AVAYA

Avaya Communication Manager

Little Instruction Book

for Basic Administration

Release 2.0
555-233-756
Issue 6
November 2003

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

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

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

Why this book?

You have told us that you want step-by-step instructions on everyday administration tasks for Avaya Communication Manager. This book contains the information you need for basic phone system administration.

Although some steps might vary between the different versions of the software, these instructions are designed to 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 forms have changed.
- We have moved the area code instructions to a section on routing.
- We have given troubleshooting its very own book, the *Avaya Communication Manager Little Instruction Book for Basic Diagnostics*, 555-233-758.

November 2003

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 Basic Administration* is divided into sections to guide you through your day-to-day operations.

Getting started provides an overview of a phone system and types of phones. It provides instructions to log in, save changes, and log 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.

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. This section also includes instructions for setting up ARS partitioning and authorization codes.

November 2003

Enhancing system security explains how to add and change user logins and passwords. This section 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. This section **also explains how to contact the** Communication Manager **helpline, and lists what information you need to 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.

- A “form” is the display of fields and prompts that appear on a terminal monitor screen. See Figure 2, Terminal form for login, 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 Advanced Administration*, 555-233-757
- 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 *Overview for Avaya Communication Manager*, 555-233-767, and the *Avaya Toll Fraud and Security Handbook*, 555-025-600.

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 Basic 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.

November 2003

3 Type **555-233-756** (the document number) in the **Search Support** text box, then click **Go**.

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 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 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.

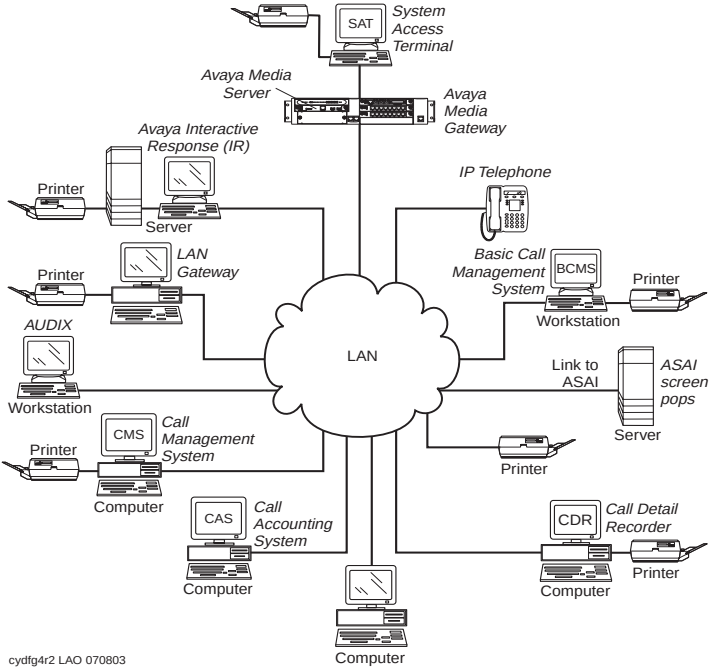
Overview of Avaya Communication Manager

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. Figure 1, Sample system running Avaya Communication Manager, on page 24 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.

Figure 1: Sample system running Avaya Communication Manager



System running Avaya Communication Manager

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

- Avaya Interactive Response (IR)— provides response to spoken information
- System Access Terminal (SAT) — allows remote connection for administration and reports

- Basic Call Management System (BCMS) — collects information and prints reports on call-center performance
- 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
- Message Manager — access to AUDIX voice processing on a personal computer
- 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 a combination of phone types 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.

For a list of phone types and how they should be administered, refer to the "Station" section in the *Administrator's Guide for Avaya Communication Manager*, 555-233-506.

NOTE:
Avaya no longer supports some older phone models.

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 112.

Logging into the system

NOTE:
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 ID and press **ENTER**.

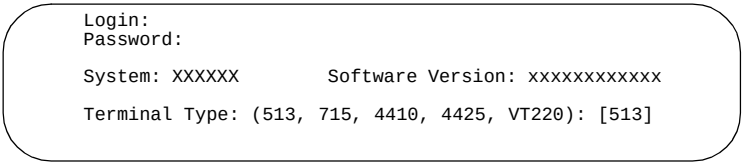
   The system prompts you for your password.

2. Type your password and press **ENTER**.

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

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

Figure 2: Terminal form for login



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

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.

NOTE:
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 **ENTER**.

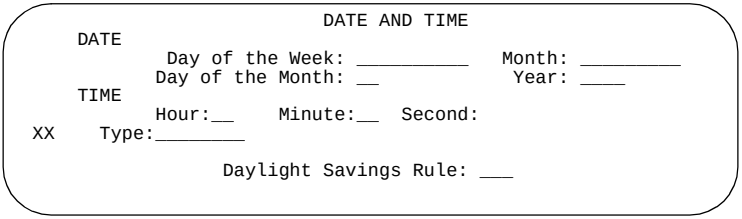
The ***DATE AND TIME*** form appears.

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.

Figure 3: Date and Time form



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

NOTE:
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 form.

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.

NOTE:
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.

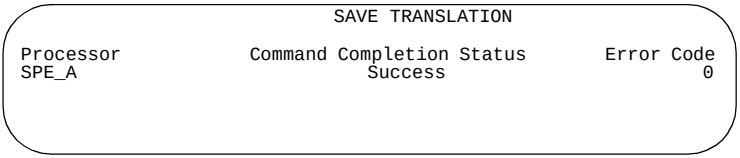
2 Check the alarms panel and clear any active alarms.

3 Type **`save translation`** and press **ENTER**.

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.

Figure 4: Save Translation form



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 **ENTER** 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 **ENTER**.

You may see a security form 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 form 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 **ENTER** 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.

2 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.

NOTE:
In this book, we do not usually explain each form as thoroughly as we do the dial plan. However, this form 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 forms 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 34. 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 41. 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 41.

Let us 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.

