Avaya™ Communication Manager

Little Instruction Books

Avaya™ Communication Manager

Little Instruction Book
for basic administration

Release 1.3
555-233-756
Issue 5
May 2003

Easy reference

Pencil in your information below. (shows example only)

Cabinets (cabinet #3 is a remote cabinet in the downtown office)

Boards (TN754 = 4 wire digital, can be used with any digital)

Extension range (8000-8999 = DID)

Coverage paths (Coverage path #1 = 3 rings, covers to AUDIX)

Hunt groups (h4 = audix 84)

Trunk groups (group 1 = CO trunks for outside calls)

Feature access codes (*21 = Abbrev dialing list 2)

Credits

Patrons	Jeff Akers, Curtis Weeks
Supporters	Ed Cote, Randy Fox, Jerry Peel, Pam McDonnell
Writers	Renee Getter, Cindy Bittner, Kim Livingston, John Fenner
Graphics	Laurie King, Karen Consigny
Production	Jacki Rosellen
Contributors	Cathi Schramm, Robert Plant, John O'Keefe
Web/CD Production	Ellen Heffington

Special Thanks to Kim Santich — Customer Champion; Steven Gaipa — Marketing; Rick Thompson — Communication Manager User Group; Doug Schneider, Marcia Bubeck, Barry Bunch, Dan Selvig, and Pat Dolphin — Communication Manager Helpline; Sherilyn McDaniel, Norma Kugler, and Dorothy Quintana — Avaya Switch Administrators

NOTE:
Please note: Many of these individuals are no longer in the positions listed here. However, we continue to credit them because they were instrumental in the creation and success of this book.

Copyright 2003, Avaya Inc.
All Rights Reserved

Notice

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

Preventing Toll Fraud

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

Avaya Fraud Intervention

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

How to Get Help

For additional support telephone numbers, go to the Avaya Web site:

http://www.avaya.com/support/

If you are:

- Within the United States, click *Escalation Lists*, which includes escalation phone numbers within the USA.
- Outside the United States, click *Escalation Lists* then click *Global Escalation List*, which includes phone numbers for the regional 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

Voice Over Internet Protocol (VoIP)

If the equipment supports Voice over Internet Protocol (VoIP) facilities, you may experience certain compromises in performance, reliability and security, even when the equipment performs as warranted. These compromises may become more acute if you fail to follow Avaya's recommendations for configuration, operation and use of the equipment. YOU ACKNOWLEDGE THAT YOU ARE AWARE OF THESE RISKS AND THAT YOU HAVE DETERMINED THEY ARE ACCEPTABLE FOR YOUR APPLICATION OF THE EQUIPMENT. YOU ALSO ACKNOWLEDGE THAT, UNLESS EXPRESSLY PROVIDED IN ANOTHER AGREEMENT, YOU ARE SOLELY RESPONSIBLE FOR (1) ENSURING THAT YOUR NETWORKS AND SYSTEMS ARE ADEQUATELY SECURED AGAINST UNAUTHORIZED INTRUSION AND (2) BACKING UP YOUR DATA AND FILES.

Standards Compliance

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

Product Safety Standards

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

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

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

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

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

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

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

The LASER devices operate within the following parameters:

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

Luokan 1 Laserlaite
Klass 1 Laser Apparat

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

Electromagnetic Compatibility (EMC) Standards

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

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

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

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

Federal Communications Commission Statement

Part 15:
For MCC1, SCC1, G600, and CMC1 Media Gateways:

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.

For the G700 Media Gateway:

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. 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. However, there is no guarantee that radio interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- **Reorient or relocate the receiving antenna.**
- **Increase the separation between the equipment and receiver.**
- **Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.**
- **Consult the dealer or an experienced radio/TV technician for help.**

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.

For MCC1, SCC1, G600, and CMC1 Media Gateways:
This equipment complies with Part 68 of the FCC rules. On the rear 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 the G700 Media Gateway:
This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. Located prominently on 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.

The REN is used to determine the quantity of devices which 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, G600, and CMC1 Media Gateways:

Manufacturer's Port Identifier	FIC Code	SOC/REN/ A.S. Code	Network Jacks
Off/On 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
120A3 channel service unit	04DU9-DN	6.0Y	RJ48C

For the G700 Media Gateway:

Manufacturer's Port Identifier	FIC Code	SOC/REN/ A.S. Code	Network Jacks
Ground Start CO trunk	02GS2	0.5A	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

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

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

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

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

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

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

Canadian Department of Communications (DOC) Interference Information

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

For the G700 Media Gateway:
This Class B digital apparatus complies with Canadian ICES-003.

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

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

DECLARATIONS OF CONFORMITY

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

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

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

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

http://www.avaya.com/support

All Avaya media servers and media gateways are compliant with FCC Part 68, but many have been registered with the FCC before the SDoC process was available. A list of all Avaya registered products may be found at:

http://www.part68.org/

by conducting a search using "Avaya" as manufacturer.

European Union Declarations of Conformity

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). This equipment has been certified to meet CTR3 Basic Rate Interface (BRI) and CTR4 Primary Rate Interface (PRI) and subsets thereof in CTR12 and CTR13, as applicable.

Copies of these Declarations of Conformity (DoCs) can be obtained by contacting your local sales representative and are available on the following Web site:

http://www.avaya.com/support/

Japan

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

For the G700 Media Gateway:
This is a Class B 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B 情報技術装置です。この装置は、家庭環境で使用すること
を目的としていますが、この装置がラジオやテレビジョン受信機に近接して
使用されると、受信障害を引き起こすことがあります。
取 扱説明書に従って正しい取り扱いをして下さい。

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 Web site:
http://www.avaya.com/support/

Contents

Welcome 17

- Why this book? 17
- We wrote this book for you! 18
- What information is in this book? 18
- How to use this book 19
- Security concerns 21
- Trademarks 21
- Related books 22
- Tell us what you think! 22
- How to get this book on the Web 23
- How to order more copies 23
- How to get help 24

Getting started 25

- Overview of Avaya Communication Manager 25
  - Sample system running Avaya Communication Manager 26
  - Phone types 27
- Accessing your system 29
  - Logging into the system 29
  - Setting the system time and date 30
  - Saving changes 31
  - Logging off the system 34

Contents

Planning the system 35

- Understanding the dial plan 35
- Dial plans with Avaya Communication Manager 36
  - Displaying your dial plan 38
  - Modifying your dial plan 38
  - Adding extension ranges to your dial plan 38
  - Adding feature access codes to your dial plan 39
- Dial plans with Avaya software release R10 or earlier 40
  - Displaying your dial plan 42
  - Modifying your dial plan 42
  - Adding extension ranges to your dial plan 43
  - Adding feature access codes to your dial plan 43
- Changing feature access codes 44

Managing phones 47

- Adding new phones 47
  - Gathering necessary information 48
  - Physically connecting the phone 50
  - Completing the station screens 50
  - Using station templates to add phones 52
  - Using an alias 53
  - Adding or changing feature buttons 55
- Customizing your phone 57
- Upgrading phones 58
- Swapping phones 59
- Removing phones 60

Contents

Managing features 63

- Changing feature parameters 63
- Setting up abbreviated dialing 65
- Creating pickup groups 68
- Setting up call forwarding 70
- Creating coverage paths 71
  - Defining time-of-day coverage 74
  - Creating coverage answer groups 76
  - Defining coverage for calls redirected to external numbers 77
  - Defining telecommuting coverage 80
- Setting up bridged call appearances 81

Routing outgoing calls 87

- World class routing 87
  - Understanding ARS analysis 88
  - Managing calling privileges 89
  - Displaying ARS analysis information 90
- Modifying call routing 90
  - Adding a new area code or prefix 91
  - Using ARS to restrict outgoing calls 93
- Overriding call restrictions 95
- ARS Partitioning 96
  - Setting up a partition group 97
  - Assigning a phone to a partition group 99

Contents

Enhancing system security 103

- Assigning and changing users 103
  - Assigning new logins and passwords 104
  - Setting login permissions 106
  - Changing passwords 107
  - Changing logins 108
- Preventing toll fraud 108
- Using reports to detect problems 111
  - Call Detail Recording 111
  - Security Violations Notification 112

Keeping records 117

- Paper records 117
- Preparing to contact Avaya 121

Glossary 123

Index 131

Helpful Avaya web sites 139

Welcome

Why this book?

You've told us that you want step-by-step instructions on everyday administration tasks for your Avaya™ Communication Manager, and we've been listening. This book contains the information you need for basic telephone system administration. Some steps may vary a bit between the different versions of Communication Manager, but the instructions provided will help you through the most basic operations.

If you are familiar with earlier versions of this book, you will notice some changes. The fields on some screens have changed, we've moved the area code instructions to a section on routing, and have given troubleshooting its very own book, the *Avaya™ Communication Manager Little Instruction Book for basic diagnostics*, 555-233-758.

We wrote this book for you!

Use this book if you are a system administrator. Use it before you attend training, and take it with you to your class. Mark it up, make notes in it, and use it daily even after you complete training. If you are a new administrator taking over the position from someone else, or you are filling in for your company's regular administrator, or if you simply want to refresh your memory, this book is for you.

What information is in this book?

The *Little Instruction Book for basic administration* is divided into sections to guide you through your day-to-day operations.

"Getting started" provides an overview of the phone system and types of phones. It provides instructions for logging in, saving changes, and logging off.

"Planning the system" explains how to read and update your dial plan. It also explains how to change feature access codes.

"Managing phones" explains how to add, change, and remove phones from your system. It also explains how to alias phones and how to customize a phone for your system administrator.

"Managing features" explains how to administer useful features including abbreviated dialing, pickup groups, call forwarding, call coverage, and bridged appearances.

"Routing outgoing calls" explains how to add area codes and prefixes. It also includes instructions for setting up ARS partitioning and authorization codes.

"Enhancing system security" explains how to add and change user logins and passwords. It also provides an overview of security issues related to Communication Manager.

"Keeping records" provides guidelines for keeping records and explains how to print certain system reports. It also explains how to contact the Communication Manager helpline and lists what information you should gather before you call.

How to use this book

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

- To "move" to a certain field, you can use the TAB key, arrows, or the RETURN key.
- A "screen" is a screen form displayed on the terminal monitor.
- In this book we always use the term phone; other Avaya books may refer to phones as voice terminals.
- If you use terminal emulation software, you need to determine which keys correspond to ENTER, RETURN, CANCEL, HELP, NEXT PAGE, etc.
- Commands are printed in bold face as follows: **command**.
- Keys and buttons are printed as follows: KEY.
- Screen displays are printed in constant width as follows: `screen display`.
- Variables are printed in bold face italics as follows: ***variable***.

- We show complete commands in this book, but you can always use an abbreviated version of the command. For example, **list configuration station** can be entered as **list config sta**.
- We show commands and screens from the newest release of Communication Manager and refer to the most current books. Please substitute the appropriate commands for your system and refer to the manuals you have available.
- If you need help constructing a command or completing a field entry, remember to use HELP.
  - When you press HELP at any point on the command line, a list of available commands appears.
  - When you press HELP with your cursor in a field on a screen, a list of valid entries for that field appears.
- The status line or message line can be found near the bottom of your monitor display. 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 our helpline.
- When a procedure requires you to press ENTER to save your changes, the screen you were working on clears and the cursor returns to the command prompt. The message line shows "`command successfully completed`" to indicate that the system accepted your changes.

You may see the following icons in this book:

Tip:
Draws attention to information that you may find helpful.

NOTE:
Draws attention to information.

CAUTION:
Denotes possible harm to software, possible loss of data, or possible service interruptions.

SECURITY ALERT:
Indicates when system administration may leave your system open to toll fraud.

Security concerns

Toll fraud is the theft of long distance service. When toll fraud occurs, your company is responsible for charges. Refer to the *Avaya Products Security Handbook*, 555-025-600, for information on how to prevent toll fraud. You can also call the Avaya Security Hotline at 1 800 643 2353 or contact your Avaya representative.

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.

Related books

The *Avaya™ Communication Manager Little Instruction Book for advanced administration*, 555-233-757, and the *Avaya™ Communication Manager Little Instruction Book for basic diagnostics*, 555-233-758, are companions to this book. We suggest you use them often.

The *Administrator's Guide for Avaya™ Communication Manager*, 555-233-506, explains system features and interactions in detail. It provides a reference for planning, operating, and administering your system, and we refer to it often. Please note that prior to April 1997, this same information was in two separate books: the *DEFINITY Implementation* and the *DEFINITY Feature Description* books.

We also refer to the *Overview for Avaya™ Communication Manager*, 555-233-767, and the *Avaya Products Security Handbook*, 555-025-600.

Tell us what you think!

Let us know what you like or don't like about this book. Although we can't respond personally to all your feedback, we promise we will read each response we receive.

Write to us at:	Avaya Inc. Product Documentation Group Room B3-H13 1300 W. 120th Avenue Denver, CO 80234 USA
Fax to:	1 303 538 1741
Send email to:	document@avaya.com

How to get this book on the Web

If you have internet access, you can view and download the latest version of *Avaya™ Communication Manager Little Instruction Book for basic administration*. To view the book, you must have a copy of Acrobat Reader.

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

To access the latest version:

1. Access the Avaya Customer Support Web site at http://www.avaya.com/support/.
2. Click PRODUCT DOCUMENTATION.
3. Search for 555-233-756 (the document number) to view the latest version of the book.

How to order more copies

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
Attn: Avaya Account Management
200 Ward Hill Ave
Haverhill, MA 01835 USA

E-mail: totalware@gwsmail.com

Order: Document No. 555-233-756, Issue 5, May 2003

We can place you on a standing order list so that you will automatically receive updated versions of this book. For more information on standing orders, or to be put on a list to receive future issues of this book, please contact the Avaya Publications Center.

How to get help

If you need additional help, first access the Avaya Customer Support Web site at http://www.avaya.com/support/. Click the ESCALATION LIST link for the most recent information. If you are outside the USA, also click the GLOBAL ESCALATION LIST link for the phone numbers for the regional Centers of Excellence.

You can also access the following services. You may need to purchase an extended service agreement to use some of these services. Contact your Avaya representative for more information.

Avaya™ Communication Manager Helpline (for help with feature administration and system applications)	1 800 225 7585
Avaya National Customer Care Center Support Line (for help with maintenance and repair)	1 800 242 2121
Avaya Toll Fraud Intervention	1 800 643 2353
Avaya Corporate Security	1 800 822 9009

Getting started

This section contains a brief overview of a system running Avaya™ Communication Manager. It also explains how to log in to your communication system, change the date and time, save changes to the system, and log off.

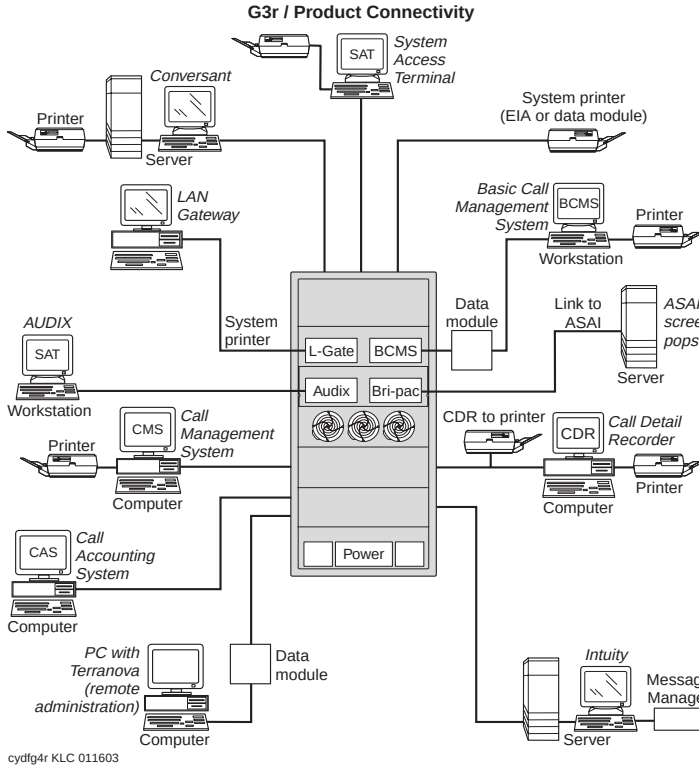
Overview of Avaya Communication Manager

Avaya™ Communication Manager organizes and routes voice, data, image, and video transmissions. Your system can be connected to communications paths that transmit voice and data signals between the phone system and a central office, and to other public and private networks. The following figure shows typical system connections, software packages, and additional hardware.

To find more detailed information and a comprehensive overview of Communication Manager, refer to your *Overview for Avaya™ Communication Manager*, 555-233-767.

NOTE:
Your equipment may be different from the equipment shown in the figure.

Sample system running Avaya™ Communication Manager



Sample system running Avaya Communication Manager

Your system running Communication Manager may include some or all of the following components:

- Conversant — provides response to spoken information
- System Access Terminal (SAT) — allows direct connection for administration and reports

- Basic Call Management System (BCMS) — collects information and prints reports on call-center performance
- Data module — provides digital information to the system
- ASAI — allows integration between adjunct computers and systems running Communication Manager
- Call Detail Recording (CDR) — collects, stores, filters, and prints records on calls handled by your system
- Intuity message manager — access to INTUITY AUDIX and embedded AUDIX voice processing on a personal computer connected to a local area network
- PC with terminal emulation software — allows remote system administration from a personal computer
- Call Accounting System (CAS) — uses call records to create billing reports for the hospitality industry
- Call Management System (CMS) — collects information and generates reports on telemarketing centers
- AUDIX workstation — allows you to administer voice mail
- System printer/LAN gateway — connects to the system printer and local area network server

Phone types

Your system may have any of the following phone types, or a combination, administered as user phones. As you make changes to your system, you'll need to know whether each phone is an analog, digital, hybrid, ISDN, or IP phone.

Analog	Digital	Hybrid	ISDN	IP
500	2402	7303S	7505D	4602
2500	2420	7305S	7506D	4606
6210	6402	7309H	7507D	4612
6218	6408, 6408+, 6408D	7313H	8503D	4620
6220	6416D+	7314H	8510T	4624
7101A	6424D+M	7315H	8520T	4630
7102A	7401D, 7401+	7316H	ASAI	
7103A	7403D	7317H		
7104A	7404D			
7302H	7405D, 7405ND			
7303H	7406D, 7406+			
8110	7407D, 7407+			
DS1FD	7410D, 7410+			
K2500	7434D, 7434ND			
	7444D			
	8403B			
	8405B, 8405B+			
	8405D, 8405D+			
	8411B, 8411D			
	602A1			
	603A1, 603D1, 603E1			
	606A1			

Accessing your system

You need to log in before you can administer your communication system. To log in, you need to know:

- your login and password
- the type of terminal or terminal emulation program that you are using

Change your password frequently, at least once a month, to help keep hackers out of your system. For instructions on how to change your password or add new logins, refer to "Assigning and changing users" on page 103.

Logging into the system

If your system requires Access Security Gateway procedures, refer to the *Administrator's Guide for Avaya™ Communication Manager*, 555-233-506, for more information.

1. At the prompt, type your login and press RETURN.

   The system prompts you for your password.

2. Type your password and press RETURN.

   Your password does not display on the screen. Be sure to keep your password private.

   The system prompts you for your terminal type. The type in square brackets is the default.

Terminal screen for login

```
Login:
Password:

System: XXXXXX        Software Version: xxxxxxxxxxxx

Terminal Type: (513, 715, 4410, 4425, VT220): [513]
```

3. Press RETURN if you are using the default terminal. Otherwise, enter the terminal type and press RETURN.

Once you log in, "`Command`" appears. The system is ready to accept a new command.

Setting the system time and date

Update the system time and date for events such as leap year or daylight savings time. The correct time and date ensure that records are correct.

Tip:
Changing the date and time may modify Call Detail Recording (CDR) data by 9 hours and 59 minutes. Therefore, you should change the date and time after normal business hours.

To set the system time and date:

1. Type **set time** and press RETURN.

   The `DATE AND TIME` screen appears.

2. Complete the appropriate fields.

   Use a 24-hour clock to set the hour. For example, for 2:00 p.m. (14:00) type **14**. Do not try to update the `Second` field because it automatically resets to `0` when you press ENTER.

3. Press ENTER to save your changes.

Date and Time screen

```
                    DATE AND TIME
DATE
        Day of the Week: __________   Month: _________
       Day of the Month: __            Year: ____
TIME
       Hour:__    Minute:__  Second: XX    Type:________

             Daylight Savings Rule: ___
```

4. Type **display time** and press RETURN to double check the new date and time.

> **Tip:**
> *When you change the date or time, some display phones may not automatically refresh the display. If this happens, have each user press the date/time button on their phone and the display should update.*

See the *Administrator's Guide for Avaya™ Communication Manager*, 555-233-506, for more information about setting the date and time on your system.

Saving changes

There are two methods for saving changes to your system: temporary saves and permanent backups.

Temporary save

As you are working with the system, your changes to the system memory are considered temporary. These changes are lost if your system loses power before the next permanent save (or backup).

1. Press ENTER to save any changes you make on a screen.

When you press ENTER, "`command successfully completed`" appears and the cursor returns to the command prompt.

Permanent backup

A permanent backup copies your changes from the system memory to a card (also called a flash ROM), disk, or tape. You can perform manual backups or your system may be administered to automatically backup every 24 hours.

Tip:
To determine if your system backs up automatically, type **display system-parameters maintenance** *and see if you have scheduled maintenance.*

When you make large changes, perform a manual backup in case your system loses power before the next backup. To create a backup:

1. Be sure that the backup card or tape is in place.
2. Check the alarms panel and clear any active alarms.
3. Type **save translation** and press RETURN.

   The save process may take up to 10 minutes. You cannot administer your system while the save process takes place.

   If an error message appears in the `Command Completion Status` field, clear the error and repeat the save process.

Save Translation screen

```
                              SAVE TRANSLATION

Processor              Command Completion Status        Error Code
SPE_A                            Success                     0
```

It is a good idea to have at least two backups. You can run the backup again to a second card, or you can copy an automatic backup with the backup command (if your system allows). You may want to keep this second (or a third) backup off premises to ensure you could recover from a disaster or system failure.

See the *Administrator's Guide for Avaya™ Communication Manager*, 555-233-506, for more information about performing backups of your system.

Saving announcements

You can save announcements only if your system has an integrated announcement board and you have administered announcements.

See the *Avaya™ Communication Manager Little Instruction Book for advanced administration*, 555-233-757, for information about Voice Announcements over LAN (VAL) and VAL Manager.

If you change your recorded announcements and you have a TN750C board, the system automatically saves your changes to the on-board FLASH memory.

If you have a TN750 or TN750B board, you need to manually save the recorded announcements on your system.

1. Type **save announcements** and press RETURN to save the changes.

   This process can take up to 40 minutes. You cannot administer your system while the system is saving announcements.

   NOTE:
   If you have both TN750B and TN750C boards, save announcements to the TN750B slot.

See the *Administrator's Guide for Avaya™ Communication Manager*, 555-233-506, for more information about saving announcements.

Logging off the system

For security reasons, log off every time you leave your terminal.

1. To log off the system, type **logoff** and press RETURN.

   You may see a security screen that indicates that you have Remote Access, Facility Test, or Busied Out administered. You may want to disable these features before you log off. For more information about these features, refer to the *Avaya™ Communication Manager Little Instruction Book for basic diagnostics*, 555-233-758.

   This screen also indicates whether or not you have any active minor or major alarms that you should address before you end your session.

2. Type **y** and press RETURN to proceed with log off.

If you use terminal emulation software to administer the switch, you should log off the system and exit the emulation application before alternating or switching to another software package.

Planning the system

This section provides you with background on system-wide functions. It explains how to read and use your dial plan, and shows you how to make simple changes such as adding extension ranges. This section also explains how to assign feature access codes.

Understanding the dial plan

Your dial plan tells your system how to interpret dialed digits. For example, if you dial 9 on your system to access an outside line, it is actually the dial plan that tells the system to find an external trunk when a dialed string begins with a 9.

The dial plan also tells the system how many digits to expect for certain calls. For example, the dial plan may indicate that all internal extensions are 4-digit numbers that start with 1 or 2.

Tip:
In this book, we do not usually explain each screen as thoroughly as we do the dial plan. However, this screen serves as the basis for almost everything in the system, so we wanted to be sure you have a clear understanding of how to read and update your dial plan. The screens shown may not exactly match your system.

If you have a system that is running Communication Manager, see "Dial plans with Avaya Communication Manager" on page 36*. If you have a system that is running Avaya software release R10 or earlier, see* "Dial plans with Avaya software release R10 or earlier" on page 40*. If you need more information, refer to the Administrator's Guide for Avaya™ Communication Manager,* 555-233-506.

Dial plans with Avaya Communication Manager

Communication Manager allows you to create your dial plan using from three to seven digits.

NOTE:
If you have a system running Avaya software release R10 or earlier, see "Dial plans with Avaya software release R10 or earlier" on page 40.

Let's take a look at an example dial plan so you'll know how to read your system's dial plan. The following figure shows an example of a simple dial plan.

Dial Plan Analysis Table screen

```
                         DIAL PLAN ANALYSIS TABLE
                                                        Percent Full: 9

Dialed  Total   Call     Dialed  Total   Call     Dialed  Total   Call
String  Length  Type     String  Length  Type     String  Length  Type
  0       1     attd       __      _     ____       __      _     ____
  1       3     dac        __      _     ____       __      _     ____
  20      5     ext        __      _     ____       __      _     ____
  21      2     fac        __      _     ____       __      _     ____
  3       5     ext        __      _     ____       __      _     ____
  4       4     ext        __      _     ____       __      _     ____
  4       7     ext        __      _     ____       __      _     ____
  5       7     ext        __      _     ____       __      _     ____
  6       7     ext        __      _     ____       __      _     ____
  8       1     fac        __      _     ____       __      _     ____
  9       5     ext        __      _     ____       __      _     ____
  *       3     fac        __      _     ____       __      _     ____
  #       3     fac        __      _     ____       __      _     ____
```

The set of three columns indicate how long the dialed string will be for each type of call. For example, this dial plan shows that when users dial a 7-digit number that starts with 4, they are dialing an extension.

The third column may have any of the following codes:

- Attendant (attd) — Defines how users call an attendant. Attd access numbers can be any number from 0 to 9 and contain 1 or more digits. In our example figure, the system calls an attendant when users dial 0.
- Dial Access Codes (dac) — Allows you to use trunk access codes (tac) and feature access codes (fac) in the same range. For example, you could define the group 100–199 for dacs, which would allow both facs and tacs in that range. Dial access codes can start with any number from 1 to 9 and contain up to 4 digits. In recent releases, * and # also can be the first digit. In our example figure, dial access codes begin with 1 and must be 3 digits long, so this company can have a feature access code set to 133 and a trunk access code assigned to 134.
- Extensions (ext) — Defines extension ranges that can be used on your system. In our example, extensions must be in the ranges: 20000–20999, 30000–39999, 4000–4999, 4000000–4999999, 5000000–5999999, 6000000–6999999, and 90000–99999.
- Feature Access Codes (fac) — facs can be any number from 1 to 9 and contain up to 4 digits. You can use * or #, but only as a first digit. In our example, this company can use *21 to activate a feature and use #21 to deactivate the same feature. Our example also shows that one fac can be set to 8 (first digit 8, only one digit long).

Displaying your dial plan

You might want to take this opportunity to look at and interpret your own dial plan. To display your system's dial plan:

1. Type **display dialplan analysis** and press RETURN.

Modifying your dial plan

It is easy to make changes to your dial plan. For example, let's add a new range of dial access codes to the dial plan. We want to be able to assign both facs and tacs in the 700–799 range.

1. Type **change dialplan analysis** and press RETURN.

   The `DIAL PLAN ANALYSIS TABLE` screen appears.

2. Move the cursor to the next available row.
3. Type **7** in the first column.
4. Type **3** in the second column.
5. Type **dac** in the third column.
6. Press ENTER to save your changes.

Adding extension ranges to your dial plan

You may find that as your needs grow you want a new set of extensions. Before you can assign a station to an extension, the extension must belong to a range that is defined in the dial plan. Let's add a new set of extensions that start with 8 and are 6 digits long (800000–899999).

To add this set of extensions to the dial plan:

1. Type **change dialplan analysis** and press RETURN.

   The `DIAL PLAN ANALYSIS TABLE` screen appears.
2. Move the cursor to the next available row.
3. Type **8** in the first column.
4. Type **6** in the second column.
5. Type **ext** in the third column.
6. Press ENTER to save your changes.

Adding feature access codes to your dial plan

As your needs change, you may want to add a new set of feature access codes for your system. Before you can assign a fac on the `FEATURE ACCESS CODE` screen, it must conform to your dial plan.

In our example, if you want to assign a feature access code of 33 to Last Number Dialed, first you need to add a new fac range to the dial plan. To add a fac range from 30–39:

1. Type **change dialplan analysis** and press RETURN.

   The `DIAL PLAN ANALYSIS TABLE` screen appears.
2. Move the cursor to the next available row.
3. Type **3** in the first column.
4. Type **2** in the second column.
5. Type **fac** in the third column.
6. Press ENTER to save your changes.

Dial plans with Avaya software release R10 or earlier

NOTE:
If you have a system running Avaya™ Communication Manager, see "Dial plans with Avaya Communication Manager" on page 36.

Let's take a look at an example dial plan so you'll know how to read your system's dial plan. The following figure shows an example of a simple dial plan.

Dial Plan Record screen

```
                                DIAL PLAN RECORD                    Page 1 of 1
                                                     Local Node Number:
                                                     ETA Node Number:
        Uniform Dialing Plan: 4-digit          ETA Routing Pattern:
  UDP Extension Search Order: local-extensions-first
FIRST DIGIT TABLE
First                                 Length
Digit    -1-          -2-          -3-         -4-          -5-         -6-
  1:  __________  __________  __________  ext_______  __________  __________
  2:  __________  __________  __________  ext_______  __________  __________
  3:  __________  __________  __________  __________  __________  __________
  4:  __________  __________  __________  __________  __________  __________
  5:  __________  __________  __________  ext_______  __________  __________
  6:  __________  __________  dac_______  __________  __________  __________
  7:  __________  __________  __________  __________  __________  __________
  8:  __________  __________  __________  __________  __________  __________
  9:  fac_______  __________  __________  __________  __________  __________
  0:  attd______  __________  __________  __________  __________  __________
  *:  __________  __________  fac_______  __________
  #:  __________  __________  fac_______  __________
```

If you look at the lower half of the `DIAL PLAN RECORD` screen, you see the `FIRST DIGIT TABLE`. This table defines the dialing plan for your system.

The rows in the `FIRST DIGIT TABLE` indicate what the system does when the row's first digit is dialed. The columns indicate how long the dialed string will be for each type of call. For example, this dial plan shows that when users dial a 4-digit number that starts with 2, they are dialing an extension.

The `FIRST DIGIT TABLE` may have any of the following codes:

- Attendant (attd) — Defines how users call an attendant. Attd access numbers can be any number from 0 to 9 and contain 1 or more digits. In our example figure, the system calls an attendant when users dial 0.
- Dial access codes (dac) — Allows you to use trunk access codes (tac) and feature access codes (fac) in the same range. For example, you could define the group 300–399 for dacs, which would allow both facs and tacs in that range. Dial access codes can start with any number from 1 to 9 and contain up to 4 digits. In recent releases, * and # also can be the first digit. In our example figure, dial access codes begin with 6 and must be 3 digits long, so this company can have a feature access code set to 633 and a trunk access code assigned to 634.
- Extensions (ext) — Defines extension ranges that can be used on your system. In our figure, extensions must be in the ranges: 1000–1999, 2000–2999, and 5000–5999.
- Feature access codes (fac) only — facs can be any number from 1 to 9 and contain up to 4 digits. You can use * or #, but only as a first digit. In our example, this company can use *21 to activate a feature and use #21 to deactivate the same feature. Our example also shows that one fac can be set to 9 (first digit 9, only one digit long).

- Miscellaneous code (misc) — (for R10 or earlier only) these codes are used if you want to have more than one kind of code start with the same digit and be the same length. Using a misc code requires that you also define a second digit table. Refer to the *Administrator's Guide for Avaya™ Communication Manager*, 555-233-506, for information about the second digit table. Our example does not show this code.

Displaying your dial plan

You might want to take this opportunity to look at and interpret your own dial plan. To display your system's dial plan:

1. Type **display dialplan** and press RETURN.

Modifying your dial plan

It is easy to make changes to your dial plan. For example, let's add a new range of dial access codes to the dial plan. We want to be able to assign both facs and tacs in the 700–799 range.

1. Type **change dialplan** and press RETURN.

   The `DIAL PLAN RECORD` screen appears.

2. Move the cursor to the 7th row in the 3rd column.

   This field defines what the system does when users dial any number from 700 to 799.

3. Type **dac** in the selected field.

4. Press ENTER to save your changes.

Adding extension ranges to your dial plan

You may find that as your needs grow you want a new set of extensions. Before you can assign a station to an extension, the extension must belong to a range that is defined in the dial plan. Let's add a new set of extensions that start with 3 and are 4 digits long (3000–3999).

To add this set of extensions to the dial plan:

1. Type **change dialplan** and press RETURN.

   The `DIAL PLAN RECORD` screen appears.

2. Move the cursor to the 3rd row in the 4th column.
3. Type **ext** in the selected field.
4. Press ENTER to save your changes.

Adding feature access codes to your dial plan

As your needs change, you may want to add a new set of feature access codes for your system. Before you can assign a fac on the `FEATURE ACCESS CODE` screen, it must conform to your dial plan.

In our example, if you want to assign a feature access code of 33 to Last Number Dialed, you need to add a new fac range to the dial plan.

To add a fac range from 30–39:

1. Type **change dialplan** and press RETURN.

   The `DIAL PLAN RECORD` screen appears.

2. Move the cursor to the 3rd row and the 2nd column.
3. Type **fac** in the selected field.
4. Press ENTER to save your changes.

Changing feature access codes

Feature access codes (FAC) allow users to activate and deactivate features from their phones. A user who knows the fac for a feature does not need a programmed button to use the feature. For example, if you tell your users that the fac for the Last Number Dialed is *33, then users can redial a phone number by entering the fac, rather than requiring a Last Number Dialed button.

Many features already have factory-set feature access codes. You can use these default codes or you can change them to codes that make more sense to you. However, every fac must conform to your dial plan and must be unique. For more information about the dial plan, refer to “Understanding the dial plan” on page 35.

Let’s try an example. If you want to change the feature access code for Call Park to *72:

1. Type **change feature-access-codes** and press RETURN.

   The `FEATURE ACCESS CODE (FAC)` screens appear.

Feature Access Code (FAC) screen

```
                              FEATURE ACCESS CODE (FAC)

          Abbreviated Dialing List1 Access Code: #01
          Abbreviated Dialing List2 Access Code: #02
          Abbreviated Dialing List3 Access Code: #03
Abbreviated Dial - Prgm Group List Access Code: #04
                      Announcement Access Code: #05
                       Answer Back Access Code: 179
      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: *9    Access Code 2: *33
                Automatic Callback Activation: #55    Deactivation: *55
Call Forwarding Activation Busy/DA: #22   All: #44    Deactivation: *44
                         Call Park Access Code: *72
                       Call Pickup Access Code: #33
CAS Remote Hold/Answer Hold-Unhold Access Code: #06
                 CDR Account Code Access Code: #33
                       Change COR Access Code: *01
                    Change Coverage Access Code: #80

                  Data Origination Access Code: #09
                      Data Privacy Access Code: #10
              Directed Call Pickup Access Code: #11
```

2. Move the cursor to the `Call Park Access Code` field.
3. Type ***72** in the `Call Park Access Code` field over the old code.
4. Press ENTER to save your changes.

   If you try to enter a code that is assigned to a feature, the system warns you of the duplicate code and does not allow you to proceed until you change one of them.

Tip:
To remove any feature access code, delete the existing fac and leave the field blank.

Managing phones

This section explains how to add, swap, or remove the phones on your system. This section also gives you tips for customizing your own phone so it has the feature buttons you need for many administration and troubleshooting tasks.

NOTE:
Note that this section does not tell you how to administer attendant consoles or IP phones. If you need to add or modify an attendant console or IP phone, refer to the *Administrator's Guide for Avaya™ Communication Manager*, 555-233-506.

Adding new phones

When you are asked to add a new phone to the phone system, what do you do first? To connect a new phone you need to do three things:

- find an available port
- wire the port to the cross-connect field or termination closet
- tell the telephone system what you're doing

Before you can determine which port to use for the new phone, you need to determine what type of phone you are installing, what ports are available, and where you want to install the phone.

Gathering necessary information

1. Determine whether the phone is an analog, digital, ISDN, or hybrid set.

   You need this information to determine the type of port you need, because the port type and phone type must match. If you do not know what type of phone you have, refer to “Phone types” on page 27 for a list of phones by model number.

2. Record the room location, jack number, and wire number.

   You may find this information on the jack where you want to install the phone, recorded in your system records, or from the technician responsible for the physical installation.

3. Display the available boards (circuit packs) and ports.

   To view a list of boards on your system, type **list configuration stations** and press RETURN.

System Configuration screen

```
                              SYSTEM CONFIGURATION
Board                                                        Assigned Ports
Number    Board Type        Code       Vintage   u=unassigned t=tti p=psa

01A05     DIGITAL LINE      TN754B     000002     01 u  03 u  05 u  07 08
01A06     ANALOG LINE       TN742      000010     01 02 03 04 u  u  u  u
01B05     ANALOG LINE       TN746B     000008     u  u  u  u  u  u  u  u
                                                  u  u  u  u  u  u  u  u
01C04     ANALOG LINE       TN746B     000008     u  u  u  u  u  u  u  u
                                                  u  u  u  u  u  u  u  u
01C05     DIGITAL LINE      TN2224     000004     01 u  u  04 u  u  07 08
                                                  u  u  u  u  u  u  u  u
u  u  u  u  u  u  u  u
01C06      HYBRID LINE           TN762B 000004      01 02 u  u  u  u  u  u
01C09      MET LINE              TN735  000005      01 u  u  u
01C10      DIGITAL LINE          TN754  000004      u  u  u  u  u  u  u  u
```

The `SYSTEM CONFIGURATION` screen shows all the boards (circuit packs) on your system that are available for connecting phones. You can see the board number, board type, and status of each board's ports.

