s number is sent on incoming or tandemed calls. Valid entries are **y**, **n**, or **r** (restricted). If **y** is entered, the ***Numbering - Public/Unknown Format*** screen is accessed to construct the actual number sent, or the ***Numbering-Private*** screen (based on the entry in the "Numbering Format:" field) is used. For SIP trunks, if the value is the default entry of **n**, or is **r**, then the connected number sent by Communication Manager is “anonymous”.

NOTE:
The AT&T Switched Network Protocol does not support restricted displays of connected numbers. Therefore, if you administer the 1a country-protocol/protocol-version combination on the DS1 screen, you should not administer the Send Connected Number field to **r** (restricted) on the ISDN Trunk Group screen, as this causes display problems.

NOTE:
The Numbering - Public/Unknown Format screen will allow you to specify or alter the Send Connected Number field’s value for any administrable block of extensions only if the entry in the Send Connected Number fiedd is set to **y** (yes).

Trunk Group screen, pages 3-5

The following screen is displayed when **sip** is entered in the "Group Type:" field on page 1:

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

Trunk Group field descriptions, cont.

The following fields are displayed on page 3 when **sip** is entered in the "Group Type:" field on page 1:

Service/Feature

Specifies the Services/Features for an incoming call type. See the Service Type field description for a list of predefined Services/Features that can be received. Or, use Type 0, Type 1, and Type 2 user defined services. The identifier **other** can be used for any Services/Features not explicitly specified, for example, for SIP trunk groups.

Called Len

Specifies the number of digits received for an incoming call. A blank entry is used as a “wild card” entry and, when used, means that any length of digits associated with the specified Service/Feature can match in this field. Valid entries are **0** to **21**, or leave blank.

Called Number

Specifies the leading digits received for an incoming call. A blank entry is used as a “wild card” entry and, when used, means that any number associated with the specified Service/Feature can match in this field. Valid entries are up to 16 digits, or leave blank.

Del

Specifies 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 are **1** to **21**, **all**, or leave blank.

Insert

Specifies the digits to be prepended to the front of the remaining digits after any (optional) digit deletion has been performed. The resultant number formed from digit deletion/insertion is used to route the call, provided 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.

Trunk Group screen, page 6

The following screen is displayed when **sip** is entered in the "Group Type:" field on page 1:

```
add trunk-group next                                            Page 6 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. These fields are automatically populated and displayed based on the number of members of SIP trunk groups specified on page 1 of this screen. 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.

Trunk Group field descriptions, cont.

The following fields are displayed on page 4 when **sip** is entered in the "Group Type:" field on page 1:

Administered Members (min/max)

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

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

This 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 which must be administered to support SIP trunking, various fields on the following screens in Communication Manager are also related to SIP:

- ***Feature-Related System Parameters screen*** (change to field name)
- ***IP Address Mapping screen on page 33*** (now supports SIP endpoints, as well as H.323)
- ***IP Network Region screen on page 34*** (added "Home Domain:" field)
- ***Locations screen on page 34*** (added "Proxy Selection Route Pattern" fields)
- ***Numbering -- Private screen on page 35*** (changed name from "ISDN Numbering -- Private")
- ***Numbering -- Public/Unknown screen on page 35*** (changed name from "ISDN Numbering -- Public/Unknown")
- ***Route Pattern screen on page 36*** (added "Secure SIP?" field)
- ***System Capacity screen on page 37*** (added a row for "SIP Trunks (included in 'Trunk ports'):")
- ***System Parameters Call Coverage / Call Forwarding screen on page 37*** (added "Disable call classifier for CCRON over SIP trunks?" field to page 2).
- ***System-Parameters Customer-Options screen on page 38*** (added "Maximum Administered SIP Trunks:" field).

Feature-Related System Parameters screen

The change is highlighted in **bold** on this 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?
```

NOTE:
The "Trunk-to-Trunk Transfer?" field must be set to **all** to support the SIP transfer feature.