Figure 5: Dial Plan Analysis Table form

```
                    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         __      _     _____       __      _     _____
 21       2     fac         __      _     _____       __      _     _____
  3       1     aar         __      _     _____       __      _     _____
  3       4     ext         __      _     _____       __      _     _____
  4       1     ars         __      _     _____       __      _     _____
  4       5     ext         __      _     _____       __      _     _____
  5       7     ext         __      _     _____       __      _     _____
  6       7     ext         __      _     _____       __      _     _____
  8       1     fac         __      _     _____       __      _     _____
  9       5     ext         __      _     _____       __      _     _____
  *       3     fac         __      _     _____       __      _     _____
  #       3     fac         __      _     _____       __      _     _____
```


A 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 5, they are dialing an extension.

The third column may have any of the following call types:

- Attendant (attd) — Defines how users call an attendant. Attd access numbers can be any number from 0 to 9 and only contain one or two digits. In our example figure, the system calls an attendant when users dial 0.

  If you use the `Attendant Access Code` field on the ***`FEATURE ACCESS CODE (FAC)`*** form, you cannot make an “attd” entry here. For more information, see Multi-location dial plans on page 40, and the *Administrator’s Guide for Avaya Communication Manager*, 555-233-506, for more information.

- Automatic Alternate Routing (aar) — Used to route calls within your company over your own private network.

NOTE:
Before you can use this call type in your dial plan, the ARS/AAR Dialing without FAC feature must be enabled. To check if this is enabled, use the **display system-parameters customer-options** command.

When dialing digits of Call Type **aar**, as soon as the dialed digits have reached the administered length, the digits are treated as if an AAR feature access code (FAC) was dialed. Control is transferred and the digits are routed according to the AAR Analysis and Digit Conversion forms.

In our example, extensions of **3xxx** cannot be dialed directly. Whenever a user dials the first digit of **3**, the system immediately interprets the dialed string as an AAR string and transfers control to AAR.

Extensions of **3xxx** can only be accessed using AAR Digit Conversion. That is, you must dial a longer AAR number from which AAR Digit Conversion deletes leading digits to form a number of the form **3xxx**.

- Automatic Route Selection (ars) — Used to route 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.

NOTE:
Before you can use this call type in your dial plan, the ARS/AAR Dialing without FAC feature must be enabled. To check if this is enabled, use the **display system-parameters customer-options** command.

When dialing digits of `Call Type` **ars**, as soon as the dialed digits have reached the administered length, the digits are treated as if an ARS feature access code (FAC) was dialed. Control is transferred and the digits are routed according to the ARS Analysis and Digit Conversion forms.

In our example, extensions of **4xxxx** cannot be dialed directly. Whenever a user dials the first digit of **4**, the system immediately interprets the dialed string as an ARS string and transfers control to ARS.

Extensions of **4xxxx** can only be accessed using ARS Digit Conversion. That is, you must dial a longer ARS number from which ARS Digit Conversion deletes leading digits to form a number of the form **4xxxx**.

For more information, see Understanding ARS analysis on page 96.

- 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. The first digit can also be * and #. 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: 3000–3999, 40000–49999, 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 *31 to activate a feature and use #31 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 **ENTER**.

Modifying your dial plan

It is easy to make changes to your dial plan. For example, let us 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 **ENTER**.

   The ***`DIAL PLAN ANALYSIS TABLE`*** form 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 us 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 **ENTER**.

   The ***DIAL PLAN ANALYSIS TABLE*** form 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 form, 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 **ENTER**.

   The ***DIAL PLAN ANALYSIS TABLE*** form 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.

Multi-location dial plans

When a customer migrates from a multiple independent node network to a single distributed server whose gateways are distributed across a data network, it may initially appear as if some dial plan functions are no longer available.

The multi-location dial plan feature preserves dial plan uniqueness for extensions and attendants that were provided in a multiple independent node network, but appear to be unavailable when customers migrate to a single distributed server. This feature is available with Communication Manager, release 2.0.

For example, in a department store with many locations, each location might have had its own switch with a multiple independent node network. The same extension could be used to represent a unique department in all stores (extension 4567 might be the luggage department). If the customer migrates to a single distributed server, a user could no longer dial 4567 to get the luggage department in their store. The user would have to dial the complete extension to connect to the proper department.

Instead of having to dial a complete extension, the multi-location dial plan feature allows a user to dial a shorted version of the extension. For example, a customer can continue to dial 4567 instead of having to dial 123-4567.

Communication Manager takes the location prefix and adds those digits to the front of the dialed number. The switch then analyzes the entire dialed string and routes the call based on the administration on the ***DIAL PLAN PARAMETERS*** form.

Prerequisites

Before you can administer the multi-location dial plan feature, the `Multiple Locations` field on the ***OPTIONAL FEATURES*** form must be enabled. To check if this is enabled, use the **display system-parameters customer-options** command. The `Multiple Locations` field is on page 3 of the ***OPTIONAL FEATURES*** form.

For a more detailed explanation of this feature, its function, and the necessary forms, see the *Administrator's Guide for Avaya Communication Manager*, 555-233-506.

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 34.

Let us 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.

Figure 6: Dial Plan Record form

```
                          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:  aar______  _________  _________  ext______  _________  _________
  4:  ars______  _________  _________  _________  ext______  _________
  5:  _________  _________  _________  ext______  _________  _________
  6:  _________  _________  dac______  _________  _________  _________
  7:  _________  _________  _________  _________  _________  _________
  8:  _________  _________  _________  _________  _________  _________
  9:  fac______  _________  _________  _________  _________  _________
  0:  attd_____  _________  _________  _________  _________  _________
  *:  _________  _________  fac______  _________  _________  _________
  #:  _________  _________  fac______  _________  _________  _________
```

If you look at the lower half of the ***DIAL PLAN RECORD*** form, 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 call types:

- Attendant (attd) — Defines how users call an attendant. Attd access numbers can be any number from 0 to 9 and only contain one or two digits. In our example figure, the system calls an attendant when users dial 0.
- Automatic Alternate Routing (aar) — Used to route calls within your company over your own private network.

NOTE:
Before you can use this call type in your dial plan, the `ARS/AAR Dialing without FAC` feature must be enabled. To check if this is enabled, use the **`display system-parameters customer-options`** command.

