Emergency Services Access Fundamentals
Avaya Communication Server 1000

Release 7.6
NN43001-613
Issue 06.01
March 2013

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products”. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Note to Service Provider

The Product may use Third Party Components that have Third Party Terms that do not allow hosting and may need to be independently licensed for such purpose.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third

parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: New in this release

This chapter describes what's new in this document for Avaya Communication Server 1000 Release 7.6.

Features

There are no updates to the feature descriptions in this document.

Other changes

There are no other changes.

Revision History

March 2013	Standard 06.01. This document is up-issued to support Avaya Communication Server 1000 Release 7.6.
December 2011	Standard 05.03. This document is up-issued to support the removal of End of Life (EoL) and Manufactured Discontinued (MD) hardware content and associated diagrams.
August 2011	Standard 05.02. This document is up-issued to support the removal of content for outdated features, hardware, and system types.
November 2010	Standard 05.01. This document is up-issued to support Avaya Communication Server 1000 Release 7.5.
June 2010	Standard 04.02. This document is up-issued to support Avaya Communication Server 1000 Release 7.0.
May 2009	Standard 03.01. This document is up-issued to support Communication Server 1000 Release 6.0.
November 2008	Standard 02.03. This document is up-issued to support changes in technical content in chapter Emergency Services Access for Communication Server 1000 Release 5.5.

October 2008	Standard 01.07. This document is up-issued to support changes in technical content for provisioning an ESA On-Site Notification phone for Communication Server 1000 Release 5.0.
September 2008	Standard 02.02. This document is up-issued to support changes in technical content for provisioning an ESA On-Site Notification phone for Communication Server 1000 Release 5.5.
February 2008	Standard 01.05. This document is reissued to support extensive up-issues in technical content, for Communication Server 1000 Release 5.0.
December 2007	Standard 02.01. This document is issued to support Communication Server 1000 Release 5.5.
June 2007	Standard 01.03. This document has been up-issued to reflect changes in technical content for CR Q01494694.
June 2007	Standard 01.02. This document is up-issued to remove the Confidential statement.
March 2007	Standard 01.01. This document is up-issued to support Communication Server 1000 Release 5.0. This document is renamed *Emergency Services Access Fundamentals, NN43001-613* and contains information previously contained in the legacy document, Emergency Services Access (553-3001-313), now retired.
August 2005	Standard 3.00. This document is up-issued to support Communication Server 1000 Release 4.5.
September 2004	Standard 2.00. This document is up-issued for Communication Server 1000 Release 4.0.
October 2003	Standard 1.00. This document is issued to support Succession 3.0 Software.

Chapter 2: Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to www.avaya.com or go to one of the pages listed in the following sections.

Navigation

Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to www.avaya.com/support.

Getting product training

Ongoing product training is available. For more information or to register, go to www.avaya.com/support. From this Web site, locate the Training link on the left-hand navigation pane.

Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at www.avaya.com/support.

Chapter 3: Introduction

This document is a global document. Contact your system supplier or your Avaya representative to verify that the hardware and software described are supported in your area.

Subject

This document describes the Emergency Services Access feature.

Note on legacy products and releases

This document contains information about systems, components, and features that are compatible with Avaya Communication Server 1000 software. For more on legacy products and release-specific information, click the **Documentation** link under **Support** on the Avaya home page:

www.avaya.com

Applicable systems

This document applies to the following systems:

- Communication Server 1000M Single Group (CS 1000M SG)
- Communication Server 1000M Multi Group (CS 1000M MG)
- Communication Server 1000E (CS 1000E)

Intended audience

This document is intended for individuals responsible for configuring the Emergency Services Access feature.

Conventions

Terminology

In this document, the following systems are referred to generically as "system":

- Communication Server 1000M (CS 1000M)
- Communication Server 1000E (CS 1000E)
- Meridian 1

The following systems are referred to generically as "Large System":

- Communication Server 1000M Half Group (CS 1000M HG)
- Communication Server 1000M Single Group (CS 1000M SG)
- Communication Server 1000M Multi Group (CS 1000M MG)
- Meridian 1 PBX 51C
- Meridian 1 PBX 61C
- Meridian 1 PBX 81
- Meridian 1 PBX 81C

Related information

This section lists information sources that relate to this document.

Documentation

The following technical publications are referenced in this document:

- *Avaya IP Deskphones Fundamentals, NN43001-368*
- *Avaya Features and Services Fundamentals, NN43001-106*
- *Avaya Branch Office Installation and Commissioning, NN43001-314*

Online

To access Avaya documentation online, click the **Documentation** link under **Support** on the Avaya home page:

www.avaya.com

Chapter 4: ESA Overview

Overview

Over the past few years, implementation of IP telephony has grown to a significant level of implementation, particularly for telephone systems used in private enterprises and academic institutions. IP telephony combines previously separate voice and data networks, and provides freedom from use restrictions due to distance. The new capabilities provided by IP Telephony also create a new challenge in the provision of Emergency Call Services (ECS) – determining the physical location of IP telephony clients and properly directing emergency calls. This problem also applies to traditional (non-IP) telephones in remote cabinets.

The purpose of ESA is to provide an appropriate Calling Line ID (CLID) and route an emergency call to the appropriate Public Safety Answering Point (PSAP). The CLID may be used by the PSTN to route the call, and by the PSAP to look up the caller's location, and call back the caller or a designated phone at the same location, if required.

With the growing use of IP telephony, a new challenge is presented: IP telephony clients are not hard-wired to a fixed port - they can connect to a Call Server from any point in the network, and so they are able to quickly move among different physical locations. This is a problem because location is not necessarily static – the CLID delivered for a user during an emergency call must correspond to their actual location, as much as possible, for an effective emergency response to occur. In addition, the solution should be automated, to reduce or eliminate the confusion due to moves adds or changes (MACs) resulting from client mobility.

ESA feature summary

ESA provides the solution to the challenge of providing effective emergency service response processing to mobile IP telephony clients through two asynchronous functions:

- Maintenance of an accurate and up to date knowledge of the physical location of phones.
- Processing of emergency calls made by IP telephony clients according to the current data of the caller.

Emergency location-based CLID assignment and routing is integrated with ESA, simplifying configuration.

ESA deployment options

This section provides a description of different deployment options available in the configuration of ESA.

Basic ESA

The Basic ESA deployment option is characterized as having no client mobility possible within the call environment - as such, location information is entirely static.

Optional internal location determination

With this deployment option, the capability of client mobility is present and location of connected IP telephony clients is determined by means of an optional internal Location Information Services (LIS), which works with the subnet lookup table.

Optional external location determination

With this deployment option, the capability of client mobility is present and location of connected IP telephony clients is determined by means of an external Discovery Manager (DM). An External DM interfaces with the Avaya Communication Server 1000 to keep the location data of an IP telephone up to date.

Location resolution with this deployment option can be obtained to the specific Ethernet port of the emergency caller (or to the Wireless Access Point (WAP) for wireless IP phones), using L2 port mapping technology or any other location determination technology implemented by the Discovery Manager.

Even when using the external location determination deployment option (with an External DM), emergency call processing remains entirely on the Call Server for maximum effectiveness.

Concepts and principles

This section describes the concepts and principles underlying the design and implementation of the Emergency Services Access feature.

Conveying information to the PSAP

When an emergency call is placed, the only information passed to the Public Safety Answering Point (PSAP) is CLID (ANI) of the caller. The PSAP uses this CLID information to look up a corresponding record in their ALI database - this record contains location information for that specific CLID, which can be used by the PSAP to call back the emergency caller or another phone in the same physical area. This is important, as the PSAP should be able to automatically identify the emergency caller in case the caller is unable to speak.

As the ALI database at the PSAP is not updated in real-time, every CLID must be provisioned with the PSAP before it can be useful when an emergency call is made. This requires that a preconfigured CLID is provisioned for every potential emergency caller location in your environment.

In some jurisdictions, the CLID (ANI) of the caller is not passed to the PSAP unless the customer subscribes to a special E911 service. In this case, only the main Listed Directory Number is passed by the Carrier Central Office to the PSAP, irrespective of the CLID of the caller. In these cases, On-Site Notification becomes very crucial in ESA planning.

The ALI record

When an emergency call is made, the responding PSAP makes use of an individualized record in the Automatic Location Identification (ALI) database to associate the phone number of the incoming emergency call with the physical location of the phone. In the case of a residential phone, for instance, the information contained in its individualized ALI Record is usually the telephone subscriber’s name and the street address, and possibly information such as access directions, special hazards and medical/disability information on the subscriber. ALI Records are usually maintained by the local Telco or other public agency, and are updated as phone numbers and addresses change with subscription. When an incoming emergency call is received, the ALI database is accessed to quickly provide accurate caller information to the PSAP agent. For obvious reasons, then, it is imperative that the information in the ALI Records be kept current.

The ALI record contains a location description field that is one of two types, as follows:

1. ECL: Corresponds to a specific location, such as an office or desk, identified by an Emergency Caller Location (ECL) number. The ECL is a number that maps a DID phone to a very specific location, such as a desk or office. Thus, the PSAP agent can determine whether or not an emergency call is being made using a DID phone at its originally provisioned location (reflected in its current ALI Record entry) allowing the DID as CLID. If the DID phone is found to be at its originally provisioned location, then its DID number is used as its CLID - if not, its CLID is based on ERL.
2. ERL: Corresponds to a more generalized location, such as a floor or building. Identified by the Emergency Response Location (ERL) number, which is a number

used to describe areas sharing a common ESA routing configuration and CLID assignment, as defined in the ERL table.

ESA lets a system administrator manage both ECL and ERL information for phones provisioned within their call environment, and uses them to send the most appropriate CLID to the PSAP when an emergency call is placed. Whether ECL or ERL is used depends on the DN configuration and location of the emergency caller, and on which of the two provides the PSAP with the most specific description of the emergency caller's location.

The optional ALI Manager facilitates ALI/ELIN management for system administrators. Without an ALI Manager, ALI records, DID/ELIN data and ECL/ERL data must be administratively (manually) managed - this is similar to existing processes used for managing CLID for groups of phones.

System components

System Components

This section provides a general description of the basic components of the Emergency Services Access architecture.

Call Server (CS)

The call server is the central processor of the IP PBX, and is where IP phones are registered on the enterprise network (by means of a Terminal Proxy Server). The call server performs all required call processing and feature processing.

There may be several call servers within an enterprise environment.

IP Line application

The IP Line application components are contained in the Signaling Server (SS) or in the Voice Gateway Media Cards (VGMC). The IP Line application serves as a proxy for connecting IP phones in their registration with the Call Server.

The IP Line application is responsible for generating notifications of IP phone events (such as IP phone registrations) by means of SNMP traps. These SNMP traps also provide interface functions by which an external DM can query or update system data as required to determine the current location of IP clients connected and registered on the network.

Location determination mechanisms

Location Information Service (LIS)

The Location Information Service (LIS) is a mechanism by which the current location of an IP phone can be determined. The LIS is configured on the call server for deployments in which the use of a DM is either not required or not desired. The internal LIS performs its function using subnet mapping technology.

The external LIS uses Layer 2 port mapping or other technology to provide dynamic discovery of connected IP telephony devices. Data network switches provide device to port mappings for a connected IP phone, and location is subsequently determined when the external LIS cross-references this data against a wiremap.

Scalability of the LIS

The Subnet LIS is an internal subnet lookup table. It effectively has no scalability limit in terms of the number of subnets it can reference, but for efficient operation it is practical to expect it to contain several hundred subnets, which map to distinct emergency locations.

To provide enterprise wide mobility coverage for all connected IP clients, the Subnet LIS must map every subnet in the enterprise network. Alternately, however, it is possible to define only local subnets and then define a common emergency call handling treatment for all remote subnets (for example, routing the calls to the locally defined PSAP, or to an internal emergency responder, such as a security desk), as allowed by local regulations.

Discovery Manager (DM)

The Discovery Manager (DM) is an optional external server that provides:

- Determination of the current location of connected IP phones using multiple sources.
- Network topology support (wiremaps, for example).
- LIS technology independence.
- Location updates of registered IP phones to call servers.

Only one DM can be configured per enterprise network, but a single DM can update multiple Call Servers - as many as are installed in the enterprise network.

The DM receives notification whenever an IP phone registers on the enterprise network through an IP Line application. It then determines the location of the connecting IP phone by using an LIS.

Having determined the location of the IP phone, the DM then updates the IP Line application with the new IP client location data, and continues to match LIS data against call server data to manage subsequent changes in IP phone location.

The DM is not in the critical path of an emergency call – that is, the DM automatically updates the enterprise call servers with current IP client location data, asynchronously to ESA call processing. Thus, the call servers do not need to involve the DM directly while processing an emergency call.

The DM may contain an internal Subnet LIS, for fallback and upgrade purposes.

Scalability of the DM

There is a single external DM installed on the enterprise, and so it must be configured to have access to all enterprise call servers for enterprise wide mobility.

The DM is designed to handle multiple LIS – there can be an LIS at every site defined in the enterprise, and these can all be handled by the DM provided they all resolve to the same location mapping scheme (such as an enterprise ERL table).

ALI Manager

The ALI Manager is an optional external server that simplifies the administrative task of managing ALI record (CLID/ELIN), Emergency Caller Location (ECL), and Emergency Response Location (ERL) data (by automating these management processes).

For more information, see The ALI record on page 21.

The ALI Manager can be configured to automatically update the ALI database at the PSAP with any changes made to internal enterprise ALI records. This capability of the ALI Manager depends on the capability of the PSAP to accommodate it, and on the nature of the update agreement in place with the PSAP.

The general capability of the ESA feature to automate ALI record management is entirely dependent on the presence of the ALI Manager. If the ALI Manager is not present, then the existing manual administrative process must be followed.

The ALI Manager provides a common user interface to manage both IP phones and non IP telephones.

OSN Alerter

The OSN Alerter is an optional 3rd party application that captures OSN records and provides various external alerts (strobes or pages, for example). Existing OSN Alerter interfaces include a digital phone emulator and a TTY parser.

A centralized OSN Alerter is a ideal for handling mobility across call server (and Branch Office) areas. Then, for example, security personnel at a Branch Office can have detailed location data of a branch user who is actually registered at the Main Office.

Feature operation

This section describes the five operational steps of the ESA feature.

Location determination of IP Deskphones

Location determination is normally asynchronous with ESA call processing – the location of an IP Deskphone is essentially determined in advance of an emergency call, so that emergency call processing can occur with greater speed and efficiency from the initial time of call. Location data (such as ERL) is stored against the registration record of an IP Deskphone.

To determine the physical location of IP Deskphones, ESA provides for operations with both an internal and external location determination mechanism. Depending on whether the IP Deskphone is wired or wireless, and on the type of LIS used, location changes by the IP Deskphone may trigger a location update.

As always, non-IP phones have static (manually configured) location data.

Abnormal operation

If ESA is configured to use an External DM, and the External DM is not available, then the last known location for the phone is used as its current location. If a phone has no previous location data or a location cannot be determined for the phone, then location fields are initialized to unknown (null) location values. Also, unknown location values are assigned if a phone location corresponds to an ERL that is not configured on a system (caused by a configuration error, for example).

A phone with unknown location values receives basic ESA call processing (as configured in Overlay 24, the ESA Data Block).

If an IP phone is not registered to a Call Server (excluding a VO logged out phone), then digit recognition cannot be performed and the phone cannot invoke ESA. Allowing VO Logged Out phones to make emergency calls is developed separately.

Determining that an emergency number has been dialed

As part of its normal operation, the ESA feature monitors the system to detect whenever an emergency call is being placed using a configured Emergency Services DN (ESDN).

Determining the correct PSAP responder for caller location

The emergency call should be handled by the designated means for the location of the caller - depending on configuration for the caller location, the emergency call will be sent to either a internal responder (such as a designated security desk) or routed externally to the PSAP.

Abnormal operation

If the phone location is unknown or is not configured (ERL=0) then emergency call processing is performed according to the configuration in the ESA block data (LD 24) - this is also the case if the ERL associated with the phone is disabled or if data does not exist for an ERL.

The exception to this is for phones using VO logins.

Non-IP and manual update IP phones may still use the CLID if configured in the CLID blocks when ERL = 0, although all other emergency call processing will use LD 24 defaults.

Routing the emergency call to the correct emergency responder

When the location of the phone has been determined and the correct emergency responder determined, ESA routes the emergency call as appropriate.

Abnormal operation:

With basic ESA call routing, if the specified route for a caller location cannot be taken the call is routed using a STEP route if this is configured. In the case that a STEP route is used in this way, no system message is generated.

With enhanced ESA call routing, an alternate route is selected if the specified route cannot be taken.

If the routing data specified for a phone location is invalid (due to a configuration error, for example) or unusable (as in the case of a system error condition), then the emergency call fails and a system message is printed.

Providing a suitable CLID to the emergency responder

The CLID provided to the emergency responder should correspond to the current location of the emergency caller as defined in the ALI database at either the PSAP or security desk The CLID may be used to call back the emergency caller or another phone in the same area.

The mechanisms available to compose a CLID, in order of precedence, are:

- CLID blocks (ESA fields in LD 15), per TNB
- Dynamic ELIN, per ERL
- Locator (static ELIN), per ERL
- Default CLID (DFCL in LD 24), per customer

For more information on calling number composition, see

Abnormal operation

Specification of either an invalid CLID block or of invalid CLID data is a configuration error. The static ELIN (or a dynamic ELIN) or the DFCL may be used instead.

Specification of a null Locator value for a phone (static ELIN) may result in the DFCL being used during an emergency call. If the DFCL is used then a system message is printed.

In the event that a CLID cannot be composed for a phone the emergency call completes without a CLID and the PSTN automatically assigns the site billing number to the call. Default PSTN routing to the PSAP will also be applied.

Location management

This section describes the location management component of Emergency Access Services functionality, which allows for client mobility (dynamic location for an IP phone).

Characteristics of ESA location management:

- Applies to IP phones only, as non-IP telephones are assigned static location information.
- Separate from actual ESA call processing, location management determines the current location of an IP phone on the network in the event that an emergency call is made.

Location as device attribute

As location management is concerned with the current physical location of a phone, location is assigned as an attribute of the phone itself and not the user of the phone. When processing an emergency call, ESA uses the current location data stored in the TN Table associated to the phone of the caller.

An IP phone obtains its location data in one of three ways:

1. Static configuration in the TNB:
    - Phone is manually provisioned with unchanging location data at initial installation (phone is Manual Update).
    - User and phone device are linked.

- When the IP phone registers, the static location data is copied to the TN table as the operational location data of the phone - this is the location data actually used in ESA call processing.

2. Dynamically assigned by Internal LIS (Subnet Lookup Table):
   - Location information is dynamically assigned to the phone upon registration with the system (phone is Auto Update).
   - Operational location information for the phone is copied to the TN Table, for use during ESA call processing.
3. Dynamically assigned by external DM
   - Current location information is determined in response to IP phone connection to the TPS (phone is Auto Update). The use of an external DM allows for the location management of IP phones that are connected but not registered (as is the case with Virtual Office logged out phones).
   - Operational location information for the phone is copied to the TN Table, for use during ESA call processing.
   - Asynchronous location information updates are possible; the location update process is independent from the registration process.

Except for statically configured TNs, location data is not stored persistently for an IP phone – the necessary location data of an IP phone is determined dynamically as needed during an emergency call:

- If an IP phone has cached location data, this data is used until a location update occurs for the phone; otherwise, location fields for the phone are initialized to unknown values
- If no LIS is configured (or if it is currently unavailable) then the location data of the IP phone is not updated.
- Phones with unknown location values receive default ESA treatment (as defined in LD 24).

Location data in the TNB (TN Block)

Location data values found in the TNB (TN Block) correspond to initially-provisioned values for the IP phone; they represent the home values for the phone - current location information for the phone is stored in the TN table after a location update.

Location management never updates the TNB itself - the TNB is only updated by the administrator during initial provisioning of the phone.

```
REQ: new
TYPE: i2004
TN    ...
DES   test
CUST  ...
...
ZONE  ...
ERL   12345
ECL   12345
...
```

Figure 1: Example of location data in IP phone TNB

Station designator (DES) field

The station designator (DES) field of the TNB is a static data field that identifies the phone itself as an entity on the network; may be used by Office Data Administration System (ODAS) to represent the phone location.

Emergency Response Location (ERL) field of TNB

Corresponds to general location description for the phone station, the ERL field in the TNB points to an entry for the phone in the ERL table - this is used to determine appropriate emergency call routing and (optionally) ELIN assignment.

The valid range of input value for this field is 0 to 65535. By default, the field is set to have no value. This means that:

- The associated phone is set to Auto Update.
- The effective value is zero (0) - this means that Basic ESA data is to be used for the phone:
  - Emergency route used for the phone is defined in the ESA Data Block (LD 24).
  - The CLID is defined using the TNB (CLID table) or is the DFCL (LD 24).

An entered ERL value is rejected if the specified ERL is not defined.

The ERL value is prompted when adding or changing a TN, and is displayed when printing TN data for the phone.

