Avaya Communication™ Manager Application Notes: Emergency Calling

Abstract

Communication Manager 2.0 software has these emergency calling features:

- Crisis Alert to Attendant,
- Crisis Alert to Digital Station,
- Crisis Alert to Pager,
- Off-Hook Alert Class of Service,
- Emergency Priority Attendant Queue,
- List Emergency,
- Location Based Routing,
- ISDN Trunks,
- CAMA Trunks,
- CPN for PSA Dissociated Sets,
- Remote Softphone Emergency Calls,
- Emergency Location Extension by Station ,
- Subnet Based Device Location for IP Phones,
- Emergency Location Extension Forwarding.

Communication Manager 2.0 software also has some emergency call handling interactions with other Communication Manager features.

Table of Contents

1. Introduction

This paper covers emergency (e.g. 911) calling features provided by Avaya Communication™ Manager 2.0 software, whether as part of the standard software or by special applications. It does not provide details of features that are:

1. Currently being considered for future Communication Manager releases past Communication Manager 2.0. For example, this paper does not cover 2.1.
2. Provided by adjuncts compatible with Communication Manager 2.0 software but not in the Communication Manager 2.0 offer, whether sold by Avaya or by outside vendors. The following section 1.1.1 on page 5 gives contact information for some of those products.
3. Used by a Communication Manager server installed inside a Public Safety Answering Point (PSAP) to distribute incoming 911 calls to PSAP agents.
4. Used to provide ordinary calling during power failures, even though the adjective "emergency" is sometimes used to describe such features.

5. Used to provide ordinary calling during a no-license condition, even though the adjective "emergency" is used on the "system-parameters features" form to describe the a no-license condition.
6. Used to trace malicious calls, even though the adjective "emergency" is sometimes used to describe such calls.

1.1.1. Development Connection Partners

These adjuncts are compatible with Communication Manager 2.0 software but are not in the Communication Manager 2.0 offer. This is not guaranteed to be a complete list of all possible adjuncts compatible with Communication Manager 2.0 software.

- Dialogics Communication Corp. (DCC) sells the Communicator![1]. Addressing the communications needs of the mission-critical environment, this high-speed notification system alerts individuals, groups or teams by phone, pager, fax, email, etc.; delivers incident-specific information and/or potentially life-saving instruction; confirms message receipt; and prints, faxes and emails comprehensive reports detailing call-out results[i]. Contact: Lorin Bristow, (615) 790- 2822, lorin.bristow@dccusa.com, http://www.dccusa.com/products.html.
- RedSky Technologies, Inc. sells the Cielo E911 Manager[2]. The Cielo E-911 Manager is a turnkey solution to E-911 optimization. This software solution automatically pinpoints the exact station location of the emergency call, managing and reporting all E-911 station information changes as they occur. The Cielo E-911 Manager requires little or no additional staff to provide a nearly maintenance-free system[ii]. Contact Penny Schyler, (312) 432- 5981, pschyler@redskytech.com, http://www.redskytech.com.
- XTEND Communications Corp. sells the Enterprise Alert[3]. XTEND Enterprise Alert translates calling party identification information to ANI (Automatic Number Identification), providing detailed location information or ALI (Automatic Location Identification) about the 911 caller to the PSAP (Public Safety Answering Point). Enterprise Alert also provides additional support for non-DID (Direct Inward Dial) numbers, ANI/ALI update facility to the public ALI database, radio paging, LED display, and private PSAP call monitoring and display capabilities for PBX environments. Enterprise Alert integrates with industry-standard CAMA trunks[iii]. Contact: Donna Messineo, (212) 951- 7674, dmessineo@xtend.com, http://www.xtend.com/productset.htm.

The Business Development Manager for the above products is Matt Parker, (732) 852- 3664, mparker@avaya.com.

[1] The Communicator! is a trademark of Dialogics Communication Corp.
[2] Cielo is a trademark of RedSky Technologies, Inc
[3] Enterprise Alert is a trademark of XTEND Communications Corp.

1.2. Notation, Terminology And Acronyms

There are several sample administration forms in this document. The fields shown in **bold** in the sample administration forms are the ones of interest to emergency call handling. Some forms have been simplified by omitting several fields not used for emergency call handling.

The following table gives meanings for most of the terms and acronyms used in this document.

Term	**Meaning**
AAR	Automatic Alternate Routing
ACTR	Automatic Customer Telephone Rearrangement, a feature allowing DCP phones to move. Section 5.2 on page 45 describes it.
ALI	Automatic Location Information, the location data associated with a specific ANI. It is used by the PSAP for looking up street addresses from the phone number sent by voice servers during 911 calls.
ALI database	The database used by the PSAP to look up street addresses from the phone number sent by voice servers during 911 calls. The database contains other location, user and service type information as well.
ARS	Automatic Route Selection, a feature for choosing which trunk will carry a call.
AWOH	Administered without hardware: an extension number lacking an associated physical telephone.
DHCP	Dynamic Host Configuration Protocol: a mechanism for signaling IP addresses from a server to an endpoint. DHCP has other capabilities not relevant to 911 call handling.
DID	Direct Inward Dialing
CAMA	Centralized Automatic Message Accounting. A type of trunk used only for emergency calls in the USA.
CCMS	Common Channel Message Set, an Avaya proprietary signaling protocol.
CESID	Caller's Emergency Service Identification, the calling party information sent to USA emergency services network over CAMA trunks. This consists of the 7 digit local number plus a one digit equivalent to the area code.
CLAN	Control-LAN, a Communication Manager IP interface circuit pack.
Close to, Nearby	This document uses these terms to mean the maximum desired distance between an emergency caller and the corresponding Emergency Location Extension. This will depend on state legislation, but will probably be between 7,000 and 40,000 square feet[iv], i.e., roughly within a circle of radius between 15 and 35 meters.
Communication Manager	The Avaya trademark for a voice server formerly called Multivantage™ Voice Server, formerly called DEFINITY® PBX.
CO	Central Office
COR	Class of Restriction, administration restricting extensions' calling

Term	Meaning
	permissions.
COS	Class of Service, administration restricting extensions' feature usage permissions.
CPN	Calling Party Number. Other documents sometimes call this Automatic Number Identification (ANI) or Caller Identification (CID).
DCP	proprietary Digital Communications Protocol for Avaya telephones.
DID	Direct Inward Dialing
DND	Do Not Disturb, a feature peventing calls from ringing at an extension.
E911	Enhanced 911. It allows the emergency response system to determine your street address from your phone number.
E911 Tandem Office	The PSTN switch that accepts an E911 call from a voice server or from a local CO connected to the voice server, and routes the call to the local PSAP. One E911 Tandem Office typically covers roughly the geographic area of 4 adjacent area codes.
Emergency Transfer	Emergency Transfer provides service to and from the local telephone company CO during a power failure or when service is impaired. Emergency Transfer is also called Power Failure Transfer; the terms are synonymous. This document does not cover power failure transfer.
FAC	Feature Access Code, a digit sequence dialed in order to use a feature.
ICC	Internal Call Controller, a processor on a Gateway.
ISDN	Integrated Services Digital Network
IP	Internet Protocol
LAN	Local Area Network
Location	This refers to the area covered by all endpoints on a Communication Manager voice server with the same Multiple Locations number administered for them on the ip-network-map, media gateway, or cabinet forms. When there might be confusion between this meaning and the broader English language meaning of the word, this document uses the phrase "Communication Manager location".
MSAG	Master Street Address Guide, a database used to validate ALI information.
MST	Message Sequence Trace, an Avaya maintenance feature.
NPI	ISDN Numbering Plan Identifier
PPP	Point to Point Protocol, the IP protocol commonly used over modems.
PSA	Personal Station Access, a feature allowing circuit switched phones to move. Section 5.2 on page 45 describes it.
PSAP	Public Safety Answering Point, the office that answers a public network emergency call such as a 911 call in the USA.
PSTN	Public Switched Telephone Network.

Term	**Meaning**
Public number	A number reachable from the public network, for example, a DID extension or a Listed Directory Number. Such numbers can have associated street addresses in the ALI database.
QSIG	ISDN signaling using the Q (private network) signaling standard.
LSP	Local Spare Processor, a backup processor to control IP devices when they can not reach the main processor.
MCT	Malicious Call Trace. A feature to trace and record calls.
SAC	Send All Calls, a feature preventing calls from ringing at an extension.
SIP	Session Initiation Protocol. An IP call control signaling protocol.
SREPN	Survivable Remote Expansion Port Network, a port network with its own backup translations and processor.
Subnet	A collection of IP addresses that can talk directly to each other through a single local data switch.
TTI	Terminal Translation Initialization, a feature allowing circuit switched phones to move. Section 5.2 on page 45 describes it.
VLAN	Virtual LAN. The VLAN ID tag is located in the 802.1Q header. IP subnets are frequently, but not always, configured with one VLAN per subnet.
VOIP	Voice over IP
TON	ISDN Type of numbering
WAN	Wide Area Network
WSP	WAN Spare Processor, a port network with its own backup translations and processor.

2. Internal Emergency Notification

There are two main types of emergency notifications: those going to the enterprise's staff, for example to a building security office, and those going to public response personnel, i.e. the folks who answer 911 calls. This section describes a Communication Manager server's treatment of the enterprise notification; section 3 on page 22 and later sections describe a Communication Manager server's treatment of public emergency calls.

2.1. Crisis Alert

If one of your users calls an emergency service such as the police or ambulance, someone, perhaps the receptionist, the security office or the front desk, needs to know who made the call. When the public emergency personnel arrive, they can be directed to the right place. You can set up Communication Manager software to alert an attendant or other extensions whenever a phone user dials an emergency number.

Crisis Alert notifies an attendant, designated extensions, or a pager when an emergency call is made, and shows the name and number of the person who placed the emergency call. This information allows an attendant or other user to direct an emergency service response to the caller. The notified set makes an audible alerting sounding like an ambulance siren. The set also flashes the crisis alert button lamp and displays the caller name and extension. The crisis alert station users must acknowledge the crisis to turn off the alerting. This crisis alert feature provides only the visual and audible alerting to the designated stations; no talk path is provided between those stations and the set that dialed the emergency call.

2.1.1. Crisis Alert To Attendant

When crisis alerting is active at an attendant console, the console is in position-busy mode so no other incoming calls interfere with the emergency call. The console can still originate calls. The attendant must press the position-busy button to unbusy the console and then press the crss-alert button to deactivate audible and visual alerting. Attendants cancel an alert by pressing the crisis alert button three times. The first button push turns off the siren, the second stops the lamp from flashing, and the third clears the display. If Centralized Attendant Service is enabled, the alert still goes to the local attendant.

The Night Service / Night Station Service feature has no impact on the Crisis Alert feature. When in Night Service, the Crisis Alert notification is delivered to the attendant console, not the night station, unless the night station also has a crss-alert button.

2.1.2. Crisis Alert To Digital Station

Digital phone users acknowledge the crisis alert alarm by pushing the crisis alert button. This silences the siren sound. If you have set the system so only one user needs to respond, the first user to do so stops the alerting at all phones. If all users must respond, each phone continues to alert until each user presses the crisis alert button to acknowledge the alarm. The emergency caller’s name and extension remain on the display at this point. To completely cancel an alert and clear their displays to be ready for the next crisis, users press the Exit button. This button may be called a variety of names (i.e. Exit, Normal, disp-norm, etc.), depending on the set type. The ringing signal associated with a Crisis Alert is silenced by pushing the crss-alert button. Once the user has pushed the crss-alert button during an active Crisis Alert, no display related button pushes will be allowed other than the Normal Display Mode (Exit) button, with the exception of the timer button.

Unlike the Attendant Crisis Alert feature, there is no attempt to block incoming calls to digital stations with the Crisis Alert to digital station feature, although the digital station user may press the Send All Calls (SAC) or Do Not Disturb (DND) button to provide this function.

2.1.3. Crisis Alert To a Digital Pager

Crisis Alert to a Digital Pager allows users to receive crisis alert messages on a pager when a crisis alert call is originated in an emergency situation. The pager displays a message of 7 to 22 digits: a crisis alert code, an extension number, and a main number if one is entered, so the pager knows the voice server from which the emergency call originated.

A crisis alert call will use from 2 to 4 trunks. This is because one trunk will be used for the actual emergency call and 1 to 3 trunks will be used to notify the pager(s) depending on the how many pagers are administered.

For CO type trunks, on the trunk group form, either:

- the trunk "Answer Supervision Timeout" field should be set to 0 (zero) and the "Receive Answer Supervision" field set to "y" or
- a value should be entered in the "Answer Supervision Timeout" field, with the "Receive Answer Supervision" field set to "n".

Communication Manager software uses answer supervision to determine whether attempts to reach the digital paging service need to be re-tried. If a crisis alert to digital pager call might route over analog trunks, then the system should contain a call classifier resource.

If you have a multiple voice server campus, you could use the Crisis Alert To a Digital Pager feature to alert security officers on one voice server that a user on a different voice server has dialed a crisis alert call. To do so, reserve one extension number on the security office's voice server for every other voice server in the campus. Make those numbers the targets of the digital page call. The security officer answering the resulting paging call could deduce from the ringing call appearance which voice server originated the crisis alert to a pager call. The officer could then look up the extension number of the station that dialed the emergency call from an administration terminal for the appropriate voice server. You don't need to dedicate a phone for this use, just an extension number. You could make the digital paging target an AWOH extension and then put bridged appearances of that on the security office's phones.

2.1.4. Administration

You can administer crisis alert as follows.

2.1.4.1 ARS

Assign the ARS call type "alrt" to the digit strings Communication Manager software should launch alerts for when dialed.

```
change ars analysis 1                                        Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location:     2         Percent Full:    6

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    11                    2    2     2        alrt         n
    911                   3    3     2        alrt         n
```

2.1.4.2 System-Parameters Crisis-Alert

```
change system-parameters crisis-alert                        Page   1 of   1
                         CRISIS ALERT SYSTEM PARAMETERS

ALERT STATION
    Every User Responds? n

ALERT PAGER
            Alert Pager? y
  Originating Extension: 84927
      Crisis Alert Code: 123
                Retries: 1
    Retry Interval(sec): 30
            Main Number: 3035380000

                          Pager Number          Pin Number
                       1:                    1:
                       2:                    2:
                       3:                    3:

                  DTMF Duration - Tone (msec): 100  Pause (msec): 100
```

These fields are used as follows.

Key Word	Usage
Every User Responds	Controls whether all users who have a crisis alert button must clear the alert for every crisis alert. If set to n, all users are notified, but only one user needs to acknowledge an alert.
Alert Pager	Turns on Crisis Alert to a Digital Pager.
Originating Extension	When some other extension originates an emergency call, this is the extension number Communication Manager uses to launch the outgoing trunk call to the digital pager. Be sure this contains an assigned extension, or the page may not be sent.
Crisis Alert Code	The first 3 digits in the message sent to the pager. It is typically set to "911".

Key Word	Usage
Retries	The number of times the system tries to call a pager in case of an unsuccessful attempt.
Retry Interval(sec)	The time period in seconds between retries to call a pager in case of an unsuccessful attempt.
Main Number	The last group of digits in the message sent to the pager. It is typically set to the LDN of the voice server originating the crisis alert call.
Pager Number	The number dialed to reach a pager.
Pin Number	The personal identification number required by the pager service.
DTMF Duration	The length of tone and pause for each digit sent in the pager message.

2.1.4.3 Crisis Alert Button

Assign a crisis alert button (crss-alert) to stations such as those used in a security office, or to an attendant. Use change station for stations, and change attendant for attendants. You can assign a maximum of 38 crss-alert buttons per system: 10 for digital sets, and 28 for attendant consoles. The button to be assigned as the crss-alert button on the set must have a lamp associated with it, and may not be a soft key. To use crisis alert to a digital pager, you still need to administer a crss-alert button on at least one attendant console or digital station. If you only use crisis alert to pagers, not to attendants or stations, and do not have any users who want such a button, you can administer the button to an AWOH extension. The extensions of all Crisis Alert stations may be displayed by using the "list usage button-type crss-alert" command.

```
list usage button-type crss-alert

                             LIST USAGE REPORT

   Located on
   Station Extension      22200             Button 7
   Station Extension      22204             Button 7
   Station Extension      22203             Button 8
   Attendant Number       1         Feature Button 2
```

2.1.5. Multiple Emergency Calls

If a crisis alert call is made while another crisis alert is still active, the newer call will be placed in queue. If you have administered the system so all users must respond, then every user must respond to every call. If you have administered the system so only one user must respond, the first crisis alert remains active at the phone where it was acknowledged. Any subsequent calls are queued to all available other crisis alert stations in the order in which the calls were made.

2.1.6. Phone Display

When an emergency call is made and a crisis alert station with a 27-character display is notified, only 17 characters of the name field appear on the first display line, followed by the extension. The second line contains the last 3 characters of the name field, followed by the word "EMERGENCY." Characters 18 through 24 of the name field do not appear at all. Consider the display for emergency notification when you complete the name field on the station form. Put the most important identifying information at the beginning of the field.

2.1.7. Terminal Self Administration

Those users who have the ability to administer their own phone buttons do not have the ability to disable a crisis alert button.

2.1.8. All Trunks Busy

If a user attempts to make an emergency call, but all trunks in the selected route pattern are busy, the call will not generate an alert. If Outgoing Trunk Queuing is enabled for a trunk group, the call will queue to the trunk group, but will not generate an alert.

2.1.9. Breaking Into Or Recording A 911 Call

If you choose to give attendants or security personnel crisis alert buttons (crss-alert) as described in section 2.1 on page 8, they would be notified of 911 calls in progress. If those support staff also had intrusion buttons or service observing buttons (serv-obsrv), they could listen in on 911 calls in progress and offer assistance, for example giving better directions to a building on a campus than a panicked user gives. There is a slight risk in using this strategy, though. If the phone user has an IP phone and moved it before dialing 911, or if the phone user has a wireless phone, the phone user is the only one who knows where it is. The security office may give good directions to where the user's phone is supposed to be, not to where it actually is. For such reasons, the general NENA membership does not usually recommend breaking into a 911 call. In some jurisdictions it is illegal to do so. Every station you might wish to observe must be built into a split. With large numbers of stations, the administration of this might get unwieldy.

In the same way, you could give attendants or security personnel the ability to start recordings of 911 calls once their crisis alert buttons had notified them that a 911 call was in progress. If you wish to, you could do this by setting up Malicious Call Trace (MCT) call recording and assigning to them MCT activation (mct-act) and MCT control (mct-contr) buttons, assigning Access to MCT permissions on their COR, and administering their extension numbers on the mct-group-extensions form.

Alternatively, if the support staff has the ability to intrude into a 911 call as mentioned above, they could use an Audix™ recording button (audix-rec) to record the 911 call. You would have to use this alternative if you have S8300 servers. MCT requires an Auxiliary trunk port, and S8300 servers do not support Auxiliary trunks.

2.2. Emergency Access To The Attendant

Emergency Access to the Attendant enables a user to place an emergency call to an attendant. Emergency access to attendant calls can be placed automatically by the system or dialed by phone users. Such calls can receive priority handling by the attendant. You can place emergency calls to the attendant in the following ways:

- Dial access by a phone user. A user can place an emergency call to the attendant by dialing the Emergency Access to the Attendant feature-access code.
- Automatically by the system. To set this up, assign a telephone the Off-Hook Alert option via its Class of Service (COS). If the terminal is left off-hook until intercept timeout, the administrable off-hook alerting timer starts. If the terminal is still off-hook when the timer expires, an emergency call is automatically placed to the attendant.

When an emergency access to attendant call is placed, one of the available attendants receives visual and audible notification of the call. If all attendants are busy, the call enters a queue for emergency access to attendant calls. Calls can be administered to redirect to another extension if the queue is full.

An emergency access to attendant call causes the following to occur:

1. The system selects the first available attendant to receive the call.
2. The attendant hears the emergency tone and sees the lamp associated with the Emergency button, if assigned, light. If the console does not have emergency-tone capability, the attendant hears normal ringing and sees the display flash. The emergency tone cannot be silenced except by answering the emergency access to attendant call.
3. The attendant display shows:
   - Calling-party identification
   - Calling-party extension
   - How many emergency access to attendant calls remain in queue

The station user who activated an Emergency Call to the attendant is not allowed to hold the call during the time the ringback tone is given to the station. The station user who dialed the emergency call to the attendant is not allowed to transfer or conference the emergency call at any time. It would not be a good idea for the attendant to answer the emergency call with "Please hold." and then put the caller on hold.

2.2.1. Centralized Attendant Service (CAS)

For a branch with CAS in effect, an emergency access to attendant call reroutes to the branch attendant group. If the branch does not have an attendant or if the branch is not in CAS Backup Service, the call is denied. If the branch voice server is in CAS Backup Service, an emergency access to attendant call routes to the backup position and is handled as any other non-emergency call.

2.2.2. Inter-PBX Attendant Service

For branches with Inter-PBX Attendant Service in effect, an emergency access to attendant call reroutes to the local attendant group. If the branch does not have an attendant or if the attendant is not on duty, the call is denied.

2.2.3. Class Of Restriction (COR)

An emergency access to attendant call overrides all COR restrictions, even controlled restriction.

2.2.4. Individual Attendant Access

An emergency access to attendant call cannot be placed to an individual attendant.

2.2.5. Night Service

When Night Service is in effect, emergency access to attendant calls route to the night destination. Such calls are included on the Emergency Record, and the call is designated as Emergency Night in the record.

To handle calls when an attendant is in night service, you should assign either a night station or a redirect extension. Otherwise emergency calls to the night attendant would hear a busy tone. The system should have at least one day and one night attendant or night service station for this feature to be useful at all times.

2.2.6. Remote Access

An emergency access to attendant call cannot be placed from a Remote Access extension.

2.2.7. Administration

To enable this feature, either the "Hospitality (Basic)" or "Emergency Access to Attendant" field must be enabled in the license file. You can verify if either of those license file options are on by reading the "System-Parameters Customer-Options" form.

Administer an Emergency Access to Attendant feature access code.

```
change feature-access-codes                                    Page   2 of   7
                               FEATURE ACCESS CODE (FAC)
                  Data Origination Access Code:
                      Data Privacy Access Code:
              Directed Call Pickup Access Code:
     Emergency Access to Attendant Access Code:
```

Emergency access to attendant calls have priority over other calls to the attendant only if they are assigned a higher priority on the "Console Parameters" form.

```
display console-parameters                                      Page   3 of   4
                              CONSOLE PARAMETERS

QUEUE PRIORITIES

            Emergency Access: 1
             Assistance Call: 6
                     CO Call: 6
            DID to Attendant: 6
                    Tie Call: 6
         Redirected DID Call: 6
             Redirected Call: 6
                 Return Call: 6
                 Serial Call: 6
 Individual Attendant Access: 6
             Interpositional: 6
    VIP Wakeup Reminder Call: 6
          Miscellaneous Call: 6
```

The "system-parameters features" form administers characteristics of the emergency access to attendant feature.

```
display system-parameters features                              Page   3 of  12
                        FEATURE-RELATED SYSTEM PARAMETERS
                     Reserved Slots for Attendant Priority Queue: 5
                                      Time before Off-hook Alert: 10
                          Emergency Access Redirection Extension:
            Number of Emergency Calls Allowed in Attendant Queue: 5
```

Reserved Slots for Attendant Priority Queue: The emergency access to attendant feature reserves a certain number of slots in the attendant queue for emergency access to attendant calls. Only emergency calls to the attendant can use these slots. Emergency calls to the attendant can also use other slots, if those happen to be available and an Emergency Access Redirection Extension has not been defined.

Emergency Access Redirection Extension: an extension number, which can be a VDN, where emergency calls will redirect to if the Number of Emergency Calls Allowed in Attendant Queue is exceeded and additional emergency calls arrive to the attendant.

Number of Emergency Calls Allowed in Attendant Queue: the number of calls allowed in the attendant queue before additional emergency calls are routed to the backup extension.

Assign an emergency access to attendant (em-acc-att) button on the attendant form:

```
change attendant 1                                                Page 3 of 4
                              ATTENDANT CONSOLE
FEATURE BUTTON ASSIGNMENTS
  1: split                              13: em-acc-att

```

2.2.8. Off-Hook Alert

Off-hook alert is a service that makes an emergency call to the attendant on behalf of a user who is unable to dial. You can assign a telephone the Off-Hook Alert option via the extension’s class of service (COS). If the terminal is left off-hook for 10 seconds without dialing, intercept tone plays and the administrable off-hook alerting timer starts. If the terminal is still off-hook when the timer expires, an emergency call is automatically placed to the attendant.

2.2.8.1 Administration

```
change cos
                                CLASS OF SERVICE

                                0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15
 Auto Callback                  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Call Fwd-All Calls             n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Data Privacy                   n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Priority Calling               n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Console Permissions            n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Off-hook Alert                 y  y  y  y  y  y  y  y  y  y  y  y  y  y  y  y
 Client Room                    n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Restrict Call Fwd-Off Net      n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n

```

Off-hook Alert: enables off-hook alert for a class of service.

```
add station next                                        Page   1 of   4
                                     STATION

Extension: 2000                           Lock Messages? n          BCC: 0
     Type: 6408D+                         Security Code:             TN: 18
     Port:                              Coverage Path 1:            COR: 1
     Name:                              Coverage Path 2:            COS: 1
                                        Hunt-to Station:
```

```
display system-parameters features                      Page   3 of  12
                         FEATURE-RELATED SYSTEM PARAMETERS
                      Reserved Slots for Attendant Priority Queue: 5
                                        Time before Off-hook Alert: 10
                           Emergency Access Redirection Extension:
            Number of Emergency Calls Allowed in Attendant Queue: 5
                                              Call Pickup Alerting? n
                      Temporary Bridged Appearance on Call Pickup? Y
```

Time before Off-hook Alert - The time in seconds a telephone with an Off-Hook Alert Class of Service can remain off-hook after intercept tone has started before an emergency call is sent to the attendant.

