Highlights of Avaya Communication Manager

555-245-704
Issue 4
January 2005

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.

Disclaimer

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

How to Get Help

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

- Within the United States, click the *Escalation Management* link. Then click the appropriate link for the type of support you need.
- Outside the United States, click the *Escalation Management* link. Then click the *International Services* link that includes telephone numbers for the international Centers of Excellence.

Providing Telecommunications Security

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

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that could be accessed 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, or IEC 60950-1, 1st Edition, including all relevant national deviations as listed in Compliance with IEC for Electrical Equipment (IECEE) CB-96A.

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

Safety Requirements for 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 used in Avaya equipment typically operate within the following parameters:

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

Luokan 1 Laserlaite

Klass 1 Laser Apparat

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

Electromagnetic Compatibility (EMC) Standards

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

Limits and Methods of Measurement of Radio Interference of Information Technology Equipment, CISPR 22:1997 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

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

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

Federal Communications Commission Statement

Part 15:

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

Part 68: Answer-Supervision Signaling

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

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

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

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

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

REN Number

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

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

For G350 and G700 Media Gateways:

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

For all media gateways:

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

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

Means of Connection

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

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

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

For G350 and G700 Media Gateways:

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

For all media gateways:

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

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

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

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

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

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

Canadian Department of Communications (DOC) Interference Information

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

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

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

Installation and Repairs

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

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

Declarations of Conformity

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

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

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

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

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

European Union Declarations of Conformity

CE

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

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

Japan

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

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

To order copies of this and other documents:

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

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

E-mail: totalware@gwsmail.com

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

Contents

About this book

Overview

Avaya Communication Manager is the centerpiece of Avaya applications. Running on a variety of Avaya Media Servers and DEFINITY® Servers, and providing control to Avaya Media Gateways and Avaya communications devices, Communication Manager can be designed to operate in either a distributed or networked call processing environment.

Communication Manager carries forward all of a customer's current DEFINITY capabilities, plus offers all the enhancements that enable them to take advantage of new distributed technologies, increased scalability, and redundancy. Communication Manager evolved from DEFINITY software and delivers no-compromise enterprise IP solutions.

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

Purpose of this book

This book describes the new and changed features and enhancements available with the most recent release of Communication Manager (release 2.x) running on any of the following:

- Avaya media servers
  - DEFINITY® servers
  - S8100, S8300, S8300B, S8500, S8500B, S8700, or S8710 Media Servers
  - IBM eServer BladeCenter HS20 Blade Server Type 8832
- Avaya media servers configured as a Local Survivable Processor (LSP).
- Avaya media gateways
  - CMC1, MCC1, or SCC1 Media Gateways
  - G150, G350, G600, G650, or G700 Media Gateways

Note:

This document does not contain information about prior releases of Communication Manager. For highlight information on previous releases of Communication Manager, check the Avaya customer support Web site (see How to obtain Avaya books on the Web on page 16 for more information).

Newer releases of Communication Manager contain all the features of prior releases.

Intended audience

This document is intended for system administrators and managers, for users interested in information about specific features, and Avaya personnel responsible for planning, designing, configuring, selling, and supporting the system.

Contents

This document includes the following chapters:

- Highlights: presents short descriptions of each of the new features or changes in the most recent release of Communication Manager.
- Hardware: describes hardware that is introduced or changed with the most recent release of Communication Manager.
- New and changed screens: provides information about new administration screens, and changes to existing screens, due to the most recent release of Communication Manager.
- New and changed commands: provides information about commands that are new or have changed for the most recent release of Communication Manager.

Terms and Conventions

Become familiar with the following terms and conventions. They help you use this book with Communication Manager.

- A "screen" is the display of fields and prompts that appear on a terminal monitor.

  See Calling Party Number Conversion for Tandem Calls screen on page 89 for an example of a screen and how it is shown in this book.
- Avaya uses the term "telephone" in this book. Other books might refer to telephones as voice terminals, stations, or endpoints.
- Keys and buttons are printed in a bold font: **Key**.
- Titles of screens are printed in a bold font: **Screen Name**.
- Names of fields are printed in a bold font: **Field Name**.
- Text (other than commands) that you need to type into a field are printed in a bold font: **text**.
- Commands are printed in a bold constant width font: **`command`**.

- Variables are printed in a bold constant width italic font: ***variable***.
- We show complete commands in this book, but you can use an abbreviated version of the command. For example, instead of typing **list configuration station**, you can type **list config sta**.
- If you need help constructing a command or completing a field, remember to use **Help**.
  - When you press **Help** at any point on the command line, the system displays a list of available commands.
  - When you press **Help** with your cursor in a field on a screen, the system displays a list of valid entries for that field.
- Messages that the system displays are printed in a bold font: **system message**.
- To move to a certain field on a screen, you can use the **Tab** key, directional arrows, or the **Enter** key on your keyboard.
- If you use terminal emulation software, you need to determine what keys correspond to **Enter**, **Return**, **Cancel**, **Help**, and **Next Page** keys.
- We show commands and screens from the newest release of Communication Manager. Substitute the appropriate commands for your system and see the manuals you have available.
- The status line or message line can be found near the bottom of your monitor. This is where the system displays messages for you. Check the message line to see how the system responds to your input. Write down the message if you need to call the helpline.
- When a procedure requires you to press **Enter** to save your changes, the screen clears. The cursor returns to the command prompt. The message line shows "**command successfully completed**" to indicate that the system accepted your changes.

Admonishments

Admonishments that might appear in this book have the following meanings:

Note:

A note calls attention to neutral information or positive information that supplements the main text. A note also calls attention to valuable information that is independent of the main text.

Important:

An important note calls attention to situations that can cause serious inconvenience.

Tip:

A tip calls attention to information that helps you apply the techniques and the procedures that the text describes. A tip can include keyboard shortcuts, or alternative methods that might not be obvious.

CAUTION:

A caution statement calls attention to situations that can result in harm to software, loss of data, or an interruption of service.

WARNING:

A warning statement calls attention to situations that can result in harm to hardware or equipment.

DANGER:

A danger statement calls attention to situations that can result in physical injury to yourself or to other people.

SECURITY ALERT:

A security alert calls attention to situations that can increase the potential for toll fraud or other unauthorized use of your telecommunications system.

ELECTROSTATIC ALERT:

An electrostatic alert calls attention to situations that can result in damage to electronic components from electrostatic discharge (ESD).

Trademarks

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

How to obtain Avaya books on the Web

If you have internet access, you can view and download the latest version of Avaya documentation products. To view any book, you must have a copy of Adobe Acrobat Reader.

Note:

If you don't have Acrobat Reader, you can get a free copy at http://www.adobe.com.

For example, to access an electronic version of this book:

1. Access the Avaya Web site at http://www.avaya.com/support/.
2. Click **Product Documentation**.
3. To find a specific book, type the document number (for example, **555-245-704** for this book) in the **Search Support** text box, and then click **GO**.
4. In the resulting list, locate the latest version of the document, and then click the document title to view the latest version of the book.

How to order documentation

In addition to this book, other description, installation and test, maintenance, and administration books are available.

This document and any other Avaya documentation can be ordered directly from the Avaya Publications Center toll free at 1-800-457-1235 (voice) and 1-800-457-1764 (fax). Customers outside the United States should use +1-410-568-3680 (voice) and +1-410-891-0207 (fax).

How to comment on this book

Avaya welcomes your feedback. Contact us through:

- e-mail: document@avaya.com
- fax: 1-303-538-1741
- Contact your Avaya representative

Mention the name, number, and issue of this document, *Highlights of Avaya Communication Manager*, 555-245-704, Issue 4.

Your comments are of great value and help improve our documentation.

How to get help

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.

If you need additional help, the following resources are available. You may need to purchase an extended service agreement to use some of these resources. See your Avaya representative for more information.

Go to the Avaya Web site at http://www.avaya.com/support:

- If you are within the United States, click the **Escalation Contacts** link that is located under the **Support Tools** heading. Then click the appropriate link for the type of support you need.
- If you are outside the United States, click the **Escalation Contacts** link that is located under the **Support Tools** heading. Then click **International Services**, which includes telephone numbers for the international Centers of Excellence.
- Contact your local Avaya authorized dealer for any additional help and questions.

Chapter 1: Highlights

This chapter presents highlights of features and enhancements as part of the most current release of Avaya Communication Manager running on Avaya DEFINITY® servers, as well as the Avaya S8000-series Media Servers with associated Avaya Media Gateways.

The most current release of Communication Manager contains all the features of prior releases. In this document, each Communication Manager feature or enhancement is listed alphabetically by release number.

For a more complete overview of all the features of Communication Manager, see the *Overview for Avaya Communication Manager*, 555-233-767.

For more information on how to administer any of these features, see the *Administrator's Guide for Avaya Communication Manager*, 555-233-506.

Release 2.2 new features and enhancements

Avaya Communication Manager, release 2.2, includes the following general telephony and system-wide features and enhancements.

Call center service observing with exclusion

Communication Manager allows service observing of a telephone with exclusion active, either by class of service (COS) or by manual activation. For more information, see the detail that is provided on the Feature-Related System Parameters screen on page 85.

E911 device location for IP telephones

Communication Manager works with an E911 Manager device from RedSky Technologies. This third-party E911 Manager provides a flexible, complete, and automated E911 management system for customers who want to implement VoIP telephony.

The E911 Manager detects when an IP telephone has moved. The next time that the system updates the Automatic Location Information (ALI) database, the E911 Manager reports the new location of the IP telephone to the public safety answering point (PSAP).

The E911 Manager from RedSky Technologies works with Communication Manager release 2.2 to keep the Automatic Location Information (ALI) record for each extension correct. The E911 Manager also provides notification whenever someone moves an IP endpoint to a new subnet.

FIPS-140-2 compliance on branch gateways

Communication Manager release 2.2 contains the certification of VPN functionality, as well as the Disabling Media Encryption and Signaling Encryption functionality for branch gateways.

Firewall in G350 Media Gateways

Firewall capabilities are now incorporated into the G350 Media Gateway.

H.323 IP system integration

H.323 IP system integration is an enhancement to the IA770 branch office messaging solution. The IA770 solution provides a co-resident, Intuity Audix-based messaging solution for S8300B Media Servers operating as a primary server. The IA770 solution is supported on the G700 and G350 Media Gateways.

Release 2.0 of IA770, offered in conjunction with Communication Manager release 2.2, supports a new switch integration based on QSIG and H.323. This integration eliminates the need for the CWY1 hardware.

The capacities for the new H.323 IP integration are the same as those currently supported for the CWY1-based integration and are as follows:

- A maximum of 8 channels for voice traffic

  Note that additional channels may be configured in the new H.323 IP integration, but are intended to support needs for transfers and MWI updates.

- A maximum of 450 users

Beginning with IA770 release 2.0, new orders for IA770 no longer require or include the CWY1 hardware. The CWY1 is only available for new sales or installations if a customer experiences problems with the H.323 IP integration. Upgrades to IA770 release 2.0 that preserves the use of an existing CWY1 is supported. The Avaya Installation Wizard also supports configuration of the new H.323 IP integration.

IP robustness, automatic trace route on errors

If the IP connectivity between a server and its port networks or media gateways or H.323 trunks is los, the system launches an automatic **`trace-route`** command. The purpose of launching an automatic **`trace-route`** command is to improve the diagnosis of network problems and more easily determine where a network outage exists. This functionality includes support for all

the Linux platforms, and includes port networks through the IPSI, and IP trunks, along with all the media gateways.

Note:

The S8300 support only applies to media gateways at this time because the S8300 does not support port networks, and does not monitor the status of IP trunks.

The results of the trace-route is written to the Linux log files, and is viewable from the Maintenance Web Pages. In order to limit the impact on performance when multiple links are lost at the same time, only a limited number of automatic trace-routes are launched in those circumstances.

IP robustness, CLAN internal flow control

Development vintage 119 (GA vintage 12) firmware contains the enhancement to complete the flow control path from one side of the CLAN to the other. The CLAN is now able to withstand network traffic spikes without entering buffer exhaustion.

IP robustness, handle trunk denial of service

This new feature is designed to mitigate a "denial-of-service" attack on a gateway's trunks by performing adaptive traffic shaping when it appears that the processor occupancy is rising to intolerable levels. The purpose is to provide a means to throttle traffic under these conditions according to the customer's pre-determined preferences.

In earlier versions of the software, a customer cannot preconfigure a call server's response to a high occupancy situation. The algorithm is hard-coded into the software, and favors the Call Center environment. Thus, in an overload condition, Communication Manager allows inbound calls from trunks, but blocks all outbound and station-to-station calls.

The introduction of these enhancements provide the means for a customer to customize their call servers' reaction to an overload conditions so that the overload mitigation better suits their environment.

IP robustness, message flow control for CLAN

In earlier versions of the software, the H.248 link between a media server and media gateway resets whenever the system experiences PCD congestion due to exhaustion of buffer resources.

This process is replaced with an end-to-end flow control mechanism that backs-off the transmission of messages from the media server to the media gateway whenever there is congestion.

This enhancement for CLAN provides three new capabilities:

- Media gateway uplink rate limiting. Communication Manager communicates with CLAN the rate at which to limit traffic coming from a media gateway. This communication occurs during 2945 listen socket creation time. This process helps with Denial-of-Service situations, and protects Communication Manager from crashing.
- Media Gateway downlink flow control. When Communication Manager hits the low downlink watermark, Communication Manager suspends selected maintenance activities, helping to prevent PCD congestion. This process keeps users from hitting the high watermark so quickly, which would take down the media gateway link.
- Access Control List. Communication Manager sends IP address information to Linux (PCLAN) during RAS processing (UDP). CLAN then keeps a list of IP addresses that are allowed to register on the 1720 listen socket (TCP). This process helps with Denial-of-Service situations, and protects Communication Manager from crashing.

IP robustness, message flow control for PCLAN

In earlier versions of the software, the H.248 link between a media server and media gateway resets whenever the system experiences PCD congestion due to exhaustion of buffer resources.

This process is replaced with an end-to-end flow control mechanism that backs-off the transmission of messages from the media server to the media gateway whenever there is congestion.

This enhancement for PCLAN provides two new capabilities:

- Media gateway uplink rate limiting. Communication Manager communicates with Linux (PCLAN) the rate at which to limit traffic coming from a media gateway. This communication occurs during 2945 listen socket creation time. This process helps with Denial-of-Service situations, and protects Communication Manager from crashing.
- Access Control List. Communication Manager sends IP address information to Linux (PCLAN) during RAS processing (UDP). PCLAN then keeps a list of IP addresses that are allowed to register on the 1720 listen socket (TCP). This process helps with Denial-of-Service situations, and protects Communication Manager from crashing.

IP robustness, RSCL priority

The design of the CLAN is heavily dependant upon a single control communication link known as the Remote Socket Control Link (RSCL). When communication on this link is blocked for whatever reason, the CLAN starts bringing down sockets and Communication Manager can eventually reset the CLAN.

In previous CLAN releases, it was possible for high network traffic to consume all communication resources and block all RSCL communication which could lead to CLAN resets. With this feature, the buffer exhaustion problem was eliminated. To ensure the RSCL always has communication resources, the pool of resources was split into a RSCL-only pool and the general pool. The RSCL can use resources from both pools, but only the RSCL can use resources from the RSCL- pool. This ensures that the RSCL always has communication resources.

Modem over IP

Enhancements to the Modem over IP feature provide support for modem relay over IP interfaces for inter-gateway and inter-system traffic. The interfaces to support this feature are media processors in port networks, and IP interfaces in media gateways. With a firmware download, this feature is offered on the G700, G350, MM760, and TN2302AP V10 or later. This feature is not available on the TN2302AP V9 or earlier.

Native administration for the 2410 telephone

A native administration screen is available for the 2410 DCP telephone. Administrators no longer need to alias 2410 DCP telephones as 2420 telephones.

In addition, the firmware download capability for DCP telephones now includes the capability to download firmware to the 2410 DCP telephone.

Native administration for the 4601 telephone

A native administration screen is available for the 4601 IP telephone. Administrators no longer need to alias 4601 IP telephones as 4602 telephones.

Port security, 802.1X for G350 Media Gateways

IEEE 802.1x is a port-based network access control protocol that provides a means of authenticating and authorizing devices that are attached to G350 port.

IEEE 802.1x is used in computer workstations using MS-XP or Linux operating systems. The protocol is also used by IP telephones, wireless access points, and other adjuncts that are connected to G350 Media Gateway.

Routing of VIP wakeup calls to attendant vector

This feature allows the system to deliver VIP wakeup reminders to attendant vectors. In prior versions of the software, the system only delivered VIP reminder calls to attendant consoles.

SCCAN updates for Extension to Cellular

Three changes have been made to the Extension to Cellular feature for the Seamless Converged Communications Across Networks (SCCAN) functionality.

- New application type. A new application type, **CSP**, was added to the **Stations with Off-PBX Telephone Integration** screen. This application type is for Cellular Service Providers (CSPs) who resell EC500 services. The four available application types are:
  - CSP
  - EC500
  - OPS
  - SCCAN
- Special Digit Conversion. A new field, **Special Digit Conversion**, was added to the **SCCAN-Related System Parameters** screen. When enabled, this field allows a user to call a cell telephone number and get the same treatment as calling an extension that is running Communication Manager.
- MM (WSM) Route Pattern. From earlier versions of the software, the **Default MM (WSM) SIP Trunk Group** field on the **SCCAN-Related System Parameters** screen has been changed to **MM (WSM) Route Pattern**. With this change, only regular routing pattern numbers that are SCCAN-enabled are allowed. Partition route patterns indexes, RHNPA indexes, deny, or nodes are not allowed.

Shared Control feature for 4601 telephones

The Shared Control feature in Communication Manager release 2.1 (see Enhanced Softphone/ Telephone Shared Control of IP telephones on page 34) allows a telephone with a speakerphone and an IP Softphone to be in service on the same extension at the same time.

Communication Manager release 2.2 adds the following enhancements to the Shared Control feature:

- Model 4601 to the list of telephones that are supported
- Handset support (the 4601 telephones have handsets but not speakerphones)
- Headset support (a headset can be plugged into a handset jack)

Show number of IP Softphone

With earlier versions of the software, when an agent is using Avaya Softphone in telecommuter mode, there is no way for agencies to know the actual telephone number that a given call was placed from. This feature provides the ability to obtain this information.

Support for ASAI switch classified calls

Gateway messaging and Communication Manager are modified to support ASAI switch classified calls, with or without Answering Machine Detection. Support for ASAI switch classified calls is launched through outgoing trunks on H.248 gateways such as the G700 and G350, and on IP-connected Port Network gateways such as the G600 and G650.

Prior to this release, existing H.248 messaging and Communication Manager does not allow for the utilization of gateway classifier resources for switch-classified calls.

The system uses routing algorithms that result in only one attempt to obtain both a trunk and a call classification resource. With these configurations, both the trunk and the classifier resource must be on the same gateway.

These changes are necessary to support ASAI Predictive Dialing and other OCM applications that require classification with H.248 gateways and IP-connected port network gateways.

Support for http file download to IP telephones

You can use existing http server software, that is running on the same hardware processor platforms as Avaya Communication Manager, to support the download of files to IP telephones. For Communication Manager release 2.2, this support applies to the S8300 Media Server only.

Two small configuration files are downloaded every time a 46xx IP telephone powers up or resets. The system stores software code files in non-volatile memory in the IP telephones, so it is not be necessary to download such a file every time a telephone is powered-up or reset. Software code file downloads are only be necessary when individual telephones are installed (if they do not already contain the latest software), or as groups of telephones are intentionally reset during off-peak hours to allow new software to be installed.

Support for Universal Access Phone Status

Universal Access Phone Status (UAPS) is a PC-based application for customers who wish to provide equal access to users who are blind. Earlier versions of UAPS work only with 4612 and 4624 IP telephones.

A new version of UAPS is a client-based application that works with all IP telephones. UAPS monitors the telephone's status through the Shared Control resource, instead of through a CTI login into the telephone itself.

Note:

Customers must have an IP Softphone RTU for this change to take place.

VPN for G350 Media Gateways

VPN is based on IPSec VPN technology that supports site-to-site IPSec VPNs, and includes AES as well as 3DES and DES encryption algorithms. The VPN is available for the G350 Media Gateway.

One of the G350 VPN applications is backup of the primary WAN connection through an xDSL modem, a backup that could be active and in continuous use for some of the data applications using Policy Base Routing. For that purpose, the Point-to-Point Protocol over Ethernet encapsulation is supported on the G350 Ethernet WAN interface. Interoperation of the VPN features are verified against leading vendors of IPSec VPN devices.

Licensing of VPN for G350 Media Gateways

RFA generates and digitally signs a gateway license file. The G350 Media Gateway validates the license by authenticating a license file signature and examining a serial number.

On finding a mismatch in either a serial number or bad signature, the G350 Media Gateway aborts the license installation. The G350 Media Gateway does not activate the VPN feature unless a valid license is downloaded.

VPNos 4.5

The enhancements to the virtual private network operating system (VPNos), release 4.5, are:

Diagnostic snapshots to console

With VPNos 4.5, you can generate diagnostic reports over the CLI. VPNos 4.5 also provides an interface to the **`tcpdump`** and **`traceroute`** commands over the CLI.

The system displays the report on the screen. The report contains the following information in the specified order:

1. Date/Time (date_time)
2. System Up Time (uptime)
3. SG VSU Info (vusinfo)
4. Kernel diagnostics (kern_diag)
5. Routing Table (route_table)
6. VPN Flow table (flow_table)
7. VPN SA Table (sa_table)
8. Interfaces Table (if_table)
9. Interface Configuration (if_config)
10. Socket Table (sock_table)
11. Network Memory (net_mem)
12. System Memory (sys_mem)
13. Interrupt State (intr_state)
14. Firewall State (fw_state)
15. Process Table (proc_table)
16. Protocol Statistics (proto_stats)
17. Route Statistics (route_stats)
18. System Statistics (sys_stats)
19. System State (sys_state)
20. Address Map Report (addr_map)
21. Security Processor Statistics (sec_proc_stats)
22. IKE SAs (ike_sa)
23. ARP Table (arp_table)

24. VPN Statistics (vpn_stats)
25. High Availability Statistics (ha_stats)
26. RIP Statistics (rip_stats)
27. VTDR Statistics (vtdr_stats)
28. H.323 Statistics (h323_stats)
29. Event Log (event_log)
30. SG XML Configuration (xml_cfg)

Dynamically addressed devices

Many Avaya customers are deploying Avaya Security Gateways (SG) at locations where the customer desires Internet service that provides dynamic IP address assignments to the public interface of the SG. These locations are predominantly branch offices and individual virtual offices. The primary reason for using dynamic IP service is the cost savings over the static IP service.

Since the public IP address of an SG that is deployed in this manner is dynamically assigned and therefore unknown, the administrator cannot use VPNmanager to manage the deployed SGs. The administrator cannot take advantage of the fact that VPNmanager is designed to centrally manage SGs and VSUs on a large scale.

Neither is the administrator able to use any of the management applications, such as the SG web interface or a 3rd-party management application, from across the Internet to the public IP address of the SG.

The dynamically addressed devices feature resolves these issues. The dynamically addressed devices feature adds the ability to remotely managed devices who receive their IP address dynamically through some means, like PPPoE.

High availability

High availability refers to the capability of a security gateway (SG) to take over and provide VPN and other services, such as firewall or NAT, when another SG fails and stops providing those services.

This feature requires two identically configured SG devices, one as master, the other as slave. The two units periodically communicate to each other. When the master unit fails to respond to the slave for a period of time, the slave takes over. Since it is identically configured, including the same IP addresses, VPN services can resume with the slave now functioning as the master.

This project extends the high availability functionality of the 3.x products into the 4.x product line.

Network failure detection

Network path failure detection capabilities help administrators to resolve network problems quickly. The network failure detection feature provides independent failure detection capabilities. Traceroute capabilities are added to Failover and Keep Alive functions. Keep Alive functionality is also added.

The main requirement is to provide capabilities that automatically detect the failure in the network path, and initiate the **`traceroute`** command to discover the exact point of failure.

Remote download

The remote download feature enhances the VPNos firmware upgrade mechanism to accommodate field provisioning upgrades. The remote download feature:

- Eliminates the need to distribute a special Patch Kernel
- Allows the SG to be upgraded without the need to be in physical contact with the unit

Session MIB access

In previous releases of VPNos, Syslog and SNMP messages were always sourced from the public interface. Syslog and SNMP messages were not encrypted, unless the public IP is part of the VPN. In dynamically addressed devices, this topology does not work because the public IP address is dynamic and changes with time.

Since the SNMP v3 engine does not support AES encryption, and Syslog does not have protocol-supported data protection, these messages are not very well protected. Since information provided by these messages is sensitive in nature, it is desirable to protect them by sending them in a VPN tunnel.

In addition, SNMP needs to support the enterprise management information base (MIB) – VPNETMIB as much as possible. Thus it is required to support Network statistics for every physical port in the system, and VPN statistics for every VPN (Remote Tunnel Endpoint) that is configured in the system. It is also required to support QOS monitoring and monitoring traceroute (network path failure detection using trace route) results through SNMP MIB in VPNos 4.5. It is also required to support sending an enterprise trap whenever a network failure condition is met.

Split tunnel

The split tunnel feature provides enormous flexibility for administrators. Administrators can make modifications in corporate network topology without affecting any remote VPN peer configuration that is connected to the corporate network. Split tunnel also provides additional security because all traffic from remote VPN peers goes through the corporate network. This security minimizes any attack that might be caused when a PC is connected to both the corporate network and the Internet at the same time.

This feature allows non-authenticated traffic to be routed out to the Internet, while authenticated traffic is properly routed to the VPN tunnel interface.

VPN default route

The system uses VPN default route (VTDR) to direct all the decrypted VPN traffic to a route on the private network. The purpose of VTDR is to minimize the configuration changes on the security gateway (SG) for any changes that are made in the routing on the private side. It also enables isolation of the SG from learning multiple routing protocols.

VPN Routing Information Protocol

Communication Manager release 2.2, and VPNos release 4.5, introduces the use of Routing Information Protocol (RIP) version 2. RIP version 2 advertises Avaya secure gateways (SGs) as gateways to networks that are protected by peer VPN devices. This applies to network routes that are statically configured by the SG administrator, as well as networks that are learned dynamically by the SG itself.

Additional aspects delivered with this feature include population of important network metrics.

VPNmanager 3.6

The enhancements to the virtual private network manager (VPNmanager), release 3.6, are:

Dynamically addressed devices

As more people use DSL and cable modems to connect to the Internet and to other corporate offices to run their business, managing the network devices is becoming more difficult for network administrators. Many customers deploy low-end devices (SG/5/5x/200) at remote locations, which use DHCP or PPPoE on the WAN interface to connect to their headquarter’s branch.

VPNmanager 3.6 allows the administrator to manage such dynamically addressed devices in user VPN mode.

High availability

This feature supports functionality similar to High Availability in the VPNos product line by providing the ability for network operation centers to configure and manage High Availability installations on a network-wide basis.

VPNmanager allows the user to:

- Configure virtual public addresses
- Configure virtual private addresses

- Configure Active-Passive transition criteria
- Configure pass phase to authenticate advertisements
- Switch a unit from passive to active
- Delete a unit from HA pair

Remote download

With VPNmanager, the user is able to remotely download a firmware image, install the image, and reboot the system so that VPNos upgrades can be done remotely and with ease.

Routing Information Protocol

VPNos 4.5 uses Routing Information Protocol (RIP) to advertise the gateway for the networks behind peer security VPN devices. VPNmanager allows the user to:

- Turn on or off the advertising of remote tunnels
- Turn on or off the advertising of Remote Client tunnels
- Configure RIP metrics
- Turn on or off dynamically learned routes

VPN default route

VPN default route (VTDR) allows administrators to deploy and manage security gateways in an easy manner by specifying a default route for decrypted traffic. Prior to this enhancement, administrators have to enter hundreds of static routes on security gateways to configure their network. By using VTDR, administrators no longer need to enter static routes.

Windows 2003 server integration

VPNmanager 3.6 provides full integration with Microsoft's Windows 2003 server product.

Release 2.1 new features and enhancements

Avaya Communication Manager, release 2.1, includes the following general telephony and system-wide features and enhancements.

Authorization codes removed from history report

In list history reports, whenever a "change auth" command was displayed, the authorization code that was changed was also shown. This report might provide access to authorization codes that can be used for toll fraud.

Authorization codes have now been removed from list history reports.

Automatic upgrade tool of server/LSP software and license

This feature adds the following functionality to the Web page upgrade tool:

- Distribution of license files from the server on which the upgrade tool is running to the LSPs that need them
- Display of SID/MID on the query results
- Support for the G350 gateways as an upgrade target
- Upgrade of the standby server
- Upgrade of the sever on which the upgrade tool is running
- Support for FTP as well as TFTP as a gateway upgrade protocol
- Support for administration of the number of simultaneous FTP/TFTP sessions

This feature is implemented only on Linux servers.

Avaya Extension to Cellular/OPS

In addition to features in previous releases of Communication Manager and Extension to Cellular, Avaya Communication Manager Extended Access enhancements for release 2.1 include the following:

Cellular Voice Mail Avoidance

The Cellular Voice Mail Avoidance feature is designed to reduce the uncertainty as to where unanswered Extension to Cellular calls are sent. An unanswered call terminates either at your system voice mail (for example, at your office telephone), or at your cellular service provider (CSP) voice mail system.

Originating Call Detail Recording on calls

If a cell phone originates a call through its mapped extension, for example, through a SIP telephone or a cell phone call, a Call Detail Recording (CDR) record is generated for that call. For this feature to work, incoming trunk CDR must be turned on. The system does not generate a CDR if the user dials a feature name extension (FNE).

- Calls that are originated from an Avaya Communication Manager Extended Access telephone are reported as OPTIM calls on the CDR record.
- When an Avaya Communication Manager Extended Access telephone originates an intra-system call and a trunk call, only the trunk call is reported on the CDR record.

Security code not needed

You can enable and disable Extension to Cellular without having to enter a security code.

New application type

Communication Manager, release 2.1, adds a new application type, CSP. Application type OPS is reserved for SIP trunks only. CSP supports ISDN, H.323, and SIP trunks. CSP cannot be disabled.

Call logs enhanced

Call logs for 2420, 4620 and 4610 telephones have been enhanced. The originating party name and number information for attendant transferred calls and hunt group calls is now captured by telephone-based call log features.

Dynamic hunt group queue slot allocation

The dynamic hunt group queue slot allocation feature eliminates the need to preallocate queue slots for hunt groups. The system dynamically allocates the queue slots from a common pool on an as-needed basis.

All possible calls can be queued. There is no additional administration needed. This feature expands the capacities of your system by eliminating the potential of missed calls due to a full queue.

When the **Queue?** field on the **Hunt Group** screen is set to **y**, this feature applies to all uses of hunt groups:

- Automatic Call Distribution (ACD) non-vector/vector splits and skills
- Non-ACD hunt group
- Voice mail

Note:

The **Queue Length** field has been removed from the **Hunt Group** screen, and related changes have been made to other screens. Queue limiting can still be provided through Call Vectoring. See the *Call Vectoring EAS Guide* for details.

For screen changes, see Hunt Group screen on page 105.

E911 ELIN for wired IP extensions

Enhancements to the E911 ELIN for wired IP extensions feature were made in Communication Manager, release 2.1. These enhancements provide a more accurate location to the public safety answering point (PSAP) when a user calls for emergency assistance from a cellular telephone.

Note:

For this important feature to work, it is critical that the system administrator properly set up their system. For more information, see the see the *Administrator's Guide for Avaya Communication Manager*, 555-233-506.

Enhanced Softphone/Telephone Shared Control of IP telephones

The Softphone/Telephone Shared Control capability is enhanced to support the control of the 4602, 4606, 4610, 4612, 4620, 4624 and 4630 IP telephones, and IP Agent. A new RTU type or customer option is supported for Shared Control. No changes were made to the types of Softphones or DCP telephones that are supported.

G350 WAN - DSL

This feature supports DSL links, modems, and interfaces. This feature is implemented through an Ethernet port.

G350 WAN - QoS

This feature improves the quality of service (QoS) mechanism to support voice and data traffic over slow links. Currently the handing of data traffic over a highly used converged traffic link may create bottlenecks for some applications. This feature solves this problem.

Identifying emergency calls on a display telephone

When the crisis alert features is activated on a digital telephone, the display begins with "E=". Prior to this release, the display began with "EM=".

This change does not affect the display on attendant consoles.