4. Choose an available port and record its port address.

   Each port that is available or unassigned is indicated by a 'u.' Choose an available port from a board type that matches your phone type (such as a port on an analog board for an analog phone).

   Every phone must have a valid port assignment, also called a port address. The combined board number and port number is the port address. So, if you want to attach a phone to the 3rd port on the 01C05 board, the port address is 01C0503 (01=cabinet, C=carrier, 05=slot, 03=port).

   Tip:
   If you add several phones at one time, you may want to print a paper copy of the `SYSTEM CONFIGURATION` *screen. To print the screen to a printer attached to the system terminal, type* **list configuration stations print** *and press* RETURN. *To print to the system printer that you use for scheduled reports, type* **list configuration stations schedule immediate** *and press* RETURN.

5. Choose an extension number for the new phone.

   The extension you choose must not be assigned and must conform to your dial plan. You should also determine whether this user needs an extension that can be directly dialed (DID) or reached via a central phone number.

   Be sure to note your port and extension selections on your system's paper records.

Physically connecting the phone

Once you have collected all the information, you are ready to physically wire the port to the cross-connect field.

If you have an Avaya representative or on-site technician who completes the physical connections, you need to notify them that you are ready to add the phone to the system. To request that Avaya install the new connections, call your Avaya representative to place an order.

If you are responsible for making the connections yourself and if you have any questions about connecting the port to the cross-connect field, refer to your system installation guide.

Now you are ready to configure the system so that it recognizes the new phone.

Completing the station screens

The information that you enter on the `Station` screen advises the system that the phone exists and indicates which features you want to enable on the phone.

To access the `STATION` screen for the new phone:

1. Type **add station *n*** and press RETURN, where ***n*** is the extension for the new phone.

   Make sure the extension conforms to your dial plan. You can also use the **add station next** command to add a phone to the next available extension.

   When the `STATION` screen appears, you see the extension number and some default field values. For example, the following screen is for a new phone at extension 2345.

Station screen

```
                                   STATION

Extension: 2345                      Lock Messages? _          BCC: _
     Type: 8411D                     Security Code: __________  TN: 1__
     Port: _______________         Coverage Path 1: ____       COR: 1
     Name: ____________________________ Coverage Path 2: ____   COS: 1
                                   Hunt-to Station: ____

STATION OPTIONS
              Loss Group: ___          Personalized Ringing Pattern: 1
            Data Module? ___                     Message Lamp Ext: 2345
           Speakerphone: 2-way                 Mute Button Enabled? y
       Display Language: english

                                                Media Complex Ext: ____
                                                     IP Softphone? n
```

2. Type the model number of the phone into the `Type` field.

   For example, to install a 8411D phone, type **8411D** in the `Type` field. Note that the displayed fields may change depending on the model you add.

3. Type the port address in the `Port` field.

4. Type a name to associate with this phone in the `Name` field.

   The name you enter appears on called phones that have display capabilities. Also, some messaging applications, such as INTUITY, recommend that you enter the user's name (last name first) and their extension to identify the phone.

5. Press ENTER to save your changes.

To make changes to this new phone, such as assigning coverage paths or feature buttons, type **change station *n*** and press RETURN, where ***n*** is the extension of the new phone.

Using station templates to add phones

A quick way to add phones is to copy the information from an existing phone and modify it for each new phone. For example, you can configure one phone as a template for an entire work group. Then, you merely duplicate the template `STATION` screen to add all the other extensions in the group.

Note that only phones of the same model can be duplicated. The duplicate command copies all the feature settings from the template phone to the new phones.

To duplicate an existing phone:

1. Type **display station *n*** and press RETURN, where ***n*** is the extension of the `STATION` screen you want to duplicate to use as a template. Verify that this extension is the one you want to duplicate.
2. Press CANCEL to return to the command prompt.
3. Type **duplicate station *n*** and press RETURN, where ***n*** is the extension you want to duplicate.

   The system displays a blank duplicate `STATION` screen.

Duplicate Station screen

```
                                   STATION

                                        Security
Ext.     Port     Name                   Code      Room      Jack   Cable
_______  _______  ______________________ _________ _________ ______ ______
_______  _______  ______________________ _________ _________ ______ ______
_______  _______  ______________________ _________ _________ ______ ______
_______  _______  ______________________ _________ _________ ______ ______
_______  _______  ______________________ _________ _________ ______ ______
_______  _______  ______________________ _________ _________ ______ ______
_______  _______  ______________________ _________ _________ ______ ______
_______  _______  ______________________ _________ _________ ______ ______
_______  _______  ______________________ _________ _________ ______ ______
_______  _______  ______________________ _________ _________ ______ ______
```

4. Type in the extension, port address, and phone name for each new phone you want to add.

   The rest of the fields are optional. You can complete them at any time.

5. Press ENTER to save your changes to system memory.

To make changes to these phones, such as assigning coverage paths or feature buttons, type **change station *n*** and press ENTER, where ***n*** is the extension of the phone that you want to modify.

Using an alias

Not every phone model has a unique `STATION` screen in the system. You might have to use an available model number as an “alias” for another. If you need to enter a phone type that the system does not recognize or support, use an alias.

For example, you may need to install a phone model that is newer than your system. In this case, you can use an available model type that best matches the features of your phone. You can refer to your phone’s manual to determine which alias to use. If your manual does not have this information, contact the Communication Manager helpline for an appropriate alias.

As an example, let’s use an alias to add a 8403B phone to a DEFINITY G3V2 or earlier system.

1. Refer to your new phone’s manual to find the correct alias.

   In our example, we find that the 8403B is administered on a G3V2 or earlier system as a 7405D phone.

2. Type **change alias station** and press RETURN.

   The `ALIAS STATION` screen appears.

Alias Station screen

```
                         ALIAS STATION
     Alias Set Type             Supported Set Type
        8403B                        7405D
        _____                        _____
        _____                        _____
        _____                        _____
        _____                        _____
        _____                        _____
        _____                        _____
        _____                        _____
        _____                        _____
        _____                        _____
'#' indicates previously aliased set type is now native
```

3. Type **8403B** in the `Alias Set Type` field.

   Enter the model of the unsupported phone in this field.

4. Type **7405D** in the `Supported Set Type` field.

   Enter the alias (supported model) in this field.

5. Press ENTER to save your changes.

Now follow the instructions for adding a new phone. Your switch now recognizes the new type you entered in the `Alias Set Type` field.

Be sure to refer to your phone's manual for instructions on how to set feature buttons and call appearance buttons. Note that if you need to use an alias for a phone, you may not be able to take advantage of all the features of the new phone.

Adding or changing feature buttons

Once you add a phone to the system, you can use the station screen to change the settings for the phone, such as adding or changing feature button assignments. The system allows you to assign features or functionality to each programmable button. It is up to you to decide which features you want for each phone and which feature you want to assign to each button.

To assign feature buttons:

1. Type **change station *n*** and press ENTER, where ***n*** is the extension for the phone you want to modify.

   The `STATION` screen appears.

2. Press NEXT PAGE until you locate the `Feature Button Assignment` fields.

   Some phones have several feature button groups. Make sure that you are changing the correct button. If you do not know which button on the phone maps to which button-assignment field, refer to your phone's manual, or refer to the *Administrator's Guide for Avaya™ Communication Manager*, 555-233-506.

3. Move the cursor to the field you want to change.

4. Type the button name that corresponds to the feature you want to add.

   To determine feature button names, press HELP or refer to the *Administrator's Guide for Avaya™ Communication Manager*, 555-233-506.

5. Press ENTER to save your changes.

Some phones have default assignments for buttons. For example, the following figure shows that the 8411D includes defaults for 12 softkey buttons. It already has assignments for features like Leave Word Calling and Call Forwarding.

If you do not use an alias, you can easily assign different features to these buttons if you have different needs.

If you use an alias, you must leave the default softkey button assignments. The system will allow you to change the button assignments on the screen, but the features will not work on the alias phone.

Default softkey assignments for an 8411D phone

```
                                        STATION
SOFTKEY BUTTON ASSIGNMENTS

 1: lwc-store
 2: lwc-cancel
 3: auto-cback
 4: timer
 5: call-fwd    Ext: _____
 6: call-park
 7: date-time
 8: priority
 9: abr-prog
10: abr-spchar  Char: ~p
11: abr-spchar  Char: ~m
12: abr-spchar  Char: ~w
```

Customizing your phone

This section provides recommendations for setting up or enhancing your personal phone. You need a phone that is powerful enough to allow you to use all the features you may give to other employees. You may want to add feature buttons that allow you to monitor or test the system, so that you can troubleshoot the system from your phone.

It will be much easier to monitor and test your system if you have a phone with:

- a large multi-button display (such as 8434D or 8410D)
- a class of service (cos) that has console permissions
- the following feature buttons
  - — ACA and Security Violations (assign to lamp buttons)
  - — Busy verify
  - — Cover message retrieval button
  - — Major/minor alarm buttons
  - — Trunk ID buttons
  - — Verify button

Once you select a phone, you'll want to determine if you want to place this phone at your desk or in the switch room. If the phone is in the switch room (near the system administration terminal), you can quickly add or remove feature buttons to test features and facilities. You may decide that you want a phone at both your desk and in the switch room — it's up to you.

You may also find it handy to set up multiple phones for testing applications and features before you provide them to users. You may want to have a phone that mimics each type of user phone in your organization. For example, if you have four basic phone templates, one for executives, one for marketing, one for technicians, and one for other employees, you may want to have examples of each of these phones so you can test new features or options. Once you are satisfied that a change works on the test phone, you can make the change for all the users in that group.

Upgrading phones

If you want to change phone types for a user and do not need to change locations, you can just access the station screen for that extension and enter the new model number.

Tip:
This method can be used only if the new phone type matches the existing port type (such as digital phone with a digital port).

For example, if a user at extension 4556 currently has a 7410+ phone and you want to replace it with a new 6408D+ phone:

1. Type **change station 4556** and press RETURN.

   The `STATION` screen for 4556 appears.

2. Overwrite `7410+` with **6408D+** in the `Type` field.

   Now you can access the functions and feature buttons that correspond to an 6408D+ phone.

Swapping phones

You will often find that you need to move or swap phones. For example, employees moving from one office to another may want to bring their phones.

In general, to swap one phone (phone A) with another phone (phone B), you change phone A's port assignment to **x**, change phone B's port assignment to A's old port, and, finally, change the **x** for phone A to B's old port. Note that these swapping instructions work only if the two phones are the same type (both digital or both analog, etc.).

NOTE:
You can use Terminal Translation Initialization (TTI) to merge an x-ported extension to a valid port. You can also use Automatic Customer Telephone Rearrangement (ACTR) to unplug certain phones from one location to move them to a new location without additional switch administration. Refer to the *Administrator's Guide for Avaya™ Communication Manager*, 555-233-506, for information about TTI and ACTR.

For example, to swap phones for extension 4567 (port 01C0505) and extension 4575 (port 01C0516), complete the following steps:

1. Type **change station 4567** and press RETURN.
2. Record the current port address (`01C0505`) and type **x** in the `Port` field.
3. Press ENTER to save your changes.
4. Type **change station 4575** and press RETURN.
5. Record the current port address (`01C0516`).
6. Type **01C0505** in the `Port` field.

7. Update the `Room` and `Jack` fields.
8. Press ENTER to save your changes.
9. Type **change station 4567** again and press RETURN.
10. Type **01C0516** in the `Port` field.

    This is the port that used to be assigned to extension 4575.
11. Update the `Room` and `Jack` fields.
12. Press ENTER to save your changes.
13. Physically unplug the phones and move them to their new locations.

Removing phones

Before you physically remove a phone from your system, check the phone's status, remove it from any group or usage lists, and then delete it from the system's memory.

For example, to remove a phone at extension 1234:

1. Type **status station 1234** and press RETURN.

   The `GENERAL STATUS` screen appears.
2. Make sure that the phone:
   - is plugged into the jack
   - is idle (not making or receiving calls)
   - has no messages waiting (message waiting lamp)
   - has no active buttons (such as Send All Calls or Call Forwarding)

3. Type **list groups-of-extension 1234** and press RETURN.

   The `EXTENSION GROUP MEMBERSHIP` screen shows whether the extension is a member of any groups on the system.

4. Press CANCEL.

5. If the extension belongs to a group, access the group screen and delete the extension from that group.

   For example, if extension 1234 belongs to pickup group 2, type **change pickup group 2** and delete the extension from the list.

6. Type **list usage extension 1234** and press RETURN.

   The `USAGE` screen shows whether the extension is used in any vectors, has any bridged appearances, or used as a controller.

7. Press CANCEL.

8. If the extension appears on the `Usage` screen, access the appropriate feature screen and delete the extension.

   For example, if extension 1234 belongs to hunt group 2, type **change hunt group 2** and delete the extension from the list.

9. Type **change station 1234** and press RETURN.

10. Delete any bridged appearances or personal abbreviated dialing entries and press ENTER.

11. Type **remove station 1234** and press RETURN.

    The system displays the station screen for this phone so you can verify that you are removing the correct phone.

Tip:
Be sure to record the port assignment for this jack in case you want to use it again later.

12. If this is the correct phone, press ENTER.

    The system responds with `command successfully completed`.

    If the system responds with an error message, the phone is busy or still belongs to a group. Press CANCEL to stop the request, correct the problem, and enter **remove station 1234** again.

13. Remove the extension from voice mail service if the extension has a voice mailbox.

14. Type **save translations** and press RETURN to save your changes.

Note that you do not need to delete the extension from coverage paths. The system automatically adjusts coverage paths to eliminate the extension.

Now you can unplug the set from the jack and store it for future use. You do not need to disconnect the wiring at the cross-connect field. The extension and port address remain available for assignment at a later date.

Once you successfully remove a set, that set is permanently erased from system memory. If you want to reactivate the set, you have to add it again as though it were a new phone.

Managing features

This section explains how to administer some of the major Avaya™ Communication Manager features. It provides instructions for changing feature parameters, using abbreviated dialing, creating pickup groups, setting up call forwarding, defining coverage paths, and administering bridged call appearances.

Changing feature parameters

You can modify the system parameters that are associated with some of the system features. For example, you can use the system parameters to allow music to play if callers are on hold or to allow trunk-to-trunk transfers on the system.

NOTE:
You can find most of the system-wide parameters on the `FEATURE-RELATED SYSTEM PARAMETERS` screen. However, if you have DEFINITY ECS R6.3.1 or later, some parameters have moved to new screens, such as the `SYSTEM PARAMETERS CALL COVERAGE/CALL FORWARDING` screen.

Generally, Avaya sets your system parameters when your system is installed. However, you can change these parameters as your organization's needs change. For example, let's say that your

company uses call park, where a call can be put on hold and picked up from any other telephone within the system. You need to change the time limit for parked calls from 10 to 5 minutes.

To change the time limit for parked calls:

1. Type **change system-parameters features** and press RETURN.

   The `FEATURE-RELATED SYSTEM PARAMETERS` screen appears.

Feature-Related System Parameters screen

```
                    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): 5
     Off-Premises Tone Detect Timeout Interval (seconds): 20
                              AAR/ARS Dial Tone Required? y
           Music (or Silence) On Transferred Trunk Calls: no
                     DID/Tie/ISDN Intercept Treatment: attd
                Messaging Service Adjunct (MSA) Connected? n
Internal Auto-Answer for Attd-Extended/Transferred Calls? transferred
                Automatic Circuit Assurance (ACA) Enabled? n
           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
```

2. Type **5** in the `Call Park Timeout Interval (minutes)` field and press ENTER to save the change.

   If a parked call is not answered within 5 minutes, the call returns to an attendant or to the user who put the call in park.

Refer to the *Administrator's Guide for Avaya™ Communication Manager*, 555-233-506, for details about changing other feature-related system parameters.

Setting up abbreviated dialing

Abbreviated dialing is sometimes called speed dialing. It allows you to dial a short code in place of an extension or phone number.

When you dial abbreviated-dialing codes or press abbreviated-dialing buttons, you access stored numbers from special lists. These lists can be personal (your list of numbers), group (a department-wide list), system (a system-wide list), or enhanced numbers (allows for a longer list of numbers). The version and type of your system determine which lists are available and how many entries you can have on each list.

NOTE:
Note that this section does not tell you how to administer IP softphones or screenphones. If you need to set up an IP phone, refer to the *Administrator's Guide for Avaya™ Communication Manager*, 555-233-506.

As an example, let's define a new group list:

1. Type **add abbreviated-dialing group next** and press RETURN.

   The `ABBREVIATED DIALING LIST` screen appears. In our example, the next available group list is group 3.

Abbreviated Dialing List screen

```
                          ABBREVIATED DIALING LIST

                             Group List: 3
    Size (multiple of 5): ___       Program Ext: _____   Privileged? _
DIAL CODE
             11: ________________________
             12: ________________________
             13: ________________________
             14: ________________________
             15: ________________________
```

2. Enter a number (in multiples of 5) in the `Size` field. This number defines the number of entries on your dialing list.

   For example, if you have 8 phone numbers you want to store in the list, type **10** in the `Size` field.

3. Enter the phone numbers you want to store, one for each dial code.

   Each phone number can be up to 24 digits long.

4. Press ENTER to save your changes.

You can display your new abbreviated-dialing list to verify that the information is correct or print a copy of the list for your paper records.

Once you define a group list, you need to define which stations can use the list. For example, let's set up station 4567 so it has access to the new group list.

To give station 4567 access to the group list:

1. Type **change station 4567** and press RETURN.

   The `STATION` screen for extension 4567 appears.

2. Press NEXT PAGE to get to the `Abbreviated Dialing List` fields.

Station screen (page 3)

```
                                        STATION
SITE DATA
     Room: _______                                          Headset? n
     Jack: _______                                          Speaker? n
    Cable: _______                                         Mounting? d
    Floor: _______                                      Cord Length: 0
 Building: _______                                        Set Color: ______

 ABBREVIATED DIALING
      List1: group   3__       List2: _________          List3: _________

 HOT LINE DESTINATION
          Abbreviated Dialing List Number (From above 1, 2 or 3): __
                                                          Dial Code: _____

     Line Appearance: _________
```

3. Type **group** in any of the `List` fields and press RETURN.

   A blank list number field appears.

4. Type **3** in the list number field.

   When you assign a group or personal list, you must also specify the personal list number or group list number.

5. Press ENTER to save your changes.

The user at extension 4567 can now use this list by dialing the feature access code for the list and the dial code for the number they want to dial.

Creating pickup groups

A pickup group is a list of phones where each member of the group can answer another member's calls. For example, if you want everyone in the payroll department to be able to answer calls to any payroll extension (in case someone is away from their desk), create a pickup group that contains all of the payroll extensions. Members of a pickup group should be located in the same area so that they can hear when the other extensions in the group ring.

Note that each extension may belong to only one pickup group. Also, the maximum number of pickup groups may be limited by your system configuration.

To create a pickup group:

1. Type **add pickup-group next** and press RETURN.

   The `PICKUP GROUP` screen appears. The system selects the next Group Number for the new pickup group.

2. Enter the extension of each group member.

   Up to 50 extensions can belong to one group.

3. Press ENTER to save your new group list.

   The system automatically completes the name field when you press ENTER to save your changes.

Pickup Group screen

```
                              PICKUP GROUP

          Group Number: __

GROUP MEMBER ASSIGNMENTS

     Ext      Name                        Ext      Name
  1: _____                            14: _____
  2: _____                            15: _____
  3: _____                            16: _____
  4: _____                            17: _____
  5: _____                            18: _____
  6: _____                            19: _____
  7: _____                            20: _____
  8: _____                            21: _____
  9: _____                            22: _____
 10: _____                            23: _____
 11: _____                            24: _____
 12: _____                            25: _____
 13: _____
```


Once you define a pickup group, you can assign call-pickup buttons for each phone in the group or you can give each member the call-pickup feature-access code. Use the `STATION` screen to assign call-pickup buttons.

To allow users to answer calls that are not in their pickup group, you may be able to use Directed Call Pickup. To allow members of one pickup group to answer calls directed to another pickup group, you may be able to add an extended pickup group. For information, refer to the *Administrator's Guide for Avaya™ Communication Manager*, 555-233-506.

Setting up call forwarding

This section explains how to administer various types of automatic call forwarding. To provide call forwarding to your users, assign each extension a Class of Service (COS) that allows call forwarding. Then assign call-forwarding buttons to the user phones (or give them the feature access code for call forwarding) so that they can easily forward calls. You use the station screen to assign the cos and any call-forwarding buttons.

Within each class of service, you can determine whether the users in that cos have the following call forwarding features:

- Call Forwarding All Calls — allows users to redirect all incoming calls to an extension, attendant, or external phone number.
- Call Forwarding Busy/Don’t Answer — allows users to redirect calls only if their extensions are busy or they do not answer.
- Call Fwd-Off Net — prevents users from forwarding calls to numbers that are outside your system network.

As the administrator, you can administer system-wide call-forwarding parameters to control when calls are forwarded. Use the `SYSTEM PARAMETERS CALL COVERAGE/CALL FORWARDING` screen to set the number of times an extension rings before the system redirects the call because the user did not answer (CFWD No Answer Interval). For example, if you want calls to ring 4 times at an extension and then, if the call is not answered, redirect to the forwarding number, set this parameter to 4. Note that this parameter also affects call coverage, so a call rings 4 times at each coverage point.

You also can use the `SYSTEM PARAMETERS CALL COVERAGE/ CALL FORWARDING` screen to determine whether the forwarded-to phone can override call forwarding to allow calls to the forwarded-from phone (Call Forward Override). For example, if an executive forwards incoming calls to an attendant and the attendant needs to call the executive, the call can be made only if Call Forward Override is set to ‘yes’.

To determine which extensions have call forwarding activated:

1. Type **list call-forwarding** and press RETURN.

   This command lists all the extensions that are forwarded along with each forwarding number.

   NOTE:
   If you have a V1, V2, or V3 system, you can see if a specific extension is forwarded only by typing **status station *n***, where ***n*** is the specific extension.

Creating coverage paths

This section explains how to administer various types of call coverage. In general, call coverage refers to what happens to incoming calls. You can administer paths to cover all incoming calls, or define paths for certain types of calls, such as calls to busy phones. You can define where incoming calls go if they are not answered and in what order they reroute to other locations. For example, you can define coverage to ring the called phone, then move to a receptionist if the call is not answered, and finally access a voice mailbox if the receptionist is not available.

With call coverage, the system redirects a call to alternate answering extensions when no one answers at the first extension. An extension can have up to 6 alternate answering points. (If you have an older system, you may have only 3 answering positions.) The system checks each extension in sequence until the call connects. This sequence of alternate extensions is called a coverage path.

The system redirects calls based on certain criteria. For example, you can have a call redirect to coverage without ever ringing on the principal set, or after a certain number of rings, or when one or all call appearances (lines) are busy. You can set coverage differently for internal (inside) and external (outside) calls, and you can define coverage individually for different criteria. For example, you can decide that external calls to busy phones can use the same coverage as internal calls to phones with Do Not Disturb active.

To create a coverage path:

1. Type **add coverage path next** and press RETURN.

   The system displays the next undefined coverage path in the sequence of coverage paths. Our example shows coverage path number 2.

2. Type a coverage path number in the `Next Path` field.

   The next path is optional. It is the coverage path to which calls are redirected if the current path's coverage criteria does not match the call status. If the next path's criteria matches the call status, it is used to redirect the call; no other path is searched.

Coverage Path screen

```
                              COVERAGE PATH

              Coverage Path Number: 2       Hunt after Coverage? n
                  Next Path Number: ____    Linkage:
COVERAGE CRITERIA

    Station/Group Status    Inside Call     Outside Call
              Active?            n               n
                Busy?            y               y
       Don't Answer?             y               y      Number of Rings: 2
                 All?            n               n
 DND/SAC/Goto Cover?             y               y

COVERAGE POINTS

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

3. Fill in the `Coverage Criteria` fields.

   You can see that the default sets identical criteria for inside and outside calls. The system sets coverage to take place for a busy phone, if there is no answer after a certain number of rings, or if the DND (do not disturb), SAC (send all calls), or Go to Cover buttons are pressed or feature-access codes are dialed.

4. Fill in the `Point` fields with the extensions you want for coverage points.

   Each coverage point can be an extension, hunt group, coverage answer group, remote number, vdn, or attendant.

5. Press ENTER to save your changes.

Now assign the new coverage path to a user. For example, let's assign this new coverage path to extension 2054:

1. Type **change station 2054** and press RETURN.

   The `STATION` screen for extension 2054 appears.

2. Type **2** in the `Coverage Path 1` field.

   To give extension 2054 another coverage path, you can type a coverage path number in the `Coverage Path 2` field.

3. Press ENTER to save your changes.

Tip:
If you want to see which extensions or groups use a specific coverage path, type **display coverage sender group *n***, *where n is the coverage path number. For example, you should determine which extensions use a coverage path before you make any changes to it.*

Defining time-of-day coverage

The Time of Day Coverage Table on your system lets you redirect calls to coverage paths according to the time of day and day of the week when the call arrives. You need to define the coverage paths you want to use before you define the time of day coverage plan.

For example, let's say you want to administer the system so that incoming calls to extension 2054 redirect to a coworker in the office from 8:00 a.m. to 5:30 p.m., and to a home office from 5:30 p.m. to 8:00 p.m. on weekdays. You want to redirect the calls to voice mail after 8:00 p.m. weekdays and on weekends.

To set up a time-of-day coverage plan that redirects calls for our example above:

1. Type **add coverage time-of-day next** and press RETURN.

   The system displays the `TIME OF DAY COVERAGE TABLE` and selects the next undefined table number in the sequence of time-of-day table numbers. If this is the first time-of-day coverage plan in your system, the table number is 1.

   Record the table number so that you can assign it to extensions later.

2. To define your coverage plan, enter the time of day and path number for each day of the week and period of time.

Time of Day Coverage Table screen

```
                    TIME OF DAY COVERAGE TABLE

         Act    CVG    Act    CVG    Act    CVG    Act    CVG    Act    CVG
         Time   PATH   Time   PATH   Time   PATH   Time   PATH   Time   PATH
Sun      00:00  3      __:__  _      __:__  _      __:__  _      __:__  _
Mon      00:00  3      08:00  1      17:30  2      20:00  3      __:__  _
Tue      00:00  3      08:00  1      17:30  2      20:00  3      __:__  _
Wed      00:00  3      08:00  1      17:30  2      20:00  3      __:__  _
Thu      00:00  3      08:00  1      17:30  2      20:00  3      __:__  _
Fri      00:00  3      08:00  1      17:30  2      20:00  3      __:__  _
Sat      00:00  3      __:__  _      __:__  _      __:__  _      __:__  _
```

   Enter time in a 24-hour format from the earliest to the latest. For this example, assume that coverage path 1 goes to the coworker, path 2 to the home, and path 3 to voice mail.

   Define your path for the full 24 hours in a day. If you do not list a coverage path for a period of time, the system does not provide coverage for that time.

3. Press ENTER to save your changes.

Now assign the time-of-day coverage to a user. For example, we use extension 2054:

1. Type **change station 2054** and press RETURN.

   The `STATION` screen for extension 2054 appears.

2. Move your cursor to `Coverage Path 1` and type **t** plus the number of the `TIME OF DAY COVERAGE TABLE`.

3. Press ENTER to save your changes.

Now calls to extension 2054 redirect to coverage depending on the day and time that each call arrives.

Creating coverage answer groups

You can create a coverage answer group so that up to eight phones simultaneously ring when calls cover to the group. Anyone in the answer group can answer the incoming call.

To add a coverage answer group:

1. Type **add coverage answer-group next** and press RETURN.

   The `COVERAGE ANSWER GROUP` screen appears.

Coverage Answer Group screen

```
                        COVERAGE ANSWER GROUP

                         Group Number: ____
                           Group Name: COVERAGE_GROUP_

GROUP MEMBER ASSIGNMENTS
   Ext  Name (first 26 characters)   Ext  Name (first 26 characters)
1: ____                              5: ____
2: ____                              6: ____
3: ____                              7: ____
4: ____                              8: ____
```

2. In the `Group Name` field, enter a name to identify the coverage group.
3. In the `Ext` field, type the extensions of each group member.
4. Press ENTER to save you new group list.

   The system automatically completes the `Name` field when you press ENTER.

Defining coverage for calls redirected to external numbers

You can administer the system to allow calls in coverage to redirect to off-net (external) or public-network numbers.

Some systems allow you to send a call to an external phone, but do not monitor the call once it leaves your system. With this remote call coverage, make the external number the last coverage point in a path.

With newer systems you may have the option to use the Coverage of Calls Redirected Off-Net feature. If this feature is active and you use an external number in a coverage path, the system can monitor the call to determine whether the external number is busy or does not answer. If necessary, the system can redirect a call to coverage points that follow the external number. With this feature, you can have a call follow a coverage path that starts at the user's extension, redirects to the user's home phone, and if not answered at home, returns to redirect to their voice mail box.

The call will not return to the system if the external number is the last point in the coverage path.

To use a remote phone number as a coverage point, you need to define the number in the `REMOTE CALL COVERAGE TABLE` and then use the remote code in the coverage path.

For example, to add an external number (303-538-1000) to coverage path 2, complete the following steps:

1. Type **change coverage remote** and press RETURN.

   The `REMOTE CALL COVERAGE TABLE` appears.

2. Type **93035381000** in one of the remote code fields.

   If you use a digit to get outside of your network, you need to add the digit before the external number. In this example, the system requires a ‘9’ to place outside calls.

Remote Call Coverage Table screen

```
                          REMOTE CALL COVERAGE TABLE
01: 93035381000_____      16: _______________      31: _______________
02: _______________       17: _______________      32: _______________
03: _______________       18: _______________      33: _______________
04: _______________       19: _______________      34: _______________
05: _______________       20: _______________      35: _______________
06: _______________       21: _______________      36: _______________
07: _______________       22: _______________      37: _______________
08: _______________       23: _______________      38: _______________
09: _______________       24: _______________      39: _______________
10: _______________       25: _______________      40: _______________
11: _______________       26: _______________      41: _______________
12: _______________       27: _______________      42: _______________
13: _______________       28: _______________      43: _______________
14: _______________       29: _______________      44: _______________
15: _______________       30: _______________      45: _______________
```

3. Be sure to record the remote code number you use for the external number.

   In this example, the remote code is r01.

4. Press ENTER to save your changes.

5. Type **change coverage path 2** and press RETURN.

   The `COVERAGE PATH` screen appears.

Tip:
Before making changes, you can use **display coverage sender group 2** *to determine which extensions or groups use path 2.*

Coverage Path screen

```
                              COVERAGE PATH
                     Coverage Path Number: 2
                                                Hunt after Coverage? n
                         Next Path Number: ____ Linkage:
COVERAGE CRITERIA
    Station/Group Status    Inside Call     Outside Call
              Active?           n               n
                Busy?           y               y
       Don't Answer?            y               y    Number of Rings: 2
                 All?           n               n
 DND/SAC/Goto Cover?            y               y

COVERAGE POINTS

 Terminate to Coverage Pts. with Bridged Appearance? __
   Point1: 4104             Point2: r01_                Point3: h77_
   Point4: ____             Point5: ____                Point6: ____
```

6. Type **r01** in a coverage `Point` field.

   In this example, the coverage rings at extension 4101, then redirects to the external number. If you administer Coverage of Calls Redirected Off-Net and the external number is not answered or is busy, the call redirects to the next coverage point. In this example, the next point is Point3 (h77 or hunt group 77).

   If you do not have the Coverage of Calls Redirected Off-Net feature, the system cannot monitor the call once it leaves the network. The call ends at the remote coverage point.

7. Press ENTER to save your changes.

Defining telecommuting coverage

Telecommuting access allows users to change their lead-coverage path or call-forwarding destination no matter where they are. You need to set up coverage paths and assign security codes before telecommuting coverage will work.

To see if telecommuting coverage is enabled on your system, make sure the Feature Access Codes screen contains the correct codes.

1. Type **display feature-access codes** and press RETURN.

   The `FEATURE ACCESS CODES` screen appears. Make sure codes are in these fields:

   - Change Coverage Access Code
   - Extended Call Fwd Activate Busy D/A, All, and Deactivation

   Telecommuters use these codes to dial into the system.

Your users can make remote changes to coverage when the Class of Restriction (COR) screen assigned to their phones has a **y** in the `Can Change Coverage` field. Users can make remote changes to call forwarding when the Class of Service (COS) assigned to their phones has a **y** in the `Extended Forwarding All` and `Extended Forwarding B/DA` fields. Display the cor and cos screens with the **display** command.

Make sure that `Coverage Path 1` and `Coverage Path 2` fields are completed on each station screen assigned to people using telecommuting access. The security code field on the station screen must also be completed.

Tip:
*If the security code has been assigned, a * appears in the* `Security Code` *field on the station screen.*

To allow users remote access to the system:

1. Type **change telecommuting-access** and press RETURN.
2. Enter the extension that you want remote users to use to access the system.

   All remote users dial this same extension.
3. Press ENTER to save your changes.

If the `Telecommuting Access Extension` is left blank, you disable the feature for all users.

SECURITY ALERT:
Invalid extensions and station security codes are logged as security violations. See the Administrator's Guide for Avaya™ Communication Manager, 555-233-506, for information on security violations.

Setting up bridged call appearances

Think of a bridged call appearance as a phone (the primary set) with an extension (the bridged-to appearance). Both phones can be used to call in and out and both show when a line is in use. A call to the primary phone is bridged to a specific appearance, or button, on the secondary phone. The secondary phone retains all its functions, and a specific button is dedicated as the bridged-to appearance from the primary phone.

Bridged call appearances have to be assigned to phones with double-lamp buttons, or lights. The phone types do not need to match, but as much consistency as possible is recommended for all phones in a bridged group. When a call comes in on bridged phones, the buttons assigned to the bridged appearances flash. You can assign as many bridged appearances as there are line appearances on the primary phone, and you can assign ringing (alerting) to one or more of the phones.

To create a bridged call appearance:

1. Note the extension of the primary phone.

   A call to this phone lights the button and, if activated, rings at the bridged-to appearance on the secondary phone.

2. If you want to use a new phone for the bridged-to extension, duplicate a station (see "Managing phones" on page 47).

3. Type **change station** and the bridged-to extension and press RETURN.

   The STATION screen appears.

Station screen

```
                                    STATION
FEATURE OPTIONS
           LWC Reception? _______        Auto Select Any Idle Appearance? _
          LWC Activation? _                     Coverage Msg Retrieval? _
  LWC Log External Calls? _                              Auto Answer? ____
            CDR Privacy? _                            Data Restriction? _
   Redirect Notification? _                  Idle Appearance Preference? _
 Per Button Ring Control? _
   Bridged Call Alerting? _                    Restrict Last Appearance? _
  Active Station Ringing: ______

        H.320 Conversion? y        Per Station CPN - Send Calling Number? y
      Service Link Mode: as-needed
        Multimedia Mode: basic                  Audible Message Waiting? _
    MWI Served User Type: ______              Display Client Redirection? n
                                            Select Last Used Appearance? n
                                              Coverage After Forwarding? s
                                                Multimedia Early Answer? n
      IP Emergency Calls: _________       Direct IP-IP Audio Connections? _
  Emergency Location Ext: ________                  IP Audio Hairpinning? _
```

4. Press NEXT PAGE until `Per Button Ring Control` appears (digital sets only).
   - If you want to assign ringing separately to each bridged appearance, type **y**.
   - If you want all bridged appearances to either ring or not ring, leave the default **n**.
5. Move to `Bridge Call Alerting`.

   If you want the bridged appearance to ring when a call arrives at the primary phone, type **y**. Otherwise, leave the default **n**.
6. Complete the appropriate field for your phone type.

If. . .	**Then. . .**
your primary phone is analog	move to the `Line Appearance` field and enter **abrdg-appr**
your primary phone is digital	move to the `Button Assignments` field and enter **brdg-appr**

7. Press RETURN.

   `Btn` and `Ext` fields appear. If `Per Button Ring Control` is set to **y** on the digital screen, `Btn`, `Ext`, and `Ring` fields appear.

Station screen (analog set)

```
                                        STATION
 SITE DATA
      Room: _______                                          Headset? n
      Jack: _______                                          Speaker? n
     Cable: _______                                         Mounting? d
     Floor: _______                                      Cord Length: 0
  Building: _______                                        Set Color: ______

ABBREVIATED DIALING
     List1: _________          List2: _________          List3: _________

HOT LINE DESTINATION

         Abbreviated Dialing List Number (From above 1, 2 or 3):
                                                        Dial Code:
      Line Appearance:  brdg-appr   Btn:     Ext:
```

Station screen (digital set)

```
                                        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: brdg-appr  Btn:   Ext:      Ring:
      1: brdg-appr  Btn:   Ext:      Ring:
```

8. Enter the primary phone's button number that you want to assign as the bridged call appearance.

   This button flashes when a call arrives at the primary phone.

9. Enter the primary phone extension.

10. If the Ring field appears:
    - If you want the bridged appearance to ring when a call arrives at the primary phone, type **y**.
    - If you do not want the bridged appearance to ring, leave the default **n**.
11. Press ENTER to save your changes.

To see if an extension has any bridged call appearances assigned, type **list bridge** and the extension, and press RETURN.

Routing outgoing calls

This section describes how Avaya™ Communication Manager routes outbound calls and how you can modify call routing. It also provides instructions for creating partitions and setting authorization codes.

NOTE:
This information represents digit analysis information for DEFINITY ECS R7 or later. If you have an earlier version, you will notice somewhat different fields on your screens.

World class routing

Your system uses world class routing to direct an outgoing call. There are two types of routing:

- Automatic Alternate Routing (AAR) is used for calls within your company over your own private network.
- Automatic Route Selection (ARS) is used for calls that go outside your company over public networks. ARS is also used to route calls to remote company locations if you do not have a private network.

This section describes only ARS call routing. If you do not use ARS routing, this information does not apply to your system.

Understanding ARS analysis

With ARS, the switch routes outgoing calls based on the dialed digits and the calling privileges of the caller. Your system uses an ARS Digit Analysis Table to determine how to handle the dialed digits and uses Class of Restriction (COR) and Facility Restriction Level (FRL) to determine the calling privileges.

Let's look at a very simple `ARS DIGIT ANALYSIS TABLE`. (Your system likely has more defined dialed strings than our example.)

ARS Digit Analysis Table screen