2.2.8.2 MASI Terminals

Multimedia Applications Server Interface (MASI) terminals have emergency access using the attendant access code, if it is administered in the MMCX dial plan. However, off-hook alerting is not administrable.

2.2.8.3 Callmaster™ Terminals

The use of a handset with a Callmaster terminal is optional. It is plugged into the headset jack and there is no switchhook. The set does not distinguish the difference between a headset and a handset; it functions the same way regardless of which is used. The Callmaster goes to the off hook state when a headset or handset is plugged into the headset jack. A single distinctive ring alert signal is used for each new incoming call. If an extension used by a Callmaster terminal were assigned to off-hook alert COS, the extension might inadvertently cause off-hook alert calls to the attendant.

2.3. Emergency Call Reports

Communication Manager software creates a record for each emergency call. This record includes:

- The extension that made the call

- The attendant or attendant group that answered the call
- The time of the call
- The following call results:
  - Call Completed: the call was answered at an attendant or listed directory number (LDN) night extension.
  - Queue Full: The emergency-access queue was full; the Communication Manager server tried to redirect the call to an emergency-access redirection extension.
  - No Attd: No active attendants were available to receive the call; the Communication Manager server tried to redirect the call to an emergency-access redirection extension.
  - Redirected Answered: The call was answered by the emergency-access redirection extension.
  - No Redirection Ext: The Communication Manager server could not redirect the call to the emergency-access redirection extension because none was administered.
  - Attd Night Service: The system was in night service. The Communication Manager server tried to redirect the call to attendant night service.
  - Failed: The caller dropped the call before it could be answered. The call was either waiting in the attendant emergency queue, ringing at an attendant console, or ringing at the LDN night extension.
  - Redirected Abandoned: The caller dropped the call before it could be answered. The call had been redirected to the emergency-access redirection extension.

2.3.1. List Emergency

You can monitor emergency-access calls by displaying them at the administration terminal. The command for listing emergency call events is "list emergency". You can use a "from time" and a "to time" option with the command. For example, if you enter the command "list emergency 8:00am 12:00pm", the report shows emergency call events that occurred during the interval.

```
list emergency

                        EMERGENCY ACCESS CALLS

Extension      Event                    Type of Call            Time
3104           crisis alert             ars alrt call type      11:01 A
3104           crisis pager1 fail       ars alrt call type      11:02 A
3104           crisis pager2 fail       ars alrt call type      11:03 A
3104           crisis pager3 fail       ars alrt call type      11:04 A
3104           crisis alert             feature access code     11:10 A
3104           crisis pager1 fail       ars alrt call type      11:11 A
3104           crisis pager2 fail       ars alrt call type      11:12 A
3104           crisis pager3 fail       ars alrt call type      11:13 A
3104           crisis alert             off-hook alert          11:21 A
3104           crisis alert ack’d       ars alrt call type      11:22 A
3104           crisis pager1 pass       ars alrt call type      11:23 A
3104           crisis pager2 pass       ars alrt call type      11:24 A
3104           crisis pager3 pass       ars alrt call type      11:25 A
```

Events:

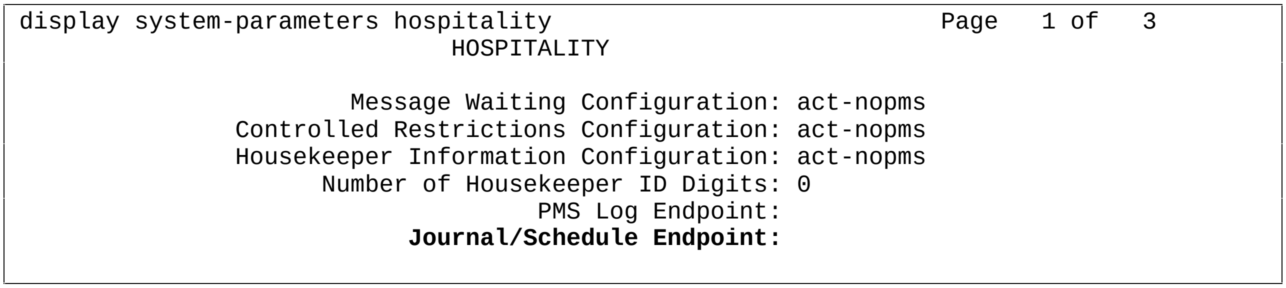
- crisis alert: a crisis alert was sent
- crisis alert ack’d: the crisis alert was acknowledged from a set with a crss-alert button
- crisis pager pass: the crisis alert was sent to a pager
- crisis pager fail: the Communication Manager server tried to send the crisis alert to a pager but the page failed

Judging from the above example form, the user at extension 3104 is having a bad day. Fortunately for him, he is fictitious.

2.3.2. Emergency Access Summary Report

You can generate an Emergency Access Summary Report of the emergency records. You can schedule the report for printing once a day at a designated printer. If the Communication Manager server has a journal printer, then Emergency Access to the Attendant audit records can print as the calls occur.

To set up the journal printer to print a record of emergency calls to the attendant as they happen, enable the printer on the hospitality form.

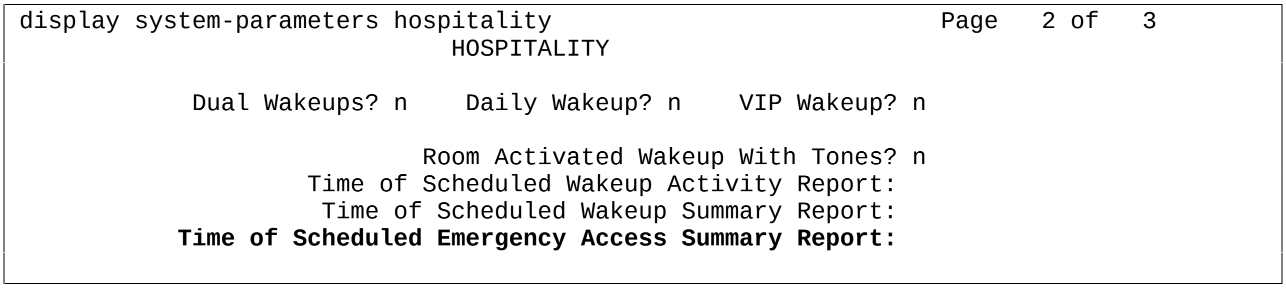


```
display system-parameters hospitality                          Page   1 of   3
                              HOSPITALITY

                       Message Waiting Configuration: act-nopms
               Controlled Restrictions Configuration: act-nopms
               Housekeeper Information Configuration: act-nopms
                     Number of Housekeeper ID Digits: 0
                                    PMS Log Endpoint:
                           Journal/Schedule Endpoint:
```

Journal/Schedule Endpoint: Enter an extension number, PMS_LOG, or PMS_JOURNAL.

- An extension number is assigned to the data module connected to the Journal/Schedule printer. The extension number cannot be a VDN extension. This extension can be the same as the PMS/Log printer and both sets of reports can be printed on the same printer. This extension is dialed by the server to send journal information or schedule reports to the printer.
- Use PMS_LOG if the printer is connected over a TCP/IP link, and this link is defined as PMS_LOG on the ip-services form.
- Use PMS_JOURNAL if the printer is connected over a TCP/IP link, and this link is defined as PMS_JOURNAL on the ip-services form.
- Leave the field blank if you do not have a journal printer.

To set up the journal printer to print a record emergency calls to the attendant at a fixed time of day, enter the time on the hospitality form.



```
display system-parameters hospitality                          Page   2 of   3
                              HOSPITALITY

            Dual Wakeups? n    Daily Wakeup? n    VIP Wakeup? n

                          Room Activated Wakeup With Tones? n
                    Time of Scheduled Wakeup Activity Report:
                     Time of Scheduled Wakeup Summary Report:
           Time of Scheduled Emergency Access Summary Report:
```

Time of Scheduled Emergency Access Summary Report: This indicates the time of day when the Emergency Access Summary Report will be printed on the Journal/Schedule printer. Enter hh:mm:am/pm where hh=hour, mm=minute, am/pm=A.M. or P.M.

2.4. Multiple Emergency Access To Attendant Codes (SA8508)

Multiple Emergency Access to Attendant Codes is a special application; it requires an additional license file entry be enabled. This feature allows you to define two unique feature access codes for the Emergency Access to the Attendant feature. By defining two emergency access codes, you can assign different meanings to each access code. For example, you could assign one access code for medical emergencies, and the other code for all other emergencies. Since each of these emergencies need special handling by the attendant, the attendant's emergency display distinguishes between the two emergency types. In addition to the attendant display changes, this feature expands the Emergency Access to the Attendant feature to allow emergency calls to be routed to another switch node using Extended Trunk Access. The priority of each access code is the same. Contact Avaya to have this special application turned on.

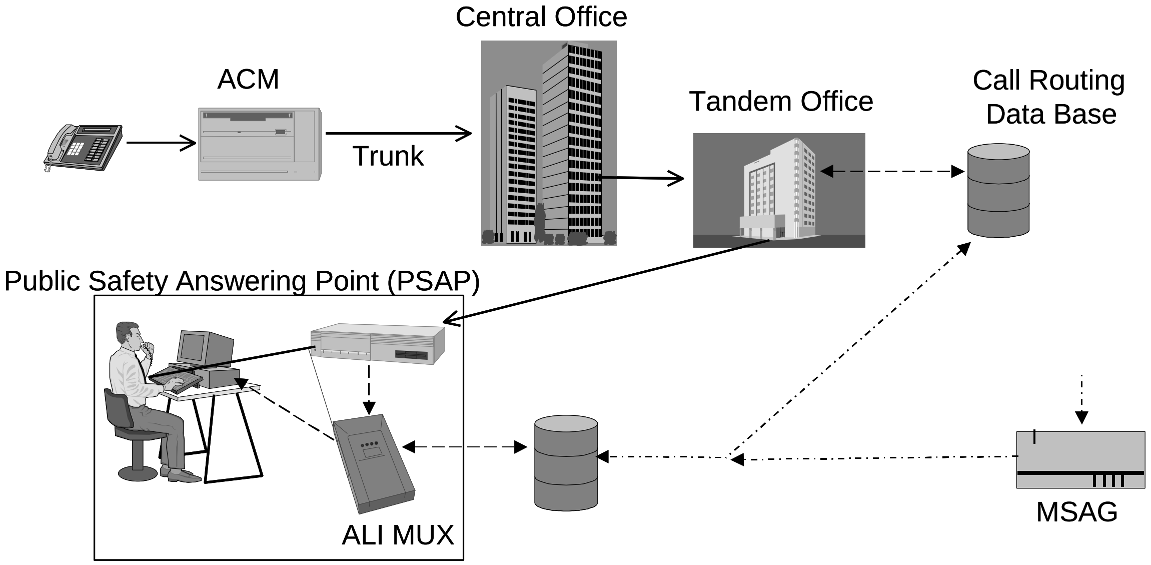
2.5. Enhanced Emergency Alert To A Station (SA7483)

Enhanced Emergency Alert to a Station is a special application; it requires an additional license file entry be enabled. The feature is an extension of Emergency priority attendant queue. If an attendant seeking emergency call redirects to a backup station, without this special feature the call just shows as an attendant redirected call. With this feature it comes to the backup station as a priority call with the word EMERGENCY on the display. Also when an Emergency access to attendant call comes in to an extension with bridged appearances and is answered at one of the bridged appearances, the other appearances will continue to ring until each of them is answered or until the call ends. Contact Avaya to have this special application turned on.

3. 911 Calling Overview

The previous section 2 starting on page 8 described emergency notifications to extensions within an enterprise. A caller needing more help than the enterprise can provide will dial a Universal Emergency Number, for example 911 in the United States[4]. The call routes through the local Central Office, through a E911 Tandem Office, to the appropriate Public Safety Answer Point (PSAP), where the call is answered.

[4] The Universal Emergency Number is 000 in Australia, and 112 in the European Community.



A typical 5ESS[5] tandem office can route the call to a PSAP within at most 4 area codes. If the PSAP receiving the call is not the correct one to handle the emergency, the PSAP may be able to transfer the call to the correct PSAP, but such transfers typically can only occur between geographically adjacent or nearby PSAPs. Each PSAP typically covers 1 city or 1 rural county. At the PSAP, emergency operators determine the nature of the emergency and contact the appropriate agency: police, fire, ambulance, etc. A single PSAP is usually responsible for an area covering several independent police and fire departments in the US.

With Enhanced 911 (E911), the voice server may send to the emergency services network the Calling Party Number (CPN) with the call over Centralized Automatic Message Accounting (CAMA) trunks or via the Calling Number IE over ISDN trunks. Once the call is terminated to the PSAP agent, the switch informs a host computer for look-up of ALI (Automatic Location Identification) information relating to the calling number. The information is then transmitted to an ALI Display Unit at the answering agent station. The ALI database is typically owned and managed by the Local Exchange Carriers but the enterprise voice server owner or operator is responsible for the updating of the ALI information for their ANI numbers. Some enterprises choose to contract with a third party to perform these updates.

The Communication Manager enterprise voice server must correctly perform two tasks to make it likely help arrives where needed:

- Route the 911 call out a trunk which will reach the correct tandem office, and so in turn the correct PSAP.
- Send a calling party number corresponding to the emergency caller's physical location.

[5] 5ESS is a trademark of Lucent Technologies, Inc.

4. ARS, Locations, And Routing To The Correct PSAP

4.1. ARS

Communication Manager software uses Automatic Route Selection (ARS) to direct outgoing public network calls such as 911 calls. ARS routing begins when a user dials the ARS feature access code (FAC) followed by the number the user wants to call. Communication Manager software analyzes the digits dialed, selects the route for the call, and routes the call over the trunks you specify in your routing tables.

The FAC for ARS is usually the digit 9 in the US. In theory, then one could administer a route for 911 calls by entering only the digit string "911" into the ARS digit analysis tables. In practice, a panicked phone user dialing 911 may forget to dial the ARS access code, so it is a good idea to administer both "911" and "11" into the digit analysis tables. Sections 2.1.4.1 on page 10 and section 4.3.2 on page 26 show examples of this.

4.2. Multiple Locations

Communication Manager software allows you to define a location number for:

- Media gateways
- R300 Remote offices
- Cabinets in DEFINITY® Server R
- IP phones and softphones according to IP network region

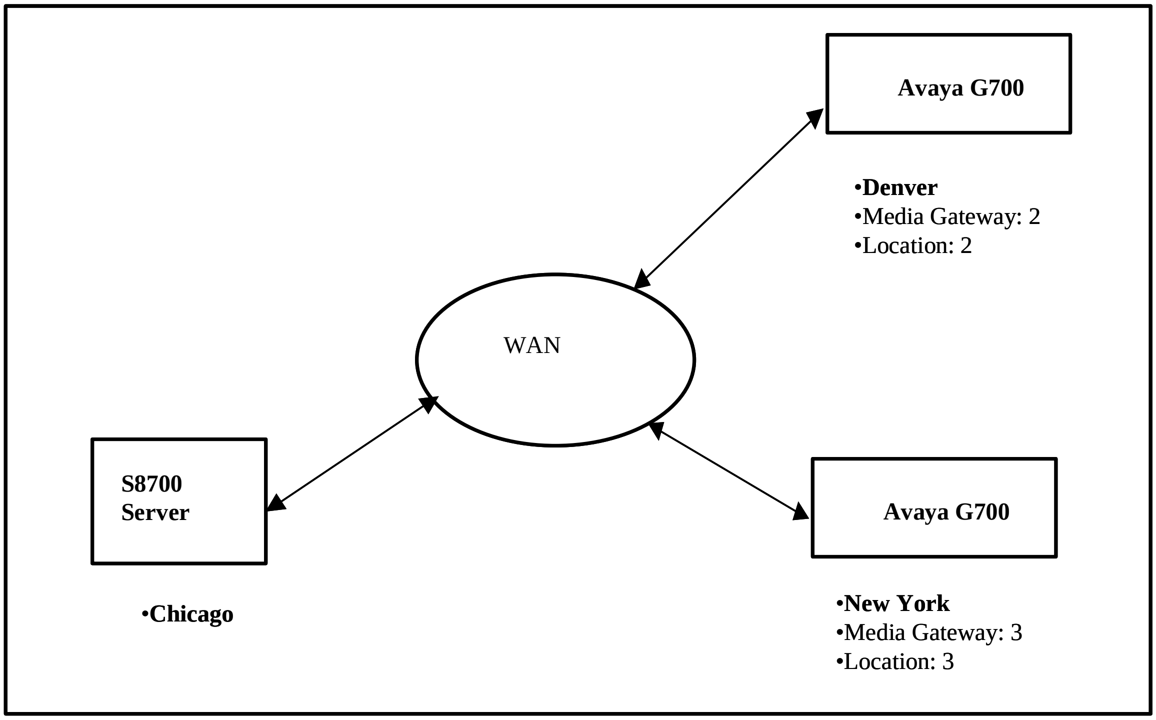
You can create routing plans, time zones and daylight savings plans specific for each of these things. For 911 calls, the item of interest is the ability to set up one routing plan for each location.

Before you start, be sure the "Multiple Locations" field on the "System-Parameters Customer-Options" form is set to y. If this field is set to n, contact your Avaya representative for more information.

When you set up multiple locations, you can define ARS call routing covering all locations as well as call routing specific to each individual location. Use your routing tables to define local routing for 911 and other local calls for each location. Leave long-distance and international numbers that apply across all locations on the routing tables with the Location field set to all.

4.3. An Example Configuration Using Media Gateways

The following diagram illustrates a plausible Communication Manager configuration with two G700 Media Gateways connected via a WAN to a central controlling S8700 server. One G700 is located in New York, New York and the other is located in Denver, Colorado. The controlling S8700 server is located in Chicago, Illinois.



Consider this sequence of events[6].

1. An individual in Denver dials 911 from a station connected to MG 2 in Denver, Colorado.
2. The digit string "911" is transmitted from MG 2 to the S8700 server located in Chicago.
3. The S8700 determines an emergency call has originated from MG 2, which is associated with Location 2.
4. ARS digit analysis of the string "911" for Location 2 indicates the call should be routed to route pattern 2.
5. Trunk Group 2 is the first, and only, preference in the list of trunk groups supported by Route Pattern 2. This trunk group is assigned to MG 2.
6. Communication Manager software sets up the call to be transmitted on a trunk interface connected to the Denver MG and terminate to the correct PSAP in Denver.

Here are sample administration forms showing this configuration.

[6] In this example sequence of events, all the media gateways, locations, trunk groups and route patterns are numbered 2. That's just to keep the example simple to follow. Communication Manager does not require you to use the same numbers for these things.

4.3.1. Media-Gateway Form

```
add media-gateway 2                                             Page 1 of 1
                                MEDIA-GATEWAY
        Number: 2
          Name: Media Gateway 2      Identifier: _____________________
    IP Address: ________________    MAC Address: _________________
Network Region: ____                   Location: 2
     Site Data: ____________________ Registered? _
```

4.3.2. ARS Analysis Form

```
change ars analysis 1                                        Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location:     2         Percent Full:    6

          Dialed           Total      Route    Call   Node  ANI
          String          Min  Max  Pattern    Type   Num   Reqd
    11                    2    2     2         emer         n
    911                   3    3     2         emer         n
```

4.3.3. Route-Pattern Form

```
change route-pattern 2                                       Page   1 of   1
                            Pattern Number: 2

   Grp. FRL NPA Pfx Hop Toll No.  Inserted                         DCS/ IXC
   No.          Mrk Lmt List Del  Digits                           QSIG
                             Dgts                                  Intw
 1:  2   0  303  1   1    1   0                                     n   user
```

The same thing happens with a call placed from a non-IP station behind an R300 Remote Office or an ATM or DS1 remoted cabinet. The locations for these things are administered on their respective forms, as shown in the following sections 4.3.4 and 4.3.5 on page 27.

4.3.4. Remote-Office Form

```
change remote-office 4                                          Page   1 of   1

                              REMOTE OFFICE  4

         Node Name: far-end
    Network Region: 4
          Location: 4
         Site Data:
```

4.3.5. Cabinet Form

```
Change cabinet                                                   page 1 of   1

CABINET DESCRIPTION
                   Cabinet: 5
            Cabinet Layout: single-carrier-stack
              Cabinet Type: expansion-portnetwork
   Number of Port networks: 2
     Survivable Remote EPN? n      Survivable Remote Processor ID: ____________
                  Location: 5
                     Room: __________  Floor: __________ Building: __________
```

4.3.6. IP Endpoints

The situation is similar for IP Telephones and IP Softphones. They can obtain their location number a little more indirectly than do Media Gateways, Remote Offices, and Cabinets. IP phones get their location number according to the following algorithm.

A. IP Phones get an IP Network Region number according to the following priority order:

1. The region number administered on the ip-network-map form which corresponds to the IP Phone’s IP address.

```
change ip-network-map                           Page   1 of   X

                   IP ADDRESS MAPPING
                                                         Emergency
                                Subnet       802.1Q      Location
FROM IP Address  (TO IP Address  or Mask) Region  VLAN   Extension
135.__9.__2.__0  135.__9.__2.255    24    __2     ___0   ________
135.__9.__3.__0  135.__9.__3.255    24    __3     ___0   ________
```

2. If the IP address of the phone does not fall into any of the IP address ranges administered on the form, then Communication Manager software uses the region number of the CLAN the phone is registering through. The CLAN gets its ip-network region number from the ip-interfaces form.

```
change ip-interfaces                                                Page 1 of 4
                                    IP INTERFACES
                                                                  Net
ON Type  Slot  Code Sfx Node Name      Subnet Mask     Gateway Address Rgn VLAN
y  C-LAN 01A08 TN799  C near-end       255.0  .0  .0      .   .   .    3   n
```

In either case, whether the phone gets its IP Network Region number from the ip-network-map or from the CLAN it registered through, the phone now has an IP Network Region number. The number can be used to assign a Location number on the ip-network-region form.

```
change ip-network-region 2                                      Page   1 of   2
                                   IP NETWORK REGION

       Region: 2                    Name: Region 2
     Location: 2
```

However, the system administrator may choose to leave the Location field on the ip-network-region form blank. If they do so, IP phones can still get a location number indirectly.

B. IP Phones can inherit their location number from the location number of the:

- cabinet containing the CLAN the endpoint registered through, or
- media gateway containing the ICC or LSP the endpoint registered through.

If you choose to use this latter method to assign locations to IP phones, an IP Phone could register with a distant CLAN and end up having its 911 calls route to a distant PSAP. You may not want that.

Now to continue the Chicago, Denver, New York example started earlier. Suppose an IP Telephone in Denver obtained IP address 135.9.2.125 from a DHCP server in Denver. According to the IP address range administered on the ip-network-map, this IP Telephone would have an IP Network Region number of 2. According to the "ip-network-region 2" form, this phone would have a location of 2. If the phone dialed 911, the call would route out a trunk on the Media Gateway in Denver, and reach a Denver PSAP.

4.4. IP Network Region And Location

One might wonder how the concepts of IP network region and location fit together. A short and accurate definition, but not a particularly useful one, is: "any way you want them to." In Communication Manager software, region and location are both administrable parameters. From the software's point of view, they are just numbers, much like a COR is just a number.

4.4.1. IP Network Region

Network region numbers are administered directly to IP circuit packs, and indirectly to IP phones via ranges of IP addresses. Network region numbers can also be assigned to IP phones via the CLAN circuit pack the phone happens to register through. Section 4.3.6 on page 27 explains this assignment in more detail.

Network region numbers control things that depend only on IP network topology: quality of service parameters, whether IP connections are allowed, etc. There need not be any correlation between IP network topology and concepts like "time zone" or "area code", but people tend to like organization; they will frequently make such a correlation anyway, just to make it easier to keep track of these numbers.

Platform	CSI	S8100	SI	S8300	S8500	R	S8700
Regions	80	80	80	50	250	250	250

4.4.1.1 Network Address Translation (NAT)

If an IP phone gets its IP Network Region number from the ip-network-map, and if the phone is behind a Network Address Translation (NAT) device, the IP network region is based on the phone's NAT translated IP address, not the native IP address.

4.4.2. Multiple Locations

Location numbers control several things that vary by state, for example time zone and ARS digit analysis and dial plan. Could one then conclude a Communication Manager location must always be within one state? No, but people tend to like organization; they will frequently make such a correlation anyway, just to make it easier to keep track of these numbers.

Location numbers are administered directly to cabinets, remote offices, and media gateways. Non-IP phones connected to these things inherit the location number of the hardware they are connected to. Location numbers are administered indirectly to IP phones, from their network regions. A location number is administered on each ip-network-region form; the number applies to all IP phones in the region. Could one then conclude a network region must always be within one location? No. An administrator could choose to leave the location field blank on the ip-network-region form; then IP phones in the region would derive their location from the cabinet holding the CLAN they are registered through. Even if all the IP phones in a network region have the same location number, the same thing is not necessarily true of the IP circuit packs in the region. However, perhaps system administrators will prefer consistency, and therefore administer Communication Manager software so IP circuit packs and IP phones in the same region are also in the same location.

Section 4.2 on page 24 contains an example of administration of multiple locations.