IP Address Mapping screen

This screen defines feature characteristics that depend on the IP address.

```
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:
This screen can now be used to help allocate resources for both H.323 and SIP endpoints.

IP Network Region screen

The change is highlighted in **bold** on this screen:

```
change ip-network-region 3                                          Page 1 of 2

                           IP NETWORK REGION
      Region: 3
     Location: __        Home Domain: ___________________________
        Name:
                  Intra-region IP-IP Direct Audio? native(NAT)
AUDIO PARAMETERS    Inter-region IP-IP Direct Audio? translated(NAT)
  Codec Set: 2                                       IP Audio Hairpinning? y
   Location: 1
 UPD Port Range                                     RTCP Reporting Enabled? y
          Min: 2048_                        RTCP MONITOR SERVER PARAMETERS
          Max: 3028                          Use Default Server Parameters? n
                                              Server IP Address: 1 .2 .3 .4
DIFFSERV/TOS PARAMETERS                                      Server Port: 5005
 Call Control PHB Value: 34_                 RTCP Report Period(secs): 5
    Audio PHB Value: 46
          BBE PHB Value: 43                 Resource Reservation Parameters
                                                               RSVP Enabled? y
                                                    RSVP Refresh Rate(secs): 15
 Call Control 802.1p Priority: 7            Retry upon RSVP Failure Enabled? y
      Audio 802.1p Priority: 6              RSVP Profile: guaranteed-service
```

Locations screen

The change is highlighted in **bold** on this screen:

```
change locations                                                 Page 1 of 3
                                     LOCATIONS

                 ARS Prefix 1 Required for 10-Digit NANP Calls? _

 Number    Name                     Timezone   Rule   NPA              Proxy Sel.
                                    Offset                             Rte. Pat.

    1      ____________________     _ __:__    __     ___               ___
    2      ____________________     _ __:__    __     ___               ___
    3      ____________________     _ __:__    __     ___               ___
    4      ____________________     _ __:__    __     ___               ___
    5      ____________________     _ __:__    __     ___               ___
    6      ____________________     _ __:__    __     ___               ___
    7      ____________________     _ __:__    __     ___               ___
    8      ____________________     _ __:__    __     ___               ___
    9      ____________________     _ __:__    __     ___               ___
   10      ____________________     _ __:__    __     ___               ___
   11      ____________________     _ __:__    __     ___               ___
   12      ____________________     _ __:__    __     ___               ___
   13      ____________________     _ __:__    __     ___               ___
   14      ____________________     _ __:__    __     ___               ___
```

NOTE:
This allows for each location to point to the pattern which is routing to its outbound SIP proxy server; this is required by features and services such as Transfer and URI Dialing.

Numbering -- Private screen

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

Avaya 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 will neither create nor send the QSIG Party Numbers or information elements.

```
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 supports the Call Identification Display feature for ISDN and SIP. The feature provides a name/number display for display-equipped stations within an ISDN or SIP network. The system uses the caller’s name and number and displays it on the called party’s display. Likewise, the called party’s name and number can be displayed on the caller’s display.

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.

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 PartyNumbers. 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.

```
change public-unknown-numbering                              Page 1 of 8
                         NUMBERING - PUBLIC/UNKNOWN FORMAT

                                   Total                                 Tota
l
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  _ _______ _____    _____________ __
 _  _______ _____    _______________ __  _ _______ _____    _____________ __
 _  _______ _____    _______________ __  _ _______ _____    _____________ __
 _  _______ _____    _______________ __  _ _______ _____    _____________ __
 _  _______ _____    _______________ __  _ _______ _____    _____________ __
 _  _______ _____    _______________ __  _ _______ _____    _____________ __
 _  _______ _____    _______________ __  _ _______ _____    _____________ __
 _  _______ _____    _______________ __  _ _______ _____    _____________ __
 _  _______ _____    _______________ __  _ _______ _____    _____________ __
 _  _______ _____    _______________ __  _ _______ _____    _____________ __
```

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 allowed depends on the configuration and memory available in your system.

Use this screen to insert or delete digits so AAR or ARS calls route over different trunk groups. 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 Avaya Communication Manager can insert the dial access code for an alternative carrier into the digit string.

The change is highlighted in **bold** on this screen.

```
change route-pattern 1                                             Page 1 of X
                              Pattern Number: 1_
                                        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
```

System Capacity screen

The change is highlighted in **bold** on this 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. Refer to the *"Capacities Table"* for more information.

System Parameters Call Coverage / Call Forwarding screen

The change is highlighted in **bold** on this 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, refer to the *"Administrator's Guide for Avaya Communication Manager"*.