Note:

ERL is only prompted if the ESA package (329) is unrestricted, regardless of whether the ESA data block configured. This enables the system administrator to configure location data for the phones before enabling the ESA feature.

Table 1: Responses for ERL field in TNB

Prompt	Response	Description
ERL	<CR> 0-65535 X	Home ERL. Enter no value to set TN to Auto Update. Enter a value to statically configure this TN (Manual Update). Enter 'X' to remove the current value in this field.

Table 2: System alarms and messages for ERL field entry

Message Number	Severity	Event	Corrective Action	Output
SCH0600	Info	Illegal input character.		TTY
SCH1627	Info	TN is Auto Update but there is no LIS configured.	Configure LIS or set TN to Manual Update (manually provision an ERL).	TTY
SCH1655	Info	ERL is out of acceptable value range.	Enter ERL from 0 to 65535.	TTY
SCH1656	Info	Specified ERL does not exist.	Enter ERL from 0 to 65535.	TTY
SCH1680	Info	ERL is disabled.	Enable ERL, otherwise ESA defaults will be used.	TTY

Emergency Caller Location (ECL) field of TNB

The value in the Emergency Caller Location (ECL) field of the TNB is a description that corresponds to a specific location, and is a number that maps the phone to a provisioned home DID phone location. As such, this value must be managed along with DID ALI records for the phone.

By comparing the current ECL for the IP phone (stored in the TN table) with the home ECL for the phone (provisioned in TNB), the system determines whether the phone is at its provisioned (home) location (as specified in the ALI database) and thus whether its DID number can be used as its ESA CLID.

The valid range of input value for this field is 0 to 65535. By default, the field is set to zero (0). This means that the home ECL (in the TNB) will never match the current ECL (in the TN table) which means that the DID CLID will not be used unless the TN is provisioned as Manual

Update. ECL can be configured for a Manual Update phone, but is not used as a Manual Update phone is deemed to always be at its originally provisioned location.

ECL is prompted when adding or changing a TN, and displayed when printing TN data.

Note:

ECL is only prompted if the ESA package (329) is unrestricted, regardless of whether the ESA data block configured. This enables the system administrator to configure location data for the phones before enabling the ESA feature.

Table 3: Responses for ECL field in TNB

Prompt	Response	Description
ECL	0-65535	Home ECL value.

Table 4: System alarms and messages for ERL field entry

Message Number	Severity	Event	Corrective Action	Output
SCH0600	Info	Illegal input character.		TTY
SCH1654	Info	Invalid ECL value	Enter ECL value from 0 to 65535.	TTY
SCH2206	Info	ECL prompt is not allowed for non-IP phone type		TTY

Data conversion during upgrade from previous ESA version

The ERL parameter is initialized automatically in the same way that the ERL table is converted automatically from the Zone ESA (ZESA) table of previous versions, as follows:

- If VPNI is less than 256, then the converted ERL value = (VPNI x 256) + Zone. This provides location based ESA functionality, as in previous ESA versions.

The Manual Update flag is set (true) for all phones during upgrade. This preserves ESA functionality from the previous version until new values are provisioned for the phone (if required). This means that:

- Since all phones will be initially set to Manual Update, and since a DID phone has its CLID ESA block configured, ESA call processing will always use the DID number for the phone as its ANI.
- Mapping of ECLs within the enterprise and changing phones to Auto Update must be done manually following an update from a previous ESA version.

Location data in LIS

The Location Information Service (LIS) provides the following location data for an IP phone:

- Current ERL (updated in the TN table)
- Current ECL (updated in the TN table)
- Location description for associated phone.

Location data in the TN table

Location data stored in the TN table is considered to be the current location data for the phone, and reflects the updated physical location of the phone. Location data values in the TN table are dynamically determined and stored in the TN table during ESA location management.

Provisioned (home) location values for the phone are stored in the TN Block.

Emergency Response Location (ERL) in the TN table

The ERL value in the TN table stores the current location (by ERL) of the associated device. This value is updated to the TN table in one of two ways:

- For an Auto Update TN, the value is determined and assigned by the LIS.
- For a Manual Update TN, the value is copied directly from the TNB, as Manual Update TNs are automatically assumed to be at the originally provisioned (home) location.

IP phones in a specific ERL can be queried. For more information, see Location reporting for IP phones on page 35.

Emergency Caller Location (ECL) in the TN table

The ECL value in the TN table stores the current location (by ECL) of the associated device. This value is updated to the TN table in one of two ways:

- For an Auto Update TN, the value is determined and assigned by the LIS.
- For a Manual Update TN, the value is copied directly from the TNB, as Manual Update TNs are automatically assumed to be at the originally provisioned (home) location.

IP phones in a specific ECL can be queried.

Location Description in the TN table

The location description value in the TN table stores a description of the current physical location of the associated device. This value is updated to the TN table in one of two ways:

- For an Auto Update TN, the value is determined and assigned by the LIS.
- For a Manual Update TN, the value is copied directly from the ERL table.

The location description value in the TN table is printed as LOC in OSN record.

Manual Update flag

The Manual Update flag is an internal flag that indicates that the TN is manually provisioned and that the location data for the phone is static. This flag is automatically set if the system administrator enters any value into the ERL field. If the TN is set to Manual Update in this way, then the current location data for the phone is copied from the TNB into the TN Table - any attempted location updates from the LIS are subsequently rejected (and a system message is generated), as the TN is set to a static location value.

If the system administrator enters no value for the ERL data field, then the TN is set to Auto Update. Therefore, because the default for a new TN is to have no value for the ERL field, the TN is also set to Auto Update by default.

IP phones that are set to Manual Update can be queried for location.

Note:

If a user performs a VO login on a phone other than their own and on a Manual Update TN, the IP Phone used is treated as Auto Update.

Needs Update flag

The Needs Update flag indicates that the current location data of an IP phone is considered to be out of date - it is used when:

- The TN is set to Auto Update and has not had its location updated by the DM since its registration. The DM can perform a query for IP phones that need location updates, in the event that registration traps may have been missed. .
- The TN is set to Auto Update and the Subnet LIS has not updated the location of the TN since its registration (or since a subnet table change has been made that has impacted the TN). The Subnet LIS can identify IP phones that need a location update, by searching for these devices during idle system cycles.

The Needs Update Flag is automatically made active (set to true) when the IP phone registers on the enterprise network. Then, following a subsequent location update by either the Subnet LIS or DM, the flag is cleared (set to false).

ESA call processing can report whether the current location data for a phone is up to date or not, by generating a system message or system alarm.

IP phones that need a location update can be queried.

IP phones with unknown location can be queried.

Location data in the TPS

The TPS contains a copy of the current location data, which is obtained from the TN table. In the event that a phone is not currently registered with the system, the TPS is considered to be the master copy of location data for that phone. If the phone is currently registered, the TPS is synchronized with the TN table to obtain the most current location information.

If the phone registers is set to Manual Update, the location data used for the phone is taken directly from the TNB. When the phone subsequently unregisters, the Manual Update flag for that phone persists on the TPS, as location information for a Manual Update TN is deemed to be static

Location data stored on the IP Deskphone

An IP Deskphone can cache location data by storing it in its DRAM (“scratchpad memory”). This is useful for survivability scenarios and for IP Deskphones using Virtual Office (VO), but does not survive power cycles.

The location data stored in an IP Deskphone is a copy of the operational location data, as it is synchronized with the TPS.

If an IP Deskphone caches location data, then the cached information is used for any new registrations it makes until a location update is available (the Needs Update flag set active during this time).

Location data can be queried from the IP Deskphone.

Selecting an LIS

The LIS prompt in the system Config Record is used to specify which LIS is to be used, as follows:.

Table 5: LD 17 – LIS selection prompt usage

Prompt	Response	Description
LIS	NONE INT SUB EXT DM	NONE - no LIS to be used. Default. Use the internal Subnet LIS. Use the External DM.

In order to configure for use with the Subnet LIS, the ESA_SUBNET_LIS package (336) must be unrestricted.

In order to configure for use with the External DM, the ESA_EXTERNAL_DM package (337) must be unrestricted. Also, if the LIS is set to EXT DM, then an External DM is required to provide location updates; otherwise all Auto Update IP Deskphones have their Needs Update flag set and a system message (OSN003) is generated during an emergency call.

If LIS=NONE, an ERL value should be entered for the IP Deskphone; otherwise, the location of the IP Deskphone is effectively unknown. Also, if the LIS is set to NONE, then all Auto Update IP Deskphones have their Needs Update flag set and a system message (OSN003) is generated during an emergency call.

Table 6: System alarms and messages for LIS selection (LD 17)

Message Number	Severity	Event	Corrective Action	Output
SCH1628	Info	Cannot configure Subnet LIS when package is restricted.	Provision the ESA Subnet LIS package (336) before using this feature.	TTY
SCH1984	Info	Cannot configure External DM when package is restricted.	Provision the ESA External DM package (337) before using this feature.	TTY

Location reporting for IP phones

This chapter discusses location reporting for IP phones.

Reporting location information in the TNB

The location data stored in the TNB is only valid for Manual Update IP phones.

LD 20 is used to print the location data in the TNB:

- Print current ERL: reports the manually provisioned value for the associated IP phone; blank if no manually provisioned value has been entered (meaning that the TN is set to Auto Update).
- Print current ECL.

Note:

ERL and ECL are only printed if the ESA package (329) is unrestricted, regardless of whether the customer has an ESA data block configured. This allows configuration of the location data for the phone before enabling the ESA feature.

```
REQ: prt
TYPE: i2004
TN   61 10
...
ZONE 0
ERL 12345
ECL 12345
...
```

Figure 2: LD 20 – Example of printing location data in TNB for IP phone

Printing location information using LD 81

Overlay (LD) 81 generates a list or a count of TNs matching the input feature type, by searching the TN Table and applying the following feature filters:

- ERL – list or count TNs by ERL.
- ECL – list or count TNs by ECL.
- MANU – list or count the IP phones that are Manual Update.

Multiple feature filters can be entered to list or count the TNs that match all filters provided.

Overlay 81 includes Attendants or BRI sets during TN traversal. Since an ERL value can be configured for these set types, Overlay 81 includes Attendants and BRI sets when the feature filter used is ERL.

Using the List (LST) command with LD 81:

- For Attendants, the descriptor (DES) field in the output is always blank, since DES configuration does not exist for an Attendant.

Using the Count (CNT) command with LD 81:

- Attendants and BRI sets are listed under the headings ATT and BRI.

Note:

These commands are only available if the ESA package (329) is unrestricted.

Listing and counting (LST/CNT) of phones by ERL using LD 81

The LST and CNT commands are used to list or count phones by ERL. Because these commands search the TNB, only the home ERL value. Therefore, these commands are intended for use with Manual Update IP phones (and non-IP phones). The current (operational) ERL value is stored in the TN table.

The LST/CNT ERL commands apply to:

- A single ERL value.
- A range of ERLs.
- All ERLs.

Table 7: LD 81 – List or count phones by ERL

Prompt	Response	Comment
REQ	LST CNT END	LIST phones. COUNT phones. END this overlay.
...	...	...
FEAT	ERL	Specifies that the ERL feature filter is to be used.
...	...	...
ERL	0-65535 0-65535 to 0-65535 <CR>	Specifies an ERL value. Specifies a range of ERLs. Process on all ERLs.

```
>ld 81
REQ   lst
...
FEAT  erl
ERL
FEAT

ERL      00          00000     TN  065 0 00 01  ISET      I2002     23 JUN 2005
ERL      00          00000     TN  065 0 00 05  ISET      I2050      9 JUN 2005
ERL      00          00000     TN  066 0 00 00  ISET      I2004     23 JUN 2005
ERL      02          00007     TN  011 0 00 00  2000      2616      21 JUL 2005
ERL      02          15331     TN  011 0 00 09  ATT                 21 JUL 2005
ERL      02 2010     00000     TN  012 0 00 00  2500      500        2 JAN 1996
ERL      02          00005     TN  014 0 00 05  BRI       BRIL      21 JUL 2005
```

Figure 3: LD 81 – Example of listing (LST) of phones by ERL

```
>ld 81
REQ   cnt
...
FEAT  erl
ERL   4
FEAT

FEAT    CUST                  TOTAL   SL1    500   2500   3000   2000   3900   ISET    DCS     PCA    ATT    BRI
ERL      00    004      CNT     4      0      0      0      0      0      0      4      0       0      0      0
```

Figure 4: LD 81 – Example of counting (CNT) of phones by ERL

Listing and counting (LST/CNT) of phones by ECL using LD 81

The LST and CNT commands are used to list or count phones by ECL. Because these commands search the TNB, only the home ECL value. Therefore, these commands are intended for use with Manual Update IP Deskphones (and non-IP phones).

The current ECL value is stored in the TN table.

The LST/CNT ECL commands apply to:

- A single ECL value.
- A range of ECLs.
- All ECLs.

Table 8: LD 81 – List or count phones by ECL

Prompt	Response	Comment
REQ	LST CNT END	LIST phones. COUNT phones. END this overlay.
...	...	...
FEAT	ECL	Specifies that the ECL feature filter is to be used.
...	...	...
ECL	0-65535 0-65535 to 0-65535 <CR>	Specifies an ECL value. Specifies a range of ECLs. Process on all ECLs.

Use of the LST and CNT commands, as detailed in the preceding table, provide outputs as show by the following examples:

```
>ld 81
REQ   lst
...
FEAT  ecl
ECL   4
FEAT

ECL      00          00004     TN  061 0 00 00  ISET      20117      9 DEC 2004
ECL      00          00004     TN  061 0 00 02  ISET      I2002     26 MAY 2004
ECL      00          00004     TN  061 0 00 05  ISET      I2050      9 JUL 2004
ECL      00          00004     TN  061 0 00 07  ISET      CUST0     14 JAN 2004
```

Figure 5: LD 81 – Example of listing (LST) of phones by ECL

```
>ld 81
REQ   cnt
...
FEAT  ecl
ECL   4
FEAT

FEAT    CUST                    TOTAL  SL1   500   2500   3000   2000   3900   ISET   DCS    PCA    ATT    BRI
ECL      00    004       CNT      4     0     0      0      0      0      0      4      0      0      0      0
```

Figure 6: LD 81 – Example of counting (CNT) of phones by ECL

Listing and counting (LST/CNT) Manual Update IP Deskphones

This section describes the commands used to list (LST) or count (CNT) Manual Update IP Deskphones.

A Manual Update telephone has a statically configured ERL (Manual Update flag is set).

Table 9: LD 81 – List or count Manual Update phones

Prompt	Response	Comment
REQ	LST CNT END	LIST phones. COUNT phones. END this overlay.
...	...	...
FEAT	MANU	Specifies that the Manual Update feature filter is to be used.
...	...	...

```
>ld 81
REQ   lst
...
FEAT  manu
FEAT

MANU      00          00010     TN   061 0 00 00   ISET       2O117       9 DEC 2004
MANU      00          00010     TN   061 0 00 02   ISET       I2002      26 MAY 2004
MANU      00          00020     TN   061 0 00 05   ISET       I2050       9 JUL 2004
MANU      00          00000     TN   061 0 00 07   ISET       CUST0      14 JAN 2004
```

Figure 7: LD 81 – Example of listing (LST) of phones by MANU

```
>ld 81
REQ   cnt
...
FEAT  manu
FEAT

FEAT    CUST              TOTAL   SL1    500   2500   3000   2000   3900   ISET   DCS    PCA    ATT    BRI
MANU    00      CNT         4      0      0      0      0      0      0      4      0      0      0      0
```

Figure 8: LD 81 – Example of counting (LST) of phones by MANU

Reporting of location data in the TN table

This section details the LOCRPT command, used in reporting location data as it is stored in the TN table. Since these commands search the TN table, the only IP phones listed are those that have a current TN table entry. This includes:

- IP phones that are currently registered.
- IP phones that have unregistered since the last system restart (warm start), so long as their TN has not been reused with another currently registered phone.

IP phones which have not yet registered have no TN table entry. However if the phone is connected to a TPS then its location data may be queried on the TPS.

Note:

These commands are only available if the ESA package (329) is unrestricted.

Table 10: LD 117 – Location Report (LOCRPT) command

Command	Description
LOCRPT ALL	Print location report for all IP phones.
LOCRPT TN x	Print location report for the IP phone(s) with the specified TN (or partially-specified TN).
LOCRPT DN x	Print location report for the IP phone(s) with the specified DN (or partially-specified DN).
LOCRPT IP x	Print location report for the IP phone(s) with the specified IP (or partially-specified IP).
LOCRPT HWID x	Print location report for the IP phone with the specified Hardware Identifier (HWID) (or partially-specified HWID).
LOCRPT ERL x	Print location report for the IP phone(s) in the specified ERL.
LOCRPT UNLOCATED LOCRPT UNKNOWN	Print location report for the IP phone(s) with unknown location. This is not the same as “LOCRPT ERL 0” – these are Auto Update phones in ERL 0.
LOCRPT ECL x	Print location report for the IP phone(s) in the specified ECL.
LOCRPT MANUALUPDATE LOCRPT MU	Print location report for the IP phone(s) that are Manual Update.
LOCRPT ROAMING	Print location report for the IP phone(s) that are not at home (i.e. their Current ECL is different from their Home ECL). This only applies when the Home ECL is not unknown (zero). This does not apply to Manual Update phones, since by definition they are always at home.
LOCRPT NEEDUPDATE LOCRPT NU	Print location report for the IP phone(s) that need a location update (i.e. their “Needs Update” flag is true).
LOCRPT UNREGISTERED	Print location report for the IP phone(s) that are unregistered but have a TN table entry.

If there are no IP phones matching the query then the LOCPRT command returns No IP Phones found in RLM table, where RLM is referring to the TN Table.

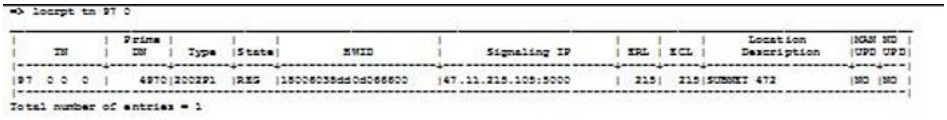


Figure 9: LD 117 – Example of LOCRPT output

Where, in the preceding example:

- TN: Terminal Number of IP phone.
- Prime DN: The prime DN of IP phone (that is, Key 0).
- Type: Type of IP phone.
- State: Current state of Registration for the IP phone.
- HWID: Hardware Identifier of IP phone.
- Signaling IP: The current IP address and signal port of the IP phone. If the phone is behind a NAT router then the Private IP of the phone is printed below the Public IP.
- ERL: Current Emergency Response Location of the IP phone.
- ECL: Current Emergency Caller Location of the IP phone.
- Location Description: Current Location Description of the IP phone.
- MAN UPD: Indicates whether this IP phone is Manual Update.
- ND UPD: Indicates whether this IP phones location Needs Updating.

Inventory Location Report

In order to provide a snapshot of the location data of all sets on the system, and to be consistent with existing inventory reports, an Inventory Location Report is available.

Location Report Inventory commands are used to print TN table Location Data. On the Call Server, these commands can be executed from LD 117, as follows:

Table 11: Inventory Location Report (INV) commands

Command	Description
INV GENERATE LOCRPT	Generates an Inventory Location Report for all IP Phones with information data stored in the TN table. System message MAT052 is printed on the TTY when report generation is complete.
INV GENERATE ALL	Generates the inventory files for Cards, Sets and LOCRPT.
INV GENERATE ABORT	Aborts the inventory report generation for Cards, Sets and LOCRPT. System message

Command	Description
	MAT055 is printed on the TTY when Inventory Location Report is aborted.
INV PRT LOCRPT	Prints the generated Inventory Location Report file.
INV PRT ALL	Prints the inventory files of Cards, Sets and LOCRPT.
INV PRT STATUS	Prints the status of the inventory for Cards, Sets and LOCRPT.

```
=> inv prt loc

Locrpt inventory:
3 1 2007 13 32 11, 3 1 2007 13 32 11, 3

 4 0 4 4,444,2616  ,2616,<N/A>,<N/A>,<N/A>/<N/A>,0,<N/A>,<N/A>,"UNKNOWN",
     YES,NO

 104 0 1 2,469,2004P1,2004P1,<N/A>,<N/A>,<N/A>/<N/A>,0,<N/A>,<N/A>,"UNKNOWN",
     YES,NO

 104 1 1 1,469,2004P2,2004P2,REG,18000ae403a4b26602,47.11.214.212:5000/
     <Unavailable>,214,214,0,"SUBNET 214",NO,NO
```

Figure 10: Example of Inventory Location Report output

The inventory file has a header with the contents “Inventory Start Date and Time, Inventory End Date and Time, Number of Records Generated”. The header contents from the above example are interpreted as follows:

- 3 1 2007 – Inventory Start Date
- 13 32 11 - Inventory Start Time
- 3 1 2007 – Inventory End Date
- 13 23 11 - Inventory End Time
- 3 - Number of Records Generated

The inventory data contains the Location Report for all phone TNs on the system. The LOCRPT record for each TN is printed on a separate line.