Platform	S8100	CSI	SI	R	S8300	S8500	S8700
Locations	1	10	10	44	50	250	250

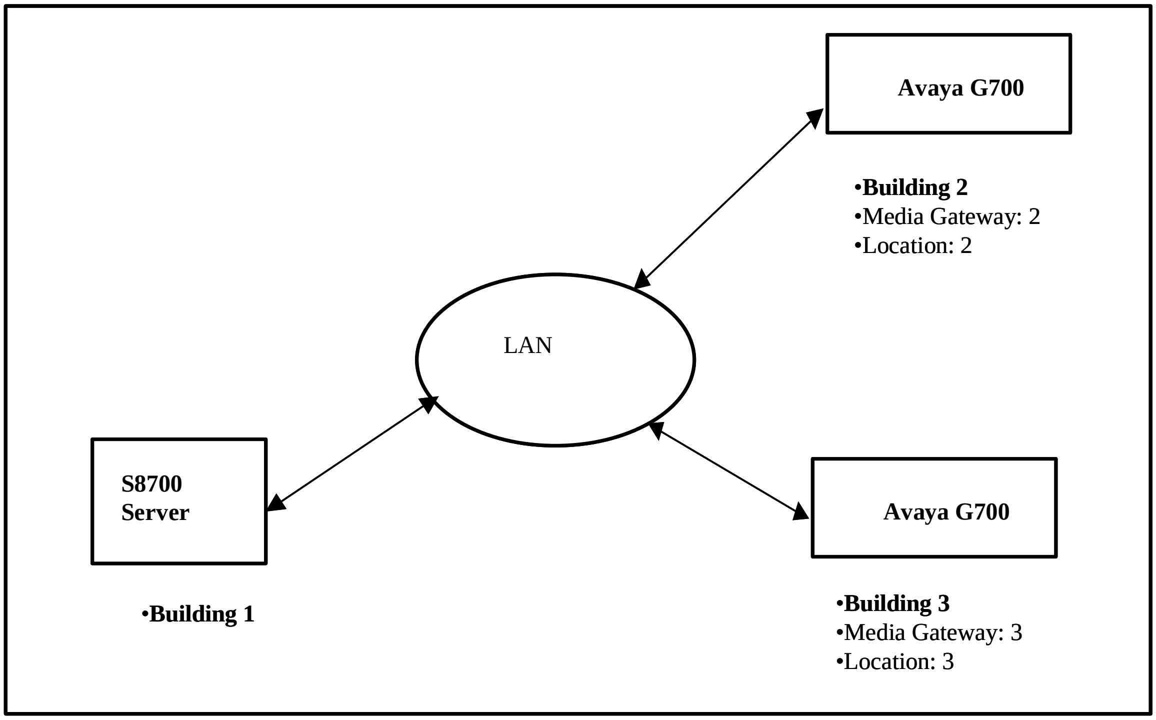
4.5. Multiple Locations And Moves Within A Campus

The example of section 4.3 on page 24 described routing a 911 call in a static situation, where the IP phone did not move. The phone need not have been stationary. The same ability to identify an IP phone's location applies whether the phone is stationary, or has been moved by a phone user. Section 5.4 on page 52 describes a feature specifically designed to track users who move phones within a campus, but the feature depends on the CO's ability to receive a calling party number. Typically, public service providers charge extra for this ability. E-911 Service charges are different for every E-911 Service Provider and generally include a one time installation cost and recurring monthly charges based on the number of ALI records in their database.

If a campus has a relatively small number of buildings compared to the number of trunks connecting the campus to the local public service provider's network, the enterprise may be able to save money by having trunks assigned different street addresses by the local service provider. Each trunk's street address will be a separate entry in the ALI database.

As phone users move their phones around a campus, the phones may change IP addresses. When an IP phone moves within the same subnet, it continues using the same IP address it had before the move. However, when an IP phone moves to a different subnet, it requests a new IP address from the DHCP server. This change in IP address is an indicator the user may have moved.

The administration required for this is exactly the same as described in section 4.3 on page 24 for cross-country networks. Just apply the example, substituting "building 1" for Chicago, "building 2" for Denver, and "building 3" for New York.



Suppose an IP Telephone in Building 2 obtained IP address 135.9.2.125 from a DHCP server. According to the IP address range administered on the ip-network-map, this IP Telephone would have an IP Network Region number of 2. According to the "IP Network Region 2" form, this phone would have a location of 2. If the phone dialed 911, the call would route out a trunk on the Media Gateway in Building 2, and the CO would determine the 911 caller has building 2's street address from the trunk number.

This method would be limited to no more buildings than the number of Location numbers provided by Communication Manager software. See section 4.7 on page 35 for Communication Manager software's location capacity.

4.5.1. Geographic Subnets

This method's ability to physically locate an IP phone from its IP address depends upon the site's data network having subnets corresponding to geographic areas. The order of the geographic areas covered by the subnets need not have any correlation to the numeric order of the IP address ranges. The geographic areas do need to avoid overlapping each other, or at least not by very much.

This requirement that subnets not overlap each other too much has been misunderstood. An enterprise may actually have geographically separate subnets, but not know they do, because of terminology.

- One enterprise had a single corporate-wide DHCP server rather than individual DHCP servers for each site, and therefore thought their IP addresses could not be geographically oriented by site. However their servers actually assigned IP addresses as follows:
    1) An end point broadcasts, looking for a DHCP server.
    2) The local data switch picks up the broadcast. The data switch does not forward it, but instead changes it into a unicast aimed at a single corporate-wide DHCP server. It also inserts into the request a data switch identification number.
    3) The DHCP server responds to the endpoint with an IP Address supported by the local data switch. Those IP Addresses are arranged by geographically oriented subnets.

- One enterprise had VLANs with no geographic significance, and assumed their subnets also had no geographic significance. They called subnets with a single VLAN "subnets" but called multiple subnets under a single VLAN "secondary subnets". Their "secondary subnets" were geographically correlated. Communication Manager software would not have cared about this terminology difference; the features that determine IP endpoint's locations from their IP addresses would still have worked.

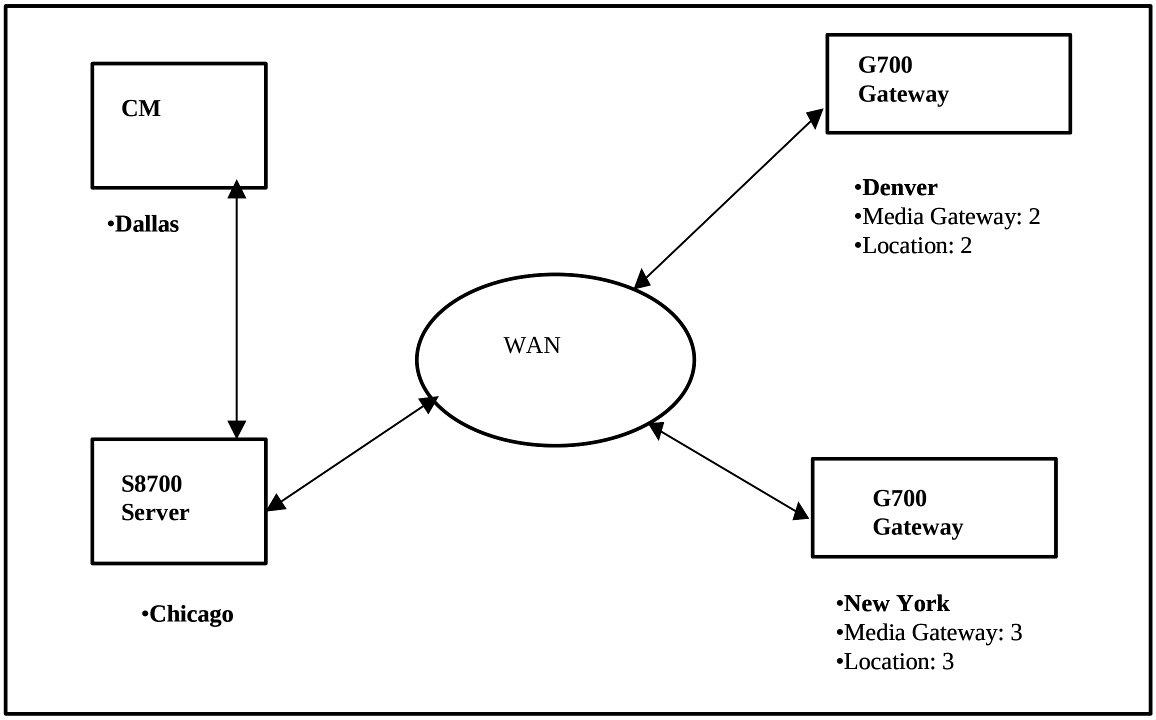
4.6. If There Is No Nearby Trunk

The example of section 4.3 on page 24, showed routing the 911 call of a caller who is in Denver out a trunk on the G700 Media Gateway in Denver. However, what would happen if the server had no PSTN trunk in the same metropolitan area or even in the same state as the 911 caller? This is not very likely, but could happen if the caller is connecting a phone into the server remotely. That is more likely with an IP Softphone on a laptop PC than with an IP Telephone, but could happen with either one. There are two sub-cases of this. They are described in the following subsections.

- there is a PSTN trunk near the caller, or
- there is no PSTN trunk anywhere near the caller.

4.6.1. Multiple Servers

In the first case: there is a PSTN trunk near the caller. To continue the previous Chicago, Denver, New York example, suppose you have a private network. One server and its gateways cover those three cities. A completely separate server is in Dallas, Tx. Tie trunks connect the two servers.



4.6.1.1 A Distributed Server And A Single Site Voice Server

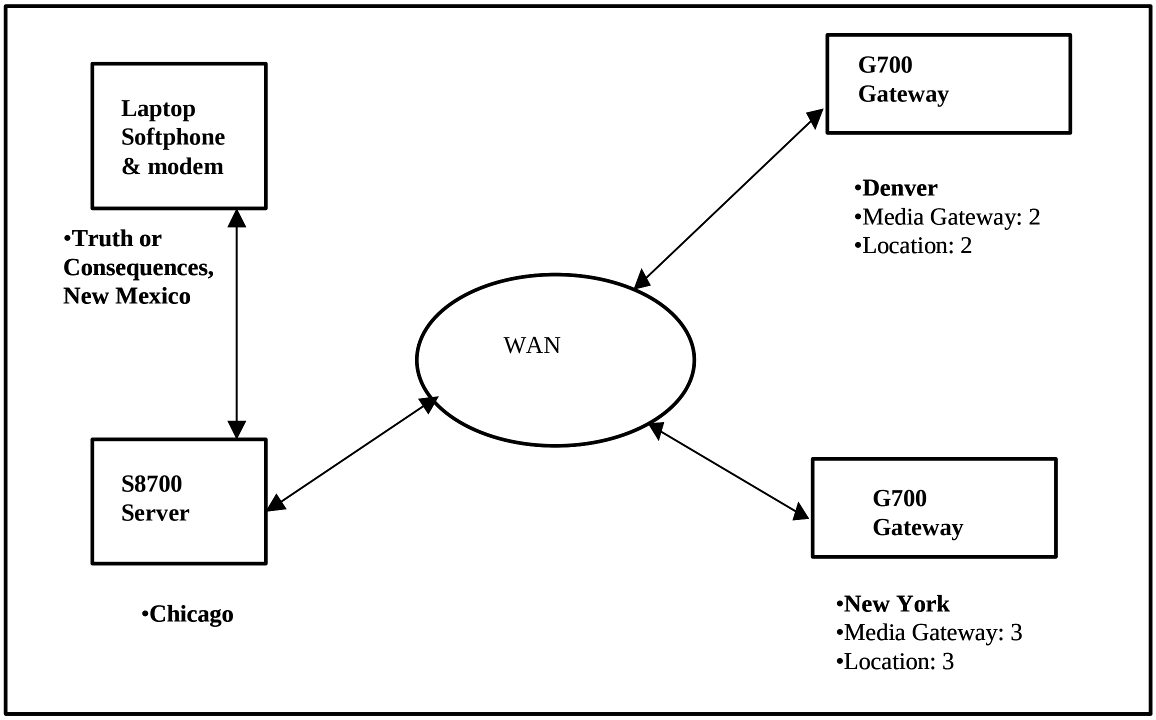
Suppose a user with a Chicago extension flies to Dallas, and connects an IP Softphone on a laptop back to the Chicago server. Suppose the user then dials 911 from the IP Softphone. The Chicago server would need to have the Dallas IP Address range pre-administered into the Chicago server's ip-network map, with a corresponding IP Network Region, and a corresponding Location. The Location would have corresponding ARS digit analysis tables that would route the 911 via the tie trunk connecting Chicago to Dallas. The Dallas server, receiving the incoming tie trunk call to 911, would route the call out one of its PSTN trunks, to the local Dallas PSAP.

4.6.1.2 Multiple Distributed Servers

Now, what happens if the Dallas voice server is not just providing service to Dallas, but is itself a distributed server, with its own gateways scattered throughout the South central USA? The Chicago voice server can route the 911 call to the Dallas voice server, but there is not an easy way for the Chicago voice server to let the Dallas voice server know how to route the incoming 911 tie trunk call to the correct Dallas gateway close to the calling party's physical location. It could be done by assigning a one-to-one correlation between tie trunks and gateways, but the administration could be complex.

4.6.2. Connection Via A Modem

Now for the second case, where there is no PSTN trunk anywhere near the caller. For example, suppose that instead of connecting back to Chicago via the corporate network from a city that at least has a Communication Manager server, you make it harder. Suppose you dial back to Chicago via modem, from Truth or Consequences, New Mexico.



Suppose the corporate WAN does not directly connect to Truth or Consequences, New Mexico, and the enterprise does not have a server or gateway anywhere near there. In the USA , PSAPs very far away from each other currently have no good way to contact each other. Even if you are able to speak, and you explain to a PSAP in one part of the country that you need help in another part of the country, the 911 staff you are talking to have no fast way to relay what you say to a PSAP near where you are located. This is a known limitation in the current USA 911 system. If you describe your location as out of state, you are likely to be told verbally to hang up and find a local phone. Communication Manager software can save you valuable time by letting a distant caller know this as soon as 911 is dialed, instead of the caller waiting for the PSAP officer to understand the situation and give the same instructions.

If the phone user places a call with ARS call type "emer" or "alert", and if

- the "Remote Softphone emergency calls" field on the station form is set to "block" or,

- the "Remote Softphone emergency calls" field on the station form is set to "option" and the IP softphone user has selected "no" to the option "Enable Emergency Call Handling Feature":

```
change station 1001                                          Page   2 of   4
                                     STATION
FEATURE OPTIONS

 Remote Softphone Emergency Calls: option   Direct IP-IP Audio Connections?
 Emergency Location Ext: 1000                          IP Audio Hairpinning? n

```

the switch will play intercept tone to the calling set, and send to the IP softphone a message indicating the call is an emergency call. The IP softphone will react to this message by dropping the call and showing a text message instructing the caller to use a nearby fixed station instead of a remote IP station for emergency calls. The "Remote Softphone emergency calls" field has other uses besides this block use. Section 5.6 on page 77 will talk about those other uses.

IP Softphone can advise the end user to save time by dialing from another phone, because it has access to a PC screen with which to pop up a warning window. What if the user is accessing the Chicago server from Truth or Consequences, New Mexico, using a modem connected to an IP Telephone? That is unlikely; more people on a trip would prefer to carry a laptop PC with them than carry a desktop telephone set. However, if it does happen, and if the Chicago administrator knows in advance some people may do this, the administrator can reserve some inbound modem ports for calls from those out of state areas. Those modem ports would be administered within an IP Address range, with corresponding IP Network regions, and a corresponding Location. That location would have corresponding ARS digit analysis tables to route the 911 call to a recorded announcement instructing the user to use a nearby fixed station instead of a remote IP station for emergency calls. Phone users would need to be trained to dial into those modem ports when connecting an IP telephone from remote areas.

4.7. Capacity

The maximum location numbers supported by a Communication Manager server limit the techniques described in these sections. Communication Manager servers supports these numbers of locations:

Server	**Number of locations**
S8700	250
S8500	250
S8300	50
R	44
CSI, SI	10, and those are only usable by IP phones, not Media Gateways, remote cabinets, nor R300s.
S8100, D1, IP600	1

4.7.1. Capacities And Routing For Large Systems

The previous section 4.7 on page 35 describes capacity limits on locations if phone users move their own phones. If phone users do not move their own phones very far, Communication Manager software provides a method for routing calls to the correct PSAP for more than 250 different physical locations. The method works as follows.

1. Ensure ARS/AAR Partitioning? is turned on in the license file, and Time of Day Routing? is turned off in the license file. Also be sure Multiple Locations is turned on in the license file, but that is assumed throughout all of this section 4.

```
display system-parameters customer-options                    Page   2 of  10
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? y
                                                      Authorization Codes? y
        Analog Trunk Incoming Call ID? y                      CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                        CAS Main? n
Answer Supervision by Call Classifier? y                Change COR by FAC? n
                                  ARS? y Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y  Cvg Of Calls Redirected Off-net? Y

```

```
display system-parameters customer-options                    Page   4 of  10
                                OPTIONAL FEATURES

                                                         Tenant Partitioning? n
                                                 Terminal Trans. Init. (TTI)? y
           Processor and System MSP? y                   Time of Day Routing? N

```

2. For each extension, administer a Class of Restriction (COR) number on the COR form.

```
change station 1001                                            Page   1 of   4
                                     STATION

Extension: 1001                          Lock Messages? n          BCC: 0
     Type: 8410D                         Security Code:             TN: 1
     Port: 01A0301                     Coverage Path 1:            COR: 1
     Name: Digital a0301               Coverage Path 2:            COS: 1
                                       Hunt-to Station:
```

3. For each COR, administer a Partition Group Number.

```
change cor 1                                                Page   1 of   4
                              CLASS OF RESTRICTION

               COR Number: 1
          COR Description:

                      FRL: 0                                APLT? y
  Can Be Service Observed? n          Calling Party Restriction: outward
Can Be A Service Observer? n           Called Party Restriction: none
 Partitioned Group Number: 1       Forced Entry of Account Codes? N
```

4. Administer location numbers as described in section 4.3 on page 24, but feel free to assign the same location number to stations and media gateways even if those stations or gateways' 911 calls need to route to up to 8 different PSAPs per location number.

5. Administer ARS analysis for each location number, as described in section 4.3.2 on page 26, but when filling out the route-pattern column, put entries of the form p1, p2, p3, etc instead of 1, 2, 3. This format of route pattern entry is not a route pattern in itself, but rather a pointer to rows in the partition-route-table form.

```
change ars analysis 1                                       Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location:     2         Percent Full:    6

          Dialed           Total      Route    Call   Node  ANI
          String          Min  Max   Pattern   Type   Num   Reqd
    11                    2    2      p20      emer         n
    911                   3    3      p20      emer         n
                                                            n
```

Administer the partition-route-table. This form correlates the Partitioned Group Numbers with actual route patterns.

```
change partition-route-table 20                             Page   1 of   1
                            PARTITION ROUTING TABLE

                               Route patterns
    Route
    Index    PGN 1  PGN 2  PGN 3  PGN 4  PGN 5  PGN 6  PGN 7  PGN 8
    -----    -----  -----  -----  -----  -----  -----  -----  -----
    20       21     22     23     24     25     26     27     28
    21
```

In this example, if station 1001 were to dial 911, the COR would be 1, the partition group number (PGN) would be 1, the index into the partition route table would be 20, and the resulting route pattern would be 21.

This method effectively increases the number of different ways to route 911 calls per location number by a factor of 8. However, the PGN routing depends on the calling station's COR, which depends on the station's extension number. Because extension numbers do not change when users move their phones, this method can only be used when users do not move their phones further than the geographic area covered by one Communication Manager location number.

5. Sending The Correct CPN

As described in the beginning of section 3 on page 22, there are two steps for a 911 caller to receive help.

1. The call must reach a PSAP serving the caller's area.
2. The call must provide a CPN corresponding to the caller's physical location or street address.

The previous section 4 beginning on page 24 described Communication Manager software's method for achieving the first of these goals. This section 5 describes Communication Manager software's method for achieving the second of these goals.

5.1. USA Trunks Used For Emergency Calls To The PSTN

Communication Manager software uses PSTN trunks to send to the PSAP the calling party number information identifying the telephone number for an extension from which 911 was dialed. If the extension number is not public, Communication Manager software can be programmed to send another public number located nearby the calling extension. There are three ways in which this information can be delivered to the public emergency services network. It can be encoded:

- Over digital ISDN (Integrated Services Digital Network) trunks.
- Over analog CAMA (Centralized Automatic Message Accounting) trunks.
- When appropriate, as a location's main telephone number associated at the CO with ordinary analog Central Office trunks.

For non-emergency calls, Communication Manager software can use either administration or feature access codes to control whether the calling party number is sent over an outgoing ISDN trunk. However, for emergency calls, those do not matter. For emergency calls, the CPN is always sent. This is true for both public and private ISDN trunks. This is true if the calling party is a station or an incoming trunk capable of providing a CPN.

5.1.1. Public ISDN Trunks

Communication Manager software considers public ISDN trunks to be those for which the "Numbering Format" field on the "ISDN Trunk Group" form is set to public or unknown. Communication Manager software expects these trunks to be connected to a central office.

```
display trunk-group 1004                                        Page   1 of  22
                                TRUNK GROUP

Group Number: 1004                 Group Type: isdn          CDR Reports: y
  Group Name: CAPACTIY PRI TRK            COR: 1        TN: 1        TAC: 4004
   Direction: two-way       Outgoing Display? n         Carrier Medium: PRI/BRI
 Dial Access? y               Busy Threshold: 255       Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n            TestCall ITC: rest
                         Far End Test Line No:
TestCall BCC: 4
TRUNK PARAMETERS
         Codeset to Send Display: 6     Codeset to Send National IEs: 6
        Max Message Size to Send: 260   Charge Advice: none
  Supplementary Service Protocol: a     Digit Handling (in/out): enbloc/enbloc

            Trunk Hunt: cyclical                    QSIG Value-Added? n
                                                  Digital Loss Group: 13
Calling Number - Delete:     Insert:                Numbering Format: public
              Bit Rate: 1200        Synchronization: async    Duplex: full
 Disconnect Supervision - In? y  Out? n
 Answer Supervision Timeout: 0
```

5.1.1.1 ISDN Numbering — Public/ Unknown

This form supports the ISDN Call Identification feature. The form allows you to specify how Communication Manager software will convert an extension number into the Calling Number IE format required by the CO, for an ISDN call to the public network. The form can also be used to instruct Communication Manager software to send the CPN of a nearby extension if the calling extension is not a public telephone number.

If the table is not properly administered, the wrong CPN would be sent. If the table is not administered, the CPN information element would be sent with "NULL" for the associated digits. If a"NULL" CPN is sent, the local service provider may substitute a "general" number for the call. In fact, the local service provider may overwrite a CPN if they have the configuration at the CO set that way.

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

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

 5  12345 1234567 123456789012345 12       5  12345         123456789012345 12
 _  _____ _______ _______________ __       _  _____ _______ _______________ __
```

Ext Len: Specifies the number of digits the extension can have; it corresponds to the extension lengths allowed by the dial plan.

Ext Code: Allows for groups of extensions to be administered. The Ext Code can be up to 7-digits long depending on the "Ext Len" field entry. The entry cannot be greater than the "Ext Len" field entry. For example, in the case of a 4-digit "Ext Len" field entry, an "Ext Code" field entry of 12 is the equivalent of all extensions of the form 12xx, excluding any explicitly listed longer codes. If a code of 123 is also listed, the 12 code is equivalent of all extensions of the form 12xx except extensions of the form 123x. The coding precludes having to list all the applicable 12xx extensions. Attd is used for the attendant. When 0 alone is entered, the "Ext Len" field must be 1 and the DDD number must be 10-digits.

Trk Grp(s): Specifies the trunk group numbers that the CPN entries apply to. If the field is left blank, the CPN entries apply no matter which trunk group the call is carried over. If all of these fields have an entry, and someone dials 911 from a trunk group not listed here, a blank CPN would be sent.

CPN Prefix: Use this field to specify the number to be added to the beginning of the extension to form a Calling or Connected Number.

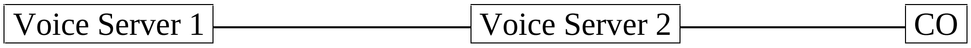
- If the length of the CPN Prefix matches the Total CPN Length, the extension number is not used to formulate the CPN number.
- If the number of digits in the CPN Prefix plus the extension length exceeds the administered Total CPN Length, excess leading digits of the extension are deleted when formulating the CPN number.
- If the number of CPN Prefix digits plus the extension length is less than the Total CPN Length, the entry is not allowed.
- If the Total CPN Length is 0, no calling party number information is provided to the called party and no connected party number information is provided to the calling party.
- If this field is blank, the extension is sent unchanged. This is useful if the public network is able to insert the appropriate CPN Prefix to form an external DID number.

Total CPN Len: the total number of digits to send.

5.1.1.2 ISDN Private Network Tie Trunks

Communication Manager software considers private ISDN trunks to be those for which the "Numbering Format" field on the "ISDN Trunk Group" form is set to private or unk-pvt. Communication Manager software expects these trunks to be connected to another voice server.

Suppose you have this network:



The trunk between voice server 1 and voice server 2 would be carrying emergency calls, even though it is a private network trunk.

- The "isdn tandem-calling-party-number" form must be filled out.
- Trunk group forms for ISDN trunks need to have:
  - the "Modify Tandem Calling Number?" field administered to Y.
  - The Incoming Calling Number fields: "Delete", "Insert", and "Format" administered.

Voice server 2's public-unknown-numbering fields do not need to contain entries for extensions on voice server 1; the public-unknown-numbering fields are not used for CPN conversion on tandem calls.

5.1.1.2.1 Trunk-Group

```
change trunk-group 1                                            Page   2 of  10
TRUNK FEATURES
          ACA Assignment? n            Measured: none      Wideband Support? n
                                 Internal Alert? n       Maintenance Tests? y
                               Data Restriction? n     NCA-TSC Trunk Member: 1
                                      Send Name: y      Send Calling Number: y
            Used for DCS? n             Hop Dgt? n
   Suppress # Outpulsing? n    Numbering Format: private
 Outgoing Channel ID Encoding: preferred     UUI IE Treatment: service-provider
       Charge Conversion: 1
           Decimal Point: none                  Replace Restricted Numbers? n
         Currency Symbol:                      Replace Unavailable Numbers? n
             Charge Type: units                      Send Connected Number: y
                                              Modify Tandem Calling Number? y
             Send UUI IE? y
               Send UCID? n
 Send Codeset 6/7 LAI IE? y                         Ds1 Echo Cancellation? n

 Path Replacement with Retention? n
 Path Replacement Method: better-route
                     SBS? n  Network (Japan) Needs Connect Before Disconnect? n
```

Modify Tandem Calling Number: Use this field to determine whether the calling party number IE received by an incoming trunk of a tandem call will be modified according to the format specified on the 'isdn numbering – tandem calling party number" form before being sent on an outgoing ISDN trunk. This applies if the incoming ISDN trunk is either QSIG or DCS over ISDN.

Send Calling Number: this field does not matter for 911 calls. The calling number is always sent for ISDN calls with ARS call type emer or alrt.