Increased efficiency in routing SIP calls

SIP calls route more efficiently after Communication Manager has selected a trunk group:

1. If there is a trunk available in a signaling group whose domain matches the caller's domain, the call uses that trunk.
2. If not, if there is a trunk available in a signaling group with blank far-end domain, the call uses that trunk.
3. If not, the call uses the first available trunk.

Link reliability and robustness

The main features provided by this item are:

- Alternate WAN connection. Establish a new WAN connection when the main link is down. The link can be established over an analog trunk using:
  - Modem over serial/USB
  - Analog port

  The idea is to use the secondary link as a backup for the signaling control from the main server. This will require support in the Call Admission Control feature.
- Support voice and data multiplexing over the G350. The module is able to get data and voice (TDM) channels on the same link, and removes the need for two links or an external DSU. The voice and data multiplexing are supported only on the G350.
- Optimize traffic flow over two dedicated IP links for converged and data traffic.

LSP file synchronization enhancement

The LSP file synchronization enhancement provides a move effective and efficient mechanism for transmitting translation data from the primary server to LSPs. A new file difference mechanism identifies the changed records within the translation file, and transmits only those changed records when a file synchronization occurs. This file is sent only to LSPs that are already registered to the system.

Note:

For all LSPs that are registering to the primary controller, whether first time or recovering from an outage, if a translation update is deemed necessary, the full compressed translation file is sent.

This feature increases efficiency by not having to tie up a customer's network by updating records that were not changed since the last update.

Media gateway serviceability/installation enhancements

The purpose of this feature is to simplify installations and maintenance for Avaya services BP and DIY customers to install G350s. Its main features include better and more integrated tools, allowing new installation scenarios mainly for BP and DIY. It provides a faster and more reliable process.

This feature supports the following functions:

- Allow remote access for BP after installing LSP license file
- Remote AIW for BP
- Support LAN and WAN installation by AIW and GIW
- Enhanced pre configuration of ECC to support 'virtual' G350
- Support USB modem and CD-ROM on G350
- Auto run CD for SW upgrade

Modem over IP

The Modem over IP (MoIP) feature provides the capability to support modem transmissions with pass-through and relay over IP interfaces for inter-gateway and inter-switch traffic. The interfaces to support this are Media Processors in port networks, and IP interfaces in Media Gateways.

Avaya has developed this solution as proprietary, pre-standards functionality to transport these kinds of communication between Avaya Port Networks and Gateways, through Media Processors and IP Media modules, both inter-switch and inter-gateway as in the case of an IP-Connect system, using the aforementioned interfaces. Modem over IP interoperates only within Avaya networks.

This feature is offered on the G700, G350, MM760, and TN2302AP V10 or later with a firmware download. It is not be available on the TN2302AP V9 or earlier. Customers with TN 2302AP V9 or earlier must purchase a new TN2302AP circuit pack if they wish to obtain this functionality.

Modem Pass through is available with Communication Manger, release 2.1. Communication Manger, release 2.1 or later is required to operate this feature.

Multinational Locations

For customers who operate in more than one country, the Multinational Locations feature provides the ability to use a single Enterprise Communication Server (ECS) across multiple countries with:

- telephones
- port networks
- remote offices
- media gateways

The Multinational Locations feature allows the following Communication Manager features to work across international borders:

- A & Mu law companding
- Call Progress Tone Generation
- Loss Plan
- Analog line board parameters
- Call Detail Recording
- R2-MFC (multifrequency signaling) trunks

The Multinational Locations feature works across all Linux platforms supported by Communication Manager release 2.1 or higher.

The S8300, S8500, S8700, and S8710 Media Server each supports 25 location parameter sets. You can administer one parameter set for each country that you support, for a maximum of 25 countries.

Analog line board parameters by location

You can administer the following analog line board parameters for each location:

- Analog Ringing Cadence
- Analog Line Transmission
- Flashhook Interval Upper Bound
- Flashhook Interval Lower Bound
- Forward Disconnect Timer (msec)
- Analog line tests use the same parameters

Analog line circuit packs use these parameters, according to the location parameters of the circuit pack.

Companding for DCP telephones and circuit packs by location

You can administer the Companding Mode for each remote office, media gateway, and the rest of the system that is circuit switched.

- When a Digital Communications Protocol (DCP) telephone comes into service, Communication Manager downloads the correct companding mode for the location of the telephone.
- When a circuit pack comes into service, Communication Manager downloads the administered companding mode for the media server, remote office, or media gateway that is supporting that circuit pack.

Location ID in Call Detail Record (CDR) records

You can administer the following CDR parameters in the custom CDR format for both the source and destination:

- location
- time zone
- country

Loss plans by location

For each location, you can administer Digital Loss & Tone Loss, DCP terminal loss parameters, and administrator-entered customizations.

When inserting loss for a multilocation intrasystem call, Communication Manager treats the call as if IP tie trunks are connecting the different parties. When an audio stream is converted from time-division multiplexing (TDM) to Internet Protocol (IP), the system adjusts the audio stream. The system adjusts the audio stream by the IP media processor board of the sending location, to an ISO standard level for voice over IP. The system then adjusts the audio stream by the media processor of the receiving location to match the TDM levels for that location.

This board level adjustment is not done for DS1 remoted expansion port networks (EPNs). Use DS1 remoted EPNs between countries only if the countries have similar voice transmit levels.

Multifrequency signaling by trunk group

Prior to Communication Manager release 2.1, you administered R2-Multifrequency Coded (MFC) signaling parameters by system. With Communication Manager release 2.1 and higher, you administer R2-MFC signaling parameters by trunk group.

R2-Multifrequency Coded signaling trunk groups use one of 8 sets of MFC signaling parameters according to the MFC signaling code administered for that trunk group.

Tone generation by location

You can administer tone generation characteristics and administrator-entered customizations by location. You can administer the server so that, when a telephone or trunk needs to play a Communication Manager ECS-generated tone, the software plays a tone into the call using the tone characteristics of the location of the listening endpoint, or of another endpoint on the call.

Native administration for the 2402 telephone

A native administration screen is provided for the 2402 telephone. This feature supports automatic administration for the Messages button. This feature also allows a feature to be administered for the "shifted #" button, which is not possible when the 2402 telephone is aliased as a 6402 telephone.

No-License mode

Changes to the license file strategy protect customers from loss of call processing. The result of No-License mode is a temporary error message on telephone displays, and blocked system administration.

License Error Timer

The License Error Timer is extended to 30 days.

Notification for bad IP address

If a far-end IP address for a signalling group is bad, the signalling group cannot come into service. The system now logs a denial event identifying this problem when it occurs.

Partitioning and privacy for inter-port-network connection

You can now administer preferences for inter-port-network connectivity. Specifically, connections using the same network regions are preferred over connections spanning network regions. Further, when connections span network regions, and multiple choices for network pairs exist, preference goes to the lowest-numbered network region first.

This enhancement enables you to create partitioned, and possibly private, inter-port-network connections. If they are private, you can use this capability to shield what would normally be TDM traffic in a MultiConnect system, even though the system is IP Connect.

Ping test interval changed

You can now change the value in the **Ping Test Interval (sec)** field on the **IP-Options System Parameters** screen from 1-999 seconds. The default value is 10 seconds. To display the **IP-Options System Parameters** screen, type **`change system-parameters ip-options`**.

Protection against saving corrupt translations

If you are logged in as ‘dadmin’, you cannot run the **`enable save-translation`** command when Communication Manager has detected translation corruption. If you encounter translation corruption, please contact your Technical Service Organization.

QSIG call diversion failure

If you set up your system to use private networking and QSIG supplementary services with rerouting, but do not assign the AAR feature access code (FAC), QSIG call diversion fails.

While rerouting a call, if the system detects that the Auto Alternate Routing (AAR) FAC is not administered, the system logs a new denial event, **DNY_FAC_NOADM**.

Redirection on IP Failure

The Redirection on IP Failure (ROIF) feature redirects a call to the split/skill queue, or to the Redirection on No Answer (RONA)-specified VDN, if IP connectivity failure is detected when that call is being delivered to an ACD auto-answer agent using an IP hard- or soft-phone. The addition of ROIF prevents loss of calls being delivered to auto-answer agents when short term IP connectivity failure is detected during call delivery to the agent. This feature does not impact Avaya CMS or other adjuncts.

A new page, with two new fields, is added to the **Feature-Related System Parameters** screen. For more information, see the Feature-Related System Parameters screen on page 103.

Rugged media gateways and closet switches

Avaya's systems meet US Government requirements for harsh environmental conditions, such as shock, vibration, and temperature extremes. To ensure that our system architecture of servers and gateways continue to meet these demands, ruggedized racks and enclosures are available.

Support for http file download to IP telephones

You can use existing http server software, that is running on the same hardware processor platforms as Avaya Communication Manager, to support the download of files to IP telephones.This support applies to all platforms, not just the S8300 Media Server.

Two small configuration files are downloaded every time a 46xx IP telephone powers up or resets. The system stores software code files in non-volatile memory in the IP telephones, so it is not be necessary to download such a file every time a telephone is powered-up or reset. Software code file downloads are only be necessary when individual telephones are installed (if they do not already contain the latest software), or as groups of telephones are intentionally reset during off-peak hours to allow new software to be installed.

Support for Secure Shell and Secure Copy

Secure Shell

You can log in remotely to the following platforms using Secure Shell (SSH) as a secure protocol:

- C360 Multilayer Modular switch
- S8300, S8500, S8700, or S8710 Media Server command line
- IBM BladeCenter HS20 Blade Server Type 8832 command line
- Communication Manager System Administration Terminal (SAT) interface on a Media Server using port 5022

The SSH capability provides a highly secure method for remote access. The capability also allows a system administrator to disable Telnet when it is not needed, making for a more secure system.

Note:

The client device for remote login must also be enabled and configured for SSH.

Refer to your client P.C. documentation for instructions on the proper commands for SSH.

Secure Copy

You can transfer files to and from the S8300, S8500, S8700, and S8710 Media Servers, Blade Server Type 8832, G350 Media Gateway, and the C360 Multilayer Modular switch using Secure Copy (SCP). The primary purpose of SCP for these devices is downloading firmware. The SCP capability allows a system administrator to disable File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) when they are not needed, making for a more secure system.

Note:

The target device for SCP data transfer must be enabled for SSH.

Refer to your client P.C. documentation for instructions on the proper commands for SCP.

T.38 Fax Interoperability

With Communication Manager 2.1, T.38 Fax Interoperability and Modem Pass Through is delivered to the following resources:

- TN2302 IP Media Processor (Hardware V10 and Higher only)
- G700 Media Gateway
- MM760 VoIP Media Module
- G350 Media Gateway

The T.38 Fax Interoperability feature delivers the functionality needed to support T.38 fax interoperability with non-Avaya elements. T.38 Fax interoperates with products based on standards supported in H.245 v6 or later, and T.38. This includes Cisco Gateways, as well as Alcatel and Clarent Gatekeepers. Multi-Tech MultiVOIP has interoperability with T.38 Fax.

Note:

Fax endpoints served by two different Avaya media servers can also send T.38 faxes to each other if both systems are enabled for T.38 fax. In this case, the media servers also use IP trunks.

However, if the T.38 fax sending and receiving endpoints are on port networks or media gateways that are registered to the same media server, the gateways or port networks revert to Avaya fax relay mode. Avaya fax relay mode is more efficient that T.38 from a bandwidth perspective.

Both the sending and receiving systems must announce support of T.38 fax data applications during the H.245 capabilities exchange. Avaya systems announce support of T.38 fax if the capability is administered on the Codec Set screen for the region and a T.38-capable media processor was chosen for the voice channel. In addition, for a successful fax transmission, both systems should support the H.245 null capability exchange (shuffling) in order to avoid multiple IP hops in the connection.

Note:

The T.38 fax capability does not support TCP.

You can assign packet redundancy to T.38 standard faxes to improve packet delivery and robustness of fax transport over the network.

Pass through mode

You cannot send faxes in pass through mode with the T.38 standard.

TTY enhancements

Relay mode

In relay mode, the system:

- detects TTY characters
- transports a representation of the characters over the IP network
- regenerates TTY characters/tones for delivery to the TTY device

This transport of TTY supports US English TTY (Baudot 45.45) and UK English TTY (Baudot 50). TTY uses RFC 2833 or RFC 2198 style packets to transport TTY characters.

Depending on the presence of TTY characters on a call, the transmission toggles between voice mode and TTY mode. The system uses up to 16 kbps of total bandwidth when sending TTY characters, and normal bandwidth of the audio codec for voice mode. This mode may be used for TTY calls to and from Communication Manager R2.0 systems.

Pass through mode

Alternatively, you can choose to have TTY signals sent in pass through mode. With pass through mode enabled, when the system detects TTY characters, the system uses G.711 encoding to transport the TTY signals end-to-end over the IP network. G.711 encoding pass through mode means the TTY signals are changed to digital format, and are delivered to the receiving endpoint after unencoding the digital signals.

Pass through mode provides higher quality transmission when endpoints in the network are all synchronized to the same clock source.

In pass through mode, you can also assign packet redundancy. Packet redundancy means the media gateways send duplicated TTY packets to ensure and improve quality over the network.

Pass through mode uses more network bandwidth than relay mode. Pass through TTY uses 87-110 kbps, depending on the packet size, whereas TTY relay uses, at most, the bandwidth of the configured audio codec. Redundancy increases bandwidth usage even more.

Unicode support for 4610SW telephone

The Unicode (formerly Multibyte) capability is enhanced to support the 4610SW telephone. This includes the Unicode (UTF-8) - Latin/Chinese/Cyrillic/Greek and Unicode (UTF-8) - Latin/ Japanese/Cyrillic/Greek font loads.

This capability increases the range of telephones that can support the Unicode capability. This allows multi-lingual solutions to be supported for customers, including support of Chinese, Japanese, Russian, Greek, and many other languages.

Field names that support a Unicode value are:

- **Station Name**
- **VDN**
- **Hunt Group**

Unicode telephone messages

All Communication Manager telephone messages support Unicode. Installing and loading of the custom_unicode.txt file does not require a reset 4.

Upload files for the local TFTP server

This feature adds a capability to the existing web pages to support download and installation of files in the **/tftpboot** directory. Such files are required to contain a valid signature. This feature supports download and installation of firmware for the G350 and G700 Media Gateways and IP telephones. The **/tftpboot** directory is editable by members of the SUSERs Linux login group.

This feature is only supported on the S8300 Media Server.

Warning for ’pending’ on main processor

From the main processor, if you change the WAN Processor Role from "main" to "pending" on the **Maintenance-Related System Parameters** screen, a warning notifies you that changing Role to ’pending’ should normally be performed only on a WSP. To display the **Maintenance-Related System Parameters** screen, use the command **change system-parameters maintenance**.

Release 2.0 new features and enhancements

Avaya Communication Manager, release 2.0, includes the following general telephony and system-wide features and enhancements.

Adjunct route support for network call redirection

This feature provides the capability to invoke network call redirection (NCR) through the route request response to an adjunct route vector step. This allows a CTI application to directly utilize NCR for redirecting an incoming call in the PSTN through the ASAI adjunct routing application.

The redirection request, along with the PSTN redirected to a telephone number, is included in the route select message from the adjunct. The redirect request invokes whatever format of network redirection that is assigned to the trunk group for the incoming call in the same manner as a vector invoked NCR. Information forwarding to the redirected destination is supported in the same manner as a vector invoked NCR.

This capability functions with either the network transfer type (the system sets up the second leg of a call), or the network deflection type (the PSTN sets up the second leg of a call) of NCR protocols.

AES encryption algorithm for bearer channels

To provide privacy for media streams that are carried over IP networks, Communication Manager supports media encryption for the:

- H.248 signaling channel between the Media Server and the Media Gateway
- H.323 signaling channel between the Media Gateway and IP endpoints
- IP bearer (voice) channel

Digitally encrypting these channels can reduce the risk of electronic eavesdropping. IP packet monitors, sometimes called sniffers, are to VoIP calls what wiretaps are to circuit-switched (TDM) calls, except that an IP packet monitor can watch for and capture unencrypted IP packets and can play back the bearer channel conversation in real-time or store it for later playback. Comprehensive network security requires encrypting the signaling channels that might carry user-dialed authorization codes and passwords.

Communication Manager supports the Advanced Encryption Standard (AES) format of signal encryption for IP telephony. This encryption algorithm is in addition to Avaya’s proprietary encryption protocol, the Avaya Encryption Algorithm (AEA).

AES encryption is a cryptographic algorithm developed by the U.S. Government to protect unclassified information. Communication Manager uses AES with 128 bit keys in counter mode (AES-128-CTR).

Administration is supported to select a combination of no encryption, AEA encryption, and/or AES encryption on a by codec set basis.

ASAI user to user information (UUI) to CMS

The ASAI user-to-user information (UUI) that is stored for a call is passed to the call management system (CMS). The ASAI UUI information (maximum of 96 bytes) is passed to the CMS in a message for storage in the external call history (ECH) call record.

This information can be used to record ASAI user data for the Variables for Vectors feature and for other applications. The UUI data is sent to CMS every time the call is routed to a VDN. This is particularly useful to supplement the Variables for Vectors feature where an "**asaiuui**" variable type is used to make decisions in vector processing for a call.

Avaya Extension to Cellular/OPS

Avaya Extension to Cellular and off-PBX stations (OPS) provides users with the capability to have one administered telephone that supports Avaya Communication Manager features for both an office telephone and one outside telephone. Extension to Cellular/OPS allows users to receive and place office calls anywhere, any time. People calling into an office telephone can reach users even if they are not in the office. Users could receive the call on their cell phone, for example. This added flexibility also allows them to use certain Communication Manager features from a telephone that is outside the telephone network.

Extension to Cellular

Previous versions of Extension to Cellular allowed for office calls to be extended to a user's cell phone. Also, calls from the cell phone would appear as if the call originated from the user's office telephone when calling another telephone on the same call server. Certain features within Communication Manager are available from the cell phone. These features are still available.

In previous versions of Extension to Cellular, cell phones had to be administered as XMOBILE stations. This is no longer necessary with Communication Manager release 2.0.

If you had administered Extension to Cellular in earlier releases of Communication Manager, you do not have to change the administration to continue using Extension to Cellular features. It still works. However, users would not have the full range of features that are now possible with Extension to Cellular/OPS.

Off-PBX station

New with Avaya Communication Manager release 2.0, the off-PBX station (OPS) application type is used to administer a Session Initiation Protocol (SIP) telephone. OPS cannot be disabled using the Extension to Cellular enable/disable feature button.

Note:

A SIP telephone, such as the 4602 SIP telephone, must register with the SIP proxy regardless of whether OPS is administered.

The Extension to Cellular/OPS application allows for many of the parameters used for the original Extension to Cellular application to be ported onto one of several DCP and IP telephone types. From a call processing perspective, Extension to Cellular/OPS is dealing with a multi-function telephone, whereas the previous Extension to Cellular implementation utilized one or two XMOBILE stations that behaved like analog telephone types.

What’s new in Extension to Cellular/OPS

In addition to features in previous releases of Communication Manager and Extension to Cellular, Extension to Cellular/OPS enhancements for release 2.0 include the following:

- The ability to support Session Initiation Protocol (SIP) telephones.
- Simplified administration of Extension to Cellular/OPS.
- The ability for the administrator to map certain Communication Manager features to telephone extensions. You just dial one of those extensions, called a feature name extension (FNE), from your cell phone to activate a Communication Manager feature.
- An Extension to Cellular feature button that allows you to extend a call that is received at the office telephone, and extend it to your cell phone.
- An Extension to Cellular feature button that allows you to exclude anyone from joining in on your conversation from your office telephone.
- The ability to administer the number of call appearances that are allowed to be mapped to the cell phone or SIP telephone.

The Extension to Cellular feature buttons are available on office telephones that support administrable feature buttons. This includes the feature button to enable and disable cell phones. You administer the buttons onto the office telephone, the telephone to which the Extension to Cellular is linked.

Note:

SIP-enabled telephones cannot be enabled or disabled using a feature button.

Avaya integrated management

Avaya integrated management is a systems management software suite that contains applications to manage a converged voice and data network. The applications include:

- network management
- fault management
- performance management
- configuration management
- directory management
- policy management functionality

Avaya Interactive Response

The Avaya Interactive Response (IR) is an interactive voice-response system that automates telephone call transactions from simple tasks, like routing to the right department, to complex tasks, such as registering college students or providing bank balances. IR communicates with customers in natural-sounding, digitally recorded speech, and performs 24-hours a day without the services of an operator. Avaya Interactive Response (IR) was formerly known as INTUITY Conversant®.

The system can handle single or multiple voice-response applications simultaneously, and can serve up to 48 callers at once. It can operate by itself to dispense information or collect data, or it can work with a host computer to access a large database such as bank account records. With its speech-recognition capability, even rotary telephone users can have access to sophisticated telephone-based services. Advanced telephone features provide intelligent call-transfer capabilities and allow you to use the system in your existing telephone environment.

Avaya IP Softphone

Avaya IP Softphone extends the level of Communication Manager services. This feature turns a PC or a laptop into an advanced telephone. Users can place calls, take calls, and handle multiple calls on their PCs.

Note:

R1 and R2 IP Softphone and IP Agent, which use a dual connect (two extensions) architecture, are no longer supported. R3 and R4 IP Softphone and IP Agent, which use a single connect (one extension) architecture, continue to be supported. This applies to the RoadWarrior configuration and the Native H.323 configuration for the IP Softphone.

The R5 release of the IP Softphone supports a number of enhanced features, including the following:

- Improved endpoint connection recovery algorithm
- AES media encryption (see AES encryption algorithm for bearer channels on page 46)
- Instant Messaging (see Converged communications server on page 52)
- Unicode support (see Unicode support on page 67)
- Softphone and Telephone Shared Control (see IP Softphone and telephone, Shared Control mode on page 50)

The IP Softphone provides a graphical user interface with enhanced capabilities when used with certain models of DCP telephones. Communication Manager supports a mode of H.323 registration that allows an IP Softphone to register for the same extension as a DCP telephone without disabling the telephone. It also allows the IP Softphone to send button-push messages and receive display and call progress messages in parallel with the telephone. In this mode, the Softphone does not terminate any audio.

IP Softphone and telephone, Shared Control mode

IP Softphone and telephone, Shared Control mode, enables users to have a telephone endpoint and an IP Softphone in service simultaneously on the same extension number. IP Softphone and an IP telephone can be integrated so that the IP softphone can control the IP telephone on a person’s desk, and vice versa. This allows the power of the PC desktop (LDAP directories, TAPI PIMs/Contact Managers, etc.) to be used in conjunction with a desktop IP telephone.

An IP softphone can register to an extension number that is already assigned to an in-service telephone endpoint. From that point on, user actions carried out by either endpoint apply to calls to or from the extension. Only the telephone endpoint carries audio for the extension.

BSR local treatment for calls queued remotely over IP or ISDN trunks

This feature allows playing announcements and music from the local system, while a call is waiting in queue at a remote system. This is a result of Multi-Site Best Service Routing. This provides a savings for IP resources and transport, because VoIP is not needed until the call is answered.

This feature also allows localization and centralized management of announcements, because they can be provided by the local system. In addition, this feature provides the capability to take back BSR calls that wait too long, because the call remains under local system control in vector processing until the call is answered.

Call admission control bandwidth management

In order to ensure quality of service for voice over IP (VoIP) calls, there is a need to limit overall VoIP traffic on WAN links. The call admission control (CAC) bandwidth management feature of Communication Manager allows the customer to specify a VoIP bandwidth limit between any pair of IP network regions. The feature then denies calls that need to be carried over the WAN link that exceed that bandwidth limit.

Camp-on/Busy-out

A **`camp-on/busy-out`** command is commonly used by system technicians to busy-out system resources that need maintenance or repair. Without it, all active calls using those resources are indiscriminately dropped if the resource is physically removed from the system. This disruptive action causes problems for customers, especially when a large number of calls are torn down.

The camp-on/busy-out feature adds the ability to remove idle VoIP resources from the system's pool of available VoIP resources.

Note:

This feature is not supported by the G700 or G350 Media Gateway platforms.

The camp-on/busy-out feature enables the user to select the media processor to be busied-out while the media processor is still in service. After a call ends that was using resources within the specified media processor, the idled resource is removed from the system's pool of available resources. Once all of the media processor's resources are in a "busy-out" state, the associated board can be removed from the system without disrupting active calls.

CLAN load balancing

CLAN load balancing is the process of registering IP endpoints to CLAN circuit packs (TN799x). Load balancing occurs among CLANs within a network region.

IP endpoint registration among CLAN circuit packs is done through an algorithm. This algorithm tracks the number of sockets being used by TN799x circuit pack, and registers IP endpoints to the TN799x with the most available (unused) sockets. This algorithm applies to H.248, H.323 signaling groups, H.323 telephones, and SIP telephones. Sockets used by adjuncts are not included in the socket count.

Communication Manager API

Communication Manager API provides a connector to Communication Manager that allows clients to develop applications that provide device and media control. Applications can register as IP extensions on Communication Manager and then monitor and control those extensions, and their RTP media streams.

Communication Manager API consists of connector server software and a connector client API library. The connector server software runs on a hardware server that is independent from Communication Manager. That is, Communication Manager API does not run co-resident with Communication Manager.

Control network on customer LAN

This enhancement eliminates the need for a private IP control network for S8700 Multi-Connect configurations. In previous releases of Communication Manager, there is a stipulation that requires that S8700 servers, the Cajun Ethernet switches, and IPSI boards be the only components delivering traffic on this network. This enhancement eliminates this restriction and affords the option to implement the control network on customer LAN, as is done for the S8700 IP-Connect systems.

Converged communications server

The converged communications server adds a leading edge set of features to current enterprise customers. Through SIP, enterprise customers can send text instant messages through an instant message client integrated with the Avaya IP Softphone.

A presence-enabled buddy list gives enterprise users information on when colleagues are available. The converged communications server includes a SIP proxy, registrar, and presence server, as well as an instant message gateway to the popular consumer instant messaging networks (such as AOL, MSN, and Yahoo).

Disk survivability

The disk survivability feature allows call processing to continue in the event of a hard disk outage. Survivability of disk outages is provided by implementing the root (/) file system in a RAM disk partition, such that all critical files and data are physically stored in RAM disk space instead of on the hard disk media. Non-essential files and data are accessed indirectly from the RAM disk file system by means of links established by boot scripts.

For Communication Manager release 2.0, this feature is only available with the S8500 Media Server.

E911 ELIN for wired IP extensions

This feature automates the process of assigning an emergency location information number (ELIN) through an IP subnetwork ("subnet") during an emergency 911 call. The ELIN is then sent over either CAMA or ISDN PRI trunks to the emergency services network when 911 is dialed. This feature properly identifies locations of wired IP telephones that call an emergency number from anywhere on a campus or location.

Note:

This feature depends upon the customer having subnets that correspond to geographical areas.

This feature works on H.323 IP endpoints. For SIP IP endpoints, you must use the off-PBX station (OPS) option of the Avaya Extension to Cellular feature (see Avaya Extension to Cellular/OPS on page 47).

A caller who needs emergency assistance dials a Universal Emergency Number, for example, 911 in the United States, 000 in Australia, and 112 in the European community. The call routes through a local Central Office, through an emergency tandem office, to the appropriate Public Safety Answer Point (PSAP). The PSAP answers the call.

With Enhanced 911 (E911), the system might send to the emergency services network the Calling Party Number (CPN) with the call over Centralized Automatic Message Accounting (CAMA) trunks or through the Calling Number IE over ISDN trunks. The PSAP uses the CPN to lookup the caller’s documented street address location from the Automatic Location Information (ALI) database. The ALI database is usually owned and managed by Local Exchange Carriers. Many enterprise customers choose to contract with a third party to update the ALI database for them.

This depends on the assumption that a CPN always corresponds to the street address that the system owner arranged to have administered into the ALI database. This assumption is not always true.

- Users who have H.323 IP telephones can move them without notifying the system administrator.
- Users who have SIP IP telephones can use the same extension number simultaneously at several different telephones.

Without this feature, if these users dial 911, the emergency response personnel might go to the wrong physical location. With this feature, the emergency response personnel can now go to the correct physical location. In addition, emergency response personnel can now go to the correct physical location if a 911 emergency call comes from a bridged call appearance.

ETSI Explicit Call Transfer protocol for NCR

The Network Call Redirection (NCR) support of the ETSI Explicit Call Transfer (ECT) protocol is desired by multi-site, non-U.S. Avaya call center customers who use various PSTN service providers for ISDN services. These non-U.S. call centers wish to accomplish call transfers between sites without holding the ISDN trunks of a transferred call at the call redirecting Communication Manager site. ETSI ECT redirects the call using the subscribed-to network transfer service instead of using a trunk-to-trunk connection.

NCR can be invoked in vectoring, or by telephone/attendant/ASAI transfer.

H.248 link encryption

To provide privacy for media streams carried over IP networks, the H.248 signaling channel between the media server (media gateway controller) and the media gateways is encrypted. This signalling channel is used to distribute the media session keys to the media gateways, and may carry user-dialed authorization codes and passwords.

This feature protects our customer investments by encrypting the signaling channel between the gateway, including the G700 and G350 Media Gateways, and server (using proprietary technology). This feature also protects media encryption key, PINs, and account codes between the media gateway and the media gateway controller.

Encryption of the H.248 link to any given media gateway may be enabled or disabled through the Media Gateway screen. The encryption protocol cannot be disabled.

H.323 link recovery

This feature supports the detection of and recovery from a failed H.323 signaling channel link between an H.323 IP endpoint and an Avaya media server running Communication Manager release 2.0.

The H.323 link between an Avaya Media Gateway and an H.323-compliant IP telephone provides the signaling protocol for:

- Call setup
- Call control (user actions such as Hold, Conference, or Transfer) while the call is in progress
- Call tear-down

If the link goes down, H.323 Link Recovery preserves any existing calls and attempts to re-establish the original link. If the endpoint cannot reconnect to the original gateway, then H.323 Link Recovery automatically attempts to connect with alternate TN799DP (CLAN) circuit packs within the original server's configuration, or to a local spare processor (LSP).

H.323 Link Recovery does not diagnose or repair the network failure that caused the link outage, however it:

- Attempts to overcome any network or hardware failure by re-registering the IP endpoint with its original gateway
- Maintains calls in progress during the re-registration attempt
- Continues trying to reconnect if the call ends and the IP endpoint has not yet reconnected to its original gateway
- Attempts connecting to and registering with an alternate gateway if so configured

Hardware errors & alarms added to hard drive trace log

Hardware errors, alarms, and alarm resolutions have been added to the trace log. Software errors and alarms are already tracked on the trace log. The trace log is kept on the hard drive on Linux- and Windows-based servers so they can be retrieved for review and action.

IP connections and disconnections

In order to improve the diagnosis of network problems, a log of all IP connections and disconnections is added to the "tracelog" for the Linux-based and Windows-based platforms. The new event types to be logged include IP endpoint registrations, IP endpoint unregistrations, Ethernet interfaces coming into service, and Ethernet interfaces going out of service.

These new events in the tracelog will be tagged as a new log type. This log will be viewable from server commands in Linux and Windows and will also be viewable from the Linux-based maintenance Web pages by selecting the new log type.

IP overload control

This enhancement more effectively manages processor occupancy overload situations. The enhancement applies selected overload mechanisms at a lower occupancy threshold in an effort to avoid more serious symptoms experienced at higher occupancy levels.

The IP overload control enhancement:

- fortifies the system against bursts of registration traffic
- provides a mechanism to alert the far-end to abstain from issuing registrations for some specified period of time
- records the event to maintain a history of potential performance problems
- optimizes the maximum number of simultaneous registrations the server can handle based on the available memory and CPU cycles
- reduces the frequency that a server might go into overload due to network problems

ISDN calls to busy stations treated as ACA short calls

ISDN calls placed to user stations that are busy were labeled as ACA short calls.

Note:

ACA stands for Automatic Circuit Assurance, a feature that tracks calls of unusual duration to help with troubleshooting. For example, a high number of very short calls, or a low number of very long calls, might indicate a problem with the trunk.

ACA short calls generate an notification to the system administrator through a lamp update and a referral call. There is also an ACA log to track events.

A customer might not want to treat short ISDN calls to busy stations as an ACA short call. Therefore, a new field has been added to the **Feature-Related System Parameters** screen. See Feature-Related System Parameters screen on page 145 for more information.

Maximum agent occupancy

This feature provides two fields on the **Feature Related System Parameters** screen to set, on a system basis, an allowed maximum occupancy level for EAS agents. When the maximum occupancy level is exceeded, the system puts the agent into Aux Work, using the specified reason code, until the occupancy of the agent goes below the assigned maximum.