Location data for registered IP phones is based on their (dynamic) TN table data The location data for unregistered IP phones, or non-IP phones, is based on (static) TN Block data.

Fields in the LOCRPT record are comma delimited, and the Location Description is enclosed within double quotes, since the string can be configured with punctuation (including commas) and spaces.

“Unavailable” is printed if field data is not available (as with Private IP addresses). “N/A” is printed if field data is not applicable (as with the IP address field for a non-IP phone).

Table 12: System messages associated with Inventory Location Report

Message	Severity	Event	Corrective Action	Output
MAT008	None	Error writing to LOCRPT inventory file; generation aborted.	Try the command later	TTY
MAT009	None	Unable to close inventory LOCRPT file; generation aborted.	Try the command later	TTY
MAT046	None	LOCRPT inventory record(s) lost; generation aborted.	Generate the inventory first and then abort the process	TTY
MAT047	None	Unable to rename inventory LOCRPT file; generation aborted.	Try the command later	TTY
MAT052	None	Inventory LOCRPT generation complete.	None	TTY
MAT054	None	Queue error; LOCRPT inventory generation aborted.	Try the command later	TTY
MAT055	None	Inventory LOCRPT generation aborted.	None	TTY

Subnet lookup table

This section details the Subnet Lookup Table.

Overview

The subnet lookup table is an internal LIS. This location determination mechanism assumes that the data network architecture (subnet distribution) of an enterprise corresponds with geographical features (like floors within a building), and that IP addresses are assigned to devices by a DHCP server. By performing a reverse DHCP lookup, the network (subnet) of a given IP address is determined, and location is deduced. For this process to be effective, the subnet lookup table must mirror the DHCP configuration of the enterprise.

The subnet lookup table contains location data (ERL, ECL, Location Description) for each subnet entry.

The subnet table is not system-specific, so it can be synchronized to all Call Servers in an enterprise, provided that the same set of ERLs are defined for every system referenced.

The subnet lookup table is used when:

- The Subnet LIS is enabled (in LD 17, LIS = SUBNET).
- The IP Deskphone is Auto Update (in LD 11, ERL = blank).

Location data in the subnet lookup table

The Subnet LIS is provisioned with location data for the subnets in the enterprise, as shown by the following:

Table 13: Data in subnet lookup table

IP Address	/	Mask Bits	ERL	ECL	Location Description
47.11.214.100	/	32	[0 - 64k]	[0 - 64k]	[0 -20 characters]

The combination of IP address and mask is the network address of a subnet or of a host.

ECL and ERL are for the current location fields for an IP Deskphone. Location Description corresponds to the geographic area of the subnet.

If the Subnet LIS does not match an IP address to an IP Deskphone, then it returns an error status. A system message is generated and unknown location data is assigned to the phone:

- ERL = 0
- ECL = 0
- Location Description = “Unknown”

Alternately, the administrator may configure a universal fallback subnet: **0.0.0.0/0**. This allows the administrator to specify a particular ERL, ECL, and Location Description for otherwise non-located IP Deskphones.

If unknown location data is assigned to theIP Deskphone, then a system message is generated to indicate that the specified IP Deskphone could not be located and will receive default ESA treatment. The Needs Update flag is cleared (as the location has been updated, even if with unknown values). Under normal circumstances, the Subnet LIS should not assign **ERL 0** to a phone.

NAT

A NAT router maps multiple private IP addresses to a single public IP address, as shown by the following:

Table 14: Example of NAT mapping

Private IP : Port	Public IP : Port
192.168.0.101 : 80	47.11.211.118 : 1200

Private IP : Port	Public IP : Port
192.168.0.102 : 80	47.11.211.118 : 1202

An IP phone behind a NAT router has two IP addresses: a private IP address, and a public IP address.

In some cases it makes sense to perform a subnet lookup on a NAT IP phone's public IP address (that of the NAT router). In other cases it makes sense to perform a subnet lookup on a NAT IP phone’s private IP address (that of the phone itself). The Subnet LIS offers the option of which IP address to use for NAT IP phones, depending on the NAT subnet distribution of the enterprise.

Table 15: LD 17 – NAT IP selection

Prompt	Response	Description
SLIS_NAT_PRIV_IP	YES or NO	This option specifies whether to look up the Private IP address or Public IP address of an IP phone behind NAT.

SLIS_NAT_PRIV_IP = NO

Setting SLIS_NAT_PRIV_IP to NO means that every phone behind the NAT router is assigned location data according to the IP address of the NAT router. The subnet lookup table contains a host entry for the NAT router, which must have a fixed IP address.

The advantage of setting SLIS_NAT_PRIV_IP to NO is that NAT domains can reuse IP addresses. The disadvantage is the resultant lack of location resolution (the NAT domain might cover several floors, but these would all resolve to the same location).

NAT_PRIV_IP = YES

Setting SLIS_NAT_PRIV_IP to YES means that every phone behind the NAT router is assigned location data according to its private IP address. Because of this, NAT domains can contain different subnets - the subnet table contains entries for subnets behind the NAT.

The NAT router IP (public IP) is not looked up by the Subnet LIS.

The advantage of setting SLIS_NAT_PRIV_IP to YES is that location resolution is down to subnet. The disadvantage is that a private IP must not be reused within the enterprise (NAT domains must not overlap).

When the SLIS_NAT_PRIV_IP is set to YES, phones not behind a NAT router (having no private IP address) are located using their public IP address.

Administration of subnet entries

This section discussed administrative tasks associated with the management of subnet entries.

Adding subnet entries using the NEW SUBNET command

Subnets are added to the subnet table using the NEW SUBNET command, as shown by the following:

Command	Description
NEW SUBNET [IP Address] [Mask Bits] [ERL] [ECL] “[Location Description]”	Adds a subnet entry.

In the preceding:

- All fields except Location Description are mandatory. If Location Description is not specified then an IP Phone Location Description (in its TN table record) is retrieved from the ERL table instead.
- Spaces and punctuation are allowed in Location Description, if the input is encapsulated in quotation marks.
- Error checking is performed when:
  - Duplicate subnet entries must not exist.
  - IP Address and network mask must match.
  - ERL and ECL must be within valid range (0-65535).
  - ERL must be defined (in LD 117), except for ERL = 0.
  - Location Description must contain an alphanumeric string up to 20 characters long. Encapsulated in quotation marks, it may contain spaces and punctuation (except for quotation marks and colons)
- Subnet entries are stored in sorted order so as to return the longest match for a multiple match: first by IP, then by network mask.
- As part of this command, an audit is performed to determine if any registered IP phones are impact by the new subnet.

```
=> NEW SUBNET 47.11.216.0 24 ...
Entry added - 47.11.216.0 / 24
Total number of entries in Subnet Lookup Table = 4

=> NEW SUBNET 47.11.216.0 24 ...
SCH1633 Duplicate entry - 47.11.216.0 / 24

=> NEW SUBNET 47.11.216.100 32 ...
SCH1633 Duplicate entry - Subnet 47.11.216.100 / 32 is actually 47.11.216.0 /
24
```

Figure 11: Example of adding subnet entries using the NEW SUBNET

Deleting subnet entries using OUT SUBNET

To delete a subnet entry, use the OUT SUBNET command as show by the following:

Table 16: LD 117 – Delete a subnet entry

Command	Description
OUT SUBNET [IP Address] [Mask Bits]	Delete a subnet entry.

If the subnet does not exist then an error message is returned. As part of this command, an audit is performed to determine if any registered IP phones are impact by the deleted subnet.

The OUT command reports the number of phones located in the specified subnet that were impacted by this change. Also, the corresponding NEW command to undo the deletion is printed.

```
=> OUT SUBNET 47.11.216.0 24
Entry deleted - 47.11.216.0 / 24
Number of IP Phones impacted = 2
To undo, enter NEW SUBNET 47.11.216.0 24 216 216 "Second floor"
Total number of entries in Subnet Lookup Table = 4
```

Figure 12: Example of removing a subnet entry using OUT SUBNET

Changing a subnet entry using CHG SUBNET

This section details the CHG SUBNET command, used to modify subnet entries, as shown by the following:

Table 17: LD 117 – Change a subnet entry

Command	Description
CHG SUBNET [IP Address] [Mask Bits] [ERL] [ECL] "[Location Description]"	Change a subnet entry.

Only the location fields (ERL, ECL, and Location Description) can be changed. To change a subnet entry's definition (IP Address and Mask Bits), remove the old subnet entry and add the new one. All fields are mandatory.

Error checking is performed as for the NEW SUBNET command.

As part of this command, an audit is performed to determine if any registered IP phones are impact by the changed subnet.

```
=> CHG SUBNET 47.11.216.0 24 <new location data>
```

Figure 13: Example of changing a subnet entry using CHG SUBNET

Printing subnet entries using the PRT SUBNET command

This section details the printing of subnet entry data using the PRT SUBNET command, as shown by the following:

Table 18: LD 117 – Print subnet entries

Command	Description
PRT SUBNET <IP Address>	Print the specified subnet entry (or all entries that match a partially-specified IP address).
PRT SUBNET ERL <erl>	Print all subnets that match the specified ERL.
PRT SUBNET ECL <ecl>	Print all subnets that match the specified ECL.

Command	Description
PRT SUBNET NTH <n-th>	Print subnets starting from ‘n-th’ entry.
PRT SUBNET [ALL]	Print all subnet entries.

```
=> PRT SUBNET 47.11.214
 ____________________________________________________________
|   IP Address / Mask   |  ERL  |  ECL  |    Location Desc     |
|-----------------------+-------+-------+----------------------|
| 47.11.214.100   / 32  |     0 |     0 | Offsite access (VPN) |
| 47.11.214.0     / 24  |   214 |   214 | Lab area             |
 ------------------------------------------------------------
Total number of entries in Subnet Lookup Table = 2
```

Figure 14: Example of printing subnet entries using PRT SUBNET command

Testing a subnet entry using TEST SUBNETLIS

To verify the Subnet LIS configuration, the TEST SUBNETLIS diagnostic command allows the administrator to enter an arbitrary IP address to determine or verify its mapping in the Subnet LIS. This command finds the best match for the specified IP in the subnet table, and prints the location data for that entry. Usage is as shown in the following:

Table 19: LD 117 – Test subnet lookup

Command	Description
TEST SUBNETLIS <IP address>	Return the location data for the subnet entry that matches the specified IP address.

```
=> TEST SUBNETLIS 47.11.216.88
Subnet LIS found a match with the following data:
  ERL = ...
  ECL = ...
  LOC = ...
```

Figure 15: Example of testing subnet table using TEST SUBNETLIS command

If the Subnet LIS does not find a subnet match then the command returns No match for a.b.c.d in Subnet Lookup Table.

System messages associated with Subnet LIS

Table 20: System alarms and messages for Subnet LIS

Message Number	Severity	Event	Corrective Action	Output
SCH0099	Info	Invalid input.		TTY
SCH1628	Info	ESA Subnet LIS package (336) is		TTY

Message Number	Severity	Event	Corrective Action	Output
		restricted ESA Subnet LIS package (336) is restricted.		
SCH1631	Info	IP address and network mask do not match.		TTY
SCH1632	Info	Entry not found in the Subnet table.		TTY
SCH1633	Info	Duplicate entry.		TTY
SCH1635	Info	Invalid Location Description.		TTY
SCH1654	Info	Invalid ECL		TTY
SCH1656	Info	ERL does not exist.		TTY
SYS0143	Major	Error loading Subnet LIS database.		TTY, RPT, SNMP
ESA011	Minor	IP Phone TN <tn> was assigned unknown location (ERL 0) by Subnet LIS – will use ESA defaults.		TTY, SNMP
ESA012	Minor	IP Phone TN <tn> was not located by Subnet LIS – will use ESA defaults.		TTY, SNMP
SRPT233	Critical	Failed to allocate protected heap memory.		TTY, RPT, SNMP
TEMU019	Major	Error dumping Subnet LIS database.		TTY, RPT, SNMP

Interworking with External DM

This chapter describes the interface with an external Discovery Manager (DM). The DM communicates with the Avaya CS 1000 to determine IP phone connections or their current location status, and to update their operational location data to the TN table for use during ESA call processing.

Overview of External DM

This section describes the CS 1000 interfaces that allow inter-working with an External DM, as follows:

- IP phone connection events from CS 1000 to DM.
- Audit queries from DM to CS 1000.
- Location updates from DM to CS 1000.

Furthermore, the audit queries and location updates can be performed using either of two interfaces, as follows:

- Web Services interface, if available.
- OAM Command Line Interface (CLI).

Web Services interface for External DM

The basic Web Services interface architecture is shown by the following:

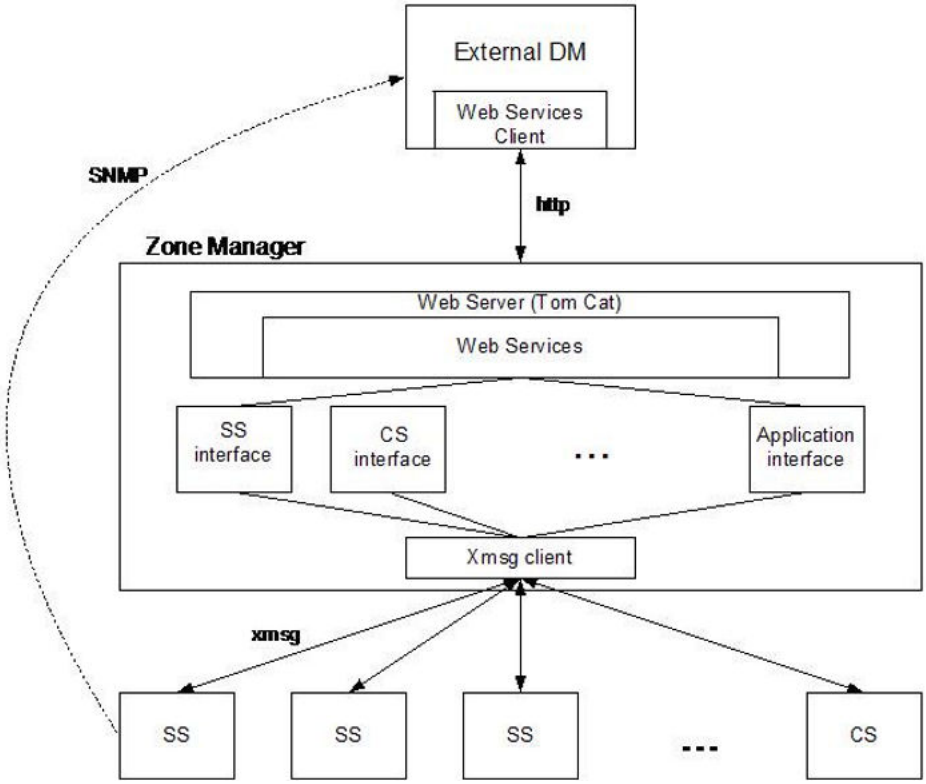


Figure 16: External DM Web Services interface architecture

Commands on the servers running the IP Line application (Signaling Servers and Voice Gateway Media Cards) are exposed as web methods by the Zone Manager using J2EE Web Services. This allows external clients such as the DM to access the commands in a way that is independent of both platform and language.

The Zone Manager web server hosts the web service and associated Web Services Definition Language (WSDL) document that is used to generate client side stubs. In order for the DM to use the exposed web methods, a Web Services client stub must be created from the supplied WSDL document using a Web Services toolkit such as Apache AXIS or the SUN wscompile tool for Java clients. Using the generated client stub code, the DM can access the above methods as if they were local method calls, however all calls go through the Web Services.

OAM Command Line Interface

Commands on the servers running the IP Line application (Signaling Servers and Voice Gateway Media Cards) are accessible in the OAM CLI shell. An External DM can log in to the OAM CLI to synchronously execute the commands and process their output. It is recommended that the System Security OAM User Account administrator create an LAPW-type user account with limited administrative access to the Call Server OA&M overlays and no PDT access, to be used by the External DM to perform audit queries and location updates via

the OAM CLI. It is neither necessary nor desirable to create a PWD1-type user account for the External DM.

Connection events and SNMP traps

The DM uses SNMP traps from the CS 1000 as the primary method for gathering the necessary information to begin tracking an IP phone location within the network.

When an IP phone connects to a TPS, the DM is notified by means of the SNMP trap ITS5008, which is generated by the TPS, and indicates the successful connection of the IP phone to the TPS. This SNMP trap is enhanced to carry IP Telephony Client (IPTC) ID and Hardware ID. IPTC ID is composed of Public IP (Terminal IP) Address and Port Number, and is unique to the phone.

```
ITS5008 Terminal connection status ok. IP=47.11.214.211:5000
HWID=1800603876065b6600
```

Figure 17: Example of enhanced ITS5008 SNMP trap

When an IP phone loses its connection to a TPS, the SNMP trap ITS2008 is generated by the TPS. This trap is also enhanced to carry IPTC ID and Hardware ID.

```
ITS2008 Terminal connection status lost. IP=47.11.214.211:5000
HWID=1800603876065b6600
```

Figure 18: Example of enhanced ITS2008 SNMP trap

Since SNMP traps are carried over User Datagram Protocol (UDP), their delivery is not guaranteed. The DM should perform periodic audits of phone status to handle any missed IP phone connection events, as shown in the section immediately following.

Audit queries for External DM

The DM performs periodic or full audits to ensure synchronization between its list of IP phones (which need to be located or tracked) and the CS 1000 systems it services. An out-of-sync condition could occur due to missed connection events (SNMP traps) or due to a system restart.

Query functions are provided which improve the efficiency of the queries and to minimize the amount of data that the DM must audit and synchronize.

If the DM issues the commands to the Zone Manager, then the commands include the IP address of the Signaling Server running the target TPS. The Zone Manager then directs the queries to the target TPS. Alternately, the DM logs in to the OAM CLI of the target TPS and issues the commands directly.

These audit query commands report on all IP phones connected to a TPS, which includes both registered and unregistered IP phones, as follows:

- IP phones may be unregistered due to being VO logged out.
- IP phones may be unregistered due to invalid TN configuration.
- IP phones may be unregistered due to duplicate TN configuration.
- IP phones may be unregistered due to invalid Node configuration.

Querying phone location data using the isetLocShow command

The command **isetLocShow** provides current location data for the specified IP phone, or if none is specified, for all IP phones connected to the TPS. The DM can use this command for a full audit as required.

This command is available from Web Services and the OAM CLI, and is also exposed via Element Manager, for diagnostic or debugging purposes.

Usage of the **isetLocShow** command is shown by the following:

Table 21: isetLocShow command to query location data

Command	Description
void **isetLocShow** (IPTC ID)	Provides the current location data for the specified IP phone, or if none is specified, all IP phones connected to the TPS.

```
oam> isetLocShow

Set Location Information
------------------------
     IP Address:Port            HWID          ERL   ECL  Location Description MU NU    State
---------------------- -------------------- ----- ----- -------------------- -- -- ------------
   47.11.215.84:5000    18-00802ddcd4b066-00   212   300 Belleville EVW        0  0 online
  47.11.215.213:5000    18-0060081ef19866-00   200   555 Toronto Office        0  0 online
   47.11.215.85:5000    18-00603876lc4c66-00     0     0                       0  1 online

Total number of sets = 3
Sets that need location update = 1
```

Figure 19: Example output of isetLocShow command

Querying phones that need a location update

The command **isetLocNeedUpdateShow** is provided for the DM to query which IP phones need a location update.

This command is available from Web Services and the OAM CLI. This command is also exposed through Element Manager, for diagnostic or debugging purposes.

Usage of the **isetLocNeedUpdateShow** command is shown by the following:

Table 22: Querying phones needing a location update

Command	Description
`void isetLocNeedUpdateShow ()`	Provides a list of IP phones, and their location data, on this TPS that need a location update.

Output format of the **`isetLocNeedUpdateShow`** command is shown in the following:

```
oam> isetLocNeedUpdateShow

Set Location Information
------------------------
     IP Address:Port            HWID          ERL   ECL  Location Description MU NU    State
---------------------- -------------------- ----- ----- -------------------- -- -- -------------
   47.11.215.85:5000    18-00603761c4c66-00     0     0                       0  1 online

Total number of sets = 3
Sets that need location update = 1
```

Figure 20: Example output of isetLocNeedUpdateShow command

Location updates with External DM

When the DM has determined the location of an IP phone (after a connection event), or a location update (due to mobility), it sends location data to the TPS using the command **`isetLocUpdate`**. This command is available through Web Services and the OAM CLI. This command is for DM use only, as it resets the External DM watchdog timer on the Call Server.

Usage of the **`isetLocUpdate`** command is shown by the following:

Table 23: isetLocUpdate command to update location data

Command	Description
`STATUS isetLocUpdate (IPTC ID, …)`	Accepts updated location data for the specified IP phone.

When used with the Zone Manager, to reduce the amount of traffic, this command can be issued with an array of IP phones and their location data along with targeted TPS. The Zone Manager will call the function as a local method to pass the location data IP phone by IP phone to the TPS.