```
change trunk-group 1                                          Page   1 of  10
                                TRUNK GROUP

Group Number: 1                   Group Type: isdn          CDR Reports: y
  Group Name: QSIG loopback 2 c18         COR: 1        TN: 1        TAC: 101
   Direction: two-way       Outgoing Display? y         Carrier Medium: PRI/BRI
 Dial Access? n               Busy Threshold: 1         Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n           TestCall ITC: rest
                         Far End Test Line No:
TestCall BCC: 4
TRUNK PARAMETERS
         Codeset to Send Display: 6     Codeset to Send National IEs: 6
        Max Message Size to Send: 260   Charge Advice: none
  Supplementary Service Protocol: b     Digit Handling (in/out): enbloc/enbloc

            Trunk Hunt: cyclical
                                                   Digital Loss Group: 13
         Calling Number - Delete:___ Insert: _______________  Format: ________
              Bit Rate: 1200         Synchronization: async    Duplex: full
 Disconnect Supervision - In? y  Out? n
 Answer Supervision Timeout: 0
```

Calling Number - Delete: the number of digits, if any, to delete from the calling party number for all incoming calls on this trunk group.

Calling Number - Insert: the specific digits, if any, to add to the beginning of the digit string of incoming calls when the calling party is a member of this trunk group.

Calling Number - Format: This field indicates the Type of numbering (TON) and Numbering Plan Identifier (NPI) encoding applied to CPN information on the tandem call. This encoding does not apply to calls originating locally. If this field is blank, Communication Manager software passes on the encoding received in the incoming setup message. If the incoming setup message did not contain CPN information and digits are added, the outgoing message will contain these digits. If the "Numbering Format" field is blank in this case, the value defaults to pub-unk. If the "Numbering Format" field on page 2 of the trunk-group form is also administered as unknown, the trunk group is modified to “unk-unk” encoding of the TON/NPI. Therefore, this field also must contain a value other than unknown.

Valid entries	Type of numbering (TON)	Numbering plan identifier (NPI)
blank	incoming TON unmodified	incoming NPI unmodified
natl-pub	national(2)	E.164(1)
intl-pub	international(1)	E.164(1)
locl-pub	local/subscriber(4)	E.164(1)
pub-unk	unknown(0)	E.164(1)
lev0-pvt	local(4)	Private Numbering Plan - PNP(9)
lev1-pvt	Regional Level 1(2)	Private Numbering Plan - PNP(9)
lev2-pvt	Regional Level 2(1)	Private Numbering Plan - PNP(9)
unk-unk	unknown(0)	unknown(0)

5.1.1.2.2 ISDN Tandem-Calling-Party-Number

```
change isdn tandem-calling-party-number                       Page   1 of   8
                 ISDN NUMBERING - CALLING PARTY NUMBER CONVERSION
                                FOR TANDEM CALLS

         CPN              Trk                                        Number
   Len   Prefix           Grp(s)   Delete    Insert              Format

    5    22               12-99    1         732852              natl-pub
    7    5381234          2        0         303                 lev0-pvt
    __   _______________  _____    __        _______________     ________
```

Len: Specifies the length of the incoming CPN.

CPN Prefix: Digits which match the beginning of the incoming CPN.

Trk Grp(s): Incoming trunk groups expected to provide a CPN. These are an administered ISDN trunk-group number or a range of group numbers. For example, if trunk groups 10 through 24 use the same CPN Prefix, enter 10-24. A blank trunk group entry on the form means all trunk groups are valid provided the “Modify Tandem Calling Party” on the trunk group form is “y”.

Delete: the number of digits to delete from the beginning of the outgoing CPN

Insert: Digits to insert at the beginning of the outgoing CPN. To generate a calling party number for the outgoing trunk, the incoming calling party number is compared to the sets of calling party lengths, calling party prefixes and trunk groups administered on this form. When a match is found, the calling party number is constructed by deleting the initial, most significant digits identified on the form and then inserting the “Insert” digits from the form.

Number Format: The numbering format specified on the new form will be used to determine the encoding of the NPI and TON fields for the calling party number. The following table summarized the encoding based on the numbering format specified.

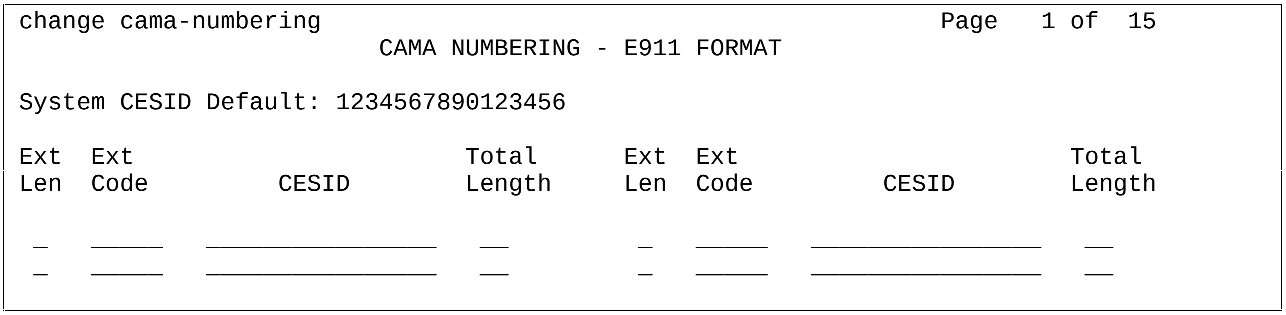
Valid entries	Type of numbering (TON)	Numbering plan identifier (NPI)
natl-pub	national(2)	E.164(1)
intl-pub i	nternational(1)	E.164(1)
locl-pub	local/subscriber(4)	E.164(1)
pub-unk	unknown(0)	E.164(1)
lev0-pvt	local(4)	Private Numbering Plan - PNP(9)
lev1-pvt	Regional Level 1(2)	Private Numbering Plan - PNP(9)
lev2-pvt	Regional Level 2(1)	Private Numbering Plan - PNP(9)
unk-unk	unknown(0)	unknown(0)

5.1.2. CAMA Trunks

CAMA trunks, like ISDN trunks, send the calling party's number to the CO. When sent over CAMA trunks, the calling party's number is called the Caller's Emergency Service Identification (CESID).

5.1.2.1 CAMA Numbering Format

This form administers Centralized Automatic Message Accounting (CAMA) trunk numbering. The trunk provides Caller's Emergency Service Identification (CESID) information to the local community's Enhanced 911 system through the local tandem office. This form provides the CESID format by extension number or number blocks. This allows for multiple CESID formats to be sent over multiple CAMA trunk groups allowing for mixed station numbering plans and some limited conversion from non-DID to DID numbers typically required by the Private Switch/Automatic Location Interface (PS/ALI) database. The default CESID defines the CESID for all extensions not defined in the "Ext Code" field. There are 446 CESID entries.



```
change cama-numbering                                             Page   1 of  15
                          CAMA NUMBERING - E911 FORMAT

System CESID Default: 1234567890123456

Ext  Ext                          Total      Ext  Ext                         Total
Len  Code         CESID           Length     Len  Code         CESID          Length

 _   _____   ________________   __           _   _____   ________________   __
 _   _____   ________________   __           _   _____   ________________   __
```

System CESID Default: This number will be sent over the CAMA trunk if the "Ext Code" field does not have an entry.

Ext Len: the number of digits in the extension.

Ext Code: the leading digits or all of the digits in the extension for the specified CESID. If the extension length is greater than the number of digits in the extension code, the extension code will be interpreted as a block of digits. For example, if the extension length is 4 and the extension code is 11, the CESID will serve extensions 1100 through 1199. The Ext Code 11 is for a DID block. An Ext Code of 126 might point a non-DID block to a nearby DID extension 5241666.

CESID: the number will be used to identify the calling terminal within an emergency service system. This field may represent a prefix to an extension or the entire CESID.

Total Length: the total number of digits to send. Unlike the public/unknown tables explained in section 5.1.1.1 on page 39, you can not set this value equal to the extension length in order to substitute the initial extension digits. For example, if all you extensions are of the form 3xxxx, i.e., they start with the digit 3, but your DID range is of the form 8xxxx, i.e., they start with the digit 8, you can't use the cama-numbering form to do that conversion. Attempting to do so results in the error message: “Total length must equal [# CESID digits] or [# CESID digits + extension length]”.

5.2. Users Moving Non-IP Phones Or Extension Numbers

There are several features in Communication Manager software that allow phone users to move their own non-IP phones or move an extension number from one phone to another.

- Terminal Translation Initialization(TTI). Communication Manager software provides Terminal Translation Initialization (TTI). It works with Administration Without Hardware (AWOH). TTI associates the terminal translation data with a specific port location through the entry of a special feature-access code, a TTI security code, and an extension number from a terminal connected to a wired but untranslated jack.

- Customer Telephone Activation (CTA) enables you to install your own phones, eliminating the need for a service technician to do the installation. This feature is based on the TTI feature and allows you to associate a physical phone with an extension. CTA is a streamlined version of TTI; it has a fixed feature-access code but does not require a security code. In addition, CTA allows only for “merging” of phones with station translations, whereas TTI allows for both “merging” and “unmerging” of phones with station translations. CTA applies only to DCP and analog touch-tone, circuit-switched phones.

- Personal Station Access (PSA).   This feature allows you to transfer your telephone station preferences and permissions to any other compatible telephone. This includes the definition of telephone buttons, abbreviated dial lists, and class of service, and class of restrictions permissions. It can be used on-site or off-site. PSA has several telecommuting applications. For example, several telecommuting employees can share the same office on different days of the week. The employees can easily and remotely make the shared telephone “theirs” for the day. Remote use of PSA with DCP sets requires DEFINITY ® Extender. Avaya is no longer selling the DEFINITY Extender.

    - Automatic Customer Telephone Rearrangement (ACTR). Automatic Customer Telephone Rearrangement (ACTR) allows a phone to be unplugged from one location and moved to a different location without additional switch administration. The switch automatically associates the extension to the new port. ACTR works with the 2420 DCP telephone and the 6400 serialized telephones, and newer DCP telephones. The 6400 serialized phone is stamped with the word “serialized” on the faceplate for easy identification. The 6400 serialized phone memory electronically stores its own part ID (comcode) and serial number. ACTR uses the stored information and associates the phone with a new port when the phone is moved. ACTR makes it easy to move phones.

As mentioned in section 2.2.7 on page 16, if the attendant queue is full, emergency calls to the attendant will ring at the extension number administered in the "Emergency Access Redirection Extension" field on the "Feature-Related System Parameters" form. An Emergency Access Redirection Extension can be separated from its port only through administration. If a phone user were to unplug the set whose extension number is administered as the Emergency Access Redirection Extension, and plug in a serialized DCP set with ACTR move permissions into the port, the switch will refuse to recognize the swap; the serialized station set will have the extension number associated with the port the set was plugged into, as long as it is plugged into the port. If CTA/PSA/TTI Transactions in History Log is turned on, the history log shows this event as an ACTR denial with reason EMERGENCY EXT, as shown in section 5.3.4 on page 49.

5.2.1. Planned Non-IP Phone Moves

The above features can only be used if the administrator grants permission, as described in the Communication Manager Administrator's Guide; refer to item 96 on page 96. Typically, permission to use these features is only turned on by an administrator when the administrator has arranged for the move in advance. The administrator will update the ALI database accordingly once the move is completed, and turn off permission to use the features.

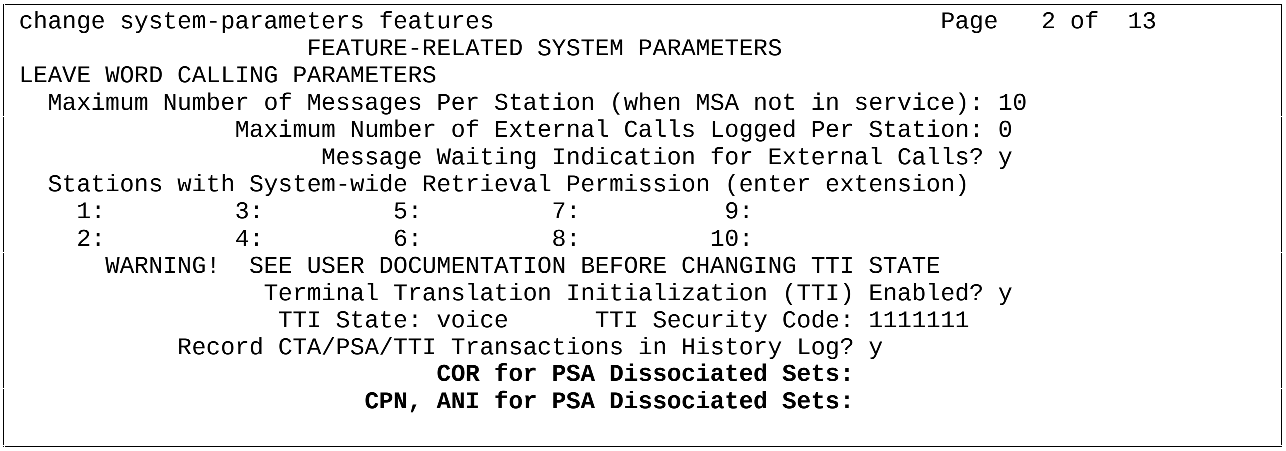
5.2.2. Unplanned Non-IP Phone Moves

An administrator could grant unlimited use of the above features, to allow some phone users with non-IP phones to move them whenever or where ever they wish. Communication Manager software can be administered as described in section 4.5 on page 30 to ensure the PSAP would receive the correct building's street address if such users dialed 911 after moving an extension or non-IP phone. As mentioned in that section, this method can only identify users in the same number of physical locations as the number of trunks the enterprise has obtained from the public service provider.

5.2.3. Dissociated Sets

If someone does have permission and uses one of these features to move an extension number from one port to another, the port the extension number moved from has no extension number. A non-IP phone plugged into such a port is called dissociated. By default only the attendant can be called from such a dissociated phone.

You can allow users to place 911 emergency and other calls from non-IP dissociated phones. To enable this, you must first assign a class of restriction (COR) for PSA-dissociated phones. You do this on the "COR for PSA Dissociated Sets" field on the "system-parameters features" form. In addition, you must give calling permissions for this COR on the "Class of Restriction" form. If you want users to be able to place emergency calls from dissociated phones, it is also a good idea to have the system send a calling party number for these calls. To do this, you must set the "CPN, ANI for PSA Dissociated Sets" field to y on the "system-parameters features" form.



```
change system-parameters features                               Page   2 of  13
                    FEATURE-RELATED SYSTEM PARAMETERS
LEAVE WORD CALLING PARAMETERS
  Maximum Number of Messages Per Station (when MSA not in service): 10
               Maximum Number of External Calls Logged Per Station: 0
                     Message Waiting Indication for External Calls? y
  Stations with System-wide Retrieval Permission (enter extension)
    1:         3:         5:         7:           9:
    2:         4:         6:         8:         10:
      WARNING!  SEE USER DOCUMENTATION BEFORE CHANGING TTI STATE
                 Terminal Translation Initialization (TTI) Enabled? y
                  TTI State: voice      TTI Security Code: 1111111
           Record CTA/PSA/TTI Transactions in History Log? y
                             COR for PSA Dissociated Sets:
                        CPN, ANI for PSA Dissociated Sets:
```

5.3. Manually Tracking Moves

As mentioned at the beginning of section 3 on page 22, many enterprises choose to contract with a third party to update the ALI database for them. Some enterprises purchase ALI database updating products and pay an employee to make the changes. In any case making changes to the ALI database does incur some cost. As mentioned in section 4.5 on page 30, typically, public service providers charge extra for the CO's ability to receive a calling party number during a 911 call. Communication Manager software provides features to reduce these costs. There are two methods an administrator could use to instruct Communication Manager software to change the CPN Communication Manager software sends during 911 calls, instead of using the phones' extension number:

- Use the "public-unknown-numbering" and "cama-numbering" forms. The following section 5.3.1 on page 47 describes this method.
- Use the "Emergency Location Extension" field on station form. The following section 5.3.2 on page 48 describes this method.

5.3.1. ISDN Numbering And CAMA Numbering

The first manual method, mentioned in section 5.1 on page 38, is to use the "public-unknown-numbering" and "cama-numbering" forms. Those forms control how Communication Manager software converts an extension number into the format the public network expects for a CPN.

- If an extension number moves and the ALI database has not yet been updated, these forms can be administered to convert the moved extension into another public number located nearby the moved phone.

- If an extension number is not DID, these forms can be administered to convert the non-DID extension into another public number located nearby the calling non-DID extension.

However, changing the isdn and cama forms is usually not the best way to accomplish this. Those forms are limited in capacity: 240 and 448 entries, respectively. They typically hold instructions for converting large blocks of extension numbers to the public network CPN format.

5.3.2. Station Form's Emergency Location Extension Field

The other manual method involves the "Emergency Location Extension" field on the station forms.

```
change station 1001                                            Page   2 of   4
                                     STATION
FEATURE OPTIONS
           LWC Reception: msa-spe         Auto Select Any Idle Appearance? n
          LWC Activation? y                        Coverage Msg Retrieval? y
  LWC Log External Calls? n                                   Auto Answer: none
            CDR Privacy? n                              Data Restriction? n
   Redirect Notification? y                    Idle Appearance Preference? n
 Per Button Ring Control? n
   Bridged Call Alerting? n                      Restrict Last Appearance? y
  Active Station Ringing: single

        H.320 Conversion? n          Per Station CPN - Send Calling Number?
       Service Link Mode: as-needed
         Multimedia Mode: enhanced                 Audible Message Waiting? n
     MWI Served User Type:                      Display Client Redirection? n
                                               Select Last Used Appearance? n
                                                 Coverage After Forwarding? s
                                                   Multimedia Early Answer? n
                                            Direct IP-IP Audio Connections? y
  Emergency Location Ext: 1001                         IP Audio Hairpinning? Y
```

This field can be used in two different ways for 911 call handling. This section describes one of those ways, a manual method. Section 5.4 on page 52 describes the other method, an automatic method. It is possible to use a mixture of the two methods on the same server, but only with care. Section 5.4 on page 52 says more about that.

The "Emergency Location Extension" field allows for a manual method to correlate calling party numbers with phone locations, even if the phone users move. The steps in this manual process are as follows.

5.3.3. Know Where Wall Jacks Are

1. Set up and maintain a table or spreadsheet of wall jack to Emergency Location Extension correlations whenever you install a wall jack. The database should contain both data

ports and traditional circuit switched DCP and analog ports. One Emergency Location Extension is associated with all the wall jacks close enough together to be covered by one location record in the ALI database. Close enough varies according to your wishes and according to state legislation. Each emergency location extension will probably cover between 7,000 and 40,000 square feet, i.e., roughly within a radius of 15 to 35 meters, on one floor of a building.

For example, suppose an enterprise has a site with two buildings, each with two floors. The enterprise wishes for emergency personnel to be able to identify a user to within the correct building, floor, and east or west wing of the larger building. The enterprise has pre-selected some phones in those areas, and arranged for their street addresses to be entered into the ALI database.

- Extension 4000: Building A, 2nd floor, west wing.
- Extension 2000: Building A, 2nd floor, east wing.
- Extension 3000: Building A, 1st floor, west wing.
- Extension 5000: Building A, 1st floor, east wing.
- Extension 1000: Building B, 2nd floor.
- Extension 6000: Building B, 1st floor.

Building A	Floor 2	4000	2000
	Floor 1	3000	5000

Building B	Floor 2	1000
	Floor 1	6000

5.3.4. Move Transactions Are Recorded In The History Log

2. Set up a process for notifying the administrator if the phone user moves an extension number or moves a phone. The system administrator can consult a previously made plan if the move was planned. If the move was unplanned, at least not planned by the administrator, Communication Manager software can notify the administrator the user did move an extension number or a phone. To arrange this, set the "Record

CTA/PSA/TTI Transactions in History Log" and "Record IP Registrations in History Log" fields on the "system-parameters features" form to yes.

```
change system-parameters features                                  page 2
                       FEATURE-RELATED SYSTEM PARAMETERS
LEAVE WORD CALLING PARAMETERS
                Maximum Number of Messages Per Station: 10
   Maximum Number of External Calls Logged Per Station: 0
         Message Waiting Indication for External Calls? n
   Stations with System-wide Retrieval Permission (enter extension)
     1: 34430    3: attd     5:         7:          9:
     2: 34412    4:          6:         8:         10:
WARNING!   SEE USER DOCUMENTATION BEFORE CHANGING TTI STATE
    Terminal Translation Initialization (TTI) Enabled? _
    TTI State: _______      TTI Security Code: _______
            Customer Telephone Activation (CTA) Enabled? _
         Record CTA/PSA/TTI Transactions in History Log? _
                           COR for PSA Dissociated Sets: _
                      CPN, ANI for PSA Dissociated Sets: _
         Prohibit Bridging Onto Calls with Data Privacy? _
              Enhanced Abbreviated Dial Length (3 or 4)? _
          Record All Submission Failures in History Log? _
              Record PMS/AD Transactions in History Log?_
                 Record IP Registrations in History Log?
  Default Multimedia Outgoing Trunk Parameter Selection: 2x64
```

Then run the command "notify history" or "list history" to see when users have moved their phones or extension numbers.