Multi-Location Dial Plan

When a customer migrates from a multiple voice server QSIG/DCS network to a single voice server whose gateways are distributed across a data network, it may initially seem as if some dial plan functions are no longer available.

This feature preserves dial plan uniqueness for extensions and attendants that were provided in a multiple QSIG/DCS network, but were lost when customers migrated to a single distributed network. This feature provides dial plan capabilities similar to those provided before the migration, including:

- extension uniqueness
- announcement by location
- local attendant access
- local ARS code administration

A major reason to migrate customers from a multiple QSIG/DCS environment to a single S8700 network is to provide a greater set of features and help reduce costs. Migrating to a single network reduces the number of systems a customer has to maintain. Migrating to a single network, in turn, lowers administration costs. You have one system to administer instead of multiple switches, one dial plan to maintain, and so on. With a single distributed network solution, some features no longer work transparently across multiple locations.

For example, in a department store with many locations, each location might have had its own system with a QSIG/DCS network. That way, the same extension could be used to represent a unique department in all stores. For example, extension 123 might be the luggage department in all stores. If the customer migrates to a single distributed network, this functionality is not available without this feature.

In addition, an S8700 solution does not assure that a call that is routed to an attendant would terminate at the local attendant. Let us use an example of a public school district that previously was networked with a system at each school. If the school district migrates to an S8700 network, dialing the attendant access code at your school may not route your call to the local attendant.

Instead of having to dial a complete extension, the Multi-Location Dial Plan feature allows a user to dial a shorted version of the extension. For example, a customer can continue to dial 4567 instead of having to dial 123-4567. Communication Manager takes the leading digits of the

location prefix, and adds those digits to the front of the dialed number. The system then analyzes the entire dialed string and routes the call based on the administration on both the **Dial Plan Parameters** screen and the **Dial Plan Analysis Table** screen.

Multiple level precedence and preemption

Multiple level precedence and preemption (MLPP) is an optional group of features that provide users the ability to interface to and operate in a Defense Switched Network (DSN). The DSN is a highly secure and standards-based communication system of the Department of Defense (DoD) of the US Government.

CAUTION:

MLPP is currently designed to meet only the US Government's Defense Switched Network Generic Switching Center Requirements (GSCR) for connection to a DSN by federal, state, or local government agencies. As such, MLPP is not currently designed for use in commercial enterprise environments. Activation of this feature in any other kind of network environment could result in unexpected and unwanted feature operations.

The MLPP features allow users to request priority processing of their calls during critical situations. The MLPP features include:

- Announcements for precedence calling
- Dual homing
- End office access line hunting
- Line load control
- Precedence call waiting
- Precedence calling
- Precedence routing
- Preemption
- Worldwide numbering and dialing plan

Announcements for precedence calling

In certain situations, precedence calls are blocked because of unavailable resources or improper use. When this occurs, recorded announcements are used to identify what went wrong. The announcements used for MLPP include:

- Blocked precedence call
- Unauthorized precedence level attempted
- Service interruption prevented call completion

- Busy, not equipped for preemption or precedence call waiting
- Vacant code

Dual homing

Dual homing allows a user to dial a telephone number and, if the initial route is unavailable, have the call route to its destination over alternate facilities.

End office access line hunting

End office access line hunting automatically hunts for an idle trunk over end office access lines, based on the precedence level of the call.

Line load control

Line load control is a feature that restricts a predefined set of telephone users from originating calls during a crisis or emergency. Through administration, users are assigned to a line load control level based on their relative importance. When an emergency occurs, the administrator manually enables the feature to restrict calling by users of lower importance. When the emergency is over, the administrator manually disables the feature.

For example, if a situation occurs that threatens national defense, telephone users in the defense department will not be restricted from originating calls, but stations in other departments, such as the accounting department, will be restricted. When the crisis is over, the system can be returned to normal operation by the administrator.

Precedence call waiting

After a precedence call is routed, the called party may already be busy on another call. Precedence call waiting allows the caller to "camp on" to the called party’s line and wait for them to answer the call. The caller hears a special ringback tone and the called party hears a call waiting tone.

Depending on the type of telephone being used, the called party can put the current call on hold and answer the call, or the called party must hang up on their current call to answer the incoming call.

Precedence calling

Precedence calling is the centerpiece of the MLPP features. Precedence calling allows users, on a call-by-call basis, to select a level of priority for each call based on their need and importance (rank). The call receives higher-priority routing, whether the call is local or going around the world.

Users may access five levels of precedence when placing calls:

- Flash Override (the highest precedence level)
- Flash
- Immediate
- Priority
- Routine (the default, and lowest precedence level)

Each telephone user is administered with a maximum precedence level, the more important or higher in rank the user, the higher the precedence level. Users cannot originate calls at precedence levels higher than their maximum administered level. Non-MLPP calls are treated as routine level precedence calls.

Precedence routing

When precedence calls are destined for other switches in a private network, the precedence routing feature is used to route the calls. The precedence routing feature routes calls based on three main criteria:

- Routing based on the destination number
- Routing based on the precedence level
- Routing based on the time of day

These routing criteria are administrable and can be changed as required. Two related features are dual homing and end office access line hunting.

Preemption

Preemption works with the precedence routing feature to further extend the call routing capabilities of the MLPP features. Preemption, when allowed through administration, can actually tear down an existing lower priority call in order to complete a more important precedence call. Even non-MLPP calls are treated as routine level precedence calls and can be preempted.

When this occurs, the callers on the existing call hear a tone indicating that the call is about to be preempted. The callers have three seconds to end the call before the call is automatically disconnected. After the existing call is disconnected, the new call is placed using preempted facility.

Worldwide numbering and dialing plan

The worldwide numbering and dialing plan (WNDP) feature allows Communication Manager to conform to the standard numbering system established by the Defense Communications Agency (DCA). WNDP defines its own format for the precedence dialing. The capability to operate with this numbering plan must be incorporated into all new switches introduced into the Defense Switched Network (DSN).

Multiple QSIG voice mail hunt groups

Communication Manager provides for ten message center hunt groups to support QSIG integrated messaging. This feature allows customers to spread users in a single Communication Manager system over multiple messaging systems. This allows users to move among Communication Manager systems while retaining their same voice mailbox. Users do not lose voice messages.

This feature also enhances customer usability of Avaya messaging systems in the enterprise by allowing not only for growth, but the ability to migrate end users on a single Communication Manager system.

National ISDN (NI-1 and NI-2) BRI voice endpoint support

Similar to Multiple level precedence and preemption on page 58, national ISDN (NI-1 and NI-2) BRI voice endpoint support is a feature that provides users the ability to interface to and operate in a Defense Switched Network (DSN). The DSN is a highly secure and standards-based communication system of the US Government's Department of Defense (DoD).

CAUTION:

National ISDN (NI-1 and NI-2) BRI voice endpoint support is currently designed to meet only the US Government's Defense Switched Network Generic Switching Center Requirements (GSCR) for connection to a DSN by federal, state, or local government agencies. As such, it is not currently designed for use in commercial enterprise environments. Activation of this feature in any other kind of network environment could result in unexpected and unwanted feature operations.

Support of the NI-1 and NI-2 standards is guided by the requirements in the GSCR. As such, this does not assure support for all the commercially available NI-1 and NI-2 compliant BRI endpoints.

Since the NI-BRI telephone can be configured in several modes, with its own capability for feature button management, it is of utmost importance that the terminal configuration must match the NI-BRI telephone support provided by Communication Manager. This implies that:

- Non-initializing NI-BRI terminals (NIT) are *not* supported.
- Valid SPID length is from 3 to 12 digits.

  Note:

  The maximum length according to NI-BRI standards is 20. Communication Manager allows a maximum SPID length of 12, consisting of 10 digits for the USID (SPID on the NI-BRI Administration screen) and 2 digits for the TID (or endpoint ID on the Administration screen).
- Native support is for NI-BRI voice endpoints only. Native support for NI-BRI data endpoints is not offered. NI-BRI data endpoints must be administered as **wcbri** data-module type.
- The NI-BRI telephone must be programmed as CACH-EKTS mode only. Any other mode is *not* supported.
- The number of call appearances programmed on the terminal must be equal to the number of call appearances administered on the corresponding NI-BRI telephone screen.
- Communication Manager does not support multiple directory numbers by endpoint. There is one extension by endpoint.
- Conference, transfer, and drop feature buttons must be programmed in order to support features above and beyond the basic call services.
- Integrated voice/data endpoints must be configured to be either a voice-only NI-BRI endpoint (administered as **NI-BRI** telephone type), or as standalone data-only endpoint (administered as **wcbri** data-module type).

No shutdown when UPS looses battery power

If there's a power failure, an uninterruptible power supply (UPS) takes over to make sure call processing can continue. Prior to release 2.0, when the UPS warns of low battery power remaining (3 minutes), the server initiated a shutdown.

With release 2.0, the UPS continues to function until it has no battery power left. No shutdown is initiated. If power can be restored within the time that the UPS battery would have run out of battery power, there is no interruption to call processing. If the UPS runs out of battery power and the server loses power, no damage is done to the server.

Parsing capabilities for the history report

The history report provides details about every data command. You can use parsing options to limit the data returned in this report. The following table identifies the parsing options that are available.

Note:

You can display these options by entering the command **`list history`**, then clicking **HELP** or pressing **F5**.

Option	Description
date	Specify the month (**MM**) or day (**MM/DD**) for which to display history data.
time	Specify the hour (**HH**) or minute (**HH:MM**) for which to display history data.
login	Specify the login for which you wish to display history data.
action	Specify the command action (the first word of the command string) for which you wish to display history data. You can view the list of available command actions by clicking **HELP** or pressing **F5** at the command line.
object	Specify the command object for which you wish to display history data.
qualifier	Specify the command qualifier for which you wish to display history data.

To limit the data displayed in the history report, enter the command **`list history`** followed by a space and the appropriate parser and, if applicable, format. Only the data for the specified parsers will appear in the report.

You can include multiple parsers, but only a single instance of any parser (for example, you may parse for **date**, **time**, and **login**, but not for **date**, **time**, and two different **logins**).

Print option for 4425 terminal

A print option has been extended to 4425 terminal types, as currently exists with 4410 terminal types.

Russian MF shuttle tone level enhancements

A gain of 0 is applied to Russian multi-frequency (MF) shuttle trunks and outgoing Russian multi-frequency ANI. Now, the received and transmitted signal gains administered on the multi-frequency screen are applied to MF shuttle trunks. Also, the transmitted signal gain is applied to outgoing Russian multi-frequency ANI. This is in order to comply with recent Russian requirements.

Service level maximizer

The service level maximizer is a packaged capability that works with active Avaya Expert Agent Selection (EAS). It includes simplified administration to bring the benefits of advanced, predictive call distribution to the widest range of potential call center customers. This is done by meeting a customer's pre-defined service level targets for all skills within a call center.

Service level maximizer maximizes agent utilization to help a call center meet service level targets for all skills. It does require Avaya Expert Agent Selection (EAS) to be active. Unlike EAS, service level maximizer does not require call surplus decisions as to the use of either skill level (ensuring most expert agent agents) or greatest need for those skills.

Agent surplus decisions tied to Expert Agent Distribution also do not apply to those skills using service level maximizer. This means that, with service level maximizer active by skill (hunt group), there is no assurance that the most expert agents answer inbound ACD calls. The reason is skill level and expert agent distribution are not used. Those skills with service level maximizer active also do not consider agent fairness because the concept of least occupied agent is overridden in support of meeting service level targets.

Session Initiation Protocol

Session Initiation Protocol (SIP) is an endpoint-oriented messaging standard defined by the Internet Engineering Task Force (IETF). The various types of existing telephones continue to be supported by Communication Manager (analog, DCP or H.323 telephones and analog, digital or IP trunks), and now the new SIP-enabled telephones, such as the Avaya 4602 SIP Telephone, are supported by the media servers/gateways with full name/number delivery between them.

In addition to its calling capabilities, IP Softphone release 5.07 and later includes instant-messaging client software, which is a SIP-enabled application, while continuing its full support of the existing H.323 standard for call control.

SIP is available with Avaya Communication Manager, release 2.0.1.

SIP trunks

With Avaya Communication Manager, release 2.0.1, SIP trunking functionality allows a Linux server (S8300, S8500, or S8700) to function as a POTS gateway between traditional legacy endpoints (stations and trunks) and SIP endpoints. It also provides SIP-to-SIP routing. In the routing scenario, the server supports call routing similar to what a SIP proxy would provide.

SIP links can be secured using TLS to encrypt signaling, and use Digest Authentication to perform validation. When using TLS, the Media Encryption feature is also available to encrypt audio channels.

SIP trunking functionality:

- Provides access to less expensive local and long distance telephone services, plus other hosted services from SIP service providers
- Provides presence and availability information to members of the enterprise and authorized consumers outside the enterprise, including other enterprises and service providers
- Facilitates SIP-enabled converged communications applications within the enterprise, such as the Seamless Service Experience.

Allowing encryption of signaling and audio channel provides the customer with the option to provide a secure communications infrastructure.

Signaling encryption for SIP trunks

Signaling encryption for SIP trunks protects customer investments by encrypting the voice channel over SIP trunks.

Support for SIP telephones

Support for SIP telephones, which are administered as off-PBX stations (OPS) using SIP trunks, allows any fully compliant SIP telephone to interoperate with Avaya telephones. This means any SIP telephone, from Avaya or a third party, that complies with the appropriate RFC or draft service standards, can:

- Dial and be dialed as an extension in the enterprise dial plan. OPS telephones support additional features as well, like bridging. For more details, refer to the *Avaya Extension to Cellular User's Guide*, 210-100-700, and the *Avaya Extension to Cellular and Off-PBX Station (OPS) Installation and Administration Guide*, 210-100-500.
- Put calls on hold and participate in transfers and conference calls.

Note:

These features are available using SIP telephones managed by media servers running Avaya Communication Manager 2.0.1 or later, but *not* using SIP telephones, which may register with a SIP proxy server, and are *not* managed directly through Communication Manager.

SNMP setting of QoS parameters

In Communication Manager release 2.0, the native SNMP agent allows setting of QoS parameters through SNMP. The check box on the administrator's **SNMP Agents** page has been changed from **Check to enable busyout/release setting** to **Check to enable busyout/ release and qos parameter setting**.

TTY

People with hearing or speech disabilities often rely on a device known as a TTY in order to communicate on telephone systems. The term "TTY" is an abbreviation for Teletypewriter. (The term "TDD", telecommunication device for the deaf, is also frequently used. The term TTY is generally preferred, however, because many people who use these devices are not deaf.)

TTY devices typically resemble small laptop computers, except that there is a one- or two-line alphanumeric display in place of the computer screen.

Connection to the telephone network is generally through an acoustic coupler into which the user places the telephone’s handset, or through an analog RJ-11 tip/ring connections.

Reliable transmission of TTY signals is supported by Communication Manager. This complies with the requirements and guidelines outlined in United States accessibility-related laws. Those laws include:

- Titles II, III, and IV of the Americans with Disabilities Act (ADA) of 1990.
- Sections 251 and 255 of the Telecommunications Act of 1996.
- Section 508 of the Workforce Investment Act of 1998.

Communication Manager’s TTY support is currently restricted to TTY devices that use the US standard TTY protocol. That protocol is specified by ANSI/TIA/EIA 825: "A 45.45 Baud FSK modem."

Important characteristics of this standard are:

- TTYs are silent when not transmitting. Unlike fax machines and computer modems, TTYs have no "handshake" procedure at the start of a call, nor do they have a carrier tone during the call. This approach has the advantage of permitting TTY tones, DTMF, and voice to be intermixed on the same call.

  Note:

  A large percentage of people who use TTY devices intermix voice and typed TTY data on the same call. The most common usage is by people who are hard of hearing, but nevertheless able to speak clearly. These people often prefer to receive text on their TTY device and then speak in response. This process is referred to as voice carry over (VCO).

- Operation is "half duplex". TTY users must take turns transmitting and typically cannot interrupt each other. If two people try to type at the same time, their TTY devices might show no text at all or show text that is unrecognizable. Also, there is no automatic mechanism that lets TTY users know when a character they have correctly typed has been received incorrectly.
- Each TTY character consists of a sequence of seven individual tones. The first tone is always a "start tone" at 1800 Hz. This is followed by a series of five tones, at either 1400 or 1800 Hz, which specify the character. The final tone in the sequence is always a "stop tone" at 1400 Hz. The stop tone is a border that separates this character from the next.

The following types of systems support TTY communication:

- Analog telephones and trunks
- Digital telephones and trunks
- VoIP gateways
- Messaging systems
- Automated attendant systems
- IVR systems
- Wireless systems in which a TTY-compatible coder is used

As long as the user's TTY device supports the following, Communication Manager allows:

- Voice and TTY tones to be intermixed on the same call.
- DTMF and TTY (with or without voice) to be intermixed on the same call. This allows TTY users to access DTMF-based voice mail, auto-attendant, and IVR systems.
- The use of acoustically coupled and "direct connect" (RJ-11) TTY devices.

TTY over analog and digital trunks

Communication Manager supports TTY calls within a gateway or port network between two analog telephones. TTY calls from a gateway or port network over analog trunks or digital trunks is also supported.

TTY over Avaya IP trunks

Communication Manager supports calls over IP trunks, as well as inter-gateway calls (IGC).

For this feature to work, both the sender (near end) and the receiver (far end) of a TTY call must each be connected to Avaya IP trunks. This feature will not work if either telephone is an IP telephone.

Unicode support

Communication Manager supports the display of non-English static and dynamic display text on Unicode-enabled endpoints. Non-English display information is entered into a Avaya Integrated Management application. Communication Manager processes, stores, and transmits the non-English text to endpoints that support Unicode displays. Unicode support is applicable to some firmware versions of the 4620 telephone, and the Softphone version of the 4620. It is not applicable to the 4690 telephone.

Unicode support provides the capability of supporting international and multi-national communications solutions. End-users are provided with a communications interface (delivered by an IP telephone or IP Softphone) in their own native language. This feature supports the Simplified Chinese, Japanese, and Korean (CJK) character sets.

Variables for Vectors

This enhancement to the call vectoring feature provides user assignable and changeable variables that can be tested in vectors using the **goto** command. Each variable is assigned a letter, such as A, B, C, and so on.

A particular variable can be used in many vectors. This allows a single user, caller, or CTI application change to effect a logic change in all vectors that the variable appears in. Local and global variables can be defined.

The threshold values and comparators that are applicable to a specific variable depend on the definition for the variable. The variables are defined in a table that is only administered through system administration.

Each variable can be assigned as a certain type that specifies its characteristics and how it gets set or changed. Types include:

- collected digits assigned
- ASAI user information for the call
- a value [between 0-9] that can be set by dialing a feature access code
- calendar/time type [day-of-year, day-of-week, or time-of-day], obtained from the system clock
- vdn, the active or latest extension of the VDN for the call

See Variables for Vectors screen on page 130 for the new screens associated with this feature.

VoIP resource selection improved

A high percentage of calls between IP endpoints and non-IP endpoints (circuit-switched endpoints) involve more than one port network (PN). A call between an IP endpoint and a non-IP endpoint located in different PNs might require TMD resources that tie up both PNs. This enhancement serves to lessen the overall TDM requirements, and therefore, the required number of PNs involved in the call.

For a call between an IP endpoint and a non-IP endpoint, the IP telephone is shuffled to the IP media processor in the non-IP telephone's PN if all of the following are true:

- if the IP media processor of the originating IP endpoint is in a different PN as the destination non-IP telephone
- if a IP media processor is available in the non-IP telephone's PN
- if both IP media processors are in the same region

Capacity changes

System capacities have been expanded for many products and features. However, the most up-to-date system capacity information is not listed in Communication Manager documentation.

Please see the *Avaya MultiVantage Solutions System Capacities Table*, 555-233-605, for the entire list of updated capacities.

To view the system capacity limits:

1. Go to the Avaya Web site at http://www.avaya.com/.
2. In the **Go To:** column, click the **Product Documentation** link.
3. In the **Search Support** text box on the **Technical Database/Product Documentation** screen, type **555-233-605**, or the words **capacities table**. Click **Go**.
4. Locate the latest version of the system capacities table document, and then click the title of the document to download the information.

Chapter 2: Hardware

This chapter presents highlights of any hardware as part of the most current releases of Avaya Communication Manager running on Avaya DEFINITY® servers, as well as the Avaya S8000 series Media Servers (with associated Avaya Media Gateways).

Release 2.2 hardware additions

Avaya Communication Manager, release 2.2, includes the following general hardware additions.

Branch gateway RFA tool

Users must register to create licenses for branch gateways. If users are already certified for Communication Manager in Remote Feature Activation (RFA), no additional certification is required for branch gateways. These users still need to register.

If not already certified, users need to take the Communication Manager training on RFA. No additional training for branch gateways is required.

DAL1 duplication memory card

The DAL1 is a circuit card similar in function to the DAJ1. The difference is that the DAL1 is designed to work with Pentium IV® processors, whereas the DAJ1 works with Pentium III® processors. The DAL1 uses a PCI-X interface, and is not compatible with Pentium III processors.

The P4 media server from Avaya is the S8710 Media Server.

DAL1 also has a different fiber interface than DAJ1. The DAL1 uses LC-type fiber connectors, while the DAJ1 uses SC connectors.

DHCP server for G350 Media Gateway

A DHCP server is introduced in the G350 Media Gateway. The DHCP server is also used as a platform for the W310 wireless Gateway. Prior to this release, the G350 Media Gateway supports only a DHCP-BOOTP relay in the router.

Support of a DHCP server on the gateway helps to connect IP telephones and other devices in a survivability mode while there is no connection to the main office.

G150 Media Gateway

The G150 gateway operates as an H.323 gateway that is managed by the Communication Manager feature server, in accordance with the Avaya Communication Manager Remote Office Feature Group. The G150 Media Gateway serves the very small market, generally defined as supporting less than 10 clients.

This gateway is available in three manufacturing build constructs, and offers:

- Analog loop start trunks
- Analog stations
- An optional PSTN WAN interface slot that is capable of supporting a T1, a quad BRI, or a quad analog trunk interface.

This gateway supports three modes of operation:

- Stand-alone IP Office
- Subtending H.323 gateway to ACM
- Survivable H.323 gatekeeper (as a subset of the subtending H.323 gateway) to allow gateway ports and co-located

IP telephones operate in basic calling mode.

S8500B Media Server

The S8500B (IBM x306) Media Server is a manufacturer’s lifecycle replacement for the S8500 (IBM x305) Media Server. The S8500B Media Server delivers exactly the same functionality as the S8500 Media Server.

The S8500B utilizes Augmentix’s Server Availability Management Processor™ (A+SAMP™) Card – a third party vendor remote maintenance board. The S8500 utilized IBM’s Remote Supervisor Adaptor (RSA) card.

Note:

The A+SAMP™ card will not function in the S8500 server, and the RSA card will not function in the S8500B server.

The S8500B system has a single USB modem connected to the A+SAMP card, whereas the S8500 uses two modems. The S8500B's modem can be accessed by both the SAMP and the HOST server (IBM x306) for dial-out purposes.

The modem is also used by Avaya Services to perform remote administration and maintenance on the entire system. All upgrade and migration paths that are available for the S8500 Media Server are also available for the S8500B Media Server. Since the functionality is exactly the same, no migration path exists from the S8500 to S8500B platform.

Augmentix remote maintenance board

The Augmentix Server Availability Management Processor™ (A+SAMP™) card is a third-party vendor Remote Maintenance Board that comes pre-installed in the S8500B (IBM x306) Media Server. The board serves the following purposes:

- Remote maintenance and serviceability to the media server
- Enhance the availability of the system
- Autonomous alarming, monitoring, and recovery of the media server

The A+SAMP™ card comes in a half card PCI form factor and is externally powered. The A+SAMP™ card supports a general purpose single USB and two 10/100BaseT Ethernet ports. The USB port comes with a USB modem attached for remote dial-in/dial-out purposes to/from the system. In other words, the HOST server (IBM x306) can access the modem through the A+SAMP™ card, and the HOST is also accessible by means of the modem through the A+SAMP™ card. One of the Etherent ports can be configured for Avaya Services laptop access, and the other is reserved for future use.

The A+SAMP™ card is treated as a Field Replaceable Unit (FRU), and runs the Linux operating system. All software and firmware that is running on the A+SAMP™ card is provided by Augmentix.

S8710 Media Server

The Avaya S8710 Media Server uses a standard microprocessor engine with an Pentium 4 Intel®-based processor on a commercial server. The S8710 Media Server uses high-speed connections to route voice, data, and video between analog and digital trunks, data lines that are connected to host computers, data-entry terminals, personal computers, and internet addresses.

Although the S8710 Media Server is provided by a different manufacturer than the S8700 Media Server, it has similar internal components and the same functionality as the S8700 Media Server. Both the S8700 Media Server and the S8710 Media Server supports and is compatible with release 2.1 of Communication Manager. The S8710 Media Server is a rack-mountable chassis.

The S8710 Media Server is the same as S8700 Media Server, except for the following characteristics:

- 10/100/1000 Ethernet ports to support IPSI network control links, services access, and administration
- 10/100 Ethernet ports to support IPSI network control links, duplication, and alarming
- External USB Compact Flash

The internal components include:

- DAL1 duplication memory card (700262306)
- 72-gigabit SCSI hard drive
- CD/DVD-ROM optical drive
- Flashdrive
- 4-port (10/100BaseT) network interface card (quad NIC)

The external components include:

- Compact flash (external; uses a USB port) (700290430)
- 15-foot (5-meter) DAL1 single-mode, fiber optic duplication cable with LC connectors (700290422), or

  300-foot (100-meter) DAL1 single-mode, fiber optic duplication cable with LC connectors (700326382)
- 15-foot (5-meter) CAT5 Ethernet arbiter duplication cable (700169998), or

  300-foot (100-meter) CAT5 Ethernet arbiter duplication cable (700244262)

The interface includes:

- Power on/off switch
- Reset switch
- 2 front panel indicators for hard disk access and power
- 2 USB, version 2, ports
- 2 10/100/1000/BaseT Ethernet ports (separate from quad NIC)

TFTP server for G350 Media Gateway

A TFTP server is introduced in the G350 Media Gateway. The main advantage of TFTP on gateway is that it provides a consistent experience for both customers and Services persons across all deployment scenarios.

A local TFTP server on a G350 gateway solves two separate problems:

- Survivability. A local TFTP server provides IP telephones with the files the system expects to receive after boot, including upgrade instructions and settings. The system provides the files even if the WAN uplink to the remote TFTP servers location is severed.
- Reducing or eliminating transmission of large firmware files over potentially low bandwidth WAN Links. This feature solves three issues:
  - The time it takes to upgrade telephones on site
  - The disruption to other traffic taking up the WAN bandwidth
  - The problems associated with using the TFTP protocol over congested low bandwidth WAN links

Release 2.1 hardware additions

Avaya Communication Manager, release 2.1, includes the following general hardware additions.

2410 DCP telephone

The 2410 digital communications protocol (DCP) telephone is a digital telephone with a streamlined small footprint design. The 2410 is geared for the general enterprise telephone user. Complementing the Avaya 2400 Telephone line with the use of a large display, the user interface is adapted to improve productivity and serviceability.

The 2410 DCP telephone has the following key features:

- High-end feature set with access to all the productivity capabilities available in Avaya Communication Manager
- Reduced installation and move costs with paperless labels
- Ready for multinational deployments with global design
- Large screen 5 line x 29 character display
- Fourteen fixed feature buttons

- Twelve label-less call appearances/feature buttons in 2 pages
- Large Message Waiting Indicator
- Full-Duplex Speaker plus Group Listen
- Local directory with 48 entries
- Local call log with 48 entries for missed, incoming answered, and outgoing calls
- Eight Personalized ring patterns
- Four softkeys
- One headset jack
- Global design (ICON labeled buttons)
- 8 user-selectable languages for softkeys and display messages:
  - English, German, French, Spanish, Italian, Dutch, Portuguese, and Katakana
- Hearing Aid compatible

Note:

The 2410 does not support any modules.

4601 IP telephone

The 4601 IP telephone is a cost-effective IP solution that is ideal for locations where basic telephone features are desired, such as entry-level staff positions, hallways, lobbies, and other common work areas.

The 4601 IP telephone connects to your IP network with a 10/1000 BaseT Ethernet LAN connection, and has the following key features:

- Two line appearance/feature keys
- Eight fixed feature keys:
  - Transfer
  - Conference
  - Drop
  - Redial
  - Message
  - Hold
  - Volume up
  - Volume down
- Message waiting indicator

- Hearing Aid compatibility
- Eight personalized ring patterns
- Downloadable software for future upgrade capability

IBM eServer BladeCenter HS20 Blade Server Type 8832

A third party server from IBM, an eServer BladeCenter HS20 Blade Server Type 8832, is now available to run Avaya Communication Manager. For more information on this blade server, see the following documentation:

- IBM eServer BladeCenter HS20 Type 8832 - Pre-Installation Job Aid
- Avaya Hosted IP Telephony Solution: Installing IBM eServer BladeCenter HS20 Type 8832, release 2.0, Installation Guide
- Avaya Hosted IP Telephony Solution: Installing IBM eServer BladeCenter HS20 Type 8832, release 2.0, Installation Guide

MM714 analog media module

The Avaya MM714 Media Module provides four analog telephone ports and four analog trunk ports. The MM714 is supported in both the G350 and the G700 Media Gateways.

MM717 DCP media module

The Avaya MM717 Media Module provides 24 Digital Communications Protocol (DCP) ports connected through an RJ21X Amphenol connector. The MM717 supports simultaneous operation of all 24 ports. Each port can be connected to a 2-wire DCP telephone. The MM717 does not support 4-wire DCP telephones. The MM717 is supported in both the G350 and the G700 Media Gateways.

MM722 BRI media module

The Avaya MM722 Media Module provides two 4-wire S/T ISDN BRI (Basic Rate Interface) 2B+D access ports with RJ-45 jacks. Each port interfaces to the central office at the ISDN T reference point. Information is communicated in the same manner as for the MM720. The MM722 is supported in both the G350 and the G700 Media Gateways.

Release 2.0 hardware additions

Avaya Communication Manager, release 2.0, includes the following general hardware additions.

2402 DCP telephone

The 2402 digital communications protocol (DCP) telephone is a digital telephone with dual (two) call appearance capabilities. The 2402 DCP telephone has both permanently-labeled feature buttons and administrable feature buttons. The 2402 does not support firmware downloads.

The 2402 telephone is aliased as a 6402 DCP telephone, with the following special instructions:

- The shifted dial pad # ("pound") key on the 6402 administration screen must be administered as an autodial button. Also, the dialup number for the voice mail system must be programmed into that autodial button. Since the Messages button on the 2402 telephone has the same button address as the 6402 shifted dial pad # ("pound") key, the 2402 Messages button now accesses the messages server.
- While aliased as a 6402, the 2402 shifted dial pad # ("pound") key cannot have an administered function. That is, the 2402 has 11, not 12, administrable feature buttons.

2420 DCP telephone firmware download

A new interface has been added for the 2420 DCP telephone firmware download that allows a user to initiate, schedule, and status the download. A user can also download multiple 2420 stations simultaneously.

4602SW IP telephone

The 4602SW telephones has improved functionality, including enhanced security and improved VLAN operation. The 4602SW telephone has a built-in Ethernet switch.

4602SIP telephone

A version of the 4602 telephone supports the Session Initiation Protocol (SIP) for basic call control. Session Initiation Protocol (SIP) is a signalling protocol used for establishing sessions in an IP network.

4610SW IP telephone

The 4610SW IP telephone has a built-in Ethernet switch. The 4610SW IP telephone provides advanced feature functionality with an intuitive and innovative user interface.

- a 168-by-80 pixel 4-gray scale display
- four softkeys
- six dynamically labeled call appearance/feature buttons
- four unique fixed feature buttons

The 4610SW IP telephone is aliased as a 4620 IP telephone.

4690 IP conference room speaker telephone

The 4690 IP SoundStation conference room speaker telephone supports Avaya's H.323-based IP single-connect protocol, including registration and proprietary DCP/CCMS messages. It supports multiple call appearances and administrable features. The 4690 IP conference telephone is aliased as a 4620 telephone so that it can receive downloaded button labels.

G350 Media Gateway

The G350 Media Gateway is a low-cost, modular device targeting the small branch office of a large enterprise. The G350 Media Gateway provides customers with an affordable converged solution for the remote/branch offices between 15-40 stations. Additionally, branch office customers do not have to sacrifice telephony features because this solution extends the power of Communication Manager in a survivable package.