Use of this command causes the DM to update location data on the TPS, as follows:

- Current ERL, which corresponds to the general area of the IP phone (such as a floor).
- Current ECL, which corresponds to the specific area of the IP phone (office, or pillar).
- Location Description, which corresponds to the specific area of the IP phone (per ECL).

The TPS validates the location data provided by the External DM.

If the DM does not locate an IP phone then it performs a location update using null values:

- ERL = 0.
- ECL = 0.
- Location Description = “Unknown”.

If an unknown location update is performed then a system message is generated that indicates that the specified phone could not be located and will receive default ESA treatment. The Needs Update flag is cleared (since technically, the location has been updated).

Under normal circumstances, the External DM should not assign ERL 0 to a phone. If the External DM assigns a phone to an undefined ERL then a system message is generated and the phone is assigned unknown location data and the Needs Update flag is cleared.

Location updates for Manual Update TNs are ignored by the TPS (but generate a system message).

An example of the output of the **`isetLocUpdate`** command is given in the following:

```
oam> isetLocUpdate "47.11.215.84" "5000" "200" "555" "Toronto Office"
LIS0010: Location data is updated.
```

Figure 21: Example output of isetLocUpdate command

Re-synchronizations of the External DM

Re-sychronizations between the External DM and the system are required in various failure and survivability scenarios, as follows:

- If the External DM restarts:
  - It must rebuild its location database since it was last saved.
  - It must perform a full audit on every TPS to list all connected phones (and their current location).
  - It must send location updates for all IP phones whose location data is out of date.
- If the Call Server restarts (warm or cold boot):
  - If the restart is fast enough, the IP phones stay connected with the TPS.
  - If the restart is too lengthy, the IP phones restart.
- If the TPS (Signaling Server or VGMC) restarts (warm or cold boot):
  - The IP phones connected to it restart.
  - The External DM receives SNMP traps for all re-connections.
  - The periodic query for IP phones that need a location update catches any missed SNMP traps.

- If IP phones stay connected to TPS (SS or VGMC):
  - The External DM keeps locations up to date.
  - No operational impact.
- If IP phones restart:
  - The External DM sees SNMP traps for all re-connections.
  - The periodic query for IP phones that need a location update catches any missed SNMP traps.

There is no impact due to Active Call Failover (ACF). With ESA, IP phones maintain their speech path, and only reboot when the call ends. After rebooting, IP phones connect to a TPS normally.

Package protection for External DM

The CS 1000 must be equipped with proper packages (ESA External DM package 337) and configuration (LD 17, LIS = EXT or DM) for the Call Server to accept location updates from the DM.

Presence management for External DM

If an External DM is configured but it has not connected to the system within a preset time period (to perform a location update or periodic audit) then a system message is generated to indicate a probable fault with the External DM or its connection. This is implemented using an internal watchdog timer that is reset every time the External DM communicates with the PBX in the form of a location update or keep-alive indicative messaging. Also, if the timer is expired and an Auto Update phone makes an emergency call then an OSN message (OSN003) indicates that location needed an update.

The timeout value must be set greater than the External DM's audit interval. For example, if the External DM performs an audit every 15 minutes then the timeout value could be set to 20 minutes. This allows some flexibility in processing delay yet ensures than an alarm is generated shortly after the absence of the External DM is detected.

If the External DM has not communicated with the PBX as above for a period greater than the configured time interval then the system message is generated. If the problem persists then the alarm message is generated again after each configured timeout interval elapses. For example, if the timeout value is configured at 15 minutes then the first message is generated 15 minutes from last time the External DM was active, and after every 15 minutes the alarm is generated again, prompting the administrator to take action.

Once the External DM has reconnected (when the first update message is received) a system message is generated informing the network administrator.

External DM timeout administration

The EXT_DM_UPDT_TIMEOUT prompt is used to set the External DM timeout value. This prompt is displayed in the system configuration record only when the External DM is configured (LIS = EXT or DM).

Appropriate usage of the EXT_DM_UPDT_TIMEOUT prompt is shown by the following:

Table 24: LD 17 – External DM update timeout

Prompt	Response	Description
EXT_DM_UPDT_TIMEOUT	5-(15)-1440	The period in minutes before an alarm is generated if the External DM has not connected to the system (to perform a location update or periodic audit).
	0	No alarm is generated.

The unit of this watchdog timer is minutes and the minimum and maximum values that it could be are 5 minutes and 1440 minutes respectively. If no value is entered at this prompt then the timeout is set to a default value of 15 minutes.

A value of zero (0) may also be entered for this prompt, which disables the External DM timeout alarm. This means that a system message is not printed if the External DM fails to connect to the system.

The currently configured value of this parameter is printed in LD 22. This field is not displayed in the output if the LIS type has not been set to EXT or DM.

```
> LD 22

REQ  PRT
TYPE ESA
ESA
     LIS    EXT/DM
     ...
     EXT_DM_UPDT_TIMEOUT xxx
```

Figure 22: LD 22 – External DM timeout delay

Table 25: System messages for External DM timeout

Message Number	Severity	Event	Corrective Action	Output
ESA037	Major	The External DM has not reported location updates for a time greater than the configured timeout value	Investigate problem with External DM.	TTY, SNMP

Message Number	Severity	Event	Corrective Action	Output
ESA038	Cleared	The External DM is back online after a reported timeout.	None.	TTY, SNMP
SCH0582	Info	Input out of range	Enter External DM timeout value from 5 to 1440 (or 0).	TTY

System messages for interworking with External DM

The error category LIS informs the External DM about the result of interface commands. The outputs of the LISxxxx messages go to the TTY port, and they are forwarded to the External DM through Web Services in the Zone Manager or simply printed in the OAM CLI.

Message Number	Severity	Event	Corrective Action	Output
LIS0001	Info	Operation aborted with an internal error.	Contact your technical support group.	TTY
LIS0002	Info	Operation aborted – Line TPS has not been initialized.	Enable Line TPS, or wait until the Line TPS is in operation.	TTY
LIS0003	Info	Invalid IP address.	Enter valid IP address.	TTY
LIS0004	Info	Invalid port number.	Enter valid port number.	TTY
LIS0005	Info	Invalid ERL.	Enter valid ERL.	TTY
LIS0006	Info	Invalid ECL.	Enter valid ECL.	TTY
LIS0007	Info	Invalid Location Description.	Enter valid Location Description.	TTY
LIS0008	Info	No sets are connected.	None.	TTY
LIS0009	Info	Location data is not updated – phone is Manual Update.	Do not update location data for Manual Update phone.	TTY
LIS0010	Info	Location data is updated.	None.	TTY
LIS0011	Info	Location data is not updated – data is up to date.	None.	TTY

The ERL table

The previous ESA configuration in the Zone (ZESA) table is moved to the new ERL table. This configuration is decoupled from Zone; it is now indexed by ERL parameter of the phone.

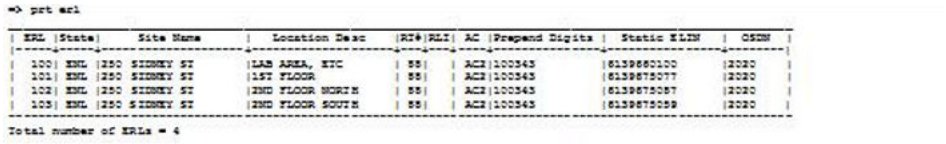
In order to support network wide mobility, the ERL table contains ESA configuration for all ERLs present in the enterprise network, and is provisioned on all Call Servers in the enterprise.

The ERL table can be used for all phone types, as all phones are now provisioned to have an ERL parameter.

ERL 0 is not a valid table entry. This value is reserved to indicate the basic (default) ESA treatment, as defined in the ESA Data Block (LD 24).

The administrator must ensure that the customer's ESA Data Block is configured as fallback, before any ERLs are defined for that customer enterprise network. There is no automatic overlay check for this - the administrator must verify manually this before starting to provision any ERLs. As the ERL table is customer-agnostic, the administrator must ensure that all parameters for ERL entries are valid for the respective customer.

An example of the ERL table is provided in the following:



```
=> prt erl
 ERL |State|     Site Name      |    Location Desc    |RT#|RLI| AC |Prepend Digits |  Static ELIN  |  OSN  |
 100| ENL |250 SIDNEY ST       |LAB AREA, ETC        | 55|   | ACS|100343        |6139660100     |2020   |
 101| ENL |250 SIDNEY ST       |1ST FLOOR            | 55|   | ACS|100343        |6139675077     |2020   |
 102| ENL |250 SIDNEY ST       |2ND FLOOR NORTH      | 55|   | ACS|100343        |6139675087     |2020   |
 103| ENL |250 SIDNEY ST       |2ND FLOOR SOUTH      | 55|   | ACS|100343        |6139675059     |2020   |
Total number of ERLs = 4
```

Figure 23: The ERL table

An ERL can be enabled or disabled. Disabling an ERL is analogous to DIS ZBR x ESA in previous releases.

Phones can still be assigned to a disabled ERL but a warning message is generated. It is advisable to not disable an ERL, as ESA call processing will use ESA Data Block (LD 24) parameters as its fallback configuration, which may result in incorrect routing and CLID assignment. This functionality is required to support disabled zones from previous releases.

ESA call processing generates a system message if the emergency caller’s ERL is disabled.

Site Name is printed in the OSN record, as SITE. It is expected (although not required) that this be a familiar name for an enterprise location that corresponds to an MSAG-validated address within an ALI record.

Location Description is printed in the OSN record (LOC) for phones that aren’t assigned a Location Description by the LIS or DM, as is the case with Manual Update IP phones and non-IP phones. It is expected, but not required, that this corresponds to the Free Form Text field within an ALI record.

Site Name and Location Description are alphanumeric strings up to 20 characters long. Encapsulated in quotation marks, they may contain spaces and punctuation (except quotations marks and colons).

Routing data is optional. Routing data includes the following:

- Route number, Access Code, and Prepend Digits for basic routing.
- RLI number, Access Code, and Prepend Digits for enhanced routing.

If routing data is not specified then ESA call processing uses the ESA Data Block routing parameters.

Configuration of Locator is optional: If Locator is not specified (and assuming no CLID or Dynamic ELIN was assigned) then ESA call processing assigns the DFCL (in the ESA Data Block) to the emergency caller. A Locator must be specified in order to support network-wide mobility, and is configured similarly in the ERL table of all Call Servers - a single Locator can be shared by multiple ERLs, and is used as a dynamic ELIN fallback.

Note:

If a single Locator is to be shared by multiple ERLs then the location description provided for the “locator” will be the common data associated with all the ERLs sharing the same locator. For example, for the building description in which all the ERLs are located - the locator does not have to terminate on the originating CS 1000, and so care is required to ensure proper location reporting.

OSDN is optional. It specifies the OSN DN for an ERL.

Administration of the ERL table

This section details the various administrative commands associated with adding, deleting, changing, and printing entries in the ERL table.

Note:

The following ESA administrative commands of previous ESA versions have been changed, and do not apply to administration of the ERL table in this ESA version:

- ZESA commands (CHG ZESA and PRT ZESA)
- the ZBR ESA flag (ENL/DIS ZBR <zone> ESA)
- the Zone Description command (CHG ZDES)

Adding an ERL entry using the NEW ERL command

Adding an ERL entry to the ERL table is accomplished through the use of the **NEW ERL** command. A token specifies the route mechanism to use for each ERL added.

Usage of the **NEW ERL** command is as shown by the following:

Table 26: LD 117 – Add an ERL entry

Command	Description
NEW ERL <ERL#> [RT <routing data>] [<Locator>] [<OSDN>]	Add an ERL entry with route number.
NEW ERL <ERL#> [RLI <routing data>] [<Locator>] [<OSDN>]	Add an ERL entry with RLI number.

A system message is generated in case of the following errors:

- The ERL number input must be within the valid ERL value range (1-65535).
- Duplicate ERL entries must not exist.
- Number of ERLs (determined by machine type) exceeded.

To specify null routing data in the addition of a **NEW ERL** entry, enter:

- Route # or RLI # = “NULL”.
- Access Code = “NULL”.
- Prepend Digits = “NULL”

To specify null Locator, enter “NULL”.

To specify null OSDN, enter “NULL” or nothing.

A new ERL entry is enabled by default.

The number of provisioned ERLs is printed.

Assigning location strings to a NEW ERL entry

With the creation of a **NEW ERL** entry, it is now possible to add location strings to further define the entry. An ERL must be defined before location strings can be assigned for it.

A site name can be added using the **CHG ERLSITE** command - Site Name is an alphanumeric string up to 20 characters long.

A location description can be added to the ERL entry using the **CHG ERLLOC** command - Location Description is an alphanumeric string up to 20 characters long.

Usage of the **CHG ERLSITE** and **CHG ERLLOC** commands are as shown in the following:

Table 27: LD 117 – Assign location strings to ERL entry

Command	Description
CHG ERLSITE <ERL#> <"Site Name">	Assign a Site Name to an ERL.
CHG ERLLOC <ERL#> <"Site Name">	Assign a Location Description to an ERL.

Strings encapsulated in quotation marks may contain spaces and punctuation (except quotations marks and colons).

Note:

Changing the Location Description of an ERL automatically causes all Manual Update IP phones to be relocated, thus updating their Location Description in the TN table.

Deleting an ERL entry using the OUT ERL command

Deleting an ERL entry from the ERL table is accomplished through the use of the **OUT ERL** command. Usage of the **OUT ERL** command is as shown by the following:

Table 28: LD 117 – Delete an ERL entry

Command	Description
OUT ERL *<ERL #>*	Delete an ERL entry.

System messages are generated if the specified ERL is out of range or does not exist.

The **OUT ERL** command is rejected if:

- There are ELINs currently defined against the specified ERL - Dynamic ELINs must be deleted before an ERL entry can be deleted.
- The specified ERL is currently defined against a phone (either in TNB or TN table, or both) or is referenced in the subnet table.
  - The administrator must ensure that the ERL is not referenced in the External DM.
  - If an IP phone is assigned an ERL that no longer exists then a system message is generated and the set is assigned null (unknown) location data.

When executing the **OUT ERL** command, the number of currently provisioned ERLs is printed

Changing an ERL entry using the CHG ERL command

Changing an ERL entry in the ERL table is accomplished through the use of the **CHG ERL** command. A token specifies the route mechanism to use for each ERL changed.

Usage of the **CHG ERL** command is as shown by the following:

Table 29: LD 117 – Change an ERL entry using CHG ERL

Command	Description
CHG ERL <ERL#> [RT <routing data>] [<Locator>] [<OSDN>]	Change ERL entry with specified route number.

Command	Description
CHG ERL <ERL#> [RLI <routing data>] [<Locator>] [<OSDN>]	Change ERL entry with RLI number.

A system message is generated if the ERL specified in the command is out of range or does not exist.

Printing an ERL entry using the PRT ERL command

Printing information for an ERL entry in the ERL table is accomplished through the use of the PRT ERL command.

Usage of the PRT ERL command is as shown by the following:

Table 30: LD 117 – Print an ERL entry using PRT ERL

Command	Description
PRT ERL <ERL#> [<+/- Count>]	Print a specific ERL entry, or create a list of ERLs starting from the specified ERL.
PRT ERL [ALL]	Print all ERL entries.

A system message is generated if the ERL specified in the command is out of range or does not exist.

Enabling and Disabling ERLs

This section details the **ENL ERL** and **DIS ERL** commands, used to enable or disable an ERL entry, respectively. Usage of these commands is shown by the following:

Table 31: LD 117 – ERL table maintenance

Command	Description
ENL ERL <ERL #>	Enable specified ERL.
DIS ERL <ERL #>	Disable specified ERL.

A system message is generated if the specified ERL is out of range or does not exist. ESA call processing generates a system message if the emergency caller's ERL is disabled.

When an ERL entry is created using the **NEW ERL** command, it is enabled by default.

Note:

The ZBR (Zone Branch) maintenance commands (**DIS ZBR**, **ENL ZBR**) of previous ESA versions do not apply to the ERL table.

ERL table data conversion from ZESA table

The ERL table of this version of ESA is an expansion of the ZESA table from previous ESA versions, and so is automatically created from previous ZESA data following an ESA version upgrade. Any new data fields are left blank, to be fully configured after upgrading.

The ERL entry data is created through a conversion using the customer number's Virtual Private Network Identifier (VPNI). This is done to ensure that multiple systems in an enterprise do not have ERL number conflicts when upgrading an existing ESA implementation using ZESA. The data conversion is calculated as shown by the following:

Table 32: ERL table data conversion from ZESA table

Previous ZESA Field Data	New ERL Field Data
(VPNI x 256) + ZONE #	ERL #
State	State
<blank>	Site Name
Description	Location Description
<routing data>	<routing data>
Locator	Static ELIN
<blank>	OSDN

A system message is generated if there are previous ZESA 0 parameters, but the ZESA 0 parameters are not converted to a corresponding ERL entry.

System Messages

This section provides a detailed description of the system messages and alerts associated with ERL table configuration, as shown by the following:

Table 33: System alarms and messages for ERL management (LD 117)

Message Number	Severity	Event	Corrective Action	Output
SCH0099	Info	Invalid input		TTY
SCH0257	Info	ESA package (329) is restricted	Provision ESA package (329) before using this feature.	TTY

Message Number	Severity	Event	Corrective Action	Output
SCH1634	Info	Invalid Site Name	Enter Site Name up to 20 characters (including acceptable punctuation).	TTY
SCH1635	Info	Invalid Location Description	Enter Location Description up to 20 characters (including acceptable punctuation).	TTY
SCH1636	Info	Invalid Route	Enter valid Route (from 0 to 127 on Small System; from 0 to 511 on Large System).	TTY
SCH1637	Info	Invalid RLI	Enter valid RLI (from 0 to 1999).	TTY
SCH1648	Info	Maximum number of ERLs for this machine type already configured	Cannot configure more ERLs on this machine type.	TTY
SCH1656	Info	ERL does not exist	Cannot reference undefined ERL.	TTY
SCH1662	Info	Failed to create ERL	Refer to Report Log messages for more information.	TTY
SCH1664	Info	Cannot remove ERL while…	Resolve the conflict first.	TTY
SCH2207	Info	ESA SUPP package (330) is restricted	Provision the ESA SUPP package (330) to unrestrict the advanced features.	TTY
TEMU017	Major	Error dumping ERL database	Contact your technical support.	TTY, RPT, SNMP
SYS0145	Major	Error loading ERL database	Restore the ERL database or contact your technical support.	TTY, RPT, SNMP
SYS0146	Major	Error converting ZESA to ERL data	Correct your configuration before trying upgrade again.	TTY, RPT, SNMP
ESA017	Major	Phone TN ‘x’, DN ‘y’ in disabled ERL ‘z’ has invoked ESA – using ESA defaults	Follow up emergency situation and correct the ERL configuration.	TTY, RPT, SNMP

ERL table in EDD/Sysload

If an equipment data dump (EDD) is performed, the existing ERL table on secondary storage is backed up (as erl.bak), and the ERL table in memory is saved as /u/db/erl.db (or as c:/u/db/erl.db for SSC). Whenever a Sysload is performed, the ERL table on secondary storage is read in to protected memory.

As with the other database files, the ERL table is copied to the other Media Gateways or Alternate Call Server during EDD.

The ERL table is backed up (BKO), restored (RES), swapped (SWP), and archived (LD 143) similarly to other database files.

Location management for non-IP lines

This section details the ESA location management functionality, as applies to non-IP phones.

For information about location management for IP phones or for a general description of location management concepts and functionality, see Location management on page 27.

Incoming Trunks

In previous versions of ESA, emergency calls received over an incoming trunk received Zone ESA treatment based on IPMG zone. This allowed tandem emergency calls to be forwarded to virtual trunk routes. Trunk initiated ESA is not an optimal configuration, however, due to the limited number of trunk types supported in emergency call handling. CAMA trunks, for example, should ideally serve as CO trunks and not as TIE trunks. Using virtual trunks, the originating system should route its calls to the Trunk Gateway system, and not to the call server.

With the present version of ESA, emergency call handling is based on the ERL parameter and trunk-initiated ESA calls receive basic ESA treatment (as defined by the ESA Data Block parameters, configured in LD 24). This allows a trunk-initiated ESA call to route using default ESA parameters instead of routing according to IPMG zone. Also, using enhanced routing, the ESA Data Block can now specify virtual trunk routing.

Non-IP phones

ESA adds the ERL parameter to all phones, IP and non-IP, to denote the specific location of the phone. This enables easier feature management due to a common ESA configuration,

flexible routing for remote cabinets (MCR and SIPE are examples), and the use Dynamic ELINs (which are ERL-based).

Non-IP phones are statically configured. Therefore, there is no requirement for a location determination mechanism with these phones, as location information for the phone is manually provisioned by the administrator.

Note:

Wireless non-IP phone mobility is not configurable with ESA location management - phones of this type should be provisioned by the administrator with an ERL that is large enough to cover the area of probable movement, as the emergency call will always reflect the static location provisioned for the base of the wireless non-IP phone.