When dialing digits of `Call Type` **aar**, as soon as the dialed digits have reached the administered length, the digits are treated as if an AAR feature access code (FAC) was dialed. Control is transferred and the digits are routed according to the AAR Analysis and Digit Conversion forms.

In our example, extensions of **3xxx** cannot be dialed directly. Whenever a user dials the first digit of **3**, the system immediately interprets the dialed string as an AAR string and transfers control to AAR.

Extensions of **3xxx** can only be accessed using AAR Digit Conversion. That is, you must dial a longer AAR number from which AAR Digit Conversion deletes leading digits to form a number of the form **3xxx**.

- Automatic Route Selection (ars) — Used to route 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.

NOTE:
Before you can use this call type in your dial plan, the `ARS/AAR Dialing without FAC` feature must be enabled. To check if this is enabled, use the **`display system-parameters customer-options`** command.

When dialing digits of `Call Type` **ars**, as soon as the dialed digits have reached the administered length, the digits are treated as if an ARS feature access code (FAC) was dialed. Control is transferred and the digits are routed according to the ARS Analysis and Digit Conversion forms.

In our example, extensions of **4xxxx** cannot be dialed directly. Whenever a user dials the first digit of **4**, the system immediately interprets the dialed string as an ARS string and transfers control to ARS.

Extensions of **4xxxx** can only be accessed using ARS Digit Conversion. That is, you must dial a longer ARS number from which ARS Digit Conversion deletes leading digits to form a number of the form **4xxxx**.

For more information, see Understanding ARS analysis on page 96.

- 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. You can use * or #, but only as a 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, 3000–3999, 40000–49999, 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 *31 to activate a feature and use #31 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 *DEFINITY Enterprise Communications Server Release 10 Administrator's Guide*, 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 **ENTER**.

Modifying your dial plan

It is easy to make changes to your dial plan. For example, let us 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 **ENTER**.

The ***`DIAL PLAN RECORD`*** form 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

As your needs grow, you may 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 us add a new set of extensions that start with 8 and are 4 digits long (8000–8999).

To add this set of extensions to the dial plan:

1. Type **`change dialplan`** and press **ENTER**.

   The ***`DIAL PLAN RECORD`*** form appears.
2. Move the cursor to the 8th 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` form, it must conform to your dial plan.

In our example, if you want to assign a feature access code of 77 to Last Number Dialed, you need to add a new **fac** range to the dial plan.

To add a **fac** range from 70–79:

1. Type **`change dialplan`** and press **ENTER**.

   The ***`DIAL PLAN RECORD`*** form appears.
2. Move the cursor to the 7th 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 33.

Let us 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 **ENTER**.

The ***FEATURE ACCESS CODE (FAC)*** form appears.

Figure 7: Feature Access Code (FAC) form

```
                              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.

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

3 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 softphones. If you need to add or modify an attendant console or IP softphone, 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 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 phone 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, IP, 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 the "Station" section in the *Administrator's Guide for Avaya Communication Manager*, 555-233-506, for a list of phone types and how they should be administered.

NOTE:
Avaya no longer supports some older phone models.

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 — or media modules and ports.

To view a list of available ports on your system, type **`list configuration stations`** and press **ENTER**.

NOTE:
Because information is 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.**

Figure 8: System Configuration form

```
                              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

01C06      HYBRID LINE       TN762B     000004       01 02 P  P  P  P  P  P
01C09      MET LINE          TN735      000005       01 u  u  u  u  u  u  u
01C10      DIGITAL LINE      TN754      000004       u  u  u  u  u  u  u  u

001V2      DCP MM            MM712AP    HW02 FW005   u  u  u  u  u  u  u  u
001V3      ANA MM            MM711AP    HW03 FW016   u  u  u  u  u  u  u  u
```

The ***SYSTEM CONFIGURATION*** form shows all the boards (circuit packs) or media modules 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.

MCC1, SCC1, CMC1, G600, or G650 Media Gateways:

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).

G350 or G700 Media Gateways:

If you want to attach a phone to the 3rd port on the MM711 media module, the port address is 001V303 (001=number of the G700 Media Gateway, V3=slot, 03=port).

NOTE:

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

5 Choose an extension number for the new phone.

The extension you choose must not be previously 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 through 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 forms

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

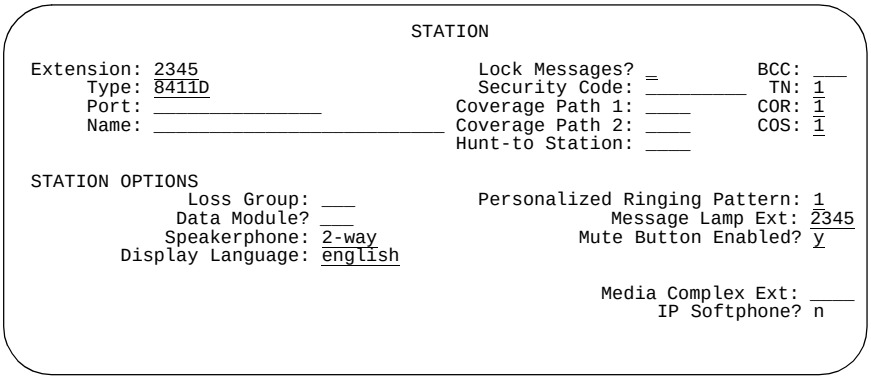
To access the ***STATION*** form for the new phone:

1. Type **add station** ***n*** and press **ENTER**, 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*** form appears, you see the extension number and some default field values. For example, the following form is for a new phone at extension 2345.

Figure 9: Station form



```
                                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 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 **ENTER**, 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*** form to add all the other extensions in the group.