Some of the highlights of the G350 Media Gateway include:

- VoIP media gateway with both trunk and line functions. A Communication Manager server acts as the call controller for the G350 Media Gateway. An S8300 ICC processor can be used in a G350 Media Gateway.
- The G350 Media Gateway can be controlled by an external S8700 or S8500 Media Server, or an internal S8300 Media Server.
- WAN (data) connectivity and routing for both H.248 connections to a call controller and for general inter/intranet connectivity, and LAN Switching, providing power over ethernet for IP telephones and wireless access points.

The G350 supports a new high density form factor, and provides a set of voice and data infrastructure services. The G350 Media Module utilizes the G700 Media Module form factor media modules (MM).

The following G700 form factor media modules have been developed:

- MM714 4FXS + 4FXO analog media module
- MM722 2-port BRI media module
- MM340 E1/T1 WAN routing media module
- MM342 V.35/X.21 WAN routing media module

The following boards conform to the new high density form factor.

- MM312 24-port DCP expansion module
- MM314 24-port PoE expansion module

G650 Media Gateway

The G650 Media Gateway is an enhanced rack mount cabinet that provides customers with an expandable gateway for traditional and IP configurations, a data form factor, and scalability.

The G650 also includes:

- Support for up to 14 universal TN- circuit pack slots in a common carrier
- Support for up to 5 G650s (70 total TN- circuit pack slots) in a port network
- A new 655A power supply design that:
  - operates from either AC or DC input power
  - can be used in either a stand alone or redundant configuration in a single carrier
  - provides load sharing and improved system availability when used in the redundant mode
- Enhanced environmental status and control, including voltage, current, temperature, and fan speed with a new serial bus that interconnects all the power supplies with the TN2312BP
- Simplified carrier address setting at installation

The redundant power supplies, coupled with the enhanced environmental reporting, improve the reliability, availability, and maintainability of the carrier over the existing G600 design.

655A power supply

The 655A power supply provides power for the G650 Media Gateway. Each power supply can communicate environmental information on the new serial bus when polled by the TN2312BP. A G650 can be equipped with one or two 655A power supplies. When two power supplies are used, they work in a current sharing mode. Either is capable of supplying power for a fully equipped G650.

The 655A power supply is capable of operating on either AC or DC input power. If both types of power are supplied, the 655A uses AC power first, but switches to DC power if AC power is unavailable.

The 655A is capable of providing North American (20 Hz) or European (25 Hz) ringing through a selection switch on the power supply. A third ringing selection can be made to provide no ringing when an external ringing source is provided, for example, TN2202 French (50 Hz) ringing. When two 655A power supplies are equipped in a single G650, only one provides ringing. The other 655A is in a standby ready mode to provide ringing if needed.

TN2312BP IPSI functionality

The G650 Media Gateway includes an enhanced Internet Protocol Server Interface (IPSI) circuit pack, the TN2312BP IPSI circuit pack. The TN2312BP circuit pack provides additional maintenance capabilities and features. The TN2312BP is backward compatible with the TN2312AP, but provides greater capabilities when used in the G650. The TN2312BP in an A carrier acts as a bus master for the G650 or G650 stack.

The TN2312BP IPSI functionality consists of:

- the existing IPSI (TN2312AP circuit pack) functions
- G650 cabinet maintenance

Features requiring the new TN2312BP I/O adapter (700263502):

- Customer provided alarm device (CPAD) control
- Emergency transfer panel control and L.E.D. indicator
- Major/minor alarm inputs from a UPS or other equipment
- IPSI duplication for IP-connected systems

Upgrades from the TN2312AP IPSI to the TN2312BP IPSI cannot be done with a firmware download only because new hardware features are included on the new circuit pack.

TN2312BP IPSI support of G650 cabinet maintenance includes:

- power/fan temperature monitoring
- an enhanced bus interface from the TN2312BP IPSI to the 655A power supplies in the G650 carrier
- a lead from the TN2312BP IPSI to the 655A power supply that provides environmental monitoring of the power supply and fan assembly

External readable CD ROM for S8300 Media Server

The S8300 Media Server supports an external readable CD ROM drive through one of the two USB ports on the S8300. The CD ROM is used for system software upgrades.

S8500 Media Server

The Avaya S8500 Media Server is a rack mounted telephony server, running the Red Hat Linux 8.0 Operating System, and featuring Avaya Communication Manager. The S8500 is capable of supporting both Internet Protocol (IP) and traditional endpoints enabling new technology, and the ease of migration from legacy Avaya systems. The S8500 Media Server is a perfect solution for mid-sized customers, with growth of up to 3200 ports.

- Migration path for DEFINITY servers CSI, SI, and S8100
- Supports distributed environment in a smaller scale
- Going forward platform to support IP telephony

Disk survivability

See Disk survivability on page 53.

Linux 8.0 support

New purchases of S8300, S8500, and S8700 Media Servers operate with the Red Hat Linux 8.0 operating system. The S8500 and S8700 Media Servers are shipped with blank hard drives. The operating system and release 2.0 of Communication Manager are shipped separately on a CD and installed on the media servers on site. The S8300 Media Server is shipped with the operating system and release 2.0 of Communication Manager on the hard drives.

Upgrading Communication Manager to release 2.0 on an existing S8300 Media Server or an S8700 Media Server requires upgrading the operating system to Red Hat Linux 8.0. The upgrade process requires remastering (reformatting) the hard drives, then loading the new software and operating system from a CD-ROM.

Chapter 3: New and changed screens

This chapter displays the new and changed administration screens for Avaya Communication Manager.

Release 2.2 new screens

Avaya Communication Manager, release 2.2, includes the following new screens. For a more complete explanation of the screens and their function, see the *Administrator's Guide for Avaya Communication Manager*, 555-233-506.

Native administration screens

2410 telephone

A native administration screen is available for the 2410 DCP telephone. Administrators no longer need to alias 2410 DCP telephones as 2420 telephones.

In addition, the firmware download capability for DCP telephones now includes the capability to download firmware to the 2410 DCP telephone.

4601 telephone

A native administration screen is available for the 4601 IP telephone. Administrators no longer need to alias 4601 IP telephones as 4602 telephones.

Release 2.2 changed screens

Avaya Communication Manager, release 2.2, includes the following changed screens. For a more complete explanation of the screens and their function, see the *Administrator's Guide for Avaya Communication Manager*, 555-233-506.

Attendant Console screen

A new field, **Always Use?**, is added to the **Attendant Console** screen. This change is prompted by the E911 device location for IP telephones feature.

To view the **Attendant Console** screen:

1. Type **change attendant** ***n***, where ***n*** is the number of the attendant console that you want to change. Press **Enter**.

   The system displays the **Attendant Console** screen.

2. Click **Next** until you see the **Always Use?** field (Attendant Console screen on page 84).

Figure 1: Attendant Console screen

```
change attendant 1                                              Page 2 of 4

                              ATTENDANT CONSOLE

VIS FEATURE OPTIONS
               Auto Start? y
      Echo Digits Dialed? y

IP FEATURE OPTIONS
Remote Softphone Emergency Calls: as-on-local Direct IP-IP Audio Connections? y
Emergency Location Ext: 4567       Always Use? n        IP Audio Hairpinning? y
```

Valid entries	Usage
y	When a user dials an emergency number, Communication Manager uses the value in the Emergency Location Extension field as the number of the calling party.
n	Default value. When a user dials an emergency number, Communication Manager uses the IP subnetwork (subnet) feature to determine the location of the calling party. This option depends upon the customer having subnets that correspond to geographical areas.

Feature-Related System Parameters screen

A new field, **Service Observing Allowed with Exclusion?**, is added to the **Feature-Related System Parameters** screen.

This change is prompted by the Call center service observing with exclusion feature.

To view the **Feature-Related System Parameters** screen:

1. Type **`change system-parameters features`**. Press **Enter**.

   The system displays the **Feature-Related System Parameters** screen.

2. Click **Next** until you see the **Service Observing** area (Feature-Related System Parameters screen on page 85)

Figure 2: Feature-Related System Parameters screen

```
                    Feature-Related System Parameters

CALL CENTER SYSTEM PARAMETERS
  EAS
         Expert Agent Selection (EAS) Enabled? y
        Minimum Agent-LoginID Password Length:
          Direct Agent Announcement Extension:                  Delay:
    Message Waiting Lamp Indicates Status for:

VECTORING
                    Converse First Data Delay: 0     Second Data Delay: 2
               Converse Signaling Tone (msec):        100 Pause (msec): 70
                     Prompting Timeout (secs): 10
                 Interflow-qpos EWT Threshold: 2
    Reverse Star/Pound Digit For Collect Step? n
           Available Agent Admustment for BSR? y

SERVICE OBSERVING
              Service Observing: Warning Tone? y    or Conference Tone? n
     Service Observing Allowed with Exclusion? n
```

Service Observing Allowed with Exclusion? field

Valid entries	Usage
y	The system allows service observing of a telephone with exclusion active, either by class of service (COS) or by manual activation.
n	Default value. Observing towards a telephone with exclusion active is denied, or if exclusion is activated by a telephone while being observed, all bridged parties including the observer are dropped.

SCCAN-Related System Parameters screen

Two changes were made to the **SCCAN-Related System Parameters** screen.

- A new field, **Special Digit Conversion**, was added.
- The **Default MM (WSM) SIP Trunk Group** field was changed to **MM (WSM) Route Pattern**.

To view the **SCCAN-Related System Parameters** screen:

1. Type **`change system-parameters sccan`**. Press **Enter**.

   The system displays the **SCCAN-Related System Parameters** screen (SCCAN-Related System Parameters screen on page 86).

Figure 3: SCCAN-Related System Parameters screen

```
                    SCCAN-Related System Parameters

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

MM (WSM) Route Pattern field

From earlier versions of the software, the **Default MM (WSM) SIP Trunk Group** field has now been changed to **MM (WSM) Route Pattern**. With this change, only regular routing pattern numbers that are SCCAN-enabled are allowed.

Partition route patterns indexes, RHNPA indexes, deny, or nodes are not allowed.

Valid entries	Usage
blank	Default value. If this field is left blank, the feature is turned off. To enable this feature, you must enter an acceptable value
1 to 254	Valid entries for an S8300 Media Server
1 to 999	Valid entries for an S8700 Media Server

Special Digit Conversion field

A new field, **Special Digit Conversion**, allows a user to call a cell telephone number and get the same treatment as calling an extension that is running Communication Manager.

Valid entries	Usage
y	ARS checks the dialed string to determine if the dialed string is a SCCAN telephone number. If the number is a SCCAN telephone number, the cell telephone number is replaced with the extension number that the cell telephone is mapped to.
n	Default value. This feature is turned off.

Station screen

A new field, **Always Use?**, is added to the **Station** screen. This change is prompted by the E911 device location for IP telephones feature.

To view the **Station** screen:

1. Type **`change station`** ***n***, where ***n*** is the extension that you want to change. Press **Enter**.

   The system displays the **Station** screen.

2. Click **Next** until you see the **Always Use?** field (Station screen on page 88).

Figure 4: Station screen

```
change station 1234567                                          Page 2 of 4

                                     STATION
FEATURE OPTIONS
           LWC Reception: spe            Auto Select Any Idle Appearance? n
          LWC Activation? y                      Coverage Msg Retrieval? y
  LWC Log External Calls? n                              Auto Answer: none
            CDR Privacy? n                           Data Restriction? n
   Redirect Notification? y                 Idle Appearance Preference? n
 Per Button Ring Control? n
   Bridged Call Alerting? n                   Restrict Last Appearance? y
  Active Station Ringing: single

        H.320 Conversion? n        Per Station CPN - Send Calling Number?
       Service Link Mode: permanent
         Multimedia Mode: basic
    MWI Served User Type:                   Display Client Redirection? n
            AUDIX Name:                   Select Last Used Appearance? n
                                            Coverage After Forwarding? y

                                       Direct IP-IP Audio Connections? n
Emergency Location Ext: 2013    Always Use? n      IP Audio Hairpinning? y
```

Valid entries	Usage
y	When a user dials an emergency number, Communication Manager uses the value in the Emergency Location Extension field as the number of the calling party.
n	Default value. When a user dials an emergency number, Communication Manager uses the IP subnetwork (subnet) feature to determine the location of the calling party. This option depends upon the customer having subnets that correspond to geographical areas.

Release 2.1 new screens

Avaya Communication Manager, release 2.1, includes the following new screens. For a more complete explanation of the screens and their function, see the *Administrator's Guide for Avaya Communication Manager*, 555-233-506.

Calling Party Number Conversion for Tandem Calls screen

The Avaya Extension to Cellular/OPS feature introduces a new screen, the **Calling Party Number Conversion for Tandem Calls** screen.

Prior to this release, users of AT&T cell phones, with the Avaya Extension to Cellular feature, may receive calls to their cell phone where the calling party number is unavailable. When tandem internal systems are used, the system had difficulty translating a caller's telephone number and displaying it to the Extension to Cellular cell phone.

By administering this new screen, in conjunction with the new **Modify Tandem Calling Number** field on the **Trunk Group** screen for ISDN trunk groups (see Trunk Group screen on page 113), you can now receive the caller's telephone number to your cell phone.

Type **`change tandem-calling-party-num`**. Press **Enter**. The system displays the **Calling Party Number Conversion for Tandem Calls** screen (Calling Party Number Conversion for Tandem Calls screen on page 89).

Figure 5: Calling Party Number Conversion for Tandem Calls screen

```
change tandem-calling-party-num                                  Page 1 of 8

                              Calling Party Number Conversion
                                      for Tandem Calls

    CPN                    Trk                                        Number
Len Prefix                 Grp (s)       Delete  Insert               Format
__  ___________________    _________     ___     ___________________  ________
__  ___________________    _________     ___     ___________________  ________
__  ___________________    _________     ___     ___________________  ________
__  ___________________    _________     ___     ___________________  ________
__  ___________________    _________     ___     ___________________  ________
__  ___________________    _________     ___     ___________________  ________
__  ___________________    _________     ___     ___________________  ________
__  ___________________    _________     ___     ___________________  ________
__  ___________________    _________     ___     ___________________  ________
```

Location Parameters screens

The Multinational Locations feature introduces a new screen, the **Location Parameters** screen. This screen is actually as series of four new screens.

Page 1, the **Location Parameters** screen, provides the user with additional administrable location characteristics related to the Multinational Locations feature. With the Multinational Locations feature enabled, the **Location Parameters** screen is actually a set of ***n*** screens, where ***n*** is:

- 1 if Multinational Locations is disabled in the license file
- 2-25 for Linux platforms
- 2-8 for csi, si, and r platforms

Type **`change location-parameters n`**, where ***n*** is a number from 1 to 25. Press **Enter**. The system displays the **Location Parameters** screen (Location Parameters screen, page 1 on page 90).

Note:

The number ***n*** appears in the screen title, unless **Multinational Locations** is disabled in the license file.

Figure 6: Location Parameters screen, page 1

```
change location-parameters 2                                    Page 1 of 4

                                  LOCATION PARAMETERS 2

                            Tone Generation Plan: 1
                          Analog Ringing Cadence: 1
                       Analog Line Transmission: 1
                    DCP Terminal-parameters Plan: 1
                            Country code for CDR: 1
                                 Companding Mode: Mu-law

RECALL TIMING
                               Flashhook Interval? _      Upper Bound (msec): 1000
                     Disconnect Timing (msec): 150    Lower Bound (msec): 200
                orward Disconnect Timer (msec): 600
                     MF Interdigit Timer (sec): 10
    Outgoing Shuttle Exchange Cycle Timer (sec): 4
```

Field Descriptions

The following fields were moved to page 1 of the **Location Parameters** screen from previously existing screens, and are not new fields. Their descriptions can be found in the Screen Reference chapter of the *Administrator's Guide for Avaya Communication Manager*, 555-233-506, for the November 2003 2.0 release.

Field	Moved From
Analog Ringing Cadence	**System Parameters Country Options**
Analog Line Transmission	**System Parameters Country Options**
Companding Mode	**System Parameters Country Options**
Flashhook Interval	**Feature-Related System Parameters**
Upper Bound (msec)	**Feature-Related System Parameters**
Lower Bound (msec)	**Feature-Related System Parameters**
Forward Disconnect Timer (msec)	**Feature-Related System Parameters**
Disconnect Timing (msec)	**Feature-Related System Parameters**
MF Interdigit Timer (sec)	**Multifrequency Signaling System Parameters**
Outgoing Shuttle Exchange Cycle Timer (sec)	**Multifrequency Signaling System Parameters**

The following fields are new:

- The **Tone Generation Plan** field appears only when the Multinational Locations feature is turned on in the license file. The value in this field is an ordinary number, not a country code. The value corresponds to the tone generation characteristics administered for location ***n*** on the **Tone Generation** screens. Valid values are 1-25.

  This field takes on the same error messages as the **Base Tone Generator Set** field that was previously on the **System Parameters Country Options** screen.

- The **DCP Terminal-Parameters Plan** field appears only when the Multinational Locations feature is turned on in the license file. The value in this field is an ordinary number, not a country code. The value corresponds to the DCP terminal transmission parameters administered for location ***n*** on the **Terminal Parameters** screens. Valid values are 1-25.

  This field takes on the same error messages as any other field with this range of values.

- The **Country Code for CDR** field appears only when the Multinational Locations feature is turned on in the license file. The value in this field is an ordinary number, not a country code. The value corresponds to the Country Code to be used for Call Detail Recording (CDR) information for a location-specific country. Valid values are 1-999.

  This field takes on the same error messages as any other field with this range of values. Some customers might prefer Communication Manager's country numbering scheme,

where 1=United States and Canada, 2=Australia and New Zealand, 3=Japan, 4=Italy, and so on. Other customers might prefer the International Telecommunications Union (ITU) country numbering scheme, where 1=USA, Canada, and Caribbean, 7=Russian and Kazakhstan, 20=Egypt, 27=South Africa, 30=Greece, and so on. The default is 1.

Loss Plans screen

Page 2 of the **Location Parameters** screen is called **Loss Plans** (Loss Plans screen, page 2 on page 92). This screen allows the user to administer loss plans by location.

Figure 7: Loss Plans screen, page 2

```
change location-parameters 2                                    Page 2 of 4

LOSS PLANS

          Inter-location Loss Group: 18

                  2 Party Loss Plan: 1                Customize? n

                     Tone Loss Plan: 1                Customize? n

End-to-End total loss (dB) in a n-party conference:
3: 15 4: 21 5: 26 6: 29                               Customize? n
```

Field Descriptions

The fields in the following table were moved to page 2 of the **Location Parameters** screen from the **System Parameters Country Options** screens as part of the November 2003, 2.0 release. Their descriptions can be found in the Screen Reference chapter of the *Administrator's Guide for Avaya Communication Manager*, 555-233-506, for the November 2003 release.

Field	Moved From
2 Party Loss Plan (renamed from **Digital Loss Plan**)	**System Parameters Country Options**
Customize (for **2 Party Loss Plan**)	**System Parameters Country Options**
Tone Loss Plan (renamed from **Digital Tone Plan**)	**System Parameters Country Options**
Customize (for **Tone Loss Plan**)	**System Parameters Country Options**
End-to-End total loss (dB) in a n-party conference	**System Parameters Country Options**

The **Inter-location Loss Group** field appears only when the Multinational Locations feature is turned on in the license file. It takes on the same ranges, Help, and error messages as the **Digital Loss Group** field on the **Tie Trunk** screen. The default value is 18. When inserting loss for a call, the server treats parties on the call who are in separate locations as if the location with the most parties were connected by an equal number of IP tie trunks as there are parties at other locations. The **Inter-location Loss Group** field specifies the digital loss group number that is used by these "virtual" IP tie trunks.

When you set the **Customize** field, for the **End-to-End total loss (dB) in a n-party conference** field, to **y**, the **End-to-End total loss (dB) in a n-party conference** fields can be changed by the administrator. When you set the **Customize** field to **n**, the **End-to-End total loss (dB) in a n-party conference** fields are re-set to the values that they would have had under the 2 Party Loss Plan that is administered on page 3 of this screen. They also become display only.

2 Party Loss Plan screen

Page 3 of the **Location Parameters** screen is called **2 Party Loss Plan** (2 Party Loss Plan screen, page 3 on page 93). The **2 Party Loss Plan** screen has moved here from page 2 of the **System Parameters Country Options** screen. All of the rules governing whether it appears or is hidden continue to apply. Now, there are ***n*** copies of this page instead of just one. With the Multinational Locations feature enabled, ***n***=25.

Figure 8: 2 Party Loss Plan screen, page 3

```
change location-parameters 2                                    Page 3 of 4

                                2 PARTY LOSS PLAN
              TO:   1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19
               1:   0  0  0  0  0  0  0  0  0  3  0  0  0  0  0  3  3  0  0
               2:   0  0  0  0  0  0  0  0  0  3  0  0  0  0  0  3  3  0  0
               3:   3  6  0  0  0  0  0  0  0  3  0  0  0  0  0  3  3  6  6
               4:   0  0 -3  0  0  3  3  3  2  3  0  0  0  0  2  3  3  0  0
               5:   0  0 -3  0  0  3  3  3  2  3  0  0  0  0  0  3  3  0  0
               6:   0  0 -3  3  3  6  8  6  5  5  5  3  3  3  5  3  3  0  0
         F     7:   0  0 -3  3  3  8  8  6  5  5  5  3  3  3  5  3  3  0  0
         R     8:   0  0 -3  3  3  6  6  6  3  5  3  3  0  0  3  3  3  0  0
         O     9:   0  0 -3  2  2  5  5  3  0  0  2 -3 -3 -3  0  3  3  0  0
         M    10:   3  3  0  3  3  5  5  5  0  0  3 -3 -3 -3  3  3  3  3  3
              11:   0  0 -3  0  0  5  5  3  2  3  0  0  0 -3  0  3  3  0  0
              12:   6  6  3  6  6  9  9  9  3  3  6  0  0  0  6  3  3  6  6
              13:   6  6  0  6  6  9  9  6  3  3  6  0  0  0  6  3  3  6  6
              14:   6  6  0  6  6  9  9  6  3  3  3  0  0  0  6  3  3  6  6
              15:   0  0 -3  2  0  5  5  3  0  3  0  0  0  0  0  3  3  0  0
              16:   3  3  3  3  3  3  3  3  3  3  3  3  3  3  3  3  3  3  3
              17:   3  3  3  3  3  3  3  3  3  3  3  3  3  3  3  3  3  3  3
              18:   0  0  0  0  0  0  0  0  0  3  0  0  0  0  0  3  3  0  0
              19:   0  0  0  0  0  0  0  0  0  3  0  0  0  0  0  3  3  0  0
```

Tone Loss Plan screen

Page 4 of the **Location Parameters** screen is called **Tone Loss Plan** (Tone Loss Plan screen, page 4 on page 94). The **Tone Loss Plan** screen has moved here from page 3 of the **System Parameters Country Options** screen. All of the rules governing whether it appears or is hidden continue to apply. Now, there are ***n*** copies of this page instead of just one. With the Multinational Locations feature enabled, ***n***=25. Also, the **End-to-End total loss (dB) in a n-party conference** fields have moved from their former location on this screen to page 2 of the **Location Parameters** screen.

Figure 9: Tone Loss Plan screen, page 4

```
change location-parameters 2                                    Page 4 of 4

                                TONE LOSS PLAN

                                                TO
                     1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19
         Dial:       0  0  0  3  3  6  6  6  5  0  6  5  5  5  5  0  0  0  0
      Confirm:       0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
      Reorder:       0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
         Busy:       0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
      Ringing:       0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
    Spec Ring:       0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
    Intercept:       0  0  0  0  0  0  0  0  1  0  0  1  1  1  1  0  0  0  0
      Waiting:       0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
       Verify:       0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
      Intrude:       0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
          Zip:       3 -3 -3  3  3 -3 -3 -3 -3 -3 -3 -3 -3 -3 -3  0  0 -3 -3
        Music:       0  0  0  3  3  6  6  6  3  0  6  3  3  3  3  0  0  0  0
```

Multifrequency-Signaling-Related Parameters screen

The Multinational Locations feature introduces a new screen, the **Multifrequency-Signaling-Related Parameters** screen. These screens replace the old system-wide **Multifrequency Signaling System Parameters** screen. The new screens allow the user to set multifrequency signaling parameters by location. The **Multifrequency Signaling System Parameters** screen is no longer available.

With Multinational Locations enabled, the **Multifrequency-Signaling-Related Parameters** screen is actually a set of ***n*** screens, where ***n*** is:

- 1 if Multinational Locations is disabled in the license file
- 2-8 if Multinational Locations is enabled in the license file

Type **change multifrequency-signaling *n***, where ***n*** is a number from 1 to 8. Press **Enter**. The system displays the **Multifrequency-Signaling-Related Parameters** screen (Multifrequency-Signaling-Related Parameters screen, page 1 on page 95).

Note:

The number ***n*** appears in the screen title, unless Multinational Locations is disabled in the license file.

Figure 10: Multifrequency-Signaling-Related Parameters screen, page 1

```
change multifrequency-signaling 3                                Page 1 of 3

                    MULTIFREQUENCY-SIGNALING-RELATED PARAMETERS 3
                Incoming Call Type: group-ii-mfc              ANI Prefix:
                Outgoing Call Type: group-ii-mfc             Default ANI:
             Maintenance Call Type: none                   NEXT ANI DIGIT
               Test Call Extension:                        Incoming: send-ani
            Interdigit Timer (sec): 10                     Outgoing: send-ani
          Maximum Resend Requests:
       Received Signal Gain (dB): 0
   Transmitted Signal Gain (dB): -3
                                  Request Incoming ANI (non-AAR/ARS)? n
                        Outgoing Forward Signal Present Timer (sec): 15
                         Outgoing Forward Signal Absent Timer (sec): 30
      MF Signaling Intercept Treatment - Incoming? n     Outgoing: tone
                                  Collect All Digits Before Seizure? n
                       Overlap Sending on Link-to-Link Tandem Calls? n
               Private Group II Permissions and Public Interworking? n
                        Outgoing Shuttle Exchange Cycle Timer (sec): 4
                                  Use COR for All Group II Responses? n
                                      Group II Called Party Category: user-type
                                  Use COR for Calling Party Category? n
```

Field Descriptions

All fields on page 1 of the **Multifrequency-Signaling-Related Parameters** screen are unchanged from the old **Multifrequency Signaling System Parameters** screen, with the following exceptions:

- The field formerly called **ANI for PBX** has been renamed **Default ANI** because it now applies by trunk group, not by system.
- The **Interdigit Timer (sec)** and **Outgoing Shuttle Exchange Cycle Timer (sec)** fields have moved to the **Location Parameters** screen.

Click Next to see page 2 of the **Multifrequency-Signaling-Related Parameters** screen (Multifrequency-Signaling-Related Parameters screen, page 2 on page 96).

Figure 11: Multifrequency-Signaling-Related Parameters screen, page 2

```
change multifrequency-signaling 3                                Page 2 of 3

                     MULTIFREQUENCY-SIGNALING-RELATED PARAMETERS 3

         Request Call Category at Start of Call? n            Outgoing II by COR
               Restart ANI from Caller Category? y                 1:  1
                  Number of Incoming ANI Digits: 0                 2:  2
                  Number of Outgoing ANI Digits: 0                 3:  3
                Truncate Station Number in ANI: n                  4:  4
    Address Digits Include End-of-digits Signal? n                 5:  5
             Call Category for Vector ii-digits? n                 6:  6
                   Request CPN at Start of Call? n                 7:  7
              Do Not Send Group B Signals to CO? n                 8:  8
       ANI Source for Forwarded & Covered Calls: caller            9:  9
                                                                  10: 10

                          INCOMING         OUTGOING
           ANI Available:
       ANI Not Available:
```

Field Descriptions

All fields on page 2 of the **Multifrequency-Signaling-Related Parameters** screen are unchanged from the old **Multifrequency Signaling System Parameters** screen, with the following exception:

- The **Outgoing II by COR** fields are new. They appear only if either the **Use COR for Calling Party Category** field, or the **Use COR for All Group II Responses** field on page 1 are set to **y**. These fields have the same ranges, Help, and error messages as the **Group II Category For MFC** field on the **Class of Restriction** screen.

  The Group II signal sent to the central office (CO) on outgoing calls can be administered by Class of Restriction (COR) and trunk group. The Group II signal is administered by COR, and then maps to a possibly different outgoing signaling parameter set. If either the **Use COR for Calling Party Category** or **Use COR for All Group II Responses** fields on the first page of the **Multifrequency-Signaling-Related Parameters** screen is set to **y**, then the mappings administered in the **Outgoing II by COR** fields determine what Group II signal that Communication Manager sends to the CO.

Click Next to see page 3 of the **Multifrequency-Signaling-Related Parameters** screen (Multifrequency-Signaling-Related Parameters screen, page 3 on page 97).

Figure 12: Multifrequency-Signaling-Related Parameters screen, page 3

```
change multifrequency-signaling 3                              Page 3 of 3

                    MULTIFREQUENCY-SIGNALING-RELATED PARAMETERS 3

INCOMING FORWARD SIGNAL TYPES                  INCOMING BACKWARD SIGNAL TYPES
(Tones from CO)                                (Tones to CO)

      Group-I              Group-II                Group-A            Group-B
  11: ignored           1: normal              1 : next-digit     1 : free
  12: ignored           2: normal              3 : end-of-dial    2 : busy
  13: ignored           3: normal              5 : send-ani       4 : congestion
  14: ignored           4: normal                :                7 : intercept
  15: ignored           5: attendant             :                  :
                        6: data-call             :                  :
                        7: normal                :                  :
                        8: normal                :                  :
                        9: normal                :                  :
                       10: normal                :                  :
                       11: normal                :                  :
                       12: normal                :                  :
                       13: normal                :                  :
                       14: normal                :                  :
                       15: normal                :                  :
```

Field Descriptions

All fields on page 3 of the **Multifrequency-Signaling-Related Parameters** screen are unchanged from the old **Multifrequency Signaling System Parameters** screen. Their descriptions can be found in the Screen Reference chapter of the *Administrator's Guide for Avaya Communication Manager*, 555-233-506, for the November 2003 release.

Native administration screens

2402 telephone

A native administration screen is available for the 2402 telephone. This supports automatic administration for the **messages** button. This screen allows a feature to be administered for the **shifted #** button, which is not possible when the 2402 telephone is aliased as a 6402 telephone.

4610SW telephone

A native administration screen is available for the 4610SW telephone.

Terminal Parameters screens

The Multinational Locations feature introduces a new screen, the **Terminal Parameters** screen. This screen is actually as series of three new screens.

The **Terminal Parameters** screens replace the following screens:

- **Terminal Parameters 302/603/606**
- **Terminal Parameters 6400/607A1/4600**
- **Terminal Parameters 8400**

Now, the **Terminal Parameters** screens are set up as follows:

- Page 1 is for 302/603/606 types
- Page 2 is for 6400/607A1/4600 types
- Page 3 is for 8400 types

The fields on the **Terminal Parameters** screen are unchanged from the old **Terminal Parameters** screens, with the following exceptions:

- The **Default Parameter Set** field has been renamed **Base Parameter Set**. It still contains a country code.
- The display-only message on the screens: **Note: Location-parameters forms assign terminal parameter sets** is new. Since the **Location Parameters** screens now control which terminal parameters sets are used, the terminal parameter no longer shows the same terminal parameters set that the administrator last changed.

With Multinational Locations enabled, the **Terminal Parameters** screen is actually a set of ***n*** screens, where ***n*** is:

- 1 if Multinational Locations is disabled in the license file
- 2-25 for Linux platforms
- 2-8 for csi, si, and r platforms

Type **`change terminal-parameters`** ***n***, where ***n*** is a number from 1 to 25. Press **Enter**. The system displays the **302/603/606-Type Terminal Parameters** screen (302/603/606-Type Terminal Parameters, page 1 on page 99).

Note:

The number ***n*** appears in the screen title, unless Multinational Locations is disabled in the license file.

Figure 13: 302/603/606-Type Terminal Parameters, page 1

```
change terminal-parameters 3                                    Page 1 of 3

                     302/603/606-TYPE TERMINAL PARAMETERS 3

          Base Parameter Set: 1                Customize Parameters? y
Note: Location-parameters forms assign terminal parameter sets.