```
notify history

                            ADMINISTRATION CHANGES

 Date Time  Login   Actn  Object       Qualifier
 2/15 10:18 actr-u  cha   station      2005
 2/15 10:18 actr-a  cha   station      2004
 2/15 10:15 tti-m   cha   station      2004
 2/15 10:15 tti-m   cha   station      2005
 2/15 10:15 tti-s   cha   station      2005
 2/15 10:12 actr-a  cha   station      2005
 2/15 10:12 ip-a    cha   station      2006
 2/15 10:12 ip-a    cha   station      2007
 2/15 10:10 ip-u    cha   station      2008
 2/15 10:10 ip-u    cha   station      2009
 2/15 10:09 actr-d  cha   station      2005 EMERGENCY EXT
```

Entries under these logins mean a user has moved a phone or moved an extension:

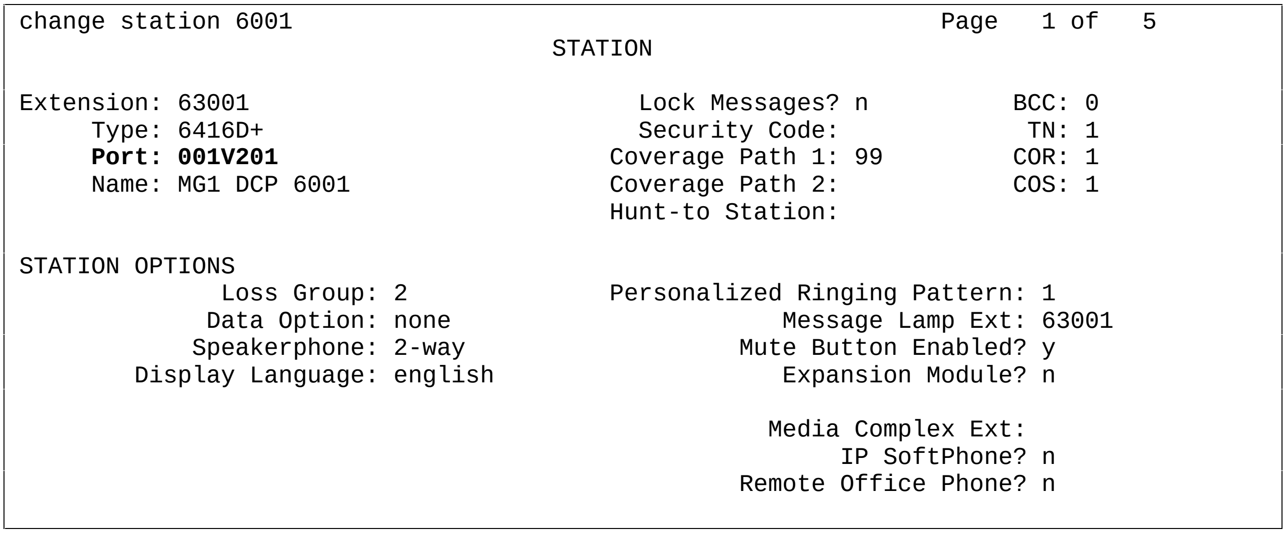
Login	Meaning
tti-m	The user has used the Terminal Translation Initialization feature to assign an extension number to a port.
tti-s	The user has used the Terminal Translation Initialization feature to remove an extension number from a port.

Login	Meaning
actr-u	The user has used the Automatic Customer Telephone Rearrangement feature to remove an extension number from a port.
actr-a	The user has used the Automatic Customer Telephone Rearrangement feature to assign an extension number to a port.
actr-d	The user has attempted to use the Automatic Customer Telephone Rearrangement feature to assign an extension number to a port, but the attempt was denied.
psa-u	The user has used the Personal Station Access feature to remove an extension number from a port.
psa-a	The user has used the Personal Station Access feature to assign an extension number to a port.
ip-u	The user has used registration of an IP phone to remove an extension number from a port.
ip-a	The user has used registration of an IP phone to move an extension number to a port.

There is one difficulty with this notification technique: if an extension has one of these entries in the history log, that does not necessarily mean the user has moved a phone. For example, it could mean an IP softphone user rebooted his PC, or a LAN glitch caused an IP Telephone to temporarily loose connectivity to the server.

5.3.5. Determine The Wall Jack

3. Determine the wall jack the user moved the phone or extension number to. For DCP or analog phones, the administrator can read the wall jack's port from the station form.

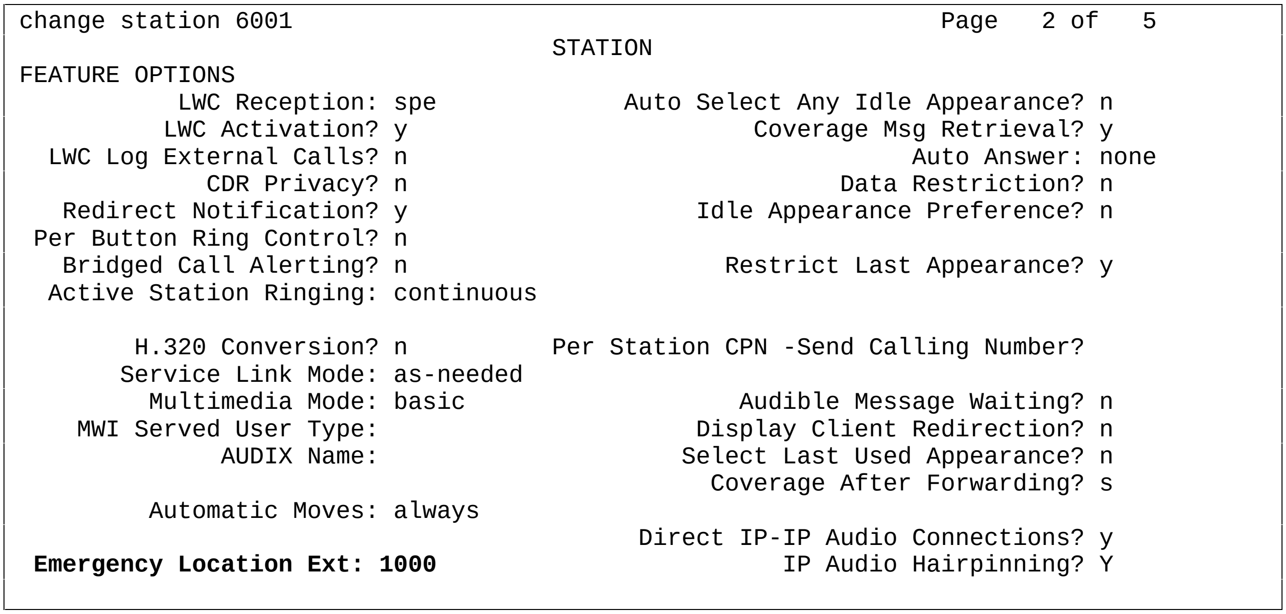


```
change station 6001                                             Page   1 of   5
                                     STATION

Extension: 63001                           Lock Messages? n          BCC: 0
     Type: 6416D+                          Security Code:             TN: 1
     Port: 001V201                       Coverage Path 1: 99         COR: 1
     Name: MG1 DCP 6001                  Coverage Path 2:            COS: 1
                                         Hunt-to Station:

STATION OPTIONS
              Loss Group: 2              Personalized Ringing Pattern: 1
             Data Option: none                       Message Lamp Ext: 63001
            Speakerphone: 2-way                   Mute Button Enabled? y
        Display Language: english                    Expansion Module? n

                                                    Media Complex Ext:
                                                         IP SoftPhone? n
                                                  Remote Office Phone? n
```

For IP phones, the administrator will have to call the user and ask. If that seems tedious or unreliable, do not use this manual method. Instead, use the automatic method of assigning Emergency Location Extensions described in section 5.4 on page 52.

5.3.6. Update The Station's Emergency Location Extension

4. Look up the corresponding Emergency Location Extension in the administrator's table or spreadsheet of wall jack to Emergency Location Extension correlations. Enter the number into the "Emergency Location Extension" field on the user's station form.



```
change station 6001                                             Page   2 of   5
                                     STATION
FEATURE OPTIONS
           LWC Reception: spe             Auto Select Any Idle Appearance? n
          LWC Activation? y                        Coverage Msg Retrieval? y
  LWC Log External Calls? n                                   Auto Answer: none
             CDR Privacy? n                              Data Restriction? n
   Redirect Notification? y                    Idle Appearance Preference? n
 Per Button Ring Control? n
   Bridged Call Alerting? n                      Restrict Last Appearance? y
  Active Station Ringing: continuous

        H.320 Conversion? n          Per Station CPN -Send Calling Number?
       Service Link Mode: as-needed
         Multimedia Mode: basic                   Audible Message Waiting? n
    MWI Served User Type:                      Display Client Redirection? n
              AUDIX Name:                     Select Last Used Appearance? n
                                                Coverage After Forwarding? s
         Automatic Moves: always
                                           Direct IP-IP Audio Connections? y
 Emergency Location Ext: 1000                        IP Audio Hairpinning? Y
```

During a call with ARS call type "emer" or "alrt", Communication Manager software will use the emergency location extension as the E911 CPN in place of the user's extension number. When the PSAP officer answers the call, the ALI database street address entry seen on the PSAP officer's screen will be the Emergency Location Extension's. That address is close to where the newly moved user physically is.

After changing the "Emergency Location Extension" field for some extensions, it is a good idea to save translations. Section 5.4.7.3.1 on page 62 goes into more detail about this.

5.4. Subnet Based Device Location For IP Telephones

The method of tracking user moves described in the previous section 5.3 beginning on page 47 works, but it requires manual effort. For IP phones, Communication Manager software provides a method for automating most of the effort. It allows administrators to use the ip-network-map form to assign an Emergency Location Extension to a range of IP addresses. Typically each range of IP addresses corresponds to an IP subnet.

5.4.1. Example IP-network-map form

```
change ip-network-map                        Page   1 of   X

                   IP ADDRESS MAPPING
                                                        Emergency
                                   Subnet       802.1Q  Location
FROM IP Address  (TO IP Address  or Mask) Region  VLAN  Extension
135.__9.__1.__0  135.__9.__1.255    24    __1      ___0   1000
135.__9.__2.__0  135.__9.__2.255    24    __1      ___0   2000
135.__9.__3.__0  135.__9.__3.255    24    __1      ___0   3000
135.__9.__4.__0  135.__9.__4.255    24    __1      ___0   4000
135.__9.__5.__0  135.__9.__5.255    24    __1      ___0   5000
135.__9.__6.__0  135.__9.__6.255    24    __1      ___0   6000
___.___.___.___  ___.___.___.___    __    ___      ____   ________
```

This feature's ability to physically locate an IP phone from its IP address depends upon the site's data network having subnets corresponding to geographic areas. As described in section 4.5.1 on page 31, this requirement can be misunderstood. The order of the geographic areas covered by the subnets need not have any correlation to the numeric order of the IP address ranges. The numeric correlations shown in the above figure, e.g. 135.9.1.* corresponding to extension 1000, is solely to make the correspondence easy to remember. The geographic areas covered by individual subnets do need to avoid overlapping each other, or at least not very much.

5.4.2. Example subnets

For example, suppose a has site has two buildings, each with two floors. The subnets in those buildings are arranged as follows.

Building A	Floor 2	135.__9.__4.__0 to 135.__9.__4.255	135.__9.__2.__0 to 135.__9.__2.255
	Floor 1	135.__9.__3.__0 to 135.__9.__3.255	135.__9.__5.__0 to 135.__9.__5.255

Building B	Floor 2	135.__9.__1.__0 to 135.__9.__1.255
	Floor 1	135.__9.__6.__0 to 135.__9.__6.255

The administrator would make sure the physical phones corresponding to the extension numbers administered into the Emergency Location Extension fields on the ip-network-map form were placed as follows:

- Extension 4000: Building A, 2nd floor, west wing.
- Extension 2000: Building A, 2nd floor, east wing.
- Extension 3000: Building A, 1st floor, west wing.
- Extension 5000: Building A, 1st floor, east wing.
- Extension 1000: Building B, 2nd floor.
- Extension 6000: Building B, 1st floor.

5.4.3. Example station form

The administrator would then administer station forms for all of the phones in the building. On each station form, the administrator would enter into the station form's "Emergency Location Extension" field the extension number corresponding to the station's physical location.

```
change station 6001                                             Page   2 of   5
                                     STATION
FEATURE OPTIONS
           LWC Reception: spe             Auto Select Any Idle Appearance? n
          LWC Activation? y                        Coverage Msg Retrieval? y
  LWC Log External Calls? n                                   Auto Answer: none
             CDR Privacy? n                              Data Restriction? n
   Redirect Notification? y                    Idle Appearance Preference? n
 Per Button Ring Control? n
   Bridged Call Alerting? n                      Restrict Last Appearance? y
  Active Station Ringing: continuous

        H.320 Conversion? n          Per Station CPN -Send Calling Number?
       Service Link Mode: as-needed
         Multimedia Mode: basic                    Audible Message Waiting? n
    MWI Served User Type:                      Display Client Redirection? n
              AUDIX Name:                     Select Last Used Appearance? n
                                                Coverage After Forwarding? s
         Automatic Moves: always
                                           Direct IP-IP Audio Connections? y
 Emergency Location Ext: 6000                        IP Audio Hairpinning? Y
```

5.4.4. Subnet algorithm

Here is how Communication Manager software uses the Emergency Location Extension to determine when a phone user has moved the phone. When an IP phone moves within the same subnet, it continues using the same IP address it had before the move. However, when an IP phone moves to a different subnet, it requests a new IP address from the DHCP server. This change in IP address is an indicator the user may have moved. Communication Manager software does not use it directly, however. It is possible an IP phone could change its IP addresses without moving. If an IP phone were to loose connectivity to the network for a long enough period of time, the DHCP server could put the IP address the phone was using back into the pool of available addresses, and then assign the address to another device. When the original phone regained connectivity, it would have to be given a different IP address. To avoid interpreting this series of events as a phone move, Communication Manager software does not compare the phone's old IP address with its new IP address. Instead, Communication Manager software counts on an administrator having entered on the phone's station form an identifier, the "Emergency Location Extension", for the phone's original subnet.

Here is an overview of how Communication Manager software tracks moving IP phones, and what calling party number Communication Manager software uses for those phones. Whenever an IP station dials an emergency call, Communication Manager software compares the "Emergency Location Extension" field administered on the ip-network-map form for the station's IP address with the "Emergency Location Ext" field administered on the station form.

1. If the two are the same, the IP station most likely has not moved, or at most moved within the same subnet. Communication Manager software uses the extension as the calling party number.

2. If the two are different and the emergency location extension administered on the ip-network-map form has an entry, then the IP station has moved from one subnet to another. Communication Manager software uses the Emergency Location Extension from the ip-network-map as the calling party number.
3. If the emergency location extension administered on the ip-network-map form is blank, then the administrator expected the IP station to be located outside the LAN. Most likely that would be true for a softphone. Communication Manager software uses the "Emergency Location Ext" field administered on the station form as the calling party number.

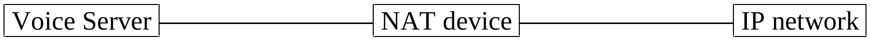
This was an overview of how Communication Manager software tracks moving IP phones, and what calling party number Communication Manager software uses for those phones. There is one exception to the above general rules. The IP station could already be using a different feature to assign calling party numbers for emergency calls from IP Softphones. Section 5.6 on page 77 describes the other feature and its interaction with this feature.

5.4.5. ARS

Communication Manager software relies on ARS digit analysis to classify a call as an emergency call. If a user dials a 911 call without using ARS, for example via a trunk access code, personal CO line button, facility test call, or AAR access code if AAR digit analysis does not overflow to ARS, then Communication Manager software does not use the "Emergency Location Extension" field to determine which CPN to send. Communication Manager software just sends the extension.

5.4.6. Network Address Translation (NAT)

If a phone is behind a Network Address Translation (NAT) device, the CPN is based on the phone’s translated IP address, not the native IP address. If the data network is using NAT, the NAT devices will have to preserve IP subnets. Communication Manager software expects a move from one geographic area to another to require a change in IP addresses. For example, suppose a site had 2 subnets, 1.1.1.* and 2.2.2.*, mapped to two different Emergency Location Extensions in the ip-network-map, and both of these were sitting behind a NAT device, as follows.



If the NAT device mapped both of 1.1.1.* and 2.2.2.* into addresses in the range 3.3.3.*, Communication Manager software would never detect a move of a phone from 1.1.1.* to 2.2.2.*.

5.4.7. Administrator Strategies

Now for some guidelines on how Communication Manager software could be administered to use the ip-network map's Emergency Location Extension fields. The basic strategies available to a system administrator are as follows.

- Pretend The Fields Do Not Exist (section 5.4.7.1 on page 57)
- Emergency Location Extensions Only For Areas (section 5.4.7.2 on page 57)
- CPN By Phone And Emergency Location Extension By Area (section 5.4.7.3 on page 60)

5.4.7.1 Pretend The Fields Do Not Exist

The first possible administrator strategy is to ignore the feature. Leave the Emergency Location fields in the ip-network-map form blank.

In countries where emergency response personnel do not have the ability to look up street addresses via an ALI database, this strategy causes Communication Manager software to send the station form's Emergency Location Extension number, which by default equals the extension number.

In the USA, and in the future in other countries that plan to add an emergency location street address system, assign a different street address in the ALI database to every extension number. Advise phone users not to move their own phones without notifying the administrator. This strategy allows precise location of phone user's locations, but requires administrator intervention every time a user moves. If a phone user should move a phone or log into a different phone without notifying the system administrator, this strategy risks having emergency personnel go to the wrong location.

If a single voice server is spread across multiple countries, administrators will want to follow this strategy in countries that do not have public network emergency location system, and follow some other strategy in countries that do. Such enterprises should administer their DHCP servers so each IP subnet is inside a single country.

5.4.7.2 Emergency Location Extensions Only For Areas

The next possible administrator strategy is to apply Emergency Location Extensions only by areas. Choose a few extensions to cover for several nearby phones: one extension per IP subnet. Make sure these extensions can not move. For example, make them non-IP phones. Administer only those extensions into the ip-network-map form. Administer the station forms' Emergency Location Ext fields to anything other than these extensions; setting each station forms' "Emergency Location Extension" field to equal its own extension number would do nicely. This is the default value for the station forms' Emergency Location Ext fields, after all.

For example, suppose that you have administered your ip-network-map form as shown in section 5.4.1 on page 53, and have IP subnets arranged as shown in section 5.4.2 on page 53. To carry out the strategy of Emergency Location Extensions Only For Areas, you could administer your stations as follows.

```
change station 1001                                          Page   2 of   5

 Emergency Location Ext: 1001                        IP Audio Hairpinning? Y
```

```
change station 1001                                          Page   3 of   5
 SITE DATA
      Floor: 2                                      Cord Length: 0
   Building: B                                        Set Color:
```

Notice that in this example, none of the subnet-based Emergency Location extensions (1000, 2000, 3000, 4000, 5000, & 6000) are in the "Emergency Location Ext" field sample station form shown above. The station form has administered its own extension number in the station form's "Emergency Location Ext" field. Now, suppose that station 1001 dials 911. Station 1001 is in building B, floor 2's subnet. The "Emergency Location Ext" field entry on the station form is 1001. The ip-network-map's "Emergency Location Extension" field entry for that subnet is 1000. Because these two numbers are not equal, Communication Manager software will assume that user 1001 recently moved. Communication Manager software will send the subnet-based calling party number, 1000, to the PSAP.

This strategy allows only a subnet based, imprecise location of phone users' physical locations, but requires no administrator intervention when a user moves. It continues to locate users even if a phone user should move a phone or log into a different phone without notifying the system administrator.

5.4.7.2.1 Non-DID Extensions And Pre-Determined Subnet Sizes

As mentioned in sections 5.1 on page 38 and 5.3 on page 47, a switch may have some non-DID extension numbers. The strategy of assigning Emergency Location Extensions by areas works nicely for such non-DID extensions. There is one potential problem, though. What if the enterprise is already using some other strategy for handling these extensions before upgrading to Communication Manager 2.0 software, for example either of the strategies mentioned in those earlier sections 5.1 and 5.3? The conversion to the ip-network-map based strategy may take some effort.

Consider a hypothetical site that has large numbers of non-DID extensions. Before upgrading to Communication Manager 2.0 software, this voice server used one DID number for every 7,000 square feet for their non-DID phones that do not move, administered via the station forms' Emergency Location Ext fields. This site has 40,000 square foot subnets. For those few phones that do move, the enterprise would be content with 40,000 square foot accuracy. The enterprise still wants to preserve 7,000 square foot accuracy for the non-DID phones that do not move.

The enterprise does not want to rearrange its data network; it wants to keep the same subnet structure. If a phone did not move, but did re-register, DHCP could give the phone a different IP address in the same subnet. This means the site administrator can not usefully administer into the ip-network-map IP address ranges with different Emergency Location Extensions for any range smaller than 40,000 square feet.

This hypothetical administrator would face a difficult choice.

1. They could administer Emergency Location Extensions into the ip-network-map only for those IP address ranges corresponding to the moving phones. This would accomplish the enterprise's goals, but in practice would be risky. There would be nothing to stop a phone user who was expected to move his phone from plugging the phone into an unused jack in the area used by the non-moving phones. If such a phone user did that and then called 911, the wrong CPN would be sent.
2. They could administer no Emergency Location Extensions into the ip-network-map. This would accomplish the enterprise's goal of keeping 7,000 square foot accuracy for the non-moving phones, but would not achieve the enterprise's goal of 40,000 square foot accuracy for the movable phones.
3. They could administer Emergency Location Extensions into the ip-network-map for all IP address ranges. This would accomplish the enterprise's goal of 40,000 square foot accuracy for the movable phones, but would not achieve the enterprise's goal of 7,000 square foot accuracy for the non-moving phones.

5.4.7.2.2 Make Sure To Complete Administration

Suppose they chose option 3, accepting its limitations. They then have to be careful to complete the required new administration of the Emergency Location Extension fields on both the station forms and on the ip-network map. If they are not careful to complete both forms, problems could result.

For example, suppose that prior to the upgrade to Communication Manager 2.0 software, 1111 is a non-DID number, so 1111's station form is administered to use a different extension than 1111 as the emergency location extension, say 1000. Now, suppose the administrator decides to upgrade to Communication Manager 2.0 software and add 1000 as an emergency location extension on the ip-network-map, for an IP address range containing 1111's IP address. Suppose the administrator forgets to update the Emergency Location Extension on 1111's station form. When 1111 dials 911, Communication Manager software will compare the two emergency location extensions, discover they are the same and therefore decide set 1111 did not move, and send the digit string "1111" to the public network as the calling party number. This would be bad because "1111" is not a DID number for that enterprise. At best the PSAP officer would not any information about where to send the emergency response personnel. At worst, the PSAP officer would direct the emergency response personnel to the wrong location. One company's non-DID number may be another company's DID number.

For example, suppose that prior to the upgrade to Communication Manager 2.0 software, 2222 is a DID number, so 2222’s station form is administered with Emergency Location Extension equal to 2222. Now, suppose the administrator decides to upgrade to Communication Manager 2.0 software and add 2000 as an emergency location extension on the ip-network-map, for an IP address range containing 2222’s IP address. Suppose they forget to update the Emergency Location Extension on 2222’s station form. When 2222 dials 911, Communication Manager software will compare the two emergency location extensions, discover they are different and therefore decide set 2222 did move, and send the digit string "2000" to the public network as the calling party number. This would not be ideal, because 2222’s street address in the ALI database more precisely identifies its physical location than does the street address for 2000 in the ALI database.

The conclusion to draw from these two scenarios is: whenever an administrator adds an extension as an Emergency Location Extension to the ip-network-map, the administrator should check all of the station forms for stations in the IP address range.

- If the station is a DID number, the administrator should make sure the station form has the same Emergency Location Extension as does the ip-network-map form.
- If the station is not a DID number, the administrator should make sure the station form has a different Emergency Location Extension than does the ip-network-map form.

5.4.7.3 CPN By Phone And Emergency Location Extension By Area

Going back to possible administrator strategies, the next possible administrator strategy is to use a hybrid of the previous strategies. Assign a different street address in the ALI database to every extension number. Also choose a few extensions: one per IP subnet, to cover for several nearby phones. Make sure these extensions can not move. For example, make them non-IP phones. Only administer those extensions into the Emergency Location Extension fields on the ip-network-map form and station forms.

For example, suppose that you have administered your ip-network-map form as shown in section 5.4.1 on page 53, and have IP subnets arranged as shown in section 5.4.2 on page 53. To carry out the strategy of Emergency Location Extensions Only For Areas, you could administer your stations as follows.

```
change station 1001                                          Page   2 of   5

 Emergency Location Ext: 1000                      IP Audio Hairpinning? Y
```

```
change station 1001                                          Page   3 of   5
 SITE DATA
      Floor: 2                                   Cord Length: 0
    Building: B                                    Set Color:
```

Notice that in this example, one of the subnet-based Emergency Location extensions (1000, 2000, 3000, 4000, 5000, & 6000) is entered in the sample station form’s "Emergency Location

Ext" field shown above, namely 1000. Now, suppose that station 1001 dials 911. Station 1001 is in building B, floor 2's subnet. The "Emergency Location Ext" field entry on the station form is 1000. The ip-network-map's "Emergency Location Extension" field entry for that subnet is 1000. Because these two numbers are equal, Communication Manager software will conclude that user 1001 has not moved. Communication Manager software will send the station's own extension number, 1001, to the PSAP.

This strategy allows precise location of phone user's locations for users who do not move, and gives subnet based, imprecise locations for phone users who do move. It requires no administrator intervention when a user moves. It continues to do so even if a phone user should move a phone or log into a different phone without notifying the system administrator.

This strategy can provide precise location of phone users' locations for users who do move, provided those users notify the administrator when they move. After a user moves, an administrator can ensure emergency personnel will go to precisely the right physical location by carrying out these steps:

- Update the ALI database with the extension's new street address.
- Set the "Emergency Location Ext" field administered on the user's station form equal to the corresponding "Emergency Location Extension" field administered on the ip-network-map form for the user's new IP address range. For example, suppose station 6001 has recently moved. The administrator can run status station to learn station 6001's new IP address.

```
status station 6001                                            Page   3 of   5

                                CALL CONTROL SIGNALING
                   Switch                     IP                         IP
                   Port     Switch-end IP Addr:Port    Set-end IP Addr:Port
     IP Signaling: 03C0617  135.  9.  3.120   :1720    135.  9.  1.238:4739
            H.245:
        Node Name:          manta_clan
   Network Region:          3                          3
                                  AUDIO CHANNEL
                   Switch                     IP                         IP
                   Port     Other-end IP Addr :Port    Set-end IP Addr:Port
            Audio:
        Node Name:
   Network Region:
    Audio Connection Type: ip-tdm
               Product ID: IP_Phone
  H.245 Tunneled in Q.931? does not apply
      Registration Status: registered-authenticated
              MAC Address: 00:04:0d:00:26:82
```

Since IP telephone 6001 is now in the 135.9.1.* subnet, the ip-network-map form in section 5.4 on page 52 shows 6001's new Emergency Location Extensions is 1000. That number should now be entered into the "Emergency Location Ext" field on extension 6001's station form.