```
                    ARS DIGIT ANALYSIS TABLE
                  Location: all                    Percent Full:    6
     Dialed        Total    Route      Call     Node     ANI
     String        Mn Mx   Pattern     Type     Num      Rq
1______________    1  1     12         svcl     ___      n
1______________    11 11    30         fnpa     ___      n
1______________    12 23    17         intl     ___      n
10xxx__________    5  5     deny       op       ___      n
1800___________    11 11    30         fnpa     ___      n
2______________    7  7     2          hnpa     ___      n
3______________    7  7     2          hnpa     ___      n
4______________    7  7     2          hnpa     ___      n
5______________    7  7     2          hnpa     ___      n
6______________    7  7     2          hnpa     ___      n
7______________    7  7     2          hnpa     ___      n
8______________    7  7     2          hnpa     ___      n
911____________    3  3     1          emer     ___      n
976____________    11 11    deny       fnpa     ___      n
```

This `ARS DIGIT ANALYSIS TABLE` is used for all locations in this system. The far-left column of the `ARS DIGIT ANALYSIS TABLE` lists the first digits in the dialed string. When a user makes an outgoing call, the system analyzes the digits, looks for a match in the table, and uses the information in the matching row to determine how to route the call.

Let's say a caller places a call to 1 303 233 1000. The switch matches the dialed digits with those in the first column of the table. In this example, the dialed string matches the '1'. Then the systems matches the length of the entire dialed string (11 digits) to the minimum and maximum length columns. In our example, the 11-digit call that started with 1 follows route pattern 30 as an `fnpa` (long distance) call.

NOTE:
For a list of all valid entries for the various fields and what those entries mean, see the *Administrator's Guide for Avaya™ Communication Manager*, 555-233-506.

Tip:
The first dialed digit for an external call is often an access code. If '9' is defined as the ARS access code, the switch drops this digit and analyzes the remaining digits with the `ARS DIGIT ANALYSIS TABLE`.

Managing calling privileges

Each time you set up a phone, you use the station screen to assign a COR. You can create a different COR for different groups of users. For example, you may want executives in your company to have different calling privileges than receptionists.

When you set up a COR, you specify a facility restriction level (FRL) on the class of restriction screen. The FRL determines the calling privileges of the user. Facility restriction levels are ranked from 0–7, where 7 has the highest level of privileges.

You also assign an FRL to each route pattern preference in the route pattern screen. When a user makes a call, the system checks the user's COR. The call is allowed if the caller's FRL is higher than or equal to the route pattern preference's FRL.

Displaying ARS analysis information

You'll want to become familiar with how your system currently routes outgoing calls. To display the `ARS DIGIT ANALYSIS TABLE` that controls how the system routes calls that begin with 1:

1. Type **display ars analysis 1** and press RETURN.

   The `ARS DIGIT ANALYSIS TABLE` for dialed strings that begin with 1 appears. Note that the switch displays only as many dialed strings as can fit on one screen at a time.

To see all the dialed strings that are defined for your system, run an `ARS DIGIT ANALYSIS REPORT`:

1. Type **list ars analysis** and press RETURN.

   The `ARS DIGIT ANALYSIS REPORT` appears. You may want to print this report to keep in your paper records.

Modifying call routing

If your system uses ARS Digit Analysis to analyze dialed strings and select the best route for a call, you must change the digit analysis table to modify call routing. For example, you'll need to update this table to add new area codes or to restrict users from calling specific areas or countries.

Adding a new area code or prefix

A common task for system administrators is to configure their system to recognize new area codes or prefixes.

Tip:
If your local area code is changing or splitting, call the Communication Manager helpline and have them walk you through all the changes needed to have your system recognize the new area code.

When you want to add a new area code or prefix, you look up the settings for the old area code or prefix and enter the same information for the new one.

Let's add a new area code. When the California area code 415 split and portions changed to 650, you'll need to add this new area code to your system.

Tip:
*If you do not need to use 1 for area code calls, omit the **1** in steps 1, 3, and 5 in our example. Also, enter **10** in the Total Min and Total Max fields (instead of 11) in step 6.*

To add this non-local area code:

1. Type **list ars route-chosen 14152223333** and press RETURN.

   You can use any 7-digit number after 1 and the old area code (415). We used 222-3333.

   The `ARS ROUTE CHOSEN REPORT` screen appears.

ARS Route Chosen Report screen

```
                    ARS ROUTE CHOSEN REPORT
Location: 1                Partitioned Group Number:  1

  Dialed        Total      Route    Call    Node        Location
  String     Min    Max   Pattern   Type   Number

  141        11     11      30      fnpa                all
```

2. Write down the `Total Min`, `Total Max`, `Route Pattern`, and `Call Type` values from this screen.

   In this example, the `Total Min` is `11`, `Total Max` is `11`, `Route Pattern` is `30`, and the `Call Type` is `fnpa`.

3. Type **change ars analysis 1650** and press RETURN.

   Type **1** and the new area code (**650**). The `ARS DIGIT ANALYSIS TABLE` screen appears.

ARS Digit Analysis Table

```
                      ARS DIGIT ANALYSIS TABLE
            Location: all                          Percent Full:   6
     Dialed           Total    Route      Call      Node      ANI
     String           Mn Mx   Pattern     Type      Num       Rq
1_______________      11 11      30       fnpa      ___       n
167_____________      11 11      30       fnpa      ___       n
1650____________      11 11      2        fnpa      ___       n
1800____________      11 11      30       fnpa      ___       n
2_______________      7  7       2        hnpa      ___       n
3_______________      7  7       2        hnpa      ___       n
4_______________      7  7       2        hnpa      ___       n
5_______________      7  7       2        hnpa      ___       n
7_______________      7  7       2        hnpa      ___       n
8_______________      7  7       2        hnpa      ___       n
911_____________      3  3       1        emer      ___       n
976_____________      11 11      deny     hnpa      ___       n
```

4. Use the arrow keys to move to a blank `Dialed String` field.

   If the dialed string is already defined in your system, the cursor appears in the appropriate `Dialed String` field, where you can make changes.

5. Enter **1650** in the `Dialed String` field.
6. Enter the minimum and maximum values from step 2 in the `Total Mn` and `Total Mx` fields.

   In our example, enter **11** in each field.

7. Enter the route pattern from step 2 in the `Route Pattern` field.

   In our example, enter **30**.

8. Enter **fnpa** in the `Call Type` field.
9. Enter the node number from step 2 in the `Node Num` field.

   For our example, you would leave the node number blank.

10. Press ENTER to save your changes.

To add a new prefix, follow the same directions, except use a shorter dial string (such as **list ars route-chosen 2223333**, where **222** is the old prefix) and a dial type of **hnpa**.

Using ARS to restrict outgoing calls

ARS allows you to block outgoing calls to specific dialed strings. For example, administrators in the United States may want to restrict users from making calls to 900 and 976 pay-per-call numbers or calls to countries where they do not do business.

SECURITY ALERT:

To prevent toll fraud, deny calls to countries where you do not do business. The following countries are currently concerns for fraudulent calling.

country	code	country	code
Colombia	57	Pakistan	92
Ivory Coast	225	Peru	51
Mali	23	Senegal	221
Nigeria	234	Yemen	967

To prevent callers from placing calls to Colombia (57):

1. Type **change ars analysis 01157** and press RETURN.

   You enter **011** (international access) and the country code (**57**). The `ARS DIGIT ANALYSIS TABLE` screen appears.

2. Use the arrow keys to move to a blank `Dialed String` field on the right of the screen.

   If the dialed string is already defined in your system, the cursor appears in the appropriate `Dialed String` field. Skip to step 5 to deny calls to this dialed string.

3. Enter **01157** in the `Dialed String` field.

4. Enter **10** in the `Total Mn` and **23** in `Total Mx` fields.

5. Enter **den** (denied) in the `Route Pattern` field.

6. Enter **intl** in the `Call Type` field.

7. Press ENTER to save your changes.

Overriding call restrictions

You can use authorization codes to enable callers to override a station's calling privileges. For example, you can give a supervisor an authorization code so they can makes calls from a phone that is usually restricted for these calls. Since each authorization code has its own COR, the system uses the COR assigned to the authorization code (and FRL assigned to the COR) to override the privileges associated with the employee's phone.

Note that authorization codes do not override route patterns that are denied. For example, if your ARS tables restrict users from placing calls to Colombia, a caller cannot override the restriction with an authorization code.

Tip:
Authorization codes are optional. To see if authorization codes are enabled on your system, use **display system-parameters customer-options**.

SECURITY ALERT:
You should make authorization codes as long as possible to increase the level of security. Set the length of authorization codes on the `FEATURE-RELATED SYSTEM PARAMETERS` *screen.*

Let's create an authorization code 4395721with a COR of 2.

1. Type **change authorization-code 4395721** and press RETURN.

   The `AUTHORIZATION CODE - COR MAPPING` screen appears.

2. In the `AC` field, type **4395721**.

3. In the COR field, enter **2**.
4. Press ENTER to save your changes.

Authorization Code - COR Mapping screen

```
                    Authorization Code - COR Mapping
         NOTE: 2 codes administered. Use 'list' to display all codes.

AC       COR  AC       COR  AC       COR  AC       COR  AC       COR  AC       COR
9260839  3    ________ __   ________ __   ________ __   ________ __   ________ __
2754609  4    ________ __   ________ __   ________ __   ________ __   ________ __
________ __   ________ __   ________ __   ________ __   ________ __   ________ __
________ __   ________ __   ________ __   ________ __   ________ __   ________ __
________ __   ________ __   ________ __   ________ __   ________ __   ________ __
```

ARS Partitioning

Most companies want all their users to be able to make the same calls and follow the same route patterns. However, you may find it helpful to provide special calling permissions or restrictions to a group of users or to particular phones.

NOTE:
If you used partitioning on an Avaya software release prior to R7 and you want to continue to use partitioning, please read this section carefully. The process for setting up partitioning has changed significantly.

Tip:
Partitioning is an optional feature. Use **display system-parameters customer-options** *to see if Partitioning is set to* y *and Time of Day Routing is set to* n*. If Time of Day Routing is* y *on System Parameters Customer Options, you specify the partition group number (PGN) on the Time of Day Routing Plan screen. Refer to the Administrator's Guide for Avaya™ Communication Manager, 555-233-506.*

You can use ARS partitioning to change the call routing plan for up to 8 different user groups within a single system. You assign a Partition Group Number (PGN) to each user group and identify different call routing treatments for each PGN.

Setting up a partition group

Let's say you allow your employees to make local, long distance, and emergency calls. However, you have a lobby phone for visitors and you want to allow users to make only local, toll-free, and emergency calls from this phone.

To restrict the lobby phone, you modify the routing for a partition group to enable only specific calls, such as U.S.-based toll-free 1 800 calls, and then assign this partition group to the lobby phone.

To enable 1 800 calls for partition group 2:

1. Type **list ars route-chosen 18002221000** and press RETURN.

   You can use any 7-digit number following the **1800** to create an example of the dialed string. The `ARS ROUTE CHOSEN REPORT` for partition group 1 appears.

ARS Route Chosen Report screen

```
                         ARS ROUTE CHOSEN REPORT

      Location :  1                     Partitioned Group Number: 1

          Dialed            Total     Route      Call      Node     Location
          String           Min  Max  Pattern     Type      Number

  1800____________________   11 11     p1___       fnpa      _____      all
```

routing

2. Record the route pattern for the selected dialed string.

   In our example, the route pattern for 1800 is `p1`. This indicates that the system uses the `PARTITION ROUTING TABLE` to determine which route pattern to use for each partition.

   NOTE:
   If there is a number (with no p) under `Route Pattern` on the `ROUTE CHOSEN REPORT`, then all partitions use the same route pattern. You need to use the `PARTITION ROUTING TABLE` only if you want to use different route patterns for different partition groups.

3. Press CANCEL to return to the command prompt.

4. Type **change partition-route-table index 1** and press RETURN.

   The `PARTITION ROUTING TABLE` screen appears. In our example, partition group 1 can make 1800 calls and these calls use route pattern 30.

Partition Routing Table screen

```
                         Partition Routing Table

                            Routing Patterns
Route
Index   PGN 1   PGN 2   PGN 3   PGN 4   PGN 5   PGN 6   PGN 7   PGN 8
-----   -----   -----   -----   -----   -----   -----   -----   -----
  1     __30    __30    deny    ____    ____    ____    ____    ____
  2     ____    ____    ____    ____    ____    ____    ____    ____
  3     ____    ____    ____    ____    ____    ____    ____    ____
  4     ____    ____    ____    ____    ____    ____    ____    ____
  5     ____    ____    ____    ____    ____    ____    ____    ____
  6     ____    ____    ____    ____    ____    ____    ____    ____
  7     ____    ____    ____    ____    ____    ____    ____    ____
```

5. In the `PGN 2` column that corresponds to `Route Index 1`, type **30** and press ENTER.

   This tells the system to use route pattern 30 for partition group 2 and allow partition group 2 members to make calls to 1800 numbers.

Assigning a phone to a partition group

To assign an extension to a partition group, you have to first assign the partition group to a class of restriction (COR) and then assign that COR to the extension.

To assign a class of restriction (COR) to partition group 2.

1. Type **list cor** and press RETURN.

   The `CLASS OF RESTRICTION INFORMATION` screen appears.

Class of Restriction Information screen

```
CLASS OF RESTRICTION INFORMATION

    COR   COR Description
     0
     1     supervisor
     2     telecommuting
     3
```

2. Choose a COR that has not been used and press CANCEL.

   In our example, select **3**.

3. Type **change cor 3** and press RETURN.

   The `CLASS OF RESTRICTION` screen appears.

routing

Class of Restriction screen

```
                                CLASS OF RESTRICTION
                 COR Number: 3
            COR Description: lobby

                        FRL: 0                                APLT? y
   Can Be Service Observed? n           Calling Party Restriction: none
 Can Be A Service Observer? n            Called Party Restriction: none
         Time of Day Chart: _       Forced Entry of Account Codes? n
          Priority Queuing? n                Direct Agent Calling? n
      Restriction Override: none       Facility Access Trunk Test? n
      Restricted Call List? n                 Can Change Coverage? n

             Access to MCT? y            Fully Restricted Service? n
      Category For MFC ANI: 7
          Send ANI for MFE? n_            Add/Remove Agent Skills? n
             MF ANI Prefix: ______        Automatic Charge Display? n
 Hear System Music on Hold? y   PASTE (Display PBX Data on Phone)? n
                         Can Be Picked Up By Directed Call Pickup? n
                                     Can Use Directed Call Pickup? n
                                     Group Controlled Restriction: inactive
```

4. Type a name for this COR in the `COR Description` field.

   In our example, type **lobby**.

5. Enter **2** in the `Partition Group Number` field.

   Tip:
   The Partition Group Number field appears only when Time of Day Routing is **n** *on the System Parameters Customer Options screen. Otherwise, you specify the partition group number (PGN) on the Time of Day Routing Plan screen. For information on Time of Day Routing, refer to the Administrator's Guide for Avaya™ Communication Manager, 555-233-506.*

6. Press ENTER to save your changes.

Now assign COR 3 to the lobby phone at extension 1234:

1. Type **change station 1234** and press RETURN.

   The STATION screen for extension 1234 appears.

2. In the COR field, type **3**.
3. Press ENTER to save your changes.

Enhancing system security

This section explains how to add and modify user logins. It also provides an introduction to phone system security issues. It describes possible security problems you should be aware of and gives you instructions for detecting these problems.

Tip:
If your organization has not yet completed the Service Agreement Indemnity Enhancement Certification, we highly recommend that you call the Security Hotline at the World-class Customer Service Center (1 800 643 2353) and ask how to become certified. When you complete this certification and administer your system according to Avaya's fraud prevention requirements, Avaya will indemnify your organization for charges associated with toll fraud.

Assigning and changing users

The system allows you to add or change user logins as needed. When you want to add or change a login, remember the following system security requirements:

- a login must be 3 to 6 alphanumeric characters in length
- a password must be from 4 to 11 alphanumeric characters in length and contain at least one non-alphabetic character

NOTE:
To create or change logins, you must log in as a superuser with administrative permissions.

Assigning new logins and passwords

As you work as an administrator, you may be fortunate enough to have help administering your switch or you may want to have an assistant make changes to the switch while you are out of the office. In these cases, you should set up a new user in the system and limit what this individual can do. As you'll see, adding logins is very easy.

Tip:
You increase system security when you choose the longest possible password with a mix of lowercase and uppercase numbers and letters.

The following example shows you how to add a new login called `angi3` with a password of `b3stm0m`.

To add this user and password, log in with a superuser ID and complete the following steps:

1. Type **add login angi3** and press RETURN.

   Use the new login name as part of the **add** command.

   The `LOGIN ADMINISTRATION` screen appears. The `Login's Name` field shows the name you typed in the **add** command; other fields contain defaults.

Login Administration screen

```
                              LOGIN ADMINISTRATION

         Password of Login Making Change:

         LOGIN BEING ADMINISTERED
                            Login's Name: angi3
                              Login Type: customer
                           Service Level: non-super-user
    Disable Following a Security Violation? y         Access to INADS Port? n

          LOGIN'S PASSWORD INFORMATION
                        Login's Password:
                 Reenter Login's Password:
     Password Aging Cycle Length (Days):

     LOGOFF NOTIFICATION
     Facility Test Call Notification? y     Acknowledgment Required? y
          Remote Access Notification? y     Acknowledgment Required? y
```

2. Complete the following fields:

   - `Password of Login Making Change`

     This is *your password*.

   - `Login's Password`

     Assign an initial password for the new login. We'll type in **b3stm0m** as part of our example. The password does not appear on the screen as you type.

   - `Reenter Login's Password`

     Retype password **b3stm0m**. The password does not appear on the screen as you type.

3. Press ENTER to save your changes.

security

Setting login permissions

Once you add the new user, you should review the user's command permissions and modify them, if necessary.

To review command permissions for our new example login:

1. Type **change permissions angi3** and press RETURN.

   Use the new login name as part of the **change** command. The `COMMAND PERMISSION CATEGORIES` screen appears.

Command Permission Categories screen

```
                         COMMAND PERMISSION CATEGORIES
                           Login Name: angi3
COMMON COMMANDS
              Display Admin. and Maint. Data? n
                          System Measurements? n
              System Mgmt Data Transfer Only? n

ADMINISTRATION COMMANDS
         Administer Stations? n                 Administer Features? n
           Administer Trunks? n              Administer Permissions? n
     Additional Restrictions? n

MAINTENANCE COMMANDS
            Maintain Stations? n       Maintain Switch Circuit Packs? n
              Maintain Trunks? n      Maintain Process Circuit Packs? n
              Maintain System? n
```

2. If you want the default permissions, press CANCEL.
3. If you want to change any permissions, enter **y** to give the user access or **n** to restrict access for each permission type.
4. Press ENTER to save your changes.

Changing passwords

You should change your passwords often.

Tip:
To force users to change passwords, set password aging in the Login Administration screen. See "Changing logins" *for instructions.*

To change the password (`b3stm0m`) for `angi3`:

1. Type **change password angi3** and press RETURN.

   The `PASSWORD ADMINISTRATION` screen appears.

Password Administration screen

```
                                PASSWORD ADMINISTRATION

Password of Login Making Change:

LOGIN BEING CHANGED
                      Login Name: angi3

LOGIN'S PASSWORD INFORMATION
                Login's Password:
        Reenter Login's Password:
```

2. Complete the following fields:
   - `Password of Login Making Change`

     This is *your password* that you used to log into the session.
   - `Login Name`
   - `Login's Password`
   - `Reenter Login's Password`
3. Press ENTER to save your changes.

security

Changing logins

Occasionally you'll need to change permissions for a user's login. For example, you may want to change a login so that the user must change their password every 30 days (a good rule of thumb).

To change the password aging for our new login, `angi3`:

1. Type **change login angi3** and press RETURN.

   The `LOGIN ADMINISTRATION` screen appears with the current information for `angi3`.

2. Type **30** in the `Password Aging Cycle Length (Days)` field.

3. Press ENTER to save your changes.

Preventing toll fraud

An important role for every administrator is to manage the security of their phone system. You need to make every effort to ensure that your phone system is not open to toll fraud. Toll fraud is the unauthorized use of telephone features and services and the theft of long distance service. When toll fraud occurs, your company is responsible for charges.

For more information on system security and preventing toll fraud, we recommend you obtain the *Avaya Products Security Handbook*, 555-025-600, and use it often, or call your Center of Excellence.

SECURITY ALERT:

When you suspect toll fraud, call the Security Hotline immediately (1 800 643 2353) or contact your Avaya representative.

Top 11 tips to help prevent toll fraud

You can reduce your company's risk of toll fraud by following a few important guidelines.

1. Protect system administration from unauthorized access.

   Make sure all system administration and maintenance logins are secure. Change your passwords frequently.

2. Deny unauthorized remote access.

   If you do not use remote access, disable all its related features. If you use remote access, require barrier codes and set your authorization codes, if applicable, at the maximum length. Also, change these codes frequently.

3. Restrict individual ability to make international calls.

   Set up class of restriction groups to allow only certain people to call international numbers required for your business.

4. Protect access to information stored in voice mail.

   Require passwords for access to voice mailboxes. Use complicated passwords and change the passwords regularly.

5. Deny any transfer from a voice mail system to a dial tone.

   Place restrictions on the ports that allow access to and from your voice mail system. Activate "secure transfer" features in voice mail systems.

6. Use system software to intelligently control call routing.

   Set up your system to control how each call is handled or routed. If possible, use time-of-day routing to limit the use of your system during off hours.

7. Place protection on systems that ask callers to dial digits.

   Restrict certain users' access to dial tone. Restrict the digit combinations dialed at prompts.

8. Monitor traffic and system activity for suspicious call patterns.

   Use your traffic reports and call detail records to monitor call activity. Activate features that deny access to your system when unauthorized attempts are detected.

9. Provide physical security for telecommunications assets.

   Restrict unauthorized access to equipment rooms and wire connection closets. Keep translation backups, system manuals, and reports in a safe place.

10. Educate system users to recognize toll fraud activity and react appropriately.

    Train your users how to protect themselves from inadvertent compromises to system security.

11. Monitor call traffic over vectors.

    Vector fraud is one of the most common types of toll fraud because vectors route calls based on the Class of Restriction (COR) assigned to the VDN. Refer to *Avaya Products Security Handbook*, 555-025-600, or your Avaya representative for more information.

Using reports to detect problems

Call Detail Recording

Call Detail Recording (CDR) collects detailed information about calls handled by your system. This CDR information can be sent directly to a printer or into call accounting software. You can use the printed CDR output or call accounting reports to monitor calls on your system and look for possible toll fraud problems.

Review your call accounting reports or CDR output each day to help detect possible toll fraud. When reviewing these records, look for:

- unusual calling patterns
  - numerous calls to the same number
  - calls outside of normal business hours
  - long calls
- calls to suspicious destinations, including international calls not typical for your business
- patterns of authorization code usage (same code used simultaneously or high activity)
- high numbers of “ineffective call attempts” indicating attempts at entering invalid codes
- undefined account codes
- attempts to change the access code or to use an invalid access code when using conferencing features.

If you are unfamiliar with reading CDR printed output, you’ll want to refer to the description of CDR in the *Administrator’s Guide for Avaya™ Communication Manager*, 555-233-506.

If your organization uses call accounting software to analyze your CDR output, you probably receive formatted reports that list the information you need to detect possible toll fraud. If you have questions about reading your call accounting reports, refer to your call accounting software manuals.

Security Violations Notification

You can administer Security Violations Notification so that the system notifies you and provides reports when users enter invalid information. You want to know about the following types of violations, which may indicate an attempt to breach your security:

- login violations
- remote access barrier code violations
- authorization code violations
- station security code violations

For example, let's have the system notify us at extension 8000 when someone tries to enter more than 3 invalid authorization codes within a 1-minute time span.

To set up Security Violations Notification for our example:

1. Type **change system-parameters security** and press RETURN.

   The `SECURITY-RELATED SYSTEM PARAMETERS` screen appears.

Security-Related System Parameters screen