OPTIONS
                Display Mode: 1                    DLI Voltage Level: automatic

PRIMARY LEVELS
          Voice Transmit (dB): 0.0               Voice Sidetone (dB): -16.0
           Voice Receive (dB): -2.0          Touch Tone Sidetone (dB): -25.0
     Touch Tone Transmit (dB): +1.0
```

Click **Next** to see page 2 of the **Terminal Parameters** screen (6400/607A1/4600-Type Terminal Parameters, page 2 on page 99).

Figure 14: 6400/607A1/4600-Type Terminal Parameters, page 2

```
change terminal-parameters 3                                    Page 2 of 3

                   6400/607A1/4600-TYPE TERMINAL PARAMETERS 3

          Base Parameter Set: 1                Customize Parameters? y
Note: Location-parameters forms assign terminal parameter sets.
Note: LEVELS do not apply to the 4600 terminals.
 OPTIONS
                Display Mode: 1           Handset Expander Enabled? y
         Volume for DCP Types: retain handset and speaker between calls
          Volume for IP Types: default settings used to begin each call
 PRIMARY LEVELS
          Voice Transmit (dB): +2.5             Voice Sidetone (dB): -11.0
           Voice Receive (dB): -2.0        Touch Tone Sidetone (dB): -25.0
     Touch Tone Transmit (dB): +1.0

 BUILT-IN SPEAKER LEVELS
          Voice Transmit (dB): 0.0               Voice Receive (dB): 0.0
                                            Touch Tone Sidetone (dB): -12.0

 6402 BUILT-IN SPEAKER LEVELS
          Voice Receive (dB): -2.0        Touch Tone Sidetone (dB): -19.0
```

Click **Next** to see page 3 of the **Terminal Parameters** screen (8400-Type Terminal Parameters, page 3 on page 100).

Figure 15: 8400-Type Terminal Parameters, page 3

```
change terminal-parameters 3                                    Page 3 of 3

                          8400-TYPE TERMINAL PARAMETERS 3

          Base Parameter Set: 1                 Customize Parameters? y
Note: Location-parameters forms assign terminal parameter sets.
 OPTIONS
                 Display Mode: 1                  DLI Voltage Level: automatic
    Handset Expander Enabled? y

 PRIMARY LEVELS
         Voice Transmit (dB): +2.5             Voice Sidetone (dB): -11.0
          Voice Receive (dB): -2.0        Touch Tone Sidetone (dB): -25.0
                                          Touch Tone Transmit (dB): +1.0
 ADJUNCT LEVELS
         Voice Transmit (dB): 0.0               Voice Receive (dB): -2.0
         Voice Sidetone (dB): -14.5       Touch Tone Sidetone (dB): -25.0
 BUILT-IN SPEAKER LEVELS
         Voice Transmit (dB): 0.0               Voice Receive (dB): 0.0
                                          Touch Tone Sidetone (dB): -12.0

 8403 BUILT-IN SPEAKER LEVELS
          Voice Receive (dB): -2.0        Touch Tone Sidetone (dB): -19.0
```

Tone Generation screens

The Multinational Locations feature introduces a new screen, the **Tone Generation** screen. The **Tone Generation** pages were previously part of the **System Parameters Country Options** screens, and tone generation was administered system-wide. With Multinational Locations enabled, tone generation can be administered by location rather than system-wide. The new **Tone Generation** screen is actually a set of ***n*** screens, where ***n*** is:

- 1 if Multinational Locations is disabled in the license file
- 2-25 for Linux platforms
- 2-8 for csi, si, and r platforms

Type **change tone-generation *n***, where ***n*** is a number from 1 to 25. Press **Enter**. The system displays the **Tone Generation** screen (Tone Generation screen on page 101).

Note:

The number ***n*** appears in the screen title, unless Multinational Locations is disabled in the license file.

Figure 16: Tone Generation screen

```
change tone-generation 2                                        Page 1 of X

                                  TONE GENERATION 2

                                                    Base Tone Generator Set: 1
        440Hz PBX-dial Tone? n                  440Hz Secondary-dial Tone? n
```

Field Descriptions

The fields in the following table were moved to page 1 of the **Tone Generation** screen from the **System Parameters Country Options** screens as part of the November 2003, 2.0 release. Their descriptions can be found in the Screen Reference chapter of the *Administrator's Guide for Avaya Communication Manager*, 555-233-506, for the November 2003, 2.0 release.

Field	Moved From
Base Tone Generator Set	**System Parameters Country Options**
440Hz PBX-dial Tone	**System Parameters Country Options**
440Hz Secondary-dial Tone	**System Parameters Country Options**

Tone Generation Customized Tones screen

Page 2 of the **Tone Generation** screen is called **Tone Generation Customized Tones** (Tone Generation Customized Tones screen on page 102). This screen allows the user to administer loss plans by location.

Figure 17: Tone Generation Customized Tones screen

```
change tone-generation 2                                        Page 1 of X
                        TONE GENERATION CUSTOMIZED TONES 2

          Tone Name             Cadence              Tone
                                 Step          (Frequency/Level)
                                   1:
                                   2:
                                   3:
                                   4:
                                   5:
                                   6:
                                   7:
                                   8:
                                   9:
                                  10:
                                  11:
                                  12:
                                  13:
                                  14:
                                  15:
```

Release 2.1 changed screens

Avaya Communication Manager, release 2.1, includes the following changed screens. For a more complete explanation of the screens and their function, see the *Administrator's Guide for Avaya Communication Manager*, 555-233-506.

CDR System Parameters

The **Data Item** field column in the **CDR System Parameters** screen allows three new key word sets:

- **country-from** and **country-to**
- **location-from** and **location-to**
- **timezone-from** and **timezone-to**

This change was prompted by the Multinational Locations feature. If the Multinational Locations feature is disabled in the license file, these key words are invalid.

The **Data Item** field takes on six new values:

- **country-from** is a country number for currency conversion. Its length is 3, the same as the length of the **Country code for CDR** field on the **Location Parameters** screen. It indicates the administered CDR country code of the system interface of the called party.
- **country-to** is a country number for currency conversion. Its length is 3, the same as the length of the **Country code for CDR** field on the **Location Parameters** screen. It indicates the administered CDR country code of the system interface of the called party.
- **location-from** is a location number for record sorting. Its length is 3, the same as the length of the location field on the cabinet, media gateway, remote office, and ip-network region screens. It indicates the location code of the system interface of the calling party.
- **location-to** is a location number for record sorting. Its length is 3, the same as the length of the location field on the cabinet, media gateway, remote office, and ip-network region screens. It indicates the location code of the system interface of the calling party.
- **timezone-from** is a time zone offset number for call time. Its length is 5, the same as the length of the **Timezone Offset** field on the **Locations** screen. It indicates the timezone offset of the system interface of the calling party.
- **timezone-to** is a time zone offset number for call time. Its length is 6, the same as the length of the **Timezone Offset** field on the **Locations** screen. It indicates the timezone offset of the system interface of the calling party.

Feature-Related System Parameters screen

A new page, with new fields, is added to the **Feature-Related System Parameters** screen for the Redirection on IP Failure feature.

1. Type **`change system-parameters features`**. Press **Enter**.

   The system displays the **Feature-Related System Parameters** screen.

2. Click **Next** until you see the **Redirection On Ip Connectivity Failure** area (Feature-Related System Parameters screen on page 104).

Figure 18: Feature-Related System Parameters screen

```
change system-parameters features                                  page 12 of 13

                        FEATURE-RELATED SYSTEM PARAMETERS

REDIRECTION ON IP CONNECTIVITY FAILURE
                  Switch Hook Query Response Timeout:
              Auto-answer IP Failure Aux Reason Code: 0

MAXIMUM AGENT OCCUPANCY PARAMETERS
                  Maximum Agent Occupancy Percentage: 100
             Maximum Agent Occupancy Aux Reason Code: 9
```

3. In the **Switch Hook Query Response Timeout** field, type the number of milliseconds (ms) that call processing must wait for a response to the switchhook query before ROIF is triggered.

Valid entries	Usage
blank	Default value. When this field is blank, it indicates that the ROIF feature is off.
500-**5000**	Number of milliseconds before ROIF is triggered. • 500ms-700ms for IP hardphones • 2000ms-3000ms for IP Agent Softphones

4. In the **Auto-answer IP Failure Aux Reason Code** field, type a currently unused auxiliary reason code.

Valid entries	Usage
0-**9**	Default=**0**.

5. Press **Enter** to save your changes.

Additional changes to the Feature-Related System Parameters screen

The following fields have moved to the **Location Parameters** screens:

- **Flashhook Interval**
- **Upper Bound (msec)**
- **Lower Bound (msec)**
- **Forward Disconnect Timer (msec)**
- **Disconnect Timing (msec)**

Hunt Group screen

The **Queue Length** field, and all related administration and error message, was removed from page 1 of the **Hunt Group** screen (Hunt Group screen on page 105).

To view the **Hunt Group** screen, use the **`change hunt-group n`** command, where ***n*** is the hunt group number. This change is prompted by the Dynamic hunt group queue slot allocation feature.

Figure 19: Hunt Group screen

```
change hunt-group 2                                              Page 1 of 3

                                  HUNT GROUP

           Group Number: 2                                         ACD? y
             Group Name: HNT-2                                   Queue? y
        Group Extension: 7330002                                 Vector? y
             Group Type: slm
                    TN: 1
                   COR: 1                              MM Early Answer? n
         Security Code:
   ISDN Caller Display:

 Calls Warning Threshold: 2     Port:
  Time Warning Threshold: 15    Port:
```

Hunt Group Measurements screen

The **Que Siz** column in **Hunt Group Measurements** screen is changed to **Que**, with a value of **y** or **n** (Hunt Group Measurements screen on page 106).

- If the **Queue?** field on the **Hunt Group** screen is set to **y**, the **Que** field on the **Hunt Group Measurements** screen displays a **y**.
- If the **Queue?** field on the **Hunt Group** screen is set to **n**, the **Que** field on the **Hunt Group Measurements** screen displays a **n**.

To view the **Hunt Group Measurements** screen, use the **`list measurements hunt-group today-peak`** command (plus other commands of this series). This change is prompted by the Dynamic hunt group queue slot allocation feature.

Figure 20: Hunt Group Measurements screen

```
list measurements hunt-group today-peak                              Page 1
Switch Name:                                  Date: 6:43 pm WED OCT 8, 2003

                            HUNT GROUP MEASUREMENTS

Grp   Grp                    Grp  Meas Total Calls  Que Calls Que  Time  Speed
No.   Name                   Siz  Hour Usage Ans/       Que   Ovfl Avail Ans
                             Typ             Aban                       (sec)

1    Skill 1                 0    1700 0     0      n   0     0    0     0
                             ucd
2    Skill 2                 0    1700 0     0      n   0     0    0     0
                             ucd
3    Skill 3                 0    1700 0     0      n   0     0    0     0
                             ucd
4    Skill 4                 0    1700 0     0      n   0     0    0     0
                             ucd
5    Skill 5                 0    1700 0     0      n   0     0    0     0
                             ucd
6    Skill 6                 0    1700 0     0      n   0     0    0     0
                             ucd
```

Hunt Group Status screen

Changed the **Q** column in **Hunt Group Status** screen to mean **Queue?** instead of **Q-Length** (Hunt Group Status screen on page 107).

- If the **Queue?** field on the **Hunt Group** screen is set to **y**, the **Q** column on the **Hunt Group Status** screen displays a **y**.
- If the **Queue?** field on the **Hunt Group** screen is set to **n**, the **Q** column on the **Hunt Group Status** screen displays a **n**.

To view the **Hunt Group Status** screen, use the **`monitor traffic hunt-groups`** command. This change is prompted by the Dynamic hunt group queue slot allocation feature.

Figure 21: Hunt Group Status screen

```
monitor traffic
hunt-groups                                                          Page 1
                                HUNT GROUP STATUS          10:18 WED OCT 8, 2003

        #    S    A    Q    W    LCIQ              #    S    A    Q    W    LCIQ
        1    0    0    y    0    0                 30   0    0    n    0    0
        2    0    0    y    0    0                 31   0    0    y    0    0
        3    0    0    y    0    0                 32   0    0    n    0    0
        4    0    0    y    0    0                 40   0    0    y    0    0
        5    0    0    y    0    0                 41   0    0    y    0    0
        6    0    0    y    0    0                 42   0    0    y    0    0
        10   0    0    y    0    0                 43   0    0    y    0    0
        11   0    0    y    0    0                 50   0    0    n    0    0
        12   0    0    y    0    0                 51   0    0    y    0    0
        13   0    0    y    0    0                 60   0    0    y    0    0
        20   0    0    y    0    0
        21   0    0    y    0    0
        22   0    0    y    0    0
        23   0    0    y    0    0
        24   0    0    n    0    0
        25   0    0    n    0    0
(#: Group;  S: Grp Size;  A: Active Members;  Q: Queue?:  W: Calls Waiting)
(LCIQ: Longest Call In Queue in seconds)
```

Hunt Groups screen

The **Que Siz** column in **Hunt Groups** screen is changed to **Que**, with a value of **y** or **n** (Hunt Groups screen on page 108).

- If the **Queue?** field on the **Hunt Group** screen is set to **y**, the **Que** field on the **Hunt Groups** screen displays a **y**.
- f the **Queue?** field on the **Hunt Group** screen is set to **n**, the **Que** field on the **Hunt Groups** screen displays an **n**.

To view the **Hunt Groups** screen, use the **`list hunt-group`** command. This change is prompted by the Dynamic hunt group queue slot allocation feature.

Figure 22: Hunt Groups screen

```
list hunt-group                                                    Page 1

                                    HUNT GROUPS
Grp  Grp
No.  Name/            Grp      ACD/           Que No. Cov  Notif/  Dom   Message
     Ext.             Type     MEAS Vec MCH       Mem Path Ctg Adj Ctrl  Center

1    Skill 1
     3001             ucd-mia y/B  SK   none  y   0        n            n
2    Skill 2
     3001             ead-loa y/N  SK   none  y   0        n            n
3    Skill 3
     3001             ucd-mia y/B  SK   none  y   0        n            n
4    Skill 4
     3001             ucd-mia y/B  SK   none  y   0        n            n
5    Skill 5
     3001             ucd-mia y/N  SK   none  y   0        n            n
6    Skill 6
     3001             ucd-mia y/N  SK   none  y   0        n            n
10   Skill 10
     3001             ucd-mia y/N  SK   none  y   0        n            n
```

Internal Data Hunt Group screen

The **max_q_leng:** __ field is replaced by **dhqueue:y/n** on the **Internal Data Hunt Group** screen. To view the **Internal Data Hunt Group** screen, use the **`display internal-data hunt group`** command. This change is prompted by the Dynamic hunt group queue slot allocation feature.

- If the **Queue?** field on the **Hunt Group** screen is set to **y**, the **dhqueue** field on the **Internal Data Hunt Group** screen displays a **y**.
- If the **Queue?** field on the **Hunt Group** screen is set to **n**, the **dhqueue** field on the **Internal Data Hunt Group** screen displays an **n**.

Note:

Since this screen is not an administrable screen, it is not shown here.

IP Server Interface (IPSI) Administration - Port Network screen

A new field, **Ignore Connectivity in Server Administration**, is added to the **IP Server Interface (IPSI) Administration - Port Network** screen (see IP Server Interface (IPSI) Administration - Port Network screen on page 109). Use the **change ipserver-interface *n*** command, where ***n*** is the number of the port network (PN) that you want to change.

This new field allows you to decide what IPSIs that you consider critical, and what IPSIs that you consider non-critical. The Arbiter uses only critical IPSIs when calculating the network state of health.

- If you set the **Ignore Connectivity in Server Administration** field to **n** (the default value), you consider that this IPSI is critical. The Arbiter uses this IPSI when calculating the network state of health.
- If you set the **Ignore Connectivity in Server Administration** field to **y**, you consider that this IPSI is non-critical. The Arbiter does not use this IPSI when calculating the network state of health.

Figure 23: IP Server Interface (IPSI) Administration - Port Network screen

```
change ipserver-interface 2                                    Page 1 of 1

           IP SERVER INTERFACE(IPSI) ADMINISTRATION - PORT NETWORK 2

                                IP Control? y              Socket Encryption? y
Ignore Connectivity in Server Arbitration? n                      Enable QoS? y


Primary IPSI                                          QoS Parameters
------------                                          --------------
 Location: 2A01                                         Call Control 802.1p: 6
     Host: 172.18.18.181                              Call Control DiffServ: 46
  DHCP ID: ipsi-A02a
```

Link/Port Status screen

A new page is added to the **Link/Port Status** set of screens. The new page is titled **Media Gateways** (see Media Gateways screen on page 110). Use either the:

- **status clan-port *n*** command, where ***n*** is the location of a clan port
- **status link *n*** command, where ***n*** is the number of a specific link

This page lists, at most, 15 media gateways that are connected to a CLAN. If there are more than 15 media gateways connected to a CLAN, the system displays the following warning message: "**Warning: Suggested maximum number of connected Media Gateways exceeded.**"

Figure 24: Media Gateways screen

```
status link 3                                                    Page 5 of 5

                                  Media Gateways

Number     Name                  MG IP Address              Type      Net Rgn

1          MG 1 simulated        169.29.19.99               g700      110
```

Locations screen

The **Locations** screen has a new column, **Location Parameters (Loc. Parms.)**. This column is an index to the **Location Parameters** screens for a specific location, not a country code. On new installs, the **Loc. Parms.** column takes on the same error messages as did the **Base Tone Generator Set** field on the **System Parameters Country Options** screen. It defaults to blank, but can only be left at that value for unused locations. If a user enters information into any other field on a location row, an entry must be made in the **Loc. Parms.** field. Otherwise, an error message displays.

Type **`change locations`**. Press **Enter**. The system displays the **Locations** screen (Locations screen on page 110).

Figure 25: Locations screen

```
change locations                                                 Page 1 of 1

                                   LOCATIONS

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

Loc. Name             Timezone  Daylight- Number ARS  Attd Loc.   Pre- Foreign
No                     Offset   Savings   Plan   FAC  FAC  Parms. fix  Domain
                                Rule      Area                       Route
                                          Code                       Pattern

  1  Main             + 00:00   0
xxx  ________________  _ __:__  __        ___    ____ ____ __     ____ _______
```

Message Waiting Indication Subscriber Number Prefixes screen

The **Message Waiting Indication Subscriber Number Prefixes** screen has a new field, **Send QSIG Message Center ID**. If you set this field to **y**, the screen displays a **MsgCenter ID** field for each machine ID. The **MsgCenter ID** field, which accepts up to 20 characters, enables a message that is left at a Siemens Hicom telephone to activate the message waiting indicator.

Type **change isdn mwi-prefixes**. Press **Enter**. The system displays the **Message Waiting Indication Subscriber Number Prefixes** screen (Message Waiting Indication Subscriber Number Prefixes screen on page 111).

Figure 26: Message Waiting Indication Subscriber Number Prefixes screen

```
change isdn mwi-prefixes                                        Page 1 of 2

                Message Waiting Indication Subscriber Number Prefixes

Send QSIG Message Center ID? y
Machine Inserted      Routing  AUDIX              MsgCenter
   ID   Digits        Digits   Mach ID               ID

   1: _____________    _____     __             _____________________
   2: _____________    _____     __             _____________________
   3: _____________    _____     __             _____________________
   4: _____________    _____     __             _____________________
   5: _____________    _____     __             _____________________
   6: _____________    _____     __             _____________________
   7: _____________    _____     __             _____________________
   8: _____________    _____     __             _____________________
   9: _____________    _____     __             _____________________
  10: _____________    _____     __             _____________________
```

System Capacity screen

Changed the title of a field in the **System Capacity** screen from **Queue Slots Per System** to **Dynamic Queue Slots Per System**. The **System Limit** column reflects the total pool of available slots (System Capacity screen on page 112).

To view the **System Capacity** screen, use the **display capacity** command. This change is prompted by the Dynamic hunt group queue slot allocation feature.

Figure 27: System Capacity screen

```
display capacity                                              Page 5 of 12
                              SYSTEM CAPACITY

                                                                    System
                                                  Used  Available   Limit
                                                  ----------------------

     HUNT GORUPS, SPLITS, OR SKILLS
                          Groups/Splits/Skills:     26     1974      2000
                  Administered Logical Agents:      21    19979     20000
     Administered Logical Agent-Skill Pairs:        21   179979    180000
                          Logged-In ACD Agents:      0     5200      5200
                     Logged-In Advocate Agents:      0     5200      5200
                Logged-In IP Softphone Agents:       0     5200      5200
                     Group Members Per System:       0    60000     60000
                     CMS Measured ACD Members:       0     1000      1000
                Dynamic Queue Slots Per System:     28     7972      8000
                     Queue/Call Status Buttons:     51    15875     15928+

                    Intercom Groups Per System:      0      256       256
                  Modem Pool Groups Per System:      0       63        63
          Personal CO Line (PCOL) Trunk Groups:      0      200       200

              '+' Limit combined with Facility Busy Indicators
```

System Parameters Country Options

The following fields and pages have moved to the **Location Parameters** screens:

- **Companding Mode**
- **Analog Ringing Cadence**
- **Analog Line Transmission**
- **440Hz PBX-dial Tone**
- **440Hz Secondary-dial Tone**
- **2 Party Loss Plan** page
- **Tone & Conference Loss Plans** page

The pages for **Tone Cadence, Frequency**, and **Level** administration have moved to the **Tone Generation** screens, as has the **Base Tone Generator Set** field.

Trunk Group screen

The **Trunk Group** screen for ISDN trunks has a new field, **Modify Tandem Calling Number**. This field is part of the changes to the Extension to Cellular feature. Use this field in conjunction with the Calling Party Number Conversion for Tandem Calls screen on page 89, to receive a caller's telephone number to your cell phone.

1. Type **change trunk-group *n***, where ***n*** is the number of an ISDN-type trunk group. Press **Enter**.

   The system displays the **Trunk Group** screen.

2. Click **Next** until you see the **Modify Tandem Calling Number** field (Trunk Group screen on page 113).

Figure 28: Trunk Group screen

```
change trunk-group 17                                          Page 2 of 22

Trunk Features
          ACA Assignment? n         Measured: none           Wideband Support? n
                                Internal Alert? n            Maintenance Tests? y
                              Data Restriction? n          NCA-TSC Trunk Member:
                                     Send Name? y           Send Calling Number: y
         Used for DCS? n              Hop Dgt? n
Suppress # Outpulsing? n    Format: unk-pvt
Outgoing Channel ID Encoding: exclusive      UUI IE Treatment: service-provider

                                                     Replace Restricted Numbers? n
                                                    Replace Unavailable Numbers? n
                                                          Send Connected Number? y
                                                   Modify Tandem Calling Number? y
            Send UUI IE? n
              Send UCID? n
Send Codeset 6/7 LAI IE? y                                 Ds1 Echo Cancellation? n

 Path Replacement with Retention? n
 Path Replacement Method: always
                   SBS? n     Netowrk (Japan) Needs Connect Before Disconnect? n
 DSN Term? n
```

3. If you want the system to modify tandem calls so that your cell phone can display incoming numbers, change **n** to **y**.

   Be sure to also change the Calling Party Number Conversion for Tandem Calls screen.

4. Press **Enter** to save your changes.

Additional changes

The **R2 MFC Signaling** field on the **Trunk Group** screen is new. It is an ordinary number, not a country code. The value range is any integer from 1 to 8. The default value is 1. This new field is prompted by the Multinational Locations feature.

The **R2 MFC Signaling** field appears only if a **Dial Type** field is set to **mf**.

- If the Multinational Locations feature is disabled in the license file, either during a new install or an upgrade, then the **R2 MFC Signaling** field is hidden. Internal to software it is always equal to 1.
- If the Multinational Locations feature is disabled in the license file for an existing system that previously had the Multinational Locations feature enabled, the **R2 MFC Signaling** field is hidden. Internal to software it is fixed at the value that it had at the time the license was disabled. Call processing ignores this field if the feature is disabled in the license file.

Release 2.0 new screens

Avaya Communication Manager, release 2.0, includes the following new screens. For a more complete explanation of the screens and their function, see the *Administrator's Guide for Avaya Communication Manager*, 555-233-506.

Change Station Extension screen

The Multi-Location Dial Plan feature introduces a new screen, **Change Station Extension** (Change Station Extension screen on page 115). Use the **`change extension-station n`** command, where ***n*** is the extension that you want to change. This screen allows an administrator to change an extension on the system without removing the extension then adding it back.

Note:

You cannot use the **`change extension-station n`** command to change the extension of a telephone if that telephone is administered as the emergency location extension for another telephone.

For example, if telephone A is administered as the emergency location extension for telephone B, then:

- You cannot change the extension of telephone A using the **`change extension-station n`** command. You must first change telephone B to assign a different emergency location extension. Then you can use the **`change extension-station n`** command to change the extension of telephone A.

- You can change the extension of telephone B. If you do, the **Change Station Extension** screen displays the extension of telephone A in the **Emergency Location Ext.** field under the **From Extension** header.

Figure 29: Change Station Extension screen

```
change extension-station 1234567                                  Page 1 of 1

                              CHANGE STATION EXTENSION

          Station Name: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx     Port: xxxxxx

                              FROM EXTENSION             TO EXTENSION
                              --------------             ------------
                         Station: xxx-xxxx                 xxx-xxxx
                   Message Lamp: xxx-xxxx                  xxx-xxxx
        Emergency Location Ext.: xxx-xxxx                  xxx-xxxx
IP Parameter Emergency Location: xxx-xxxx                  See IP-Network Map Form
```

Function

When the screen is filled out and submitted, all administration that was associated with the current extension will now be associated with the new extension. Any administration references of the extension being changed, such as references used in a vector, coverage, etc., will now reference the new extension. Once the extension has been changed, all references to the previous extension will be removed from the system.

If an extension is changed that is also administered on an adjunct (such as voice mail or an ASAI link), the extension on the adjunct must also be changed to ensure proper functionality.

Exceptions

Administration that is associated with most buttons on the current extension (for example, call forwarding digits and abbreviated dial) are not changed with the new extension through the **`change extension-station n`** command.

Note:

A forwarded extension administered as a button will not be handled by the **`change extension-station n`** command, The reason is the extension for the call forwarded button are stored as digits rather than as a UID. It is recommended that the administrator use the **`list usage`** command prior to changing any extensions.

Updating the **ISDN BRI SPID** field for BRI telephones is omitted from this command. Changing BRI telephones is a 2-step process. The change must be made both on the system and on the telephone. Updating this field remains a manual process.

Audits

- If an attempt is made to change an extension that is administered on the same system as an **emergency location extension** on the **Station** screen, or as an **emergency location extension** on the **IP Address Mapping** screen, the following warning message appears:

  Extension exists as Emergency Location. Continue?

  Click **yes** to continue to process the change. Click **no** to stop the process.

  The **`change extension-station`** ***n*** command will be denied under the following conditions:

  - If the extension being changed is active on a call
  - If the extension is being accessed by administration

- If an attempt is made to change an extension that is administered on the same system as a **media complex extension** on the **Station** screen, the extension cannot be changed to a 6-digit or 7-digit number. The reason is the **media complex extension** field on the **Station** screen does not support 6-digit or 7-digit numbers.

  For example, if extension 50002 is an H.323 telephone and is administered on extension 50012 as the media complex, the **`change extension-station`** ***n*** command does not allow you to change extension 50002 to 7050002, since a 7-digit media complex number is not supported. The command would permit changing 50002 to 52222, since the resulting extension is a 5-digit extension.

Field descriptions

Station Name - This field is read only, and displays the name of the existing extension (the extension that was typed in the **`change extension-station`** ***n*** command).

Port - This field is read only, and displays the port of the existing extension.

For the fields in the **From Extension** column (all fields are read only):

Station - This field displays the current extension that is being changed (the extension that was typed in the **`change extension-station`** ***n*** command).

Message Lamp - This field displays the **Message Lamp Extension** associated with the current extension.

Emergency Location Ext. - This field displays the **Emergency Location Ext.** from the **Station** screen associated with the current extension.

IP Parameter Emergency Location - This field displays the **Emergency Location Extension** from the **IP Address Mapping** screen associated with the current extension.

For the fields in the **To Extension** column:

Station - Type a new extension that you want the current extension changed to.

Valid entries	Usage
0 to 9	Type up to seven numbers that make up a valid extension number for your dial plan.

Message Lamp - Type a new extension for the Message Lamp Extension.

Valid entries	Usage
0 to 9	Type up to seven numbers that make up a valid extension number for your dial plan.

Emergency Location Ext. - Type a new extension for the **emergency location ext.** field that will appear on the **Station** screen.

Valid entries	Usage
0 to 9	Type up to seven numbers that make up a valid extension number for your dial plan.

IP Parameter Emergency Location - The message **See Ip-Network Map Form** is displayed. The administrator can only change this field on the **IP Address Mapping** screen (using the **`change ip-network-map`** command).

CLAN (TN799x) Socket Usage screen

The CLAN socket load balancing feature introduces a new screen, **CLAN (TN799x) Socket Usage** (CLAN (TN799x) Socket Usage screen on page 118). Use the **`status clan-usage`** command. This new screen lists information about the socket usage for all TN799x circuit packs administered on a system (up to 64). Page 2 of the screen has the same fields as page 1. Up to 32 C-LANs can be listed on each page.

Figure 30: CLAN (TN799x) Socket Usage screen

```
status clan-usage                                                Page 1 of 2

                          CLAN (TN799x) SOCKET USAGE

TN799       Socket   Net     TN799       Socket   Net    TN799      Socket   Net
Loc     Sfx Usage    Rgn     Loc     Sfx Usage    Rgn    Loc    Sfx Usage    Rgn
02A14   C   245/400  20      02C09   D   125/250  20     03C06  D   400/400  125
```

Field descriptions

TN799 Loc - This is the cabinet/carrier/slot location of the TN799x circuit pack.

Sfx - This is the suffix of the TN799 circuit pack (C or D).

Socket Usage - The first number shows the number of sockets in use on the specified TN799x circuit pack when the command was entered. The second number is the value administered in the **Number of CLAN Sockets Before Warning** field using the **add/change ip-interfaces** command. The socket usage number does not include sockets used by adjuncts.

Net Rgn - This is the network region to which the TN799x circuit pack is assigned using the **add ip-interfaces** command.

The remaining fields are described in other documentation.

Events Report screen

The **reset ip-stations** command displays a new screen, **Events Report** (Events Report screen on page 118).

Figure 31: Events Report screen

```
display events

                                EVENTS REPORT

EVENT EVENT
                    Event      Event      First        Last        Evnt
TYPE  DESCRIPTION              Data 1     Data
2     Occur        Occur      Cnt
2033 IP FURQ-Demand Unregister  0          0         03/15/09:51 03/15/09:51  1
```

Extensions to Call which Activate Features By Name screen

The Extension to Cellular feature introduces a new screen, **Extensions to Call which Activate Features By Name** (Extensions to Call which Activate Features By Name screen, page 1 on page 119). The **Extensions to Call which Activate Features By Name** screen is where you map a dialed extension to a feature within Communication Manager. These are called Feature Name Extensions (FNE). These extensions are paired with Feature Access Codes (FAC). When the extension is called, the feature access code is activated.

Note:

The Feature Access Codes are administered on the **Feature Access Code (FAC)** screen.

To map a dialed extension to a feature within Communication Manager:

1. Type **`change off-pbx-telephone feature-name-extensions`**. Press **Enter**.

   The system displays the **Extensions to Call which Activate Features By Name** screen.

Figure 32: Extensions to Call which Activate Features By Name screen, page 1

```
change off-pbx-telephone feature-name-extensions                    Page 1 of 1

              EXTENSIONS TO CALL WHICH ACTIVATE FEATURES BY NAME

   Active Appearance Select: 31001            Idle Appearance Select: 31020
           Call Forward All: _________            Last Number Dialed: _________
 Call Forward Busy/No Answer: _________          Malicious Call Trace: _________
        Call Forward Cancel: _________    Malicious Call Trace Cancel: _________
                  Call Park: _________                Priority Call: _________
      Call Park Answer Back: _________               Send All Calls: _________
               Call Pick-Up: _________         Send All Calls Cancel: _________
       Conference on Answer: _________           Transfer On Hang-Up: _________
       Calling Number Block: _________       Transfer to Voice Mail: _________
     Calling Number Unblock: _________
      Directed Call Pick-Up: _________
      Drop Last Added Party: _________
  Exclusion (Toggle On/Off): _________
     Held Appearance Select: _________
```

Valid parameters

Action	Object	Qualifier
`change`	**`off-pbx-telephone feature-name-extensions`**	
`display`	**`off-pbx-telephone feature-name-extensions`**	

Field descriptions

Extension - Each **Extension** field is an extension that matches your dial plan. A user would dial the extension from their cell phone, thereby activating a Feature Access Code (FAC) administered for that feature.

Valid entries	Usage
blank **0**-**9**	Default = blank. Type an extension number, up to eight digits, of the Communication Manager feature you want to be able to access from the cell phone.

IP Interfaces screen

The CLAN Socket Load Balancing feature introduces a new screen, **IP Interfaces**. Use the **`list ip-interface <all|clan>`** command (the default is ***`all`***).

- IP Interfaces screen on page 120, shows the screen when the **`list ip-interfaces clan`** command is used.
- IP Interfaces screen on page 121, shows the screen when the **`list ip-interfaces all`** command is used with an S8500 or S8700 Media Server.
- IP Interfaces screen on page 121, shows the screen when the **`list ip-interfaces all`** command is used with an S8300 Media Server.

Figure 33: IP Interfaces screen