```
change station 6001                                             Page   2 of   5
                                     STATION
FEATURE OPTIONS
           LWC Reception: spe             Auto Select Any Idle Appearance? n
          LWC Activation? y                        Coverage Msg Retrieval? y
  LWC Log External Calls? n                                   Auto Answer: none
             CDR Privacy? n                              Data Restriction? n
   Redirect Notification? y                    Idle Appearance Preference? n
 Per Button Ring Control? n
   Bridged Call Alerting? n                      Restrict Last Appearance? y
  Active Station Ringing: continuous

        H.320 Conversion? n          Per Station CPN -Send Calling Number?
       Service Link Mode: as-needed
         Multimedia Mode: basic                   Audible Message Waiting? n
    MWI Served User Type:                      Display Client Redirection? n
              AUDIX Name:                     Select Last Used Appearance? n
                                                Coverage After Forwarding? s
         Automatic Moves: always
                                           Direct IP-IP Audio Connections? y
 Emergency Location Ext: 1000                        IP Audio Hairpinning? Y
```

Remember, this manual intervention step is only required to provide precise location of phone user's locations for users who do move. Without any manual intervention, Communication Manager software provides general, subnet-based locations for phone users who do move.

5.4.7.3.1 Saving Translations

After you update the ALI database with the extension's physical location and then change the "Emergency Location Extension" field to match the extension's new IP subnet, save translations. Otherwise, if the system resets, causing translations to be reloaded, the "Emergency Location Extension" field in the loaded translations would still be set to the old value. Should the user dial 911, emergency response personnel would go to the user's approximate instead of exact location. To prevent this, system administrators should save translations after changing any "Emergency Location Extension" fields.

A Local Spare Processor (LSP) copies administration translations from its primary server once a day. Translations are never copied from the LSP to the primary server. After an IP extension moves, a system administrator may update the ALI database with the extension's physical location and then change the "Emergency Location Extension" field to match the extension's new IP subnet. If then the phone registers with the LSP before the next copying of translations from the main to the LSP, the "Emergency Location Extension" field in the loaded translations would still be set to the old value. If the user dials 911, emergency response personnel would go to the user's approximate instead of exact location.

A Survivable Remote EPN (SREPN) and WAN Spare Processor (WSP) have their own translations. If someone changed the Emergency Location Extension fields on the SREPN or WSP, but did not make the equivalent change on the primary server, or vice versa, they would cause a problem. If a phone controlled by a SREPN or WSP calls 911 under these circumstances, the reported CPN would be wrong. Emergency response personnel would go to the wrong location. To prevent this, you should make all administration changes on both the main server and on the SREPN or WSP.

5.4.8. Cross-Country Moves And Multiple Servers

Section 4.6.1 on page 32 talks about routing calls to the correct PSAP across a private network consisting of multiple servers. As noted in the section, to route calls to the correct PSAP after cross-country moves by IP phones, each voice server in the enterprise's network would need to be administered with IP address ranges covering locations throughout the enterprise's entire network. This takes care of routing the call to the correct PSAP. How about sending the correct CPN after a move across the country? The principle is the same; only the granularity is finer.

To route cross-country 911 calls to the correct PSAP, it sufficed to have IP Address range entries in the ip-network-map corresponding to the area covered by each PSAP. That is roughly one entry in the ip-network-map per area code or metropolitan area. To also send the correct CPN for a cross-country 911 call, one would expect to need entries corresponding to the area covered by each subnet.

- If the voice servers are connected by tie trunks that can not signal the CPN of the calling party, there is not much hope of sending a CPN corresponding to the physical location of the calling party. The only way this could be done is the trivial case where the area covered by the receiving voice server has fewer street addresses than there are tie trunks connecting the two voice servers. You would have to set up a one-to-one correlation between tie trunks and the CPNs used by the voice server routing the 911 call into the public network. That would only be practical for small branch offices.

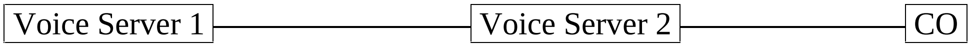
- If the two voice servers are connected by tie trunks that can signal the CPN, it would be necessary to have IP Address range entries in the ip-network-map corresponding to each subnet in the enterprise's network. This is the most likely case. This would limit the enterprise's network to no more subnets than there are ip-network-map entries, currently 500.

5.5. PSAP Calls Forwarded To Caller's Extension

If an emergency call should accidentally drop, the public safety personnel may call back. If the sent CPN was not equivalent to the caller's extension number, the return call would ring the Emergency Location Extension rather than the one that dialed 911. To overcome this limitation, Communication Manager software can be administered to automatically forward the return call to the set that placed the emergency call. The call is forwarded as a priority call. This means it will be answered by a person, rather than proceeding down a coverage path and being answered by voice mail.

5.5.1. All Incoming Trunk Calls Forwarded

Central offices do not signal to a Communication Manager server whether an incoming trunk call is from a PSAP office, or from some other party. To ensure that after a 911 calls drops the return call from the PSAP does get forwarded, Communication Manager software must forward every incoming trunk call. This includes incoming tie trunk calls, not just public network calls, in case the enterprise has a campus network like this:



and a user on voice server 1 dials 911.

5.5.2. What Kind Of Phone To Use As An Emergency Location Extension

This Emergency Location Extension forwarding feature does affect the types of extensions you will want to use for Emergency Location Extensions. There are advantages and disadvantages to each kind of extension.

5.5.2.1 Phone Types

5.5.2.1.1 AWOH Extensions

AWOH extensions do not require any physical set or any wiring. Their street address in the ALI database can be anywhere the administrator wants, and they stay there. Phone users can not move them unexpectedly. On the other hand, if the emergency location extension forwarding does not happen for some reason, AWOH extensions would not be able to answer the return call. One could make this potential problem less likely by giving the AWOH extension a coverage path including only extensions likely to be answered by a human. Ideally, that would be a human whose phone is in or relatively close to the area covered by the AWOH Emergency Location extension.

5.5.2.1.2 Circuit Switched Phones

Circuit switched phones such as DCP or analog phones require a physical set. If the extension is fairly far away from the main server, additional wiring may be required. However, phone users usually can not unexpectedly move these phones. Moving one of these phones requires use of one of the features described in section 5.2 on page 45. Administrators would have to grant permission before phone users can use those features. Circuit switched sets have the advantage that someone can answer them if the emergency location extension forwarding does not happen for some reason, and the person will be close to the emergency. DCP sets have an advantage over analog sets because digital sets can be administered with call forwarding and crisis alert buttons. Section 5.5.5.14.1 on page 76 explains how those buttons could be useful for an Emergency Location Extension set.

5.5.2.1.3 IP Phones

IP phones such as IP Telephones or IP Softphone require a physical set. However, even if the extension is fairly far away from the main server, additional wiring probably would not be required, as long as the phone can connect to the LAN. Phone users can easily and unexpectedly move these phones. If the emergency location extension forwarding does not happen for some reason, and someone at the Emergency Location Extension does answer the returning PSAP call, the person is not guaranteed to be close to the emergency. IP phones can be administered with call forwarding and crisis alert buttons. Section 5.5.5.14.1 on page 76 explains how those buttons can be useful for an Emergency Location Extension set.

5.5.2.2 Extension Types

The Emergency Extension Forwarding feature could in theory forward incoming trunk calls originally directed towards any kind of emergency location extension on the voice server. There are many kinds of extensions not typically assigned to ordinary station users: Hunt groups, Listed Directory Number, Terminating Extension Group, Expert Agent Login extensions, Vector Directory Numbers, Multimedia Applications Server Interface, Attendant Common Shared Call Park Extensions, MASI extensions, Xmobile extensions, XDID extensions, Recorded announcement extensions, Attendant console personal numbers, Data modules, UDP extensions, Access endpoints, Wideband access endpoints, Remote access extensions, PRI endpoints, Voice mail extensions, Telecommuting Access Extension, CDR System Parameters Primary/Secondary Output Endpoint, Administered connections, 9601 Wireless Terminals, etc.

The above is not a complete list of extensions not typically assigned to ordinary station users. System administrators will probably want to avoid assigning of them to entries in the emergency location extension fields of the ip-network-map form. Some of them in particular would be bad choices, as described below.

5.5.2.2.1 High Call Volume Sets

A wise system administrator will make sure the Emergency Location extensions typically receive few calls. If an Emergency Location Extension had a high call volume, for example:

- a hunt group or
- an automatic call distribution group, or
- a vector directory number, or
- a listed directory number

then the activation of call forwarding from the Emergency Location Extension to the set which placed the 911 call would result in the set being flooded with more calls than it can handle. This would have two side effects:

- Large numbers of outside callers who are expecting to reach a business service would instead reach busy tone.
- If the call to the 911 service should accidentally drop, the return call from the public safety access point would also likely reach busy tone.

5.5.2.2.2 Forwarding From Important Extensions

Similarly, a wise system administrator will make sure the extensions administered into the ip-network-map form would not cause problems if forwarded. For example, if someone entered the company's security office extension as an emergency location extension into the ip-network-map form, the most recent person to drop from a 911 from the emergency location extension's subnet would receive calls intended for the security office. This might prevent some other emergency from being responded to.

5.5.2.2.3 Extensions That Can Not Be Forwarded

An Emergency Location Extension should not be one of the following extensions, because call forwarding from these types of extensions is not possible:

- A multimedia set,
- An EAS agent ID,
- A hunt group extension,
- A data extension,
- A terminating extension group extension,
- An attendant
- An extension with "Call Coverage: All" administered for it. Call Coverage Criteria: "all" is administered on the "call coverage" form. It is typically used if someone goes on a leave of absence, for example.   It prevents any calls from terminating at an extension. Call Forwarding is set up at the station calls are being forwarded from. If a call never reaches the station, the call can not be forwarded on. If the Emergency Location Extension has call coverage All enabled, a return call from the PSAP would never have a chance to be forwarded to the station that dialed 911.

5.5.3. Non-Humans

If the public safety staff should happen to call back and forwarding is not possible for one of the reasons mentioned in the following section 5.5.5 on page 67, the return call should have a reasonable chance of being answered by a human. If the return call were to connect to, for example, a VDN, the emergency personnel's return call might reach an announcement prompting them for an account number or something similar. They could then think they had been given a wrong number, and might then also begin to doubt whether the street address they received from the ALI database was correct.

5.5.4. Media Gateways And Emergency Location Extensions

Suppose an IP phone and a nearby Media Gateway providing its connection to the PSTN are both registered to a primary server. Suppose the gateway is backed up by an LSP, and the IP Phone has some LSPs in its alternate gatekeeper list. Suppose the IP phone dials 911, and then the LAN crashes and partially recovers. If both the IP phone and the Media Gateway can re-register to the primary server, everything is fine. If both the IP phone and the Media Gateway are forced to register with the same LSP, everything is fine.

But if one of them re-registers to one LSP and the other re-registers to the primary server, or if they re-register to different LSPs, there is a minor problem. When the emergency response personnel call back, the server the Media Gateway is registered with will think the IP phone is unregistered. The Media Gateway's server will not be able to forward the call to the IP phone. Instead, the Media Gateway's server will attempt to ring the call at the Emergency Location Extension.

Even with automatic emergency return call forwarding, it is still wise to pick the Emergency Location Extensions to be on Media Gateways having incoming PSTN trunks, and on the same Media Gateway as the phones they cover for.

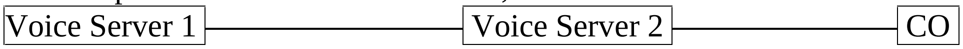
5.5.5. Why Forwarding May Not Happen

The earlier section 5.5.2 on page 67 says that sometimes emergency location extension forwarding may not happen when the PSAP officer calls back. Here are some reasons why it may not happen, what would happen instead, and how to avoid it.

5.5.5.1 Different Voice Servers

Choosing where to place Emergency Location Extensions is more difficult for a campus network than for a stand alone voice server. This is because the voice server dialing 911 is the one setting up the call forwarding from the Emergency Location Extension to the set dialing 911. A voice server can set up forwarding only for itself. If the Emergency Location Extension happens to be on a different voice server than the set dialing 911, the call forwarding can not be set up.

For example, suppose the following.

1. An enterprise has a network as follows, with each voice server in its own building.
   

2. All the Emergency Location Extensions in building 1 are stations on voice server 1, and all the Emergency Location Extensions in building 2 are stations on voice server 2.
3. User 1111, whose extension is on voice server 1, walks over to building 2 and registers the extension 1111 to a phone in building 2.
4. User 1111 dials 911.
5. Voice Server 1 looks up the IP address of the calling phone in voice server 1's ip-network-map, and finds the IP address maps to Emergency Location Extension 2000, an extension on voice server 2.

6. Voice Server 1 launches the call to 911, using 2000 as the calling party number. However, voice server 2 can not set up call forwarding from extension 2000 to extension 1111, because extension 2000 is not an extension on voice server 2.

This is not really a bad situation. If the 911 call should accidentally drop, and the PSAP officer were to call back, the return call would be answered by someone who is physically close to user 1111.

However, the situation could have been avoided. If desired, one could administer voice server 1's ip-network-map with Emergency Location Extensions on voice server 1, for each IP subnet in building 2. Then the call forwarding could be set up, because both the 911 caller and the Emergency Location Extension would be on the same voice server. At first glance, this might seem to require a lot of extra phones, and possibly some extra wiring, but it is not necessarily so. As mentioned in section 5.5.2.1.1 on page 64, one could use AWOH extensions as Emergency Location Extensions. For a campus, AWOH extensions would probably provide a workable solution. For a nation wide network, there is not an easy way to guarantee that Emergency Location Extension forwarding will always happen.

5.5.5.1.1 LSP

A similar situation occurs if a station is controlled by a S8700 but its corresponding Emergency Location Extension station is controlled by a LSP. Suppose the station dials 911 and then the call drops. When the emergency response personnel call back, the LSP will not be able to forward the call to the set that dialed 911. Instead, the LSP would ring the call at the Emergency Location Extension station.

5.5.5.1.2 Accidental Removal Of An Emergency Location Extension

An administrator might inadvertently try to remove an extension being used as an Emergency Location Extension by some other set. If an emergency location extension were removed and a 911 call using the extension as the source for the CPN were to drop, the return call from the PSAP would fail. Worse, if after removing the extension from Communication Manager software the administrator were to remove the extension from the ALI database, the 911 call would not show a street address for any 911 caller from the extension's former subnet. Communication Manager software will not allow an extension being used as an Emergency Location Extension on the same voice server to be removed. However, Communication Manager software can not prevent an extension from being removed from a different voice server. If you choose to use Emergency Location Extensions from multiple voice servers, be careful when removing those extensions.

5.5.5.2 System Capacity Limits On Forwarding

Forwarding has its capacity limits. It is possible the maximum number of call forwarding requests would already be active on the switch when someone drops from a 911 call. The current system limits are:

Platform	CSI	S8100	SI	S8300	S8500	R	S8700
Maximum simultaneous call forwarding requests.	2,400	2,400	2,400	2,400	36,000	25,000	36,000

The only way to avoid this is to tell users not to do so much call forwarding. Fortunately, these limits are high; exceeding them is not very likely.

5.5.5.3 Simultaneous Nearby E911 Calls

Communication Manager software sets up forwarding from the Emergency Location Extension to the set that dialed 911. If two sets dial 911 almost simultaneously, and they are physically close enough together to use the same Emergency Location Extension, Communication Manager software does not set up forwarding from the Emergency Location Extension to both of those sets simultaneously. Communication Manager software sets up forwarding to the extension most recently dropped from a 911 call.

The only way to avoid this is to use fairly small subnets, so it is not likely two people will simultaneously call 911 from the same subnet. Fortunately, if this does happen and the PSAP does call back, at least the person answering the call will either be the correct party, or will be physically close to them.

5.5.5.4 Too Much Digit Manipulation

Emergency Location Extension forwarding applies to the extension number as administered on the station forms or on the ip-network-map forms. That may not necessarily equal the CPN as sent by the voice server, if the CAMA numbering or the public/unknown numbering tables manipulate the Emergency Location Extension digits. For example, suppose phone 1111 has moved from its own subnet to another subnet, and 1111's IP address now corresponds in the ip-network-map to emergency location extension 3333. Suppose phone 1111 calls 911. The chosen emergency location extension is 3333. Communication Manager software sets up Emergency Extension forwarding from 3333 to 1111. However, suppose the Public/unknown numbering tables convert the digit string 3333 to "303-538-3000." When the PSAP officer calls back, the call would go to extension 3000. There is no forwarding from 3000 to 1111.

You can avoid this situation by not using the CAMA numbering or public/unknown numbering tables to manipulate digits so much the extension that the PSAP would call back to changes.

5.5.5.5 Trunks Dialing 911

Emergency Location Extension Call forwarding applies to calls from extensions. It does not apply if the party dialing 911 is something other than an extension, for example an incoming tie trunk. However, there are certain circumstances under which a trunk can act like an extension. Under those circumstances, Emergency Location Extension Call forwarding does apply. Section 6.5 on page 86 describes those circumstances.

5.5.5.6 Permissions can Block Forwarding

Communication Manager software will not set up forwarding from the Emergency Location Extension to the set that dialed 911 if system permissions prohibit it. Set up COR, Tenant, and IP Network Region permissions accordingly.

5.5.5.6.1 COR And Tenant

Emergency Location Extensions should be assigned to Classes of Restriction and Tenant Partitions with permission to reach every other extension on the switch.

5.5.5.6.2 Change COR Via FAC

It is probably best for station users to avoid using the change COR via FAC feature while the Emergency Extension Forwarding timer is running. There is a chance such users could do so to change their COR to one blocking forwarding of calls between the Emergency Location Extension and the extension that dialed 911.

```
display feature-access-codes                                    Page   1 of   7
                              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:
                      Announcement Access Code:
                       Answer Back Access Code: #11
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code:
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA:        All:        Deactivation:
                         Call Park Access Code: *11
                       Call Pickup Access Code: *13
CAS Remote Hold/Answer Hold-Unhold Access Code:
                  CDR Account Code Access Code:
                        Change COR Access Code:
```

Station users who have a need to change their COR to one specific value would be better off using the Station Lock feature to change the COR than using the Change COR via FAC feature. The Station Lock feature is more under the control of the system administrator. The system administrator can pre-administer the one COR each user can change to. The administrator can then make sure each COR reachable by each station user has permission to receive forwarded calls from Emergency Location Extensions.

```
display cor 1                                                   Page   2 of   4
                             CLASS OF RESTRICTION

                     MF Incoming Call Trace? n
               Brazil Collect Call Blocking? n
                     Block Transfer Display? n
Block Enhanced Conference/Transfer Displays? y
                     Remote Logout of Agent? n


                           Station Lock COR: 1
  Outgoing Trunk Disconnect Timer (minutes):
```

```
display feature-access-codes                                    Page   3 of   7
                               FEATURE ACCESS CODE (FAC)

 PASTE (Display PBX data on Phone) Access Code:
  Personal Station Access (PSA) Associate Code:        Dissociate Code:
        Per Call CPN Blocking Code Access Code:
      Per Call CPN Unblocking Code Access Code:

                  Priority Calling Access Code:
                           Program Access Code:
       Refresh Terminal Parameters Access Code:
              Remote Send All Calls Activation:        Deactivation:
               Self Station Display Activation:
                     Send All Calls Activation: *12    Deactivation: #12
         Station Firmware Download Access Code:
                       Station Lock Activation:        Deactivation:
      Station Security Code Change Access Code:
```

5.5.5.6.3 Network Region Permissions

If an Emergency Location Extension is an IP station, and someone has administered the ip-network-region form so the IP station's region is not interconnected with the region of the IP station that dialed 911, the call forwarding would set up, but the return call from the PSAP might fail. If there existed a TDM connection between CLANs and Media Processors in both regions, the return call would succeed, being carried in part via the TDM bus. However, if there was no circuit switched path between the two regions, then the return call would fail.

If you use IP phones as Emergency Location Extensions, you should administer IP network regions so an Emergency Location Extension's network region is always interconnected with the IP network regions of the sets it supports. Typically this will not take any effort, because those sets will be in the same subnet.

```
display ip-network-region 1                                    Page   3 of  19

                   Inter Network Region Connection Management

 src dst
 rgn rgn      codec-set  direct-WAN  WAN-BW-limits  Intervening-regions
 1   1          1
 1   2          1           y             :NoLimit
 1   3          2           y             :NoLimit
 1   4
 1   5
 1   6
 1   7          3           y             :NoLimit
 1   8
 1   9
 1   10
 1   11
 1   12
 1   13
 1   14
 1   15
```

5.5.5.7 Very Frequent Forwarding

Call forwarding is temporarily blocked if a previous call had been forwarded within the past 15 seconds from the same extension. This temporary blockage prevents an infinite loop, with a single call bouncing back and forth between two destinations. There is no way to prevent this, but it is unlikely the Emergency Location Extension user would have manually set up call forwarding and a non-emergency call would have been forwarded 15 seconds before an emergency call drops.

5.5.5.8 Set Not Working

Communication Manager software does set up call forwarding, but it may not appear to happen, if the 911 call drops because the 911 caller's set suddenly stops working. Here are some ways that could happen, and what the results would be from the user's perspective.

If the 911 caller's set is in out-of-service state when the PSAP calls back, the call goes down the 911 caller's coverage path. There are two common ways a set could get into out-of-service state.

- The 911 caller is busied out.
- If the 911 caller is a DCP set on a Media Gateway, and the media gateway providing service to the DCP set is not able to set up an IP communication path to the main server, and the incoming trunk carrying the return PSAP call is under the control of the main server, the set is also out-of-service as seen from the incoming trunk's point of view.

If the 911 caller's set is in disconnected state when the PSAP calls back, the call rings silently at the 911 caller's set. There are two common ways a set could be put into disconnected state.

- The 911 caller unplugs the set. If user happens plug the set back in during the return call from the PSAP, the call instantly starts to audibly ring at the 911 caller's set.
- The LAN crashes during the 911 call. If the LAN happens to recover during the return call from the PSAP, the call instantly starts to audibly ring at the 911 caller's set.

5.5.5.9 Silent Ringing

There are several features in Communication Manager software that can cause a call to ring silently or to ring with only one brief ping at the set: Abbreviated and Delayed Ringing, Active Station Ringing, Ringer Cutoff, Station User Button Ring Control. Users and administrators would be wise to avoid applying those features to a set shortly after the set dials 911, or applying them to Emergency Location Extensions.

5.5.5.10 Bridged Call Appearances

To make sure the Emergency Location Extension can ring should forwarding not happen for one of the reasons mentioned in this section 5.5.5, it is also wise to make sure the Emergency Location Extension has at least one call appearance of its own, i.e., it does not have only bridged appearances of other extensions.

5.5.5.11 Call Forwarding Deactivation

Emergency Location Extension forwarding will not happen if the user at the emergency location extension phone enters the Call Forwarding Deactivation FAC, or enters the activation FAC directed at a different destination than the set most recently dropped from a 911 call. Users at the emergency location extension phone should use these features only if they are sure the emergency response personnel have already arrived.

5.5.5.12 Conference & Transfer

It is not likely, but it is possible someone could add a 911 call into a conference call, or dial a 911 call and then transfer the call to someone else. If the extension that dialed 911 is still on the call when the 911 call drops, Communication Manager software sets up forwarding from the Emergency Location extension to the extension that dialed 911. However, if the extension that dialed 911 is not on the call when the call drops, Communication Manager software does not set up Emergency Location Extension forwarding.

5.5.5.13 Send All Calls And Do Not Disturb

Send All Calls and Do Not Disturb, if active at the set that dialed 911, have no effect on Emergency Location Extension forwarding. The forwarded call will override these features and ring at the set that dialed 911. However, Send All Calls and Do Not Disturb, if active at the Emergency Location Extension set, would prevent the return call from the PSAP from ever reaching the extension in the first place in order to be forwarded on to the set that dialed 911. To prevent this from happening, Communication Manager software turns SAC and DND off at the Emergency Location Extension when the 911 call drops. Communication Manager software turns SAC back on when the Emergency Location Extension forwarding timer expires. You may not have heard of the timer. The following section 5.5.5.14 on page 75 talks about it.

5.5.5.14 Forwarding Timer

The user at the Emergency Location Extension would not want to have his calls forever forwarded to the set most recently dropped from a 911 call. True, forwarding can be turned off manually after the emergency response personnel arrive, but what if the Emergency Location Extension set user happened to be on vacation when the 911 call happened? When the user returned from vacation, instead of finding important messages in his voice mail, he would find an annoyed co-worker who had recovered from the emergency and is getting tired of answering all those forwarded calls. To prevent this sort of situation, Communication Manager software automatically turns off Emergency Extension forwarding after an administrable period of time.