```
                         SECURITY-RELATED SYSTEM PARAMETERS

SECURITY VIOLATION NOTIFICATION PARAMETERS

 SVN Login Violation Notification Enabled? n


 SVN Remote Access Violation Notification Enabled? n


SVN Authorization Code Violation Notification Enabled? y
       Originating Extension: _____      Referral Destination: 8000
Authorization Code Threshold: 3_               Time Interval: 0:01
      Announcement Extension: _____
```

2. In the `SVN Authorization Code Violation Notification Enabled` field, type **y** and press RETURN.

   Additional fields now display on the screen.

3. In the `Originating Extension` field, type the extension you want the system to use to originate the call.

   Use the extension of an unused non-dial station.

4. Type **8000** in the `Referral Destination` field.

   Use the extension you want the system to notify.

5. If the referral destination is on a different system or is a non-display phone, fill in the `Announcement Extension` field.

6. Type **3** in the `Authorization Code Threshold` field.

   Enter the maximum number of invalid entry attempts you want to allow.

7. Type **0:01** (1 minute) in the `Time Interval` field.

   Use an hour:minute format for the amount of time you want the system to use for the monitor interval.

8. Press ENTER to save your changes.

Viewing security reports

Your system generates two types of Security Violations reports:

- `SECURITY VIOLATIONS DETAIL` report — displays the number of successful and failed login attempts by login ID.
- `SECURITY VIOLATIONS SUMMARY` report — displays valid and failed access attempts, as well as security violations for logins, authorization codes, barrier codes, and station security codes.

To display a `SECURITY VIOLATIONS DETAIL` report and see a list of login data:

1. Type **list measurements security-violations detail** and press RETURN.

To display a `SECURITY VIOLATIONS SUMMARY` report:

1. Type **list measurements security-violations summary** and press RETURN.

Printing security reports

You may want to keep a paper copy of a Security Violations report to monitor security trends for a specific time period.

To print a `SECURITY VIOLATIONS SUMMARY` report to the slave printer associated with the administration terminal:

1. Type **list measurements security-violations summary print** and press RETURN.

To print a `SECURITY VIOLATIONS SUMMARY` report to the system printer:

1. Type **list measurements security-violations summary schedule** and press RETURN.

   The system prompts whether you want to print the report immediately or schedule to print it later.

2. Type the appropriate `Print Interval` and press ENTER to send the report.

Clearing security reports

Once you review the security measurement reports, you may want to clear the current measurements and reset the `Counted Since` field.

To clear measurements for security violations and reset the counter:

1. Type **clear measurements security-violations** and press RETURN.

Keeping records

Record keeping plays a vital role in system administration. Your records should provide a current status of what hardware and features are installed on your system. Your records also help you determine which phone features are available for your users.

Whether you are the administrator of a new or existing switch, follow your own company policy concerning keeping records. We have included the information below only as a guide. Our list contains different types of information for you to consider, but you need to determine which method of record keeping works best for you and your organization.

Paper records

Your switch keeps an electronic record of your system configuration and any changes you make.

A common method for keeping paper records is to print copies of screens and reports so you have backup copies of the information stored on your system. If you use this method, be sure to keep the copies in a safe and easy-to-access location.

If you end a **list** or **display** command with the command **print**, the system prints a paper copy of the selected list or display screen to the slave printer associated with the administration terminal.

For example, to print a list of stations that are currently administered on your system, complete the following steps at the command prompt:

1. Type **list station print** and press RETURN.

Tip:
*To print a screen or report to the system printer, end a **list** or **display** command with the word **schedule**. The system then prompts you to select to print immediately or schedule printing.*

For more information about generating reports, refer to the *Avaya™ Communication Manager Little Instruction Book for advanced administration*, 555-233-757, or to the *Reports for Avaya™ Communication Manager*, 555-233-505.

System information

You should keep current copies of each of the following system lists in your records. If you ever need to replace information because of a system failure, these lists help Avaya rebuild your system.

Use the following commands to print general system lists, and save these lists as your paper records:

- **display dialplan print** — prints your dialing parameters
- **display system-parameters customer-options print** — prints the current software version and shows which features have been enabled on your system

- **display system-parameters features print** — prints the parameter settings for features on your system
- **display feature-access-codes print** — prints the current feature access codes by feature
- **list configuration all print** — prints your slot and port assignments
- **list extension-type print** — prints information for each extension on your system
- **list station print** — prints information for each station on your system
- **list data print** — prints information for each data module on your system
- **list *type* group print** — where *type* can be replaced with hunt, trunk, pickup, and so on. Prints parameters for the specified group.
- **list coverage path print** — prints each defined coverage path and each of the coverage points

In addition to the above reports, you may want to periodically print other lists, traffic reports, or security reports to monitor the use of your system.

Specific extension information

You'll probably want to keep both system and individual extension records. To keep extension records, print a copy of the station form for each extension. For example, to print a station form for extension 4567:

1. Type **display station 4567 print** and press RETURN.

As another example, to print a station form for data module 5567:

1. Type **display data 5567 print** and press RETURN.

Other information

You may find that you want to keep track of information that is not stored on the system and is specific to your company, such as:

- switch locations and handles (names)
- groups of extensions you've reserved for certain departments or types of lines
- login names and privileges
- customized soft-key assignments

Basically, you can track whatever information is appropriate for your company. And you can decide whether you want to keep just paper copies or perhaps design a computer database to track all your system information. It is up to you.

Remember that the better records you keep, the better able you'll be to solve problems, reconstruct information, and make the best use of the features on your system.

Preparing to contact Avaya

Do you need to call Avaya for additional information or help in solving a problem?

If you do, please have the following information handy. This helps the person taking your call find the answer to your question.

- Your installation location ID (also called your IL)

  _____

  (Write your IL number here for easy reference)
- Your name
- Your phone number (in case we need to call you back)
- Your company's main listed phone number
- The task you want to accomplish, complete with all the numbers involved in the task (for example, extensions or phone numbers, trunk group numbers, phone types, or report types)

Once you gather the information you need, refer to the section "How to get help" on page 24.

Notes

Glossary

A

abbreviated dialing
: A feature that allows callers to place calls by dialing just one or two digits.

access code
: A dial code used to activate or cancel a feature or access an outgoing trunk.

analog phone
: A phone that receives acoustic voice signals and sends analog electrical signals along the phone line.

ARS partitioning
: A feature that allows you to route calls differently for different groups of users. *See also:* Automatic Route Selection (ARS).

attendant
: A person at a console who provides personalized service for incoming callers and voice-services users by performing switching and signaling operations.

attendant console
: The workstation used by an attendant. The attendant console allows the attendant to originate a call, answer an incoming call, transfer a call to another extension or trunk, put a call on hold, and remove a call from hold. Attendants using the console can also manage and monitor some system operations.

audio information exchange (AUDIX)
: A fully-integrated voice-mail system. Can be used with a variety of communications systems to provide call-history data, such as subscriber identification and reason for redirection.

Automatic Alternate Routing (AAR)
: A feature that routes calls to alternate routes when facilities are unavailable.

Automatic Call Distribution (ACD)
: A feature that gives users more flexibility in routing calls to hunt group agents. ACD also allows external measurement systems such as BCMS and CentreVu® CMS to be used.

Automatic Circuit Assurance (ACA)
: A feature that tracks calls of unusual duration to facilitate troubleshooting.

Automatic Route Selection (ARS)
: A feature that allows the system to automatically choose the least-cost route for toll calls.

B

barrier code
: A security code used with Remote Access to prevent unauthorized access.

bridge (bridging)
: The appearance of a phone's extension at one or more other phones.

bridged appearance
: A call appearance on a phone that matches a call appearance on another phone for the duration of a call.

C

call appearance
: For the phone or attendant console, a button labeled with an extension and used to place outgoing calls, receive incoming calls, or hold calls. Lights next to the button show the status of the call appearance.

Call Detail Recording (CDR)
A feature that records call data.

call vectoring
A feature that allows users to provide flexible, customized call handling by writing a series of instructions in a simple programming language.

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

centum call seconds (CCS)
A CCS is a unit for measuring call traffic. One CCS equals 100 seconds. Call traffic for a facility, such as a hunt group or phone, is scanned every 100 seconds. If the facility is busy, it is assumed to have been busy for the entire scan interval. There are 3600 seconds per hour, so a facility that is busy for an entire hour will be measured as being busy for 36 CCS.

Central Office (CO)
The location of phone switching equipment that provides local phone service and access to toll facilities for long-distance calling.

circuit
A channel or transmission path between two or more points.

Class of Restriction (COR)
A feature that defines call-origination and call-termination restrictions.

Class of Service (COS)
A feature that determines whether users can activate certain features.

coverage answer group
A group of phones that ring simultaneously when a call is redirected to it.

coverage path
The order in which calls are redirected to alternate phones.

coverage point
An extension designated as an alternate phone in a coverage path.

D

data module
A digital interface device between the switch and data equipment.

Direct Department Calling (DDC)
A method for distributing hunt group calls to agents. The switch searches through all the hunt group extensions in order, starting with the first extension. As soon as the switch finds an available extension, it connects the call. Compare to Uniform Call Distribution (UCD).

E

Expert Agent Selection (EAS)
A feature allowing incoming calls to be routed to specialized groups of agents within a larger pool of agents.

extension
A number by which calls are routed through a communications system.

external call
A connection between a communications system user and a party on the public network or on another communications system in a private network.

F

facility
A telecommunications transmission pathway and associated equipment.

Feature Access Code (FAC)
: A code users dial to access a system feature.

feature button
: A button on a phone or attendant console used to access a specific feature.

H

hunt group
: A group of extensions that can simultaneously answer multiple calls to a single phone number. When a call arrives at the group number, the switch searches (“hunts”) for an available extension in the group and connects the call to that extension.

I

internal call
: A connection between two users on the same phone system.

M

major alarm
: An indication of a component failure that requires immediate attention.

minor alarm
: An indication of a component failure that could affect customer service.

multiappearance phone
: A phone equipped with several call-appearance buttons allowing the user to handle more than one call on that same extension at the same time.

P

pickup group
: A group of individuals authorized to answer any call directed to an extension within the group.

port carrier
: A carrier in a cabinet containing port circuit packs, power units, and service circuits. Also called a port cabinet.

primary extension
: The main extension associated with the physical phone or data terminal.

principal
: A phone that has its primary extension bridged on one or more other phones.

public network
: The network that can be openly accessed by all customers for local and long-distance calling.

R

redirection criteria
: Information administered for each phone's coverage path that determines when an incoming call is redirected to coverage.

S

skill
: An attribute assigned to an agent in a system using Expert Agent Selection. An agent's skill indicates a specialty in which the agent is proficient.

split
An ACD hunt group.

system administrator
The person who maintains overall customer responsibility for system administration.

system printer
An optional printer that may be used to print scheduled reports via the report scheduler.

system report
A report that provides historical traffic information for internally measured splits.

T

trunk
A dedicated telecommunications channel between 2 phone systems or COs.

trunk group
Telecommunications channels assigned as a group for certain functions that can be used interchangeably between two communications systems or COs.

U

Uniform Call Distribution (UCD)
A method for distributing hunt group calls to agents by comparing agents' workloads. Avaya™ Communication Manager can deliver each new call to the most idle agent (the available agent who has been idle the longest since their last hunt group call) or to the least occupied agent (the agent who has spent the least amount of time on hunt group calls in their current shift). Compare to Direct Department Calling (DDC).

Uniform Dial Plan (UDP)
: A feature that allows a unique 4- or 5-digit number assignment for each point in a multiswitch system.

V

vector
: A set of call handling instructions for Avaya™ Communication Manager written in Avaya's call vectoring programming language.

Index

A

AAR. *See* Automatic Alternate Routing (AAR)
abbreviated dialing, 65
access, remote, 81
accessing the system, 29
ACTR. *See* Automatic Customer Telephone Rearrangement (ACTR)
adding
  area codes, 91
  extension ranges
    Communication Manager, 38
    software release R10 or earlier, 43
  feature access codes
    Communication Manager, 39
    software release R10 or earlier, 43
  phones, 47
  prefixes, 91
alias, 53
announcement board circuit packs, 33
announcements, saving, 33
answering
  backup, *see* call coverage
  shared, *see* pickup groups
area codes, adding, 91
ARS. *See* Automatic Route Selection (ARS)
assigning
  coverage paths, 74
  logins, 104
  ringing, 83
attd code, 37, 41
AUDIX, 27
  Intuity, 27
Automatic Alternate Routing (AAR), 87
Automatic Customer Telephone Rearrangement (ACTR), 59
Automatic Route Selection (ARS), 87
  partitioning, 96
Avaya support Web site, 24

B

backup answering, *see* call coverage
backups, translations, 33
Basic Call Management System (BCMS), 27
books
  how to order more copies, 23
bridged call appearance, 81
buttons
  call appearance, 82
  feature, 51
  help, 20
  programmed, 44

C

Call Accounting System (CAS), 27
call appearance, 82
call coverage, 71
Call Detail Recording (CDR), 27, 111
call forwarding, 70
Call Management System (CMS), 27
calling Avaya, 121
CAS. *See* Call Accounting System (CAS)
CDR. *See* Call Detail Recording (CDR)

changing
Feature Access Codes (FAC), 44
feature buttons, 55
logins, 108
paths, *see* call coverage
phones, 59
routing, 91
Class of Restriction (COR), 80, 88, 110
Class of Service (COS), 70, 80
CMS. *See* Call Management System (CMS)
commands
add abbreviated-dialing group, 65
add coverage path, 72
add coverage time-of-day, 75
add login, 104
add pickup-group, 68
add station, 50
change ars analysis, 92, 94
change authorization-code, 95
change coverage path, 78
change coverage remote, 78
change dialplan, 42, 43
change dialplan analysis, 38, 39
change feature-access-codes, 44
change login, 108
change password, 107
change permissions, 106
change station, 51, 66, 74, 76, 82
change system feature, 64
change system-parameters security, 112
change telecommuting-access, 81
display coverage sender group, 74
display dialplan, 42
display dialplan analysis, 38
display feature-access codes, 80
display station, 52
display system-parameters maintenance, 32
display time, 31
commands, (continued)
duplicate station, 52
list ars route-chosen, 91
list bridge, 85
list call-forwarding, 71
list configuration station print, 49
list configuration stations, 48
list cor, 99
list measurements security-violations, 114
logoff, 34
save announcements, 33
save translation, 32
set time, 30
status station, 71
Communication Manager
adding feature access codes, 39
dial plans, 36
adding extension ranges to, 38
displaying, 38
modifying, 38
sample system running, 26
connecting phones, 50
COR. *See* Class of Restriction (COR)
COS. *See* Class of Service (COS)
coverage answer group, 76
coverage paths
assigning, 74
creating, 72
remote, 77
time-of-day, 75
customizing phones, 57

D

DAC. *See* Dial Access Codes (DAC)
data modules, 27
dates, system, 30
detecting problems, 111
Dial Access Codes (DAC), 37, 41

dial plans
adding extension ranges
Communication Manager, 38
software release R10 or earlier, 43
adding feature codes
Communication Manager, 39
software release R10 or earlier, 43
Communication Manager, 36
displaying
Communication Manager, 38
software release R10 or earlier, 42
first digit table, 40
modifying
Communication Manager, 38
software release R10 or earlier, 42
software release R10 or earlier, 40
understanding, 35
directed call pickup, 69
displaying dial plans
Communication Manager, 38
software release R10 or earlier, 42

E

extensions, 37, 41, 49

F

FAC. *See* Feature Access Codes (FAC)
Facility Restriction Level (FRL), 88, 89
Feature Access Codes (FAC), 37, 39, 41, 43
feature buttons, 51, 55
FRL. *See* Facility Restriction Level (FRL)

G

group answering, *see* pickup groups

H

help
buttons, 20
numbers to call, 24
how to use this book, 19

I

information, system, 118
Intuity AUDIX, 27

K

keeping records, 117

L

last number dialed, 39, 43
logging in, 29
logging off, 34
logins
assigning, 104
changing, 108
permissions, 106
requirements, 103

M

message line, 20
miscellaneous code, 42
modifying dial plans
Communication Manager, 38
software release R10 or earlier, 42

O

off-net, *see* coverage path, remote

P

parameters, system, 63
Partition Group Number (PGN), 97
partitioning, Automatic Route Selection (ARS), 96
passwords, 29, 103, 107
permanent backups, 32
permissions, login, 106
PGN. *See* Partition Group Number (PGN)
phones
  adding, 47
  alias, 53
  analog, 27, 49, 83
  changing, 59
  connecting, 50
  customizing, 57
  digital, 27, 83
  duplicate, 52
  hybrid, 27
  IP, 27
  IP screenphone, 65
  IP softphone, 47, 65
  ISDN, 27
  removing, 60
  swapping, 59
  upgrading, 58
pickup groups, 68
port address, 49
prefixes, adding, 91
problems, detecting, 111
programmed buttons, 44

R

records, keeping, 117
redirecting calls, *see* call coverage
remote access, 81
remote coverage paths, 77
removing phones, 60
reports, security, 114
ringing, assigning, 83
routing, changing, 91

S

SAT. *See* System Access Terminal (SAT)
saving
  announcements, 33
  permanent backups, 32
  temporary changes, 31
  translations, 32
screens, 20
  Abbreviated Dialing List, 65
  ARS Digit Analysis Table, 88, 92
  ARS Route Chosen Report, 92, 97
  Authorization Code - COR Mapping, 96
  Class of Restriction, 100
  Class of Restriction Information, 99
  Command Permission Categories, 106
  Coverage Path, 73, 76, 79
  Date and Time, 31
  Dial Plan Analysis Table, 36
  Dial Plan Record, 40
  Duplicate Station, 52
  Feature Access Codes, 80
  Feature-Related System Parameters, 64

screens, (continued)
Login Administration, 105
Partition Routing Table, 98
Password Administration, 107
Pickup Group, 69
Remote Call Coverage Table, 78
Save Translation, 32
Security-Related System Parameters, 113
Station, 51, 67, 82 to 84
System Configuration, 48
System Parameters Call Coverage/Call Forwarding, 70
Terminal screen for login, 30
Time of Day Coverage Table, 75
security
concerns, 21
hotline, 103
passwords, 104
reports, 114
violations, 81
notification, 112
shared answering, *see* pickup groups
software release R10 or earlier dial plans, 40
adding extension ranges, 43
adding feature access codes, 43
displaying, 42
modifying, 42
speed dialing, *see* abbreviated dialing
status line, 20
swapping phones, 59
system
access, 29
parameters, 63
time and date, 30
System Access Terminal (SAT), 26
system information, 118

T

TAC. *See* Trunk Access Codes (TAC)
telecommuting, 80
temporary changes, 31
Terminal Translation Initialization (TTI), 59
terminal type, 29
time, system, 30
time-of-day coverage path, 75
toll fraud, 21, 108
trademarks, 21
translations
backups, 33
saving, 32
Trunk Access Codes (TAC), 37, 41
TTI. *See* Terminal Translation Initialization (TTI)

U

upgrading phones, 58

V

violations, security, 81
voice terminals, *see* phones

W

Web sites
Avaya support, 24

We'd like your opinion.

We welcome your feedback! Please let us know what you think about this book.

Avaya™ Communication Manager Little Instruction Book for basic administration, 555-233-756, Issue 5, May 2003

1. Please check the ways you feel we could improve this book:

- ❒ Improve the overview
- ❒ Improve the table of contents
- ❒ Improve the organization
- ❒ Add more figures
- ❒ Add more examples
- ❒ Add more detail
- ❒ Make it more concise
- ❒ Add more step-by-step procedures

Please add details about what you think. _____
_____
_____

2. What did you like most about this book? _____
_____
_____
_____

3. Feel free to write additional comments._____
_____
_____
_____
_____
_____
_____

If we may contact you concerning your comments, please complete the following:

Name:_____Telephone Number: (____)_____

Company/Organization_____Date:_____

Address:_____
_____

When you have completed this form, please fax your feedback to **1 303 538 1741**.
Thank you.

Helpful Avaya web sites

Do you need more information or assistance? Try these web sites!

Avaya main site

Check here often to see what's new at Avaya!

http://www.avaya.com/

Avaya Customer Support

Use this site to find answers to questions, review maintenance tickets, or to get the latest version of this book.

http://www.avaya.com/support/

Avaya™ Communication Manager site

Go here to offer suggestions for what you would change if you were in charge of updating Communication Manager.

http://www.avaya.com/ac/common/index.jhtml

International Alliance of Avaya Users (InAAU) site

This organization was formerly known as the International DEFINITY Users or the International MultiVantage Users group. Use this site to find more users, just like you!

http://www.indug.org/

Avaya Communication Manager

Little Instruction Book

for Advanced Administration

Release 2.0
555-233-757
Issue 6
November 2003

Copyright 2003, Avaya Inc.
All Rights Reserved

Notice

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

Warranty

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

Preventing Toll Fraud

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

Avaya Fraud Intervention

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

How to Get Help

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

If you are:

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

Providing Telecommunications Security

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

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

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

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

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

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

Responsibility for Your Company's Telecommunications Security

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

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

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

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

TCP/IP Facilities

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

Standards Compliance

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

Product Safety Standards

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

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

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

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

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

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

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

The LASER devices operate within the following parameters:

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

Luokan 1 Laserlaite
Klass 1 Laser Apparat

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

Electromagnetic Compatibility (EMC) Standards

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

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

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

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

Federal Communications Commission Statement

Part 15:

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

Part 68: Answer-Supervision Signaling

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

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

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

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

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

REN Number

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

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

For G350 and G700 Media Gateways:

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

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/On 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
120A3 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

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

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

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

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

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

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

Canadian Department of Communications (DOC) Interference Information

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

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

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

DECLARATIONS OF CONFORMITY

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

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

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

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

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

European Union Declarations of Conformity

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

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

Japan

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

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

To order copies of this and other documents:

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

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

E-mail: totalware@gwsmail.com

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

Contents

Welcome 13

- Why another instruction book? 13
- We wrote this book for you! 13
- What information is in this book? 14
- How to use this book 14
  - Systems, circuit packs, and media modules 16
- Admonishments 17
- Security concerns 18
- Trademarks 18
- Related books 18
- Tell us what you think! 20
- How to get this book on the Web 20
- How to order more copies 21
- How to get help 21

1 Managing trunks 23

- Understanding trunks 23
- Adding trunk groups 26

2 Setting up night service 31

- Setting up night service for hunt groups 32
- Setting up night station service 33

- Setting up trunk group night service 35
- Setting trunk answer from any station 36
- How do night service types interact? 38

3 Managing announcements 41

- What is an announcement? 41
- Adding announcements 43
  - Voice Announcement over LAN (VAL) 43
  - VAL Manager 46
- Recording announcements 46
- Deleting announcements 50
- Backing up your announcements 51

4 Managing hunt groups 53

- What are hunt groups? 53
- Setting up hunt groups 54
  - Setting up a queue 57
  - Adding hunt group announcements 58
- Call distribution methods 60

5 Managing vectors and VDNs 63

- What are vectors? 64
  - Writing vectors 64
  - Allowing callers to leave a message 70
  - Inserting a step 73

Deleting a step 73
Diagnosing a vector problem 74
- Vector Directory Numbers 76
- Meet-me Conference 78
Verifying the customer options 79
Setting up a Meet-me Conference VDN 80
Creating a Meet-me Conference vector 81
Options for vector steps 84
Disabling Meet-me Conference 85

6 Using reports 87

- Using report scheduler 87
Setting printer parameters 88
Scheduling and printing reports 90
Listing scheduled reports 91
Changing scheduled reports 92
Removing scheduled reports 93
- Analyzing report data 93
- Using attendant reports 94
Measuring attendant group traffic 94
Measuring individual attendant performance 95
Measuring attendant group performance 96
- Trunk group reports 96
Summary of trunk group activity 97
Hourly trunk group activity 97
Out-of-service trunks 99

Current trunk group status 99
Least used trunks 100
- Measuring call center performance 100
  - What should I measure? 101
  - How many people can use switch reports? 102
  - Viewing hunt group reports 102
- Using security reports 104

7 Understanding call centers 105

- What is a call center? 105
- Planning a call center 106
  - Setting up the call flow 106
  - Testing the system 108
  - Monitoring your call center 109
  - Viewing system capacity 110
- Understanding Automatic Call Distribution 110
  - Enhancing an ACD system 111
  - Selecting a call management system 112

Index 115

Welcome

Why another instruction book?

You have told us that you want step-by-step instructions on advanced administration tasks for Avaya Communication Manager. This book contains the information you need for advanced administration for your phone system.

This book contains instructions for completing tasks that were not covered in the *Avaya Communication Manager Little Instruction Book for Basic Administration*, 555-233-756. Some steps may vary between the different versions of the software, but the instructions will help you through the more advanced operations.

We wrote this book for you!

Use this book if you are a system administrator. Use it before you attend training, and take it with you to your class. Mark it up, make notes in it, and use it daily even after you complete training.

This book is for you if:

- You are a new administrator taking over from someone else.
- You are filling in for your company's regular administrator.
- You want to refresh your memory.

What information is in this book?

The *Little Instruction Book for Advanced Administration* is divided into sections to help you find information about advanced topics.

Managing trunks describes the different types of trunks and how to add a trunk group.

Setting up night service explains how to set up night service and explains how different types of night service work together.

Managing announcements explains how to add, record, change, delete, and back up announcements.

Managing hunt groups describes how to set up hunt groups. It explains how calls to a hunt group are handled and shows you different call distribution methods.

Managing vectors and VDNs provides an overview of vectors and Vector Directory Numbers (VDN). It gives you basic instructions for writing simple vectors.

Using reports describes how to generate, list, print, and schedule some of the basic reports on your system. It also explains when to use some common reports and how to interpret the report information.

Understanding call centers gives an overview of call centers. It shows how to set up a simple inbound call center and lists things to consider as you plan and design your center.

How to use this book

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

- A “form” is the display of fields and prompts that appear on a terminal monitor screen. See Figure 1, Trunk Group form, on page 27 for an example of a form and how it is shown in this book.
- We use the term “phone” in this book. Other Avaya books might refer to phones as telephones, voice terminals, stations, or endpoints.
- Keys and buttons are printed as follows: **KEY**.
- Titles of forms are printed in a bold constant width italic font, as follows: ***FORM DISPLAY***.
- To move to a certain field on a form, 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**, **NEXT PAGE**, etc.
- Commands are printed in a bold constant width font, as follows: **`command`**.
- Variables are printed in a bold constant width italic font, as follows: ***`variable`***.
- We show complete commands in this book, but you can always use an abbreviated version of the command. For example, **`list configuration station`** can be typed as **`list config sta`**.
- We show commands and forms from the newest release of Communication Manager and refer to the most current books. Substitute the appropriate commands for your system and refer to the manuals you have available.
- 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, a list of available commands appears.

— When you press **HELP** with your cursor in a field on a form, a list of valid entries for that field appears.

- Text (other than commands) you should type in a form are printed in a bold font, as follows: **text**.
- 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 form you were on clears. The cursor then returns to the command prompt. The message line shows "`command successfully completed`" to indicate that the system accepted your changes.

Systems, circuit packs, and media modules

- The word "system" is a general term encompassing all references to an Avaya media server running Communication Manager.
- Circuit pack codes (for example, TN780 or TN2182B) are shown with the *minimum acceptable* alphabetic suffix (like the "B" in the code TN2182B). Generally, an alphabetic suffix higher than that shown is also acceptable. However, not every *vintage* of either the minimum suffix or a higher suffix code is necessarily acceptable. A suffix of "P" means that firmware can be downloaded to that circuit pack.
- The term "cabinet" refers to the external casing (shell) of an MCC1, SCC1, CMC1, G600, or G650 Media Gateway. Circuit packs are installed in the cabinet in a specific carrier (row), and in a specific slot within that carrier.

- The designation "***UUCSSpp***" refers to the location (address) of a circuit pack in cabinet-carrier-slot-port order. In this address designation, ***UU*** is the cabinet number, ***C*** is the carrier letter, ***SS*** is the slot number of a specific circuit pack, and ***pp*** (if applicable) is a specific port on the circuit pack. A sample address for port 4 on a circuit pack on an MCC1 Media Gateway might look like this: 02A0704.
- A G350 or G700 Media Gateway uses media modules instead of circuit packs. The media module address is designated as ***XXX*V*Spp***, where ***XXX*** is the administered number of the media gateway, **V*S*** is the slot number of a specific media module location on the media gateway, and ***pp*** (if applicable) is a specific port on the media module. The **V** is not a variable and needs to be included in the command exactly where shown. A sample address for port 4 in slot V3 on an MM711 Media Module on a G700 Media Gateway might look like this: 002V304.

  If an S8300 Media Server is installed in a G700 Media Gateway, it must be installed in slot number V1.

Admonishments

We use the following icons in this book:

NOTE:
Draws attention to information.

CAUTION:
Indicates possible harm to software, possible loss of data, or possible service interruptions.

SECURITY ALERT:
Indicates when system administration might leave your system open to toll fraud.

Security concerns

Toll fraud is the theft of long distance service. When toll fraud occurs, your company is responsible for charges. See the *Avaya Toll Fraud and Security Handbook, 555-025-600,* for information on how to prevent toll fraud. You can also call the Avaya Security Hotline at 1 800 643 2353 or contact your Avaya representative.

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.

Related books

There are two companions to this book:

- The *Avaya Communication Manager Little Instruction Book for Basic Administration*, 555-233-756
- The *Avaya Communication Manager Little Instruction Book for Basic Diagnostics*, 555-233-758

The *Administrator's Guide for Avaya Communication Manager*, 555-233-506, explains system features and interactions in greater detail. The Administrator's Guide provides a reference how to plan, operate, and administer your system.

NOTE:
Prior to April 1997, this same information was in two separate books: the *DEFINITY Implementation* and the *DEFINITY Feature Description* books.

We also refer to the following books:

- *Overview for Avaya Communication Manager*, 555-233-767
- *Reports for Avaya Communication Manager, 555-233-505*
- *Avaya MultiVantage™ Call Center Software Call Vectoring and Expert Agent Selection (EAS) Guide*, 555-230-714
- *Avaya MultiVantage™ Call Center Software Guide to ACD Call Centers*, 555-230-716
- *Installation for Adjuncts and Peripherals for Avaya Communication Manager*, 555-233-116
- *Avaya Products Security Handbook*, 555-025-600
- *Avaya MultiVantage™ Call Center Software Basic Call Management System (BCMS) Operations*, 555-230-706
- *BCMS Vu Software R2 V3 Software User Guide*, 585-217-102
- *CentreVu CMS Switch Connections and Administration*, 585-215-876

Tell us what you think!

Tell us what you like or do not like about this book. Although we cannot respond personally to all your feedback, we read each response. Your suggestions make this book more useful for everyone.

Write to us at: Avaya
Product Documentation Group
Room B3-H13
1300 W. 120th Avenue
Denver, CO 80234 USA

Fax to: 1 303 538 1741

Send e-mail to: document@avaya.com

How to get this book on the Web

If you have internet access, you can view and download the latest version of *Avaya Communication Manager Little Instruction Book for Advanced Administration*. To view this book, you must have a copy of Acrobat Reader.

NOTE:
If you do not have Acrobat Reader, you can get a free copy at http://www.adobe.com.

To get the latest version of this book:

1. Go to the Avaya customer support Web site at http://www.avaya.com/support/.
2. Click the **Product Documentation** link.
3. Type **555-233-757** (the document number) in the **Search Support** text box, then click **Go**.

November 2003

How to order more copies

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 Attn: Avaya Account Management 200 Ward Hill Ave Haverhill, MA 01835 USA
E-mail:	totalware@gwsmail.com
Order:	Document No. 555-233-757, Issue 6, November 2003

We can put your name on an order list so you will automatically receive updated versions of this book. For more information and to receive future issues of this book, contact the Avaya Publications Center.

How to get help

If you need additional help, go to the Avaya customer support Web site at 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, which includes phone numbers for the international Centers of Excellence.

You can also access the following services in the USA. You might need to purchase an extended service agreement to use some of these services. Contact your Avaya representative for more information.

Avaya Communication Manager Helpline (for help with feature administration and system applications)	1 800 225 7585
Avaya National Customer Care Center Support Line (for help with maintenance and repair)	1 800 242 2121
Avaya Toll Fraud Intervention	1 800 643 2353
Avaya Corporate Security	1 800 822 9009

1 Managing trunks

This section provides an overview of trunks and tells you how to add trunk groups to your system.

Understanding trunks

Trunks carry phone signals from one place to another. For example, one type of trunk carries phone signals from your switch to the central office (CO).

Groups of trunks perform specific functions. Use the following table to help determine which types of trunk groups your company uses.

trunk group	description
Access	Use access trunks to connect satellite switches to the main switch in Electronic Tandem Networks (ETN). Access trunks do not carry traveling class marks (TCM) and thus allow satellite callers unrestricted access to out-dial trunks on the main switch.
APLT	Advanced Private Line Termination (APLT) trunks are used in private networks. APLT trunks allow inband ANI.
CAMA	Centralized Automatic Message Accounting (CAMA) trunks route emergency calls to the local community's Enhanced 911 systems.
CO	Central Office (CO) trunks typically connect your switch to the local central office, but they can also connect adjuncts such as external paging systems and data modules.
CPE	Customer Premise Equipment (CPE) trunks connect adjuncts, such as pagers and announcement or music sources, to the switch.
DID	Direct inward dialing (DID) trunks connect incoming calls directly to internal extensions without going through an attendant or some other central point.
DIOD	Direct inward and outward dialing (DIOD) trunks connect incoming and outgoing calls directly to your switch.
DMI-BOS	Digital multiplexed interface bit-oriented signaling (DMI-BOS) trunks connect a switch to a host computer, or one switch to another switch.

trunk group	description
FX	Foreign exchange (FX) trunks connect calls to a non-local central office as if it were a local central office. Use FX trunks to reduce long distance charges if your organization averages a high volume of long-distance calls to a specific area code.
ISDN	Integrated Services Digital Network (ISDN) trunks allow voice, data, video, and signaling information to be sent with calls. There are two types of ISDN trunks: ISDN-Basic Rate Interface (ISDN-BRI) connect telephones, personal computers, and other desktop devices to the switch. ISDN-Primary Rate Interface (ISDN-PRI) connect equipment such as switches to the network, and acts as an interface between equipment such as switches and computers.
RLT	Release-link trunks (RLT) use Centralized Attendant Service (CAS) to connect remote switches to attendants who are at a central location.
Tandem	Tandem trunks are a type of tie trunk used for large networks.
Tie	Tie trunks connect a switch to a CO, or two switches together in a private network.
WATS	Wide Area Telecommunications Service (WATS) trunks allow calls to certain areas for a flat-rate charge. Use WATS trunks to reduce long-distance bills when your company places many calls to a specific geographical area in North America.

Adding trunk groups

Occasionally, your company's phone requirements change and you need to add new trunk groups to your system. For example, maybe your company is expanding and you must have additional two-way access between your switch and your local phone company or CO. After doing some research, you decide that you need to add another CO trunk.

Once you decide that you want to add a new trunk, contact your vendor. Depending on the type of trunk you want to add, the vendor may be your local phone company, a long distance provider, or some other service provider.

When you talk to your vendor, they'll want to know what kind of service you want to add. In our example, request CO service.

The vendor should confirm the type of signal you want and provide you with a circuit identification number for the new trunk. Be sure to record any vendor-specific ID numbers or specifications in case you ever have any problems with this trunk.

NOTE:
Remember to keep records of any changes you make to the system for future reference.

Once you've ordered your new service and have gathered all the information associated with the new trunk, you need to configure the system to recognize the new trunk group.

Before you start

Before you can administer any trunk group, you must have one or more circuit packs of the correct type with enough open ports to handle the number of trunks you need to add. To find out what circuit

packs you need, see the *Hardware Guide for Avaya Communication Manager.*

To add a new trunk-group:

1 Type **`add trunk-group next`** and press ENTER.

The ***TRUNK GROUP*** form appears.

The system assigns the next available trunk group number to this group. In our example, we are adding trunk group 5.

Figure 1: Trunk Group form

```
                                TRUNK GROUP
Group Number: 5                     Group Type: co            CDR Reports: y
  Group Name: outside calls               COR: 85 TN: 1         TAC:647
   Direction: two-way        Outgoing Display? n
 Dial Access: n               Busy Threshold: 99          Night Service: 1234
Queue Length: 0           Country: 1                 Incoming Destination:
____
   Comm Type: voice                 Auth Code? n   Digit Absorbtion List: ____
   Prefix-1?: y                   Trunk Flash? n         Toll Restricted? y
TRUNK PARAMETERS
         Trunk Type: loop start
 Outgoing Dial type: tone                                  Cut Through? n
  Trunk Termination: rc                         Disconnect Timing(msec): 500
        Auto Guard?: n       Call Still Held? n     Sig Bit Inversion: none
  Analog Loss Group:                                Digital Loss Group:
                                 Trunk Gain: high
Disconnect Supervision - In? y   Out? n
Answer Supervision Timeout: 10             Receive Answer Supervision? n
```

2 In the `Group Type` field, type the type of trunk you want to add. In our example, type **co**, which is also the default.

If you select a different trunk type, such as DID, the system changes the form to show only those fields that apply to the type of trunk-group you are adding.

3 Type a name to identify this trunk group in the `Group Name` field.

In our example, type **outside calls**.

4 In the `COR` field, assign a class of restriction (COR) that is appropriate for the calling permissions administered on your system. This field controls what users can make and receive calls over this trunk group.

In our example, type **85**.

5 In the `TAC` field, type the code you want to use to access the new trunk group.

In our example, type **647**.

6 In the `Direction` field, indicate the call-flow direction.

For our example, leave the default of **two-way**.

7 If you want to direct calls to a night extension, type the extension number in the `Night Service` field.

In our example, direct night calls to extension **1234**.

8 In the `Comm Type` field, type the type of communication that you want the new trunk to use.

In our example, type **voice**.

9 In the `Trunk Type` field, type **loop start**.

This field tells the system how the calls on this trunk will be sent or received. Your vendor should know what trunk type you can use to complete this field.

10 Use NEXT PAGE to go to the `GROUP MEMBER ASSIGNMENTS` page.

Different fields appear on this form depending on the configuration of your switch.

Figure 2: Trunk Group form (Group Member Assignments page)

```
                                   TRUNK GROUP
                                     Administered Members (min/max): xxx/yyy
                                           Total Administered Members: xxx

GROUP MEMBER ASSIGNMENTS
    Port       Code Sfx  Name          Night         Mode      Type    Ans Delay
 1: 1B1501___            5211________  ___________   _________ ________ ______
 2: 1B1523___            5212________  ___________   _________ ________ ______
 3: 1B1601___            5213________  ___________   _________ ________ ______
 4: 1B1623___            5214________  ___________   _________ ________ ______
 5: 1B1701___            5215________  ___________   _________ ________ ______
 6: _________            ____________  ___________   _________ ________ ______
 7: _________            ____________  ___________   _________ ________ ______
 8: _________            ____________  ___________   _________ ________ ______
 9: _________            ____________  ___________   _________ ________ ______
10: _________            ____________  ___________   _________ ________ ______
11: _________            ____________  ___________   _________ ________ ______
12: _________            ____________  ___________   _________ ________ ______
13: _________            ____________  ___________   _________ ________ ______
14: _________            ____________  ___________   _________ ________ ______
15: _________            ____________  ___________   _________ ________ ______
```

11 In the `Port` field, type the port number of the physical connection for each member you are adding to the trunk group.

12 In the `Name` field, type the circuit ID or telephone number for each member.

This information is very helpful for tracking your system or troubleshooting problems, but the fields need to be updated whenever the information changes.

13 Press ENTER to save your changes.

2 Setting up night service

You can use night service to direct calls to an alternate location when the primary answering group is not available. For example, you can administer night service so that anyone in your marketing department can answer incoming calls when the attendant is at lunch or has left for the day.

Once you administer night service to route calls, your end-users merely press a button on the console or a feature button on their phones to toggle between normal coverage and night service.

There are five types of night service:

- Hunt group night service — directs hunt group calls to a night service destination
- Night station night service — directs all incoming trunk calls to a night service destination
- Night console night service — directs all attendant calls to a Night or Day/Night console
- Trunk group night service — directs incoming calls to individual trunk groups to a night service destination
- Trunk Answer from Any Station (TAAS) — directs incoming attendant calls and signals a bell or buzzer to alert other employees that they can answer the calls

Setting up night service for hunt groups

You can administer hunt group night service if you want to direct hunt group calls to a night service destination. As an example, say your helpline on hunt group 3 does not answer calls after 6:00 p.m. (18:00). When customers call after hours, you would like them to hear an announcement that asks them to try their call again in the morning.

To set up night service for your helpline, you need to record the announcement (in our example, the announcement is on extension 1234) and then modify the hunt group to send calls to this extension.

To administer hunt group night service:

1. Type **`change hunt-group 3`** and press ENTER.

   The ***HUNT GROUP*** form appears for hunt group 3.

Figure 3: Hunt Group form

```
                                HUNT GROUP
Group Number: 3                                   ACD: n
              Group Name: Accounting                          Queue: y
          Group Extension: 2011                              Vector: n
              Group Type: ucd-mia                     Coverage Path: 1
                      TN: 1              Night Service Destination: 1234
                     COR: 1                        MM Early Answer: n
           Security Code: _____
      ISDN Caller Display: _____

            Queue Length: 4
  Calls Warning Threshold: ________________    Port:  _____
   Time Warning Threshold: ________________    Port:  _____
```

2. Type **1234** in the `Night Service Destination` field.

   The destination can be an extension, a recorded announcement extension, a vector directory number, a hunt group extension, or **attd** if you want to direct calls to the attendant.

3. Press ENTER to save your changes.

Once you modify the hunt group, you also need to assign a `hunt-ns` feature button to a hunt group phone, so that the users in the hunt group can activate and deactivate night service.

Setting up night station service

You can use night station service if you want to direct incoming trunk calls, DID-LDN (direct inward dialing-listed directory number) calls, or internal calls to the attendant (dialed ‘0’ calls) to a night service destination.

As an example, say your attendant, who answers extension (List Directory Number or LDN) 8100, usually goes home at 6:00 p.m. When customers call extension 8100 after hours, you would like them to hear an announcement that asks them to try their call again in the morning.

To set up night station service, you need to record the announcement (in our example, it is recorded at announcement extension 1234).

All trunk groups are routed through the attendant direct to this night service destination unless you assign trunk group night service to the individual trunk group. See Setting up trunk group night service on page 35.

To set up night station service:

1. Type **`change listed-directory-numbers`** and press ENTER.

   The ***`LISTED DIRECTORY NUMBERS`*** form appears.

Figure 4: Listed Directory Numbers form

```
                    LISTED DIRECTORY NUMBERS
    Ext         Name                                TN
 1: 8100        attendant 8100_________________     _______
 2: _______     ______________________________      _______
 3: _______     ______________________________      _______
 4: _______     ______________________________      _______
 5: _______     ______________________________      _______
 6: _______     ______________________________      _______
 7: _______     ______________________________      _______
 8: _______     ______________________________      _______
 9: _______     ______________________________      _______
10: _______     ______________________________      _______
                                        Night Destination: 1234
```

2 Type **1234** in the `Night Destination` field.

The destination can be an extension, a recorded announcement extension, a vector directory number, or a hunt group extension.

3 Press ENTER to save your changes.

4 Type **`change console-parameters`** and press ENTER.

The ***`CONSOLE PARAMETERS`*** form appears.

Figure 5: Console Parameters form

```
                         CONSOLE PARAMETERS
  Attendant Group Name: OPERATOR
                   COS: 1                                  COR: 1
Calls in Queue Warning: 5                     Attendant Lockout? y
                   CAS: none
                                        Night Service Act. Ext.:1234
          IAS (Branch)? n               IAS Tie Trunk Group No.:
  IAS Att. Access Code:                   Alternate FRL Station:
       Backup Alerting? n        DID-LDN Only to LDN Night Ext? n
```

5 In the `DID-LDN Only to LDN Night Ext?` field, type **n**.

6 Press ENTER to save your changes.

After you set up night station service, have the attendant use the night console button to activate and deactivate night service.

Setting up trunk group night service

You can use trunk group night service if you want to direct individual trunk groups to night service. The system redirects calls to the trunk group to the group's night service destination.

Trunk group night service overrides night station service. As an example, say that you administer trunk group night service, and then your attendant activates night station service. In this case, calls to the trunk group use the trunk night service destination, rather than the station night service destination.

Let us direct night calls for trunk group 2 to extension 1245.

To set trunk group night service:

1 Type **`change trunk-group 2`** and press ENTER.

The ***TRUNK GROUP*** form appears.

Figure 6: Trunk Group form

```
                                 TRUNK GROUP
Group Number: 2                     Group Type: co            CDR Reports: y
  Group Name: outside calls               COR: 1       TN: 1         TAC:647
   Direction: two-way        Outgoing Display? n
 Dial Access: n               Busy Threshold: 99         Night Service: 1245
Queue Length: 0           Country: 1                 Incoming Destination:
____
   Comm Type: voice                  Auth Code? n   Digit Absorbtion List: ____
    Prefix-1?: y                    Trunk Flash? n         Toll Restricted? y
TRUNK PARAMETERS
         Trunk Type: loop start
 Outgoing Dial type: tone                                   Cut Through? n
  Trunk Termination: rc                          Disconnect Timing(msec): 500
        Auto Guard?: n       Call Still Held? n     Sig Bit Inversion: none
  Analog Loss Group:                                Digital Loss Group:
                                    Trunk Gain: high
Disconnect Supervision - In? y   Out? n
Answer Supervision Timeout: 10             Receive Answer Supervision? n
```

2 Type **1245** in the `Night Service` field.

The destination can be a night service extension, a recorded announcement extension, a vector directory number, a hunt group extension, a terminating extension group, or **attd** if you want to direct the call to the attendant.

3 Press ENTER to save your changes.

Setting trunk answer from any station

There may be situations where you want everyone to be able to answer calls when the attendant is away. Use Trunk Answer from Any Station (TAAS) to configure the system so that it notifies everyone when calls are ringing. Then, you can give users the TAAS feature access code so they can answer these calls.

When the system is in night service mode, attendant calls redirect to an alerting device such as a bell or a buzzer. This lets other people in the office know when they should answer the phone.

NOTE:
If no one answers the call, the call will not redirect to night service.

Before you start

You need a ringing device and 1 port on an analog line circuit pack. See the *Hardware Guide for Avaya Communication Manager* for more information on the circuit pack.

Let us define a feature access code (we'll use 71) and configure the alerting device for trunk answer any station.

To set the feature access code for TAAS:

1 Type **change feature-access-codes** and press ENTER.

The ***FEATURE ACCESS CODE (FAC)*** form appears.

Figure 7: Feature Access Code (FAC) form

```
                                FEATURE ACCESS CODE (FAC)
      Per Call CPN Unblocking Code Access Code: #27

                   Priority Calling Access Code: #29
                            Program Access Code: #30
       Refresh Terminal Parameters Access Code: #31
              Remote Send All Calls Activation: #91     Deactivation: #92
               Self Station Display Activation:
                     Send All Calls Activation: #32     Deactivation: *32
         Station Firmware Download Access Code: #97
                       Station Lock Activation:         Deactivation:
      Station Security Code Change Access Code: #34
              Station User Admin of FBI Assign:                Remove:
  Station User Button Ring Control Access Code:
             Terminal Dial-Up Test Access Code: #35
Terminal Translation Initialization Merge Code: #36  Separation Code: *36
            Transfer to Voice Mail Access Code: #37
          Trunk Answer Any Station Access Code: 71
              User Control Restrict Activation: #39     Deactivation: *39
  Voice Coverage Message Retrieval Access Code: #40
 Voice Principal Message Retrieval Access Code: #41
```

2 Move to page 3.

3 In the `Trunk Answer Any Station Access Code` field, type **71**.

4 Press ENTER to save your changes.

Once you set the feature access code, determine where the external alerting device is connected to the switch (we'll use port 01A0702).

To set up external alerting:

1 Type **change console-parameters** and press ENTER.

The ***CONSOLE PARAMETERS*** form appears.

Figure 8: Console Parameters form

```
                        CONSOLE PARAMETERS

  Attendant Group Name: Operator
                   COS: 0                                  COR: 0
Calls in Queue Warning: 5                  Attendant Lockout? y
 EXT Alert Port (TAAS): 01A0702
                   CAS: none
                                       Night Service Act. Ext.:
          IAS (Branch)? n              IAS Tie Trunk Group No.:
  IAS Att. Access Code:                  Alternate FRL Station:
       Backup Alerting? n      DID-LDN Only to LDN Night Ext? n
```

2. In the `EXT Alert Port (TAAS)` field, type **01A0702**.

   Use the port address assigned to the external alerting device.

3. Press ENTER to save your changes.

How do night service types interact?

Let us look at an example of how several types of night service might be used in one company.

Assume that you already administered the following night service settings:

- night station night service redirects to extension **3000** and `DID-LDN only to LDN Night Ext` is set to **n**
- `EXT Alert Port (TAAS)` field is not defined
- Trunk group 4 redirects to extension **2000**

Let us look at how calls for this company are directed after hours:

call type	directs to
An LDN call on a DID trunk	extension 3000
A call on trunk group 4	extension 2000
An internal call to ‘0’	extension 3000
A call that redirects to the attendant through a coverage path.	the attendant queue

3 Managing announcements

This section explains how to use announcements effectively, and how to add, change, delete, and back up your announcements.

What is an announcement?

An announcement is the recorded message a caller hears while the call is in a queue. An announcement is often used in conjunction with music.

Three types of announcements are:

- delay announcement — explains the reason for the delay and encourages the caller to wait.
- forced announcement — explains an emergency or service problem. Use when you anticipate a large number of calls about a specific issue.
- information announcement — gives the caller instructions on how to proceed, information about the number called, or information that the caller wants.

Announcements are most effective when they are:

- short, courteous, and to-the-point
- played for calls waiting in queue
- spaced close together when a caller on hold hears silence
- spaced farther apart when a caller on hold hears music or ringing

Music on Hold is a package of professionally-recorded music available from Avaya. Contact your Avaya representative for more information.

Announcements can be either integrated or external. Integrated announcements reside on a circuit pack in the switch carrier, or embedded within a G350 or G700 Media Server. External announcements are stored and played back from adjunct equipment.

For more information on external announcements, see the *Avaya MultiVantage™ Call Center Software Guide to ACD Call Centers*, 555-230-716, and the *Installation for Adjuncts and Peripherals for Avaya Communication Manager*, 555-233-116.

NOTE:

Because instructions might be slightly different for different system configurations, portions of this chapter are divided into two groups: **MCC1, SCC1, CMC1, G600, or G650 Media Gateways**, and **G350 or G700 Media Gateways.**

Also see the *Installation for Adjuncts and Peripherals for Avaya Communication Manager*, 555-233-116, and the *Administrator's Guide for Avaya Communication Manager*, 555-233-506.

Adding announcements

You first need to tell the switch you want an announcement before you can record it. You assign an extension for each announcement so the switch can identify the announcement. Each extension that you choose cannot be in use, and each must conform to your dial plan.

NOTE:
Use the **change announcement** command to administer an announcement extension. See the *Administrator's Guide for Avaya Communication Manager*, 555-233-506, for more information.

Voice Announcement over LAN (VAL)

Voice Announcement over LAN (VAL) allows you to share, backup, and restore announcement files over your local area network.

MCC1, SCC1, CMC1, G600, or G650 Media Gateways: You can record announcements on a downloadable VAL circuit pack (TN2501AP), or for S8100 Media Server only, on the Integrated Scalable Speech Processor Application (ISSPA) circuit pack.You can also use TN750, TN750B, and TN750C announcement circuit packs to record announcements on your switch. You can have only one TN750 or TN750B per system, but you can use one TN750B with many TN750C and/or TN2501AP (VAL) circuit packs.

G350 or G700 Media Gateways: You can record announcements through the embedded Voice Announcement over LAN (VAL) feature, hereafter referred to as "Virtual VAL" or "VVAL".

As an example, say we have calls coming into unassigned DID extensions. Let us record a general message to tell these callers to dial the company's main number.

We'll assign the announcement to extension 1234.

MCC1, SCC1, CMC1, G600, or G650 Media Gateways: In this example, use the integrated announcement circuit pack located on 01B18. (See Systems, circuit packs, and media modules on page 16 for an explanation of the circuit pack address.)

NOTE:
Use the **`display integrated-annc-boards`** command to find the cabinet, carrier, and slot addresses of your announcement circuit packs. The ***`INTEGRATED ANNOUNCEMENT BOARD`*** form lists the location and the type, as well as showing the number of recordings and number of seconds (at the administered rate) left on each circuit pack.

G350 or G700 Media Gateways: For VVAL, use 012V9 as an example. (See Systems, circuit packs, and media modules on page 16 for an explanation of the media module address.)

Our example explains how to add an integrated announcement, but other types of announcements are available. See the *Administrator's Guide for Avaya Communication Manager*, 555-233-506, for more information about other announcement types, especially how to manage VAL announcements using the SAT and using FTP.

To add an announcement extension 1234:

1. Type **`change announcements`** and press ENTER.

   The ***`ANNOUNCEMENTS/AUDIO SOURCES`*** form appears.

Figure 9: Announcements/Audio Sources form