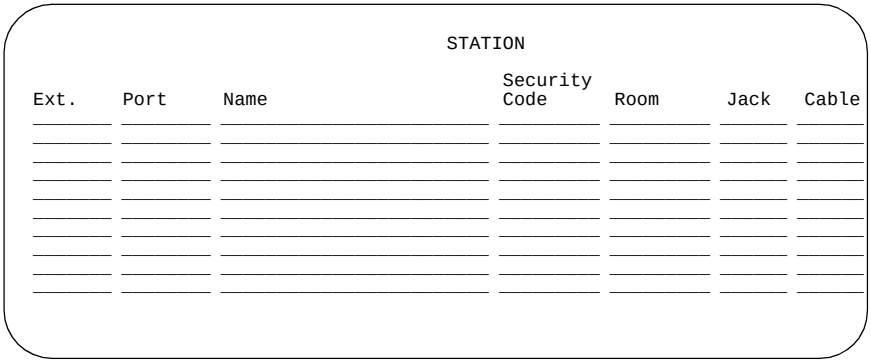
Note that only phones of the same model can be duplicated. The duplicate command copies all the feature settings from the template phone to the new phones.

To duplicate an existing phone:

1. Type **display station** ***n*** and press **ENTER**, where ***n*** is the extension of the ***STATION*** form 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 **ENTER**, where ***n*** is the extension you want to duplicate.

   The system displays a blank duplicate ***STATION*** form.

Figure 10: Duplicate Station form



```
                                    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*** form 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.

For example, we will create two aliases: one to add a new 6220 phone and one to add modems to our system.

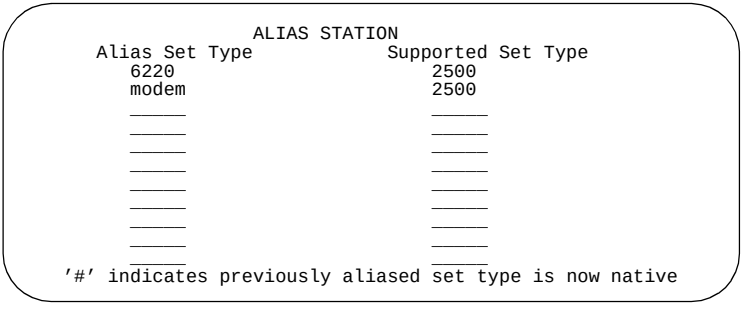
1 See your new phone's manual to find the correct alias.

In our example, we find that the 6220 should be administered on an older system as a 2500 phone.

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

The ***ALIAS STATION*** form appears.

Figure 11: Alias Station form



```
                    ALIAS STATION
   Alias Set Type              Supported Set Type
      6220                        2500
      modem                       2500
      _____                       _____
      _____                       _____
      _____                       _____
      _____                       _____
      _____                       _____
      _____                       _____
      _____                       _____
      _____                       _____
      _____                       _____
'#' indicates previously aliased set type is now native
```

3 Type **6220** in the `Alias Set Type` field.

This is the name or model of the unsupported phone.

4 Type **2500** in the `Supported Set Type` field.

This is the name or model of the supported phone.

5 Type **modem** in the second `Alias Set Type` field.

You can call the alias set anything you like. Once you define the alias, you can use the alias set in the `Type` field on the ***`Station`*** screen.

6 Type **2500** in the second `Supported Set Type` field.

Entering 2500 indicates to the system that these models are basic analog devices.

7 Press **ENTER** to save your changes.

Now you can follow the instructions for adding a new phone (or adding a fax or modem). Communication Manager now recognizes the new type (6220 or modem) that you entered in the `Type` field.

Be sure to see 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 form 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.

NOTE:
If you have 6400-series phones, your users can administer some of their own feature buttons. See "Setting up Terminal Self Administration" in the *Administrator's Guide for Avaya Communication Manager*, 555-233-506, for more information.

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`*** form 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.

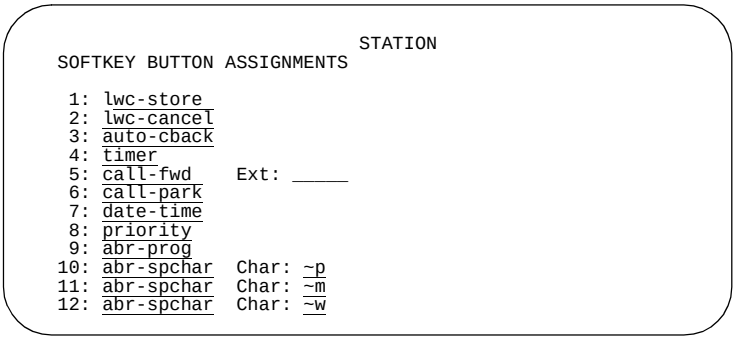
4. Type the button name that corresponds to the feature you want to add.

   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.

Figure 12: Default softkey assignments for an 8411D phone



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 allows you to change the button assignments on the form, and the features work on the alias phone. However, the labels on the display do not change.

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 form for that extension and enter the new model number.

NOTE:
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 **ENTER**.

The ***STATION*** form for extension 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 non-IP phone (phone A) with another non-IP 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.

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.

To swap an IP phone, simply move the phone and update the site data (see step #7 in the following instructions). For an IP phone, you should also update the 911 information. See E911 ELIN for IP wired extensions on page 93 for more information.

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 **ENTER**.
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 **ENTER**.
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 **ENTER**.
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.

When you swap phones, the system keeps the old button assignments. If you are swapping to a phone with softkeys, the phone could have duplicate button assignments, because softkeys have default assignments. You may want to check your button assignments and modify them as necessary.

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 **ENTER**.

   The ***GENERAL STATUS*** form 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 **ENTER**.

   The ***EXTENSION GROUP MEMBERSHIP*** form 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 form 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 **ENTER**.

   The ***USAGE*** form 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*** form, access the appropriate feature form 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 **ENTER**.

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

11 Type **`remove station 1234`** and press **ENTER**.

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

NOTE:
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 **ENTER** 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.

4 Managing features

This section explains how to administer some of the major 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*** form. However, if you have DEFINITY ECS R6.3.1 or later, some parameters have moved to new forms, such as the ***SYSTEM PARAMETERS CALL COVERAGE/CALL FORWARDING*** form.

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

As an example, say that your company uses Call Park, where a call can be put on hold and picked up from any other phone 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 **ENTER**.

   The ***FEATURE-RELATED SYSTEM PARAMETERS*** form appears.

Figure 13: Feature-Related System Parameters form

```
                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.