Table 34: ERL prompt for non-IP phones

Prompt	Response	Description
ERL	(0)-65535	Defines the current ERL for the non-IP phone. ERL 0 means ESA call processing uses the default ESA Data Block (LD 24) parameters.

The ERL value is rejected if the ERL is not defined.

By default, the ERL value of a phone is set to zero (0), indicating that default ESA call processing is to be used, as defined in the ESA Data Block (LD 24).

ERL prompt for analog telephones

This section details the use of ERL with analog non-IP phones.

Table 35: LD 10 – ERL prompt for analog telephones

Prompt	Response	Comment
REQ	aaa	Request.
TYPE:	a…a	Type of analog phone.
TN	l s c u	Terminal Number Loop-Shelf-Card-Unit.
...	...	...
CUST	...	...
ERL	(0)-65535	Current ERL.
WRLS	...	...

A sample printout of the TN Block of an analog non-IP phone is shown in the following:

```
REQ: prt
TYPE: tnb
TN   <tn>
CDEN
CUST
TEN
DATE
PAGE
DES

DES  ...
TN   ...
TYPE ...
CDEN ...
CUST ...
ERL  xxxxx
WRLS ...
...
```

Figure 24: LD 20 – Print analog telephone TNB

ERL prompt for digital telephones

This section details the use of ERL with digital non-IP phones.

Table 36: LD 11 – ERL prompt for digital telephones

Prompt	Response	Comment
REQ	aaa	Request.
TYPE:	a…a	Type of digital phone.
TN	l s c u	Terminal Number Loop-Shelf-Card-Unit for Large System.
...	...	...
AOM	...	...
ERL	(0)-65535	Current ERL.
FDN	...	...

A sample printout of the TN Block of a digital non-IP phone is shown in the following:

```
REQ: prt
TYPE: tnb
TN   <tn>
CUST
DATE
PAGE
DES

DES  ...
TN   ...
TYPE ...
CDEN ...
CUST ...
AOM  ...
ERL  xxxxx
FDN  ...
...
```

Figure 25: LD 20 – Print digital telephone TNB

Attendant consoles

This section details the use of ERL with (non-IP phone) attendant consoles.

Table 37: LD 12 – ERL prompt for attendant consoles

Prompt	Response	Comment
REQ	aaa	Request.
TYPE:	a…a	Type of attendant console.
TN	l s c u	Terminal Number Loop-Shelf-Card-Unit for Large System.
...	...	...
IADN	...	...
ERL	(0)-65535	Current ERL.
SSU	...	...

A sample printout of the TN Block of an attendant console non-IP phone is shown in the following:

```
REQ: prt
TYPE: tnb
TN   ...
...
IADN ...
ERL xxxxx
SSU ...
...
```

Figure 26: LD 20 – Print attendant console TNB

Note:

Attendant consoles are not managed by the system management tool (EM).

ERL prompt for BRI telephones

This section details the use of ERL with non-IP BRI telephones.

Table 38: LD 27 – ERL prompt for BRI telephones

Prompt	Response	Comment
REQ	aaa	Request.
TYPE:	DSL	Digital Subscriber Line
DSL	l s c dsl	Digital Subscriber Loop address
...	...	...

Prompt	Response	Comment
USID	...	...
ERL	(0)-65535	Current ERL.
...	...	...

A sample printout of the TN Block of a digital non-IP phone is shown in the following:

```
REQ prt
TYPE dsl
DSL  ...
...
CUST ...
ERL xxxxx
CTYPE ...
...
```

Figure 27: LD 27 – Print BRI telephone TNB

System alarms and messages for station administration

This section details the system alarms and messages for station administration relating to non-IP analog, digital, attendant set, and BRI phones, as in the following:

Table 39: System alarms and messages for station administration (LD 10, 11, 12, 27)

Message Number	Severity	Event	Corrective Action	Output
SCH0600	Info	Illegal input character		TTY
SCH1655	Info	ERL is out of range	Enter ERL from 0 to 65535.	TTY
SCH1656	Info	ERL does not exist	Enter valid ERL from 0 to 65535.	TTY
SCH1680	Info	ERL is disabled	Enable the ERL, otherwise ESA defaults will be used.	TTY

ESA enhanced routing

In addition to basic emergency call routing methods, ESA also has enhanced routing methods based on Route List Index (RLI) architecture. The enhanced routing functionality depends on ESN packaging, although NARS/BARS does not have to be configured.

A list of available routes can be programmed into an RLI. The RLI number is then configured in the ESA Data Block (LD 24) or the ERL table (LD 117). This allows the administrator to specify multiple alternate routes for ESA calls, should default routes fail for any reason.

The LD 24 ESA Data Block and the LD117 ERL table are mutually exclusive. RLI based routing as well as ESRT based routing options are available in each block. The administrator must choose the emergency call routing method as required in each data block.

Local Termination and Digit Manipulation (for Called Number) are implemented for ESA call handling. This enhances the flexibility offered to customers for ESA call treatment. Note that Digit Manipulation is required for proper functionality of multiple ESDNs when they are supported.

There is no cascading between the ESRT (or RLI) specified in the ERL table and the ESA Data Block. One suggestion is to configure the last route entry in an RLI so that it is the same as the default ESRT. Another suggestion is to make the last entry in the RLI a local termination. If the ESA fails to terminate after making these adjustments, then the emergency caller will receive intercept treatment.

Note:

When a previous ESA version configured is upgraded to the current version, the existing ESA routing data is retained as is - no new configuration is required to sustain the ESA call processing.

ESA enhanced routing is an advanced configuration that provides more emergency call handling functionality by maintaining alternate routing across different route types. This is a significant advantage over the ESRT/STEP route mechanism of previous versions - presently, ESA enhanced routing can use alternate routes specified in the RLI, and these can be of different types (IP Peer, PRI, CAMA). Alternate routes are stepped through in the search for an unallocated trunk.

Using RLI, local termination can be achieved without the need for loopback trunks: LTER information is directly entered into the RLI configuration in LD 86.

After all the routes are entered into an RLI, the RLI may be associated with an ESA block (LD 24 or LD 117).

ESA enhanced routing operation

One of the main motivators for implementing the ESA enhanced routing feature is the apparent limitation imposed on ESA call handling by the STEP route option to spill over calls which cannot be routed on the first-choice route specified.

The enhanced routing feature utilizes a Route List Index (RLI) to specify a list of routes. This route list specifies a sequence of routes that are available for use for call termination.

For example, in a RLI, a PRI route can be specified as the first option, an IP Peer route can be the second entry, and Local Termination can be the third entry. In the event that the first routing choice is not available (meaning that all trunks in the PRI route list have been used up by other calls), the call spills over to the second routing choice - in our example, the IP peer route.

Some of the scenarios under which calls may spill over from one route to the next are as follows:

- Trunks are all busy or are disabled.
- The trunks specified in the route do not pass the eligibility criteria for call termination.
- Bandwidth zone is disabled for an IP phone or IP Peer trunk.

A system message is generated if the selected route is not the primary route (RLI entry 0), as a warning that the emergency call may not go to the right PSAP.

Local termination

With RLI routing, ESA calls can be sent to an internal emergency responder, such as a security desk, if the customer chooses. Local termination of emergency calls can be the first (and only) choice available to a customer, or may be the last choice in a long list of routes.

Note, however, that alternate routing options do not proceed beyond the local termination entry – from a routing standpoint, the local termination is always assumed to succeed regardless of the result of the termination. It is recommended to locally terminate emergency calls to an ACD DN - this allows for correct operation if there are multiple security agents or if they are unable to immediately answer the emergency call.

Local termination to a NARS DN is possible, but not recommended, as the ESA status of the call can be lost during NARS routing or upon subsequent local termination. This possibility of this occurring affects the configured ESA intercept treatment (per ACCD) and the generation of OSN records.

Local termination should be to a local DN.

Administration of ESA enhanced routing

This section details the administration tasks of ESA enhanced routing, and their associated commands.

In order to utilize the flexibility of the RLI based routing, all relevant configuration of RLI data and DMI (Digit Manipulation Index) data is a prerequisite.

The details of RLI and DMI configuration are described in the Basic Network Features document.

As the STEP mechanism and the RLI mechanism are two different means to achieve the same end result, their functionally are mutually separated.

The administrator should not configure a STEP route if they are opting for the RLI based route selection mechanism.

Configuring RLI in ESA Data Block

To configure RLI information in a new ESA Data Block, enter no values at the ESRT prompt and enter the RLI number at the RLI prompt. This ensures that only the RLI is active as the routing method.

For an example of the configuration of RLI in the ESA Data Block (LD 24), refer to the following:

```
>ld 24
REQ new
TYPE esa
CUST <customer number>
ESDN <emergency services DN>
ESRT
RLI <RLI number>
DDGT ...
```

Figure 28: LD 24 – Configuring RLI in ESA Data Block

Changing RLI in ESA Data Block

To modify existing RLI information in the ESA Data Block, enter no values at the ESRT prompt and enter the RLI number at the RLI prompt. This ensures that only the RLI is active as the routing method.

For an example of modifying RLI data in the ESA Data Block (LD 24), refer to the following:

```
>ld 24
REQ chg
TYPE esa
CUST <customer number>
ESDN
ESRT
RLI <new RLI number>
DDGT ...
```

Figure 29: LD 24 – Changing RLI in ESA Data Block

Changing RLI to ESRT in ESA Data Block

To change from RLI to ESRT in the ESA Data Block, enter the route number at the ESRT prompt. With a valid route entered at the ESRT prompt, the existing RLI is removed and RLI is not prompted. This ensures that only the ESRT is in effect.

If the ESRT is left blank and the RLI is deleted (by entering X), a system message is generated and route information is re-prompted, starting with the ESRT. allowing recovery from a data entry error.

```
>ld 24
REQ chg
TYPE esa
CUST <customer number>
ESDN
ESRT <new ESA route>
DDGT ...
```

Figure 30: LD 24 – Changing RLI to ESRT in ESA Data Block

```
>ld 24
REQ chg
TYPE esa
CUST <customer number>
ESDN
ESRT X
RLI

SCHxxxx

ESRT ...
```

Figure 31: LD 24 – System error when no ESRT or RLI in ESA Data Block

Configuring ESRT in ESA Data Block

To configure an ESRT in a new ESA Data Block, enter the route number at the ESRT prompt. With a valid route entered at the ESRT prompt, RLI is not prompted. This ensures that only the ESRT is in effect

```
>ld 24
REQ new
TYPE esa
CUST <customer number>
ESDN <emergency services DN>
ESRT <ESA route>
DDGT ...
```

Figure 32: LD 24 – Configuring ESRT in ESA Data Block

Changing ESRT in ESA Data Block

To modify the ESRT data existing in the ESA Data Block, enter the new route number at the ESRT prompt. With a valid route entered at the ESRT prompt, the RLI is not prompted. To retain the current configuration, enter nothing at both the ESRT and RLI prompts.

```
>ld 24
REQ chg
TYPE esa
CUST <customer number>
ESDN
ESRT <new ESA route>
DDGT ...
```

Figure 33: LD 24 – Changing ESRT in ESA Data Block

Changing ESRT to RLI in ESA Data Block

To change from an RLI to an ESRT in the ESA Data Block, enter the route number at the ESRT prompt. With a valid route entered at the ESRT prompt, the existing RLI is removed and RLI is not prompted. This ensures that only the ESRT is in effect.

If the ESRT is left blank and the RLI is deleted (by entering X), a system message is generated and the route information is re-prompted, starting with the ESRT. This allows the administrator to recover from a data entry error.

```
>ld 24
REQ chg
TYPE esa
CUST <customer number>
ESDN
ESRT X
RLI <new RLI number>
DDGT ...
```

Figure 34: LD 24 – Changing ESRT to RLI in ESA Data Block

```
>ld 24
REQ chg
TYPE esa
CUST <customer number>
ESDN
ESRT X
RLI

SCHxxxx

ESRT ...
```

Figure 35: LD 24 – System error when no ESRT or RLI in ESA Data Block

Printing ESA Data Block

When printing the ESA Data Block, only the configured type of route data is displayed - if ESRT is defined in the ESA block, then the RLI prompt is not displayed.

Configuring route in ERL table

The token RT in the NEW ERL command specifies route number data in the ERL table. For an example of this, refer to the following:

```
NEW ERL RT <ERL #> <Route #> <AC config> <Prepend Digits> <Locator> <OSDN>
```

Figure 36: LD 117 – Configuring route in ERL table

Configuring RLI in ERL table

The token RLI in the NEW ERL command specifies the Route List Index number in the ERL table.

The Prepend Digits specified in this command applies to all routes specified in the RLI. All called number manipulations (through DMI) take effect only after this. The keyword NULL may be specified in place of the Prepend Digits, so that no routing digits are used.

```
NEW ERL RLI <ERL #> <RLI #> <AC config> <Prepend Digits> <Locator> <OSDN>
```

Figure 37: LD 117 – Configuring RLI in ERL table

Printing the ERL table

The PRT ERL output has columns for displaying both ESRT and RLI routing information. Since these routing options are mutually exclusive, data is only displayed for the active routing option for each ERL.

System alarms and messages for ESA enhanced routing

This section provides a detailed description of the system messages and alerts associated with ESA enhanced routing configuration, as shown by the following:

Table 40: System alarms and messages for ESA enhanced routing

Message Number	Severity	Event	Corrective Action	Output
SCH0214	Info	Invalid ESRT	Enter a valid ESRT.	TTY
SCH0214	Info	Invalid route type	Enter a valid route.	TTY
SCH0256	Info	Input out of range	Enter a valid route.	TTY
SCH1637	Info	Invalid RLI	Enter a valid RLI.	TTY
SCH1982	Info	No ESRT or RLI data entered	Enter a valid ESRT or RLI. Both fields cannot be blank.	TTY
SCH0099	Info	Invalid mnemonic entered	Enter a valid mnemonic, such as RLI.	TTY
ESA018	Major	Unable to route ESA call on RLI	Correct resource problem/ configuration.	TTY, SNMP
ESA019	Major	Invalid ESA RLI configuration	Correct the ESA RLI configuration	TTY, SNMP

Message Number	Severity	Event	Corrective Action	Output
ESA022	Minor	Unable to use emergency route. (Emergency call may not route to correct emergency responder.)	Follow up with emergency authorities to ensure that the emergency has been resolved, and investigate problem with the emergency route.	TTY, SNMP
ESA059	Critical	Local termination error	Follow up emergency situation, and investigate location termination problem.	TTY, SNMP
ESA062	Major	Invalid ESA RT configuration	Correct the ESA RT configuration.	TTY, SNMP
ESA063	Major	ESA RLI and RT are both unconfigured	ESA RLI and RT are both unconfigured	TTY, SNMP

Display of RLI routing information in CLIDVER

RLI routing information is displayed in the CLIDVER report.

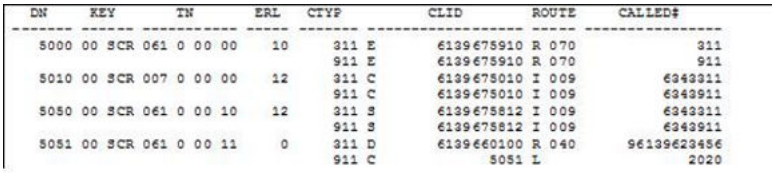
The Route displayed is the first valid route configured in the RLI that would be used for call routing in an actual emergency call. CLIDVER does not consider the dynamic availability of trunks or other network resources (either busy or disabled units).

The Called Number is the actual number as first manipulated by the ERL parameters and then by the DMI for that route entry.

The CLIDVER short form report displays routing information, with a token to make the route more informative. The tokens are interpreted as follows:

- I:route is from a Route List Index (LD 24 or LD 117).
- R means that route is from ESRT (LD 24) or Route (LD 117).
- L means Local Termination; there is no route.

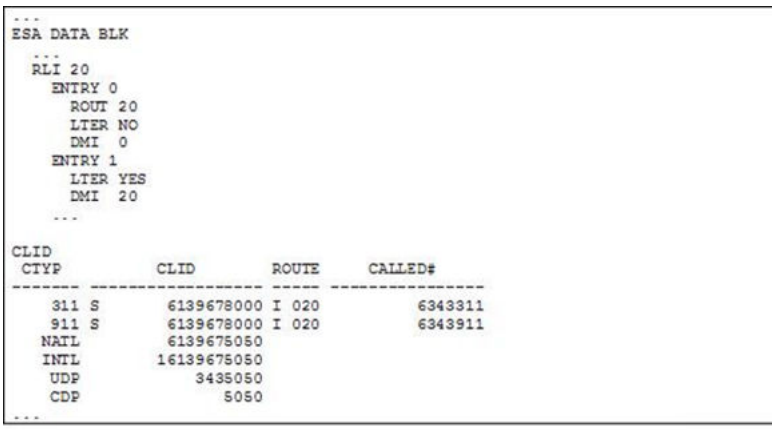
A sample of the short format CLIDVER report is as follows:



DN	KEY	TN	ERL	CTYP	CLID	ROUTE	CALLED#
5000	00 SCR	061 0 00 00	10	311 E	6139675910	R 070	311
				911 E	6139675910	R 070	911
5010	00 SCR	007 0 00 00	12	311 C	6139675010	I 009	6343311
				911 C	6139675010	I 009	6343911
5050	00 SCR	061 0 00 10	12	311 S	6139675812	I 009	6343311
				911 S	6139675812	I 009	6343911
5051	00 SCR	061 0 00 11	0	311 D	6139660100	R 040	96139623456
				911 C	5051	L	2020

Figure 38: CLIDVER report with RLI route data, short format

Also, for an example of the long format CLIDVER report, refer to the following:



```
...
ESA DATA BLK
  ...
  RLI 20
    ENTRY 0
      ROUT 20
      LTER NO
      DMI  0
    ENTRY 1
      LTER YES
      DMI  20
    ...

CLID
 CTYP          CLID        ROUTE     CALLED#
------- ------------------ ----- ----------------
    311 S       6139678000 I 020          6343311
    911 S       6139678000 I 020          6343911
   NATL         6139675050
   INTL        16139675050
    UDP            3435050
    CDP               5050
...
```

Figure 39: CLIDVER report with RLI route data, long format

The CLIDVER command works on the same principle as an emergency call and prints the configuration data relevant to the call at that point in time.

If a virtual trunk is selected for call termination, it is assumed that the call will be successful. Network parameters like available bandwidth, IP resource availability, or endpoint reachability are not considered by CLIDVER.

ESA enhanced routing packaging requirements

The ESN package is required for ESA enhanced routing:

- With Basic Alternate Route Selection, RLI=0-127 and DMI=1-255.
- With Network Alternate Route Selection, RLI=0-255 and DMI=1-255 without the Flexible Number Plan (FNP) package, or RLI=0-1999 and DMI=1-1999 if FNP package is equipped.

Dynamic ELIN

This section details the use of ELINs and Dynamic ELINs to provide emergency caller location data to the PSAP at the time of an emergency call.

The only way to convey location information to the PSAP during an emergency call is to send an ANI (CLID) that corresponds to the caller's emergency location. To this end, a reconfigured ANI, in the form of a static DID number or ELIN, is required for all potential emergency locations.

To handle network wide client mobility, every ERL is defined on every Call Server in the enterprise. Each ERL requires that a static ELIN (Locator) be assigned to an emergency caller from that location. (Multiple ERLs on the same system could be assigned a common static ELIN, or even the DFCL.) It is important to note that the static ELIN sent to the PSAP is associated with a static phone (or zone phone) for callback purposes, and not to the phone of the emergency caller.

The Dynamic ELIN feature allows preconfigured DIDs (ELINs) to be associated to an ERL, so that ESA can dynamically map a non-DID phone in that ERL (or a DID phone not at its home location) to one of these ELINs, temporarily, for location identification to the PSAP and for direct callback.

An ELIN can be assigned to an ERL as long as:

- The ELIN allow emergency calls to route to the correct PSAP using either private or public network.
- The ELIN is valid in the ALI database associated with the ERL.
- The ELIN allows callback to the call server when dialed from the PSTN.
- Multiple Call Servers providing local service to an ERL can have separate ELINs for that ERL.

The use of Dynamic ELIN functionality is optional, and applies to both IP phones and non-IP phones.

Dynamic ELIN operation

Dynamic ELIN is an association of pre-configured DID TNs to ERLs, for the purpose of sending emergency caller location data to the PSAP at the time of an emergency call.

When an emergency call is made from an ERL with an available ELIN, operation is as described as follows:

- ESA call processing assigns the ELIN to the emergency call, for routing to the PSAP and location identification.
- ESA call processing configures call forward (CFW) on the ELIN (to the DN of the emergency caller).
- A system message is generated to log the ELIN mapping.

When a callback is made by the PSAP while the ELIN is mapped, operation is as follows:

- The emergency operator calls back using the ELIN (DID number), which routes to the Call Server of the original call.
- The ELIN redirects the callback to the emergency caller DN.
- The original emergency caller is given a chance to answer the call.