```
                                ANNOUNCEMENTS/AUDIO SOURCES
Ann.
No.  Ext.     Type        COR  TN  Name             Q  QLen Pr Rt   Port

1:   1234___  integrated  1_   1_  unassigned DID   n  N/A  n  32   01B18
2:   _______  __________  1_   1_  _______________  n
3:   _______  __________  1_   1_  _______________  n
4:   _______  __________  1_   1_  _______________  n
5:   _______  __________  1_   1_  _______________  n
6:   _______  __________  1_   1_  _______________  n
7:   _______  __________  1_   1_  _______________  n
8:   _______  __________  1_   1_  _______________  n
9:   _______  __________  1_   1_  _______________  n
10:  _______  __________  1_   1_  _______________  n
11:  _______  __________  1_   1_  _______________  n
12:  _______  __________  1_   1_  _______________  n
13:  _______  __________  1_   1_  _______________  n
14:  _______  __________  1_   1_  _______________  n
15:  _______  __________  1_   1_  _______________  n
16:  _______  __________  1_   1_  _______________  n
```

2 In the `Ext` field, type **1234**.

3 In the `Type` field, type **integrated**.

4 In the `Name` field, type **unassigned DID**.

5 In the `Pro` (protected) field, type **n**.

If you type **n**, users with console permissions can change the announcement. If you type **y**, the announcement cannot be changed.

6 In the `Rt` (rate) field, type **32** for TN750 circuit packs, or **64** for TN2501AP circuit packs.

7 In the `Port` field, type **01B18**.

NOTE:
For S8100 Media Server, use **1A13** as an example. For G350 or G700 Media Gateways, use **012V9** as an example.

8 Press ENTER to save your work.

VAL Manager

VAL Manager is a standalone application that allows you to copy announcement files and announcement information to and from a TN2501AP announcement circuit pack (or VVAL) over a LAN connection.

VAL Manager offers the following basic features:

- Simplified administration to add, change, and remove announcement information
- The ability to back up and restore announcement files and information
- The ability to view the status of announcements on the TN2501AP circuit pack

Contact your Avaya representative to obtain VAL Manager.

Recording announcements

MCC1, SCC1, CMC1, G600, or G650 Media Gateways: You need to have special circuit packs (TN750, TN750B, TN750C, or TN2501AP) to record announcements.

G350 or G700 Media Gateways: The announcement feature is embedded within the G700 Media Gateway, and no special media module is required.

You can record announcements using any phone or console whose Class of Service (COS) provides console permissions. You can use the **`display cos`** command to review COS permissions.

You also need the announcement feature access code for your system. Use the **`display feature-access-codes`** command to find the announcement access code.

The announcement extension must be set up before you record. Use the **`list station data-module`** command to determine the announcement extension.

In our example, use your phone to record the announcement for the unassigned DIDs to extension 1234. Our announcement access code is *56.

To record the announcement:

1 Dial the announcement access code.

In our example, we'll dial ***56**.

- If you hear dial tone, go to step 2.
- If you hear a fast busy signal, hang up and redial the FAC and extension every 45 seconds until you hear dial tone.

2 Dial the announcement extension.

In our example, we'll dial **1234**. You hear dial tone.

3 Dial **1** to begin recording.

- If you hear a beep or stutter tone, begin speaking. If the circuit pack memory becomes full during recording, the system drops your connection and does not retain the announcement.
- If you hear intercept tone, hang up and record your announcement on another extension that is assigned to a different circuit pack.

4 End the recording.

- If you are using a digital phone, press **#**. You hear dial tone allowing you to continue your session (for example, dial **2** to hear the announcement just recorded).

- If you are using an analog phone, hang up. If your analog phone is not connected through lineside DS1, the system records an electrical click at the end of the recording. You have to redial the announcement feature access code to continue your session.

NOTE:
The announcement records the sound of the receiver returning to the phone. Hang up gently, press the drop button, or press the switch hook with your finger.

5 To listen to the announcement you just recorded:

- If you are using a digital phone, do not hang up. Dial **2**. The recording plays back through the handset.

6 If you are not satisfied with the announcement,

- dial **1** to re-record the announcement.
- dial **3** to delete the announcement and end the recording session.

7 If you want to listen to the announcement after you have hung up, dial the extension from any phone or console. In this example, dial **1234**. The announcement plays through the handset.

You have to wait 15 seconds after you record the announcement before you can dial the extension to hear your announcement. During this 15-second window, you cannot record a new announcement and no one can play this announcement. You can re-record the announcement. Dial the feature access code, dial the extension, and press 2 before the 15-second timer expires.

Professional or computer recordings

If you are using the VAL TN2501AP announcement circuit pack, or if you have a G350 or G700 Media Gateway with VVAL, you can record announcements at a computer rather than at a system phone. You can also record announcements at an off-site location and transfer them using VAL Manager or File Transfer Protocol (FTP).

To be compatible with the TN2501AP circuit pack (the circuit pack is applicable to MCC1, SCC1, CMC1, G600, or G650 Media Gateways only) and Communication Manager, announcement recordings must have the following parameters:

- CCITT A-Law or CCITT μ-Law companding format (do not use PCM)
- 8KHz sample rate
- 8-bit resolution (bits per sample)
- Mono (channels = 1)

Recording new announcements at a computer

To record an announcement at a computer:

1. At the computer, open the application that you use to record “wave” (.wav) files.
2. Set the recording parameters.
3. Record the announcement by speaking into a microphone connected to the computer.
4. Play the announcement back at the computer before transferring the file to the VAL (TN2501AP) circuit pack (the circuit pack is applicable to MCC1, SCC1, CMC1, G600, or G650 Media Gateways only), or to your G350 or G700 Media Gateway.

Deleting announcements

Let us delete the unassigned DID announcement assigned to extension 1234.

We know that the announcement access code is *56. Use any console or phone with console permissions to delete the announcement.

To delete the announcement, use a phone with console permissions to complete the following steps:

1. Dial the announcement access code.

   In our example, we'll dial ***56**. You hear dial tone.

2. Dial the announcement extension.

   In our example, we'll dial **1234**. You hear dial tone.

3. Dial **3** to delete the announcement from the circuit pack.

4. Hang up the phone.

You also need to remove the information from the system. To remove the information, use your system administration terminal to complete the following steps:

1. Type **`change announcements`** and press ENTER.

   The ***`ANNOUNCEMENTS/AUDIO SOURCES`*** form appears.

2. Delete the information in the `Ext` and `Type` fields.

3. Press ENTER to save your work.

Backing up your announcements

NOTE:
To back up announcements, you need to use either FTP or VAL Manager. See the *Administrator's Guide for Avaya Communication Manager*, 555-233-506, or your Avaya representative for more information about these tools.

MCC1, SCC1, CMC1, G600, or G650 Media Gateways: Make sure you back up your announcements recorded on TN750 and TN750B circuit packs. The system loses announcements stored on these circuit packs if power is shut down or the circuit pack is removed.

The TN750C circuit pack has on-board FLASH memory so you do not have to back it up. However, you may want to back up your TN750C to another TN750C circuit pack or tape for extra security. You need to administer the data module that is built into the TN750 circuit pack before you save your announcements. See the *Administrator's Guide for Avaya Communication Manager*, 555-233-506, for more information.

CAUTION:
Do not copy, save, or restore announcements from a TN750C to a TN750 or TN750B. It may corrupt the announcement.

To backup announcements on TN750 or TN750B circuit packs:

1. Type **`save announcements`** and press ENTER to save the changes.

NOTE:
If you have both TN750B and TN750C circuit packs, save the announcements from the TN750B slot.

The save announcement process can take up to 40 minutes. You cannot administer your system while it is saving announcements.

4 Managing hunt groups

This section shows you how to set up hunt groups. It explains how calls to a hunt group are handled and shows you different call distribution methods.

What are hunt groups?

A hunt group is a group of extensions that receive calls according to the call distribution method you choose. When a call is made to a certain phone number, the system connects the call to an extension in the group.

Use hunt groups when you want more than one person to be able to answer calls to the same number. For example, set up a hunt group for:

- a benefits department within your company
- a travel reservations service

Setting up hunt groups

Let us set up a hunt group for an internal helpline. Before making changes to the switch, we'll decide:

- the phone number for the hunt group
- the number of people answering calls
- the way calls are answered

Our example dial plan allows 4-digit internal numbers that begin with 1. The number 1200 is not in use. So, we'll set up a helpline hunt group so anyone within the company can call extension 1200 for help with a phone.

We will assign 3 people (agents) and their extensions to our helpline. We want calls to go to the first available person.

To set up our helpline hunt group:

1. Type **`add hunt-group next`** and press ENTER.

   The ***HUNT GROUP*** form appears. The `Group Number` field is automatically filled in with the next hunt group number.

Figure 10: Hunt Group form

```
                              HUNT GROUP

         Group Number: 5                                   ACD? n
           Group Name: internal helpline                 Queue? n
      Group Extension: 1200                             Vector? n
           Group Type: ucd-loa                   Coverage Path:
                   TN: 1            Night Service Destination:
                  COR: 1                       MM Early Answer? n
       Security Code: __
 ISDN Caller Display: ________
```

2. In the `Group Name` field, type the name of the group.

   In our example, type **internal helpline**.

3 In the `Group Extension` field, type the phone number.

We'll type **1200**.

4 In the `Group Type` field, type the code for the call distribution method you choose.

We'll type **ucd-loa** so a call goes to the agent with the lowest percentage of work time since login.

NOTE:
The COS for all hunt groups defaults to 1. Therefore, any changes to COS 1 on the ***CLASS OF SERVICE*** form changes the COS for all your hunt groups. A COS field does not appear on the ***HUNT GROUP*** form.

5 Click NEXT PAGE to find the `GROUP MEMBER ASSIGNMENTS` page.

Figure 11: Hunt Group form, Group Member Assignments page

```
                                HUNT GROUP
          Group Number: 5   Group Extension: 1200   Group Type: ucd-loa
  Member Range Allowed: 1 - 999 Administered Members (min/max): 1  /9
                                          Total Administered Members: 3
GROUP MEMBER ASSIGNMENTS
     Ext      Name                            Ext      Name
  1: 1011                                 14:
  2: 1012                                 15:
  3: 1013                                 16:
  4:                                      17:
  5:                                      18:
  6:                                      19:
  7:                                      20:
  8:                                      21:
  9:                                      22:
 10:                                      23:
 11:                                      24:
 12:                                      25:
 13:                                      26:
At End of Member List
```

hunt groups

6 In the `Ext` field, type the extensions of the agents you want in the hunt group.

We'll type **1011**, **1012,** and **1013**.

NOTE:
For a **`ddc`** group type (also known as "hot seat" selection), the call is sent to the extension listed in the first *`Ext`* field. The system uses this form to determine the hunting sequence. See Call distribution methods on page 60 for more information.

7 Press ENTER to save your work.

The `Name` fields are display-only and do not appear until the next time you access this hunt group.

To make changes to a hunt group:

1 Type **`change hunt-group`** ***n*** and press ENTER, where ***n*** is the number of the hunt group.

2 Change the necessary fields.

3 Press ENTER to save your changes.

NOTE:
Type **`list member hunt group`** to see a list of logged-in members of a hunt group by group number. For splits and skills, the login ID, name, and different fields for EAS and Advocate appear on the list. See Call distribution methods on page 60 for a definition of "splits" and "skills."

Setting up a queue

You can tell your switch how to handle a hunt-group call when it cannot be answered right away. The call waits in a “queue.”

Let us tell the switch that up to 10 calls can wait in the queue, but that you want to be notified if a call waits for more than 30 seconds.

You also want the switch to send a warning when 5 or more calls are waiting in the queue. This warning flashes queue-status buttons on phones that have a status button for this hunt group. When the buttons flash, everyone answering these calls can see that the helpline calls need more attention.

To set up our helpline queue:

1. Type **`change hunt-group`** ***n*** and press ENTER, where ***n*** is the number of the hunt group to change.

   In our example, type **`change hunt-group`** ***5***.

   The ***HUNT GROUP*** form appears.

Figure 12: Hunt Group form

```
                              HUNT GROUP

           Group Number: 5                                ACD? n
             Group Name: internal helpline              Queue? y
        Group Extension: 1200                         Vector? n
             Group Type: ucd-loa                 Coverage Path:
                     TN: 1           Night Service Destination:
                    COR: 1                     MM Early Answer? n
          Security Code: __
     ISDN Caller Display: ________

           Queue Length: 10
Calls Warning Threshold: 5                 Calls Warning Port:
 Time Warning Threshold: 30                 Time Warning Port:
```

2. In the `Queue` field, type **y**.

3 In the `Queue Length` field, type the maximum number of calls that you want to wait in the queue.

   In our example, type **10**.

4 In the `Calls Warning Threshold` field, type the maximum number of calls that can be in the queue before the system flashes the queue status buttons.

   In our example, type **5**.

5 In the `Time Warning Threshold` fields, type the maximum number of seconds you want a call to wait in the queue before the system flashes the queue status buttons.

   In our example, type **30**.

6 Press ENTER to save your changes.

Adding hunt group announcements

You can add recorded announcements to your hunt group queue. Use announcements to encourage callers to stay on the line or to provide callers with information. You can define how long a call remains in the queue before the caller hears an announcement.

See Recording announcements on page 46 for information on how to record an announcement.

Let us add an announcement to our internal helpline. We want the caller to hear an announcement after 20 seconds in the queue, after approximately 4 or 5 rings. Our announcement is already recorded and assigned to extension 1234.

NOTE:
You can use the **`display announcements`** command to find the extensions of your recorded announcements.

To add an announcement to our helpline queue:

1. Type **`change hunt-group`** ***n*** and press ENTER, where ***n*** is the number of the hunt group to change.

   In our example, type **`change hunt-group`** ***5***.

   The ***HUNT GROUP*** form appears.

2. Press NEXT PAGE to find the `First Announcement Extension` field.

Figure 13: Hunt Group form

```
                              HUNT GROUP

                       Message Center: ________
                      AUDIX Extension: ____
            Message Center AUDIX Name: ______
                             Primary? _
Calling Party Number to INTUITY AUDIX? _
                        LWC Reception: _______
                           AUDIX Name: _______
                 Messaging Server Name: _______

                First Announcement Extension: 1234   Delay (sec): 20
               Second Announcement Extension: _____  Delay (sec):
__               Recurring? _
```

3. In the `First Announcement Extension` field, type the extension of the announcement you want callers to hear.

   In our example, type **1234**.

4. In the `Delay (sec)` field, type the number of seconds you want the caller to wait before hearing the first announcement.

   In our example, type **20**.

NOTE:
If you set the delay announcement interval to **0**, calls automatically connect to the announcement before they are queued, follow coverage, or connect to an available agent. This is called a “forced first announcement.”

5 Press ENTER to save your work.

You can use the same announcement for more than one hunt group. See the *Administrator's Guide for Avaya Communication Manager*, 555-233-506, for more information on announcements and hunt groups.

Call distribution methods

You have more call distribution choices if your company acquires Automatic Call Distribution (ACD) or Expert Agent Selection (EAS).

ACD and EAS allow you to distribute calls according to the work loads and skill levels of your agents in each hunt group. You can track call handling and monitor the efficiency of your agents.

- When you assign ACD to a hunt group, the group is called a "split."
- When you assign EAS to a hunt group, the group is called a "skill."

The following table shows 6 types of call distribution methods and the software required for each method.

Method	The system hunts for...	I need...
Direct Department Calling- (DDC)	the first agent administered in the hunt group. If the first agent is busy, it goes to the second agent, and so forth. This "hot seat" method puts a heavy call load on the first few agents.	no extra software (you cannot use this method if you have EAS enabled)
Circular (circ)	the next available agent in a chain.	no extra software

Method	The system hunts for...	I need...
Uniform Call Distribution - Most Idle Agent (UCD-MIA)	the available agent who has been idle the longest since their last call.	no extra software
Uniform Call Distribution - Least Occupied Agent (UCD-LOA)	the available agent with the lowest percentage of work time since login.	ACD, EAS, and CentreVu Advocate
Expert Agent Distribution - Most Idle Agent (EAD-MIA)	the available agent with the highest skill level who has been idle the longest since their last call.	EAS
Expert Agent Distribution - Least Occupied Agent (EAD-LOA)	the available agent with the highest skill level and the lowest percentage of work time since login.	EAS and CentreVu Advocate

5 Managing vectors and VDNs

This section provides an introduction to vectors and Vector Directory Numbers (VDN). It gives you basic instructions for writing simple vectors.

This section also outlines the enhancements made to the conferencing feature of Communication Manager.

SECURITY ALERT:

Vector fraud is one of the most common types of toll fraud because vectors route calls based on the Class of Restriction (COR) assigned to the VDN. Refer to the *Avaya Products Security Handbook*, 555-025-600, or your Avaya representative for more information.

This section references announcements, hunt groups, queues, splits, and skills, which are covered in detail in other sections of this book. You can find information about these topics in the *Administrator's Guide for Avaya Communication Manager*, 555-233-506, and the *Avaya MultiVantage™ Call Center Software Call Vectoring and Expert Agent Selection (EAS) Guide*, 555-230-714.

What are vectors?

A vector is a series of commands that you design to tell the system how to handle incoming calls. A vector can contain up to 32 steps and allows customized and personalized call routing and treatment. Use call vectoring to:

- play multiple announcements
- route calls to internal and external destinations
- collect and respond to dialed information

NOTE:
The vector follows the commands in each step in order. The vector “reads” the step and follows the command if the conditions are correct. If the command cannot be followed, the vector skips the step and reads the next step.

Your system can handle calls based on a number of conditions, including the number of calls in a queue, how long a call has been waiting, the time of day, day of the week, and changes in call traffic or staffing conditions.

Writing vectors

Writing vectors is easy, but we recommend that you set up and test your vectors before you use them across the system.

We’ll write a vector to handle calls to our main number. It is the first vector so we’ll use number 1.

NOTE:
Type **`list vector`** to see a list of existing vectors. Type **`list usage vector`** to see where each vector is used throughout the switch. Type **`list usage digit string`** to see all the vectors, vector tables, and Best Service Routing (BSR) plans that use a specific dial string.

Before you start

- On the ***`SYSTEM-PARAMETERS CUSTOMER-OPTIONS`*** form, verify the `Basic Call Vectoring` field is **y**. If not, contact your Avaya representative.

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

- To provide announcements, you need an Announcement circuit pack. See the *Hardware Guide for Avaya Communication Manager* for more information on the circuit pack.
- Use one of the following:
  - — Tone Clock with Call Classifier - Tone Detector circuit pack
  - — Call Classifier - Detector circuit pack

For G350 and G700 Media Gateways:

- To provide announcements, no circuit packs are required. The announcement feature is embedded within the media gateway, and no special media module is required.

To write a vector:

1. Type **`change vector`** ***`1`*** and press ENTER.

   The ***`CALL VECTOR`*** form appears.

The vector `Number` field on the left side of the form is filled in automatically.

Figure 14: Call Vector form

```
                                CALL VECTOR
    Number: 1             Name: main number calls
Multimedia? n                                        Lock? n
     Basic? y EAS? n   G3V4 Enhanced? n  ANI/II-Digits? n   ASAI Routing? n
 Prompting? y LAI? n  G3V4 Adv Route? n          CINFO? n             BSR? n
01
02
03
04
05
```

2 Type a description for the vector in the `Name` field.

In our example, type **main number calls**.

NOTE:
The information in the heading of the ***CALL VECTOR*** form is display only. Use the **`display system-parameters customer-options`** command to see the features that are turned on in your switch.

3 Type your vector steps in the numbered column on the left of the form.

NOTE:
When you type your vector steps, the switch automatically completes some of the vector step information for you. For example, if you type "**q**" in a vector step field, the switch fills in "**queue-to**". Also, additional fields appear when you complete a field and press `TAB`. This makes it very easy to type in your vector steps.

Now that vector 1 is set up, let us add a vector step to it to tell the switch how to handle the calls to our main number.

Putting a call in a queue

Write a vector so that calls that come into the main business number redirect to a queue.

We'll use a vector-controlled hunt group for the main number queue. This hunt group was set up as main split 47. When calls first arrive, all calls to our main number should be queued as "**pri l**" for low priority.

To queue calls, write the following vector (step 2). (Please note, we started our example on step 2 because step 1 is used later in this chapter.)

Figure 15: Call Vector form

```
                                CALL VECTOR
    Number: 1            Name: main number calls
Multimedia? n                                        Lock? n
     Basic? y EAS? n   G3V4 Enhanced? n  ANI/II-Digits? n   ASAI Routing? n
 Prompting? y LAI? n  G3V4 Adv Route? n          CINFO? n            BSR? n
01
02 queue-to main split 47 pri l
03
04
05
```

NOTE:
Remember, the switch automatically fills in some of the information when you type your vector step and press TAB.

Playing an announcement

Write a vector to play an announcement for callers in a queue. Use the announcement to ask callers to wait. You need to record the announcement before the vector can use it. For more information see Adding announcements on page 43.

Let us play our announcement 4001, asking the caller to wait, then play music for 60 seconds, then repeat the announcement and music until the call is answered. The **goto** command creates the loop to repeat the announcement and the music. **Unconditionally** means under all conditions.

NOTE:
Rather than loop your vectors directly back to the announcement step, go to the previous queue-to step. This way, if for some reason the call does not queue the first time, the switch can attempt to queue the call again. If the call successfully queued the first time through, it merely skips the queue-to step and plays the announcement. The system cannot queue a call more than once in the exact same priority level.

To play and repeat an announcement, write this vector (steps 3-5):

Figure 16: Call Vector form

```
                                CALL VECTOR
    Number: 1            Name: main number calls
Multimedia? n                                          Lock? n
     Basic? y EAS? n   G3V4 Enhanced? n  ANI/II-Digits? n   ASAI Routing? n
 Prompting? y LAI? n  G3V4 Adv Route? n          CINFO? n            BSR? n
01
02 queue-to main split 47 pri l
03 announcement 4001 (''All agents are busy, please wait...'')
04 wait-time 60 secs hearing music
05 goto step 2 if unconditionally
```

Routing based on time of day

Write a vector for calls that come in after your office closes.

Assume that your business is open 7 days a week, from 8:00 a.m. to 5:00 p.m. When calls come in after business hours, you want to play your announcement 4002, which states that the office is closed and asks callers to call back during normal hours. The call is disconnected after the announcement is played.

For after-hours treatment, write this vector (steps 1, 6, 7):

Figure 17: Call Vector form

```
1. goto step 7 if time-of-day is all 17:00 to all 8:00
2. queue-to main split 47 pri l
3. announcement 4001 (All agents are busy, please wait...)
4. wait-time 60 secs hearing music
5. goto step 2 if unconditionally
6. stop
7. disconnect after announcement 4002 (“We’re sorry, our
    office is closed...)
8.
```

If the **goto** command in step 5 fails, the switch will go to the next step. The **stop** in step 6 prevents callers from incorrectly hearing the “office is closed” announcement in step 7. **Stop** keeps the call in the state it was in before the command failed. In this case, if step 5 fails, the call remains in step 4 and the caller continues to hear music.

CAUTION:

Add a stop vector step only after calls are routed to a queue. If a stop vector is executed for a call NOT in queue, the call is dropped.

Allowing callers to leave a message

Write a vector that allows callers to leave messages. This type of vector uses a hunt group called a messaging split. For our example, we send after-hours calls to the voice mailbox at extension 2000 and use messaging split 99.

Once the vector routes a call to the mailbox, the caller hears a greeting (that was recorded with the voice mail for mailbox 2000) that tells then they can leave a message.

To let callers leave messages, write this vector (step 7).

Figure 18: Call Vector form

```
1. goto step 7 if time-of-day is all 17:00 to all 8:00
2. queue-to main split 47 pri l
3. announcement 4001 (All agents are busy, please wait...)
4. wait-time 60 secs hearing music
5. goto step 2 if unconditionally
6. stop
7. messaging split 99 for extension 2000
8.
```

Redirecting calls during an emergency or holiday

You can provide a quick way for a supervisor or agent to redirect calls during an emergency or holiday. Use a special mailbox where you can easily change announcements. This vector is also an alternative to making sure all agents log out before leaving their phones.

NOTE:

You can also use Holiday Vectoring, which simplifies vector writing for holidays and other times when you need to provide special handling for date-related calls. This feature allows you to administer up to ten different holiday tables, then use those tables to make vectoring decisions. For information, see the *Avaya MultiVantage™ Call Center Software Call Vectoring and Expert Agent Selection (EAS) Guide*, 555-230-714.

In our example, no agents are normally logged in to split 10. We'll use split 10 for an emergency. We preset buttons on our agents' phones so people with these phones can log in at the touch of a button.

To quickly redirect calls:

1. Create a special mailbox with the appropriate announcement such as "We are unable to answer your call at this time" or "Today is a holiday, please call back tomorrow."

   In our example, we recorded the mailbox greeting for extension 2001.

2. Insert the following bold vector steps (steps 1, 10, 11):

Figure 19: Call Vector form

```
01. goto step 10 if staffed agents split 10 > 0
02. goto step 8 if time-of-day is all 17:00 to all 8:00
03. queue-to main split 47 pri l
04. announcement 4001 ("All agents are busy, please wait...")
05. wait-time 60 secs hearing music
06. goto step 3 if unconditionally
07. stop
08. messaging split 99 for extension 2000
09. stop
10. messaging split 99 for extension 2001
11. stop
```

When there is an emergency, fire drill, or holiday, the supervisor or agent logs into this split.

When an agent logs into split 10, the system looks at vector step 1, sees that more than 0 people are logged into split 10, and sends calls to step 10 (which sends to messaging split 99).

When your business returns to normal and the agent logs out of split 10, call handling returns to normal.

Giving callers additional choices

You can give your callers a list of options when they call. Your vector tells the switch to play an announcement that contains the choices. The switch collects the digits the caller dials in response to the announcement and routes the call accordingly.

We'll create a vector that plays an announcement, then lets callers dial an extension or wait in the queue for an attendant.

Please note, the following example of this "auto attendant" vector is a new vector and is not built on the vector we used in the previous examples.

To let callers connect to an extension, write this kind of vector:

Figure 20: Call Vector form

```
                              CALL VECTOR
       Number: 20              Name: extension or attendant
   Multimedia? n                                          Lock? n
        Basic? y   EAS? n    G3V4 Enhanced? n   ANI/II-Digits? n   ASAI
Routing? n
   Prompting? y   LAI? n   G3V4 Adv Route? n         CINFO? n          BSR? n
1. wait-time 0 seconds hearing music
2. collect 4 digits after announcement 4004 (You have reached our
     company. Please dial a 4-digit extension or wait for the attendant.)
3. route-to digits with coverage y
4. route-to number 0 with cov n if unconditionally
5. stop
```

Inserting a step

It is easy to change a vector step and not have to retype the entire vector. Let us add announcement 4005 between step 3 and step 4 in vector 20.

To insert a new vector step in vector 20:

1. Type **`change vector 20`** and press ENTER.

   The ***CALL VECTOR*** form appears.

2. Press EDIT.

3. Type **i** followed by a space and the number of the step you want to add.

   In our example, type **i 4**.

4. Type the new vector step.

   We'll type **announcement 4005 (Please wait...)**.

5. Press ENTER to save your changes.

NOTE:
When you insert a new vector step, the system automatically renumbers the rest of the vector steps and all references to the vector steps. The switch inserts a "*" when the numbering needs more attention.

Deleting a step

To delete vector step 5 from vector 20:

1. Type **`change vector 20`** and press ENTER.

   The ***CALL VECTOR*** form appears.

2 Press EDIT.

3 Type **d** followed by a space and the number of the step you want to delete.

In our example, type **d 5**.

NOTE:
You can delete a range of vector steps. For example, to delete steps 2 through 5, type **d 2-5** and press ENTER.

4 Press ENTER to save your changes.

NOTE:
When you delete a vector step, the system automatically renumbers the rest of the vector steps and all references to the vector steps. The switch inserts a * when the numbering needs more attention.

Diagnosing a vector problem

If there is a problem with a vector, the switch records the error as a vector event. Vector events occur for a number of reasons including problems with a trunk, full queue slots, or the vector reaching the maximum 1000 steps allowed.

Use the **`display events`** command to access the ***EVENT REPORT*** form and see the event record. Use the event record to see why the vector failed.

To view the event report:

1 Type **`display events`** and press ENTER.

The ***EVENT REPORT*** form appears.

Figure 21: Event Report form

```
                          EVENT REPORT
The following option control which events will be displayed.
   EVENT CATEGORY
                  Category: Vector
   REPORT PERIOD
              Interval: _a_   From: __/__/__:__  To: __/__/__:__
   SEARCH OPTIONS
          Vector Number: ______
             Event Type: ______
              Extension: ______
```

2 To see all current vector events, press ENTER

or

Indicate the events that you want to see by completing the `Report Period` and `Search Option` fields. See the *Avaya MultiVantage™ Call Center Software Call Vectoring and Expert Agent Selection (EAS) Guide*, 555-230-714, *for more information.*

3 Press ENTER to view the report.

The ***EVENT REPORT*** (detail) form appears.

Figure 22: Event Report form (detail)

```
                                EVENT REPORT
Event  Event                   Event     Event    First        Last
Event
Type   Description            Data 1    Data 2   Occur        Occur       Cnt
  20   Call not queued        12/5      B       09/28/13:43  09/28/13:43   21
```

Look at the information in the `Event Data 1` field to diagnose the vector event. In this example, there was a problem with:

- Vector 12, step 5
- Split 89

Vector Directory Numbers

A Vector Directory Number (VDN) is an extension that directs an incoming call to a specific vector. This number is a “soft” extension number not assigned to an equipment location. VDNs must follow your dial plan.

Let us create VDN 5011 for our sales department. A call into 5011 routes to vector 11. This vector plays an announcement and queues calls to the sales department.

SECURITY ALERT:

Vector fraud is one of the most common types of toll fraud because vectors route calls based on the Class of Restriction (COR) assigned to the VDN. Refer to the *Avaya Products Security Handbook*, 555-233-600, or your Avaya representative for more information.

To add a VDN:

1. Type **add VDN *5011*** and press ENTER.

   You type the VDN extension you want to add. The ***VECTOR DIRECTORY NUMBER*** form appears.

Figure 23: Vector Directory Number form

```
                VECTOR DIRECTORY NUMBER

                   Extension: 5011
                        Name: Sales Department
             Vector Number: 11

       Allow VDN Override? n
                      COR: 1
                       TN: 1
                 Measured: both
```

2 Type a description for this VDN in the `Name` field.

In our example, type **Sales Department**.

The information in the VDN Name field appears on a display phone. This allows the agent to recognize the nature of the call and respond accordingly.

NOTE:
The Allow VDN Override field on the Vector Directory Number form controls the operation of the display.

3 Type the vector number in the `Vector Number` field.

In our example, type **11**.

4 In the `Measured` field, indicate how you want to measure calls to this VDN.

In our example, type **both** (for CMS and BCMS).

NOTE:
BCMS must be enabled to use "both." Use the **`display system-parameters customer-options`** command to see if BCMS is enabled. See the *Administrator's Guide for Avaya Communication Manager*, 555-233-506, for more information.

5 Press ENTER to save your changes.

To see the VDNs already associated with your vectors:

1 Type **`list VDN`** and press ENTER.

The ***`VECTOR DIRECTORY NUMBERS`*** form appears.

Figure 24: Vector Directory Numbers form

```
                         VECTOR DIRECTORY NUMBERS
                                                                Event
                           VDN            Vec          Orig   Notif  Skills

Name                       Ext   Ovrd  COR TN  Num   Meas  Annc   Adj 1st 2nd
3rd
Tech Support               5000   y     59  1   234   none  301
Customer Serv.             5001   n     1   1         none  302
New Orders                 5002   y     23  1   5     none  303
```

Each VDN maps to one vector. Several VDNs can map to the same vector.

Meet-me Conference

Use the Meet-me Conference to set up a dial-in conference of up to six parties. Meet-me Conference uses Call Vectoring to process the setup of the conference call.

Meet-me Conference can require an access code. If an access code is assigned, and if the vector is programmed to expect an access code, each user dialing into the conference call must dial the correct access code to be added to the call. Any user can dial the Meet-me Conference extension if the extension number is part of the customer's DID block.

Administering Meet-me Conference takes three basic steps:

1. Make sure the customer options are set up to accept Meet-me Conferencing.
2. Create a Meet-me Conference VDN.
3. Create a vector for the Meet-me Conference.

Verifying the customer options

Let us first make sure the customer options are correctly set up.

1. Type **`display system-parameters customer-options`** and press ENTER.

   The ***`OPTIONAL FEATURES`*** form appears.

Figure 25: Optional Features form

```
                         VECTOR DIRECTORY NUMBERS
                                                          Event
                           VDN            Vec          Orig   Notif  Skills

Name                       Ext    Ovrd  COR TN  Num    Meas  Annc   Adj 1st 2nd
3rd
Tech Support               5000    y     59  1   234    none  301
Customer Serv.             5001    n     1   1          none  302
New Orders
               5002   y     23  1   5      none  303
       OPTIONAL FEATURES
                                                                   Used
     G3 Version: V11                      Maximum Ports: 2800     856
       Location: 1              Maximum XMOBILE Stations: 700      0
       Platform: 2

IP PORT CAPACITIES
                         Maximum Administered IP Trunks: 200      84
           Maximum Concurrently Registered IP Stations: 480       6
             Maximum Administered Remote Office Trunks: 0         0
Maximum Concurrently Registered Remote Office Stations: 0         0
                Maximum Concurrently Registered IP eCons: 2       0
                      Maximum Administered IP SoftPhones: 1000    20

   Maximum Number of DS1 Boards with Echo Cancellation: 5         0
                             Maximum TN2501 VAL Boards: 3         1


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

2. On the first form, make sure the `G3 Version` field is set to **V11** (the default setting for Communication Manager). On the third page (not shown), make sure the `Enhanced Conferencing` field is set to **y**.

Setting up a Meet-me Conference VDN

Now let us set up a Meet-me Conference VDN. For this example, we'll set it up at extension 36090:

1. Type **add vdn *36090*** and press ENTER.

   The ***Add VDN*** form appears for extension 36090. Let us assign vector 90 to this VDN.

Figure 26: Vector Directory Number, first add form

```
                    VECTOR DIRECTORY NUMBER

                      Extension: 36090
                           Name: Meet-me Conference VDN
                 Vector Number: 90

          Meet-me Conferencing? y

                            COR: 1
                             TN: 1
```

NOTE:
If the VDN extension is part of the customer's DID block, external users will be able to access the conference VDN. If the VDN extension is not part of the customer's DID block, only internal callers on the customer's network (including DCS or QSIG) or remote access callers can access the conference VDN.

The second Add VDN form allows you to assign a six digit access code for the Meet-me conference, and to indicate the person responsible (the extension number) for controlling the access code.

Let us assign access code 937821 and extension number 80214 as the responsible party.

SECURITY ALERT:

It is recommended that you always assign an access code. However, if you do not want to assign an access code, leave the Conference Access Code field blank.

Figure 27: Vector Directory Number, second add form

```
                    VECTOR DIRECTORY NUMBER

MEET-ME CONFERENCE PARAMETERS:

  Conference Access Code: 937821
   Conference Controller: 80214
```

Creating a Meet-me Conference vector

Finally, let us create a vector for the Meet-me Conference.

NOTE:

Before you can set up a vector that references announcements, first you must set up the announcements in the system. See the chapter on Announcements in this book for more information.

1 Type **`change vector 90`** and press ENTER.

The ***CHANGE VECTOR*** form appears for VDN 90. Let us write a call vector for this Meet-me Conference. (See the following two form samples to help you set up a Meet-me Conference.)