```
list ip-interface clan                                          Page 1 of x

                                IP INTERFACES

                                                                  Num
                                                                  Skts Net
On   Slot  Code  sfx Node Name       Subnet Mask   Gateway Address Warn Reg VLAN
y    01B04 TN799 D   clan1xxxxxxxxxx 255.255.0 .0  172. 22. 22.254 400  1   1
```

Figure 34: IP Interfaces screen

```
list ip-interface all                                              Page 1 of x

                                IP INTERFACES

                                                                        Net
On Type   Slot  Code  sfx  Node Name     Subnet Mask   Gateway Address Reg VLAN
y  C-LAN  01B04 TN799  D   clan1xxxxxxxx 255.255.0 .0  172. 22. 22.254  1   1
y  MEDPRO 01A05 TN2302 AP  medpro1xxxxxx 255.255.0 .0  172. 22. 22.254  1   1
y  VAL    01B06 TN2501 AP  val1xxxxxxxxx 255.255.0 .0  172. 22. 22.254  1   1
```

Figure 35: IP Interfaces screen

```
list ip-interface all                                              Page 1 of x

                                IP INTERFACES

                                                                        Net
On Type   Slot  Code  sfx  Node Name     Subnet Mask   Gateway Address Reg VLAN
y  PROCR                  135.6.41.121  255.255.0 .0  172. 22. 22.254  1   1
```

Field descriptions

Num Skts Warn - The value administered in the **Number of CLAN Sockets Before Warning** field using the **`add/change ip-interfaces`** command. This field is displayed only when the ***`clan`*** option is entered. When the ***`all`*** option is entered, the **Type** field is displayed. The **Num Skts Warn** field is not displayed.

Type - For the S8700 and S8500 Media Servers, the possible values are **CLAN**, **MEDPRO**, and **VAL**. For the S8300 Media Server, the only possible value is **PROCR**.

Node Name - For the S8700 and S8500 Media Servers, the **Node Name** field displays the node name of the IP interface as administered on the **Node Names** screen. For the S8300 Media Server, the **Node Name** field displays the IP address of the S8300, which is associated with the reserved node name procr on the **Node Names** screen.

The remaining fields are described in other documentation for the **IP Interfaces** screen.

IP Interface Status screen

The Camp-On/Busy-Out feature introduces a new screen, **IP Interface Status** (IP Interface Status on page 122). Use a new command, **`status media-processor <cabinet/carrier/slot>`**, to display this screen This new screen shows the busyout status of the specified MedPro or IPMedPro media processor board.

Figure 36: IP Interface Status

```
status media-processor 1c18                                    Page 1 of 1

                              IP INTERFACE STATUS

                            Link status: connected
                              Node Name: IPMEDPRO1
                        Source IP Address: 192.168.22.11
                              Subnet Mask: 255.255.255.0
                        Broadcast Address: 192.168.22.255
                         Physical Address: XX:XX:XX:XX:XX:XX
                                  Enabled? yes

                             DSP Channel Status
     DSP1: in-service/idle                    DSP5: in-service/idle
     DSP2: in-service/active, 1 calls         DSP6: in-service,/active, 4 calls
     DSP3: in-service/active, 3 calls         DSP7: in-service,/idle
     DSP4: in-service/active, 2 calls         DSP8: in-service,/idle
```

Valid parameters

Action	Object	Qualifier
`status`	**`media-processor`**	***`<cabinet/carrier/slot>`***

Field descriptions

Note:

All fields are display-only.

Link Status - Link Status indicates whether an Ethernet connection is being detected by the media processor. Values are **connected** or **disconnected**.

Node Name - This is the node name of the media processor administered with the **`add/change ip-interfaces`** command.

Source IP Address - This is the IP address of the media processor associated with the node name administered on the **IP Node Names** screen.

Subnet Mask - This is the subnet mask value administered with the **add/change ip-interfaces** command.

Broadcast Address - This is the broadcast address value administered with the **add/change ip-interfaces** command.

Physical Address - This is the physical IP address queried from the media processor.

Enabled? - This designates whether the IP interface is enabled or not. Values are **yes** or **no**.

DSP1-DSP8F - This is the service state of the DSPs when the **status media-processor** command was issued. Values are:

- in-service/idle
- in-service/active, ***x*** calls (where ***x*** indicates the number of calls active on the media processor)
- craft busied out
- PENDING busy out, ***x*** calls (marked for busy-out but not performed)
- out-of-service (for another specified reason; for example, "no link")

Stations with Off-PBX Telephone Integration screen, page 1

The Extension to Cellular feature introduces a new screen, **Stations with Off-PBX Telephone Integration** (Stations with Off-PBX Telephone Integration screen, page 1 on page 124). The **Stations with Off-PBX Telephone Integration** screen is where you map a user's office (host) telephone to an Extension to Cellular telephone (for example, a cell phone). A person's outside telephone number, like a cell phone, is mapped to an office telephone in Communication Manager. The telephone may be a standard office number (presumably the user's primary extension), or may be an AWOH (administration without hardware) extension.

Note:

When Extension to Cellular is administered, the initial state of the cell phone is disabled. You must enable the Extension to Cellular in order to receive calls on the cell phone from the Avaya server running Communication Manager.

To map a user's office (host) telephone to your cell phone:

1. Type **add off-pbx-telephone station-mapping**. Press **Enter**.

   The **Stations with Off-PBX Telephone Integration** screen appears.

Figure 37: Stations with Off-PBX Telephone Integration screen, page 1

```
add off-pbx-telephone station-mapping                          Page 1 of 2

                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

Station     Application   Dial   Phone Number          Trunk       Configuration
Extension                 Prefix                       Selection   Set
43001         EC500       ____ - 9736831204           ars         1
43005         EC500       ____ - 6093451298           ars         2
43007         OPS         ____ - 12345                ars         3
43009         OPS         ____ - 67890                aar         4
_______       _______     ____ - ________________     ____        __
_______       _______     ____ - ________________     ____        __
_______       _______     ____ - ________________     ____        __
_______       _______     ____ - ________________     ____        __
_______       _______     ____ - ________________     ____        __
_______       _______     ____ - ________________     ____        __
_______       _______     ____ - ________________     ____        __
_______       _______     ____ - ________________     ____        __
_______       _______     ____ - ________________     ____        __
_______       _______     ____ - ________________     ____        __
_______       _______     ____ - ________________     ____        __
_______       _______     ____ - ________________     ____        __
```

Valid parameters

Action	Object	Qualifier
add	**off-pbx-telephone station-mapping**	
change	**off-pbx-telephone station-mapping**	***<extension>***
display	**off-pbx-telephone station-mapping**	***<extension>***
list	**off-pbx-telephone station-mapping**	***<variable>***

- The **add off-pbx-telephone station-mapping** command displays a blank screen of two pages. It allows for the addition of sixteen extension to external telephone number associations. For each **Station Extension**, the remaining fields on the first page (except for the **Dial Prefix** field) must be filled in. The **Station Extension** fields on the second page are defaulted based upon the values entered for the first page.
- The **change off-pbx-telephone station-mapping *<extension>*** command displays a screen of two pages. It allows you to change one extension to external telephone number association. The first line contains the information for the extension you entered as the command variable. Additional entries may be added after the changed one. The table is filled in and validated as described for the add command.

If the specified extension is a valid type, but has not been previously administered for Extension to Cellular, then the screen is blank except for the first **Station Extension** field.

- The **`display off-pbx-telephone station-mapping <extension>`** command displays a screen of two pages. It lists up to sixteen entries, starting with the extension that you entered as the command variable. If this extension is not administered for Extension to Cellular, the display starts with the first administered Extension to Cellular extension following it.
- The extension may be omitted, in which case the display starts with the first extension administered for Extension to Cellular.
- The **`list off-pbx-telephone station-mapping <variable>`** command shows, on a single line, information about the association between an extension and external telephone number. The command variable specifies the telephone number or numbers of interest. The command variable may be:
  - a complete telephone number
  - a partial telephone number followed by an asterisk (acting as a "wildcard" character)
  - blank

Field descriptions

Station Extension - The **Station Extension** field is an administered extension in your dial plan for the "host" or office telephone.

Valid entries	Usage
a valid number in your dial plan	Default = blank. Type an extension number of the "host" office telephone up to eight digits.

Application - The **Application** field is where you indicate what type of application is associated with this telephone.

Valid entries	Usage
blank **EC500** **OPS**	Default = blank **EC500** = cell phone **OPS** = other outside telephone type (for example, the 4602 SIP-enabled telephone)

Dial Prefix - The **Dial Prefix** field are any digits that are prepended to the telephone **Number** field before dialing the outside telephone.

Valid entries	Usage
blank **0**-**9**, *****, #	Default = blank. Type up to four digits, including "*****" or "#". If included, "*****" or "#" must be in the first digit position.

Phone Number - The telephone **Number** field is the telephone number of the outside telephone.

Valid entries	Usage
0-**9**	Default = blank. Type up to fifteen digits.

Trunk Selection - The **Trunk Selection** field is where you define which outgoing trunk group you choose to use for outgoing calls.

Valid entries	Usage
ars aar	Default = blank.

Configuration Set - The **Configuration Set** field is used to administer the Configuration Set number that contains the desired call treatment options for this Extension to Cellular extension. There are ten Configuration Sets.

Valid entries	Usage
1-**10**	Default = blank. Type the number of the Configuration Set.

Stations with Off-PBX Telephone Integration screen, page 2

The second page of the **Stations with Off-PBX Telephone Integration** screen (Stations with Off-PBX Telephone Integration screen, page 2 on page 127) continues the administration of the telephone mapping. The information you entered in the **Station Extension** field on the first page appears as read only information on the second page.

Figure 38: Stations with Off-PBX Telephone Integration screen, page 2

```
add off-pbx-telephone station-mapping                          Page 2 of 2

                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

Station         Call       Mapping        Calls       Bridged
Extension       Limit      Mode           Allowed     Calls
43001           2          both           all         both
43005           2          both           all         both
43007           2          both           all         both
43009           2          both           all         both
                __         ____________   _________   ____________
                __         ____________   _________   ____________
                __         ____________   _________   ____________
                __         ____________   _________   ____________
                __         ____________   _________   ____________
                __         ____________   _________   ____________
                __         ____________   _________   ____________
                __         ____________   _________   ____________
                __         ____________   _________   ____________
                __         ____________   _________   ____________
                __         ____________   _________   ____________
                __         ____________   _________   ____________
```

Call Limit - The **Call Limit** field sets the maximum number of Extension to Cellular calls that may be simultaneously active at the telephone.

Valid entries	Usage
blank **1**-**10**	Default = **2**.

Mapping Mode - The **Mapping Mode** field contains the mode of operation in which the cell phone operates. See Mapping Modes on page 128 for information on the possible entries.

Valid entries	Usage
termination **origination** **both** **none**	Default = **both** (if the telephone **`Number`** field has not been previously administered for another extension with a **`Mapping Mode`** of **both** or **origination**. Otherwise, the default = **termination**).

Calls Allowed - The **Calls Allowed** field is used to identify the call filter type for an Extension to Cellular telephone. See Calls Allowed on page 129 for information on the possible entries.

Valid entries	Usage
internal **external** **all** **none**	Default = **all**.

Bridged Calls - The **Bridged Calls** field is used to determine if bridged call appearances, that may be administered on this **Stations with Off-PBX Telephone Integration** screen, should also be extended to the Extension to Cellular telephone. See Mapping Modes on page 128 for information on the possible entries.

Valid entries	Usage
termination **origination** **both** **none**	Default = **both.**

Mapping Modes

There are four modes in which an Extension to Cellular telephone can be mapped to the user's main office telephone.

- termination
- origination
- both
- none

These modes are used to control the degree of integration between their cell phone and main office number. The modes are valid for Extension to Cellular calls only. The modes are valid for:

- Calls to the user's main office number when Extension to Cellular is enabled
- Calls from the cell phone into the user's system when Extension to Cellular is enabled.

Mapping modes are administered on the second page of the **Stations with Off-PBX Telephone Integration** screen (Stations with Off-PBX Telephone Integration screen, page 2 on page 127).

Calls terminating to a cell phone

The termination mode is enabled by setting the **Mapping Mode** field on the second page of the **Stations with Off-PBX Telephone Integration** screen to **termination**. In termination mode, the cell phone may only be used to terminate (receive) calls from its associated host telephone. The cell phone may not be used to originate calls from its associated host telephone.

Calls originating from the cell phone are completely independent of Extension to Cellular, and behave exactly as before enabling Extension to Cellular.

Calls originating from a cell phone

The origination mode is enabled by setting the **Mapping Mode** field on the second page of the **Stations with Off-PBX Telephone Integration** screen to **origination**. In origination mode, the cell phone may only be used to originate calls from its associated host telephone. The cell phone may not be used to terminate (receive) calls from its associated host telephone.

Calls both to and from a cell phone

This mode is enabled by setting the **Mapping Mode** field on the second page of the **Stations with Off-PBX Telephone Integration** screen to **both**. In this mode, the cell phone may be used to originate calls and to terminate calls from its associated host telephone.

No calls to or from a cell phone

This mode is enabled by setting the **Mapping Mode** field on the second page of **the Stations with Off-PBX Telephone Integration** screen to **none**. In this mode, In this mode, the cell phone may not be used to originate calls or to terminate calls from its associated host telephone.

Calls Allowed

There are four values to define what kind of calls can be associated with the cell phone.

- internal
- external
- all
- none

These entries are used to filter the calls to the cell phone.

The **Calls Allowed** field is administered on the second page of the **Stations with Off-PBX Telephone Integration** screen (Stations with Off-PBX Telephone Integration screen, page 2 on page 127).

Internal

When **internal** is chosen as the call filter type, the cell phone receives only internal calls. External calls are not delivered to the cell phone.

- When **all** is chosen as the call filter type, the cell phone receives both internal and external calls.
- When **none** is chosen as the call filter type, the cell phone does not receive Extension to Cellular calls.

  Note:

  Regular calls placed to the cell phone number are still received.

External

When **external** is chosen as the call filter type, the cell phone receives only external calls. Internal calls are not delivered to the cell phone.

All

When **all** is chosen as the call filter type, the cell phone receives both internal and external calls.

None

When **none** is chosen as the call filter type, the cell phone does not receive Extension to Cellular calls.

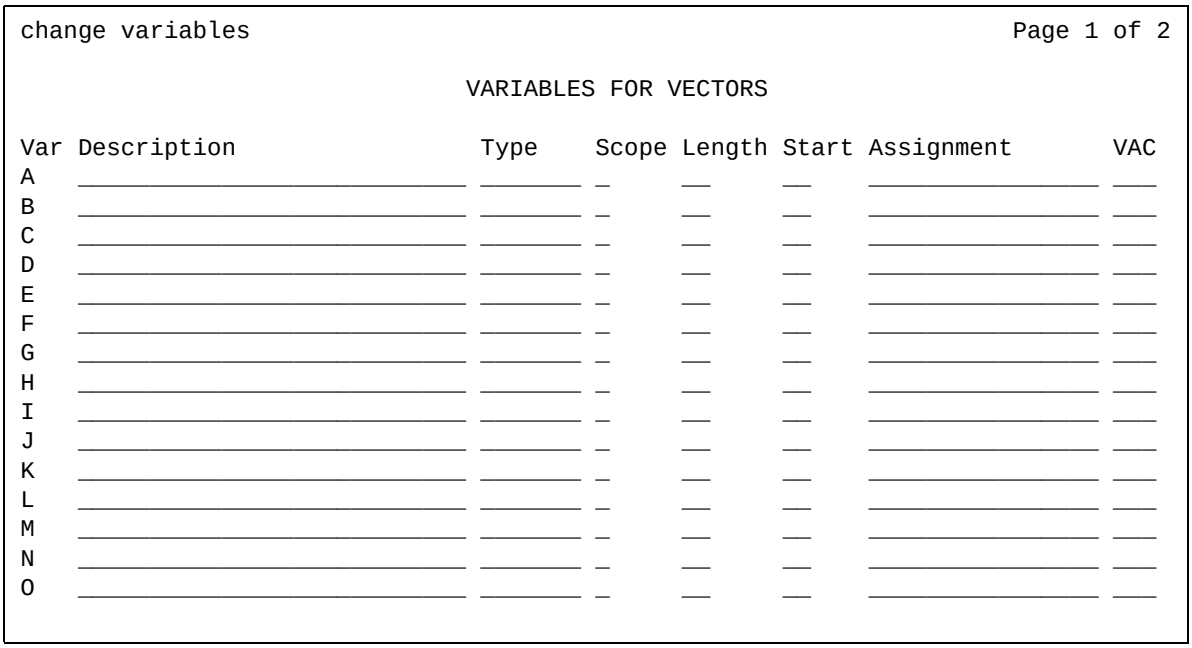
Note:

Regular calls placed to the cell phone number are still received.

Variables for Vectors screen

The Variables for Vectors feature introduces a new screen, **Variables for Vectors** (Variables for Vectors screen on page 131). Use the **`change variables`** command. On these two screens, you can assign variable definitions for vectors. For this feature to be activated, the **Vectoring (Variables)** field must be set to **y** on the **Call Center Optional Features** screen (use the **`display system-parameters customer-options`** command. See Call Center Optional Features screen on page 140). For more information on the Variables for Vectors feature, see Variables for Vectors on page 68.

Figure 39: Variables for Vectors screen



```
change variables                                                Page 1 of 2

                                VARIABLES FOR VECTORS

Var Description                    Type    Scope Length Start Assignment       VAC
A   ______________________________ ________ _     __     __    ________________ ___
B   ______________________________ ________ _     __     __    ________________ ___
C   ______________________________ ________ _     __     __    ________________ ___
D   ______________________________ ________ _     __     __    ________________ ___
E   ______________________________ ________ _     __     __    ________________ ___
F   ______________________________ ________ _     __     __    ________________ ___
G   ______________________________ ________ _     __     __    ________________ ___
H   ______________________________ ________ _     __     __    ________________ ___
I   ______________________________ ________ _     __     __    ________________ ___
J   ______________________________ ________ _     __     __    ________________ ___
K   ______________________________ ________ _     __     __    ________________ ___
L   ______________________________ ________ _     __     __    ________________ ___
M   ______________________________ ________ _     __     __    ________________ ___
N   ______________________________ ________ _     __     __    ________________ ___
O   ______________________________ ________ _     __     __    ________________ ___
```

Var - The **Var** field lists the variable letters **A**-**Z**, one for each row.

For the remaining fields, the following applies:

Table 1: Field values for the Variables for Vectors screen

Type	Scope: **L** (for local) or **G** (for global)	Length: the maximum number of digits to use	Start: the character position of the digit string to start with	Assignment: a number to be preassigned to the variable	VAC (variable access code) - the vector variable (VV) feature access code to use for changing the value
collect	Type either **L** or **G**. This is a required field.	Type a number between 1-16 to be used from the up to 16-digit collected digit string. This is a required field. The default is **16**.	Type a number between 1-16 for the start position. This is a required field. The default is **1**.	For **Type L**, this does not apply. For **Type G**, type a number between 0-9999999999999999 (sixteen digits long). This is an optional field. The default is blank if null, or displays the current value when not null.	Does not apply.
asaiuui	Entry of **L** is pre-entered.	Type a number between 1-16 to be used from the up to 96-digit ASAI user information digit string. This is a required field. The default is **16**.	Type a number between 1-96 for the start position. This is a required field. The default is **1**.	Does not apply.	Does not apply.

1 of 2

Table 1: Field values for the Variables for Vectors screen (continued)

Type	Scope: **L** (for local) or **G** (for global)	**Length**: the maximum number of digits to use	**Start**: the character position of the digit string to start with	**Assignment**: a number to be preassigned to the variable	**VAC** (variable access code) - the vector variable (VV) feature access code to use for changing the value
value	Entry of **G** is pre-entered.	Entry of **1** is pre-entered.	Does not apply.	Type a number between 0-9. This is an optional field. The default is blank if null, or displays the current value when not null.	Type a value of **VVx**, where **x** is a number between 1-9. This is an optional field. The default is blank if null or if **VVx** is not assigned. (To assign **VVx** values, see Feature Access Code (FAC) screen, page 6 on page 144.)
tod	Entry of **G** is pre-entered.	Does not apply.	Does not apply.	Displays current value from system clock.	Does not apply.
doy	Entry of **G** is pre-entered.	Does not apply.	Does not apply.	Displays current value from system clock.	Does not apply.
dow	Entry of **G** is pre-entered.	Does not apply.	Does not apply.	Displays current value from system clock.	Does not apply.
vdn	Entry of **L** is pre-entered.	Does not apply.	Does not apply.	Entry of **active** or **latest** is required. The default is blank.	Does not apply.

2 of 2

Release 2.0 changed screens

Avaya Communication Manager, release 2.0, includes the following changed screens. For a more complete explanation of the screens and their function, see the *Administrator's Guide for Avaya Communication Manager*, 555-233-506.

Fields moved or changed

A number of fields have been moved from one screen to a different screen. The purpose was to make a more logical grouping and for future features. In addition, other fields have been renamed for a more logical explanation. The function of these fields, however, remains the same.

Table 2 shows a list of the fields that have moved or changed.

Note:

In these examples, the screen "name" is actually the command that you type to access the screen. For example, the **location-parameters** screen means that you should type the command **`change location-parameters`** to access the proper screen.

Table 2: Fields that have moved or changed names

Field name	Changed to	From screen	Moved to screen
Analog Ringing Cadence	**-------**	**system-parameters country-options**	**location-parameters**
Analog Line Transmission	**-------**	**system-parameters country-options**	**location-parameters**
Companding Mode	**-------**	**system-parameters country-options**	**location-parameters**
Digital Loss Plan	**2 Party Loss Plan**	**system-parameters country-options**	**location-parameters**
Digital Tone Plan	**Tone Loss Plan**	**system-parameters country-options**	**location-parameters**
End-to-End total loss (db) in a n-party conference	**-------**	**system-parameters country-options**	**location-parameters**

1 of 3

Table 2: Fields that have moved or changed names (continued)

Field name	Changed to	From screen	Moved to screen
Customize (associated with the **End-to-End total loss (db) in a n-party conference** field)	-------	(new)	**location-parameters**
Base Tone Generator Set	-------	**system-parameters country-options**	**tone-generation**
440Hz PBX-dial Tone	-------	**system-parameters country-options**	**tone-generation**
440Hz secondary-dial Tone	-------	**system-parameters country-options**	**tone-generation**
Tone Name	-------	**system-parameters country-options**	**tone-generation**
Cadence Step	-------	**system-parameters country-options**	**tone-generation**
Tone (Frequency/ Level)	-------	**system-parameters country-options**	**tone-generation**
Flashhook Interval	-------	**system-parameters features**	**location-parameters**
Disconnect Timing	-------	**system-parameters features**	**location-parameters**
RECALL TIMING Upper Bound	-------	**system-parameters features**	**location-parameters**
RECALL TIMING Lower Bound	-------	**system-parameters features**	**location-parameters**
Forward Disconnect Timer	-------	**system-parameters features**	**location-parameters**
ani for pbx	**Default ANI**	**system-parameters multifrequency-signaling**	-------
(all fields except the following three fields)	-------	**system-parameters multifrequency-signaling**	**multifrequency-signaling**

Table 2: Fields that have moved or changed names (continued)

Field name	Changed to	From screen	Moved to screen
MF Interdigit Timer	**-------**	**system-parameters multifrequency-signaling**	**location-parameters**
Outgoing Shuttle Exchange Cycle Timer	**-------**	**system-parameters multifrequency-signaling**	**location-parameters**
MF Test Call Extension	**-------**	**system-parameters multifrequency-signaling**	**system-parameters maintenance**
(all fields)	**-------**	**terminal-parameters 302/ 603/606**	**terminal-parameters** (page 1)
(all fields)	**-------**	**terminal-parameters 6400/607A1/4600**	**terminal-parameters** (page 2)
(all fields)	**-------**	**terminal-parameters 8400**	**terminal-parameters** (page 3)
default parameter set	**Base Parameter Set**	**terminal-parameters**	**-------**

3 of 3

Administration Changes screen

If the **station set port type** field is **IP**, and if the **Record IP Registrations in History Log?** field on the **System Parameters Features** screen is set to **y**, the history log already records IP registrations, just not unregistrations. Changes to the **Administration Changes** screen now records IP unregistrations (Administration Changes screen on page 137). This change is prompted by the E911 emergency location information number (ELIN) for wired IP feature.

This log is viewable through the **`list history`** and **`notify history`** commands. This log contains the following information:

- Date and time of feature use
- Extension number
- Port number

Unregistrations will be logged under login "ip-u". The "-u" part of the login is for consistency with PSA and ACTR, which use "-a" for associations and "-u" for unassociations.

Figure 40: Administration Changes screen

```
notify history

                              ADMINISTRATION CHANGES

Date Time  Login   Actn  Object       Qualifier
2/15 10:18 actr-d  cha   station      2005
2/15 10:18 actr-u  cha   station      2004
2/15 10:17 init    cha   system-param features
2/15 10:15 tti-m   cha   station      2004
2/15 10:15 tti-m   cha   station      2005
2/15 10:15 tti-s   cha   station      2005
2/15 10:12 actr-a  cha   station      2005
2/15 10:12 ip-u    cha   station      2006
2/15 10:12 ip-u    cha   station      2007
2/15 10:10 ip-u    cha   station      2008
2/15 10:10 ip-a    cha   station      2009
```

Attendant Console screen

On the **Attendant Console** screen (Attendant Console screen, page 2 on page 138), the field **IP Emergency Calls** in earlier releases of Communication Manager has been renamed to **Remote Softphone Emergency Calls** in release 2.0. This newly-renamed field also allows a new value, **as-on-local**. The value **extension** is no longer allowed for this field. Use the **change attendant *n*** command, where ***n*** is the number of the attendant console. This change is prompted by the E911 emergency location information number (ELIN) for wired IP feature.

This field only appears if the **IP Softphone** field in the **Station** screen is set to **y**. The restriction, (current in previous releases of Communication Manager) that this field can only be changed if the extension is unregistered, remains in force for release 2.0.

Figure 41: Attendant Console screen, page 2

```
change attendant 2                                              Page 2 of 4

                                  ATTENDANT CONSOLE

VIS FEATURE OPTIONS
              Auto Start? y
      Echo Digits Dialed? y

EMERGENCY CALL HANDLING
Remote Softphone Emergency Calls: as-on-local
          Emergency Location Ext: 1001
```

Note:

The fields are not accessible if the set type is not one of the IP telephone or IP softphone types.

Field descriptions

Remote Softphone Emergency Calls - This field has been renamed. In earlier releases of Communication Manager, this field was named **IP Emergency Calls**.

Valid entries	Usage
as-on-local	Type **as-on-local** to achieve the following results: • If the administrator chooses not to use the new feature outlined in the next bullet item and chooses to leave the **Emergency Location Extension** fields (that correspond to this telephone's IP address) on the **IP Address Mapping** screen blank, the value **as-on-local** sends the extension entered in the **Emergency Location Extension** field in the **Station** screen to the Public Safety Answering Point (PSAP). • If the administrator does choose to use the new feature and populates the **IP Address Mapping** screen with emergency numbers, the value **as-on-local** functions as follows: - If the **Emergency Location Extension** field in the **Station** screen is the same as the **Emergency Location Extension** field in the **IP Address Mapping** screen, the value **as-on-local** sends the extension to the Public Safety Answering Point (PSAP). - If the **Emergency Location Extension** field in the **Station** screen is different from the **Emergency Location Extension** field in the **IP Address Mapping** screen, the value **as-on-local** sends the extension in the **IP Address Mapping** screen to the Public Safety Answering Point (PSAP).
block	Type **block** to prevent the completion of emergency calls. Use this entry for users who move around but always have a circuit-switched telephone nearby, and for users who are farther away from the media server or system than an adjacent area code served by the same 911 Tandem office. When users attempt to dial an emergency call from an IP telephone and the call is blocked, they can dial 911 from a nearby circuit-switched telephone instead.

Valid entries	Usage
cesid	Type **cesid** to allow Communication Manager to send the CESID information supplied by the IP softphone to the PSAP. The end user enters the emergency information into the IP softphone. Use this entry for IP softphones with Road Warrior service that are near enough to the media server or system that an emergency call routed over the trunk reaches the PSAP that covers the server or system. If the media server or system uses ISDN trunks for emergency calls, the digit string is the telephone number, provided that the number is a local direct-dial number with the local area code, at the physical location of the IP softphone. If the media server or system uses CAMA trunks for emergency calls, the end user enters a specific digit string for each IP softphone location, based on advice from the local emergency response personnel.
option	Type **option** to allow the user to select the option (**as-on-local**, **block**, or **cesid**) that the user selected during registration and the IP softphone reported. Use this entry for extensions that may be switched back and forth between IP softphones and a telephone with a fixed location. The user chooses between **as-on-local**, **block** and **cesid** on the softphone. A DCP telephone in the office use the **Emergency Location Extension** field in the **Station** screen. During registration, users and administrators see the following choices on the IP softphone user interface: **This is the softphone interface equivalent to as-on-local:** The box "Use the following information to identify your location to a PSAP should you need to make a 911 call: your extension number" is checked. **This is the softphone interface equivalent to block:** The box "Enable Emergency Call Handling Feature" is not checked. **This is the softphone interface equivalent to cesid:** The box "Use the following information to identify your location to a PSAP should you need to make a 911 call: telephone number _____" has a telephone number entered.

Call Center Optional Features screen

The **Call Center Optional Features** screen (Call Center Optional Features screen on page 141) is screen 6 using the **`display system-parameters customer-options`** command.

For the Variables for Vectors feature to work, the **Call Center Release** field must be set to **12.0** or later. In addition, your license file must set both the **Vectoring (Basic)** and **Vectoring (Prompting)** fields to **y**. Once these conditions are met, the **Vectoring (Variables)** field can also be set to **y**.

For the Service level maximizer feature to work, the **Service Level Maximizer** field must be set to **y**.

Figure 42: Call Center Optional Features screen

```
display system-parameters customer-options                      Page 6 of 10

                          CALL CENTER OPTIONAL FEATURES

                           Call Center Release: 12.0

                                ACD? n      PASTE (Display PBX Data on
telephone)? n
                      BCMS (Basic)? n                          Reason Codes? n
         BCMS/VuStats Service Level? n              Service Level Maximizer? y
  BSR Local Treatment for IP & ISDN? n             Service Observing (Basic)? n
                 Business Advocate? n      Service Observing (Remote/By FAC)? n
                   Call Work Codes? n              Service Observing (VDNs)? n
      DTMF Feedback Signals For VRU? n                           Timed ACW? n
                 Dynamic Advocate? n                    Vectoring (Basic)? y
       Expert Agent Selection (EAS)? n                Vectoring (Prompting)? y
                          EAS-PHD? n              Vectoring (G3V4 Enhanced)? n
                Forced ACD Calls? n      Vectoring (ANI/II-Digits Routing)? n
             Least Occupied Agent? n      Vectoring (G3V4 Enhanced Routing)? n
          Lookahead Interflow LAI)? n                   Vectoring (CINFO)? n
Multiple Call Handling (On Request)? n       Vectoring (Best Service Routing)? n
    Multiple Call Handling (Forced)? n                  Vectoring (Holidays)? n
                                                       Vectoring (Variables)? y

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

Dial Plan Analysis Table screen

The **Dialed String** fields on the **Dial Plan Analysis Table** screen (Dial Plan Analysis Table screen, page 1 on page 142) allows an entry up to four digits. Use the **`display dialplan analysis`** command. By widening the **Dialed String** column to four digits, customers can allocate blocks of 1000 numbers. This change is prompted by the Multi-Location Dial Plan feature.

The screen has also been increased to twelve pages, with three columns of fifteen entries on each page.

Figure 43: Dial Plan Analysis Table screen, page 1

```
display dialplan analysis                                    Page 1 of 12

                          DIAL PLAN ANALYSIS TABLE
                                                          Percent Full: 7

      Dialed  Total  Call        Dialed  Total  Call        Dialed  Total  Call
      String  Length Type        String  Length Type        String  Length Type
        00      2    attd
        1       3    dac
        2       4    ext
        2       5    ext
        3       5    ext
        4       5    ext
        4       7    ext
        5       5    ext
        5       7    ext
        6       5    ext
        7210    7    ext
        8       7    ext
        9       1    fac
        *       3    fac
        #       3    fac
```

The **Call Type** allows a **Dialed String** value of either a given first digit (for example, **7**), a set of two-digit pairs (for example, **70**, **71**, **72**, ...), a set of three-digit pairs (for example, **701**, **702**, **703**, ...), or a set of four-digit pairs (for example, **7001**, **7002**, **7003**, ...).