```
change system-parameters features                               Page   4 of  12
                        FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
              System Printer Endpoint:                    Lines Per Page: 60
                  EIA Device Bit Rate: 9600

 Emergency Extension Forwarding (min): 10

SYSTEM-WIDE PARAMETERS
                          Switch Name:
         Emergency Numbers - Internal:           External: 911
      No-License Incoming Call Number:

MALICIOUS CALL TRACE PARAMETERS
               Apply MCT Warning Tone? n   MCT Voice Recorder Trunk Group:

SEND ALL CALLS OPTIONS
     Send All Calls Applies to: station    Auto Inspect on Send All Calls? n

UNIVERSAL CALL ID
     Create Universal Call ID (UCID)? n    UCID Network Node ID:
```

The "Emergency Extension Forwarding" field takes on values from 0 through 999 minutes. Its default value is 10 for both new installations and upgrades to Communication Manager software from Multivantage™ software and from DEFINITY® software.

5.5.5.14.1 Recommended Duration

So, how long should the "Emergency Extension Forwarding" timer field be set to? Roughly as long as you think it may take for emergency response personnel to arrive.

5.5.5.14.1.1 Call Forwarding Button

If Emergency Extension Forwarding timer is set to a too large value, the emergency response personnel may have long since come and gone, and the person at the Emergency Location Extension station is still having all his incoming trunk calls ring at the station that most recently dialed 911. If he notices he is not receiving incoming trunk calls, he can manually turn off the forwarding by using the Call Forwarding Deactivation feature access code.

However, he may not notice he is not receiving incoming trunk calls. This possibility could be alleviated somewhat by giving the Emergency Location Extension station a call forwarding button. He can tell by looking at the lamp adjacent to the button that his incoming trunk calls are being forwarded. Otherwise, the only way he would know would be a brief ring-ping as each call was forwarded.   The lamp on the forwarding button also lets such users know why, on rare occasions, they will not be able to use Send All Calls or Do Not Disturb, as described in section 5.5.5.13 on page 75. Emergency Location Extension users should also be trained not to use the forwarding button to turn off call forwarding until they are sure the emergency response personnel have arrived.

5.5.5.14.1.2 Crisis Alert Button

If Emergency Extension Forwarding timer is set to a too short value, the PSAP officer may call back and reach someone other than the person who dialed 911, someone who is not aware of exactly what happened or exactly where the emergency response personnel need to go. This possibility could be alleviated somewhat by giving the Emergency Location Extension station a crisis alert button. The crisis alert button will let the Emergency Location Extension station user know when someone has dialed 911. When answering the return call after the timer expires, he would at least know a 911 call had been dialed, and know the extension number of the person who dialed it. The Emergency Location Extension user could manually transfer the return call from the emergency personnel to the extension that made the emergency call.

Follow this advice only if you have fewer than 38 Emergency Location Extensions per voice server. Communication Manager software has a system limit of 38 crisis alert buttons per voice server: 10 for digital sets, and 28 for attendant consoles.

5.5.5.14.2 Reset System 2

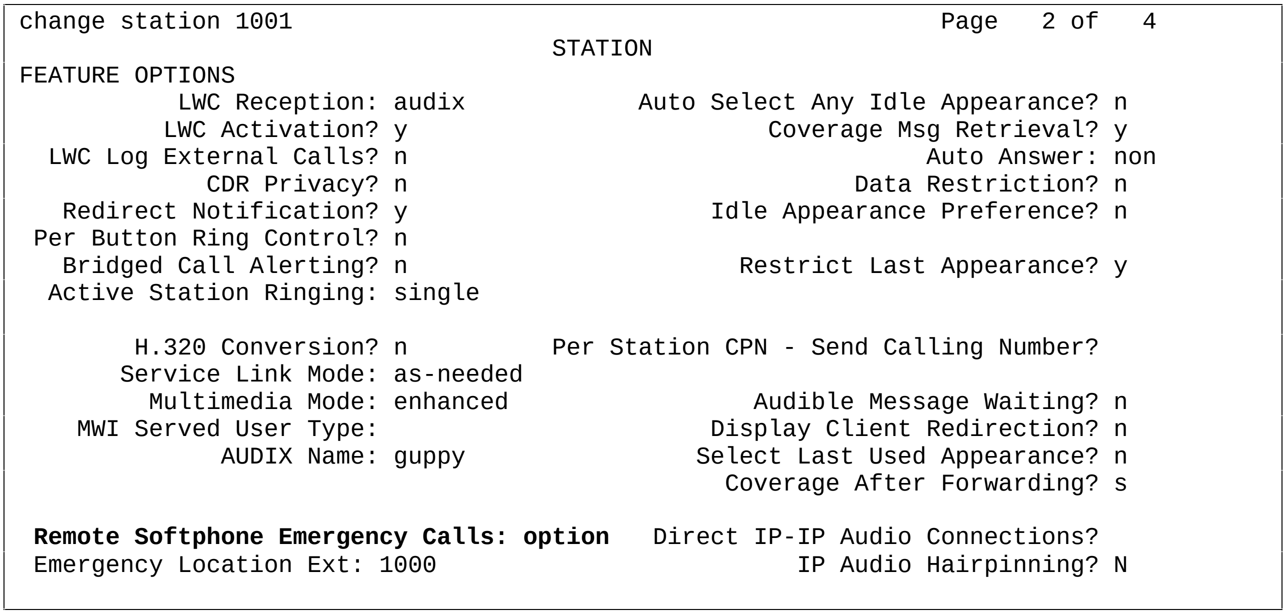
Timers are stopped by a reset system 2, but call forwarding is not erased by a reset system 2. If the switch should do a reset system 2 while the Emergency Extension Forwarding timer is running, the Emergency Extension forwarding would stay in effect until the Emergency Location Extension's call forwarding was manually cancelled by a user. That is another reason to give Emergency Location Extension sets a call forwarding button.

5.5.5.15 Unanswered Calls & Forwarding

Communication Manager software does not set up emergency location extension forwarding if the emergency call fails. However, failure or success is determined at the time the Communication Manager voice server does a trunk seizure. If someone dials 911 and then hangs up before the PSAP officer answers, emergency location extension forwarding would still be set up, even though the PSAP will probably never call back.

5.6. Remote Softphone Emergency Calls Field

The previous section 5.5, pages 63 through 77, describes how Communication Manager software automatically assigns a CPN based on the phone's IP address. However, as pointed out in section 4.6.2 on page 34, there may be times when a softphone running on a laptop PC is connected from a remote location via a modem. In such situations, the softphone's IP address is not really useful for determining where the phone actually is. To handle these situations, Communication Manager software provides a field on the station form, "Remote Softphone Emergency Calls".



```
change station 1001                                             Page   2 of   4
                                     STATION
FEATURE OPTIONS
           LWC Reception: audix           Auto Select Any Idle Appearance? n
          LWC Activation? y                        Coverage Msg Retrieval? y
  LWC Log External Calls? n                                   Auto Answer: non
             CDR Privacy? n                              Data Restriction? n
   Redirect Notification? y                  Idle Appearance Preference? n
 Per Button Ring Control? n
   Bridged Call Alerting? n                    Restrict Last Appearance? y
  Active Station Ringing: single

        H.320 Conversion? n          Per Station CPN - Send Calling Number?
       Service Link Mode: as-needed
         Multimedia Mode: enhanced                Audible Message Waiting? n
     MWI Served User Type:                       Display Client Redirection? n
              AUDIX Name: guppy                 Select Last Used Appearance? n
                                                  Coverage After Forwarding? s

 Remote Softphone Emergency Calls: option   Direct IP-IP Audio Connections?
 Emergency Location Ext: 1000                          IP Audio Hairpinning? N
```

5.6.1. Block

Section 4.6.2 on page 34 described one use of the field, when the softphone is not anywhere near the enterprise's network.

5.6.2. CESID

Another use for the field occurs when the softphone is physically in the area covered by the enterprise's voice server, but the softphone is dialing in via modem. There is no correlation between the softphone's IP address and the softphone's current street address. In this case, the 911 call would reach the correct PSAP, but it is up to the user to supply the correct calling party number at the time the softphone is configured. This feature is mainly useful if the user has two phones: a telephone at the office, and a softphone mostly used at home.

If the phone user places a call with ARS call type "emer" or "alert", and if:

- the "Remote Softphone Emergency Calls" field on the station form is set to "cesid" or,
- the "Remote Softphone Emergency Calls" field on the station form is set to "option" and the IP softphone user has selected "Settings, Login Settings, Emergency, Enable Emergency Call Handling, Telephone Number", the switch will send to the CO the telephone number supplied by the IP Softphone user. If the media server or switch uses ISDN trunks for emergency calls, the number should be a local direct-dial number with the local area code, at the physical location of the IP Softphone. If the media server or switch uses CAMA trunks for emergency calls, the phone user should enter a specific digit string for the IP Softphone location, based on advice from the local emergency response personnel.

From Multivantage Release 9.5 through Communication Manager release 1.3, this field was called "IP Emergency Calls". It is only used for softphones.

5.6.3. As-on-local

The third use for the "Remote Softphone Emergency Calls" field is when the user has a softphone used mostly at the office. If users ever walk around the building with a laptop PC, they would like for the automatic device location feature described in section 5.4 on page 52 to apply to the softphone. The field's key word "as-on-local" tells Communication Manager software to treat the softphone the same way it would treat any other IP phone on the Local Area Network.

5.6.4. Option

Sometimes the system administrator will not know in advance what a Softphone user plans to do. For example, a user may have an IP Telephone on his desk at the office, and an IP Softphone at home. As stated earlier in section 5.6.2 on page 78, ordinarily this user's "Remote Softphone Emergency Calls" field would be set to "cesid". But what if this phone user occasionally brings a laptop PC into the office, and runs Softphone on the PC, with the PC plugged into a LAN jack in one of several conference rooms? If the phone user could be trusted to enter into the softphone the correct telephone number for the conference room, everything would be fine. However, the site may be using CAMA trunks and the correct number to enter for the conference room may not be obvious. It may be safer to set the "Remote Softphone Emergency Calls" field on the station form to "option" and have the phone user select:

- "Settings, Login Settings, Emergency, Enable Emergency Call Handling, Telephone Number" when he is at home, and
- "Settings, Login Settings, Emergency, Enable Emergency Call Handling, Your Extension Number" when he is at the office. This setting on the softphone will apply the user's extension number when the softphone is in the user's office, and apply the automatic device location feature described in section 5.4 on page 52 when the softphone is plugged into the LAN away from the office, for example in one of those conference rooms.

5.6.5. A Mixture Of The Three

Softphone users are sometimes unpredictable. For example, suppose a user says he will always use his IP Softphone from his desk. The system administrator accordingly administers the "Remote Softphone Emergency Calls" field to "as-on-local" instead of "option". Suppose one day the user enters a number into softphone's menu: "Settings, Login Settings, Emergency, Enable Emergency Call Handling, Telephone Number", then dials the softphone into the LAN remotely, via a modem, and tries to register.

These kinds of unanticipated behavior can happen. The following table shows what would happen under all possible differences of settings between the endpoint's settings and the Communication Manager server's administration. In the following table, * means any value.

1. The phone is a softphone
2. The phone is not a softphone

A. "Remote Softphone Emergency Calls" = cesid, or option and the softphone requested the cesid option.
B. "Remote Softphone Emergency Calls" = block, or option and the softphone requested the block option,
C. "Remote Softphone Emergency Calls" = as-on-local, or option and the softphone requested the extension option.

I. The Station form's emergency location extension equals the ip-network-map form's emergency location extension, and the latter is not blank.
II. The Station form's emergency location extension does not equal the ip-network-map form's emergency location extension, and the latter is not blank.
III. The ip-network-map form's emergency location extension is blank.

Conditio n	Communication Manager software response	Circumstances under which this is likely to happen.
1, A, *	Use the offered cesid.	The user has both an IP telephone and a Softphone. Usually the softphone dials in from an adjacent area code via ppp, but today is in the same subnet as the IP Telephone.
1, B, *	Block the emergency call.	The user has both an IP telephone and a Softphone. Usually the softphone dials in from across the country via ppp, and did so today.
1, C, I	Use the extension.	The user has an IP softphone on the LAN, and has not moved it to a different subnet.
1, C, II	Use the ip-network-map form's Emergency Location Extension.	The user has an IP softphone, and has moved it to a different subnet on the LAN.
1, C, III	Use the station form's Emergency Location Extension.	The user has an IP softphone. It usually connects to the LAN but today is dialed in via PPP.
2, *, I	Use the extension.	The user has an IP telephone on the LAN and has not moved it to a different subnet.
2, *, II	Use the ip-network-map form's Emergency Location Extension.	The user has an IP telephone, and has moved it to a different subnet on the LAN.

Conditio n	Communication Manager software response	Circumstances under which this is likely to happen.
2, *, III	Use the station form's Emergency Location Extension.	The user's extension is not known to the ALI database. Usually the user dials in a softphone via ppp, but today is using an IP telephone dialed in via ppp.

5.7. Making Test Emergency Calls

Someone could accuse Communication Manager software of failing and causing a 911 problem. If this happened, there would be no way to check on exactly what CPN digits were sent to the emergency services network at the time of the emergency.   However, a services person could later place a test call and then check the entries in list trace station or list mst commands to see exactly what digits are sent as the calling party number under the same circumstances. One could place a test call to 911, but only with agreement of the PSAP staff in advance. They are there to handle emergencies, not to test telephone equipment.

5.7.1. Test Call To An Extension, Via Loop Around Trunks

A safer way to test the CPN to be sent is to administer into ARS digit analysis another digit string, besides 911, as having call type 'emer'. Any digit string not likely to be dialed by an end user will do.

```
change ars analysis 1                                           Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location:     2          Percent Full:    6

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    11                    2    2     2        emer         n
    811                   3    3     8        emer         n
    911                   3    3     2        emer         n
```

Administer the test digit string's route pattern to go to a different trunk group than the one used for real emergency calls.

If you are using ISDN trunks to handle emergency calls, you can set up an outgoing ISDN trunk that loops around, coming back into the Communication Manager server as an incoming ISDN trunk. Then administer the "Number of Deleted Digits" field and the "Inserted Digits" field to make the call terminate at a pre-determined extension. For example, the following route pattern will cause a call to "811" to terminate at extension 88888.

```
change route-pattern 8                                            Page   1 of   1
                            Pattern Number: 8

   Grp. FRL NPA Pfx Hop Toll No.  Inserted                              DCS/ IXC
   No.          Mrk Lmt List Del  Digits                                QSIG
                             Dgts                                       Intw
1:  8   1  303  1   1    1   3     88888                                n   user
```

Place a test call to the test emergency digit string you set up, and read the calling party number on the called set's display. That is the calling party number the PSAP would have received if a real 911 call had been placed.

If you are using CAMA trunks to handle emergency calls, this technique can not apply, because the Communication Manager server does not provide an inbound CAMA trunk interface. While you could purchase inbound CAMA trunk handling equipment, the same as used by PSAPs, you may not want that trouble or expense just to test your emergency call handling administration. You can use a variant of it, however. Apply the above technique, but route the call out a non-CAMA loop around trunk capable of signaling the calling party number. The following trunks are capable of signaling calling party numbers, in addition to ISDN and CAMA already mentioned: DCS, ATM CES, H.323, and SIP. Once you see the calling party number sent over the other trunk type, compare it to the entries in the cama-numbering form to see what would have been sent over a CAMA trunk.

5.7.2. Test Call, Monitoring Trunk Signaling

If you do have permission from the local PSAP to make real test calls to them, or if you have learned from the local public network service provider of a test digit string that can be safely dialed out an ISDN or CAMA trunk without causing the call to route to the PSAP, another technique is to monitor the digits sent out the trunk. There are two methods of doing this: "list trace station", and "message sequence trace". List trace station is easier, but it does not work for CAMA trunks.

5.7.2.1 List Trace Station

The actual string of digits sent to the emergency services network as the ISDN CPN are displayable via list trace station. Run the command immediately prior to placing the test emergency call.

```
List trace station 25112

                                LIST TRACE

time            data

10:58:44     active station    25112 cid 0x1c3a
10:58:56     dial 9911
10:58:56     route-pattern  47 preference 1  cid 0x1c3a
10:58:56     term trunk-group 12    cid 0x1c3a
10:58:56     dial 9911
10:58:56     seize trunk-group 12 member 2  cid 0x1c3a
10:58:56     Setup digits 911
10:58:56     Calling party 3035385112
10:59:07     idle station    25112 cid 0x1c3a
```

The list trace station command does not require setup prior to running the command. The list trace station command does not show digits sent to the emergency services network over CAMA trunks.

5.7.2.2 List MST

The actual string of digits sent to the emergency services network as the CAMA CESID or the ISDN CPN are displayable via message sequence trace, although they are displayed in hex. To do so requires some prerequisite administration.

For ISDN, set up filters to monitor only calls from a particular station UID, and only for dialed digits 911. Monitor all D-channels with this filter, and read the CPN, which will be written in hexadecimal number. However, it is probably better to avoid MST for this and just use the "list trace station" command, because the command requires no preliminary setup and displays the result in decimal numbers.

For CAMA, set up the same filter, and monitor the CCMS downlinks to trunk boards. From the SAT form:
"change MST" and set the field "CCMS" to "Y".
"enable MST"
"clear MST"

The following downlink message "TND_UPD" shows the digits outpulsed over the CAMA trunk; in this example they are 303 537 8020.

```
list mst

                           MESSAGE SEQUENCE TRACE DATA

Number    Date/Time     Type            Message

   230    12:23:48.240  31 00001c00 <-- TND_UPD    mfc tone dialing
            | 00 00 1c 00 01 01 15 1c 09 20 c1 8f 0d 01 02 03 03 0a 03 05 03
            | 07 08 0a 02 0a 0f
```

6. Other

6.1. Bridging

When a bridged appearance places an emergency call via ARS, and ARS digit analysis classifies the call as call type "emer" or "alrt":

- The location number used to route the call is the location of the physical phone placing the call.
- The CPN sent to the CO belongs to the physical set containing the bridged appearance. The Emergency Location Extension feature described in section 5 starting on page 38 does apply to the physical set's extension.
- The extension number displayed to the attendant and to digital sets with crisis alert buttons is the principal's extension, i.e., the extension number of the bridged appearance rather than the extension number of the physical set holding that appearance.

Suppose a softphone has a bridged appearance of another set, and a user places an emergency call from the bridged appearance on the softphone. In this case the calling softphone's Remote Softphone Emergency Calls setting {as-on-local, nearby, cesid, block, or option} does apply. If the selected emergency call handling option is "as-on-local" and the softphone is in its own subnet, the extension sent is the calling softphone's extension, not the principal set's extension. This is true even if the principal extension itself is another softphone.

6.2. EAS Agent

If a logged-in EAS agent dials an emergency call:

- The location number used to route the call is the location of the physical phone placing the call.

- The CPN sent to the CO depends on administration on the agent-loginID form.

```
add agent-loginID next                                            Page   1 of   2
                                 AGENT LOGINID

                Login ID: 2000                                      AAS? n
                    Name:                                         AUDIX? n
                      TN: 1                               LWC Reception: spe
                     COR: 1                         LWC Log External Calls? n
           Coverage Path:                         AUDIX Name for Messaging:
           Security Code:
                                                  LoginID for ISDN Display? n
```

LoginID for ISDN Display: Y means the "Agent LoginID CPN and Name" field is to be included in ISDN messaging over ISDN trunks. N means the physical station extension CPN and Name is sent over ISDN trunks.

- The extension number displayed to the attendant and to digital sets with crisis alert buttons is the agent's ID.

If a logged-in EAS agent dials an emergency call and the call drops, the return call from the PSAP is forwarded to the physical station that dialed 911, not to the EAS agent ID. If an agent EAS dials 911, hangs up, then walks to a nearby phone and logs in, the return call from the PSAP would still ring the original phone that dialed 911.

6.3. Shared Control

If a telephone endpoint and an IP softphone are sharing control of an extension number, i.e. they are both simultaneously in service on the same extension, Communication Manager software will treat emergency calls from the softphone as if they were from the telephone endpoint.

- The multiple location number of a softphone in the Shared Control configuration is the location of the telephone endpoint.
- The Remote Softphone Emergency Calls feature described in section 4.6.2 on page 34 and in section 5.6 on page 77 does not apply.

6.4. Telecommuter Softphone

If a telephone endpoint is providing audio for an IP softphone in telecommuter mode, Communication Manager software will treat emergency calls from the softphone as if they were from the softphone, not from the telephone.

- The multiple location number of a softphone in the Telecommuter configuration is the location of the softphone endpoint.
- The Remote Softphone Emergency Calls feature described in section 4.6.2 on page 34 and in section 5.6 on page 77 does apply.

If you are using a softphone in telecommuter configuration and you wish to dial 911, it is better to dial 911 through the telephone's keypad than through the softphone user interface. The telephone is almost always going to route the call to the correct PSAP and send to the PSAP a CPN corresponding to your precise street address. The only exception might be if the telephone itself is remotely connected to the Communication Manager server, for example via DEFINITY Extender or via dialing through a trunk acting as an extension. The following section 6.5 on page 86 discusses this.

6.5. Trunks Acting As Extension

There are a few cases where a trunk can act as if it were an extension. If such an extension dials 911 and Communication Manager software sends a corresponding Emergency Location Extension number as the CPN, there may not be a physical telephone set to forward calls to. However, there is an extension number corresponding to the person who dialed 911.

- A typical pre-OPTIM wireless user has both a wireless phone (xmobile or 9601) and a DCP station set. The DCP station set has no call appearances of its own, only bridged appearances of the wireless extension number. When a user within the building served by a Communication Manager server places a PSTN call using the wireless phone, the call is picked up by an in-building wireless system. The system routes the call into the Communication Manager server through an incoming tie trunk for xmobile or through the TN789B Radio Controller for 9601. The Communication Manager server then routes the call to the PSTN, treating the call as if it had come from the wireless extension.

- A typical line side DS1 user has an analog phone connected to a multiplexer connected to a DS1 trunk connected to a Communication Manager server. When a user of such a phone places a PSTN call, the call routes into the Communication Manager server through an incoming DS1 tie trunk. The Communication Manager server then routes the call to the PSTN, treating the call as if it had come from the line side extension. The line side DS1 station types are {ds1fd, ds1sa, ops, vrufd, or vrus}.

- A typical OPTIM user has both a wireless phone and a telephone station set. When a user calls into a Communication Manager server via an incoming ISDN trunk or a SIP trunk, Communication Manager software compares the calling party number provided by the incoming trunk call with a table of OPTIM calling party numbers and associated OPTIM extensions. If Communication Manager software finds a match, Communication Manager software then routes the call to the PSTN, treating the call as if it had come from the associated extension.

- A typical remote access user has a telephone set, but can dial into the remote access extension from the PSTN, enter an extension number and security code, and then place calls as if from the extension.

6.5.1. Location

For Communication Manager 1.3 software, the location of a trunk acting as an extension is the location of the trunk circuit pack.

- For non-IP trunks, this is the location of the cabinet containing the trunk circuit pack.
- For IP trunks, this is the location of the cabinet containing the CLAN circuit pack carrying the signaling for the trunk. If the signaling is being carried by a gateway instead of by a CLAN circuit pack, the location of the gateway applies.

6.5.2. Calling Party Number

The CPN used for a call placed by a trunk acting as an extension is the associated extension number.

6.5.3. Emergency Location Extension Forwarding

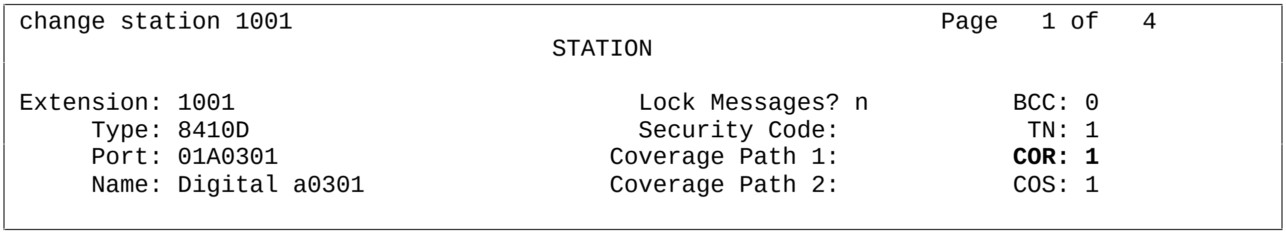
Emergency Location Extension forwarding does work for 911 calls placed from trunks acting as extensions. If an emergency call was placed from a trunk acting as an extension, the return incoming trunk call from the PSAP will ring at the extension that placed the emergency call. If that extension is a directly connected telephone, the return call rings as a priority call. If that extension is a cellular phone, the return call is not a priority call because the cellular network does not carry Communication Manager's priority call signaling.

6.6. Calling Permissions

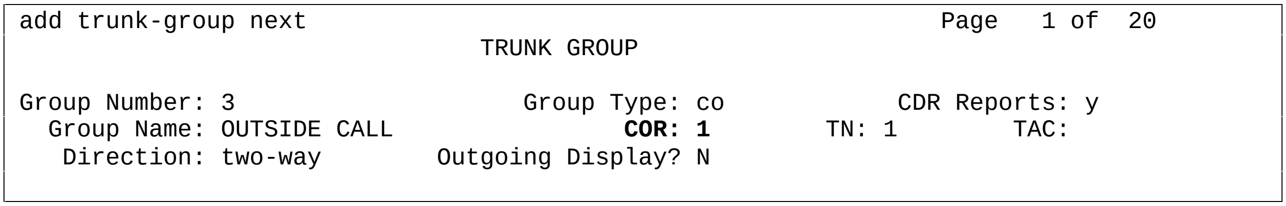
6.6.1. Class Of Restriction (COR)

Class of Restriction (COR) defines many different classes of call origination and termination privileges. Communication Manager software may have no restrictions, only a single COR, or may have as many classes of restrictions as necessary to effect the desired restrictions. Many different types of classes of restriction can be assigned to many types of facilities on the switch. Your system may use only one COR or as many as necessary to control calling privileges. You can assign up to 96 different CORs (0 – 95).

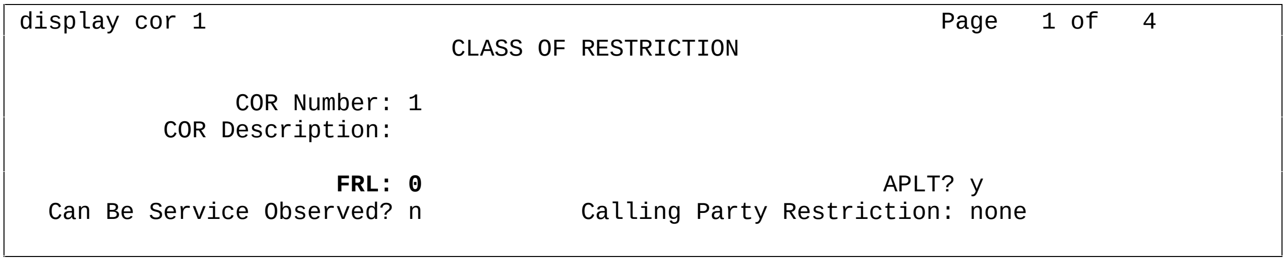
CORs are capable of blocking emergency calls. You should administer COR permissions so all CORs can reach at least one public network trunk group.



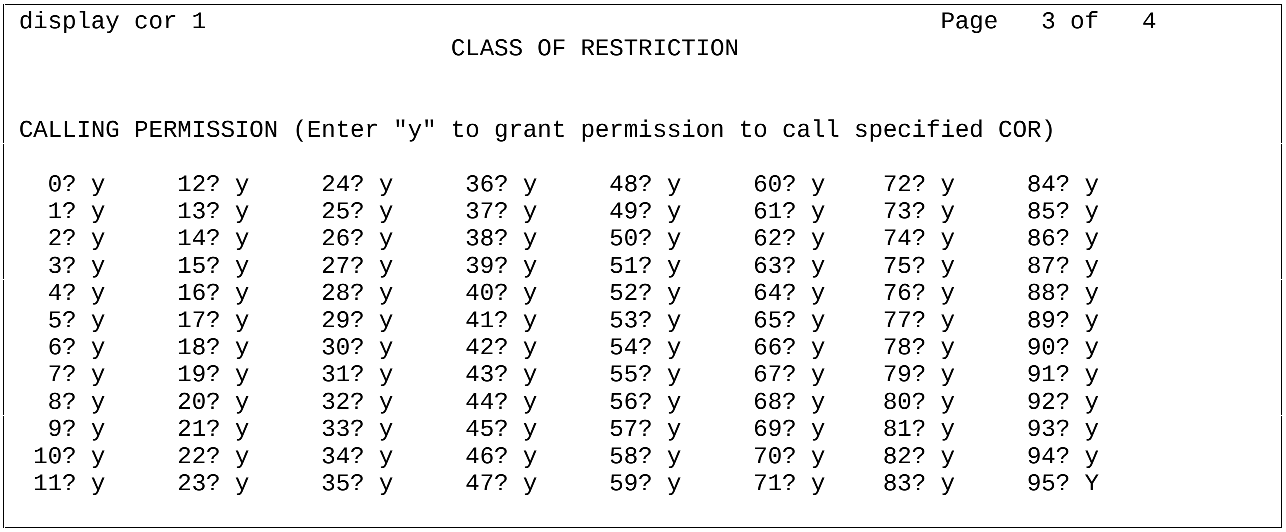
```
change station 1001                                           Page   1 of   4
                                     STATION