Figure 28: Call Vector, first change form

```
change vector 90                                                Page  1 of 3
  SPE A
                                   CALL VECTOR

    Number: 90                Name: Enh Conf Vec
                     Attendant Vectoring? n    Meet-
me Conf? y            Lock? y
     Basic? y    EAS? n   G3V4 Enhanced? n   ANI/II-
Digits? n   ASAI Routing? n
 Prompting? y    LAI? n  G3V4 Adv Routs? n   CINFO? n   BSR? n   Holidays?
 n

01 collect       6 digits after announcement 12340
02 goto          step 6 if digits = meet-me-access
03 collect       6 digits after announcement 12341
04 goto          step 6 if digits = meet-me-access
05 disconnect    after announcement 12342
06 goto          step 11 if meet-me-idle
07 goto          step 14 if meet-me-full
08 announcement  12343
09 route-to      meetme
10 stop
11 announcement  12344
```

Figure 29: Call Vector, second change form

```
change vector 90                                                Page  2 of 3
  SPE A
                                   CALL VECTOR

    Number: 90                Name: Enh Conf Vec
                     Attendant Vectoring? n    Meet-
me Conf? y            Lock? y
     Basic? y    EAS? n   G3V4 Enhanced? n   ANI/II-
Digits? n   ASAI Routing? n
 Prompting? y    LAI? n  G3V4 Adv Routs? n   CINFO? n   BSR? n   Holidays?
 n

12 route-to      meetme
13 stop
14 disconnect    after announcement 12345
15 stop
16
17
18
19
20
21
22
```

This is what happens when a person calls the Meet-me Conference telephone number:

Each caller hears announcement 12340, which says something like: “Welcome to the Meet-me Conferencing service. Enter your conference access code.” Each caller enters the access code 937821. The **`collect`** vector step 1 collects the access code digits. If the access code is valid, the vector processing continues with vector step 6.

If the access code is invalid, the vector processing continues with vector step 3, which plays announcement 12341. Announcement 12341 says something like: “The access code you entered is invalid. Please enter the access code again.”

If the caller enters the wrong access code again, the vector processing continues with vector step 5, which plays announcement 12342. Announcement 12342 says something like: “This access code is invalid. Please contact the conference call coordinator to make sure you have the correct conference telephone number and access code. Good bye.” The caller is disconnected.

Vector step 6 is only valid for the first caller into the Meet-me Conference. The **`meet-me-idle`** condition routes the first caller to announcement 12344 (vector step 11). The recorded announcement says something like: “You are the first party to join the call.” The caller is then routed to the Meet-me Conference call by vector step 12 and vector processing stops.

Vector step 7 is used when the Meet-me Conference already has the maximum of six parties on the call. The **`meet-me-full`** condition disconnects the caller after playing announcement 12345 (vector step 14). The recorded announcement 12345 says something like: “This Meet-me Conference is filled to capacity. Please contact the conference call coordinator for assistance. Good bye.”

If a caller enters the correct access code, is not the first caller, and the conference call is not full, vector processing continues with vector step 8, which plays announcement 12343. The announcement says something like: “Your conference call is already in progress.” The caller is then routed to the Meet-me Conference call by vector step 9 and vector processing stops.

As each caller enters the conference call, all parties on the call will hear an “entry” tone. When the conference call is over and callers drop out of the conference call, any remaining parties on the call will hear an “exit” tone.

Options for vector steps

`collect` — When the Meet-me Conf field is enabled, the **`collect`** vector step collects the next six digits and uses those digits as the access code for a Meet-me Conference call. See vector steps 1 and 3 in the example.

`goto` — The **`goto`** vector step has two conditions:

- meet-me-idle
- meet-me-full

  The **`meet-me-idle`** condition routes the first caller accessing a Meet-me Conference to the conference call. An announcement step, saying they are the first party to access the call, can be given to the caller. See vector steps 6 and 11 in the example.

  The **`meet-me-full`** condition is used when the Meet-me Conference already has the maximum of six parties on the call. See vector steps 7 and 14 in the example.

The **goto** step vector also has an option, **meet-me access**, for the digits condition to verify that the access code is valid. If the access code entered by the caller equals the access code administered for the VDN, vector processing continues. See vector steps 2 and 4 in the example.

route-to — The **route-to** vector step has one condition: **meetme**. When successful, this condition adds the caller to the Meet-me Conference call, and all parties on the call hear an “entry” tone to signify that another caller has joined the conference. This condition is valid when the caller has entered the correct access code and there are not already six parties on the call. See vector steps 9 and 12 in the example.

If the **route-to meetme** step ever fails, vector processing stops and the caller hears busy tone.

Disabling Meet-me Conference

If you want to disable Meet-me Conference, you must first remove all Meet-me Conference VDNs and vectors. If you do not, the change is not allowed, and a message appears telling you that you must first remove all Meet-me Conference VDNs and vectors before you can disable this option.

6 Using reports

This section explains how to generate, display, list, and print some of the basic reports from Communication Manager, and provides instructions for scheduling reports.

This section also contains information on how and when to use the system monitoring reports. It explains how to interpret some of the information displayed in the reports.

Using report scheduler

Use report scheduler to print reports automatically. Because printing reports requires significant switch processor resources, it is a good idea to print reports during off-peak hours.

NOTE:
There is no port on the G350 or G700 Media Server to hook up a printer, but you can print to a LAN connected-printer. Therefore, the report scheduler would not work with a G350 or G700 Media Server.

Setting printer parameters

Report scheduler prints to the system printer connected to your switch. There are two ways to connect the system printer:

- Use a data module extension to connect to a printer outside of the switch room.
- Use the EIA port to connect directly to the printer.

Some of the defaults for the system printer are set when the system is installed. If you make any changes to your system configuration, you may need to change the system parameters for the reports to print accurately.

Let us set the parameters for the EIA port. (Note that G3R cabinets do not have EIA ports.)

To set system parameters:

1. Type **`change system-parameters features`** and press ENTER.

   The ***`FEATURE-RELATED SYSTEM PARAMETERS`*** form appears.

NOTE:
The ***`FEATURE-RELATED SYSTEM PARAMETERS`*** form contains numerous pages. Move to the page that contains the `SYSTEM PRINTER PARAMETERS` section.

Figure 30: Feature-Related System Parameters form

```
                    FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
           System Printer ENdpoint: eia              Lines Per Page: 60
               EIA Device Bit Rate: 9600

SYSTEM-WIDE PARAMETERS
                       Switch Name: ST12
      Emergency Numbers - Internal: 56107      External: 911
   No-License Incoming Call Number: 56107

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)? y
                                       UCID Network Node ID: 12
```

2 In the `System Printer Endpoint` field, type **eia**.

NOTE:
If you're connecting to a data module instead of EIA, type the extension for the data module. The EIA option is not available for DEFINITY R.

3 In the `Lines Per Page` field, type the number of lines per page.

For our example, leave the default of **60** in this field.

4 In the `EIA Device Bit Rate` field, type **9600**.

NOTE:
If you are connecting to a data module instead of EIA, the data module controls the speed.

5 Press ENTER to save your changes.

NOTE:
Check frequently to ensure that the system printer has enough paper. Reports lost due to printer failure cannot be recovered.

For more information, refer to both the *Administrator's Guide for Avaya Communication Manager*, 555-233-506, and *Reports for Avaya Communication Manager*, 555-233-505.

Scheduling and printing reports

You can schedule up to 50 reports at a time. If you need to schedule more reports, you can purchase CMS or BCMS VU. For more information on CMS and BCMS VU, see Selecting a call management system on page 112.

To schedule or print a report:

1. Type a **`list`** or **`display`** command, followed by the report name, and followed by the word **`schedule`**, and press ENTER.

   For example:

   `list measurement attendant group schedule`

   The ***`REPORT SCHEDULER`*** form appears.

Figure 31: Report Scheduler form

```
                         REPORT SCHEDULER

Job Id: 2                      Job Status: none
Command: list measurements attendant group
Print Interval: scheduled
Print Time: 23:00
      Sun: n  Mon: y  Tue: n  Wed: y  Thu: n  Fri: y  Sat: n
```

2 In the `Print Interval` field, specify one of the following print options:

- **immediate** — prints the report immediately
- **scheduled** — enables you to specify the day and time you want the report to print on a daily or weekly basis
- **deferred** — enables you to print the report once for the date and time you specify

3 For scheduled and deferred reports, complete the `Print Time` field to indicate the time you want the report to print.

NOTE:
You can schedule reports in 15-minute intervals. If a deferred report does not print within 4 hours of the scheduled time, it is canceled and you must reschedule it. If scheduled reports do not print within 4 hours, they print at the next scheduled time.

4 In the days of the week fields, type **y** for each day of the week the report should print.

5 Press ENTER to save your changes.

Listing scheduled reports

You can list all of the scheduled reports and the time and day they are scheduled to print.

To list scheduled reports:

1 Type **`list report-scheduler`** and press ENTER.

The ***`REPORT SCHEDULER`*** form appears.

Figure 32: Report Scheduler form

```
                         REPORT SCHEDULER

Job Id     Days(smtwtfs)     Time     User     Status     Type
     Command

1          nynynyn           23:00    johnston  waiting    scheduled
     list measurements attendant positions
4          nnnnynn           23:45    johnston  waiting    scheduled
     list measurements attendant-group
```

Changing scheduled reports

It is easy to reschedule the time and day a report prints. As an example, let us change the time on job ID 12 so that it prints at 10:00 p.m. (22:00).

To change the report scheduler for job ID 12:

1. Type **`list report-scheduler`** and press ENTER.

   The ***`REPORT SCHEDULER`*** form appears.

2. Locate the job ID for the report you want to change.

   In our example the job ID is 12.

3. Type **`change report-scheduler`** ***`12`*** and press ENTER.

   The ***`REPORT SCHEDULER`*** form for job ID 12 appears.

4. In the `Print Time` field, type **22:00**.

5. Press ENTER to save your changes.

Removing scheduled reports

As your needs change, you may want to remove certain reports from the report scheduler. The following example removes Job 12 from the report scheduler.

NOTE:
You can use the **`list report-scheduler`** command to determine which reports you want to remove.

To remove job 12 from the report scheduler:

1. Type **`remove report-scheduler`** ***`12`*** and press ENTER.

   The ***`REPORT SCHEDULER`*** form for job ID 12 appears.

2. Press ENTER to remove the report.

NOTE:
If you want to print a different report, you must remove the old report from the report scheduler, and then add the new report.

Analyzing report data

Most of the information displayed in these reports is measured in centum call seconds (CCS). CCS equals the amount of call traffic it takes to keep one piece of traffic-sensitive equipment busy for 0.6 minutes. To convert CCS to minutes, use the following equation:

minutes = the number of CCS/0.6

For more information, refer to *Reports for Avaya Communication Manager*, 555-233-505.

Using attendant reports

Attendant group reports enable you to assess the quality of service provided to anyone who calls your attendant. Monitor these reports to ensure that attendant groups are adequately staffed. There are three attendant reports:

- Attendant Group Measurements report — measures attendant group traffic
- Attendant Positions Report — measures individual attendant performance
- Attendant Group Performance report — measures attendant group performance

The system automatically gathers the information for these reports, so you can use them to view attendant information at any time.

Measuring attendant group traffic

The Attendant Group Measurements report provides peak hour traffic measurements for any attendant group. It displays a summary of attendant group activity for yesterday's peak, today's peak, and the last hour.

To display the Attendant Group Measurements report:

1. Type **`list measurements attendant group`** and press ENTER.

   The ***`ATTENDANT GROUP MEASUREMENTS`*** form appears.

Figure 33: Attendant Group Measurements form

```
                          ATTENDANT GROUP MEASUREMENTS

Grp Meas  ---------Calls----------  ------Time-----  Time  Speed
Siz Hour  Ans Abnd Qued H-Abd Held  Avail Talk Held  Abnd  Ans(sec)
6   1000  100 0    0    0     0     200   80   0     0     0      YEST PEAK
9   1100  106 0    0    0     0     212   76   0     0     0      TODAY PEAK
9   1500  107 0    0    0     0     224   64   0     0     1      LAST HOUR
```

There are several ways to determine if traffic flow is optimal. For example:

- If the `Time Abnd` (time abandon) field approximately equals the average delay, the attendant group is staffed appropriately.
- If the number of calls in the `Time Abnd` field is high, according to your company standards, you may need to schedule additional attendants during peak hours.

For information on how to calculate the average answering delay, and what the data in the fields represent, refer to *Reports for Avaya Communication Manager*, 555-233-505.

Measuring individual attendant performance

The Attendant Positions Report provides peak individual attendant position measurements. It displays a summary of each attendant's activity for yesterday's peak, today's peak, and the last hour. This report enables you to assess personnel performance and to identify when additional attendant training is necessary.

To display the Attendant Positions report:

1 Type **`list measurements attendant positions`** and press ENTER.

   The ***`ATTENDANT POSITIONS MEASUREMENTS`*** form appears.

Measuring attendant group performance

The Attendant Group Performance report displays the average speed of calls answered for each hour of a 24-hour period, for either yesterday or today.

To display today's Attendant Group Performance report:

1 Type **`list performance attendant today`** and press ENTER.

   The ***`ATTENDANT SPEED OF ANSWER`*** form appears.

Trunk group reports

Trunk Group Reports can help you detect traffic flow problems such as out-of-service trunks, load balance, or peak-hour blocking.

NOTE:
If a trunk appears to have intermittent service, use the **`list testcalls summary`** command to determine whether a specific trunk member is not functioning.

If you suspect a trunk is having problems, use Automatic Circuit Assurance (ACA) to monitor the trunk group. Refer to the *Avaya Communication Manager Little Instruction Book for Basic Diagnostics*, 555-233-758, for more information about ACA.

Summary of trunk group activity

The Trunk Group Summary Report displays traffic measurements for all trunk groups except for personal central office line groups. The Trunk Group Summary Report displays traffic measurements for yesterday's peak, today's peak, or the last hour.

To display the Trunk Group Summary Report for the last hour:

1. Type **`list measurements trunk-group summary last-hour`** and press ENTER.

   The ***`TRUNK GROUP SUMMARY REPORT`*** form appears.

Use this report to determine general traffic flow. For more detailed information about a particular trunk group, see Hourly trunk group activity on page 97.

The Trunk Group Summary Report allows you to determine measurement data such as the trunk group's total usage, the total number of calls, and trunk blockage.

If a trunk is out of service, see Out-of-service trunks on page 99. It is best to make adjustments to a trunk group only when all of the trunks are functioning.

For more information on interpreting the reports, refer to *Reports for Avaya Communication Manager, 555-233-505*.

Hourly trunk group activity

Trunk Group Hourly reports are used in conjunction with the Trunk Group Summary Report to locate trunk problems. For example, if the Traffic Group Summary Report indicates a traffic flow problem, run the hourly report to help you locate the problem.

When you run this report, you first specify the trunk group you want to monitor on the Trunk Group Measurement Selection form. Once you select the trunk group you want to gather data on, the system starts collecting information on the trunk group activity. The Trunk Group Hourly report can display up to 24 hours of information. For example, if you started data collection on Thursday at noon (12:00) you would have 24-hours of data by noon (12:00) on Friday.

To monitor trunk group 12 for the next hour:

1. Type **`change meas-selection trunk-group`** and press ENTER.

   The ***`TRUNK GROUP MEASUREMENT SELECTION`*** form appears.

Figure 34: Trunk Group Measurement Selection form

```
                    TRUNK GROUP MEASUREMENT SELECTION

                          Trunk Group Numbers
     1:  44     6:  12     11:        16:        21:
     2:  17     7:         12:        17:        22:
     3:   3     8:         13:        18:        23:
     4: 245     9:         14:        19:        24:
     5:  39    10:         15:        20:        25:
```

2. Move to the next blank field and type **12**.
3. Press ENTER to save your changes.

   The system records the activity of trunk group 12 for the next hour.
4. After a minimum of one hour has elapsed, type **`list measurements trunk-group hourly`** ***`12`*** and press ENTER.

   The ***`TRUNK GROUP HOURLY`*** report displays data from the previous hour.

Out-of-service trunks

The Trunk Out of Service Report lists the trunks that were out-of-service during a selected period of time. This report may include up to five out-of-service trunks and lists how many times each trunk was out during the specified time. The system records trunk-outage data for the last hour, current day, and previous day.

To display the Trunk Out of Service Report for yesterday:

1. Type **`list measurements outage-trunk yesterday`** and press ENTER.

   The ***`TRUNK OUT OF SERVICE REPORT`*** appears.

   If there are no outages, the form is blank.

The Trunk Out of Service Report samples trunk activity once per hour. Therefore, if the report covers several hours, but indicates only a small number of outages, a trunk member may be providing intermittent service.

Current trunk group status

The Trunk Group Status report displays a current view of the load on various trunk groups by showing the number of calls waiting for service. This report shows data for 60 trunk groups at a time, but you can start the display at any number you want. For example, let us display trunk groups 5 and up.

To display the Trunk Group Status report:

1. Type **`monitor traffic trunk-groups 5`** and press ENTER.

   The ***TRUNK GROUP STATUS*** report displays trunk groups 5 through 64. This report shows only administered trunk groups.

2. Press CANCEL to return to the prompt.

Least used trunks

The Trunks Lightly Used Measurements report lists the five trunk members with the lowest number of calls carried for each trunk group. The system shows trunk lightly-used data for the last hour, current day, or previous day. To display the Trunks Lightly Used Measurements report for today:

1. Type **`list measurements lightly-used-trunk today`** and press ENTER.

If the trunk member in the `Calls Carried` field has an unusually low number of calls compared to other trunk members, use Facility Test Calls to determine how a specific trunk member is functioning. To monitor a particular trunk group, use Automatic Circuit Assurance (ACA). Refer to *Avaya Communication Manager Little Instruction Book for Basic Diagnostics, 555-233-758,* for more information.

Measuring call center performance

Standard switch reports on Communication Manager provide valuable data about your center's operation.

What should I measure?

Focus on three things:

- How many calls are answered?
- How fast are calls answered?
- How cost-effective is the system?

Communication Manager has three hunt group reports that give you information about agents, hunt groups, trunks, and trunk groups to help you answer these questions. The reports are:

- Hunt Group Measurements
- Hunt Group Performance
- Hunt Group Status

The table below shows you how to monitor the performance of your call center by using these reports. To use the table, pick what you want to measure from the column headings. As you read down the column, each row shows the fields on a particular hunt group report — if any — that measure that aspect of call center performance.

Reports	How many calls are answered?	How fast?	Cost-effective?
Hunt Group Measurements	Calls Ans/Aban.	Speed Ans (sec)	Total Usage Time Available
Hunt Group Performance		Speed Ans (sec)	
Hunt Group Status		LCIQ	

For detailed information on these reports, see *Reports for Avaya Communication Manager, 555-233-505*.

How many people can use switch reports?

The number of switch administrators and super-users who can log in simultaneously to view switch reports varies with the type of configuration you have. Please see the System Capacities Table for the most up-to-date list of system capacities. The most up-to-date system capacity information is not listed in Communication Manager documentation. Instead, this information is available online at http://www.avaya.com/support.

A scheduled report counts as a login. Therefore, you should schedule reports to print during off-hours.

Viewing hunt group reports

These procedures tell you how to display or print switch hunt group reports.

Viewing Hunt Group Measurements reports

The Hunt Group Measurements report displays call data for each hunt group in your system. You can print this report for yesterday's peak, today's peak, or the last hour.

A peak hour is the hour during which the greatest usage of agent time occurred. Use this report to determine the time of day with the most traffic or to measure traffic during the previous hour.

Let us print the Hunt Group Measurements report for today's peak:

1. Type **`list measurements hunt-group today-peak print`** and press ENTER.

Viewing Hunt Group Performance reports

The Hunt Group Performance report gives both the slowest hourly average speed of answer for each hunt group and the daily average. You can run the report for today or yesterday. This report can help you quickly find times during the day when your staffing is too low.

To display a Hunt Group Performance report for yesterday:

1. Type **`list performance hunt-group yesterday`** and press ENTER.

Viewing Hunt Group Status reports

The Hunt Group Status report displays a current view of your hunt groups. This report shows 32 hunt groups at a time. To display higher-numbered hunt groups, type the number of the first hunt group to be displayed. For example, let us display hunt groups 2 and higher.

To display the Hunt Group Status report:

1. Type **`monitor traffic hunt-groups`** ***`2`*** and press ENTER.

   The ***`HUNT GROUP STATUS`*** report displays hunt groups 2 through 33.

2. Press CANCEL to return to the prompt.

This report shows all hunt groups in the range, even if you have not administered them.

For more information on interpreting any of these reports, refer to *Reports for Avaya Communication Manager*, 555-233-505.

Using security reports

Security Violation Notification lets you know when someone may be trying to break into the system. Refer to the *Avaya Communication Manager Little Instruction Book for Basic Administration*, 555-233-756, for information on how to set Security Violation Notification.

7 Understanding call centers

This section introduces you to inbound call centers. It shows how to set up a simple inbound call center and lists things to consider as you plan and design your center.

What is a call center?

A call center is a way of organizing people and equipment to achieve particular business goals. For example, you can use a call center to make several people accessible through one number or to handle multiple calls simultaneously. Call centers work by organizing staff (called agents) with specific functions or expertise into hunt groups.

Call centers use some of the features covered in other chapters of this book: hunt groups, announcements, vectors, and VDNs. In this section, we'll show you how these features work together in a call center.

Planning a call center

Good planning is crucial to setting up an effective call center. Before you administer any part of your call center, you should have a plan that is thorough and specific. Your call center plan should identify:

- the purpose of the call center — what the call center has to do to be successful
- expected call volume — the number of calls you expect per day, per week, and per month
- type of calls — whether the call center should answer internal or external calls or both
- agent functions — the major agent functions
- necessary resources — the resources you must add to the system, such as trunk groups and phones

Once you develop a plan for the call center, organize agents according to their functions. These agent groups will be your hunt groups.

Setting up the call flow

Decide how you want your system to handle calls and what you want callers to experience. You may find it helpful to list the possible situations a call may encounter. Set up the call flow by adding hunt groups, setting up queues, adding announcements, and writing vectors. Refer to earlier sections of this book for details on completing these tasks.

Let us set up an example call flow. We'll set up a hunt group so that the work load is evenly distributed and up to 2 calls wait in a queue.

1. Type **`add hunt-group next`** and press ENTER.

   The ***`HUNT GROUP`*** form appears. In our example, the next available hunt group is number 2.

Figure 35: Hunt Group form

```
                              HUNT GROUP

           Group Number: 2 ACD: n
             Group Name: Accounting                          Queue: y
        Group Extension: 2011                               Vector: y
             Group Type: ucd-mia                   Coverage Path: 1
                     TN: 1             Night Service Destination: 1234
                    COR: 1                       MM Early Answer: n
          Security Code: ______
     ISDN Caller Display: ______

           Queue Length: 2
Calls Warning Threshold: ________________     Port:  ______
 Time Warning Threshold: ________________     Port:  ______
```

2. In the `Group Type` field, type **ucd-mia**.

   This directs the call to the most idle agent — the agent who has waited the longest since handling a call to the hunt group.

3. In the `Queue` field, type **y**.
4. In the `Queue Length` field, type **2**.
5. In the `Vector` field, type **y**.
6. Complete the rest of the ***HUNT GROUP*** form.
7. Press ENTER to save your changes.

Now that we've created a hunt group, let us write a simple vector that plays announcement 2340. This announcement asks callers to stay on the line. If a call isn't answered in 1 minute, the vector sends the call to voice mail (extension 2000).

Write this vector:

Figure 36: Call Vector form

```
                                CALL VECTOR
    Number: 1            Name: main number calls
Multimedia? n                                    Lock? n
     Basic? y EAS? n   G3V4 Enhanced? n  ANI/II-Digits? n   ASAI Routing? n
 Prompting? y LAI? n  G3V4 Adv Route? n          CINFO? n            BSR? n
01 queue-to split 2 pri m
02 announcement 2340 (“You have reached...”)
03 wait-time 60 sec hearing music
06 messaging split 99 for extension 2000
```

NOTE:

Vectors are an optional feature. To see if your company has vectoring, use the ***display system-parameters customer-options*** command.

To make this vector work correctly, you need to create the announcement at extension 2340 and assign a voice mailbox to extension 2000.

Testing the system

Before your new call center goes live, test the system to make sure it works the way you expect it to work.

- With agents available, call each outside number you’ve created for the call center. Does an agent in the appropriate hunt group answer?
- With only one agent available in a hunt group, make several calls at once to that hunt group. Now that several calls are in queue, call again and listen to the treatment your call receives in queue.

If you've administered an announcement, do you hear it? Does it play when it's supposed to? If there's a music source, does it play when it's supposed to? Do queue warning lamps flash when they're supposed to?

- With all agents in Aux Work, call the hunt group. Does the call follow the intended path?

Monitoring your call center

This step never ends. Monitor your call center's performance regularly so you can solve problems quickly and adjust to changing conditions.

It's critical that you monitor a new call center closely for the first month. Use the hunt group and trunk reports described in Using reports on page 87 to track your system. If you underestimated call volume and trunk capacity, or overestimated agent productivity, you need to change your system immediately.

In addition, perform a traffic analysis when your call center begins operation. Work with your Avaya representative and your local network provider. A traffic analysis gives you a comprehensive picture of the demands on your system and how well the system is performing.

For example, trunk reports tell you how often your trunks reach 100% occupancy. Your network provider may be able to tell you how many callers are getting a busy signal from the CO when all of your incoming trunks are in use. You need both pieces of information to determine the total demand that your system needs to meet.

If your business is growing, regular traffic analysis is crucial. Use traffic analysis to project future demands on your system and plan expansions accordingly.

Viewing system capacity

The capacities of your system depend on the type of switch you have, the software you're using, and your contract with Avaya. Use the System Capacity form to view the maximum capacities of your system and your current level of usage. Remember, however, that the capacities you've purchased from Avaya may be lower than the maximums shown on the switch.

For example, to find out how many hunt groups your system can support:

1. Type **`display capacity`** and press ENTER.

   The ***`SYSTEM CAPACITY`*** form appears.

2. Go to the page that shows capacities for hunt groups, splits, or skills.

   This form shows the system limits for hunt groups and how much of this capacity is currently used.

Understanding Automatic Call Distribution

Automatic Call Distribution (ACD) is a Communication Manager feature used in many call centers. ACD gives you greater flexibility to control call flow and to measure the performance of agents.

ACD systems operate differently from non-ACD systems, and they can be much more complex. ACD systems can also be more powerful because they allow you to use features and products that are not available in non-ACD systems.

Enhancing an ACD system

All call center management systems (such as Avaya's Basic Call Management System (BCMS), BCMSVu, and the sophisticated CentreVu® Call Management System) require ACD. These management systems give you the ability to measure more aspects of your center's operation, and in more detail, than is possible with standard Communication Manager reports. For a comparison of these systems, see Selecting a call management system on page 112.

Call vectoring greatly enhances the flexibility of a call center, and most vectoring functions require ACD. Vectoring is a simple programming language that allows you to custom design every aspect of call processing. For more information on call vectoring, see What are vectors? on page 64.

Together, ACD and vectoring allow you to use Expert Agent Selection (EAS). For a variety of reasons, you may want certain agents to handle specific types of calls. For example, you may want only your most experienced agents to handle your most important customers. You may have multilingual agents who can serve callers in a variety of languages.

EAS allows you to classify agents according to their specific skills and then to rank them by ability or experience within each skill. Communication Manager uses these classifications to match each call with the best available agent.

For more information on call vectoring and EAS, see the *Administrator's Guide for Avaya Communication Manager*, 555-233-506, and the *Avaya MultiVantage™ Call Center Software Call Vectoring and Expert Agent Selection (EAS) Guide*, 555-230-714.

Selecting a call management system

Avaya provides management systems for the call centers that need more detailed and flexible reporting. These applications are optional. Contact your Avaya representative for more information.

Basic Call Management System (BCMS)	BCMS runs on the switch. With BCMS, you can print reports to a printer connected to your terminal, or schedule reports to print on the system printer.
BCMS Vu	BCMS Vu software runs on a PC with Windows 95 or Windows NT. BCMS Vu takes BCMS data and stores it on a PC. Users can run real-time and historical reports and export data to other applications such as spreadsheets.
VuStats	VuStats runs on the switch. An administrator, split supervisor, or agent uses VuStats to view BCMS data on a display telephone.
CentreVu CMS	CentreVu CMS is a large, multi-faceted reporting system that runs on a Sun SPARC server or Sun Enterprise workstation. CentreVu CMS can measure more aspects of switch performance and produce a greater variety of reports than any of the other 3 products. CMS also allows streamlined ACD administration.

Use the following criteria to help you choose a call management system.

How many people need to monitor splits simultaneously?	more than 3	use CentreVu CMS, VuStats, or BCMS Vu
	3 or fewer	use standard switch reports or BCMS
How long do you need to store report data?	more than 7 days	use CentreVu CMS or BCMS Vu
	7 days	use BCMS (summary report)
	1 day	use standard switch reports (up to 24 hours), VuStats, or BCMS (24-hour detail)
What ACD elements do you need to monitor?	work code or stroke count data, individual trunks, vectors	use CentreVu CMS
	agents, trunk groups, splits/skills, VDNs	use CentreVu CMS, BCMS Vu, BCMS, or VuStats
	trunk group or hunt group data only	use standard switch reports

Use the following criteria to help you choose a reporting system. If the following scenarios do not describe your needs, standard switch reports or BCMS are probably adequate.

Do small inefficiencies or lapses in service cause big loss of profits?	Use CentreVu CMS or BCMS Vu. Both systems have exception alerting to notify you of problems immediately.
Do you frequently generate special reports for clients or senior management?	Use CentreVu CMS or BCMS Vu. Both systems allow custom report development, though CentreVu CMS allows maximum flexibility in those reports. In addition, CentreVu CMS allows you to create forecasts of call volume and needed staffing.
Do you need an electronic wallboard to display status for your center?	Use CentreVu CMS or BCMS Vu. Both systems allow wallboard display of report data.

Where to get more information

The *Administrator's Guide for Avaya Communication Manager*, 555-233-506, has more details about BCMS, BCMS Vu, VuStats, and CentreVu CMS. For more complete information, see:

- *Avaya MultiVantage™ Call Center Software Basic Call Management System (BCMS) Operations*, 555-230-706
- *BCMS Vu Software R2 V3 Software User Guide*, 585-217-102
- *CentreVu CMS Switch Connections and Administration*, 585-215-876

Index

A

ACA. *See* Automatic Circuit Assurance (ACA)
ACD. *See* Automatic Call Distribution (ACD)
adding
  announcements, 43
  hunt group announcements, 58
  hunt groups, 54
  trunk groups, 26
  vector directory numbers, 76
address/location designation
  circuit packs, 17
  media modules, 17
admonishments, 17
analyzing report data, 93
announcements
  adding, 43
  backing up, 51
  definition, 41
  deleting, 50
  hunt group, 58
  list of options, 72
  recording, 46
  types
    delay announcements, 41
    forced announcements, 41
    information announcements, 41
  vector, 68
assigning hunt group agents, 55
attendant group measurements report, 94
attendant group performance, 96
attendant positions measurement report, 95
attendant reports, overview, 94
Automatic Call Distribution (ACD), 60, 110
  enhancing, 111
Automatic Circuit Assurance (ACA), 96
Avaya support Web site, 20, 21, 102

B

backing up, announcements, 51
Basic Call Management System (BCMS), 112
BCMS Vu, 112
Best Service Routing (BSR), 65
books
  how to order more copies, 21
BSR. *See* Best Service Routing (BSR)
buttons
  help, 15

C

cabinet, definition of, 16
call center
  Automatic Call Distribution (ACD), 110
  call flow, 106
  creating, 106
  definition, 105
  management systems, 112
  measuring agent performance, 110
  measuring performance, 109
  planning, 106
  system capacity, 110
  testing, 108
call center management system, 111
  selecting, 112
call distribution, 60
CAMA trunks, 24
CCS. *See* centum call seconds (CCS)
CentreVu CMS, 112
centum call seconds (CCS), 93
circuit pack codes, 16
circuit packs
  Integrated Scalable Speech Processor Application (ISSPA), 43
  TN2501AP, 43, 46
  TN750, 43, 46
  TN750B, 43, 46
  TN750C, 43, 46
CO trunks, 24
commands
  add hunt-group next, 54
  add trunk-group, 27
  add VDN, 76
  change announcements, 44, 50
  change console-parameters, 34, 37
  change hunt-group, 32, 57, 59
  change listed-directory-numbers, 33
commands, (continued)
  change meas-selection trunk-group, 98
  change system-parameters features, 88
  change trunk-group, 35
  change vector, 65, 73
  display announcements, 58
  display capacity, 110
  display integrated-annc-boards, 44
  display system-parameters customer-options, 66
  list measurements attendant group, 94
  list measurements attendant positions, 96
  list measurements lightly-used-trunk, 100
  list measurements outage-trunk yesterday, 99
  list measurements trunk-group hourly, 98
  list measurements trunk-group summary, 97
  list member hunt group, 56
  list performance attendant-group today, 96
  list report-scheduler, 91, 93
  list testcalls summary, 96
  list usage digit string, 65
  list usage vector, 65
  list VDN, 77
  list vector, 65
  monitor traffic trunk-group, 100
  remove report-scheduler, 93
  save announcements, 51
CPE trunks, 24
creating, call center, 106

D

delay announcements, 41
deleting a step, vectors, 73
deleting announcements, 50
DID trunks, 24
DIOD trunks, 24
directory numbers, vectors, 76
display events, 74
DMI-BOS trunks, 24

E

EAS. *See* Expert Agent Selection (EAS)
Expert Agent Selection (EAS), 60

F

File Transfer Protocol (FTP), 49
forced announcements, 41
forms, 15
  Announcements/Audio Sources, 45
  Attendant Group Measurements, 95
  Call Vector, 66 to 72, 108
    first Change, 82
    second Change, 82
  Console Parameters, 34, 38
  Event Report, 75
    detail, 75
  Feature Access Code (FAC), 37
  Feature-Related System Parameters, 89
  Hunt Group, 32, 54 to 59, 107
  Listed Directory Numbers, 34
  Optional Features, 79
forms, (continued)
  Report Scheduler, 90 to 92
  Trunk Group, 27, 29, 35
  Trunk Group Measurement Selection, 98
  Vector Directory Number, 76
    first Add, 80
    second Add, 81
  Vector Directory Numbers, 78
FTP. *See* File Transfer Protocol (FTP)
FX trunks, 25

H

handling calls
  system conditions, 64
help
  buttons, 15
  numbers to call, 21
hunt groups
  adding, 54
  announcements, 58
  assigning agents, 55
  definition, 53
  night service setup, 32

I

information announcements, 41
inserting a step, vectors, 73
Integrated Scalable Speech Processor Application (ISSPA) circuit pack, 43
ISDN-BRI trunks, 25
ISDN-PRI trunks, 25
ISSPA. *See* Integrated Scalable Speech Processor Application (ISSPA) circuit pack

L

List Directory Number (LDN), 33
list of options, vectors, 72
listing scheduled reports, 91

M

management systems, call center, 112
measuring agent performance, call center, 110
Meet-me Conference, 78
    Creating a vector, 81
    Disabling, 85
    Setting up a VDN, 80
    Vector step options, 84
    Verifying customer options, 79
message line, 16
message, vector, 70
Music on Hold, 42

N

night service
    hunt group setup, 32
    interactions, 38
    night station setup, 33
    trunk group setup, 35
    types, 31

O

out-of-service trunks, report, 99

P

performance, attendant group, 96
planning, call center, 106
printer parameters, setting, 88
printing reports, 90

Q

queue, setting up, 57
queueing calls, 67

R

recording announcements, 46
redirecting calls, vectors, 70
removing scheduled reports, 93
reports
    analyzing data, 93
    attendant group measurements, 94
    attendant positions measurement, 95
    attendant speed of answer, 96
    least used trunks, 100
    listing scheduled, 91
    out-of-service trunks, 99
    printing, 90
    scheduling, 90
    trunk group, 96
    trunk group status, 99
    trunk group summary, 97
RLT trunks, 25

S

scheduled reports, removing, 93
scheduling reports, 90
screens, *see* forms, 15
security
    concerns, 18
setting up a queue, 57
setting, printer parameters, 88
skill, definition of, 60
split, definition of, 60
status line, 16
system capacity, call center, 110
system, definition of, 16

T

TAAS. *See* Trunk Answer from Any Station (TAAS)
tandem trunks, 25
testing, call center, 108
tie trunks, 25
time of day, vector, 69
TN2501AP circuit pack, 43, 46
TN750 circuit pack, 43, 46
TN750B circuit pack, 43, 46
TN750C circuit pack, 43, 46
toll fraud, 18
trademarks, 18
Trunk Answer from Any Station (TAAS), 31, 36
trunk group
    adding, 26
    least used report, 100
    night service setup, 35
    reports, 96
    status report, 99
    summary report, 97
trunks
    CAMA, 24
    CO, 24
    CPE, 24
    DID, 24
    DIOD, 24
    DMI-BOS, 24
    FX, 25
    ISDN-BRI, 25
    ISDN-PRI, 25
    RLT, 25
    tandem, 25
    tie, 25
    WATS, 25
trunks, out-of-service report, 99

U

UUCSSpp designation, 17

V

VAL Manager, 46
VAL. *See* Voice Announcement over LAN (VAL)
Vector Directory Number (VDN), 76
vectors
    announcements, 68
    definition, 64
    deleting a step, 73
    inserting a step, 73
    list of options, 72
    message, 70
    queueing calls, 67
    redirecting calls, 70
    time of day routing, 69
    writing, 64
Virtual VAL, 43
Voice Announcement over LAN (VAL), 43

voice terminals, *see* phones
VuStats, 112
VVAL. *See* Virtual VAL

W

WATS trunks, 25
Web sites
    Avaya support, 20, 21, 102
writing vectors, 64

X

XXXVSpp designation, 17

Avaya™ Communication Manager

Little Instruction Book
for basic diagnostics

Release 1.3
555-233-758
Issue 5
May 2003

A relationship that's responsive to you

Avaya Service Agreement

Helping you serve your company's customers better

Three Ways the Service Agreement Relationship Delivers Real Value to Your Company

I — Additional support to maximize uptime

- Around-the-clock remote monitoring, proactive diagnosis and resolution delivered in seconds
  - Possible only with the Avaya Expert Systems
- Priority response times, *and* the right technical skills & necessary parts on-site
  - Intelligent dispatch possible only with the Avaya Expert Systems
- Fast and effective mobilization of resources and equipment in the event of an emergency
  - Emergency Service Plan restores phone service with interim systems

II — Proactive response to your company's needs

- Unprecedented hacker protection to manage the risk of toll fraud related losses
  - System security includes toll fraud security checks and offers toll fraud indemnification
- Proactive notice of new developments that enhance your system's quality and reliability
  - Quality Protection Plan includes hardware, software, and labor scheduled proactively with you

III — The help that your company expects and deserves

- The Avaya™ Communication Manager Helpline provides personal assistance from experts to answer questions and provide advice
  - Access to support from the National Customer Care Center
- Web-based assistance: access to unique features for managing your communications
  - On-line technical information, support, and status at:
    http://www.avaya.com/support/
- Answers that maximize your company's communications, quickly and consistently
  - Ready access to service professionals and to Avaya expertise

Value Available Only Through an Avaya Service Agreement

Available through Avaya Authorized Dealers subscribing to ServiceSpan II
Please contact your account representative for more information on Avaya Service Agreement Support

Credits

Patrons	Curtis Weeks
Supporters	Ed Cote, Randy Fox, Jerry Peel, Pam McDonnell
Writers	Renee Getter, Cindy Bittner, Larry Brown, Kim Livingston, Bob Sisterhen, John Fenner
Graphics	Laurie King, Karen Consigny
Production	Jacki Rosellen
Contributors	Cathi Schramm, Robert Plant, John O'Keefe
Web/CD Production	Ellen Heffington

Special Thanks to Kim Santich — Customer Champion; Steven Gaipa — Marketing; Rick Thompson — Communication Manager User Group; Doug Schneider, Marcia Bubeck, Barry Bunch, Dan Selvig, and Pat Dolphin — Communication Manager Helpline; Sherilyn McDaniel, Norma Kugler, and Dorothy Quintana — Avaya Switch Administrators

NOTE:
Please note: Many of these individuals are no longer in the positions listed here. However, we continue to credit them because they were instrumental in the creation and success of this book.