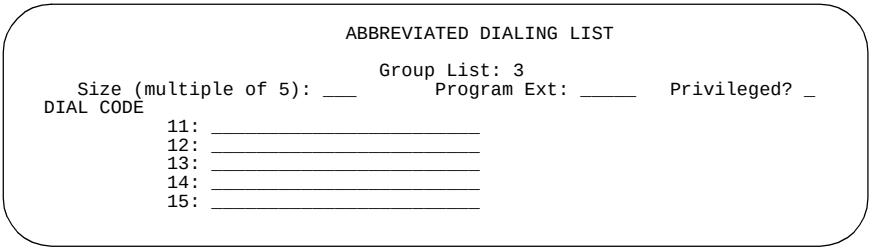
NOTE:
Note that this section does not tell you how to administer IP softphones or screenphones. If you need to set up an IP phone, refer to the *Administrator's Guide for Avaya Communication Manager*, 555-233-506.

As an example, let us define a new group list:

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

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

Figure 14: Abbreviated Dialing List form



```
                          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 If you want another user to be able to add numbers to this list, enter their extension in the `Program Ext` field.

For example, if you want the user at 4567 to be able to change group list 3, enter **4567** in this field.

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

Each phone number can be up to 24 digits long.

5 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 us 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 **ENTER**.

The ***`STATION`*** form for extension 4567 appears.

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

Figure 15: Station form (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 **ENTER**.

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.

features

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 **ENTER**.

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

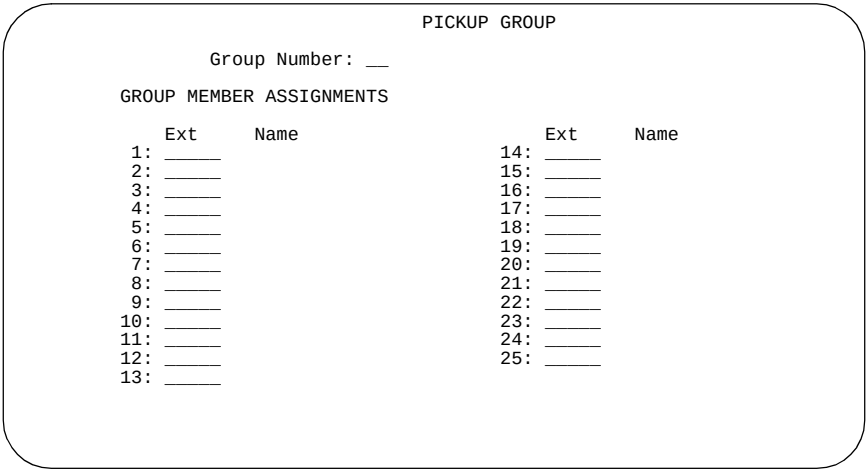
2. Enter the extension of each group member.

   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.

Figure 16: Pickup Group form



```
                              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*** form 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 form 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*** form 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*** form 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 **ENTER**.

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 **ENTER**.

   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.

Figure 17: Coverage Path form

```
                          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: ____
```

features

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 us assign this new coverage path to extension 2054:

1. Type **`change station 2054`** and press **ENTER**.

   The ***`STATION`*** form 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.

NOTE:
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 what 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.

As an example, 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 **ENTER**.

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.

Figure 18: Time of Day Coverage Table form

```
                        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 **ENTER**.

   The ***STATION*** form 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 **ENTER**.

   The ***COVERAGE ANSWER GROUP*** form appears.

Figure 19: Coverage Answer Group form

```
                    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**.

Setting up advanced call coverage

Advanced incoming call coverage:

- redirects calls based on time-of-day.
- allows coverage of calls that are redirected to sites not on the local server running Communication Manager.
- allows users to change back and forth between two coverage choices (either specific lead coverage paths or time-of-day tables).

Covering calls redirected to an off-site location

You can provide coverage for calls that have been redirected to an off-site location (for example, your home). This capability, called Coverage of Calls Redirected Off-Net (CCRON) allows you to redirect calls onto the public network and bring back unanswered calls for further coverage processing.

Before you start

- On the ***SYSTEM-PARAMETERS CUSTOMER-OPTIONS*** form, verify the `Coverage of Calls Redirected Off-Net Enabled` field is **y**. If not, contact your Avaya representative.
- You need call classifier ports for all situations except ISDN end-to-end signaling, in which case the ISDN protocol does the call classification. For all other cases, use one of the following:
  - — Tone Clock with Call Classifier - Tone Detector circuit pack. See the *Hardware Guide for Avaya Communication Manager* for more information on the circuit pack.
  - — Call Classifier - Detector circuit pack.

To provide coverage of calls redirected to an off-site location:

1 Type **`change system-parameters coverage-forwarding`** and press **ENTER**.

The ***SYSTEM PARAMETERS -- CALL COVERAGE / CALL FORWARDING*** form appears. Go to page 2.

Figure 20: System Parameters -- Call Coverage / Call Forwarding form

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

          SYSTEM PARAMETERS -- CALL COVERAGE / CALL FORWARDING

COVERAGE OF CALLS REDIRECTED OFF-NET (CCRON)

                    Coverage of Calls Redirected Off-Net Enabled? y
Activate Answer Detection (Preserve SBA) On Final CCRON Cvg Point? y
                                 Ignore Network Answer Supervision? n
              Disable call classifier for CCRON over ISDN trunks? n
```

2 In the `Coverage of Calls Redirected Off-Net Enabled` field, type **y**.

   This instructs Communication Manager to monitor the progress of an off-net coverage or off-net forwarded call, and provide further coverage treatment for unanswered calls.

3 In the `Activate Answer Detection (Preserves SBA) On Final CCRON Cvg Point` field, leave the default as **y**.

4 In the `Ignore Network Answer Supervision` field, leave the default as **n**.

5 In the `Immediate Redirection On Receipt Of PROGRESS Inband Information` field, leave the default as **n**.

6 Press **ENTER** to save your changes.

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*** form 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 **ENTER**.

The ***REMOTE CALL COVERAGE TABLE*** form appears.

Figure 21: Remote Call Coverage Table form

```
                        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: _________________
```

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.

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 **ENTER**.

The ***`COVERAGE PATH`*** form appears.

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

Figure 22: Coverage Path form

```
                         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 form contains the correct codes.