Repeat emergency calls

A user making a repeat emergency call before their original Dynamic ELIN mapping has expired is handled as follows:

- If the caller has not moved since the time of the first emergency call (same ERL as original emergency call), then they keep their assigned Dynamic ELIN. The expiry time is simply refreshed.
- If the caller has moved since the time of the first emergency call (to a different ERL from the original emergency call), then a new Dynamic ELIN is assigned corresponding to the new ERL. The original ELIN remains assigned until it expires. This allows callback to the original ELIN as well as the new ELIN, which it is believed is the most sensible behavior as it provides the greater amount of coverage. The Dynamic ELIN overflow behavior helps to ensure that denial of service situations do not arise

Dynamic ELIN configuration considerations

The number of ELINs required per ERL depends on the following considerations:

- The number of non-DID users in this ERL (DID users use their DID as ANI, when they are at their originally provisioned ECL).
- The amount of possible user mobility within the ERL, and the amount of DID mobility within this ERL (how often the phone is not "at home").
- The expected (or possible) number of simultaneous emergency calls from this ERL - if a high-risk environment, consider over-provisioning dynamic ELINs to accommodate for increased emergency call traffic.
- The usage policy for the area - whether callback to the emergency caller is considered to be important, instead of a callback to a static ELIN (zone phone).

Using Dynamic ELINs with a Virtual TN

It is possible to use Dynamic ELINs with a Virtual TN - if a Virtual TN is used, the administrator must ensure that no IP phones register to the TN, as this can cause a call forward conflict (and impact emergency services resources).

- A Station Control Password (SCPW) should be configured to prevent IP phones from registering to the Virtual TN.
- Class of Service (CLS) Virtual Office User Denied (VOUD) should be configured to deny VO logins to the Virtual TN.

Before mapping a dynamic ELIN TN, ESA call processing performs a check to determine if there is a phone registered to it. If there are registered phones, the dynamic ELIN TN is rejected and an error is generated and another ELIN or the static ELIN (Locator) will be used instead.

Using Dynamic ELINs with a Phantom TN

It is possible to use Dynamic ELINs with a Phantom TN - if a Phantom TN is used, the administrator must ensure that no IP phones register to the TN, as this can cause a call forward conflict (and impact emergency services resources).

Phantom TNs must be configured with a Default Call Forward (DCFW) DN for times when regular call forward is not active (when the ELIN is not mapped).

Callback fallback

A PSAP callback is treated as a normal incoming call, and could fail if:

- The emergency caller is off-hook at time of callback (line is busy).
- The emergency caller has unregistered since the time of initial emergency call (or been pre-empted).
- The ELIN mapping has expired since the time of initial emergency call .
- The emergency caller does not answer.

The following existing features are fallback call forward mechanisms that the administrator can configure on the ELIN TNs to ensure that a callback succeeds.

Default Call Forward (DCFW)

This feature applies to Phantom TNs only.

If call forward is not active on the Phantom TN (ELIN is not mapped) then all calls to the Phantom TN DN (ELIN) route to the DCFW DN. It is recommended that the administrator configure the DCFW DN to the static ELIN (Locator) for the ERL, or perhaps the Default CLID

(DFCL) for the system. This ensures that the callback terminates if the ELIN mapping has expired.

Flexible Call Forward No Answer

This feature applies to both Virtual TNs and Phantom TNs.

If the ELIN TN's call forward mapping (the original emergency caller) does not answer, Flexible Call Forward No Answer forwards the call to the FDN configured on the ELIN TN. It is recommended that the administrator configure the Flexible Call Forward No Answer DN (FDN) to the static ELIN (Locator) of the ERL, or perhaps to the Default CLID (DFCL) for the system. This ensures that the callback terminates if the emergency caller does not answer.

Second Level Call Forward No Answer

The Second Level Call Forward No Answer (SFNA) allows unanswered calls to receive Call Forward No Answer (CFNA) treatment twice. If this feature is configured, and the emergency caller is off-hook (busy), the callback may route to the hunt DN (voicemail), which is undesirable. In this case, the best course of action is for the PSAP to call back the site billing number associated with the ELIN.

Call Forward Save on Sysload

If the system option Call Forward Save on Sysload (CFWS in LD 17) is set to YES, all sets will have their call forward status saved and set to the state they were in as of the last successful data dump following a Sysload. The post-Sysload Dynamic ELIN audit ensures that mappings that are active as (re)mapped, while mappings that are inactive are unmapped. (This is only applicable if Sysload occurs within 'x' hours after data dump, where 'x' is the Dynamic ELIN Timeout, otherwise any ELINs mapped at the time of data dump will have expired by the time of Sysload.)

Dynamic ELIN overflow option

DYNAMIC_ELIN_REUSE is used to specify Dynamic ELIN behavior if all ELINs for an ERL are in use (not expired) and another emergency call occurs, and is used as shown by the following:

Table 41: LD 17 – Dynamic ELIN overflow option

Prompt	Response	Description
DYNAMIC_ELIN_REUSE	(YES) NO	Option to specify whether to reuse the oldest ELIN or fall back to the Locator when all dynamic ELINs for an ERL are in use and another emergency call occurs.

If the overflow option is set to fall back to Locator, the static ELIN (Locator) is used for the new emergency call. If the overflow option is set to reuse oldest ELIN, the oldest ELIN mapping is remapped to the new emergency caller. In this case, the last emergency caller can be called back but not the earlier caller. Since both emergency calls have sent the same CLID to the PSAP, this is similar to the case where the static ELIN (Locator) was used.

Expired Dynamic ELIN mappings

The DYNAMIC_ELIN_TIMEOUT configuration parameter is used to specify the delay before a dynamic ELIN is unmapped.

Table 42: LD 17 – Dynamic ELIN overflow option

Prompt	Response	Description
DYNAMIC_ELIN_TIMEOUT	5-(180)-1440	The period in minutes before a dynamic ELIN mapping is timed out. Countdown to expiry begins at time of emergency call.

Emergency caller unregistrations

If the emergency caller has unregistered, the dynamic ELIN mapping becomes obsolete. Otherwise, a callback might route to an unregistered number or possibly the wrong user. This covers the following use cases:

- VO user has logged out.
- The emergency caller was pre-empted by a VO login.
- The emergency caller has unregistered due to a connectivity problem

When an emergency caller unregisters, a system message is generated.

ELIN TN configuration

This section details the configuration of analog and digital Phantom TNs, and for Virtual TNs, as shown by the following examples:

```
>ld 10
REQ: new
TYPE: 500
TN   61 0          /* Phantom TN on "analog" card */
...
ERL                /* Any value (is not used) */
...
DN  4610           /* DID DN */
...
FTR cfw 7          /* CFW + max number of digits */
FTR dcfw 7 4600    /* DCFW + max number of digits + */
                   /* DN of zone phone (Locator) or default (DCFL) */
```

Figure 40: Example configuration for analog Phantom TN

To minimize system resources, it is recommended that the most basic type of digital Phantom TN (i.e. 3903V) be configured for ELIN use

```
>ld 11
REQ: new
TYPE: 3903v
TN   65 0          /* Phantom TN on "digital" card */
...
ERL                /* Any value (is not used) */
...
DCFW 4600          /* DN of zone phone (Locator) or default (DFCL) */
KEY 0 SCR 4650     /* DID DN */
```

Figure 41: Example configuration for digital Phantom TN

To minimize system resources, it is recommended that the most basic type of Virtual TN (i.e. i2001) be configured for ELIN use:

```
>ld 11
REQ: new
TYPE: i2001
TN   69 0          /* Virtual TN */
...
ERL                /* Any value (is not used) */
...
KEY 0 scr 4690     /* DID DN */
```

Figure 42: Example configuration for Virtual TN

Administration for Dynamic ELIN

This section details the commands used in the administration of Dynamic ELINs.

Table 43: LD 117: Associate ELIN TN

Command	Description
NEW ELIN <ERL><TN>	Associate the specified TN to the specified ERL. The TN must already be configured to compose an ANI that is registered in the ALI database against this emergency location. For Large System, the TN format is “l s c u”.

- The ERL must be defined before dynamic ELINs can be configured against it.
- The NEW command does not create TNs. An ELIN (TN) must be provisioned before it can be associated to an ERL.
- The administrator must ensure that the ELIN corresponds to the same customer as the ERL.
- The NEW command reports the ESA CLID that is composed by the specified TN (according to its CLID block configuration). If the ESA CLID is invalid, the command is rejected.

Table 44: LD 117: Disassociate ELIN TN

Prompt	Description
OUT ELIN <ERL><TN>	Disassociate specified TN from specified ERL. For Large System, the TN format is “l s c u”.

The OUT command is rejected if the specified ERL or ELIN entry does not exist, automatically makes an active mapping obsolete, and generates a warning message.

Table 45: LD 117 - Print ELIN table

Prompt	Description
PRT ELIN <ERL>	Print ELINs for specified ERL.
PRT ELIN [ALL]	Print ELINs for all ERLs.

The PRT command reports the CLID composed by each TN. This ensures that TN configuration changes are reflected and that the DCFW number (if configured) is also printed.

```
> NEW ELIN 3 61 0
ERL 3, ELIN TN 61 0 added
Dynamic ELIN = 6139671234
Total number of Dynamic ELINs = 1

> NEW ELIN 1000 81 0
ERL 1000, ELIN TN 81 0 added
Dynamic ELIN = 6139675678
Total number of Dynamic ELINs = 2

> PRT ELIN
_____________________________________________________________
| ERL |     TN     |  Dynamic ELIN  |              DCFW             |
|-----+------------+----------------|-------------------------------|
|    3|61  0 0  0  |      6139671234|                     6139660100|
|-----+------------+----------------|-------------------------------|
| 1000|81  0 0  0  |      6139675678|                     6139660100|
+-------------------------------------------------------------------+
Number of Dynamic ELINs = 2
```

Figure 43: LD 117 – Example of ELIN administration

Dynamic ELIN table maintenance

This section details the commands used in administration of ELIN tables.

Table 46: LD 117 – ELIN table maintenance

Prompt	Description
STAT ELIN <ERL>	Print the current status of all ELINs in specified ERL.
STAT ELIN [ALL]	Print the current status of all ELINs in all ERLs.
STAT ELIN [<ERL>]	Print active mappings for specified ERL, or all ERLs if none is specified.

The STAT command reports the ELIN that is assigned, the mapped DN, the expiry time and the status of the mapping. This is useful for diagnostic purposes – it ensures that TN configuration changes are reflected.

Status is ACTIVE if the ELIN mapping is in effect, EXPIRED if the mapping expired within the past 30 days (is not active), or blank if the mapping expired more than 30 days ago.

A system message and the OSN record identify when an ELIN mapping was made.

```
=> stat elin
 _____ _____________ _____________ _______ ____________________________ ____________________
|     |             |             |       |                            |     Expiry Time    |
| ERL |     TN      |  Dynamic ELIN |Status |          Mapped DN         |mm/dd/yyyy hh:mm:ss|
|-----+-------------+---------------+-------+----------------------------+--------------------|
|  214|73  0 0  0   |      6139674730| FREE  |                            |                    |
|-----+-------------+---------------+-------+----------------------------+--------------------|
|  214|61  0 0  0   |      6139674610| FREE  |                            |                    |
|-----+-------------+---------------+-------+----------------------------+--------------------|
|  214|81  0 0  0   |          SCH1646|       |                            |                    |
|-----+-------------+---------------+-------+----------------------------+--------------------|
|  214|93  0 0  0   |      6139674930|EXPIRED|                        4690|07/14/2006 10:59:12|
+-----+-------------+---------------+-------+----------------------------+--------------------+
Number of Dynamic ELINs = 4
```

Figure 44: LD 117 – Example of ELIN maintenance

Configuration considerations for Dynamic ELIN

Since ERL data (routing and DN information) is customer specific, the administrator must ensure that Dynamic ELIN TNs configured for an ERL belong to the customer for which the ERL is configured. Error message ESA016 is generated during an ESA call if the customer number of the ELIN TN does not match that of the ESA caller.

Dynamic ELINs are assigned but not used in a local termination scenario. The administrator should consider factors such as other (multiple) ESDNs, local termination and enterprise networking to other systems (tandems or gateways) in determining whether Dynamic ELINs should be configured, how many should be configured or for how long the mappings should exist.

Dynamic ELIN audit

A background procedure checks if any dynamic ELINs have timed out and can be unmapped (freeing up the ELIN for reuse). This processing is initiated by the system every 30 seconds during idle cycles. This processing is transparent to the administrator, except for the generation of an Info system message.

System messages for Dynamic ELIN

The system alarms and messages associated with Dynamic ELIN are detailed in the following table:

Table 47: System alarms and messages for Dynamic ELIN

Message Number	Severity	Event	Corrective Action	Output
SCH0099	Info	Invalid Input		TTY
SCH0582	Info	Dynamic ELIN timeout out of range	Enter value from 5 to 1440.	TTY
SCH1655	Info	ERL is out of range	Enter ERL from 1 to 65535.	TTY
SCH1641	Info	ELIN TN is not configured	Enter valid ELIN.	TTY
SCH1642	Info	ELIN(s) not configured for the ERL	Enter valid TN.	TTY
SCH1643	Info	Invalid TN format entered. Enter TN as [Loop Shelf] Card Unit	Enter valid TN.	TTY
SCH1644	Info	TN is in use – IP set is registered	Enter valid TN.	TTY
SCH1645	Info	TN is already assigned to ERL <x>.	Enter valid TN.	TTY
SCH1646	Info	TN composes invalid CLID	Correct CLID configuration.	TTY
SCH1686	Info	WARNING – TN has multiple DNs	Avoid using TNs with multiple DNs as ELINs.	TTY
SCH1687	Info	Not an ELIN – TN is not a Phantom or Virtual TN	Enter valid TN.	TTY
SCH1999	Info	CFW is not configured for the given ELIN TN	Configured CFW for the ELIN TN.	TTY

Message Number	Severity	Event	Corrective Action	Output
ESA005	Major	ERL ‘x’ is not configured	Correct the ERL configuration.	TTY, SNMP
ESA006	Minor	Cannot map ELIN ‘x’ – invalid CLID	Correct the CLID configuration.	TTY, SNMP
ESA007	Minor	Cannot map ELIN ‘x’ – CFW error	Correct the ELIN configuration.	TTY, SNMP
ESA008	Warning	No free ELIN found for ERL ‘x’ – fallback options initiated	Consider provisioning additional ELINs for this ERL.	TTY, SNMP
ESA010	Major	ERL number <x> has invalid Static ELIN <dn>	Correct the Static ELIN configuration.	TTY, SNMP
ESA015	Minor	Auto Update IP phone is using ESA defaults	Follow up emergency situation – attempt to locate the caller.	TTY, SNMP
ESA016	Major	ESA caller customer number and ELIN customer number do not match <caller dn> <caller cust #> <elin dn> <elin cust #>	Check the ERL configuration, which includes route/RLI, Static ELIN, Dynamic ELINs, and OSDN	TTY, SNMP
ESA023	Info	ELIN ‘x’, DN ‘y’ is mapped to ESA caller DN ‘z’	None.	TTY, SNMP
ESA024	Info	ELIN mapping removed because ELIN was removed – TN ‘x’, DN ‘y’ is no longer CFW to DN ‘z’	None.	TTY, SNMP
ESA025	Info	ELIN mapping removed because timeout has occurred – TN ‘x’, DN ‘y’ is no longer CFW to DN ‘z’	None.	TTY, SNMP
ESA026	Info	ELIN mapping removed because phone has unregistered – TN ‘x’, DN ‘y’ is no longer CFW to DN ‘z’	None.	TTY, SNMP
ESA032	Info	ELIN ‘x’ is reused	Consider provisioning additional ELINs for this ERL.	TTY, SNMP
ESA033	Major	ELIN ‘x’, DN ‘y’ parameters cannot be	Contact your technical support.	TTY, SNMP

Message Number	Severity	Event	Corrective Action	Output
		updated for ESA caller DN ‘z’		
ESA034	Minor	Failed to remove ELIN mapping though ELIN was removed – TN ‘x’, DN ‘y’ is still CFW to DN ‘z’	Manually unmap ELIN and investigate unmap problem.	TTY, SNMP
ESA035	Minor	Failed to remove ELIN mapping though timeout has occurred – TN ‘x’, DN ‘y’ is still CFW to DN ‘z’	Manually unmap ELIN and investigate unmap problem.	TTY, SNMP
ESA036	Minor	Failed to remove ELIN mapping though phone has unregistered – TN ‘x’, DN ‘y’ is still CFW to DN ‘z’	Manually unmap ELIN and investigate unmap problem.	TTY, SNMP
SRPT233	Critical	Failed to allocate protected memory	Contact your technical support group.	TTY, RPT, SNMP
SYS0144	Major	Error loading ELIN database	Restore the ELIN database or contact your technical support group.	TTY, RPT, SNMP
TEMU024	Major	Error dumping ELIN database	Contact your technical support group.	TTY, RPT, SNMP

Callback to Multiple Appearance DNs

It is possible that the target DN of a Dynamic ELIN mapping (the emergency caller) is a Multiple Appearance DN. In this case, a callback from the PSAP causes all instances of the DN to ring.

Dynamic ELIN Survivability

As the dynamic ELIN table is stored in protected memory, it survives call server warm starts and CP switchovers (graceful and ungraceful). Active mappings are stored in protected TN blocks, and so they also survive warm starts and switchovers.

ELIN callback mappings do not survive a Call Server cold start, because the restored ELIN table (from secondary storage) is not guaranteed to be current as it depends on last data dump.

ESA call processing

ESA call processing is the feature component that selects the appropriate emergency route and composes an appropriate CLID. ESA call processing applies to both IP phones and non-IP phone, as well at attendants and incoming trunks (tandem ESA calls).

ESA call processing is separate from location management, which determines location data for an IP phone and keeps it updated. ESA call processing uses either the operational location data from the TN table (for IP phones) or the home location data in the TNB (for non-IP phones).

ERL 0

ERL 0 is a special value that indicates that basic ESA Data Block (LD 24) parameters are to be used in ESA call processing. This applies to the following:

- Non-IP phones (statically provisioned).
- Manual Update IP phones (statically provisioned).
- Auto Update IP phones not yet located by the LIS/DM – this is an error condition. Under normal circumstances, an Auto Update IP phone should not be assigned to ERL 0 by the LIS/DM.
- Auto Update IP phones that could not be located by the LIS/DM – this is an error condition. Under normal circumstances, an Auto Update IP phone should not be assigned to ERL 0 by the LIS/DM.
- Phones in a currently disabled ERL.

When an ERL is 0:

- The OSN Record will contain no Site Name or Location Description.
- It is not possible to configure Dynamic ELINs.
- Emergency route is defined in the ESA Data Block.
- OSN DN is defined in the ESA Data Block.

Route selection during ESA call processing

ESA routing options are configured in both the basic ESA Data Block (LD 24) and (optionally) the ERL table (LD117). All phone types have an ERL (Emergency Response Location) parameter that denotes their location. This location data is used to reference corresponding routing data contained in the ERL table – except for ERL 0, which is a reserved value signifying that the basic ESA Data Block should be used.

Phones configured in previous releases of software are automatically assigned an ERL value during data conversion. This ensures that route configuration is compatible with previous software releases.

Calling number composition during ESA call processing

Non-IP phones are, by definition, always at home – therefore if they have CLID block ESA data, it is always used.

The rules for composing a calling number provide backward compatibility as well as maximum coverage for potential emergency callers. The mechanisms, in order of precedence, are:

- CLID blocks (ESA fields, in LD 15), as defined in the TNB.
  - Used unconditionally for non-IP phones.
  - Used unconditionally for Manual Update IP phones.
  - Used for DID IP phones, if they are at their originally provisioned location.
- Dynamic ELIN, as defined by the associated ERL (optional).
- Locator (a static ELIN which resolves to a zone phone), as defined by the associated ERL.
- Default CLID (DFCL in LD 24), per customer.

Calling number composition for trunk-initiated ESA call

The operation of calling number composition for trunk-initiated ESA calls is as follows:

- If a valid CLID is passed in by the trunk, it is used as the calling number. Otherwise, compose calling number locally using the CLID blocks for the route.
- Routing is as defined in the basic ESA Data Block (LD 24).
- There is no Site Name and no Location Strings (in the OSN record).

Calling number composition for non 7/10 digit calling numbers

When CAMA trunks are used for ESA, a valid ANI can be 7 or 10 digits.

With previous software versions, a non 7/10 digit Default CLID (DFCL) was configurable only if customer option FNP was set to Yes. Now, if customer option FNP is set to No, a warning message is generated instead of rejecting the non 7/10 digit length DFCL. This is because the non 7/10 digit length DFCL may actually be valid on a non-CAMA trunk. Additional messages

are also generated during emergency call processing. These messages are generated only when the ANI package (12) is unrestricted, and are detailed as follows:

- SCH0429 is generated during configuration of static ELIN, dynamic ELIN, or DFCL if they are not 7 or 10 digits. This check cannot be performed for static ELINs (Locators) because the customer option FNP cannot be checked (as the customer number of a static ELIN cannot be determined from the ERL table).
  - ESA009 is generated during calling number composition if the calling number is not 7 or 10 digits.
  - ESA060 is generated during CAMA ANI processing if the calling number is not 7 or 10 digits. This is an error, and no ANI will be sent to the PSAP.