The following apply:

- When a three-digit entry exists, a new three-digit entry with the same dial string cannot be added if the total length is different.
- When a four-digit entry exists, a new four-digit entry with the same dial string cannot be added if the total length is different.
- The **Dialed String** column on the **Dial Plan Analysis Table** screen allows mixed (different) length dial strings for the same first digit. This allows a mix of 1-digit, 2-digit, 3-digit, and 4-digit entries having the same first digit. This removes previous screen validations.

  The **Dialed String** column on the **Dial Plan Analysis Table** screen does not allow mixed (different) lengths for 2-digit, 3-digit, or 4-digit dial strings.
- A new entry cannot be administered if it causes an existing extension (ext), FAC, or TAC entry to become inaccessible. For example, let us say that a customer has the following range administered:

```
Dialed  Total   Call
String  Length  Type
  4       4     ext
```

If the customer now adds this entry:

```
Dialed  Total   Call
String  Length  Type
  41      3     fac
```

The system ensures that no extensions of the format **41xx** are administered. If any are administered, the new "fac" entry is blocked.

Feature Access Code (FAC) screen

A new field, **Attendant Access Code**, is added to page 1 of the **Feature Access Code (FAC)** screen (Feature Access Code (FAC) screen, page 1 on page 143). Use the **change feature-access-codes** command. This field only appears and is valid if an **attd** entry does not exist on the **Dial Plan Analysis** screen. You cannot have an entry in both the **Dial Plan Analysis** screen and in the **Feature Access Code (FAC)** screen. This change is prompted by the Multi-Location Dial Plan feature.

Figure 44: Feature Access Code (FAC) screen, page 1

```
change features-access-codes                                    Page 1 of 8

                            FEATURE ACCESS CODE (FAC)

         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code:
                       Answer Back Access Code:
                         Attendant Access Code: 00
      Auto Alternate Routing (AAR) Access Code: *88
    Auto Route Selection (ARS) - Access Code 1: 9          Access Code 2:
                Automatic Callback Activation:              Deactivation:
Call Forwarding Activation Busy/DA:        All: *20         Deactivation: #20
                        Call Park Access Code:
                      Call Pickup Access Code:
CAS Remote Hold/Answer Hold-Unhold Access Code:
                  CDR Account Code Access Code:
                        Change COR Access Code:
                   Change Coverage Access Code:

                  Data Origination Access Code:
                      Data Privacy Access Code:
```

Attendant Access Code - The **Attendant Access Code** field on the **Feature Access Code (FAC)** screen takes on the same characteristics as the **attd** call type administered on the **Dial Plan Analysis** screen. Entries in this field mcfust conform to the existing **Feature Access Code (FAC)** screen rules.

The **Dial Plan Analysis** screen allows administration of only one **attd** code that connects to one attendant. To allow more than one attendant access code in a single distributed network, the **Attendant Access Code** field has been added to the **Feature Access Code (FAC)** screen.

Valid entries	Usage
0-9	Defines how users call an attendant. Attendant access numbers can start with any number from 0-9 and contain 1 or 2 digits. If a telephone's COR restricts the user from originating calls, this user cannot access the attendant using this code.

Another page of the **Feature Access Code (FAC)** screen has been changed, prompted by a different feature.

New fields for the Variables for Vectors feature have been added to page 6 of the **Feature Access Code (FAC)** screen (Feature Access Code (FAC) screen, page 6 on page 144). Use the **change feature-access-codes** command. These fields all you to assign nine unique vector variable feature access codes, in the format **VVx** (where **x** is a number from 1-9), for **value** type variables. For an explanation of **value** type variables, see Variables for Vectors screen on page 130.

Figure 45: Feature Access Code (FAC) screen, page 6

```
change features-access-codes                                  Page 6 of 8

                            FEATURE ACCESS CODE (FAC)

                        Call Vectoring/Call Prompting Features

   Converse Data Return Code:  ____

Vector Variable 1 (VV1) Code:  ____
Vector Variable 2 (VV2) Code:  ____
Vector Variable 3 (VV3) Code:  ____
Vector Variable 4 (VV4) Code:  ____
Vector Variable 5 (VV5) Code:  ____
Vector Variable 6 (VV6) Code:  ____
Vector Variable 7 (VV7) Code:  ____
Vector Variable 8 (VV8) Code:  ____
Vector Variable 9 (VV9) Code:  ____
```

Feature-Related System Parameters screen

A new field, **Treat ISDN Call to Busy User as ACA Short Holding Time Call**, has been added to page 1 of the **Feature-Related System Parameters** screen (Feature-Related System Parameters screen, page 4 on page 145). Use the **`change system-parameters features`** command. This field allows the administrator to indicate whether ISDN calls placed to user telephones that are busy should be considered ACA short calls (see ISDN calls to busy stations treated as ACA short calls on page 56).

Note:

The **Automatic Circuit Assurance (ACA) Enabled** field must be set to **y** for this field to appear.

Figure 46: Feature-Related System Parameters screen, page 4

```
change system-parameters features                                Page 4 of 12

                          FEATURE-RELATED SYSTEM PARAMETERS

                               Self Station Display Enabled? n
                                    Trunk-to-Trunk Transfer: none
    Automatic Callback - No Answer Timeout Interval (rings): 3
                       Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                 AAR/ARS Dial Tone Required? y
                                         Music/Tone on Hold: none
              Music (or Silence) on Transferred Trunk Calls? no
                              DID/Tie/ISDN Intercept Treatment: attd
    Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                  Automatic Circuit Assurance (ACA) Enabled? y
                                         ACA Referral Calls: local
                                  ACA Referral Destination: 8102
               ACA Short Holding Time Originating Extension: 8122
                ACA Long Holding Time Originating Extension: 8123
Treat ISDN Call to Busy User as ACA Short Holding Time Call? y
             Abbreviated Dial Programming by Assigned Lists? n
       Auto Abbreviated/Delayed Transition Interval (rings): 2
                    Protocol for Caller ID Analog Terminals: Bellcore
    Display Calling Number for Room to Room Caller ID Calls? n
```

Another page of the **Feature-Related System Parameters** screen has been changed, prompted by a different feature.

If an emergency call should drop (get disconnected), the public safety personnel will attempt to call back. If the ELIN that was sent was not equivalent to the caller's extension number, the return call would ring some other set than the one that dialed 911. To overcome that limitation, this feature automatically forwards that return call to the set that placed the emergency call for an administered period of time.

This Emergency Extension Forwarding only applies if the emergency location extension number is an extension on the same PBX as the extension that dialed 911. Customers who have several PBXs in a campus should assign emergency location extensions accordingly.

A new field, **Emergency Extension Forwarding (min)**, has been added to page 4 of the **Feature-Related System Parameters** screen (Feature-Related System Parameters screen, page 4 on page 146). Use the **`change system-parameters features`** command. This field sets the Emergency Extension Forwarding timer for all incoming trunk calls if an emergency call gets cut off (drops). This change is prompted by the E911 emergency location information number (ELIN) for wired IP feature.

Note:

It is important to realize that the call forwarding timer, once it is running, applies to *all* incoming trunk calls and is not limited to just incoming calls from an emergency care provider. The reason is there is no way for the system to know that an incoming trunk call is actually a return call from an emergency care provider.

Figure 47: Feature-Related System Parameters screen, page 4

```
change system-parameters features                                Page 4 of 12

                          FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
               System Printer Endpoint:                      Lines Per Page: 60
                   EIA Device Bit Rate: 9600

 Emergency Extension Forwarding (min): 10

SYSTEM-WIDE PARAMETERS
                           Switch Name:
         Emergency Numbers - Internal:           External: 911
      No-License Incoming Call Number:

MALICIOUS CALL TRACE PARAMETERS
                Apply MCT Warning Tone? n       MCT Voice Recorder Trunk Group:

SEND ALL CALLS OPTIONS
     Send All Calls Applies to: station        Auto Inspect on Send All Calls? n

UNIVERSAL CALL ID
     Create Universal Call ID (UCID)? n        UCID Network Node ID:
```

Field descriptions

Emergency Extension Forwarding (min) -

Valid entries	Usage
0-999	Type a number between 0-999 that represents the time (in minutes) that an incoming trunk call will forward to the extension that made the initial 911 call. The default value for both new installs and upgrades is **10**. If a user at the emergency location extension (the extension that made the initial 911 call) manually turns off the Call Forwarding feature, the feature is off no matter how many minutes might remain on the timer.

While the emergency extension forwarding timer is running, the feature turns on the lamp on the call forwarding button, and appears in the **CF Destination Ext** field on the first page of the **General Status** screen. Use the **`status station` *n*** command, where ***n*** is the telephone number. Also, the Send All Calls (SAC) and Do Not Disturb (DND) features, if on, will temporarily be turned off. Once the Emergency Extension Forwarding timer expires, the Send All Calls feature will be turned on again.

Note:

The Do Not Disturb (DND) feature remains turned off and must be reset manually.

The status of the call forwarding, and of SAC and DND, appears on the first page of the **General Station** screen for the emergency location extension. Use the **`status station` *n*** command, where ***n*** is the telephone number.

Hunt Group screen

A new **Group Type** of **slm** is allowed on page 1 of the **Hunt Group** screen (Hunt Group screen, page 1 on page 148). Use the **`change hunt-group` *n*** command, where ***n*** is the hunt group number. This change is prompted by the Service level maximizer feature.

Figure 48: Hunt Group screen, page 1

```
change hunt-group 2                                              Page 1 of 3

                                  HUNT GROUP

           Group Number: 2                                   ACD? y
             Group Name: HNT-2                             Queue? y
        Group Extension: 7330002                          Vector? y
             Group Type: slm
                     TN: 1
                    COR: 1                          MM Early Answer? n
          Security Code:
   ISDN Caller Display:

          Queue Length: 5
 Calls Warning Threshold: 2     Port:
  Time Warning Threshold: 15    Port:
```

Click **Next** to go to page 2 of the **Hunt Group** screen (Hunt Group screen, page 2 on page 148). The **Maximum Auto Reserve Agents** field only displays if the **Group Type** on page 1 is **slm**.

Figure 49: Hunt Group screen, page 2

```
change hunt-group 2                                              Page 2 of 3

                                  HUNT GROUP

                  Skill? y           Expected Call Handling Time (sec): 180
                    AAS? n             Target Service Level (% in sec): 80 in 20
               Measured: both
   Supervisor Extension:


    Controlling Adjunct: none


      VuStats Objective:
Timed ACW Interval (sec):                    Maximum Auto Reserve Agents: 0
  Multiple Call Handling: none

                                          Redirect on No Answer (rings): 4
                                                       Redirect to VDN: 52002
                        Forced Entry of Stroke Counts or Call Work Codes? n
```

IP Address Mapping screen

A new column and fields, **Emergency Location Extension**, has been added to the first page of the **IP Address Mapping** screen (IP Address Mapping screen, page 1 on page 149). Use the **`change ip-network-map`** command. This change is prompted by the E911 emergency location information number (ELIN) for wired IP feature.

Figure 50: IP Address Mapping screen, page 1

```
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      ________
___.___.___.___  ___.___.___.___    __      ___        ____      ________
___.___.___.___  ___.___.___.___    __      ___        ____      ________
___.___.___.___  ___.___.___.___    __      ___        ____      ________
___.___.___.___  ___.___.___.___    __      ___        ____      ________
___.___.___.___  ___.___.___.___    __      ___        ____      ________
___.___.___.___  ___.___.___.___    __      ___        ____      ________
___.___.___.___  ___.___.___.___    __      ___        ____      ________
___.___.___.___  ___.___.___.___    __      ___        ____      ________
```

The administrator needs to fill out the **IP Address Mapping** screen with emergency location extensions for every IP address range in their LAN's data network. Telephones that are physically close together but have different IP addresses could have the same ELIN. Once completed, the administrator would not need to update the **IP Address Mapping** screen again unless they re-wire the building.

If users tell the system administrator that they have moved their extensions, then the system administrator should make sure that the ALI database will have their telephone's new physical locations. After doing so, the administrator should update each user's **Station** screen.

Field descriptions

Emergency Location Extension - When updating Communication Manager, release 2.0, from an earlier version of Communication Manager, the **Emergency Location Extension** fields take on the same values as the **Emergency Location Ext** field on the **Station** screen.

Valid entries	Usage
0-**9**	Enter the emergency location extension for this telephone, up to 7 digits.

Similar to the **Emergency Location Ext** field on the **Station** screen, these entries have to be blank or of a type extension in the dial plan. They do not have to be extensions on the local system. They can be UDP extensions on another PBX. The entries default to blank. A blank entry typically would be used for an IP softphone dialing in through PPP from somewhere outside the customer's network, and used outside the USA and Canada.

IP Interfaces screen

Changes to the **`add/remove ip-interface`** command have prompted changes to the **IP Interfaces** screen (IP Interfaces screen on page 150). The layout of the fields on the **IP Interfaces** screen is changed to a vertical display for a single circuit pack rather than the previous horizontal display for multiple circuit packs.

Figure 51: IP Interfaces screen

```
add ip-interface 02c08                                          Page 1 of X

                                IP Interfaces

                    Type: CLAN
                    Slot: 02c08
                Code Sfx: TN799 D
               Node Name: clan1xxxxxxxxxx
              IP Address: 123.456.789.012
             Subnet Mask: ___.___.___.___
         Gateway Address: ___.___.___.___
     Enable Ethernet Pt? n
         Network Region: 20
                    VLAN: 0


Number of CLAN Sockets Before Warning: 400
```

Field descriptions

Number of CLAN Sockets Before Warning - This field appears only if the value in the **Type** field is **CLAN**.

Valid entries	Usage
1-**499**	Default = **400**. Type a threshold number of CLAN sockets that can be used (for registering endpoints) before a warning is issued.

Type - This field is display-only, based on the board location entered on the command line.

Valid entries	Usage
CLAN, MEDPRO, VAL	Valid for S8700 and S8500 Media Servers.
PROCR	Valid for S8300 Media Server.

Slot - This field is display-only, based on the slot number entered on the command line.

Valid entries	Usage
2-6 alpha-numeric characters or (blank)	For the S8300 Media Server, the value is (blank).

Code Sfx - This field is display-only, based on the circuit pack in the location specified on the command line.

Valid entries	Usage
7 characters or (blank)	The first 6 alpha-numeric characters are for the TN code, followed by 1 alpha character Code Suffix. If the board has an A suffix, the value in the **Sfx** portion of the field is (blank). For an S8300 Media Server, this field is (blank).

Node Name - This field is user-specified, based the name administered on the **IP Node Names** screen.

Valid entries	Usage
15 alpha-numeric characters	User-specified, based the name administered on the **IP Node Names** screen.

IP Address - This field is display only, from the **IP Node Names** screen, based on the node name entered.

Valid entries	Usage
valid IP address	Displays an IP address from the **IP Node Names** screen, based on the node name entered.

IP Network Region screen

With the increase to 250 possible network regions the **IP Network Region** screen was changed. Use the **`change ip-network-region`** ***n*** command, where ***n*** is the number of the network region you want to change.

The **Ip Network Region** screen shows specific IP region information on page 1 (IP Network Region screen, page 1 on page 153), which includes not only the codec set, but also shows bandwidth management information, such as:

- Whether the regions are directly or indirectly connected
- The WAN bandwidth limits (if any), the units for those bandwidth limits
- The intervening regions when the regions are indirectly connected

Note:

Only one path is allowed to be administered at this time for the non-adjacent regions.

Figure 52: IP Network Region screen, page 1

```
add ip-network-region 1                                          Page 1 of 19

                                IP NETWORK REGION

  Region: 1
Location: 1                Home Domain:
    Name: Rosebud NR 1
                                Intra-region IP-IP Direct Audio: yes
AUDIO PARAMETERS                Inter-region IP-IP Direct Audio: yes
   Codec Set: 1                           IP Audio Hairpinning? y
UDP Port Min: 2048
UDP Port Max: 3028                      RTCP Reporting Enabled? y
                                 RTCP MONITOR SERVER PARAMETERS
DIFFSERV/TOS PARAMETERS           Use Default Server parameters: y
 Call Control PHB Value: 34
        Audio PHB Value: 46
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 7
        Audio 802.1p Priority: 6       AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
   H.323Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

For Linux platforms in release 2.0, page 2 (IP Network Region screen, page 2 on page 153) is the LSP names page. This page covers the information for the LSP names in priority order.

Figure 53: IP Network Region screen, page 2

```
add ip-network-region 1                                          Page 2 of 19

                                IP NETWORK REGION

LSP NAMES IN PRIORITY ORDER
1
2
3
4
5
6
```

To accommodate the maximum of 250 regions for the Linux platforms, seventeen additional pages are now needed for each region's inter-region connectivity information. Page 3 (Inter Network Region Connection Management screen, page 3 on page 154) to page 19 are called the **Inter Network Region Connection Management** screens. These seventeen pages show the inter-region connectivity, numbered 1-250, for 15 region pairs.

Figure 54: Inter Network Region Connection Management screen, page 3

```
add ip-network-region 1                                          Page 3 of 19

                    INTER NETWORK REGION CONNECTION MANAGEMENT

src dst
rgn rgn         codec-set  direct-WAN  WAN-BW-limits  Intervening-regions
1   1              1           y          256:Kbits
1   2              1           n                      1    ___ ___ ___
1   3              1
1   4              1           n                      1    ___ ___ ___
1   5              1           n                      6    ___ ___ ___
1   6              1           y             :NoLimit
1   7              1           y           10:Calls
1   8
1   9
1   10
1   11
1   12
1   13
1   14
1   15
```

Field descriptions

Codec-set - Indicates which codec set is to be used between the two regions. If the two regions are not connected at all, this field is blank. When the codec set is blank, the **direct-WAN**, **WAN-BW-limits**, and **Intervening-regions** entry fields are not displayed. This field cannot be blank if this route through two regions is being used by some non-adjacent pair of regions.

Direct-WAN - Indicates whether the two regions (source and destination) are directly connected by a WAN link. The default value is **y** if the **codec-set** field is not blank. If so, the **WAN-BW-limits** field displays, but the **Intervening-regions** fields do not display. If the **direct-WAN** field is set to **n**, then the **WAN-BW-limits** field does not display, but the **Intervening-regions** fields are displayed.

WAN-BW-limits - The **WAN-BW-limits** field is divided into two parts, values and units.

- The value portion of the field allows entry of the bandwidth limits for direct WAN links. This field may be entered in the number of connections, bandwidth in Kbits/sec, bandwidth in Mbits/sec, or left blank. The default is blank.

  Note:

  For release 2.0, the number must be less than or equal to **65** when the units part of the field is set to **Mbits/sec**.

- The unit portion of the field allows entry of the units for the bandwidth limits for direct WAN links. This field may represent connections, Kbits/sec, Mbits/sec, or NoLimit.

Intervening-regions - Four fields allowing entry of up to four intervening region numbers between the two indirectly-connected regions.

Note:

Entry is not allowed for indirect region paths until all direct region paths have been entered. In addition, the order of the path through the regions must be specified starting from the source region to the destination region.

The **status ip-network-region *n*** command, where ***n*** is the network region you want to review, displays the modified **Inter Network Region Bandwidth Status** screen. This screen was modified to show statistics on the Call Admission Control-Bandwidth Limitation feature. The following two figures show two different command options.

The first command option (an existing option) is **status ip-network-region *n*** (Inter Network Region Bandwidth Status screen on page 155). Each line on the screen shows the connection that region ***n*** has to either a direct or indirect region. For the direct regions, the bandwidth and number of connections being used is shown in both the transmit and receive directions. For indirect regions, only the status of the connection is shown.

Note:

Regions not connected either directly or indirectly to region ***n*** are not shown.

Figure 55: Inter Network Region Bandwidth Status screen

```
status ip-network-region 2                                        Page 1 of 1
                    INTER NETWORK REGION BANDWIDTH STATUS

                                                                      #Times
Src Dst   Conn    Conn   BW-limits  BW-Used (Kbits)  #-of-Connections  BW-Limit
Rgn Rgn   Type    Stat                 Tx      Rx       Tx      Rx     Hit Today

  2   1  direct   pass   128 Kbits      0       0        0       0        0
  2   3  indirect pass
  2   4  indirect pass
  2   5  indirect pass
```

The second command option (a new option) is **status ip-network-region *n/m*** (Inter Network Region Bandwidth Status screen on page 156), where ***n*** and ***m*** are two separate and connected regions. Use this option for more details on the indirect regions. This command option shows all the bandwidth being used between region ***n*** and region ***m***, which in this example includes all the intermediate regions because region ***n*** and region ***m*** are indirectly connected.

Figure 56: Inter Network Region Bandwidth Status screen

```
status ip-network-region 2                                          Page 1 of 1
                    INTER NETWORK REGION BANDWIDTH STATUS


                                                                      #Times
Src Dst   Conn    Conn   BW-limits  BW-Used (Kbits)  #-of-Connections  BW-Limit
Rgn Rgn   Type    Stat                 Tx      Rx       Tx      Rx     Hit Today

  2   1  direct   pass   128 Kbits      0       0        0       0        0
  1   3  direct   pass   256 Kbits      0       0        0       0        0
```

Field descriptions

Src Rgn - Source region

Dst Rgn - Destination region

Conn Type - Connection type (direct or indirect)

Conn Stat - Connection status (pass or fail)

BW-limits - Bandwidth and limits as administered on the **IP Network Region** screen

BW-Used (Kbits) Tx - Transmit bandwidth used (for direct connections only)

BW-Used (Kbits) Rx - Receive bandwidth used (for direct connections only)

#-of-Connections Tx - Transmit connection count (for direct connections only)

#-of-Connections Rx - Receive connection count (for direct connections only)

#Times BW-Limit Hit Today - Daily count of how many times the CAC threshold limits have been reached (for direct connections only)

Note:

This log is cleared at midnight (server time).

IP-Options System Parameters screen

An additional option has been added to a field on the **IP-Options System Parameters** screen (IP-Options System Parameters screen on page 157). Use the **`change system-parameters ip-options`** command.

The additional option for the **Intra-System IP DTMF Transmission Mode** field is **rtp-payload**. The option **rtp-payload** allows for dual-tone multi-frequency (DTMF) signals, also known as touchtones, to be transmitted over SIP trunks.

When the **rtp-payload** option is applied to an IP connection, the VoIP audio resource (on TN2302 Medpros, or on G700 or G350 Media Gateways), is configured to implement RFC2833. RFC2833 is an internet standard for sending and receiving telephony events.

The VoIP resource detects speech on an internal bus. Normal speech is encoded according to the specified voice coder (for example, G711). The VoIP resources places the encoded audio into packets and identifies the audio packets with a well known payload type value.

When the other end receives the packets, based on this payload type value, the receiver knows the packets contain encoded audio and that the encoding was G711.

When the **rtp-payload** option is set, the VoIP resource not only detects speech, but it is also detecting DTMF tones. When a DTMF tone is detected, it is not encoded using the selected voice encoder. Instead, the VoIP resource produces a special packet with a special payload type. The special packet includes the dynamic payload type, the digit detected, duration, and volume. This packet is sent along in the same RTP stream as the encoded audio, but since it has a different payload type, the receiver handles it differently. The receiver regenerates a DTMF tone based on the data in the received packet.

Figure 57: IP-Options System Parameters screen

```
change system-parameters ip-options                                  Page 1

                         IP-OPTIONS SYSTEM PARAMETERS

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

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

IP DTMF TRANSMISSION MODE
      Intra-System IP DTMF Transmission Mode: rtp-payload
      Intra-System IP DTMF: See Signaling Group Forms

H.248 MEDIA GATEWAY                  H.323 IP ENDPOINT
 Link Loss Delay Timer (min): 5       Link Loss Delay Timer (min): 60
                                        Primary Search Time (sec): 75
```

List Trace screen

Previously, the G700 Media Gateway call controller did not provide packet loss and jitter statistics for IP telephones or trunks. The screens for displaying the information were available within Communication Manager, but were not populated with measurements obtained from the G700 VoIP engines.

With Communication Manager release 2.0, VoIP engine statistics are collected from the G700 Media Gateway, and displayed in a manner consistent with existing gateway reporting formats for other platforms. The commands used for this change are:

- **list trace station *n*** (List Trace screen on page 158)
- **list trace tac *n*** (List Trace screen on page 159)
- **status station *n*** (Station Status screen on page 160)
- **status trunk *n*** (Trunk Status screen on page 161)

In each of these commands, ***n*** is the variable for the specific component you want to review.

The **list trace station *n*** command displays call progress, as well as jitter and packet loss statistics, for a specified IP telephone (List Trace screen on page 158).

Figure 58: List Trace screen

```
list trace station 2152                                              Page 1
                                    LIST TRACE

time              data
10:02:43      active station      2152 cid 0xa2
10:02:43      G711MU ss:off ps:20 rn:1/1 135.9.78.43:62210 135.9.77.174:5736
10:02:46      dial 2301
10:02:46      ring station    2301 cid Oxa2
10:02:46      alert station    2301 cid Oxa2n
10:02:54      Jitter:0 0 0 0 0 0 0 0 0 0: Buff:8 UC:1 Avg:0
10:02:54      Pkloss:0 0 0 0 0 0 0 0 0 0: Oofo:0 UC:0 Avg:0
10:02:55      active station      2301 cid 0xa2
10:03:05      Jitter:0 0 0 0 0 0 0 0 0 0: Buff:8 UC:1 Avg:0
10:03:05      Pkloss:0 0 0 0 0 0 0 0 0 0: Oofo:0 UC:0 Avg:0
10:03:15      Jitter:0 0 0 0 0 0 0 0 0 0: Buff:8 UC:1 Avg:0
10:03:15      Pkloss:0 0 0 0 0 0 0 0 0 0: Oofo:0 UC:0 Avg:0
10:03:25      Jitter:0 0 0 0 0 0 0 0 0 0: Buff:8 UC:1 Avg:0
10:03:25      Pkloss:0 0 0 0 0 0 0 0 0 0: Oofo:0 UC:0 Avg:0
10:03:35      Jitter:0 0 0 0 0 0 0 0 0 0: Buff:8 UC:1 Avg:0

 press CANCEL to quit -- press NEXT PAGE to continue.
```

The **list trace tac *n*** command displays call progress, as well as jitter and packet loss statistics, for a specified IP trunk (List Trace screen on page 159).

Figure 59: List Trace screen

```
list trace tac 415                                                    Page 1
                                   LIST TRACE

time              data
10:05:32      dial 95676002
10:05:32      route-pattern  15 preference 1  cid 0xa3
10:05:32      seize trunk-group 15 member 3  cid 0xa3
10:05:32      Setup digits 6002
10:05:32      Calling Number & Name NO-CPNumber NO-CPName
10:05:32      Proceed trunk-group 15 member 3  cid 0xa3
10:05:33      Alert trunk-group 15 member 3  cid 0xa3
10:05:33      G711MU ss:off ps:20 rn:1/1 135.9.78.41:30588 135.9.77.174:5804
10:05:42      active trunk-group 15 member 3  cid 0xa3
10:05:43      Jitter:0 0 0 0 0 0 0 0 0 0: Oofo:0 UC:0 Avg:0
10:05:43      Pkloss:0 0 0 0 0 0 0 0 0 0: Oofo:0 UC:0 Avg:0
10:05:54      Jitter:0 0 0 0 0 0 0 0 0 0: Buff:8 UC:0 Avg:0
10:05:54      Pkloss:0 0 0 0 0 0 0 0 0 0: Oofo:0 UC:0 Avg:0
10:06:04      Jitter:0 0 0 0 0 0 0 0 0 0: Buff:8 UC:0 Avg:0
10:06:04      Pkloss:0 0 0 0 0 0 0 0 0 0: Oofo:0 UC:0 Avg:0

 press CANCEL to quit -- press NEXT PAGE to continue.
```

The **`status station`** ***n*** command displays loss statistics for a specified IP telephone (Station Status screen on page 160).

Figure 60: Station Status screen

```
status station 2152                                                Page 4
                                STATION STATUS

NETWORK STATUS
      Average Jitter (ns)              Packet Loss per Second
       Last Ten Seconds                  Last Ten Seconds
       # - more than 255ns               x - 100% loss

             0                                  0          Per Call Info
             0                                  0
             0                                  0     Out of Order Counter: 0
             0                                  0     SSRC Change for Call: 0
             0                                  0       Last Rx Sequence #: 43394
             0                                  0       Last Tx Sequence #: 62421
             0                                  0
             0                                  0
             0                                  0
             0                                  0

SUMMARY
Worst Case this Call (ns): 1         Worst Case this Call: 1
   Average this Call (ns): 0            Average this Call: 0
 Current Buffer Size (ns): 9
```

The **`status trunk`** ***n*** command displays jitter and loss statistics for a specified IP trunk (Trunk Status screen on page 161).

Figure 61: Trunk Status screen

```
status trunk 1573                                                    Page 2
                                  TRUNK STATUS

NETWORK STATUS
      Average Jitter (ns)            Packet Loss per Second
       Last Ten Seconds                Last Ten Seconds
       # - more than 255ns              x - 100% loss

             0                                  0          Per Call Info
             0                                  0
             0                                  0     Out of Order Counter: 0
             0                                  0     SSRC Change for Call: 0
             0                                  0       Last Rx Sequence #: 43394
             0                                  0       Last Tx Sequence #: 62421
             0                                  0
             0                                  0
             0                                  0
             0                                  0

SUMMARY
Worst Case this Call (ns): 1         Worst Case this Call: 1
   Average this Call (ns): 0            Average this Call: 0
 Current Buffer Size (ns): 9
```

Locations screen

Three new columns are added to the **Locations** screen (Locations screen, page 1 on page 162):

- **ARS FAC** field
- **Attd FAC** field
- **Prefix** field

Note:

These three columns only appear if the **Multiple Locations** field on the third page of the **Optional Features** screen is set to **y**. Otherwise, the three columns and the column headers do not appear.

This change is prompted by the Multi-Location Dial Plan feature.

Figure 62: Locations screen, page 1

```
change locations                                              Page 1 of 1
                                    LOCATIONS

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

 Loc. Name          Timezone   Rule     NPA   ARS   Attd          Pre-   Foreign
 No                  Offset                   FAC   FAC           fix    Rte pat
 1:   Main          + 00:00    0
 2:   _____________ _ __:__    __       ___   ____   __           _____  _______
 3:   _____________ _ __:__    __       ___   ____   __           _____  _______
 4:   _____________ _ __:__    __       ___   ____   __           _____  _______
 5:   _____________ _ __:__    __       ___   ____   __           _____  _______
 6:   _____________ _ __:__    __       ___   ____   __           _____  _______
 7:   _____________ _ __:__    __       ___   ____   __           _____  _______
 8:   _____________ _ __:__    __       ___   ____   __           _____  _______
 9:   _____________ _ __:__    __       ___   ____   __           _____  _______
10:   _____________ _ __:__    __       ___   ____   __           _____  _______
11:   _____________ _ __:__    __       ___   ____   __           _____  _______
12:   _____________ _ __:__    __       ___   ____   __           _____  _______
13:   _____________ _ __:__    __       ___   ____   __           _____  _______
14:   _____________ _ __:__    __       ___   ____   __           _____  _______
```

The following applies for all fields:

- If the **Multiple Locations** field on the **Optional Features** screen is set to **y**, 10, 50, or 250 rows appear where data can be entered.
- If the **Multiple Locations** field on the **Optional Features** screen is set to **n**, only one row appears where data can be entered.

ARS FAC - The **ARS FAC** field is controlled by the **Multiple Locations** field on the **Optional Features** screen (use the **`display system-parameters customer-options`** command). Administration of this field must follow the same rules that exist for administering an ARS code on the **Feature Access Code (FAC)** screen.

Valid entries	Usage
0 to 9	Any valid FAC format is acceptable, up to four digits. Characters ***** or # are permitted, but only in the first position. Many locations are expected to share the same access code.

Attd FAC - The **Attd FAC** field is controlled by the **Multiple Locations** field on the **Optional Features** screen (use the **display system-parameters customer-options** command). Administration of this field must be a **Call Type** of **FAC/DAC** on the **Dial Plan Analysis Table** screen for first digit **0**-**9**.

Note:

Within a dial plan, **FAC/DAC** codes and extensions cannot both start with the same first digits.Either the **FAC/DAC** entries or the block of extensions must be changed to have a different first digit.

A user cannot administer an **Attd FAC** unless an **Attendant Access Code** has first been administered on either the **Dial Plan Analysis Table** screen or the **Feature Access Code (FAC)** screen.

Valid entries	Usage
0 to **9**	Values up to two digits are permitted. Characters ***** or # are not permitted. Many locations are expected to share the same access code.

Prefix - The **Prefix** field is used to prepend the leading digits for **Uniform Dial Plan Table** screen entries for calls that match the **Uniform Dial Plan Table** entry. This field is controlled by the **Multiple Locations** field on the **Optional Features** screen (use the **display system-parameters customer-options** command).

Valid entries	Usage
0 to 9	Values from one to five digits (0-99999) are permitted.

Optional Features screen

Before you can administer Extension to Cellular/Off-PBX Station (OPS) extensions, certain settings must be enabled for your system, as determined by the installed license file. These settings are on the **Optional Features** screen. This change is prompted by enhancements to the Extension to Cellular feature.

To make sure the system is set up to administer Extension to Cellular/OPS extensions:

1. Type **display system-parameters customer-options**. Press **Enter**.

   The system displays the **Optional Features** screen (Optional Features screen, page 1 on page 164).

Figure 63: Optional Features screen, page 1

```
display system-parameters customer-options                    Page 1 of 10

                                OPTIONAL FEATURES

G3 Version: V12                              RFA System ID (SID): 123456789012
  Location: 2                                RFA Module ID (MID): 123456
  Platform: 2
                                                             USED
                                       Maximum Ports: 300    174
                                Maximum XMOBILE Stations: 30     28
                      Maximum Off-PBX Telephones - EC500: 1200   0
                      Maximum Off-PBX Telephones -   OPS: 1200   0
                      Maximum Off-PBX Telephones - SCCAN: 0      0



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

The following settings must be enabled for your system, as determined by the installed license file.