1 Type **`display feature-access codes`** and press **ENTER**.

The ***`FEATURE ACCESS CODES`*** form 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) form 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 forms with the **`display`** command.

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

NOTE:

If the security code has been assigned, a ***** appears in the `Security Code` field on the ***`STATION`*** form.

To allow users remote access to the system:

1. Type **`change telecommuting-access`** and press **ENTER**.
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 49).

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

   The ***`STATION`*** form appears.

Figure 23: Station form

```
                                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? _
```

features

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 type **abrdg-appr**
your primary phone is digital	move to the `Button Assignments` field and type **brdg-appr**

7 Press **ENTER**.

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

Figure 24: Station form (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:
```

Figure 25: Station form (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`** ***n***, where ***n*** is the extension, and press **ENTER**.

E911 ELIN for IP wired extensions

This feature automates the process of assigning an emergency location information number (ELIN) through an IP subnetwork during a 911 emergency call. The ELIN is then sent over CAMA or ISDN PRI trunks to the emergency services network.

Users have the ability to move their IP phones without notifying the administrator. If a user dials 911 after moving their IP phone without administering this feature, the emergency response personnel might go to the wrong physical location.

This feature properly identifies locations of wired IP phones that call an emergency number from anywhere on a campus or location. This feature is available with Communication Manager, Release 2.0.

This feature performs three essential functions:

- Emergency response personnel can now go to the correct physical location if an emergency call came from a moved IP wired telephone.
- Emergency response personnel can now go to the correct physical location if an emergency call came from a bridged call appearance.
- Emergency response personnel can return a call to the proper extension if a caller gets disconnected during the emergency call.

NOTE:
This feature depends upon the customer having subnetworks that correspond to geographical areas.

If you have Communication Manager, Release 2.0 or greater, this is an important feature to administer. For a detailed explanation of this feature, its function, and its forms, see the *Administrator's Guide for Avaya Communication Manager*, 555-233-506.

5 Routing outgoing calls

This section describes how 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 forms.

routing

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 us look at a simple ***ARS DIGIT ANALYSIS TABLE***. (Your system may have more defined dialed strings than our example.)

Figure 26: ARS Digit Analysis Table form

```
                    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.

As an example, 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.

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 form 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 form. 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 form. 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 **ENTER**.

The ***ARS DIGIT ANALYSIS TABLE*** for dialed strings that begin with the number 1 appears. Note that the switch displays only as many dialed strings as can fit on one form 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 **ENTER**.

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.

NOTE:
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 us 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.

NOTE:
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 **ENTER**.

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

The ***`ARS ROUTE CHOSEN REPORT`*** form appears.

Figure 27: ARS Route Chosen Report form

```
                    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 form.

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 **ENTER**.

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

Figure 28: 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 Type **1650** in the `Dialed String` field.

6 Type the minimum and maximum values from step 2 in the `Total Mn` and `Total Mx` fields.

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

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

In our example, type **30**.

8 Type the call type from step 2 in the `Call Type` field.

In our example, type **fnpa**.

9 Type 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 **ENTER**.

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

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

   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. Type **01157** in the `Dialed String` field.

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

5. Type **deny** (denied) in the `Route Pattern` field.

6. Type **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.

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

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*** form.

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

1. Type **`change authorization-code`** ***`4395721`*** and press **ENTER**.

   The ***AUTHORIZATION CODE - COR MAPPING*** form appears.

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

3 In the COR field, type **2**.

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

Figure 29: Authorization Code - COR Mapping form

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

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.

ARS partitioning allows you to provide different call routing for a group of users or for specific phones.

NOTE:

If you used partitioning on a prior release of Communication Manager and you want to continue to use partitioning, please read this section carefully. In this release of Communication Manager, partition groups are defined on the ***PARTITION ROUTE TABLE*** form. If you want to define routing based on partition groups, use the ***PARTITION ROUTE TABLE*** form. Partition groups are no longer defined on the ***DIGIT ANALYSIS TABLE*** form.

Before you start

Verify that the `Tenant Partitioning` field on the ***SYSTEM PARAMETERS CUSTOMER OPTIONS*** form is **y**.

Verify that the `Time of Day Routing` field on the ***SYSTEM PARAMETERS CUSTOMER OPTIONS*** form is **n**.

Setting up a partition group

As an example, 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.

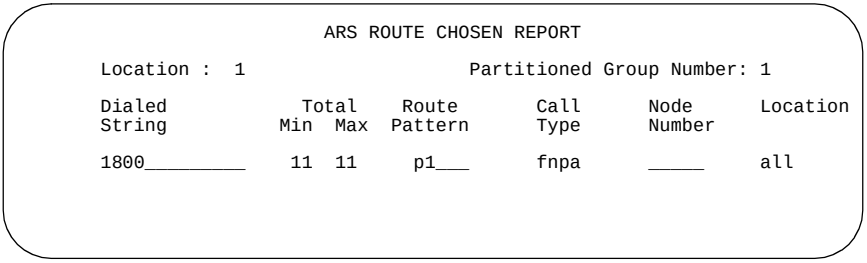
To enable 1 800 calls for partition group 2:

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

   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.

routing

Figure 30: ARS Route Chosen Report form



```
                    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
```

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:

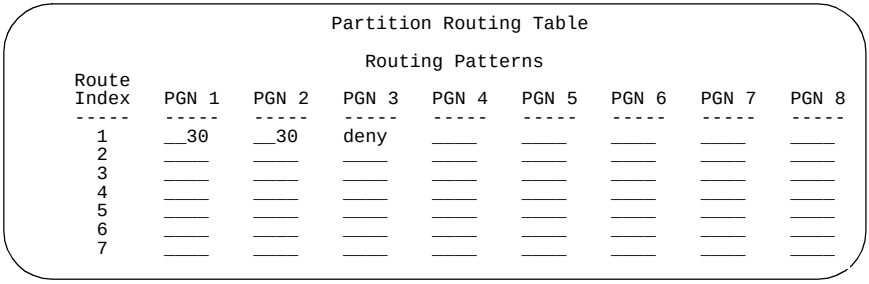
If there is a number (with no **p**) under `Route Pattern` on the ***ROUTE CHOSEN REPORT***, then all partitions use the same route pattern. You need to use the ***PARTITION ROUTING TABLE*** only if you want to use different route patterns for different partition groups.

3 Press **CANCEL** to return to the command prompt.

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

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

Figure 31: Partition Routing Table form



```
                    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 **ENTER**.