System-Parameters Customer-Options screen

The change is highlighted in **bold** on this screen:

```
display system-parameters customer-options                             page 1 of __
                              OPTIONAL FEATURES
                                                                              Used
        G3 Version: V12                    Maximum Ports: 2800   1041
         Location: 1          Maximum XMOBILE Stations: 0      0
         Platform: 2

IP PORT CAPACITIES
                       Maximum Administered H.323 Trunks: 100    96
             Maximum Concurrently Registered IP Stations: 10     10
               Maximum Administered Remote Office Trunks: 0      0
  Maximum Concurrently Registered Remote Office Stations: 0      0
                Maximum Concurrently Registered IP eCons: 0      0
                        Maximum Administered SIP Trunks: 100    50

     Maximum Number of DS1 Boards with Echo Cancellation: 0      0
                              Maximum TN2501 VAL Boards: 1      0
                               Maximum G700 VAL Sources: 0      0

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

Many fields on this screen are controlled by the Avaya license file. The web-based RFA process is used to generate these license files for customers. For more detailed descriptions of the fields on this screen, refer to the *"Administrator's Guide for Avaya Communication Manager"*.

Glossary

A

access code
A dial code of 1 digit to 3 digits that is used to activate a feature, cancel a feature, or access an outgoing trunk.

Access Security Gateway (ASG)
An optional interface that can be used to secure the administration and maintenance ports on the system.

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

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, wideband 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 is used to transfer 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 feature 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 is used to transmit voice and data. (3) In wideband 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 switch 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 private networks. *See also* switch.

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 Internet Protocol (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 Initiation 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 an Integrated Services Digital Network Primary Rate Interface (ISDN-PRI). *See also* bearer channel (B-channel); data channel (D-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 packet assembly/disassembly (PAD) device.

data module

An interconnection device between an Integrated Services Digital Network Basic Rate Interface (ISDN-BRI) or a Digital Communications Protocol (DCP) interface of the switch, and 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 is used to transmit 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 that are 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 is used to route calls through a communications system. With a Uniform Dial Plan (UDP) or a main-satellite dialing plan, extensions are also used to route calls through a private network.

F

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 local area network (LAN)-based multimedia endpoint and a gatekeeper. *See also* Session Initiation Protocol (SIP).

host computer

A computer that is connected to a network, and that processes data from data-entry input 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.x is a version of Avaya IP Softphone R5 or 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, among other things, produces standards for local area network (LAN) equipment.

Integrated Services Digital Network (ISDN)

A public network or a private network that provides end-to-end digital communications for all services to which users have access. 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 Integrated Services Digital Network (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) (i.e. 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 networks to a final destination. IP 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.

N

narrowband

A circuit-switched call at a data rate of 64 kbps or less. All switch calls that are not wideband are considered to be narrowband.

network

A series of points, nodes, or stations that are connected by communications channels.

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.

O

Off-Premises 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 Initiation 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.

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* switch.

port

A data-transmission access point or voice-transmission access point on a device that is used for communicating with other devices.

Plain Old Telephone Service (POTS)

Basic voice communications with standard, single-line phones accessing the public switched telephone network (PSTN).

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.

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

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.

RFC
Request For Comment designates Internet Engineering Task Force (IETF) standards that are Drafts.

RPM
RedHat Package Manager

RTC
Real Time Communication

RTCP
Real Time Control Protocol

S

Session Initiation 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).

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 preallocating short time slots to each transmitter. In a switch, all port 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 switch, 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 supercede Netscapes' Secure Socket Layer (SSL) and provide host-to-host data connections with encryption and certification at the transport layer, as the name implies.

trunk

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

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.

U

UDP

(1) User Datagram Protocol (UDP); (2) Uniform Dial Plan.

universal serial bus (USB)

A high-speed serial interface that is used primarily to add a printer, a modem, a keyboard, a mouse, or another peripheral device to a personal computer.

User Datagram Protocol (UDP)

A packet format that is included in the TCP/IP suite of protocols. UDP is used for the unacknowledged transmission of short user messages and control messages.

V

Voice over IP (VoIP)

A set of facilities that use the Internet Protocol (IP) to manage the delivery of voice information. In general, VoIP means to send voice information in digital form in discrete packets instead of in the traditional circuit-committed protocols of the public switched telephone network (PSTN). Users of VoIP and Internet telephony avoid the tolls that are charged for ordinary telephone service.

W

wideband

A circuit-switched call at a data rate that is greater than 64 kilobits per second. A circuit-switched call on a single T1 facility or a single E1 facility with a bandwidth that is between 128 kilobits per second and 1536 kilobits per second (T1) or 1984 kilobits per second (E1) in multiples of 64 kilobits per second. H0, H11, H12, and N x digital signal-level 0 (DS0) calls are wideband. *Compare with* narrowband.

Index

T