On page 1 of the **Optional Features** screen:

- the **G3 Version** field must be set to **V12** or greater.
- either the **Maximum Off-PBX Telephones - EC500** field, or the **Maximum Off-PBX Telephones - OPS** field must be greater than zero. Either or both of these fields must be set to the number of telephones that are to be used for Extension to Cellular/OPS.

  Note:

  The **Maximum Off-PBX Telephones - SCCAN** field is not used at this time.

Field descriptions

Maximum Off-PBX Telephones - EC500 - The **Maximum Off-PBX Telephones - EC500** field is a new field with release 2.0 having following parameters:

Valid entries	Usage
0 to system limit	Default = 0. Type a number between **1**-**99999**. The "system limit" is defined as follows: • On DEFINITY® systems, the upper limit is 1/2 of the maximum number of administrable telephones. • On S8300, S8500, and S8700 systems, the upper limit is the maximum number of administrable telephones. Telephones that are administered for any Extension to Cellular/OPS application count against this limit.

To be usable, the system must also have the **IP Trunks, ISDN-BRI Trunks**, or **ISDN-PRI** field enabled. Those fields are on page 4 of the **Optional Features** screen.

Maximum Off-PBX Telephones - OPS - The **Maximum Off-PBX Telephones - OPS** field is a new field with release 2.0 having following parameters:

Valid entries	Usage
0 to license max	Default = 0. Type a number between **1**-**99999**. The "license max' is defined as follows: • On legacy systems, the upper limit is 1/2 of the maximum number of administrable telephones. • On S8300, S8500, and S8700 systems, the upper limit is the maximum number of administrable telephones. Telephones that are administered for any Extension to Cellular/OPS application count against this limit.

To be usable, the system must also have the **IP Trunks, ISDN-BRI Trunks**, or **ISDN-PRI** field enabled. Those fields are on page 4 of the **Optional Features** screen.

Registered IP Stations screen

The **Registered IP Stations** screen (Registered IP Stations screen on page 166) has been modified, based on changes to the **`list registered-ip-stations`** command. (For more information on the changes to the command, see list registered-ip-stations on page 188.)

The screen has been reformatted, and the following new fields were added:

- **Station Type**
- **Product ID**
- **Product Release**
- **Stations IP Address/Port**
- **Network Region**

Figure 64: Registered IP Stations screen

```
list registered-ip-stations gatekeeper-address 135.9.49.156

                              REGISTERED IP STATIONS

Command Options: gatekeeper-address 135.9.49.156

Station  Station  Product      Product   Stations IP        Network     Original
Ext      Type     ID           Release   address/port       Region      Port

3030     4624     IP_Phone     1.700     135.9.44.56           1
3031     4624     IP_Soft      1.800     135.9.44.56           1
3032     6408D+   IP_Soft      1.800     135.9.44.57           2        1E0303
3033     console  IP_eCons     1.500     135.9.44.57           2
3034     606A1    IP_Agent     1.800     135.9.44.57           2
3035     8410D    IP_ROMax     1.100     135.9.44.58           3
```

Signaling Group screen

An additional option has been added to a field on the **Signaling Group** screen (Signaling Group screen, page 1 on page 167). Use the **`change signaling-group`** ***n*** command, where ***n*** is the number of the signaling group you want to change. The additional option for the **DTMF Over IP** field is **rtp-payload**. The option **rtp-payload** allows for dual-tone multi-frequency (DTMF) signals, otherwise known as touchtones, to be transmitted over SIP trunks.

For more information on how this option works, see IP-Options System Parameters screen on page 156.

Figure 65: Signaling Group screen, page 1

```
change signaling-group 1                                        Page 1 of 5

                                SIGNALING GROUP

Group Number: 1              Group Type: h.323
                           Remote Office? n              Max number of NCA TSC: 0
                                     SBS? n               Max number of CA TSC: 0
                                                        Trunk Group for NCA TSC:
       Trunk Group for Channel Selection: 1
          Supplementary Service Protocol: a             Network Call Transfer: n

        Near-end Node Name: clan1b09            Far-end Node Name: Newclan1c20
      Near-end Listen Port: 1720              Far-end Listen Port: 1720
                                           Far-end Network Region:
              LRQ Required? n             Calls Share IP Signaling Connection? n
              RRQ Required? n
                                             Bypass If IP Threshold Exceeded? n

              DTMF over IP: rtp-payload        Direct IP-IP Audio Connections? y
                                                         IP Audio Hairpinning? y
                                          Interworking Message: PROGress
```

Station screen

On the **Station** screen (Station screen, page 3 on page 168), the field **IP Emergency Calls** in earlier releases of Communication Manager has been renamed to **Remote Softphone Emergency Calls** in release 2.0. This newly-renamed field also allows a new value, **as-on-local**. The value **extension** is no longer allowed for this field. Use the **change `station` *n*** command, where ***n*** is the number of the telephone.

This field only appears if the **IP Softphone** field in the **Station** screen is set to **y**. The restriction (current in previous releases of Communication Manager) that this field can only be changed if the telephone is unregistered remains in force for release 2.0. This change is prompted by the E911 emergency location information number (ELIN) for wired IP feature.

Figure 66: Station screen, page 3

```
change station 1001                                              Page 3 of 5
                                     STATION

            IP Audio Hairpinning? y
  Direct IP-IP Audio Connections? y

EMERGENCY CALL HANDLING
Remote Softphone Emergency Calls: as-on-local
          Emergency Location Ext: 1001
```

Note:

The fields are not accessible if the set type is not one of the IP telephone or IP softphone types.

Field descriptions

Remote Softphone Emergency Calls - This field has been renamed. In earlier releases of Communication Manager, this field was named **IP Emergency Calls**.

Valid entries	Usage
as-on-local	Type **as-on-local** to achieve the following results: • If the administrator chooses not to use the new feature outlined in the next bullet item and chooses to leave the **Emergency Location Extension** fields (that correspond to this telephone's IP address) on the **IP Address Mapping** screen blank, the value **as-on-local** sends the extension entered in the **Emergency Location Extension** field in the **Station** screen to the Public Safety Answering Point (PSAP). • If the administrator does choose to use the new feature and populates the **IP Address Mapping** screen with emergency numbers, the value **as-on-local** functions as follows: - If the **Emergency Location Extension** field in the **Station** screen is the same as the **Emergency Location Extension** field in the **IP Address Mapping** screen, the value **as-on-local** sends the extension to the Public Safety Answering Point (PSAP). - If the **Emergency Location Extension** field in the **Station** screen is different from the **Emergency Location Extension** field in the **IP Address Mapping** screen, the value **as-on-local** sends the extension in the **IP Address Mapping** screen to the Public Safety Answering Point (PSAP).

Valid entries	Usage
block	Type **block** to prevent the completion of emergency calls. Use this entry for users who move around but always have a circuit-switched telephone nearby, and for users who are farther away from the media server or system than an adjacent area code served by the same 911 Tandem office. When users attempt to dial an emergency call from an IP telephone and the call is blocked, they can dial 911 from a nearby circuit-switched telephone instead.
cesid	Type **cesid** to allow Communication Manager to send the CESID information supplied by the IP softphone to the PSAP. The end user enters the emergency information into the IP softphone. Use this entry for IP softphones with Road Warrior service that are near enough to the media server or system that an emergency call routed over the trunk reaches the PSAP that covers the server or system. If the media server or system uses ISDN trunks for emergency calls, the digit string is the telephone number, provided that the number is a local direct-dial number with the local area code, at the physical location of the IP softphone. If the media server or system uses CAMA trunks for emergency calls, the end user enters a specific digit string for each IP softphone location, based on advice from the local emergency response personnel.
option	Type **option** to allow the user to select the option (**as-on-local**, **block**, or **cesid**) that the user selected during registration and the IP softphone reported. Use this entry for extensions that may be switched back and forth between IP softphones and a telephone with a fixed location. The user chooses between **as-on-local**, **block** and **cesid** on the softphone. A DCP telephone in the office use the **Emergency Location Extension** field in the **Station** screen. During registration, users and administrators see the following choices on the IP softphone user interface: **This is the softphone interface equivalent to as-on-local:** The box "Use the following information to identify your location to a PSAP should you need to make a 911 call: your extension number" is checked. **This is the softphone interface equivalent to block:** The box "Enable Emergency Call Handling Feature" is not checked. **This is the softphone interface equivalent to cesid:** The box "Use the following information to identify your location to a PSAP should you need to make a 911 call: telephone number _____" has a telephone number entered.

Station screen (for NI-BRI)

A new telephone type, **NI-BRI**, has been added to the **Station** screen. (For more information on NI-BRI, see National ISDN (NI-1 and NI-2) BRI voice endpoint support on page 61.) Use the **`change station`** ***n*** command, where ***n*** is the number of the telephone.

When the **NI-BRI** telephone type is selected, the remaining fields on the **Station** screen reflect only those fields that are relevant to NI-BRI (Station screen, page 1 on page 170).

Figure 67: Station screen, page 1

```
add station next                                              Page 1 of 3
                                    STATION

Extension: 22878                        Lock Message: n             BCC: 0
     Type: NI-BRI                       Security Code:               TN: 1
     Port:                            Coverage Path 1:              COR: 1
     Name:                            Coverage Path 2:              COS: 1
                                      Hunt-to Station:

STATION OPTIONS
              Loss Group: 3
                                                     Message Lamp Ext: 22878

       Display Language: english
                  Model: other



BRI OPTIONS
                XID? n       Fixed TEI? n
                           Endpt Init? y     SPID: 22878         Endpt ID: 01
```

Click **Next** to go to the next screen (Station screen, page 2 on page 171).

Figure 68: Station screen, page 2

```
add station next                                              Page 2 of 3
                                    STATION

FEATURE OPTIONS
           LWC Reception: spe
          LWC Activation? y                  Coverage Message Retrieval? y
  LWC Log External Calls? n
            CDR Privacy? n
   Redirect Notification? y

                                                Restrict Last Appearance? y

                                        Per Station CPN - Send Calling Number?


    MWI Served User Type:
              AUDIX Name:
                                               Coverage After Forwarding? y
```

Click **Next** to go to the next screen (Station screen, page 3 on page 171).

Figure 69: Station screen, page 3

```
add station next                                              Page 3 of 3
                                    STATION

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



ABBREVIATED DIALING
     List1:                     List2:                        List3

BUTTON ASSIGNMENTS
 1: call-appr                            6:
 2: call-appr                            7:
 3: call-appr                            8:
 4:                                      9:
 5:                                     10:
```

Station Status screen

Two new fields, **Product ID and Release** and **Native NAT Address**, are added to the third page of the **Station Status** screen, **Call Control Signaling** (Call Control Signaling screen, page 3 on page 172). Use the **`status station`** ***n*** command, where ***n*** is the telephone number.

Figure 70: Call Control Signaling screen, page 3

```
status station 3032                                          Page 3 of 3
                              CALL CONTROL SIGNALING

                   Switch              IP                        IP
                   Port      Switch-End Addr:Port         Set-End Addr:Port
     IP Signaling: 01E0617   172. 28.208. 21 :1720        172. 28. 3. 77:1673
            H.245:
        Node Name:           clan
   Network Region:           1                            1
                                   AUDIO CHANNEL
                   Switch              IP                        IP
                   Port      Switch-End Addr:Port         Set-End Addr:Port
           Audio:
        Node Name:
   Network Region:
    Audio Connection Type: ip-tdm
   Product ID and Release: IP_Phone 1.700
  H.245 Tunneled in Q.931? does not apply
      Registration Status: registered-authenticated
    MAC Address: 00:60:1d:24:47:38                 Native NAT Address: 10.0.0.1
```

Field descriptions

Product ID and Release - A ten-character field containing the product identifier of the endpoint that is registered with the associated extension, plus a five-character field, in the format **9.999**, that contains the release number of the endpoint as it provided to the gatekeeper upon registration.

Native NAT Address - A fifteen-character field, in the format **999.999.999.999**, that specifies the NAT IP address of the endpoint when a network device is providing the Network Address Translation function on behalf of the endpoint. The endpoint's NAT address is provided to the gatekeeper upon registration.

Also see Station Status screen on page 160.

Trunk Status screen

See Trunk Status screen on page 161.

System Capacity screen

A new field, **Meet-me Conference vectors per system**, has been added on the third page of the **System Capacity** screen (System Capacity screen, page 3 on page 173). Use the **`display capacity`** command. On the **System Capacity** screen, the system displays:

- meet-me conferencing vectors that are used
- meet-me conferencing vectors that are available
- the system limit for meet-me conferencing vectors

Also, the group heading on page 10 of the **System Capacity** screen (not shown) is changed to **Concurrent Registration Counts**.

Figure 71: System Capacity screen, page 3

```
display capacity                                              Page 3 of 12
                                SYSTEM CAPACITY

                                                                    System
                                                  Used Available    Limit
                                                  ----------------------

                    CALL COVERAGE
                            Coverage Answer Groups:    0    1000      1000
                                    Coverage Paths:    0    9999      9999

                                Call Pickup Groups:    0    5000      5000

                                      Call Records:    -       -     15424

              CALL VECTORING/CALL PROMPTING
                       Total Vector Directory Numbers:    0   20000     20000
                  Meet-me Conference VDNs per system:    0    1800      1800
                             Total Vectors per system:    0     999       999
                Meet-me Conference vectors per system:    0     999       999
           BSR Application-Location Pairs per system:    0    2560      2560
```

Uniform Dial Plan Table screen

A new value, **L*x*** (where ***x*** indicates a number of digits), is allowed in the **Insert Digits** field in the **Uniform Dial Plan Table** screen (Uniform Dial Plan Table screen, page 1 on page 174). Use the **change uniform-dialplan *n*** command, where ***n*** is the number of the dial plan. This change is prompted by the Multi-Location Dial Plan feature.

Figure 72: Uniform Dial Plan Table screen, page 1

```
change uniform-dialplan 3                                        Page 1 of 2
                            UNIFORM DIAL PLAN TABLE

                                                                 Percent Full: 0

  Matching          Insert          Node    Matching          Insert          Nod
e
  Pattern   Len Del Digits Net Conv Num    Pattern   Len Del Digits Net Conv Num
  3          3   0  L1     ext  y                                        n
  5          5   1  005    aar  y                                        n
  538        7   0         aar  y                                        n
  6          5   1  006    aar  y                                        n
  852        7   0         aar  y                                        n
                           n                                            n
                           n                                            n
                           n                                            n
                           n                                            n
                           n                                            n
                           n                                            n
                           n                                            n
                           n                                            n
                           n                                            n
                           n                                            n
                           n                                            n
```

The new value **L*x*** represents taking the location prefix from the **Locations** screen, and prepending the leading ***x*** digits to the dialed string. The value ***x*** on the **Uniform Dial Plan Table** screen must match the number of digits in the location prefix.

Use of this new value requires the **Multiple Locations** field to first be set to **y** on the **Optional Features** screen.

Field descriptions

Insert Digits - The variable ***x*** in the value **L*x*** in the **Insert Digits** field is only valid when the **Call Type** on the **Dial Plan Analysis Table** screen (the **Net** field on the **Uniform Dial Plan Table** screen) is **ext**.

Valid entries	Usage
1 to 5	Type a number between 1 and 5 that represents the number of digits that should be prepended to (added to the front of) the dialed string. The number of digits should be equal to or less than the number of digits of the location prefix.

Chapter 4: New and changed commands

This chapter displays the new and changed commands for Avaya Communication Manager.

Release 2.2 new commands

Avaya Communication Manager, release 2.2, includes no new commands.

Release 2.2 changed commands

Avaya Communication Manager, release 2.2, includes no changed commands.

Release 2.1 new commands

Avaya Communication Manager, release 2.1, includes the following new commands.

busyout board

The command **busyout board** is now available for Asynchronous Transfer Mode (ATM) interface circuit packs (TN2305 or TN2306).

location-parameters

The Multinational Locations feature introduces a new command, **location-parameters *n***, where ***n*** is a number between 1 and 25. This command displays a new set of screens, beginning with the **Location Parameters** screen.

Valid parameters

Action	Object	Qualifier
change	**location-parameters**	***n***

See the section beginning with the Location Parameters screens on page 90 for information on the four pages of this new screen.

multifrequency-signaling

The Multinational Locations feature introduces a new command, **multifrequency-signaling *n***, where ***n*** is a number between 1 and 25. This command displays a new set of screens, beginning with the **Multifrequency-Signaling-Related Parameters** screen.

Valid parameters

Action	Object	Qualifier
change	**multifrequency-signaling**	***n***

See the section beginning with the Multifrequency-Signaling-Related Parameters screen on page 94 for information on the three pages of this new screen.

tandem-calling-party-num

The Avaya Extension to Cellular/OPS feature introduces a new command, **tandem-calling-party-num**. This command displays a new screen, the **Calling Party Number Conversion for Tandem Calls** screen.

Valid parameters

Action	Object	Qualifier
change	**tandem-calling-party-num**	
display	**tandem-calling-party-num**	

See Calling Party Number Conversion for Tandem Calls screen on page 89 for information on this new screen.

terminal-parameters

The Multinational Locations feature introduces a new command, **change terminal-parameters *n***, where ***n*** is a number between 1 and 25. This command displays a new set of screens, beginning with the **302/603/606-Type Terminal Parameters** screen.

Valid parameters

Action	Object	Qualifier
change	**terminal-parameters**	***n***

See the section beginning with the 302/603/606-Type Terminal Parameters, page 1 on page 99 for information on the two pages of this new screen.

tone-generation

The Multinational Locations feature introduces a new command, **change tone-generation *n***, where ***n*** is a number between 1 and 25. This command displays a new set of screens, beginning with the **Tone Generation** screen.

Valid parameters

Action	Object	Qualifier
change	**tone-generation**	***n***

See the section beginning with the Tone Generation screens on page 100 for information on the two pages of this new screen.

trace media-gateway

The new command **list trace media-gateway <*identifier* | *ip-address*>** enables you to trace the following gateway registration messages:

- Service Change Request
- Service Change Reply
- Keep Alive

You can trace the registration of a media gateway in one of two ways:

- Use **list trace media-gateway identifier *n***, where ***n*** is the identification number of the media gateway.
- Use **list trace media-gateway ip-address *n***, where ***n*** is the IP address of the media gateway.

Valid parameters

Action	Object	Qualifier
list	**trace media-gateway identifier**	***n***
list	**trace media-gateway ip-address**	***n***

Release 2.1 changed commands

Avaya Communication Manager, release 2.1, includes no changed commands.

Release 2.0 new commands

Avaya Communication Manager, release 2.0, includes the following new commands.

extension-station

The Multi-Location Dial Plan feature introduces a new command, **extension-station *n***, where ***n*** is a valid telephone extension number to be changed. This command allows an administrator to change a station extension on the system without removing the station then adding it back.

Valid parameters

Action	Object	Qualifier
change	**extension-station**	***n***

CAUTION:

The **change extension-station *n*** command changes most instances of an extension as it appears in the system. However, if an extension is used as an **emergency location extension** on the **Station** screen or the **IP Address Mapping** screen, the change is blocked.

When you use the **change extension-station *n*** command, the system displays a new screen, the **Change Station Extension** screen. See Change Station Extension screen on page 114 for information on this new screen.

G650 Media Gateway

The addition of the new G650 Media Gateway, with the new TN2312BP IP Server Interface (IPSI) circuit pack, and the new 655A power supply, has produced numerous new or changed commands. The new and changed commands are:

- **add cabinet**
- **add fiber-link**
- **add/change/list ipserver-interface**
- **change circuit-packs**
- **change system-parameters duplication**
- **display system-parameters customer-options**
- **get power-shutdown**
- **list configuration hardware-group**
- **list configuration power-supply**
- **list registered-ip-stations**
- **recycle carrier**
- **set emergency-xfr**
- **status environment**
- **test customer-alarm**
- **test environment**

The many commands and accompanying screens relating to the G650 are not shown in this document. They are described in the *Maintenance Commands Reference*, 555-245-101.

ip-interface

The new **list ip-interface <*all* | *clan*>** command displays the **IP Interfaces** screen. This new screen lists information about the IP interfaces administered on the system.

- When the ***all*** option is used, all the administered IP interfaces are listed showing the **Type** field and not showing the **Num Skts Warn** field.
- When the ***clan*** option is used, all the administered C-LANs are listed showing the new **Num Skts Warn** field and not showing the **Type** field.

Valid parameters

Action	Object	Qualifier
change	**ip-interface**	
display	**ip-interface**	
list	**ip-interface**	***all*** or ***clan***

The IP interface types depend on the media server.

- **C-LAN**, **MEDPRO**, and **VAL** types for the S8700 and S8500 Media Servers
- **PROCR** type for the S8300 Media Server

The new **list ip-interface** command is identical to the current **display ip-interfaces** command. The new **change/display ip-interface** command is changed for Communication Manager release 2.0 as described in Changed Commands/ Screens.

See IP Interfaces screen on page 120 for information on this new screen and its function.

multi-media ip-unregistered

A new option, **ip-unregistered**, has been added to the existing **list multi-media** command. This command shows a list of all unregistered IP telephones. This new option allows an administrator to quickly identify what IP telephones are unregistered and to resolve any related network problems.

Note:

This new command option does not list IP Softphones that are unregistered, since in most instances, the end-user has purposely unregistered their IP softphones to regain control back at their office telephone set.

Valid parameters

Action	Object	Qualifier
`list`	`multi-media ip-unregistered`	

off-pbx-telephone feature-name-extensions

The Extension to Cellular feature introduces a new command, **`off-pbx-telephone feature-name-extensions`**.

Valid parameters

Action	Object	Qualifier
`change`	`off-pbx-telephone feature-name-extensions`	
`display`	`off-pbx-telephone feature-name-extensions`	

This command displays a new screen, the **Extensions to Call which Activate Features By Name** screen. See Extensions to Call which Activate Features By Name screen on page 119 for information on this new screen and its function.

off-pbx-telephone station-mapping

The Extension to Cellular feature introduces a new command, **`off-pbx-telephone station-mapping`**. This command displays a new screen, the **Stations with Off-PBX Telephone Integration** screen.

Valid parameters

Action	Object	Qualifier
`add`	`off-pbx-telephone station-mapping`	
`change`	`off-pbx-telephone station-mapping`	
`display`	`off-pbx-telephone station-mapping`	

Action	Object	Qualifier
list	**off-pbx-telephone station-mapping**	
status	**off-pbx-telephone station-mapping**	

In prior releases of Extension to Cellular, cell phones had to be administered as XMOBILE stations. If there were two line appearances allowed on your cell phone (for example, if Call Waiting was a feature that was supported on your cell phone), two separate XMOBILE station settings had to be administered.

With Communication Manager release 2.0, this is no longer needed. See Stations with Off-PBX Telephone Integration screen, page 1 on page 123 for information on this new screen and its function.

reset ip-stations

Use the **reset ip-stations** command to simultaneously reset all IP endpoints on a system, or a certain group of IP stations. You can limit the reset to only IP telephones, to IP telephones in a specific network region, or to all IP endpoints in a specific network region.

Use **reset ip-stations** to reset H.323 stations including:

- IP telephones
- IP Softphones
- IP Agents
- IP E-consoles
- All endpoints that appear as IP stations to Communication Manager, including stations on R300 Remote Office and stations on G350 Media Gateways

Valid parameters

Action	Object	Qualifier
reset	**ip-stations**	***<ip-phones | all-ip>*** and ***<ip-network-region (1-250) | all-regions>***

Use **reset ip-stations** to initiate simultaneous firmware upgrades to many IP stations, or a certain group of IP stations. You can reset IP stations on one IP network region to prevent overloading a system with large numbers of IP station resets.

When **reset ip-stations** is submitted, each IP station receives a reset message and is unregistered. When **reset ip-stations** is run, a new event is logged. See the Events Report screen on page 118 for information on this screen and its function.

status clan-usage

The new **status clan-usage** command displays the **IP Interfaces** screen.

Valid parameters

Action	Object	Qualifier
status	**clan-usage**	

See CLAN (TN799x) Socket Usage screen on page 117 for information on this new screen and its function.

status ip-network-region

The **status ip-network-region** command has a new option: ***n*** or ***m***, where ***n*** and ***m*** are two separate and connected regions.

Valid parameters

Action	Object	Qualifier
status	**ip-network-region**	***n*** or ***m***

See IP Network Region screen on page 152 for more information.

status media-processor

The new **status media-processor <*cabinet/carrier/slot*>** command displays a new screen showing the busyout status of the specified MedPro or IPMedPro media processor board. This command displays a new screen, the **IP Interface Status** screen.

Valid parameters

Action	Object	Qualifier
status	**media-processor**	***<cabinet/carrier/slot>***

See IP Interface Status screen on page 122 for information on this new screen and its function.

test media-gateway

A new command, **test media-gateway *n***, where ***n*** is the number of a media gateway that you want to test. This command allows customers to run an H248 link audit. The H248 link audit might be necessary if, for instance, there is an alarm against a media gateway for being unregistered, even though the media gateway is registered. For another example, the **status media-gateway** and **list media-gateway** commands might show that a media gateway is unregistered, when it is registered and processing telephone calls.

These conflicts can arise if there has been a server interchange while a media gateway is registering or un-registering, because it is possible for an inter-process message to become lost.

Valid parameters

Action	Object	Qualifier
list	**media-gateway**	
status	**media-gateway**	
test	**media-gateway**	***n***

The **test media-gateway *n*** command has one test:

Test #1527 - Link Audit. This test verifies that the link states between various system processes are consistent, and clears up any erroneous alarms.

Two symptoms of a problem can be resolved by this test:

- A server interchange or other system operation occurs that results in a registration alarm for a media gateway, although the media gateway is registered and functioning properly
- The **Display Events** screen shows that a media gateway is trying to register, but is being denied access (usually the result of a lost message because of abnormal server operation)

The test result is always PASS. Therefore, there are no error codes associated with the test.

variables

The Variables for Vectors feature introduces two new commands, **change variables** and **display variables**. The **change variables** command allows an administrator to define variables to be used in vector steps for call vectoring. The **display variables** command displays a list of already defined variables.

Valid parameters

Action	Object	Qualifier
change	**variables**	
display	**variables**	

When you use the **change variables** command, a new screen, the **Variables For Vectors** screen, appears. See Variables for Vectors screen on page 130 for information on this new screen.

Release 2.0 changed commands

Avaya Communication Manager, release 2.0, includes the following changed commands.

add/remove ip-interface

The existing **change | display ip-interface** command is changed to include the **add** and **remove** actions, and a specification of a single IP interface circuit pack location. The full command syntax is **add | change | remove | display ip-interface <*cabinet/carrier/slot* | *procr*>**.

- For the S8700 and S8500 Media Servers, you must specify the slot location of a C-LAN, Medpro, or VAL circuit pack.
- For the S8300 Media Server, **procr** is the only valid argument. In this case, the IP interface is embedded in the S8300 processor.

See IP Interfaces screen on page 150 for information on this new screen and its function.

add station next

The command **add station next** ignores the new entries in the **Uniform Dial Plan Table** screen when calculating the next extension number to use. This is consistent with the **Uniform Dial Plan Table** screen and the **add station next** command today. The **add station next** command ignores entries in the **Uniform Dial Plan Table** screen if the type is other than **ext**.

For example, if the dial plan has an entry for leading digit **7**, length **5**, as an extension (**ext**), and the **Uniform Dial Plan Table** screen has an entry for matching pattern **72**, length **5**, as **aar**, the **add station next** command skips all instances of 72000-72999 as valid extensions that can be used.

Note:

If someone explicitly entered an extension, say **72111**, the **add station next** command allows it. The same is true for the new **Uniform Dial Plan Table** screen entry.

campon-busyout media-processor

A new object key word **media-processor** has been added to the **campon-busyout** command. The syntax is now **campon-busyout media-processor <*cabinet/carrier/slot*>**. The command produces a **Command Results** report that shows the port address, the maintenance object name, any alternate name for the maintenance object, and any result and error codes.

list registered-ip-stations

Four new options have been added to the **list registered-ip-stations** command that enhance the sorting capabilities of the command, including the ability to sort by network region. A new field, **Command Options**, has been added to the **Registered IP Stations** screen that repeats the qualifiers specified after the **list registered-ip-stations** command. See Registered IP Stations screen on page 166 for information on this new screen and its function.

Using the options allows you to see only the extensions that have the attribute you specify:

- **list registered-ip-stations gatekeeper-address *xxx.xxx.xxx.xxx***. This option lists the CLAN's or processor's IP address.
- **list registered-ip-stations network-region *xx***. This option lists the network region of the extension.

- **`list registered-ip-stations product-id xxxxxx`**. This option lists the product type that is registered to the extension. For example, if a softphone is registered to a hardphone's extension, this command displays the release information of the registered endpoint. The **Product Release** field is the release information passed from the endpoint during registration. It contains one major character (***x***) and three minor characters (***y***): ***x.yyy***.
- **`list registered-ip-stations station-type xxxxxx`**. This option lists the administered set type. This is needed since the firmware loads may be different between IP telephone types.

list usage

The **`list usage`** command allows short extensions as a qualifier for the command. The **List Usage Report** that results includes all instances of a short extension's administration.

list usage ip-address

It is often necessary to determine the extension number associated with an IP address. Other than checking the status of one station at a time by extension number, there had been no way to get a cross-reference of IP address to extension.

The **`list usage ip-address`** ***n*** command. where ***n*** is the IP address, has been enhanced. The **List Usage Report** that results now shows station/extension usage.

save translation

Prior to release 2.0, the **`save translation`** command caused **`filesync`** to run to all LSPs. Since many administrators execute the **`save translation`** command many times a day, this can cause a heavy load on the network. This also can cause the SAT to lock for many hours, depending on the size of the network, the size of translations, and the number of LSPs in the system.

Four changes to the **`save translation`** command are added to help in lessening this issue:

- New qualifier: A new optional qualifier ***`[lsp]`*** is added to the **`save translation`** command. This option specifies the IP address of the desired LSP. The specified IP address must also exist on the **node-names** IP screen, or it will not be accepted. The message passed to begin **`filesync`** is modified to include the information about the type of **`save translation`** being issued.

- Filesync change: If the message sent to **filesync** indicates that the qualifier was not present, **filesync** only runs to the standby server. If the message sent to **filesync** indicates that the qualifier was present, **filesync** runs to the standby server, as well as to all LSPs.
- Scheduled maintenance: There is an option on the **System Maintenance** screen (use the **change system-maintenance** command): **Update LSPs when saving translations?**. This option indicates whether the **filesync** to LSP is on or off during the scheduled maintenance save translations. This field defaults to **y**.
- Registering LSPs: The main server issues a **filesync** command when an administered LSP registers with the main server.

The **save translation** command by itself (with no qualifier) causes **filesync** to run to the active and standby server. It does not initiate a **filesync** to any administered LSPs.

Index

Numerical

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W