The ***`CLASS OF RESTRICTION INFORMATION`*** form appears.

Figure 32: Class of Restriction Information form

```
                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 **ENTER**.

The ***`CLASS OF RESTRICTION`*** form appears.

Figure 33: Class of Restriction form

```
                              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 Type **2** in the `Partition Group Number` field.

NOTE:

The Partition Group Number field appears only when *Time of Day Routing* is **n** on the **SYSTEM PARAMETERS CUSTOMER OPTIONS** form. Otherwise, you specify the partition group number (PGN) on the ***TIME OF DAY ROUTING PLAN*** form. 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 **ENTER**.

The ***STATION*** form for extension 1234 appears.

2 In the COR field, type **3**.

3 Press **ENTER** to save your changes.

routing

6 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.

NOTE:
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.

NOTE:
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 **ENTER**. (Use the new login name as part of the **add** command.)

The ***LOGIN ADMINISTRATION*** form appears.

Figure 34: Login Administration form

```
                              LOGIN ADMINISTRATION

              Password of Login Making Change:

           LOGIN BEING ADMINISTERED
                                Login's Name: angi3
                                  Login Type:
                               Service Level:
     Disable Following a Security Violation?
                                                 Access to INADS Port? _

           LOGIN'S PASSWORD INFORMATION
                           Login's Password:
                    Reenter Login's Password:
         Password Aging Cycle Length (Days): 30

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

ACCESS SECURITY GATEWAY PARAMETERS
   Access Security Gateway? n
```

The `Login's Name` field shows the name you typed in the **add** command. Other fields contain defaults.

2 In the `Password of Login Making Change` field, type your superuser password.

3 In the `Disable Following a Security Violation` field, type **y** to disable this login following a login security violation.

This field appears only if on the ***SECURITY-RELATED SYSTEM PARAMETERS*** form, the SVN `Login Violation Notification` field is **y**.

4. In the `Login's Password` field, assign an initial password for the new login. For our example, type **b3stm0m**.

   The password does not appear on the form as you type.

5. In the `Reenter Login's Password` field, retype the initial password for the new login. For our example, retype **b3stm0m**.

   The password does not appear on the form as you type.

6. In the `Password Aging Cycle Length (Days)` field, type **30**.

   This requires the user to change the password every 30 days.

7. Press **ENTER** to save your changes.

   Now you need to set the permissions for this new login.

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 **ENTER**. (Use the new login name as part of the **`change`** command.)

   The ***`COMMAND PERMISSION CATEGORIES`*** form appears.

Figure 35: Command Permission Categories form

```
                              Login Name: angi3
 COMMON COMMANDS
                  Display Admin. and Maint. Data? n
                              System Measurements? n

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

MAINTENANCE COMMANDS
          Maintain Stations? n         Maintain Switch Circuit Packs? n
            Maintain Trunks? n        Maintain Process Circuit Packs? n
           Maintain Systems? n                  Maintain Enhanced DS1? n
```

If you want the default permissions, press **CANCEL**.

If you want to change any permissions, type **y** to give the user access, or **n** to restrict access for each permission type. For example:

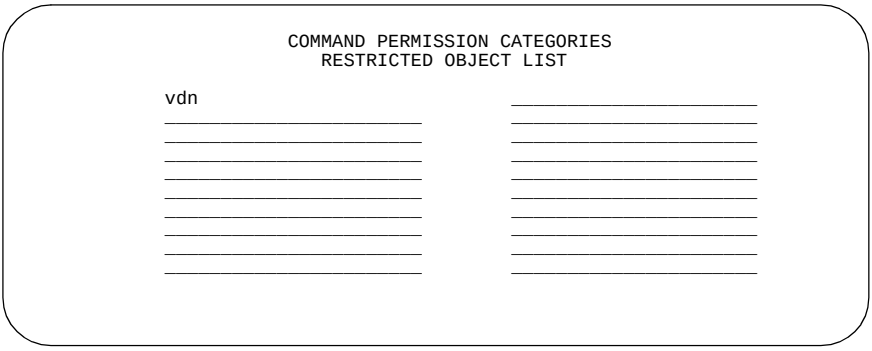
2 In the `Administer Stations` field, type **y**.

This allows your user to add, change, duplicate, or remove stations (phones), data modules, and associated features.

3 In the `Additional Restrictions` field, type **y**.

A **y** in this field brings up the second and third pages of this form.

Figure 36: Command Permission Categories form



4 In the first field, type **vdn**.

This restricts your user from administering a VDN.

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

Changing passwords

You should change your passwords often.

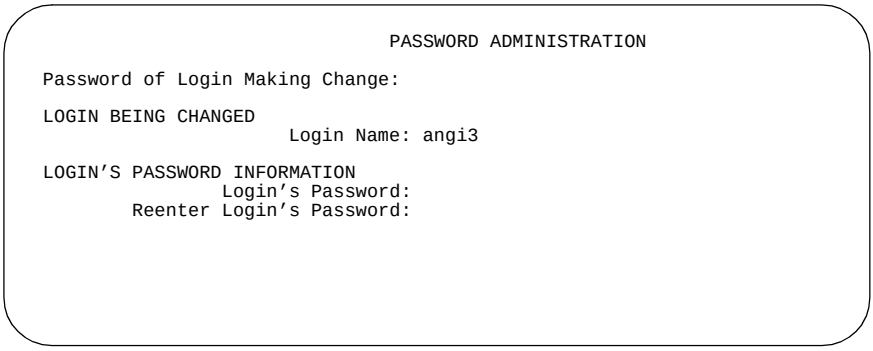
NOTE:
To force users to change passwords, set password aging in the Login Administration form. See Changing logins for instructions.