Extension: 1001                           Lock Messages? n          BCC: 0
     Type: 8410D                          Security Code:             TN: 1
     Port: 01A0301                      Coverage Path 1:            COR: 1
     Name: Digital a0301                Coverage Path 2:            COS: 1
```



```
add trunk-group next                                          Page   1 of  20
                                TRUNK GROUP

Group Number: 3                   Group Type: co           CDR Reports: y
  Group Name: OUTSIDE CALL               COR: 1        TN: 1        TAC:
   Direction: two-way       Outgoing Display? N
```



```
display cor 1                                                 Page   1 of   4
                               CLASS OF RESTRICTION

               COR Number: 1
          COR Description:

                      FRL: 0                                 APLT? y
  Can Be Service Observed? n           Calling Party Restriction: none
```



```
display cor 1                                                 Page   3 of   4
                               CLASS OF RESTRICTION


CALLING PERMISSION (Enter "y" to grant permission to call specified COR)

  0? y     12? y     24? y     36? y     48? y     60? y    72? y     84? y
  1? y     13? y     25? y     37? y     49? y     61? y    73? y     85? y
  2? y     14? y     26? y     38? y     50? y     62? y    74? y     86? y
  3? y     15? y     27? y     39? y     51? y     63? y    75? y     87? y
  4? y     16? y     28? y     40? y     52? y     64? y    76? y     88? y
  5? y     17? y     29? y     41? y     53? y     65? y    77? y     89? y
  6? y     18? y     30? y     42? y     54? y     66? y    78? y     90? y
  7? y     19? y     31? y     43? y     55? y     67? y    79? y     91? y
  8? y     20? y     32? y     44? y     56? y     68? y    80? y     92? y
  9? y     21? y     33? y     45? y     57? y     69? y    81? y     93? y
 10? y     22? y     34? y     46? y     58? y     70? y    82? y     94? y
 11? y     23? y     35? y     47? y     59? y     71? y    83? y     95? Y
```

If you wish to allow a station to dial 911 but not other destinations, you can administer a low Facility Restriction Level (FRL) to the station's COR. 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.

So, to allow 911 calls but prevent all other PSTN calls, assign to the 911 route pattern a FLR of 0, and assign to all other route patterns an FRL of 1 or higher. Assign an FRL of 0 to the station you wish to restrict, and assign to all other stations an FRL of 1 or higher.

```
change route-pattern 2                                          Page   1 of   1
                            Pattern Number: 2

   Grp. FRL NPA Pfx Hop Toll No.  Inserted                            DCS/ IXC
   No.          Mrk Lmt List Del  Digits                              QSIG
                             Dgts                                     Intw
 1:  2   0  303  1   1    1   0                                        n   user
```

6.6.2. Tenant

Tenant partitioning allows partitioning of the system in order to restrict the system's services and features to groups of endpoints called tenants. This provides attractive services and revenue for virtual landlords. It provides the robust features of a large system at affordable rates to small business tenants. Communication Manager software supports these numbers of tenants:

Platform	CSI	S8100	SI	S8300	S8500	R	S8700
Tenants	20	20	20	20	100	100	100

Multiple attendant groups can be assigned to each partition. Stations, hunt groups, and other endpoints assigned to a Class of Service (COS) can be partitioned. Network route pattern preferences also support the assigned tenant partitioning. Tenant partitioning also allows you to assign a unique music source for each tenant partition for callers who are put on hold.

Tenant restrictions are capable of blocking emergency calls. You should administer tenant permissions so that all tenant stations can reach at least one public network trunk group.

```
change station 1001                                             Page   1 of   4
                                     STATION

Extension: 1001                         Lock Messages? n          BCC: 0
     Type: 8410D                        Security Code:             TN: 18
     Port: 01A0301                    Coverage Path 1:            COR: 1
     Name: Digital a0301              Coverage Path 2:            COS: 1
                                      Hunt-to Station:
```

```
add trunk-group next                                               Page   1 of  20
                                TRUNK GROUP

Group Number: 3                    Group Type: co           CDR Reports: y
  Group Name: OUTSIDE CALL                COR: 1        TN: 1        TAC:
   Direction: two-way        Outgoing Display? N

```

```
change tenant 18
                        Tenant 18
              Tenant Description: New York
                 Attendant Group: 2
           Ext Alert Port (TAAS): x       Ext Alert (TAAS) Extension: 2001
               Night Destination: 2000
                    Music Source: 2
         Attendant Vectoring VDN:
                Emergency Number:
```

```
change tenant 18
                        Tenant 18

CALLING PERMISSION (Enter y to grant permission to call specified Tenant)

  1? y  11? n  21? n  31? n  41? n  51? n  61? n  71? n  81? n   91? n
  2? n  12? n  22? n  32? n  42? n  52? n  62? n  72? n  82? n   92? n
  3? n  13? n  23? n  33? n  43? n  53? n  63? n  73? n  83? n   93? n
  4? n  14? n  24? n  34? n  44? n  54? n  64? n  74? n  84? n   94? n
  5? n  15? n  25? n  35? n  45? n  55? n  65? n  75? n  85? n   95? n
  6? n  16? n  26? n  36? n  46? n  56? n  66? n  76? n  86? n   96? n
  7? n  17? n  27? n  37? n  47? n  57? n  67? n  77? n  87? n   97? n
  8? n  18? y  28? n  38? n  48? n  58? n  68? n  78? n  88? n   98? n
  9? n  19? n  29? n  39? n  49? n  59? n  69? n  79? n  89? n   99? n
 10? n  20? n  30? n  40? n  50? n  60? n  70? n  80? n  90? n  100? n

```

6.6.3. Call Admission Control (CAC) Bandwidth Management

In order to ensure Quality of Service for Voice over IP calls, there is a need to limit overall VoIP traffic on WAN links. The Call Admission Control (CAC) Bandwidth Management feature of Communication Manager software allows you to specify a VoIP bandwidth limit between any pair of IP network regions. The feature denies calls carried over the WAN link if they would exceed the bandwidth limit.

Call Admission Control is capable of blocking emergency calls. You should set up routes used for emergency calls to always include at least one non-IP route to a PSTN trunk. If the calling party is an IP station this may not be possible, but if the calling party is a set behind an IP remoted gateway, this can be accomplished by putting at least one PSTN trunk on the gateway.

6.7. Automatic Callback

You can administer your system to call users back if they try to place an outgoing call over a trunk group while all trunks are busy. This is sometimes called Ringback Queuing. If a multiappearance telephone user has an idle Automatic Callback button (auto-cback) and tries to access an all-trunks-busy trunk group, the call is queued automatically. The lamp associated with the Automatic Callback button (auto-cback) lights and confirmation tone is heard. Ringback Queuing is automatic for a single-line telephone with the Auto Callback class of service.

```
change cos
                                CLASS OF SERVICE

                                0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15
 Auto Callback                  y  y  y  y  y  y  y  y  y  y  y  y  y  y  y  y
 Call Fwd-All Calls             n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Data Privacy                   n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Priority Calling               n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Console Permissions            n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Off-hook Alert                 n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Client Room                    n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Restrict Call Fwd-Off Net      n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
```

After dialing is complete, the user hears confirmation tone if the queue is available. No action is required. The system will queue as many calls as allowed based on the "Queue Length" field on the each trunk-group form.

```
change trunk-group 1                                           Page   1 of  10
                                TRUNK GROUP

Group Number: 1                    Group Type: isdn          CDR Reports: y
  Group Name: QSIG loopback 2 c18         COR: 1        TN: 1        TAC: 101
   Direction: two-way       Outgoing Display? y         Carrier Medium: PRI/BRI
 Dial Access? n               Busy Threshold: 1         Night Service:
Queue Length: 9
Service Type: tie                   Auth Code? n            TestCall ITC: rest
                         Far End Test Line No:
TestCall BCC: 4
TRUNK PARAMETERS
         Codeset to Send Display: 6     Codeset to Send National IEs: 6
        Max Message Size to Send: 260   Charge Advice: none
  Supplementary Service Protocol: b     Digit Handling (in/out): enbloc/enbloc

            Trunk Hunt: cyclical
                                                   Digital Loss Group: 13
         Calling Number - Delete:___ Insert: _______________  Format: ________
              Bit Rate: 1200         Synchronization: async    Duplex: full
 Disconnect Supervision - In? y  Out? n
 Answer Supervision Timeout: 0
```

If you have remote offices with relatively few public network trunks available for 911 calls, you may want to administer those trunk groups to use automatic callback (ringback queuing), and administer the stations to use automatic callback. If someone is trying to place a 911 call and all trunks are in use, the caller will get through as soon as possible. However, for really small remote offices, this feature may not provide much additional value. If someone in a really small office could not get an available trunk for an emergency call, all they would have to do is scream. Everyone else in the office would hear the scream, hang up, and come running. This would free the busy trunks.

6.8. NI-BRI Sets Can Not Hold 911 Calls

Section 3.6 of the National BRI standard, GR-858-CORE, says 911 calls should not be held, conferenced, or transferred if the calling set is an NI-BRI set. Communication Manager software follows this standard for these NI-BRI sets, but allows these features if the calling party is any other type of set. Reasonable arguments could be made for both types of operation.

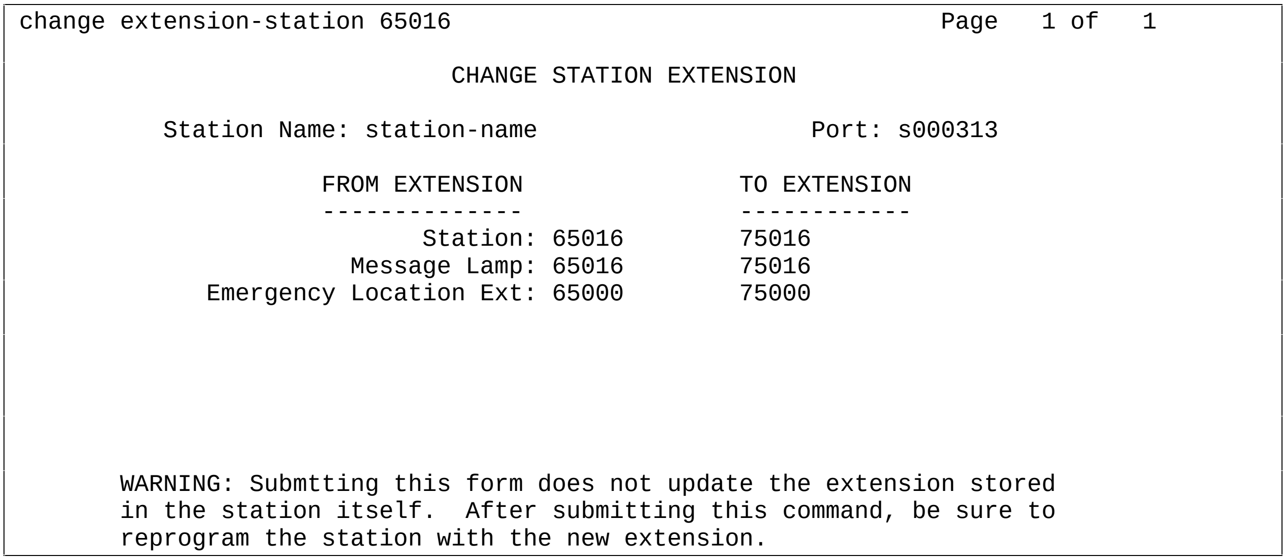
- If the phone user happens to have the call on hold when the PSAP officer answers, the PSAP officer would hear silence or music on hold. The officer may misinterpret those to mean the caller can not speak, or is playing a practical joke.
- If the phone user makes a mistake while trying to use the transfer or conference features, the user may accidentally drop the call.

- A phone user has an emergency, and calls the building security. Building security listens to the user's story, and decides it is a more severe emergency than building security can handle. Building security conferences in 911 or transfers the call to 911.
- Phone user A is on a call with user B when user A suffers a stroke. User A can no longer dial, but can still talk. User A tells B to call 911. B conferences in 911, or transfers the call to 911.

Communication Manager software determines whether to apply this hold, conference, and transfer restriction to all calls with ARS call type emer or alrt based on the station set type, NI-BRI, administered on the station form.

6.9. Changing Extension Numbers

The change extension-station command allows an administrator to change extensions on the switch from one extension to another all at once. When the screen is filled out and submitted, all administration that was associated with the current extension will now be associated with the new extension. Any administration references of the extension being changed, such as references used in a vector, coverage, etc., will now reference the new extension. Once the extension has been changed, all references to the previous extension will be removed from the switch.



```
change extension-station 65016                              Page   1 of   1

                            CHANGE STATION EXTENSION

          Station Name: station-name                   Port: s000313

                     FROM EXTENSION              TO EXTENSION
                     --------------              ------------
                            Station: 65016       75016
                       Message Lamp: 65016       75016
             Emergency Location Ext: 65000       75000




       WARNING: Submtting this form does not update the extension stored
       in the station itself.  After submitting this command, be sure to
       reprogram the station with the new extension.
```

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

Emergency Location Extension: The Emergency Location Extension from the Station screen associated with the current extension is displayed under “From Extension.” Type a new extension for the Emergency Location Ext. field that will appear on the Station screen, up to seven numbers that make up a valid extension number for your dial plan.

6.10. Emergency Calling Outside The USA

The Universal Emergency Number, i.e. the equivalent of 911 in the USA, is 000 in Australia, and 112 in the European Community.

6.10.1. Emergency Location Extension Forwarding

Even in countries where emergency response personnel do not have the ability to look up street addresses via an ALI database, there would still be some value in setting the Emergency Extension Forwarding timer to a non-zero number. If an emergency call should drop, the return call from the public safety agency would at least ring as a priority call while the timer is running. This increases the chance the return call will be answered by the person who called in the emergency instead of being answered by voice mail.

6.10.2. Spain

Communication Manager software, when used with Spain E1 CO trunks, has a feature called Call Retention. Call Retention holds a trunk active when an emergency number has been dialed even though the station user may attempt to drop the call. If the station user does go on hook with an emergency call still active, the trunk is kept active, and an Operator Services signal is sent to the Central Office. If the station user then goes off-hook again, the user is reconnected to the call instead of being provided dial tone, and the Operator Services signal is no longer sent. For this feature, an emergency call is one defined in the ARS administration as an "emer" call type.

Attendants support this feature, with one exception. They must press the loop to be reconnected to the trunk carrying the emergency call, rather than automatically be reconnected upon going off-hook. There is one exception. Since the "forced release" button on the attendant console is intended as a bail out action, Communication Manager software does drop the trunk upon a forced release.

To use this feature, administer an E1 trunk with the Spain country code, 11.

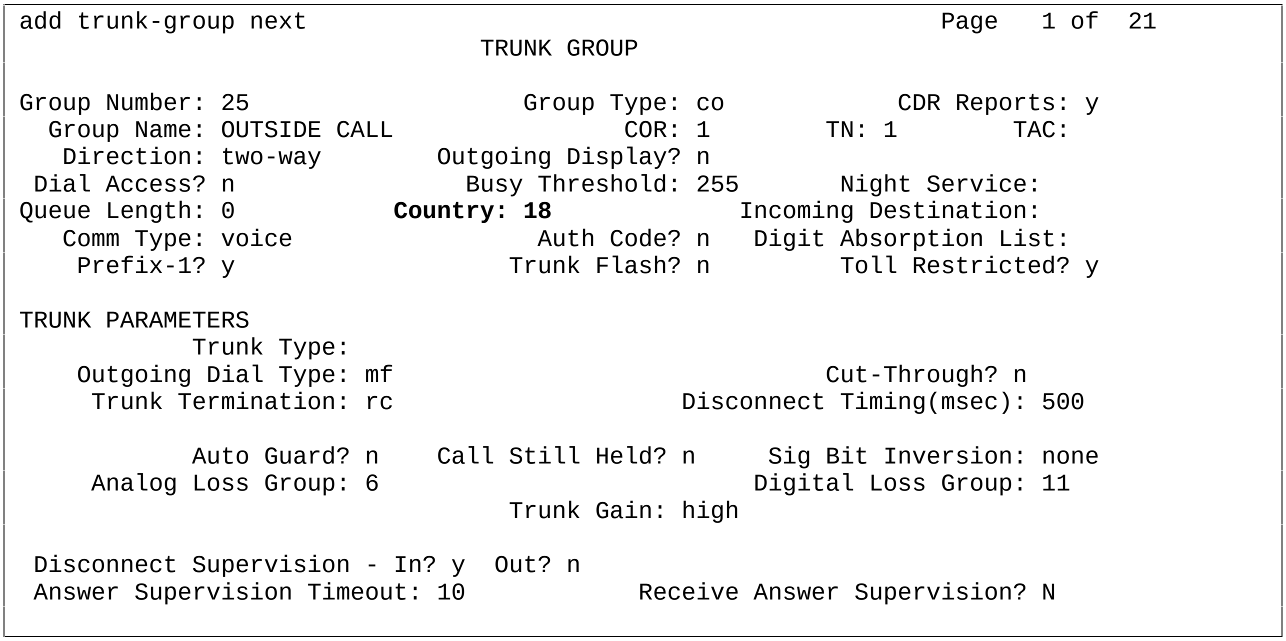
```
add trunk-group next                                            Page   1 of  21
                                TRUNK GROUP

Group Number: 25                  Group Type: co            CDR Reports: y
  Group Name: OUTSIDE CALL               COR: 1        TN: 1        TAC:
   Direction: two-way       Outgoing Display? n
 Dial Access? n               Busy Threshold: 255       Night Service:
Queue Length: 0          Country: 11            Incoming Destination:
   Comm Type: voice                Auth Code? n   Digit Absorption List:
    Prefix-1? y                  Trunk Flash? n         Toll Restricted? y

TRUNK PARAMETERS
            Trunk Type:
    Outgoing Dial Type: tone                             Cut-Through? n
     Trunk Termination: rc                   Disconnect Timing(msec): 500

            Auto Guard? n    Call Still Held? n     Sig Bit Inversion: none
     Analog Loss Group: 6                          Digital Loss Group: 11
                                  Trunk Gain: high

 Disconnect Supervision - In? y  Out? n
 Answer Supervision Timeout: 10           Receive Answer Supervision? N
```

```
add ds1                                                             Page 1 of 2
                             DS1 CIRCUIT PACK
            Location: 01A13                          Name: _______________
            Bit Rate: 2.048                   Line Coding: cmi
      Signaling Mode: CAS
        Interconnect: co
                                          Country Protocol: 11
```

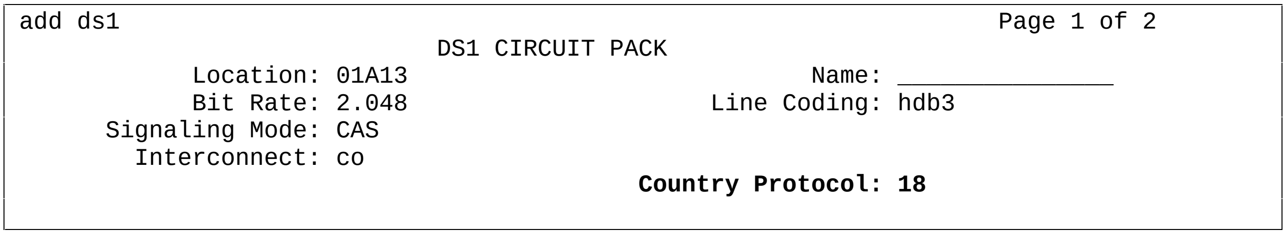
6.10.3. China

Communication Manager software, when used with China Number 1 multifrequency signaling trunks, has a feature, Called Party Control. Called Party Control holds a trunk active when an emergency number has been dialed even though the voice server user may attempt to drop the call. If the station user does go on hook with an emergency call still active, the trunk is kept active. If the station user then goes off-hook again, the user is reconnected to the call instead of being provided dial tone. For this feature, an emergency call is one defined in the ARS administration as an "emer" call type. Attendants do not support this feature.

To use this feature, administer a multifrequency signaling E1 trunk with the China country code, 18.



```
add trunk-group next                                            Page   1 of  21
                                TRUNK GROUP

Group Number: 25                   Group Type: co            CDR Reports: y
  Group Name: OUTSIDE CALL                COR: 1        TN: 1        TAC:
   Direction: two-way        Outgoing Display? n
 Dial Access? n                Busy Threshold: 255       Night Service:
Queue Length: 0           Country: 18             Incoming Destination:
   Comm Type: voice                 Auth Code? n   Digit Absorption List:
    Prefix-1? y                   Trunk Flash? n         Toll Restricted? y

TRUNK PARAMETERS
            Trunk Type:
    Outgoing Dial Type: mf                              Cut-Through? n
     Trunk Termination: rc                    Disconnect Timing(msec): 500

            Auto Guard? n    Call Still Held? n     Sig Bit Inversion: none
     Analog Loss Group: 6                          Digital Loss Group: 11
                                  Trunk Gain: high

 Disconnect Supervision - In? y  Out? n
 Answer Supervision Timeout: 10            Receive Answer Supervision? N
```



```
add ds1                                                             Page 1 of 2
                             DS1 CIRCUIT PACK
            Location: 01A13                            Name: _______________
            Bit Rate: 2.048                     Line Coding: hdb3
      Signaling Mode: CAS
        Interconnect: co
                                           Country Protocol: 18
```

7. Conclusion

Communication Manager 2.0 software has these emergency calling features:

- Crisis Alert to Attendant,

- Crisis Alert to Digital Station,
- Crisis Alert to Pager,
- Off-Hook Alert Class of Service,
- Emergency Priority Attendant Queue,
- List Emergency,
- Location Based Routing,
- ISDN Trunks,
- CAMA Trunks,
- CPN for PSA Dissociated Sets,
- Remote Softphone Emergency Calls,
- Emergency Location Extension by Station ,
- Subnet Based Device Location for IP Phones,
- Emergency Location Extension Forwarding.

Communication Manager 2.0 software also has some emergency call handling interactions with other Communication Manager features. Communication Manager 2.1 software will have additional emergency call handling features.

8. Additional References

1. Solving the Challenges of E911 Service with Avaya IP Telephony Networks, November 2002, Issue 1.1, http://www1.avaya.com/enterprise/whitepapers/lb1879.pdf
2. Overview for Avaya™ Communication Manager, Release 2.0, 555-233-767, Issue 5. November 2003, http:\\support.avaya.com\elmodocs2\comm_mgr\r2_0\245801_1_1\233767_5\233767_5.pdf.
3. Administrator's Guide for Avaya™ Communication Manager, 555-233-506, Issue 7, November 2003, http:\\support.avaya.com\elmodocs2\comm_mgr\r2_0\245801_1_1\233506_7\233506_7.pdf.
4. Administration for Network Connectivity for Avaya™ Communication Manager, 555-233-504, Issue 7, November 2003, http:\\support.avaya.com\elmodocs2\comm_mgr\r2_0\245801_1_1\233504_7\233504_7.pdf.
5. System Capacities Table for Avaya Communication Manager on Avaya Media Servers, Release 2.0, 555-233-605, 555-245-601, Issue 1.0, December 2003, http:\\support.avaya.com\elmodocs2\comm_mgr\r2_0\245601_1.pdf.

[i] DCC web site, http://www.dccusa.com/products.html, 14 October 2003.© 2003 DCC (Dialogic Communications Corporation).

[ii] RedSky web site, http://www.redskytech.com/src/03_sec/software/htm/e911_manager.htm, 14 October 2003. Copyright © 1998-2003. RedSky Technologies, Inc.

[iii] XTEND web site, http://www.xtend.com/ealert.htm, 15 October 2003. Copyright © 2003 XTEND Communications Corp.

[iv] Technical Information Document on Model Legislation, Enhanced 9-1-1 for Multi-line Telephone Systems, November 2000, Prepared by: National Emergency Number Association (NENA), ALEC/Private PBX Technical Committee, http://www.nena9-1-1.org/9-1-1_Standards_Development/TechInfoDocs/MLTS_ModLeg_Nov2000.PDF