Copyright 2003, Avaya Inc.
All Rights Reserved

Notice

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

Preventing Toll Fraud

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

Avaya Fraud Intervention

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

How to Get Help

For additional support telephone numbers, go to the Avaya Web site:

http://www.avaya.com/support/

If you are:

- Within the United States, click *Escalation Lists*, which includes escalation phone numbers within the USA.
- Outside the United States, click *Escalation Lists* then click *Global Escalation List*, which includes phone numbers for the regional 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

Voice Over Internet Protocol (VoIP)

If the equipment supports Voice over Internet Protocol (VoIP) facilities, you may experience certain compromises in performance, reliability and security, even when the equipment performs as warranted. These compromises may become more acute if you fail to follow Avaya's recommendations for configuration, operation and use of the equipment. YOU ACKNOWLEDGE THAT YOU ARE AWARE OF THESE RISKS AND THAT YOU HAVE DETERMINED THEY ARE ACCEPTABLE FOR YOUR APPLICATION OF THE EQUIPMENT. YOU ALSO ACKNOWLEDGE THAT, UNLESS EXPRESSLY PROVIDED IN ANOTHER AGREEMENT, YOU ARE SOLELY RESPONSIBLE FOR (1) ENSURING THAT YOUR NETWORKS AND SYSTEMS ARE ADEQUATELY SECURED AGAINST UNAUTHORIZED INTRUSION AND (2) BACKING UP YOUR DATA AND FILES.

Standards Compliance

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

Product Safety Standards

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

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

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

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

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

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

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

The LASER devices operate within the following parameters:

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

Luokan 1 Laserlaite
Klass 1 Laser Apparat

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

Electromagnetic Compatibility (EMC) Standards

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

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

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

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

Federal Communications Commission Statement

Part 15:
For MCC1, SCC1, G600, and CMC1 Media Gateways:

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.

For the G700 Media Gateway:

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. 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. However, there is no guarantee that radio interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- **Reorient or relocate the receiving antenna.**
- **Increase the separation between the equipment and receiver.**
- **Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.**
- **Consult the dealer or an experienced radio/TV technician for help.**

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.

For MCC1, SCC1, G600, and CMC1 Media Gateways:
This equipment complies with Part 68 of the FCC rules. On the rear 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 the G700 Media Gateway:
This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. Located prominently on 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.

The REN is used to determine the quantity of devices which 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, G600, and CMC1 Media Gateways:

Manufacturer's Port Identifier	FIC Code	SOC/REN/ A.S. Code	Network Jacks
Off/On 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
120A3 channel service unit	04DU9-DN	6.0Y	RJ48C

For the G700 Media Gateway:

Manufacturer's Port Identifier	FIC Code	SOC/REN/ A.S. Code	Network Jacks
Ground Start CO trunk	02GS2	0.5A	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

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

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

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

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

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

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

Canadian Department of Communications (DOC) Interference Information

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

For the G700 Media Gateway:
This Class B digital apparatus complies with Canadian ICES-003.

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

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

DECLARATIONS OF CONFORMITY

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

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

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

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

http://www.avaya.com/support

All Avaya media servers and media gateways are compliant with FCC Part 68, but many have been registered with the FCC before the SDoC process was available. A list of all Avaya registered products may be found at:

http://www.part68.org/

by conducting a search using "Avaya" as manufacturer.

European Union Declarations of Conformity

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). This equipment has been certified to meet CTR3 Basic Rate Interface (BRI) and CTR4 Primary Rate Interface (PRI) and subsets thereof in CTR12 and CTR13, as applicable.

Copies of these Declarations of Conformity (DoCs) can be obtained by contacting your local sales representative and are available on the following Web site:

http://www.avaya.com/support/

Japan

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

For the G700 Media Gateway:
This is a Class B 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B 情報技術装置です。この装置は、家庭環境で使用すること
を目的としていますが、この装置がラジオやテレビジョン受信機に近接して
使用されると、受信障害を引き起こすことがあります。
取 扱説明書に従って正しい取り扱いをして下さい。

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 Web site:
http://www.avaya.com/support/

Contents

Welcome 17

- Why this book? 17
- We wrote this book for you! 17
- Information contained in this book 18
- How to use this book 19
- Security concerns 21
- Trademarks 21
- Related books 21
- Tell us what you think! 22
- How to get this book on the Web 23
- How to order more copies 23
- How to get help 24

Keeping system information 27

- Keeping baseline information 27
- Retrieving baseline information 28
- Securing backups 30

Checking system status 33

- Problem-solving strategies 33
  - Viewing the system status 34
  - Viewing general system operations 35
  - Viewing the status of a station 36
  - Viewing the status of your cabinets 37
  - Viewing changes to the system (history report) 38
- How can Avaya help? 39

Contents

Solving common problems 41

- Diagnosing a problem 41
- Solving common phone problems 42
  - The user cannot dial out 43
  - Incoming calls ring but do not reach the user 44
  - The message lamp on the phone does not go out 45
  - Diagnosing general trunk problems 45
  - Diagnosing tie trunk problems 46
  - Diagnosing modem problems 46
  - Diagnosing printer troubles 47
  - Diagnosing password, login, and terminal access problems 47
  - Diagnosing SAT problems 47
- Solving call center problems 48
  - Can't record an announcement on Integrated Announcement Boards 48
  - Callers don't hear announcement 49
  - A device in an Auto Answer hunt group doesn't respond 50
  - Too many abandoned calls 50
  - Customers complain they get a busy signal 51

Alarms and errors 53

- Maintenance reports 53
  - Alarm logs 59
  - Clearing alarm logs 62
  - Assigning alarm buttons 62

Contents

- Understanding common error types 62
  - Error type 18 – busied out 63
  - Error type 513 – equipment “missing” 64
  - Error type 1 — circuit pack removed 65
- Preventing alarms and errors 66
  - Turn off maintenance 66
  - Remove unused circuit packs 67
  - DS1 administration 68

Using features to troubleshoot 69

- Using features to troubleshoot 69
  - Automatic Circuit Assurance 69
  - Busy Verify 71
  - Facility Busy Indication 74
  - Facility Test Calls 75
  - Trunk Identification 77

Solving IP and H.323 problems 79

- Solving softphone problems 79
  - Users cannot login (register) with IP softphone 79
  - User is logged in, but cannot use softphone for calls 80
  - Cannot listen to messages with INTUITY Message Manager 80
  - Users get message “Action cannot be completed” 81
  - User cannot conference or transfer 81
  - Users cannot use Directory 81
  - Other tips 81

Contents

- Sound quality problems 82
  - Isolating problems in the LAN or the Communication Manager setup 82
  - Running a mute test 83
  - Checking the PC volume control 83
  - Checking for packet loss and jitter 83
  - Other possible causes 84
- Basic troubleshooting tools 84
  - Using ping 84
  - Using trace-route 85
  - Finding the IP address 87
  - Verifying the IP softphone registration 87
  - Verifying the trunk type 88
  - When all else fails 88

Contacting Avaya 89

- Preparing to contact Avaya 89
- Contacting Avaya 91

Glossary 93

Index 101

Avaya Customer Support web site 107

Welcome

Why this book?

You've told us that you want more information on how to keep your system up and running, and we've been listening. This book contains the basic technical knowledge you need to understand your telephone system running Avaya™ Communication Manager. There are some differences between the different versions of Communication Manager, but the information provided will help you with the most basic operations.

We wrote this book for you!

Use this book if you are a system administrator. Mark it up, make notes in it. If you are a new administrator taking over the position from someone else or if you simply want to refresh your memory, this book is for you.

Information contained in this book

The *Little Instruction Book for basic diagnostics* is divided into sections to guide you through your day-to-day operations.

"Keeping system information" explains what kind of baseline information you should keep and how to retrieve the information from your switch. It also shows you how to verify that your backups are successful.

"Checking system status" explains different problem-solving strategies. It also tells you how to view the status of your system and any changes that have been made.

"Solving common problems" tells you what questions to ask to solve common problems. It walks you through examples of diagnosing and correcting typical problems, and explains how to solve basic call center problems.

"Alarms and errors" provides information on maintenance reports, frequently- encountered error types, and how to prevent some alarms and errors.

"Using features to troubleshoot" explains how to use specific features to determine the status of phones, trunk lines, and facilities.

"Solving IP and H.323 problems" tells you how to solve basic IP softphone and IP trunk and H.323 trunk problems.

"Contacting Avaya" explains how to escalate problems to Avaya and lists what information you should gather before you call.

How to use this book

Become familiar with the following terms, procedures, and conventions. They help you use this book with your telephone system and its software.

- To “move” to a certain field, you can use the TAB key, arrows, or the RETURN key.
- A “screen” is a screen form displayed on the terminal monitor.
- In this book we always use the term phone; other Avaya books may refer to phones as voice terminals.
- If you use terminal emulation software, you need to determine which keys correspond to ENTER, RETURN, CANCEL, HELP, NEXT PAGE, etc.
- Commands are printed in bold face as follows: **command**.
- Keys and buttons are printed as follows: KEY.
- Screen displays are printed in constant width as follows: `screen display`.
- Variables are printed in italics as follows: *variable*.
- We show complete commands in this book, but you can always use an abbreviated version of the command. For example, **list configuration station** can be entered as **list config sta**.
- We show commands and screens from the newest release of Communication Manager and refer to the most current books. Please substitute the appropriate commands for your system (if necessary) and refer to the manuals you have on hand.

- If you need help constructing a command or completing a field entry, remember to use HELP.
  - When you press HELP at any point on the command line, a list of available commands appears.
  - When you press HELP with your cursor in a field on a screen, a list of valid entries for that field appears.
- The status line or message line can be found near the bottom of your monitor display. 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 our helpline.
- When a procedure requires you to press ENTER to save your changes, the screen you were working on clears and the cursor returns to the command prompt. The message line shows "`command successfully completed`" to indicate that the system accepted your changes.

You may see the following icons in this book:

Tip:
Draws attention to information that you may find helpful.

NOTE:
Draws attention to information.

CAUTION:
Denotes possible harm to software, possible loss of data, or possible service interruptions.

SECURITY ALERT:
Indicates when system administration may leave your system open to toll fraud.

Security concerns

Toll fraud is the theft of long distance service. When toll fraud occurs, your company is responsible for charges.

Call the Avaya Security Hotline at 1 800 643 2353 or contact your Avaya representative for more information. Refer to the *Avaya Products Security Handbook*, 555-025-600, for tips on how to prevent toll fraud.

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.

Related books

The *Avaya™ Communication Manager Little Instruction Book for basic administration*, 555-233-756, and the *Avaya™ Communication Manager Little Instruction Book for advanced administration*, 555-233-757, are companions of this book. We suggest you use them often.

The *Administrator's Guide for Avaya™ Communication Manager*, 555-233-506, explains system features and interactions in detail. It provides a reference for planning, operating, and administering your system, and we refer to it often. Please note that prior to April 1997, this same information was in two separate books: the *DEFINITY Implementation* and the *DEFINITY Feature Description* books.

We also refer to the *Overview for Avaya™ Communication Manager*, 555-233-767, *Administration for Network Connectivity for Avaya MultiVantage™ Software*, 555-233-504, and the *Avaya Products Security Handbook*, 555-025-600.

Tell us what you think!

Let us know what you like or don't like about this book. Although we can't respond personally to all your feedback, we promise we will read each response we receive.

Write to us at:	Avaya Inc. Product Documentation Group Room B3-H13 1300 W. 120th Avenue Denver, CO 80234 USA
Fax to:	1 303 538 1741
Send email to:	document@avaya.com

Mention this document's name and number, *Avaya™ Communication Manager Little Instruction Book for basic diagnostics*, 555-233-758. Your comments are of great value and help improve our documentation.

How to get this book on the Web

If you have internet access, you can view and download the latest version of the *Avaya™ Communication Manager Little Instruction Book for basic diagnostics*, 555-233-758. To view the 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.

To access the latest version:

1. Access the Avaya customer support Web site at http://www.avaya.com/support/.
2. Click **Product Documentation**.
3. Type **555-233-758** (the document number) in the Search Product Documentation search 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 more copies

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 Attn: Avaya Account Management 200 Ward Hill Ave Haverhill, MA 01835 USA
E-mail:	totalware@gwsmail.com
Order:	Document No. 555-233-758, Issue 5, May 2003

We can place you on a standing order list so that you will automatically receive updated versions of this book. For more information on standing orders, or to be put on a list to receive future issues of this book, please contact the Avaya Publications Center.

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.

- If you are within the United States, go to the Avaya Web site at http://www.avaya.com/support/ for support telephone numbers. Click the **Escalation Lists** link, which includes escalation phone numbers within specific regions of the United States. If you are outside the USA, also click the **Global Escalation List** link for the phone numbers for the regional Centers of Excellence.

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

Communication Manager Helpline (for help with feature administration and system applications)	1 800 225 7585
National Customer Care Center Support Line (for help with maintenance and repair)	1 800 242 2121
Avaya Toll Fraud Intervention	1 800 643 2353
Avaya Corporate Security	1 800 822 9009

Keeping system information

This section explains what kind of system records to keep and how to collect the data. It also tells you how to make sure your backups are successful.

Keeping baseline information

Baseline information consists of:

- the original switch configuration
- any upgrades and changes
- switch capabilities (for example, if your company uses a call center or telecommuting)

The very best set of records starts with information on the original set up of your switch. Most companies keep at least one paper copy of baseline information, with duplicate paper or electronic copies kept off site. Update this information any time you make changes to your switch.

Use baseline information to help you diagnose problems with your phone system. Also, this information is crucial in the event you need to reconstruct the information on your switch, such as in a disaster recovery.

Tip:

Avaya Warranty and Service Agreement customers are automatically enrolled in the Emergency Service Plan. The plan provides coverage for disasters such as fire, flood, and storms. Under this plan, Avaya restores basic telephone service on a priority basis. We can also lease a system running Communication Manager to Warranty and Service Agreement customers or can ship a replacement system, if necessary.

Retrieving baseline information

You can retrieve much of the hardware and configuration information you need right from your System Administration Terminal (SAT).

- Use **display** commands to see individual records.
- Use **list** commands to view a group of records.

If you are using an SAT with a local printer attached, you can also:

- Add **print** to display or list commands to create paper copies of the records from your switch.
- Add **schedule** to a **display** or **list** command to create paper copies of the records at the system printer (if administered).

Tip:

Be sure your printer is set up to print from the SAT. See the Avaya™ Communication Manager Little Instruction Book for basic administration, 555-233-756, for more information.

Keep track of the equipment and settings listed in the following table. Use the commands in the table to access the appropriate screens.

switch component	**information**	**group records**	**individual records**
switch configuration	the features your company purchased	display system parameters customer-options	
switch capacity	capacities enabled on your system	display capacity	
cabinets and carriers	number of cabinets and carriers	list cabinet	
circuit packs	board type and vintage	list configuration all	display circuit-packs
trunks	type of service	list trunk-group	display trunk-group *n*
phones	model number, extension number, name, location, cable, and jack	list station list extension-type	display station *n* display extension *n*
class of restriction (COR)	calling privileges	list cor	display cor *n*
class of service (COS)		display cos	
feature access codes		display feature-access-codes	
feature parameters		display system-parameters features	
dial plan		display dialplan	
coverage paths		list coverage path	display coverage path *n*

switch component	information	group records	individual records
announcements	extension, type, name, port	display announcements	
vectors	Vector Directory Number (VDN), vector number	list vector list VDN	display vector *n* display VDN *n*
hunt groups		list hunt-group	display hunt-group *n*

Securing backups

Backup your system regularly to keep your records up to date.

- Use **save translations** to backup changes to your switch.
- Use **save announcements** to backup changes to announcements.

To verify that a backup was successful, review the `Command Completion Status` field.

- If the status field says `Success`, then the backup of the translations or the announcements was successful.
- If the status field does not say `Success`, record the Error Code and use the following list to determine what happened:
  - 1 = unable to save to active-spe device
  - 2 = unable to save to standby-spe device

Tip:

See the Avaya™ Communication Manager Little Instruction Book for basic administration, 555-233-756, for more information on performing backups.

Checking system status

This section explains how to use switch information to keep track of the general health and status of your system. It tells you how to access system-wide and individual information, and describes how to check when changes are made to your system.

Problem-solving strategies

As an administrator, one of your responsibilities is to check the status of your switch to determine whether it is performing properly. This is a proactive approach to system diagnostics.

- Use the **status** command to check on the operation of your system. See "Viewing the system status" for more information.
- Use **display alarms** and **display errors** to closely monitor your switch. See "Alarms and errors" on page 53 for more information.

Another of your responsibilities is to respond to reports of phone problems from your users. You generally have to use a reactive approach to system diagnostics to perform this important function. See "Solving common problems" on page 41 for more information.

Viewing the system status

Use system status screens to monitor various parts of your system. To be prepared for problems, you'll want to become familiar with what these reports look like when your system is operating well.

To view a list of the types of status reports you can run:

1. Type **status** and press HELP.

   The HELP screen appears.

   This screen lists all the possible items for which you can request status.

Help screen for status command

```
Please enter one of the following object command words:
access-endpoint          hardware-group           psa
administered-connection  health                   processor-channels
attendant                interface                remote-access
bri-port                 journal-link             signaling-group
card-mem                 link                     sp-link
cdr-link                 logins                   station
clan-ip                  mst                      synchronization
clan-port                packet-interface         sys-link
cleared-alarm-notif      periodic-scheduled       system
conference               pms-link                 trunk
data-module              pri-endpoint             tti
esm
```

Let's look at a few example status screens.

Viewing general system operations

Use the STATUS HEALTH screen to determine whether everything is operating smoothly and to see a summary of your system status. You can use this report to look at alarms, see if anything is busied out, or check for any major problems.

To view the STATUS HEALTH screen:

1. Type **status health** and press RETURN.

   The STATUS HEALTH screen appears.

Status health screen

```
_______: status health (page 1) 2/26/2002 2:27:15 PM

SPE: B/auto     A/functional          OCC:St:  2%   Sm: 23%  Cp:  1%  Idl: 74%
PNC: B-PNC/auto A-PNC/functional   ALARMS:Maj: 16  Min:   3 Wrn: 505
Pwr: comm Sync:primary  Logins:5  BUSYOUT:Trk:  0  Stn:   0 Oth:   0

Cab EmTr  Maj Min Wrn PNC                Cab EmTr  Maj Min Wrn PNC
 1  auto-   0   1  57 up                  __ _____ ___ ___ ___ ___
 2  auto-   0   0  51 up                  __ _____ ___ ___ ___ ___
 3  auto-  16   1  54 up                  __ _____ ___ ___ ___ ___
 4  auto-   0   1 103 up                  __ _____ ___ ___ ___ ___
 5  auto-   0   0 240 up                  __ _____ ___ ___ ___ ___
```

Viewing the status of a station

Use **status station** to view the setup of each individual station. This command is often the first place to gather information when a user reports a problem with a phone.

For example, if a user tells you that the phone rings a short ring and the call goes directly to coverage, use **status station** to see if send all calls (SAC) is activated on the user's extension.

To view the status of extension 7236:

1. Type **status station 7236** and press RETURN.

   The `GENERAL STATUS` screen appears. In our example, you can see that this 6408D+ phone is working properly (in-service/on-hook), but send all calls (SAC) is active. This would explain why they cannot answer their calls before they go to coverage.

General Status screen

```
                                GENERAL STATUS
                   Type: 6408D+              Service State: in-service/on-hook
              Extension: 7236             Download Status: not-applicable
                   Port: 02A0306            SAC Activated? yes
            Call Parked? no              User Cntrl Restr: none
       Ring Cut Off Act? no             Group Cntrl Restr: none
 Active Coverage Option: 1             CF Destination Ext:
        Message Waiting:
        Connected Ports:

               ACD STATUS                        HOSPITALITY STATUS
 Grp/Mod Grp/Mod Grp/Mod Grp/Mod Grp/Mod      Awaken At:
    /       /       /       /       /          User DND: not activated
    /       /       /       /       /         Group DND: not activated
    /       /       /       /       /        Room Status: non-guest room
        On ACD Call? no   Occupancy: 0.0
```

Viewing the status of your cabinets

Use the `SYSTEM STATUS CABINET` screen to become familiar with the service state of your individual cabinets. This screen also reports any alarms against your cabinets.

To view the status of your system cabinets:

1. Type **status system all-cabinets** and press RETURN.

   The `SYSTEM STATUS CABINET` screen appears.

System Status Cabinet screen

```
                          SYSTEM STATUS CABINET 1
                         SELECT  SPE ALARMS    TONE/  SERVICE SYSTEM  SYSTEM
SPE  MODE                SWITCH  MAJOR MINOR   CLOCK  STATE   CLOCK   TONE
1A   standby              auto     0    0       1A     in     standby standby
1B   active               spe b    0    0       1B     in     active  active
    SERVICE   CONTROL  DEDICATED          SERVICE  BUS ALARMS    BUS   OPEN BUS
TDM  STATE    CHANNEL    TONES      PKT   STATE  MAJOR MINOR   FAULTS  LEADS
1B    in         n         n
1A    in         y         y       1       in     n     n       0        0
EMERGENCY     SELECT                    SERVICE              CABINET
TRANSFER      SWITCH      EXP-LINK      STATE     MODE       TYPE
1A            on          01A01-02A01    in       active     MCC
1B            auto-off    01B01-02B02    in       standby
```

Using a number of the status commands can go a long way in helping you know if your system is running OK.

Viewing changes to the system (history report)

Use the history report to see what kind of changes have been made to your system. For example, if users report that the coverage on their phones is not working, check the history report to see if any changes have been made to a coverage path.

The history report lists the date, time, login level, action taken, and the screen for any change to your system. The history report does not show you exactly what data or field was changed.

To view the history report and review the recent changes to your system:

1. Type **list history** and press RETURN.

   The `HISTORY` screen appears.

History screen

```
                                    HISTORY
          Date of Loaded Translation: 2:48pm Sat Jul 26, 1997
Date  Time Port      Login   Actn  Object       Qualifier
3/16  2:33 INADS     inads   logn
3/16  1:16 INADS     inads   logf
3/16  1:16 MGR1      craft   logf
3/16  0:39 INADS     inads   logn
3/15  7:17 MGR1      craft   cha   hunt-group   2
3/15  7:05 MGR1      craft   cha   system-param features
3/15  7:04 INADS     inads   logf
3/15  7:04 MGR1      craft   cha   system-param features
3/15  7:04 MGR1      craft   cha   coverage     path 1
3/15  7:03 MGR1      craft   cha   system-param features
3/15  6:09 MGR1      craft   cha   console-para
3/15  6:06 MGR1      craft   add   station      next
3/15  6:06 MGR1      craft   add   station      next
3/15  5:35 MGR1      craft   cha   console-para
```

How can Avaya help?

With an Avaya Service Agreement or warranty coverage, your system running Communication Manager is linked to Avaya Expert Systems for constant remote monitoring, proactive diagnosis and trouble resolution. This electronic monitoring is so effective that 70% of all troubles are remotely identified, diagnosed, and resolved. This round-the-clock coverage is the best in the industry, helping to provide maximum up-time for your voice communication system.

Also, Avaya is the first in the industry to provide Power Surge Protection, completely covering the costs of product damage due to power surges. You are automatically covered if your system is under Warranty or Service Agreement, and power protection has been installed, all local and national electrical codes have been followed, and Avaya site requirements have been met. Service Agreement and warranty customers will receive first priority toward resolution of these problems.

Solving common problems

This section tells you the questions to ask and the information to gather to solve some of the most basic phone problems. It also describes how to solve common call-center problems.

Diagnosing a problem

As a system administrator, an important part of your job is to respond to trouble calls from users. You can identify some of the most common of these problems by following a few simple steps, asking the right questions, and trying to recreate the problem.

Use a set of questions to determine if:

- the equipment or process has worked before and is now broken, or if this is a new set-up that you need to correct
- the problem comes from your company's own equipment, or if the problem comes from your vendor
- the problem originates within your switch, or if the source of the problem is outside of your own facility

Ask the following basic questions of yourself, your users, and other switch administrators who work with you:

- Is this a new feature or piece of equipment, or did it work before but does not work now?
- Does the trouble arise when dialing outside the switch, dialing into the switch, or dialing inside the switch?
- Can we duplicate the problem?

Solving common phone problems

This section describes the approach that many administrators take to diagnose and correct common problems. Following is a list of suggested actions you can take if you have a problem.

- ask for the exact symptoms
- try to duplicate the problem or have the user show you the problem
- look at the phone
- find out if the phone was swapped out
- check the physical connections (for example, see if the phone is plugged in)
- check that the phone is where it is supposed to be
- try the phone at another location
- ask if the cord or handset was changed
- check **status station**
- use **display station** to look at the station screens page-by-page
- check the station screens for SAC, coverage paths

- look at printed switch records for discrepancies
- check the alarms and errors logs
- clear any alarms and errors
- test the circuit packs

Let's take a look at the types of problems users report to their system administrators, and see how to diagnose and correct the problem.

The user cannot dial out

A user calls to report that his phone "does not work." Strangely enough, this seems to be the most commonly reported problem! Ask questions to find out what is really wrong and how to fix it.

To find out why a phone "does not work," ask these questions:

- How does the phone "not work?" Does the problem occur when:
  - — they try to answer a ringing incoming call
  - — they try to make a call
- If the problem occurs when they try to make a call, is the call
  - — internal, station to station
  - — external, to an outside phone
- Is the problem with just one number, or are they unable to place any outgoing calls?
- Is this a new phone, or is this a new problem with an existing phone (were they able to call out before)
- Do they hear dial tone before they try to call?

- What do they hear after they dial?
  - — a tone of some kind
  - — a message
  - — static
  - — nothing
- If they hear a message after they dial, what is the exact message?

  If the message says that the call cannot be completed as dialed, the problem is likely your ARS programming. See the *Avaya™ Communication Manager Little Instruction Book for basic administration*, 555-233-756, for more information on changing your outbound routing.

Incoming calls ring but do not reach the user

Another user calls to report that his phone “does not work.” Ask questions similar to the ones listed above. You determine that the user can call out, and that the phone rings but there is no call on the line when the user picks up.

Type **status station** to see if send all calls (SAC) is activated.

The message lamp on the phone does not go out

This problem often occurs even when the messages associated with the phone have been cleared.

To clear a message waiting light:

1. At the command prompt, type **clear amw all *n***, where ***n*** is the extension, and press RETURN.

Diagnosing general trunk problems

The following questions help you determine a problem with a trunk.

- Is the trouble on every call or is the trouble intermittent?
- Are you getting any sort of recordings when you try to dial out on this trunk?
- Can you identify the trunk in question?

  Use a trunk access code (tac) to identify the trunk, especially if the console has a trunk ID button.
- Is there static on the call?

  This is likely a problem with the trunk external to the switch.
- Have you notified your vendor of this problem?

Diagnosing tie trunk problems

- Is the problem on incoming calls only?
- Is the problem on outgoing calls only?
- What happens when you try to use this trunk?
- Have you notified the T1 vendor?
- Does this trunk connect to another location?

  If so, try to determine the IL number of that location.
- Do you know the circuit ID of this trunk?

Diagnosing modem problems

- What is the extension of the modem?
- Is the modem connected through the switch?
- What is the modem connected to?

  For example, computer, fax, or CMS?
- Have the setup options been changed or checked recently?
- What company manufactures the modem?
- What is the model number?

Diagnosing printer troubles

- What is the problem with the printer?
- What is the printer used for?

  For example, is it connected to the switch, CMS, CAS, or maybe AUDIX?
- Who manufactures the printer?
- What is the model number?

Diagnosing password, login, and terminal access problems

If the problem is with remote dial-in access, ask:

- How do you dial in?
- What type of software or dialing program do you use?
- What error messages do you see when you try to dial in?

If your password expired, is not working, or is incorrect, call Avaya for assistance in getting the issue resolved.

Diagnosing SAT problems

- What type of terminal is it?
- What type of trouble are you having?

Solving call center problems

This section helps you identify and solve common problems affecting hunt groups, splits, announcements, and caller access.

The tables below describe symptoms and solutions for common problems in call centers not using ACD or call vectoring.

Can't record an announcement on Integrated Announcement Boards

Possible Causes	Solutions
You do not get port 0 when you start to record an announcement.	If port 0 is in use when you start to record an announcement, you hear a reorder (or fast-busy) tone followed by silence. Redial the announcement access code and extension every 45 seconds until your recording session is successful.
The phone you are using to record the announcement does not have a COS with console permission.	Use the station screen to change the COS for that phone to a different COS that has console permissions.
The Pro (protected) field on the Recorded Announcements screen is **y**.	Set this field to **n** to allow changes from a phone with console permissions.
The proper procedure was not used.	Try again. Verify the Feature Access Code (FAC) you're using.
The extension you want to use is not assigned to an announcement.	Check the number you're dialing, or assign the extension to an announcement on the Recorded Announcements screen.

Can't record an announcement on Integrated Announcement Boards

Possible Causes	Solutions
There is insufficient time left on the announcement board.	Use **list integrated-annc-boards** to display the Integrated Announcement Board screen to show the time remaining on each board. ■ Create a shorter announcement. ■ Shorten existing announcements. ■ Rerecord existing announcements at a lower compression rate. Be sure the audio quality at the lower compression rate is acceptable. ■ Delete some announcements. ■ Add an additional announcement board.

Callers don't hear announcement

Possible Causes	Solutions
All announcement ports are frequently busy and no queue is administered for the announcement.	Set the Q field on the Recorded Announcements screen to **y**. (Set this field to **y** for every extension assigned to an integrated announcement board.) If the problem continues, add another announcement board.
No announcement is recorded.	Dial the announcement extension. If you hear a fast busy signal, there is no announcement. Record one.
The announcement board malfunctioned.	Re-record the announcement.

A device in an Auto Answer hunt group doesn't respond

Possible Causes	Solutions
The device is off or malfunctioning.	With UCD-MIA, since a malfunctioning unit will be the most idle port all calls to the hunt group may begin to go to the malfunctioning device. 1. Dial each modem's extension until you find the one that isn't answering. 2. Busy out that device, or remove its extension number from the Hunt Group screen until the device can be fixed.

Too many abandoned calls

Possible Causes	Solutions
There is no coverage path.	Assign a coverage point in the Coverage Path field on the Hunt Group screen.
Announcements are not being used or need to be changed.	Create announcements that encourage callers to wait. Tell callers their call is very important and ask them to stay on the line.
Customers aren't willing to wait until the call is answered.	Add agents to reduce average speed of answer.

Customers complain they get a busy signal

Possible Causes	Solutions
Trunk capacity is insufficient.	Check the system Trunk Summary report, including yesterday-peak, today-peak and last hour. Print last-hour once an hour during business hours. Check the % ATB (All Trunks Busy) field for both incoming and two-way trunks. If this figure is consistently high for ONE-WAY incoming trunks, calls are probably being blocked. Add trunks. If ARS is being used on a two-way trunk, it may need further investigation. Communication Manager can't tell you if calls are being blocked in the central office. Ask your network provider to do a traffic study on incoming calls.
The administered queue length is too short.	Set the Queue Length field on the Hunt Group screen to a value equal to or greater than the number of hunt group agents. Add more agents.
There's no coverage path.	Assign a coverage point in the Coverage Path field on the Hunt Group screen.

Alarms and errors

This section is for adventurous administrators who are curious about how to diagnose and fix common problems. The information here will help you understand how to read and interpret:

- error logs
- alarm logs

Maintenance reports

Avaya™ Communication Manager monitors many switch components. When a component fails or performs unacceptably, the subsystem generates two kinds of reports:

- detailed reports in the error log
- general reports in the alarm log

The system detects error conditions in its components through Maintenance Objects (MO). MOs are the software modules that monitor, test, and report possible fault conditions.

Viewing error logs

It is a good idea to run and inspect error logs on a regular basis. You can view all active system errors on the error log. You can also specify a particular component of your system or a certain time period to be reported on the error log.

To view the error log:

1. Type **display errors** and press RETURN.

   The `ERROR REPORT` screen appears.

Error Report screen

```
                              ERROR REPORT
The following options control which errors will be displayed.
   ERROR TYPES
      Error Type:                Error List: active-alarms
   REPORT PERIOD
      Interval: a      From:   /  /  :   To:   /  /  :
   EQUIPMENT TYPE ( Choose only one, if any, of the following )
                         Cabinet:
                    Port Network:
                    Board Number:
                            Port:
                        Category:
                       Extension:
        Trunk ( group/member ):   /
```

2. To see all current errors, press RETURN

   OR

   Indicate the errors that you want to see by entering the information requested in each field. See the field descriptions listed in the following section.

3. Press ENTER to view the report.

Error report field descriptions

Field	What to enter
`Error Type`	error type
`Error List`	active-alarms, errors, or cleared-errors
`Interval`	h(our), d(ay), w(eek), m(onth), a(ll)
`From/To`	time interval by date and time
`Cabinet`	cabinet number (1 - 44)
`Port Network`	port network number (1 - 44)
`Board Number`	5-character board number in **UUCSS** format: UU = cabinet (1-44), C = carrier (A-E), SS = slot (0-20)
`Port`	7-character port address in **UUCSSss** format: UU = cabinet (1-44), C = carrier (A-E), SS = slot (0-20), ss = circuit
`Category`	category name (choose from the list below):

adm-conn	announce	bri/asai	cdr	data-mod
detector	dup-spe	environ	exp-intf	ext-dev
generatr	inads-link	infc	maint	mass-st
mbus	memory	misc	mmi	mnt-test
modem	mssnet	pkt	pms/jrnl	pnc
pncmaint	pnc-peer	procr	quick-st	s-syn
spe	stabd	stacrk	stations	sys-link
sys-prnt	tape	tdm	tone	trkbd
trkcrk	trunks	vc	vsp	wideband
wireless				

`Extension`	assigned extension, or blank
`Trunk Group`	group number between 1-666
`Trunk Member`	group member between 1-255, or blank

Hardware Error Report

```
                    HARDWARE ERROR REPORT - ACTIVE ALARMS

Port     Mtce     Alt    Err   Aux     First       Last      Err Err Rt/ Al Ac
         Name     Name   Type  Data    Occur       Occur     Cnt Rt  Hr  St
01AXX1   PI-LINK         257   25    05/02/08:07  05/04/08:38 255 5  13  a  n
01AXX1   PI-LINK         2049  1     05/02/12:03  05/02/12:03 1   0  0   a  n
01AXX1   PI-LINK         1     25    05/02/18:48  05/03/13:57 2   0  0   a  n
01A0101  DIG-LINE Attd1  1537  40968 05/02/12:29  05/02/12:29 1   0  0   a  n
01A0101  DIG-LINE Attd1  513   0     05/02/12:29  05/02/12:29 3   0  0   a  n
```

Make special note of the information in these fields:

- The `Port` field contains information in several formats:
  - circuit pack address (UUCSS)
  - port address (UUCSSss)
  - 2-digit signaling number
  - administered port network number
- `Mtce Name` (the name of the Maintenance Object)
- `Alt Name` (the extension with the error)
  In this example, Attd1 is the digital port with the errors.
- `Err Type` (represents the error condition category)
- `Aux Data` (represents a detail of the Error Type)
- `First Occur` (indicates the date/time of the first occurrence)
- `Last Occur` (indicates the date/time of the last occurrence)
- `Err Cnt` (lists how many occurrences since the first one)

Interpreting the error log

The `HARDWARE ERROR REPORT` in our example shows five error entries. The switch detected an unplugged digital phone. Here is how to interpret the report:

- `PI-LINK` is the MO monitoring the processor interface links to digital equipment, including adjuncts. You can see that over 2 days (May 2 to May 4) it incurred 255 type-257 errors, 1 type-2049 error, and 2 type-1 errors.
- The `DIG-LINE` errors indicate that the system can't find the phone administered to port 01A0101. According to the switch, that is supposed to be attendant 1 (`Alt Name`).