Additional system errors and messages pertaining to Ccalling number composition for non 7/10 digit calling numbers is given in the following table:

Table 48: System alarms and messages for Dynamic ELIN

Message Number	Severity	Event	Corrective Action	Output
SCH0429	Warning	Length of DFCL or Dynamic ELIN or Static ELIN is not 7 or 10. It will be discarded if used with a CAMA trunk and no ANI will be sent to the PSAP.	Correct the configuration.	TTY
ESA065	Major	Undefined CLID entry is configured for the originating DN of an ESA call. Calling number is set to customer's DFCL.	Correct the database.	TTY, SNMP
ESA066	Major	Invalid CLID length	Correct the CLID configuration.	TTY, SNMP
ESA009	Warning	The composed calling number is not 7 or 10 digits. It will be discarded if used with a CAMA trunk and no ANI will be sent to the PSAP.	Consider changing the configuration.	TTY, SNMP
ESA031	Major	Invalid DFCL	Correct the DFCL configuration.	TTY, SNMP
ESA030	Info	DFCL 'x' is used	None.	TTY, SNMP
ESA017	Major	Phone TN 'x', DN 'y' in disabled ERL 'z' has invoked ESA – using ESA defaults	Follow up emergency situation and correct the ERL configuration.	TTY, SNMP

Message Number	Severity	Event	Corrective Action	Output
ESA060	Major	The ANI is not 7 or 10 digits and the trunk is CAMA. The ANI is discarded and no ANI is sent to the PSAP.	Follow up the calling number composition. Look for system message ESA009 to track the condition.	TTY, SNMP
OSN003	Minor	ESA LOCATION NEEDS UPDATE	Follow up with emergency authorities to ensure that the emergency has been resolved and investigate why IP phone was not located.	TTY, SNMP

OSN TTY

The TTY output message type, OSN, is used for printing OSN system messages. This feature makes it practical to have a dedicated output device, like a printer, for OSN messages and may alleviate the requirement for OSN phones. A dedicated OSN TTY may also increase the robustness of 3rd party OSN alerters, since they won't have to parse other message types.

Note that ESA processing errors (ESAxx) are printed only on MTC terminals. It is reasonable that these are not printed to the OSN terminal, since they indicate a configuration or system state problem, which only a system administrator should be aware of; security personnel only need to be aware of emergency call alerts. Also, this keeps system level messages less visible on the OSN terminal than they might otherwise be.

Multiple TTYs can be configured for OSN output - this allows the deployment of TTYs at remote locations. All OSN TTYs print all system OSN messages.

An OSN TTY functions and is deployed independently of OSN phones - OSN TTYs print all system OSN system messages, while OSN phones may display only events from their associated location.

OSN TTY Administration

This section details the administration of OSN TTY.

Table 49: LD 17 – Configure an OSN output device

Prompt	Response	Description
REQ	CHG	Change.
TYPE	ADAN	Action Device And Number.
- ADAN	CHG bbb x	Change ADAN, where: bbb = TTY or HST x = port number

Prompt	Response	Description
…		
USER	OSN	OSN output device.

```
REQ PRT
TYPE ADAN TTY 11

ADAN     TTY 11
  ...
  USER MTC SCH BUG OSN
  ...

REQ ****
```

Figure 45: LD 22 – Print OSN TTY

OSN phone display

A Meridian or Succession display phone may be designated as an On-Site Notification (OSN) phone - the phone is provisioned with an OSN key to display ESA caller information. There are three types of ESA calls and the OSN phone displays relevant ESA caller information according to the call type:

- Station phone initiated ESA call.
- Attendant initiated ESA call.
- Incoming trunk initiated (tandem) ESA call.

The ESA caller information displayed on the OSN phone is designed to be compact (as only two lines are available on the phone to display the information) but informative enough to alert and notify on-site emergency personnel so that they can identify the caller.

In the case of an incoming trunk-initiated tandem ESA call, however, the information on the OSN phone displays incoming trunk information, which is not very informative to identify the emergency caller and may even confuse the emergency staff.

A common type of tandem ESA call is one from a Branch User registered at the Main Office: the ESA call is routed through the Branch Office so that it can then go to the PSAP serving the BO (the OSN phone at the branch must be in Local Mode).

Network-wide phone mobility (including VO) also results in tandem ESA calls.

Operation of OSN Phone display

The following figure shows the OSN phone display for an incoming trunk-initiated ESA call:

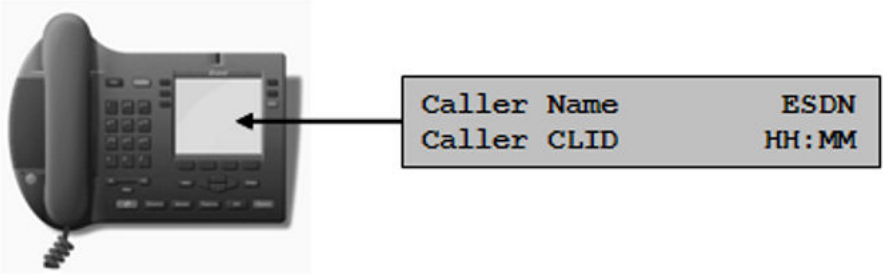


Figure 46: OSN phone display for trunk-initiated ESA call

In the preceding figure:

- Caller Name is up to 16 characters (truncated if necessary).
- ESDN is up to 7 digits.
- Caller CLID is up to 16 digits.
- HH:MM is 5 characters.

First line of display

If the emergency caller name (CPND Name), composed at the originating node, is carried across the trunk then it is printed on the first line of the display. If it is not available then as a fallback, the incoming trunk route name is printed. (In a Branch User/Main Office scenario, the caller's name is configured on the MO. It is the administrator's responsibility to maintain the MO and the BO user configurations.)

If neither the caller name nor the trunk route name are available then a language-specific string "No Name" is printed. This is to notify the on-site personnel that there is no valid name data available.

In summary, the first line of the OSN phone display shows (in order of preference) :

- Emergency caller's name, or
- Incoming trunk route name, or
- "No Name"

The first line of the display also prints the ESDN.

First line of display for DPNSS trunks

DPNSS does not transmit a caller's name (CPND) information to the far end. Therefore, a DPNSS trunk-initiated ESA call is unable to display the emergency caller name on the OSN phone. As a result, the first line of the OSN phone display shows (in order of preference) :

- Incoming trunk route name, or
- "No Name".

Second line of display

If the emergency caller CLID, composed at the originating node, is carried across the trunk and is valid then it is printed on the second line of the display. If it is not available or is invalid then a local CLID is composed according to the incoming trunk route's CLID configuration or the customer configuration (DFCL).

If there is no valid caller CLID and no valid local CLID then, as a fallback, the incoming trunk route's ACOD and RTMB are printed.

In summary, the second line of the OSN phone display shows (in order of preference) :

- Emergency caller's CLID, or
- Local trunk route CLID, or
- Local DFCL, or
- Trunk route ACOD and RTMB.

The second line of the display also prints DES or ATT# or RTMB, as appropriate.

Second line of display for DPNSS trunks

DPNSS trunks require an Originating Line Identity (OLI) string (the caller CLID), otherwise the call fails. In order to prevent intercept treatment at the originating node, if no ESA CLID is composed then the caller DN is sent as OLI. (System message ERRxxxx is generated to report this configuration error.)

When the emergency call reaches the tandem node, since the OLI (CLID) is not empty, it is passed through directly to the PSAP or security desk. However, if the CLID is the caller DN then it is not a valid PSTN number (and cannot be used for routing, ALI lookup, and callback purposes).

If the emergency call routes to the PSTN then the CLID will not be recognized and default PSAP routing will be used. If the emergency call routes to a security desk then the attendant may be unable to automatically identify the caller. The lack of an ESA CLID is an extreme misconfiguration scenario, but it is believed that the above handling is better than intercept treatment.

As a result, the second line of the OSN phone display shows (in order of preference):

- Emergency caller's CLID, or
- Emergency caller's DN.

The OSN record

When an ESA call is made, the ESA call record (system message OSN000) is generated to alert the event to the designated local security authority. At the same time, a SNMP trap is generated for the event.

OSN record for a station phone-initiated ESA call

This section details the OSN record for a station phone-initiated ESA call.

```
(Operator Data Unit)
OSN000 CUST cust#  esdn CALL ALERT
(two blank lines)

TIME: hh:mm:ss  mmm dd, yyyy
NAME: orig_name
ORIG DN: orig_dn
SITE: orig_site
LOC: orig_loc
(one blank line)

(Expert Data Unit)
DES: orig_des
SET: orig_set
ERL: erl
TER RTMB: ter_rtmb  ACOD: ter_acod
CALLED#: called#_dialed
CALLING#: calling#_sent
(one blank line)

OSN000 RECORD END
```

Figure 47: OSN record for a station phone-initiated ESA call

Where, in the preceding figure:

- cust# is the customer number, as defined using the CUST prompt in LD 10, 11, or 27.
- esdn is the customer Emergency Services DN, as defined using the ESDN prompt in LD24.
- hh:mm:ss is the 24-hour time stamp of when the call was made.
- mmm dd, yyyy is the date stamp of when the call was made (month, day, and year).
- orig_name is the name associated with the originating DN as defined using the NAME prompt in LD 95.
- orig_dn is the DN associated with the originating phone.
- orig_site is the Site Name description of the caller (from ERL table, if ERL is not zero; otherwise, orig_site is blank).
- orig_loc is the Location Description of the caller (from TN table), if the phone is an Auto Update IP phone. Otherwise, orig_loc is the ERL description of the caller (from ERL table, if ERL is not zero; otherwise, orig_loc is blank).
- orig_des is the telephone designator of the originating station phone (from its TNB).
- orig_set is the phone type of the emergency caller (IP SET, DIGITAL SET, ANALOG SET, or UNKNOWN).
- erl is the 16 bit number corresponding to ERL.
- ter_rtmb is the route and member number of the outgoing trunk on which the ESA call terminated, as defined using the RTMB prompt in LD 14.

- ter_acod is the route access code of the outgoing trunk on which the ESA call terminated.
- called#_dialed is the number that was actually dialed.
- calling#_sent is the calling number that was actually sent.

OSN record for an attendant console-initiated ESA call

The following shows the call record printed on the OSN record for an attendant console-initiated ESA call:

```
(Operator Data Unit)
OSN000 CUST cust#  esdn CALL ALERT
(two blank lines)

TIME: hh:mm:ss  mmm dd, yyyy
ORIG DN: orig_dn
NAME: att_name
SITE: orig_site
LOC: orig_loc
(one blank line)

(Expert Data Unit)
ATT: att#
ERL: erl
TER RTMB: ter_rtmb  ACOD: ter_acod
CALLED#: called#_dialed
CALLING#: calling#_sent
(one blank line)

OSN000 RECORD END
```

Figure 48: OSN record an attendant console-initiated ESA call

Where, in the preceding figure:

- att_name is the name associated with the attendant DN, as defined using the NAME prompt in LD 95.

OSN record for an incoming trunk-initiated ESA call

The following shows the call record printed on the OSN record for an incoming trunk-initiated ESA call:

```
(Operator Data Unit)
OSN000 CUST cust#  esdn CALL ALERT
(two blank lines)

TIME: hh:mm:ss  mmm dd, yyyy
NAME: caller_name
ORIG RTMB: orig_trmb  ACOD: orig_acod
CALLING# RCV: calling#_rcv
(one blank line)

(Expert Data Unit)
CALLING# COMP: esa_calling#
TER RTMB: ter_rtmb  ACOD: ter_acod
CALLED#: called#_dialed
CALLING#: calling#_sent
(one blank line)

OSN000 RECORD END
```

Figure 49: OSN record for an incoming trunk-initiated ESA call

Where, in the preceding figure:

- caller_name is the CPND of the original caller, if it is received in the trunk SETUP message. Otherwise, caller_name is the name associated with the incoming trunk route, as defined using the NAME prompt in LD 95
- calling#_rcv is the ANI (CLID) of the original caller, received from the incoming trunk.
- esa_calling# is the calling number composed by the ESA Call Termination Identification function for the originating station phone.
- orig_acod is the route access code of the incoming trunk on which the ESA call was initiated, as defined using the ACOD prompt in LD 16.

If there is a calling number received from the incoming trunk (calling#_rcv) and it is valid then it is used as the actual ESA calling number. If there is no calling number received or it is not valid then the calling number composed (esa_calling#) is used as the actual ESA calling number (calling#_sent).

Note:

DTI and DTI2 trunks do not support Calling Number or Called Number, therefore this information cannot be provided in the OSN record (or on the OSN phone).

OSN record for a locally terminated ESA call

ESA calls can now be locally terminated, using enhanced routing. The Expert Data Unit of the OSN record identifies this scenario, as in the following:

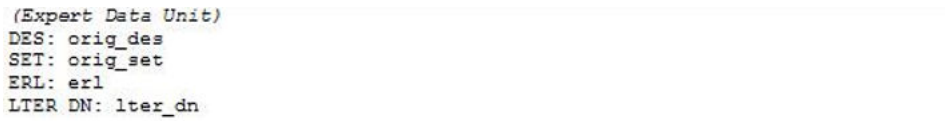


Figure 50: OSN record for a locally terminated ESA call

Where, in the preceding figure:

- lter_dn is the DN that the ESA call is terminated on, which was specified by a RLI and DMI.

ESA Misdial Prevention

The ESA Misdial Prevention feature provides the ability to prevent ESA calls that are misdialed. If an ESA DN is dialled with extra trailing digits, the system assumes the caller was trying to dial a different number - the identified misdialed call is intercepted and thus is not routed to the PSAP. The caller receives the intercept treatment as configured in the Customer Data Block. The On Site Notification (OSN) telephone is alerted and an OSN log message is recorded with misdial indication.

As a result of the operation of ESA Misdial Prevention, all normally dialed emergency calls are delayed (2 seconds by default) prior to being routed to the PSAP. Pressing the "#" (octothorpe) key (for example "9-1-1-#") results in the call being routed immediately. Administrators might consider updating the “emergency local” number to “911#” to avoid delay.

There are three types of ESA calls, as follows:

- Station phone initiated ESA call.
- Attendant initiated ESA call.
- Incoming trunk (ISDN and non-ISDN) initiated (tandem) ESA call.

Note:

The Misdial Prevention feature does not apply to attendant initiated ESA calls, BRI set initiated ESA calls, non-ISDN and ISDN trunk initiated ESA calls at the tandem node.

The ESA Misdial Prevention feature is configurable per ESDN entry.

Operation of ESA Misdial Prevention

This section details the operation of the ESA Misdial Prevention feature, for different cases.

Operation of ESA Misdial Prevention for ESA call

A configurable timer (2 seconds by default) is started once the dialed digits are recognized to be any of the ESDNs configured in LD 24 (ESA Data Block) for the caller.

If the timer expires and no additional digits are entered then the call is processed as an ESA call and routed to the PSAP. If the octothorpe key (#) is pressed within the delay period then the call is immediately processed as a normal ESA call, with no delay.

Operation of ESA Misdial Prevention for a misdialed call

If another digit (other than octothorpe) is entered within the delay period, then intercept treatment is applied to the call. It is assumed that the caller wished to make a regular call but misdialed the ESDN instead.

A configurable intercept treatment is provided for the misdialed ESA call.

Operation of ESA Misdial Prevention for On Site Notification

When an ESA call is intercepted, the On Site Notification (OSN) telephone is alerted as with an actual ESA call – no changes are incorporated in the OSN phone display. The assumption is that the call could be a real emergency and should be followed up by local emergency personnel.

A Misdial Call Alert message (OSN004) is printed on all system OSN terminals for intercepted calls. This message is similar to the actual OSN000 Call Alert message. An example of the OSN004 Misdial Call Alert message is provided by the following figure:

```
OSN004 CUST 1 911 MISDIAL CALL ALERT


TIME: 01:56:08 SEP 18, 2005
NAME: CUST1
ORIG DN: 3002
SITE: WIPRO
LOC: TOWER 8

DES: CUST1
SET: IP SET
ERL: 5
911 CALL MISDIALED - OVERFLOW

OSN004 RECORD END
```

Figure 51: OSN004 record for ESA Misdialed Call Alert

The actual intercept treatment is identified in the OSN004 record and can be one of:

- OVERFLOW
- BUSY
- ATTENDANT
- RAN ROUTE xxx

Allow Last Digit Repeat

This is an additional functionality of the ESA Misdial Prevention feature - an ESDN entry specific option is provided to enable or disable this feature.

This feature allows a repeated last digit of the ESDN to terminate the call immediately, similar to pressing the octothorpe (#) key. This is to not only ensure that an ESA call is not dropped if the last digit is accidentally dialed again (9-1-1-1), but also to process the call immediately.

Administration of ESA Misdial Prevention

This section describes the processes and commands associated with the administration of the ESA Misdial Prevention feature.

ESA Misdial Prevention feature control

Customer-specific options control the ESA Misdial Prevention feature. The prompts are located in the ESA Data Block in LD 24, ad are detailed in the following table:

Table 50: LD 24 – ESA Misdial Prevention prompts

Prompt	Response	Description
REQ	NEW CHG	Create new ESA Data Block. Change existing ESA Data Block.
TYPE	ESA	Emergency Services Access.
CUST	0-99	Customer number.
ENTR	0-15	ESDN entry.
...		
MISDIAL_PREVENTION	(NO) YES	Disable/enable ESA Misdial Prevention feature.
MISDIAL_DELAY	1-(2)-3-4	Misdial delay, in seconds.
ALOW_LAST_DIG_REPEAT	(YES) NO	Allow/Deny last ESDN digit repeat.

The valid inputs for the MISDIAL_PREVENTION prompt are YES and NO, or if nothing is entered then the default value is taken. SCH0587 is generated if any other input is entered.

If the MISDIAL_PREVENTION option is set to YES then the misdial feature is enabled. Any calls with trailing digits (other than octothorpe) dialed post ESDN receive intercept treatment.

A banner is printed to warn the administrator of the potential outcome of the feature. A second level confirmation, “ARE YOU SURE?”, is prompted for confirmation of the feature activation. The valid inputs for this prompt are YES and NO. SCH0587 is generated if any other input is

entered. Carriage return is not accepted for this prompt: SCH0703 is generated and “ARE YOU SURE?” is prompted again. An example of this is provided by the following:

```
MISDIAL_PREVENTION yes

    WARNING: THE MISDIAL PREVENTION FEATURE
    HAS THE POTENTIAL TO SUPPRESS ACTUAL
    EMERGENCY CALLS; HENCE ALL INTERCEPTED
    EMERGENCY CALLS NEED TO BE IDENTIFIED
    AND INVESTIGATED.
    SYSTEM MESSAGE OSN004 WILL BE PRINTED
    FOR THE SUPPRESSED ESA CALLS
    REFER TO NTP FOR MORE DETAILS

ARE YOU SURE? yes
```

Figure 52: MISDIAL_PREVENTION configuration example

If the MISDIAL_PREVENTION option is set to NO then the ESA call recognition feature continues to behave as it did previously.

If NO is entered for the MISDIAL_PREVENTION prompt or for the “ARE YOU SURE?” prompt then the next ENTR is prompted.

If a carriage return is entered for the MISDIAL_PREVENTION prompt for a CHG ESA block configuration then the previous value is retained. If the previous value was YES then the subsequent misdial feature options, MISDIAL_DELAY and ALOW_LAST_DIG_REPEAT, are prompted. Otherwise the next ENTR is prompted.

The warning banner is printed only once per Overlay 24 session, until the feature has been enabled (YES was entered for MISDIAL_PREVENTION and “ARE YOU SURE?”) for any of the ENTR. For a CHG ESA block, the banner is not printed if the feature was previously enabled.

MISDIAL_DELAY and ALOW_LAST_DIG_REPEAT are prompted only if the Misdial Prevention feature is enabled.

The MISDIAL_DELAY option specifies the delay, in seconds, between the time an ESDN is recognized and the emergency call is processed normally. A lower number causes a real emergency call to be processed sooner but increases the chance of a misdialed ESA call. The allowable delay values are 1, 2, 3 or 4, with a default of 2 seconds. SCH0030 is generated if any alpha character is entered; SCH0256 is generated if a numeric value beyond the allowable range is entered.

The valid inputs for the ALOW_LAST_DIG_REPEAT prompt are YES and NO, or if nothing is entered then the default value is taken. SCH0587 is generated if any other input is entered.

If the ALOW_LAST_DIG_REPEAT option is set to YES then a repeated last ESDN digit terminates the ESA call immediately. Otherwise, a repeated last digit is handled as a misdialed ESA call. This option is configurable per ESDN. The default value of this prompt is YES.