To change the password (b3stm0m) for angi3:

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

The ***PASSWORD ADMINISTRATION*** form appears.

Figure 37: Password Administration form



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.

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 **ENTER**.

   The ***`LOGIN ADMINISTRATION`*** form 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 phone 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 Toll Fraud and 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 15 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 access.

Make sure secure passwords exist for all logins that allow System Administration or Maintenance access to the system. Change the passwords frequently.

Set logoff notification and forced password aging when administering logins. You must assign passwords for these logins at setup time.

Establish well-controlled procedures for resetting passwords.

2 Prevent voice mail system transfer to dial tone.

Activate "secure transfer" features in voice mail systems.

Place appropriate restrictions on voice mail access/egress ports.

Limit the number of invalid attempts to access a voice mail to five or less.

3 Deny unauthorized users direct inward system access (screen).

If you are not using the Remote Access features, deactivate or disable them.

If you are using Remote Access, require the use of barrier codes and/or authorization codes set for maximum length. Change the codes frequently.

It is your responsibility to keep your own records regarding who is allowed to use which authorization code.

4 Place protection on systems that prompt callers to input digits.

Prevent callers from dialing unintended digit combinations at prompts.

Restrict auto attendants and call vectors from allowing access to dial tone.

5 Use system software to intelligently control call routing.

Create Automatic Route Selection or World Class Routing patterns to control how each call is to be handled.

Use "Time of Day" routing capabilities to limit facilities available on nights and weekends.

Deny all end-points the ability to directly access outgoing trunks.

6 Block access to international calling capability.

When international access is required, establish permission groups.

Limit access to only the specific destinations required for business.

7 Protect access to information stored as voice.

Password restrict access to voice mail mailboxes.

Use non-trivial passwords and change passwords regularly.

8 Provide physical security for telecommunications assets.

Restrict unauthorized access to equipment rooms and wire connection closets.

Protect system documentation and reports data from being compromised.

9 Monitor traffic and system activity for abnormal patterns.

Activate features that "turn off" access in response to unauthorized access attempts.

Use Traffic and Call Detail reports to monitor call activity levels.

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

From safely using calling cards to securing voice mailbox password, train your users on how to protect themselves from inadvertent compromises to the system's security.

11 Monitor access to the dial-up maintenance port. Change the access password regularly and issue it only to authorized personnel. Consider activating Access Security Gateway (see the *Administrator's Guide for Avaya Communication Manager, 555-233-506*).

12 Create a system-management policy concerning employee turnover and include these actions:

- Delete any unused voice mailboxes in the voice mail system.
- Immediately delete any voice mailboxes belonging to a terminated employee.
- Immediately remove the authorization code if a terminated employee had screen calling privileges and a personal authorization code.
- Immediately change barrier codes and/or authorization codes shared by a terminated employee. Notify the remaining users of the change.
- Remove a terminated employee's login ID if they had access to the system administration interface. Change any associated passwords immediately.

13 Back up system files regularly to ensure a timely recovery. Schedule regular, off-site backups.

14 Callers misrepresenting themselves as the "phone company," "AT&T," "RBOCS," or even known employees within your company may claim to be testing the lines and ask to be transferred to "900," "90," or ask the attendant to do "start 9 release." This transfer reaches an outside operator, allowing the unauthorized caller to place a long distance or international call. Instruct your users to never transfer these calls. Do not assume that if "trunk to trunk transfer" is blocked this cannot happen.

15 Hackers run random generator PC programs to detect dial tone. Then they revisit those lines to break barrier codes and/or authorization codes to make fraudulent calls or resell their services. They do this using your telephone lines to incur the cost of the call.

Frequently these call/sell operations are conducted at public pay phones located in subways, shopping malls, or airport locations. See the "QSIG to DCS TSC Gateway" section in the *Administrator's Guide for Avaya Communication Manager, 555-233-506*, to prevent this happening to your company.

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 Toll Fraud and 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 (SVN) 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

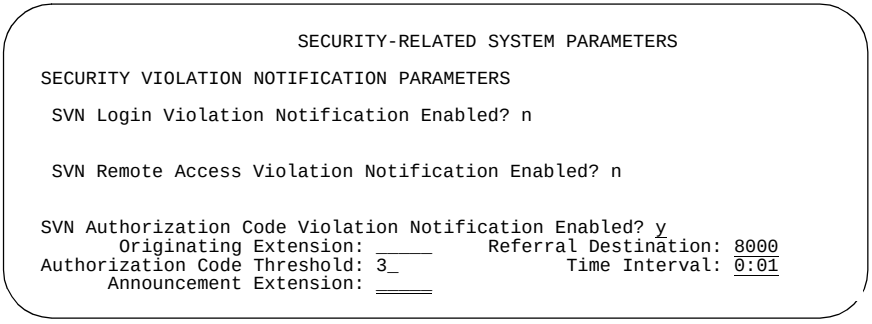
For example, let us have the system notify us at extension 8000 when someone tries to enter more than 3 invalid authorization codes within a 1-minute time span.

To set up Security Violations Notification for our example:

1 Type **`change system-parameters security`** and press **ENTER**.

The ***SECURITY-RELATED SYSTEM PARAMETERS*** form appears.

Figure 38: Security-Related System Parameters form



```
                        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 Login Violation Notification Enabled` field, type **y** and press **ENTER**. Additional fields now display on the form.

This sets SVN login violation notification.

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.

This is 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.

This is 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.

For more examples, see the Enhancing System Security section in the *Administrator's Guide for Avaya Communication Manager, 555-233-506*.

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 **ENTER**.

To display a ***SECURITY VIOLATIONS SUMMARY*** report:

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

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 **ENTER**.

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

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

   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 **ENTER**.

7 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 forms 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 form 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 **ENTER**.

NOTE:
To print a form 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 analysis print** — prints your dial plan analysis table
- **display dialplan parameters print** — prints your dial plan 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 **ENTER**.

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

1 Type **`display data 5567 print`** and press **ENTER**.

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 22.

Notes

Index

A

B

C

D

E

F

G

H

I

K

L

M

O

P

R

S

T

U

V

W

X