Notice that the `Err Type` and `Aux Data` fields for both MOs contain many different numbers. The numbers are software codes that represent a specific error condition.

Clearing the error

If an important component in your system fails, the software records that "event" with code numbers in the error or alarm log.

To interpret the error codes and clear the error:

1. Look up the MO (for example, `DIG-LINE` or `PI-LINK`) in the Communication Manager maintenance books for your switch.
2. Find the error type in the Hardware Error Type table for that MO.

3. Find the note associated with that error type for an explanation of the conditions that generated the error.
4. Perform the recommended procedure to clear the error.

   The recommended procedure may require you to test alarmed components. Be sure to have test permissions enabled.

   If any tests fail or abort, you will get an error code for the test.
5. Look up the test error code by MO in your Communication Manager maintenance books.
6. Find the numbered test listed in the test results.
7. Look for the correct *combination* of error code and test result in the numbered-test tables.

Alarm logs

Alarms are classified as major, minor, or warning, depending the degree of severity and the effect on the system.

warning level and description	reported to INADS?	reported to console?	take this action
major Critical service degradation	Y	Y (occurs after 4 attempts to call INADS)	Immediate attention
minor Some service degradation, but system is operable, usually limited to a few trunks or stations or a single feature.	Y	Y (occurs after 4 attempts to call INADS)	Check to see what service is affected
warning Failure that causes no significant service degradation Note: DS1 off board faults (error type 138) generate warning alarms only, indicating a customer network problem. In this case, warning alarms can cause critical service degradation.	N (INADS can receive some downgraded warning alarms)	N	Monitor the situation; check for service or equipment interruption or failure outside the switch.

Alarms are further classified as:

- *on-board* problems originate within the circuitry of the alarmed circuit pack
- *off-board* problems originate in a process or component that is external to the circuit pack

Reading the alarm log

Let's look at an alarm log that results from an unplugged digital phone.

To the view the alarm log:

1. Type **display alarms** and press RETURN.

   The ALARM REPORT screen appears.

Alarm Report screen

```
                                ALARM REPORT
The following options control which alarms will be displayed.
  ALARM TYPES
             Active? y    Resolved? n
              Major? y       Minor? y      Warning? y
  REPORT PERIOD
            Interval: m      From:   /  /  :      To:   /  /  :
  EQUIPMENT TYPE ( Choose only one, if any, of the following )
                         Cabinet:
                    Port Network:
                    Board Number:
                            Port:
                        Category:
                       Extension:
        Trunk ( group/member ):   /
```

2. Indicate which alarms you want to view by entering **y** and ENTER after each alarm type.

Tip:

Unless you can restrict the trouble to a particular time period, press ENTER *to see all active alarms.*

If you choose **n** *for major alarms and* **y** *for minor and warning alarms, you will not see the high-level information that you may need to determine what is wrong with your system.*

3. Press ENTER to view the alarm report.
4. The `ALARM REPORT` detail screen appears.

Alarm Report detail screen

```
                                ALARM REPORT
Port        Maintenance On   Alt     Alarm   Svc    Ack?  Date        Date
            Name        Brd? Name    Type    State  1 2   Alarmed     Resolved
01AXX1      PI-LINK     n            WARNING               05/02/09:48 00/00/00:00
01AXX1      PI-LINK     n            WARNING               05/02/09:48 00/00/00:00
01A0101     DIG-LINE    n    Attd1   WARNING RDY           05/02/12:29 00/00/00:00
01A0101     DIG-LINE    n    Attd1   WARNING RDY           05/02/12:29 00/00/00:00
01AXX1      PI-LINK     n            WARNING               05/02/18:49 00/00/00:00
```

Interpreting alarm logs

The `ALARM REPORT` lists the major alarms first, followed by the minor and warning alarms.

The alarm log in the example above shows:

- a processor interface link (`PI-LINK`) at address `01AXX1` has alarmed three times on May 2 with *off-board* (`On Brd?` = `n`) warnings.
- the same port (`01A0101`) on a digital line (`DIG-LINE`) circuit pack has alarmed twice on May 2 in response to two different error counters (refer to the error log example).

Clearing alarm logs

To clear an alarm log:

1. Investigate or fix the first major alarm in the log.
2. See if other alarms are retired by fixing the most severe problem first.

Assigning alarm buttons

You can administer feature button lamps on any phone to act as alarm indicators, similar to the alarm lamp on the attendant console. The following table describes the meaning of the green light associated with an alarm button.

status of light	meaning
flashing green	an alarm occurs
steady green	INADS notified and acknowledges alarm
light goes off	an alarm is resolved

Press the alarm button to turn off the light. The light flashes again if the alarm is still active when the next maintenance routine runs.

Understanding common error types

This section discusses frequently-encountered error types, and explains why they occur.

Error type 18 – busied out

Error type 18 is a reminder from the switch that a component has been busied out. The busyout command is used to temporarily disable a component and is usually used before you test or replace a component.

Use the **release** command (permissions enabled) to restore a component to its normal operating mode.

For example, you receive a complaint that a phone does not work. As part of your diagnosis, you:

- use **status station**

  OR

- view the hardware error report for error 18

To view a hardware error report for error 18:

1. Type **display errors** and press RETURN.

   The `HARDWARE ERROR REPORT` screen appears.

2. Fill in the `Err Type` field and press RETURN.

   In our example, type **18**.

   The `HARDWARE ERROR REPORT` for error 18 appears.

Hardware Error Report (error type 18)

```
                    HARDWARE ERROR REPORT - ACTIVE ALARMS
Port     Mtce     Alt      Err   Aux      First       Last      Err Err Rt/ Al Ac
         Name     Name     Type  Data     Occur       Occur     Cnt Rt  Hr  St

01A0901 DIG-LINE 1234      18          03/09/00:30 03/09/00:30  1   0   0   a  n
```

The log entry indicates that extension 1234, a digital line, is busied out (ERR TYPE 18).

Use the **release** command (permissions enabled) to remove the busyout status from the station. In our example:

1. Type **release port 01A0901** (permissions enabled) and press RETURN.

   The station is no longer busied-out.

Error type 513 – equipment "missing"

Error type 513 notifies you that equipment such as phones, data modules, or circuit packs, are administered but not physically connected to the switch.

For example, view a hardware error report for error 513:

1. Type **display errors** and press RETURN.

   The HARDWARE ERROR REPORT screen appears.

2. Fill in the Err Type field and press RETURN.

   In our example, type **513**.

   The HARDWARE ERROR REPORT for error 513 appears.

Hardware Error Report (error type 513)

```
                        HARDWARE ERROR REPORT - ACTIVE ALARMS
Port      Mtce     Alt     Err   Aux     First       Last      Err Err Rt/ Al Ac
          Name     Name    Type  Data    Occur       Occur     Cnt Rt  Hr  St
01C0507   DIG-LINE 7157    513   0     03/09/00:30 03/09/00:30 1   0   0   a  n
```

In this example, a digital phone is missing. A port on the digital line circuit pack (`DIG-LINE`) at cabinet 1, carrier C, slot 05, port 07 does not have its administered equipment physically present (`Err Type 513`).

To fix error 513 in our example:

1. Plug the phone into the jack assigned to port 01C0507.
2. Type **test station 7157** (permissions enabled) and press RETURN to test the phone.

   The system will clear the error only after the system runs its administered checks and diagnostics.

Error type 1 — circuit pack removed

Error type 1 often indicates that an administered circuit pack has been removed.

To correct the problem and clear Error type 1:

1. Replace and latch the circuit pack in its administered slot.

   The next time the system runs its routine maintenance program, it should be able to “see” the circuit pack and the error will not appear.

Preventing alarms and errors

This section lists a few common causes of unnecessary alarms.

Turn off maintenance

The Remote Loop-Around Test sends a burst of current to activate a phone's ringer. If the ringer responds, the test detects the return. Data modules, fax machines and modems do not have ringers and do not respond to this test. This generates an error on that port.

You should turn off this test for data modules, fax machines and modems. Turning off the test does *not* affect the performance of any of these devices.

To turn off the maintenance test:

1. Type **change data-module *n***, where ***n*** is the extension number, and press RETURN.

   The `DATA MODULE` screen appears:

Data Module screen

```
                                DATA MODULE
  Data Extension: 3151            Name: joes r2cms pdm                BCC: 2
            Type: pdm              COS: 1         Remote Loop-Around Test? n
            Port: 01C0501          COR: 1           Secondary data module? n
             ITC: restricted        TN: 1                    Connected to: dte
ABBREVIATED DIALING
  List1:
SPECIAL DIALING OPTION:
ASSIGNED MEMBER ( Station with a data extension button for this data module )
         Ext     Name
      1:
```

2. Change the `Remote Loop-Around Test` field to **n**.
3. Press ENTER to save your changes.

Remove unused circuit packs

Occasionally, a company upgrades phones from analog models to digital phones. The upgrade process is to:

1. Remove the analog line and trunk administration
2. Remove the old analog equipment
3. Rewire the workplace for the new digital phones and jacks
4. Administer the new digital phones and circuit packs

If the analog circuit packs remain physically plugged into the system and are *still administered as circuit packs (*even though the administration is removed in Step 1 above), the system generates errors. This stops when you remove the administration (**change circuit-pack *UUCSS***) for this unused circuit pack.

DS1 administration

Depending on whether a DS1 circuit pack is present and whether its ports are assigned or not, the system reports faults according to the following table:

circuit pack present?	circuit pack administered?	ports administered?	alarm level	action
N	Y	N	warning	1. Replace and latch the board in its assigned slot. 2. Remove the trunk and DS1 administration (**change circuit-pack *UUCSS***), *leaving the circuit pack in its assigned slot*.
N	Y	Y	minor	1. Replace and latch the board in its assigned slot. 2. Administer one or more ports (**change circuit-pack *UUCSS***), *leaving the circuit pack in its assigned slot*.
Y	N	N	varies	1. Remove the circuit pack from the carrier.

Using features to troubleshoot

Using features to troubleshoot

You can use some Avaya™ Communication Manager features to help you identify if your system is having problems or to help you diagnose problems you know are occurring. The table below shows you which features to use for various kinds of system problems.

	problem area			
feature	**trunks**	**phones**	**hunt groups**	**paging groups**
Automatic Circuit Assurance	X			
Busy Verify	X	X	X	
Facility Busy Indication	X	X		X
Facility Test Calls	X	X		
Trunk Identification	X			

Automatic Circuit Assurance

You can use Automatic Circuit Assurance (ACA) to help identify faulty trunks. If activated (**change system-parameters features**), your system notifies you with a referral call when it detects unusual trunk usage like very short or very long calls. It needs to be turned on for each individual trunk group.

The referral call arrives on an idle call appearance. If you answer the call, your display shows:

- that the call is an ACA call
- the trunk-group access code
- the trunk-group member number
- the reason for the call (short or long holding time)

To use ACA on a G3V2 or older switch

1. Assign an ACA button to your phone.
2. Press the ACA button to activate your phone for referrals.
3. When you receive an ACA referral call, answer the call.
4. Record the information listed on your display to use for further troubleshooting.

To use ACA on a G3V3 or newer switch

1. Assign an ACA-Halt button to your phone.
2. Leave the ACA-Halt button OFF to keep your phone active for referrals.
3. When you receive an ACA referral call, answer the call.
4. Record the information listed on your display to use for further troubleshooting.

Busy Verify

You can use Busy Verify to place test calls to check the busy condition of trunks, phones, or hunt groups. This test helps you determine if the trunk, phone, or hunt group is busy because of heavy use or appears busy because of a problem.

To use Busy Verify, you should administer a Busy Verify button on your phone.

To busy-verify a phone

1. Press the BUSY VERIFY button on your phone.

   The busy verify light turns green.

2. Dial the extension of the phone you want to test.

You hear a tone and see a display. The following table describes what the tone and display indicate and how to respond.

display	tone	frequency	pattern (seconds)	status of extension	next step
Invalid	intercept	440 Hz alternating 620 Hz	.25 on .25 on repeated	invalid number	cancel and try again
Terminated	ringback	combined 440 Hz + 480 Hz	1 on 3 off repeated	idle and ringing (working properly)	release the call
Bridged	none			bridged onto active call (working properly)	release the call
Out of service	reorder	combined 480 Hz + 620 Hz	.25 on .25 off repeated	trouble condition or station administered without hardware and no coverage path	cancel; use **status station *extension*** command for more information

To busy-verify a hunt group

1. Press the BUSY VERIFY button on your phone.

   The busy verify light turns green.

2. Dial the extension for the hunt group you want to test.

You hear a tone and see a display. The following table describes what the tone and display indicate and how to respond.

display	tone	frequency	pattern (seconds)	status of extension	next step
Invalid	intercept	440 Hz alternating 620 Hz	.25 on .25 on repeated	invalid number	cancel and try again
Terminated	ringback	combined 440 Hz + 480 Hz	1 on 3 off repeated	idle and ringing	release the call
All made busy	reorder	combined 480 Hz + 620 Hz	.25 on .25 off repeated	made busy is active	release the call and try again later
Denied	reorder	same as above	same as above	active on a call	release the call and try again later
Out of service	reorder	same as above	same as above	trouble condition or station administered without hardware	cancel; report an out-of-service condition

To busy-verify a trunk

1. Press the BUSY VERIFY button on your phone.

   The busy verify light turns green.

2. Dial the trunk access code for the trunk you want to test.

   Your display should be blank and you should hear dial tone. If your display shows “DENIED” and you hear intercept tone, repeat steps 1 and 2.

   If you have trunk group select buttons on your phone, you can also press the BUSY VERIFY button and then press the TRUNK GROUP SELECT button for the appropriate trunk.

3. Dial the trunk-group member number you want to verify.

You hear a tone and see a display. The following table describes what the tone and display indicate and how to respond.

display	tone	frequency	pattern (seconds)	status of extension	next step
Invalid	intercept	440 Hz alternating 620 Hz	.25 on .25 on repeated	invalid	cancel and try again
Verified	confir-mation			idle and ringing (working properly)	release the call
none	ringback	combined 440 Hz + 480 Hz	1 s on 3 s off repeated	idle automatic or release link (working properly)	release the call
none	dial tone	combined 350 Hz + 440 Hz	continuous	idle (working properly)	release the call
Bridged	none			bridged onto active call (working properly)	release the call
Out of Service	reorder	combined 480 Hz + 620 Hz	.25 on .25 off repeated	trouble condition	cancel; report an out-of-service condition

Facility Busy Indication

You can use Facility Busy Indication to display the idle or busy condition of phones, trunks, or paging zones.

To use this feature you need to add facility busy indication buttons to your phone. Label the facility busy buttons as “Busy” followed by the number or name of the facility being monitored.

If the green light associated with the Facility Busy Indication button stays lit for a long time, the facility may have a problem.

Facility Test Calls

You can use Facility Test Calls to place test calls to specific trunks or phones. Because this feature bypasses the regular system traffic, it is very helpful in finding noisy lines and other problems. However, this feature can be easily misused by outside parties. Disable this feature when you are not using it.

SECURITY ALERT:
Whenever you use this feature, enable the feature access code only for the tests you want to make. Be sure to immediately remove the access code when you are through testing because leaving this feature enabled can leave you open to security breaches.

To place a test call to a trunk or touch-tone phone

1. At the system terminal, enable a feature access code for Facility Test Call.
2. At your phone, dial the feature access code for Facility Test Call. Listen for dial tone.
3. Dial the 6- or 7-digit port address in **UUCSSss** format, where:

   UU = cabinet number (01, 02, etc.)
   C = carrier number (A=1, B=2, C=3, D=4, E=5)
   SS = slot number (depends on system)
   ss = port number (depends on circuit pack)

Tip:
If you have problems with this step, try dialing the port address without the first zero in the cabinet number.

You hear a tone and see a display. The following table describes what the tone and display indicate and how to respond.

tone	frequency	pattern (seconds)	status	next step
dial	combined 350 Hz + 440 Hz	continuous	connected	go to step 4
reorder	combined 480 Hz + 620 Hz	.25 on .25 off repeated	busy	release the call
intercept	440 Hz alternating 620 Hz	.25 on .25 on repeated	no access	release the call

4. If you are testing a trunk, place the call.
   or
   If you are testing a touch-tone receiver, dial the number.
5. If you receive a dial tone, the test passed.
   or
   If you receive an intercept tone, the test failed.

SECURITY ALERT:
At the system terminal, BE SURE to disable the Facility Test Call feature access code.

Trunk Identification

You can identify a faulty or noisy trunk with Trunk Identification. You can use Trunk Identification:

- on an active call
- while accessing a trunk

To identify the specific trunk used on a call:

1. Press the TRUNK ID button.

   Trunk access code and trunk group member number appears on the display.

   If 2 trunks are used on the call, the identification of the last trunk added to the call displays. If more than 2 trunks are on a call, Trunk Identification is denied.

2. See if there are any *on-board* alarms against a trunk circuit pack.

   If no, report the trunk problem to the appropriate vendor.

   If yes, report the trunk problem and the identification information to Avaya.

Solving IP and H.323 problems

This section describes some basic troubleshooting tips and tools that may help you solve problems with IP (internet protocol) softphones, and IP and H.323 trunk issues.

In addition to using this section, you may want to refer to *Administration for Network Connectivity for Avaya MultiVantage™ Software*, 555-233-504, for basic IP administration.

Solving softphone problems

This section discusses some common problems you or your users may encounter while using IP softphones (telecommuter or road warrior types).

Users cannot login (register) with IP softphone

The user's password needs to be the same as the administered station security code. So, the first thing to verify is whether or not the user is using the correct password. If they are using the correct password, then you should determine if the problem is with their PC.

To determine if the problem is related to the user's PC, try to register (login) this extension from another PC. If you can successfully register, then the problem is within the user's PC. If you cannot register, then the extension may not be administered correctly or you may have a network problem.

User is logged in, but cannot use softphone for calls

If you see the message "Telephony is not available" in the call status area, then you may have COR to COR restrictions between the IP softphone and the actual hard phone used to make calls.

If you do not have restrictions, then try logging off and back in again. If that fails, reboot the PC that the softphone is running on.

WARNING:
Some system platforms also run on a PC. If you reboot a system PC that is running a D1, all calls will be lost. In that case, you might want to wait until after normal business hours to reboot the PC.

Cannot listen to messages with INTUITY Message Manager

When a user is logged in to IP softphone in the roadwarrior application, the softphone has control of the PC sound card. Since only one application can control the PC sound card at a time, the sound card will not be available to Message Manager.

Users get message “Action cannot be completed”

The user may have a button on the IP softphone that is not actually administered on the Station screen for the extension. Or the user is trying to dial a feature access code that is not administered in the system.

User cannot conference or transfer

Both the conference and the transfer operations require at least two lines. Make sure the user has more than one line available to place calls. To determine if the user has more than one line appearance, complete the following steps:

1. At the IP softphone, select Number of Calls from the Options menu.
2. Verify that the Minimum or Default number of lines to be displayed is more than one.

Users cannot use Directory

In order to use the directory, users must have a Directory, Normal and Next button available.

Other tips

If your users get the message “Communication to the server has been lost. You will be logged off by the server,” the only option is to click OK. However, if the user is active on a call, they can finish the call before they click OK.

Sound quality problems

Because of the myriad of networks and equipment involved in an IP call, there are a lot of factors that may contribute to sound quality problems. This section contains tips for how to determine the source of the problem, and some things you can do that may help.

Isolating problems in the LAN or the Communication Manager setup

There are a few easy things you can do to determine if a voice quality problem is in the Communication Manager setup or in your LAN or PC.

To check the PC sound quality, create and play back a sound file using the PC sound recorder. If the sound quality is unacceptable, the problem is somewhere in your headset or sound card.

To check sound quality over the LAN, shut down IP softphone. Now start up NetMeeting and initiate a call. This completely bypasses the Communication Manager. Therefore, if you are still experiencing sound quality problems, the source must be somewhere within the LAN. If this resolves the sound quality problem, the issue is with the Communication Manager setup.

NOTE:
For more information on NetMeeting, see Microsoft's Web site at www.microsoft.com.

Running a mute test

The mute test can also help determine the source of a sound quality problem. To run this test, set up an IP softphone test call between two users who are experiencing voice quality problems. Have one user mute their phone and have the other user count aloud to 10. If the sound quality improves, then the problem is in the sound card, microphone, or headset of the muted phone. If the sound quality does not improve, try the test again, but this time mute the other phone.

Checking the PC volume control

Softphone has its own volume controls, but sometimes the volume controls on the PC need to be adjusted. If the PC volume controls are set too loud, it can cause sound quality to be distorted. If the PC volume controls are set too low, it may be difficult to hear clearly. Try adjusting the volume control on the PC to resolve the problem.

Checking for packet loss and jitter

Packet loss and jitter can cause a noisy connection that eventually breaks up, creating gaps in the conversation and making speech unintelligible. Use **status station** to check for station-side IP problems, including problems with an IP phone, and use **status trunk** to check for trunk-side IP problems. Each command generates snapshot jitter buffer size (ms) and packet loss report for a particular station or trunk group member that shows:

- the number of packets that are lost or corrupted
- amount of jitter on the connection

In this instance, jitter is the variability in the amount of time (in milliseconds) that packets are received over the network. When jitter increases, the user experiences a noisy connection, delays, and a general loss of quality, making speech unintelligible.

NOTE:
If you issue a **status station** or **status trunk** command for a non-IP station, or the connection is hairpinned or shuffled, then the packet loss and jitter size information does not appear. See the *Administration for Network Connectivity for Avaya MultiVantage™ Software*, 555-233-504, for more information.

Other possible causes

If a user is browsing the web while using softphone and they are accessing web sites with large graphics, they may experience an interruption in voice transmission.

Basic troubleshooting tools

This section describes some basic tools that you can use to understand better what is going on in your network and with the IP hardware and software.

Using ping

The **ping** command helps you to determine if endpoints on the network are available to place or receive calls and if nodes in the network are active. You can specify which circuit pack you want to use to ping.

For example, to ping from a C-LAN circuit pack at 01A011 to an endpoint at 111.122.133.144, complete the following steps:

1. At the command line, type **ping ip-address 111.122.133.144 board 01A011**.

   Use the IP address of the endpoint you want to ping and the board location for the specific pack you want to test.

   You can also use the **ping node-name** to ping a node defined on the `NODE NAMES` screen.

2. Press RETURN.

   The `PING RESULTS` report appears.

Ping Results report

```
                              PING RESULTS

End-pt  Node-name  Port       Port Type  Result    Time (ms)  Error code
111.122.133.144    01A011     ETH-PT     PASS      60
```

3. Review the report to see if pinging the endpoints failed or if the round-trip time was too long.

Using trace-route

The trace-route command helps you test the path that a call takes from the PC endpoint, through the various nodes in a network. Trace-route can help you see where in the network a problem may be occurring.

For example, to determine the path from a C-LAN circuit pack at 01A011 to an endpoint at 111.122.133.144, complete the following steps:

1. At the command line, type **trace-route ip-address 111.122.133.144 board 01A011**.

   Use the IP address of the endpoint you want to reach and the board location for the specific pack you want to test.

   You can also use the **trace-route node-name** to test the path to a node defined on the Node Names screen.

2. Press RETURN.

   The TRACE ROUTE RESULTS report appears.

Trace Route Results report

```
                    TRACE ROUTE RESULTS

Hop                 Time (ms)               IP Address
0                   Start Addr:             111.44.33.122
1                     5,  6,  6             111.44.33.144
2                    35, 36, 37             111.44.33.111
3                    49, 51, 51             111.122.133.111
4                    58, 58, 59             111.122.133.144
```

3. Verify that the last IP address on the report is the same as the IP endpoint you specified in Step 1.

   If the system was unable to follow the full path, it lists the last address that it could successfully reach. This information may help you narrow which part of the network is experiencing problems.

Finding the IP address

In some cases, you will want to know the IP address of a PC so that you can ping it or trace the route of a call to it. To determine the IP address, complete the following steps:

1. At the PC, open a Command Prompt (DOS) window.

   Typically you can access the command prompt by selecting Start > Programs > Command Prompt.

2. At the Command prompt, type **winnt\system32\ipconfig** (Windows NT/2000) or **winipcfg** (Windows 95/98).

3. Record the IP address for the PC.

Verifying the IP softphone registration

Sometimes you will need to know whether or not an IP softphone is registered. For example, to determine whether the softphone at extension 4455 is registered, complete the following steps:

1. Type **status station 4455** and press RETURN.

   The `GENERAL STATUS` screen appears.

2. Look at the `Registration Status` field on the second page. If the word “authenticated” appears, the softphone is registered.

Verifying the trunk type

Sometimes you will need to know whether or not a trunk group is an IP type endpoint. For example, to determine whether the trunk member 01 of trunk group 40 is an IP endpoint, complete the following steps:

1. Type **status trunk 40/01** and press RETURN.

   The `TRUNK STATUS` screen appears.

2. Verify that the `Port` field is `T000`*nn*.

   If this field displays a standard port address (for example, 01A0210), then the trunk is not an IP endpoint.

When all else fails

Reboot the PC! When you are experiencing unexpected behavior that you cannot easily fix, you may want to close all your applications and reboot the machine.

WARNING:
Some system platforms also run on a PC. If you reboot a system PC that is running a D1, all calls will be lost. In that case, you might want to wait until after normal business hours to reboot the PC.

Contacting Avaya

This section describes what information you should have handy when you need to contact the Avaya Technical Service Center (TSC). This section also provides a list of phone numbers you can call when you have a problem with your system.

Preparing to contact Avaya

Do you need to call Avaya for additional information or help in solving a problem?

If you do, please have the following information handy. This helps the person taking your call.

- your name and number (in case we need to call you back)
- your installation location number (also called your IL)

  _____

  (Write your IL number here for easy reference)
- your company's main phone number
- the type of your switch
- the number of trunks on your system
- the number of stations on your system

Also, use the information in this book to determine the possible source of your problem. It always helps to keep a log of the steps you took and the information you gathered while performing your diagnosis. This information is extremely helpful when you partner with an Avaya representative in solving your switch problems.

Remember, if the problem is with equipment or service outside of your own equipment, you need to call your vendor or service provider. If you determine that the problem is with your own equipment, such as on your own stations, switch, or trunks, give Avaya a call.

If you are not sure where the problem is located, double-check your system information. Refer to ‘‘Problem-solving strategies’’ on page 33 for more information.

Be ready to talk about:

- the problem you want to solve
- if the problem is with a new component or feature
- if something that used to work now does not work
- any numbers involved with the problem (for example, extensions or phone numbers, trunk group numbers, phone types, or report types)
- the contents of any recorded messages received
- error messages from the switch
- type of ringback tones received on phones
- the names and numbers of your vendors
- any other pertinent information

Contacting Avaya

The following table lists additional services available to you. If you are outside of the 1 800 calling area, contact your local Avaya representative.

Technical Service Center for Large-Systems Customers and Toll Fraud Crisis Intervention (for help with repairs)	1 800 242 2121
Communication Manager Helpline (for administration and software problems, including vectors, how features work, administration, and interactions)	1 800 225 7585

Glossary

A

abbreviated dialing
: A feature that allows callers to place calls by dialing just one or two digits.

access code
: A dial code used to activate or cancel a feature or access an outgoing trunk.

analog phone
: A phone that receives acoustic voice signals and sends analog electrical signals along the phone line.

ARS partitioning
: A feature that allows you to route calls differently for different groups of users.

attendant
: A person at a console who provides personalized service for incoming callers and voice-services users by performing switching and signaling operations.

attendant console
: The workstation used by an attendant. The attendant console allows the attendant to originate a call, answer an incoming call, transfer a call to another extension or trunk, put a call on hold, and remove a call from hold. Attendants using the console can also manage and monitor some system operations.

Audio Information Exchange (AUDIX)
: A fully-integrated voice-mail system. Can be used with a variety of communications systems to provide call-history data, such as subscriber identification and reason for redirection.

Automatic Alternate Routing (AAR)
A feature that routes calls to alternate routes when facilities are unavailable.

Automatic Call Distribution (ACD)
A feature that gives users more flexibility in routing calls to hunt group agents. ACD also allows external measurement systems such as BCMS and CentreVu® CMS to be used.

Automatic Circuit Assurance (ACA)
A feature that tracks calls of unusual duration to facilitate troubleshooting.

Automatic Route Selection (ARS)
A feature that allows the system to automatically choose the least-cost route for toll calls.

B

barrier code
A security code used with Remote Access to prevent unauthorized access.

bridge (bridging)
The appearance of a phone's extension at one or more other phones.

bridged appearance
A call appearance on a phone that matches a call appearance on another phone for the duration of a call.

C

call appearance
For the phone or attendant console, a button labeled with an extension and used to place outgoing calls, receive incoming calls, or hold calls. Lights next to the button show the status of the call appearance.

Call Detail Recording (CDR)
A feature that records call data.

Call Vectoring
A feature that allows users to provide flexible, customized call handling by writing a series of instructions in a simple programming language.

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

centum call seconds (CCS)
CCS is a unit for measuring call traffic. One CCS equals 100 seconds. Call traffic for a facility, such as a hunt group or phone, is scanned every 100 seconds. If the facility is busy, it is assumed to have been busy for the entire scan interval. There are 3600 seconds per hour, so a facility that is busy for an entire hour will be measured as being busy for 36 CCS.

central office (CO)
The location of phone switching equipment that provides local phone service and access to toll facilities for long-distance calling.

circuit
A channel or transmission path between two or more points.

Class of Restriction (COR)
A feature that defines call-origination and call-termination restrictions.

Class of Service (COS)
A feature that determines whether users can activate certain features.

coverage answer group
A group of phones that ring simultaneously when a call is redirected to it.

coverage path
The order in which calls are redirected to alternate phones.

coverage point
An extension designated as an alternate phone in a coverage path.

D

data module
A digital interface device between the switch and data equipment.

Direct Department Calling (DDC)
A method for distributing hunt group calls to agents. The switch searches through all the hunt group extensions in order, starting with the first extension. As soon as the switch finds an available extension, it connects the call. Compare to Uniform Call Distribution (UCD).

E

Expert Agent Selection (EAS)
A feature allowing incoming calls to be routed to specialized groups of agents within a larger pool of agents.

extension
A number by which calls are routed through a communications system.

external call
A connection between a communications system user and a party on the public network or on another communications system in a private network.

F

facility
A telecommunications transmission pathway and associated equipment.

feature access code (FAC)
A code users dial to access a system feature.

feature button
A button on a phone or attendant console used to access a specific feature.

H

hunt group
A group of extensions that all can receive calls directed to a single phone number. When a call arrives at the group number, the switch searches (“hunts”) for an available extension in the group and connects the call to that extension.

I

internal call
A connection between two users on the same phone system.

M

major alarm
An indication of a component failure that requires immediate attention.

minor alarm
An indication of a component failure that could affect customer service.

multiappearance phone
A phone equipped with several call-appearance buttons allowing the user to handle more than one call on that same extension at the same time.

P

pickup group
: A group of individuals authorized to answer any call directed to an extension within the group.

port carrier
: A carrier in a cabinet containing port circuit packs, power units, and service circuits. Also called a port cabinet.

primary extension
: The main extension associated with the physical phone or data terminal.

principal
: A phone that has its primary extension bridged on one or more other phones.

public network
: The network that can be openly accessed by all customers for local and long-distance calling.

R

redirection criteria
: Information administered for each phone's coverage path that determines when an incoming call is redirected to coverage.

S

skill
: An attribute assigned to an agent in a system using Expert Agent Selection. An agent's skill indicates a specialty in which the agent is proficient.

split
An ACD hunt group.

system administrator
The person who maintains overall customer responsibility for system administration.

system printer
An optional printer that may be used to print scheduled reports via the report scheduler.

system report
A report that provides historical traffic information for internally measured splits.

T

trunk
A dedicated telecommunications channel between 2 phone systems or COs.

trunk group
Telecommunications channels assigned as a group for certain functions that can be used interchangeably between two communications systems or COs.

U

Uniform Call Distribution (UCD)
A method for distributing hunt group calls to agents by comparing agents' workloads. Avaya™ Communication Manager can deliver each new call to the most idle agent (the available agent who has been idle the longest since their last hunt group call) or to the least occupied agent (the agent who has spent the least amount of time on hunt group calls in their current shift). Compare to Direct Department Calling (DDC).

Uniform Dial Plan (UDP)

A feature that allows a unique 4- or 5-digit number assignment for each point in a multiswitch system.

V

Vector

A set of call handling instructions for Avaya™ Communication Manager that can direct the switch to queue calls, play announcements, play music, route calls to voice messaging, as well as many other things.

Index

A

about this book
- intended audience, 17
- purpose, 17

alarm buttons, 62
alarm logs, 59
alarms
- classifications of, 59
- clearing, 62
- DS1, 68
- off-board, 59
- on-board, 59
- preventing, 66

Automatic Circuit Assurance (ACA), 69

B

backups, 30
baselining
- definition, 27
- retrieving information, 28

books
- how to order more copies, 23

busy-verify
- hunt groups, 72
- trunks, 73

buttons
- Alarm, 62
- Busy Verify, 71
- help, 20
- Trunk ID, 77

C

cabinet status, viewing, 37
call center, problems, 48
calling Avaya, 89
circuit packs, removing, 67
clearing alarms, 62
clearing errors, 57
commands
- change circuit-pack, 68
- change data-module extension, 66
- display alarms, 33, 60
- display errors, 33, 54
- list history, 38
- ping, 84
- save announcements, 30
- save translations, 30
- status, 33
- status health, 35
- status station, 36, 83
- status station extension, 36
- status system all-cabinets, 37
- status trunk, 83
- test station extension, 65
- trace-route, 85

D

diagnosing problems, 41
dialing out, problems, 43
DS1, alarms, 68

E

error logs
- interpreting, 57
- viewing, 54

error types, 62
- 1 – circuit pack removed, 65
- 18 – busied out, 63
- 513 – equipment missing, 64

errors
clearing, 57
preventing, 66

F

Facility Busy Indication, 74
Facility Test Calls, 75

H

H.323 trunk, 79
help
buttons, 20
help, numbers to call, 24
history, viewing, 38
hunt groups, busy-verify, 72

I

IL number. *See* installation location (IL) number
incoming calls, problems, 44
installation location (IL) number, 89
intended audience, 17
internet protocol (IP), 79
IP address, 87
IP softphone, 79

L

login, problems, 47
logs
alarms, 59
clearing alarms, 62
error, 54

M

maintaining records, 28
Maintenance Objects (MO), 53
message lamp problems, 45
message line, 20
modem problems, 46

P

password, problems, 47
phone problems, solving, 42
phones, busy-verify, 71
printer problems, 47
problems
call center, 48
diagnosing, 41
dialing out, 43
incoming calls, 44
login, 47
message lamp, 45
modem, 46
password, 47
phone, 42
printer, 47
SAT, 47
softphone, 79
sound quality, 82
terminal access, 47
tie trunks, 46
trunks, 45
problem-solving, strategies, 33

R

records, maintaining, 28
removing circuit packs, 67
reports
error, 54
history, 38

S

SAT problems, 47
screens, 19
    Alarm Report, 60
    Alarm Report detail, 61
    Data Module, 66
    Error Report, 54
    General Status, 36
    Hardware Error Report, 56, 63, 64
    Help, 34
    History, 38
    Status Health, 35
    System Status Cabinet, 37
security
    access codes, 75
    concerns, 21
softphone, 79
    solving problems, 79
status
    cabinet, 37
    station, 36
    system health, 35
status line, 20
strategies, problem-solving, 33
system backups, 30
system changes, viewing, 38
system health, viewing, 35
system logs
    alarms, 53
    errors, 53
system status, viewing, 34

T

terminal access, problems, 47
testing
    phones, 75
    trunks, 75
testing, busy phones, 71
tests, 66
tie trunk problems, 46
toll fraud, 21
trademarks, 21
troubleshooting
    phone problems, 42
    trunks, 77
    using features, 69
Trunk Identification, 77
trunks
    busy-verify, 73
    identifying problems, 45, 83
    troubleshooting, 77
turning off tests, 66
turning-off, 66

V

viewing
    error logs, 54
    station status, 36
    system changes, 38
    system status, 34
voice terminals, *see* phones

We'd like your opinion.

We welcome your feedback! Please let us know what you think about this book.

Avaya™ Communication Manager Little Instruction Book for basic diagnostics, 555-233-758, Issue 5, May 2003

1. Please check the ways you feel we could improve this book:

- ❒ Improve the overview
- ❒ Improve the table of contents
- ❒ Improve the organization
- ❒ Add more figures
- ❒ Add more examples
- ❒ Add more detail
- ❒ Make it more concise
- ❒ Add more step-by-step procedures

Please add details about what you think. _____
_____
_____

2. What did you like most about this book? _____
_____
_____
_____

3. Feel free to write additional comments._____
_____
_____
_____
_____
_____
_____

If we may contact you concerning your comments, please complete the following:

Name:_____Telephone Number: (____)_____

Company/Organization_____Date:_____

Address:_____
_____

When you have completed this form, please fax your feedback to **+1 303 538 1741**.
Thank you.

Avaya Customer Support web site

This web site allows you to find answers to questions, review maintenance tickets, or get the latest version of this book.

http://www.avaya.com/support/

Online Expert

Access this interactive site to find out how to administer your system or to get help with solving basic problems.

Create Service Request

Create and submit a service request for specific location. We will provide you with both a case number and a commitment time.

Case status

Review the status of your maintenance requests by entering your case (ticket) number. You can get the status for any open case or for a case closed within the last 60 days.

Replacement equipment

Order replacements for defective equipment. Replacement equipment is shipped overnight.

Documentation

Search and view over 1,600 documents including system and feature descriptions, administration guides, maintenance manuals, and the latest Little Instruction Books.

Frequently asked questions and Live chat

View answers to frequently-asked questions or join live chat sessions to discuss your Avaya products.