The configuration can be printed through Overlay 24, as shown in the following:

```
REQ prt
TYPE esa
CUST 1
ENTR x
...
   MISDIAL_PREVENTION yes/no
   MISDIAL_DELAY 1/2/3/4
   ALOW_LAST_DIG_REPEAT yes/no
```

Figure 53: LD 24 – Print ESA misdial configuration

Intercept treatment

A customer specific option, ESAM, specifies the type of intercept treatment provided to the misdialed caller. If RAN treatment is configured for a misdialed ESA call then it is suggested that the cause of the intercept (“you have dialed digits that resemble an emergency number, but your call has been intercepted”) and a corrective action (“please try again”) be mentioned.

The ESAM prompt is at the end of the Intercept Data Block in LD 15. This prompt is displayed if the ESA package (329) is unrestricted, and is displayed regardless of the value of the MISDIAL_PREVENTION prompt in LD 24.

The valid inputs for the ESAM prompt are as follows:

- OVF or OVFL (overflow treatment)
- BSY or BUSY (busy treatment)
- RAN (recorded announcement)
- ATT (intercept to an attendant)

The default value of this prompt is Overflow. SCH0111 is generated if invalid input is entered.

If RAN is entered for this prompt then the sub-prompt RRT is displayed. The valid input for this prompt is a preconfigured RAN route. SCH0030 is generated if any alpha character is entered; SCH0481 is generated if a numeric value beyond the allowable range is entered; SCH0406 is generated if a non-RAN route number is entered.

A example of the ESAM prompt is shown in the following figure:

```
ld 15
CDB000
...

REQ: chg
TYPE: int

TYPE INT_DATA
CUST 1
ACCD
...
ESAM ovf

REQ:
```

Figure 54: LD 15 – ESA misdialed call intercept treatment configuration

The configuration can be printed through LD 21, as shown in the following figure. This prompt is displayed if the ESA package (329) is unrestricted.

```
ld 21
CDB000
...

REQ prt
TYPE int


TYPE INT_DATA
CUST 1
ACCD ovf ovf ovf atn
...
DNDT bsy
ESAM ovf

REQ:
```

Figure 55: LD 21 – Print ESA misdial configuration

ESA Misdial configuration considerations

Administrators might consider changing the NARS access code to prevent possible misdials due to similar emergency numbers. For example, do not use ‘9’ in North America, where 9-1-1 is the usual ESDN.

Administrators must consider and accept the possibility of real emergency calls being intercepted before enabling this feature. For example, an attacker could prevent a victim from calling for help by dialing an extra digit during the emergency call dialing sequence.

Blind transfer should never be used to forward emergency calls – it is always preferable to establish a conference (No-Hold Conference) instead, so that all parties are on the line simultaneously – but especially with Misdial Prevention enabled, a blind transfer when the emergency number is misdialed will intercept the original emergency caller.

System messages

System alarms and messages associated with ESA Misdial configuration are shown in the following table:

Table 51: System alarms/messages for ESA Misdial Prevention

Message Number	Severity	Event	Corrective Action	Output
OSN004	Info	ESA MISDIAL CALL ALERT The ESDN was dialed followed by other digits. The caller may have misdialed a normal call or this may be an actual emergency call.	Follow up with the caller whether this was a misdialed normal call or an actual emergency call.	TTY, SNMP

Multiple ESDNs

This section details the recognition, configuration, and operation of multiple ESDNs within the emergency services network.

Multiple ESDN Overview

It is assumed that all ESDNs in use on the network are to be used for emergency calls only - this allows all calls being made using an ESDN to be treated at the same high priority level.

An ESDN can be a public external number or a local directory number.

The following global ESA configuration parameters are common to all ESDNs (and all customers):

- LD 17 Config Record ESA block:
  - LIS
  - SLIS_NAT_PRIV_IP
  - DYNAMIC_ELIN_TIMEOUT
  - DYNAMIC_ELIN_OVERFLOW

- EXTERNAL_DM_TIMEOUT

- LD 117 Subnet table
- LD 117 Dynamic ELIN table

The following customer specific ESA parameters are defined in an ESA Data Block (LD 24):

- A mandatory Primary ESDN.
- 15 optional additional ESDNs.
- Each ESDN can be from 1 up to 7 digits long and must be digits only.
- Duplicate ESDNs are not allowed.
- Any new ESDN cannot conflict with any existing ESDN, as illustrated by the following:
  - If ESDN 1234 exists then ESDN 123 cannot be configured - attempts to do so cause error message SCH1685 (Duplicate ESDN or shorter ESDN already exists) to be printed. Likewise, if ESDN 123 exists then ESDN 1234 cannot be configured; attempts to do so result in the same error being displayed.
- Each ESDN specifies its own routing parameters, ESRT or RLI, and DDGT. These are used for local and tandemmed (trunk initiated) emergency calls - remote calls use the ERL table for routing information – all ESDNs route to same remote gateway.
- All ESDNs use the same OSDN.
- All ESDNs use the same DFCL.

ESDNs and access code configuration

ESDN configuration is independent of ESN configuration. It is not required to dial AC1/AC2 to dial an ESDN. The following are guidelines for the configuration relating to ESDNs:

- Do not configure any internal DN or Steering Code (for CDP numbering) that conflicts with any of the ESDNs in the ESA Data Block.
- Do not configure any BARS/NARS DN (AC1/AC2 + LOC/NPA/NXX/SPN) that conflicts with any of the ESDNs in the ESA Data Block.

To dial any ESDN as AC1+ESDN or AC2+ESDN, the following conditions must be met:

- The ESDN must be configured as an SPN (Special Number) in LD 90.
- An RLI (Route List Index) must be configured with LTER=YES (to allow reprocessing of the ESDN).
- A DMI (Digit Manipulation Index) must be configured (which in this case needs to do nothing). Do not use DMI 0.

These configurations are illustrated in the following figures:

```
> ld 86
REQ new
CUST 0
FEAT dgt
DMI 3      % Pick an unused number. Don't use zero.
...        % No digit manipulation is required. AC is automatically
...        % removed by SPN processing.

REQ ****
```

Figure 56: Configuring DMI for AC+ESDN

```
> ld 86
REQ new
CUST 0
FEAT rlb
RLI 2      % Pick an unused number.
ENTR 0
...
DMI 3      % As configured in previous step.
...

REQ ****
```

Figure 57: Configuring RLI for AC+ESDN

```
> ld 90
REQ new
CUST 0
FEAT net
TRAN ac1     % Translation for AC1.
TYPE spn
SPN 911      % The ESDN.
...
RLI 2        % As configured in previous step.
...

REQ new
CUST 0
FEAT net
TRAN ac2     % Translation for AC2.
TYPE spn
SPN 911      % The ESDN.
...
RLI 2        % As configured in previous step.
...

REQ ****
```

Figure 58: Configuring SPN for AC+ESDN

Alternately, the AC1+ESDN or AC2+ESDN numbers can be configured as an alternate ESDN - for example, configure 911 as an ESDN and also 9911 and 6911 as ESDN so that the access codes 9 and 6 are part of the ESDN itself.

Administration of ESDNs

This section details the configuration of ESDNs through the ESA Data Block (LD 24), as shown by the following:

```
> ld 24
REQ new
TYPE esa
CUST 0
ENTR 0        % ESDN entry 0 (Primary ESDN)
  ESDN 911
  ESRT 80
  DDGT 911
ENTR 1        % ESDN entry 1 (additional ESDN)
  ESDN 112
  ESRT
  RLI  10
  DDGT 112
ENTR 2        % ESDN entry 2 (additional ESDN)
  ESDN 999
  ESRT
  RLI  10
  DDGT 999
ENTR          % End of ESDN entries
DFCL xxx
OSDN yyy

REQ ****
```

Figure 59: LD 24: Creating a new ESA Data Block

In the preceding figure:

- Configuration of Entry 0 (Primary ESDN) is mandatory when creating a new ESA Data Block. An error (SCH1683) is printed if this is not done.
- Configuration of Entries 1-15 (additional ESDNs) are optional:
  - An error (SCH1638) is printed for an invalid entry number.
  - An error (SCH0030) is printed if entry number contains alpha characters.
  - Error is printed when no more entries can be configured.
  - A Null input value for ENTR means the end of entries.
- Each entry made must specify an ESDN:.
  - An error (SCH0703) is printed if an entered ESDN is not configured.
  - An error (SCH1685) is printed if an entered ESDN conflicts with another shorter ESDN.
  - An error (SCH1685) is printed if an entered ESDN conflicts with another longer ESDN.
  - An error (SCH0212) is printed if an entered ESDN is too long.
  - An error (SCH0030) is printed if an entered ESDN contains alpha characters.
  - A warning (SCH2225) is printed if an entered ESDN conflicts with an existing DN.
- Each entry must specify either ESRT or RLI. An error (SCH1982) is printed if ESRT or RLI are not configured.
- Each entry must specify DDGT. An error (SCH0703) is printed if DDGT is not configured.
- Each entry also has Misdial Prevention parameters.

- DFCL is common for all the entries. A warning (SCH1979) is printed if DFCL is not configured.
- OSDN is common for all the entries. An error (SCH0278) is printed for invalid OSDN.

```
> ld 24
REQ new
TYPE ESDN (or ENTR)
CUST 0
ENTR 3        % ESDN entry 3 (additional ESDN)
  ESDN 113
  ESRI
  RLI  10
  DDGT 113
ENTR          % End of ESDN entries

REQ ****
```

Figure 60: LD 24 – Add an ESDN entry to an existing ESA Data Block

- Entry 0 (Primary ESDN) cannot be added. An error is printed if trying to add the Primary ESDN (SCH1640).
- Entries 1-15 (additional ESDNs) can be added.
  - An error is printed for invalid entry number (SCH1638).
  - An error is printed if entry number contains alpha characters (SCH0030).
  - An error is printed when no more entries can be configured.
  - A Null input for ENTR means end of entries.
- Each entry must specify ESDN.
  - An error is printed if ESDN is not configured (SCH0703).
  - An error is printed if ESDN conflicts with another shorter ESDN (SCH1685).
  - An error is printed if ESDN conflicts with another longer ESDN (SCH1685).
  - An error is printed if ESDN is too long (SCH0212).
  - An error is printed if ESDN contains alpha characters (SCH0030).
  - A warning is printed if ESDN conflicts with an existing DN (SCH2225).
- Each entry must specify ESRT or RLI - an error is printed if ESRT or RLI are not configured (SCH1982).
- Each entry must specify DDGT - an error is printed if DDGT is not configured (SCH0703).
- Each entry also has Misdial Prevention parameters
- DFCL and OSDN cannot be added here, since this data is not ESDN specific.

```
> ld 24
REQ chg
TYPE ESDN (or ENTR)
CUST 0
ENTR 1       % Change ESDN entry 1
  ESDN 112
  ESRT 1
  DDGT 112
ENTR x4      % Remove ESDN entry 4
ENTR         % End of ESDN entries

REQ ****
```

Figure 61: LD 24 – Change or remove an ESDN entry from an ESA Data Block

- Any ESDN entry including Entry 0 (Primary ESDN) can be changed.
  - An error is printed for invalid entry number (SCH1638).
  - An error is printed if entry number contains alpha characters (SCH0030).
  - An error is printed if trying to change a non-existent entry (SCH1668).
  - The ESDN can be changed.
    - An error is printed if ESDN conflicts with another shorter ESDN (SCH1685).
    - An error is printed if ESDN conflicts with another longer ESDN (SCH1685).
    - An error is printed if ESDN is too long (SCH0212).
    - An error is printed if ESDN contains alpha characters (SCH0030).
    - A warning is printed if ESDN conflicts with an existing DN (SCH2225).
  - The ESRT or RLI can be changed.
  - The DDGT can be changed.
  - The Misdial Prevention parameters can be changed.
- Any entry, other than Entry 0 (Primary ESDN) can be deleted.
  - An error is printed if trying to remove the Primary ESDN (SCH1647).
  - An error is printed if trying to remove an undefined entry (SCH1668).
- New entries cannot be added here.
- Common ESA data (DFCL, OSDN) cannot be changed here.
- A Null input for ENTR means end of the entries.

```
> ld 24
REQ out
TYPE ESDN (or ENTR)
CUST 0
ENTR 1        % Delete ESDN entry 1
ENTR 3        % Delete ESDN entry 3
ENTR          % End of ESDN entries

REQ ****
```

Figure 62: LD 24 – Remove an ESDN entry from an ESA Data Block

- The input to the ENTR prompt need not be prefixed with ‘x’.
- Any ESDN entry except Entry 0 (Primary ESDN) can be deleted.
  - An error is printed for invalid entry number (SCH1638).
  - An error is printed if entry number contains alpha characters (SCH0030).
  - An error is printed if trying to remove the Primary ESDN (SCH1647).
  - An error is printed if trying to remove an undefined entry (SCH1668).
- A new entry cannot be added here.
- Entries cannot be modified here.
- The ESA Data Block cannot be deleted with this command.
- A Null input for ENTR means end of the entries.

```
> ld 24
REQ out
TYPE esa
CUST 0

REQ ****
```

Figure 63: LD 24 – Remove an ESA Data Block

- The whole ESA Data Block can be deleted without deleting ESDN entries first.
- Error is printed if trying to remove an ESA Data Block that is not configured (SCH1630).

```
> ld 24
REQ chg
TYPE esa
CUST 0
ENTR 1        % Change ESDN entry 1
  ESDN 999
  ESRT
  RLI  10
  DDGT 999
ENTR x2       % Delete ESDN entry 2
ESDN          % End of ESDN entries
DFCL xxx
OSDN yyy

REQ ****
```

Figure 64: LD 24 – Change an ESA Data Block

- Any Entry including Entry 0 (Primary ESDN) can be changed.
  - An error is printed for invalid entry number (SCH1638).

- An error is printed if entry number contains alpha characters (SCH0030).
- An error is printed if trying to change a non-existent entry (SCH1668).
- The ESDN can be changed.
  - An error is printed if ESDN conflicts with another shorter ESDN (SCH1685).
  - An error is printed if ESDN conflicts with another longer ESDN (SCH1685).
  - An error is printed if ESDN is too long (SCH0212).
  - An error is printed if ESDN contains alpha characters (SCH0030).
  - A warning is printed if ESDN conflicts with an existing DN (SCH2225).
- The ESRT or RLI can be changed.
- The DDGT can be changed.
- The Misdial Prevention parameters can be changed.

• Any Entry, other than Entry 0 (Primary ESDN) can be deleted.

- An error is printed for invalid entry number (SCH1638).
- An error is printed if entry number contains alpha characters (SCH0030).
- An error is printed if trying to remove the Primary ESDN (SCH1647).
- An error is printed if trying to remove an undefined entry (SCH1668).

• A new entry cannot be added here.

• Common ESA data (DFCL, OSDN) cannot be changed here.

• Null input for ENTR means end of the entries.

• DFCL is common for all the entries and can be modified - a warning is printed if DFCL is not configured (SCH1979).

• OSDN is common for all the entries and can be modified - an error is printed for an invalid OSDN (SCH0278).

```
> ld 24
REQ prt
TYPE esa
CUST 0

CUST 0
ENTR 0
  ESDN aaa
  ESRT bbb
  RLI  ccc
  DDGT ddd
ENTR 1
...
DFCL xxx
OSDN yyy

REQ ****
```

Figure 65: LD 24 – Print an ESA Data Block

- Error message is printed if ESA Data Block is not configured (SCH0152).
- ESDN entries are printed as part of ESA Data Block.
- Each entry also has Misdial Prevention parameters.

```
> ld 24
REQ prt
TYPE ESDN (or ENTR)
CUST 0
ENTR 0
  ESDN aaa
  ESRT bbb
  RLI  ccc
  DDGT ddd

REQ ****
```

Figure 66: LD 24 – Print an ENTR of the ESA Data Block

- An error is printed if the ESA Data Block is not configured (SCH1630).
- An error is printed if the ESDN entry is not configured (SCH1668).
- An error is printed for invalid entry number (SCH1638).
- An error is printed if entry number contains alpha characters (SCH0030).
- An error is printed if trying to change a non-existent entry (SCH1668).
- Only one entry can be printed at a time. Repeat the steps to print additional entries, or use PRT ESA to print the entire ESA Data Block including all ESDNs.
- Common ESA Data Block parameters (DFCL, OSDN) are not printed in the output.

CLIDVER for multiple ESDNs

The short format of this report already has a field for call type (CTYP), which is reused for additional ESDNs, as shown in the following figure:

```
  DN     KEY       TN       ERL   CTYP          CLID        ROUTE     CALLED#
------- ------ ---------- ----- ------- ------------------ ----- ----------------
   5000 00 SCR 061 0 00 00    10     311 E       6139675910 R 070              311
                             911 E       6139675910 R 070              911
   5010 00 SCR 007 0 00 00    12     311 C       6139675010 I 009          6343311
                             911 C       6139675010 I 009          6343911
   5050 00 SCR 061 0 00 10    12     311 S       6139675812 I 009          6343311
                             911 S       6139675812 I 009          6343911
   5051 00 SCR 061 0 00 11     0     311 D       6139660100 R 040      96139623456
                             911 C            5051 L                   2020
```

Figure 67: Example CLIDVER output with multiple ESDNs, short format

The long format of this report prints ESA data for all configured ESDNs as shown by the following figure:

```
...
ESA DATA BLK
  ...
  RLI 20
    ENTRY 0
      ROUT 20
      LTER NO
      DMI  0
    ENTRY 1
      LTER YES
      DMI  20
    ...

CLID
 CTYP          CLID        ROUTE     CALLED#
------- ------------------ ----- ----------------
    311 S       6139678000 I 020          6343311
    911 S       6139678000 I 020          6343911
   NATL         6139675050
   INTL        16139675050
    UDP            3435050
    CDP               5050
...
```

Figure 68: Example CLIDVER output with multiple ESDNs, long format

Data conversion for multiple ESDNs

If the previous release had an ESA Data Block configured then:

- The previous ESDN, ESRT and DDGT becomes the ENTR 0 (Primary ESDN) data.
- No additional ENTR exist.
- DFCL and OSDN are retained.

If the previous release did not have an ESA Data Block configured then data conversion is not required. The user must configure a new ESA Data Block to use this feature.

System messages for multiple ESDN

The following system messages are identified for the implementation of the multiple ESDN functionality.

Table 52: System messages for multiple ESDN

Message Number	Severity	Description	Corrective Action	Output
ESA067	Major	VO ESA call is processed using Primary ESDN instead of unknown ESDN	Follow up emergency situation and configure the unknown ESDN similarly in all systems in the enterprise network.	TTY, SNMP
ESA042	Major	ESA call not processed due to data corruption	Check with the system administrator.	TTY, SNMP
SCH0703	Info	NULL input is not allowed	Enter an input value.	TTY
SCH1638	Info	Invalid Entry input	Enter a valid input in the range [0-15].	TTY
SCH1640	Info	Duplicate Entry input	Entry configuration exists. Enter a different input in the range [0-15].	TTY
SCH1647	Info	Cannot delete Entry 0 (Primary ESDN)	Use CHG to change Entry 0 (Primary ESDN).	TTY
SCH1668	Info	ESDN entry does not exist in this ESA Data Block	Configure the ESA ESDN entry first.	TTY
SCH1683	Info	Entry 0 (Primary ESDN) is not configured	Configure Entry 0 (Primary ESDN).	TTY
SCH1684	Info	Invalid ESDN	Enter a valid input for ESDN. An ESDN can be configured up to 7 digits.	TTY
SCH1685	Info	Duplicate ESDN or shorter ESDN exists	ESDN configuration already exists. Enter a different ESDN input.	TTY
SCH1630	Info	ESA Data Block does not exist for this customer	Configure the ESA Data Block first.	TTY
SCH2225	Warning	ESDN conflicts with the existing DN	Configure a different ESDN.	TTY
SCH2226	Warning	DN conflicts with an existing ESDN	Configure a different DN.	TTY

Availability/survivability scenarios

It is essential that reasonable ESA handling be provided to phones even during failure scenarios, within the limits of the remaining resources. Degraded performance, particularly in the tracking mobility of clients, is acceptable. However, emergency calls must complete in the best manner available.

Cached location data survives if the phone simply reconnects or performs a soft-reset - if the phone hard-resets, the cached location data does not survive. In the following examples, an IP phone should retain its cached location data:

- TLAN interruption (if the defined watchdog timer value expires or a key is pressed).
- TPS restarts (if the defined watchdog timer value expires or a key is pressed).
- In the event that the IP phone registers to a geographically redundant call server, an alternate call Server, or to a backup TPS.

Survivability for call server restarts or switchovers

Full service is eventually restored after a call server restart or a call processor switchover (either graceful and ungraceful). In the event that a restart of switchover occurs, the subsequent location update may be delayed, but location data cached either in the phones or in the TPS is available until the LIS or DM provides the necessary updates.

The TN table is stored in unprotected memory, and as such must be rebuilt when the IP phones register on the network following the restart or switchover.

If the Call Server restarts quickly enough, the IP phones remain connected to their TPS.

- Location data from the TPS is copied back to the TN table during phone registration.
- If the system is configured to obtain location updates from an External DM, the Needs Update flag is preserved (by the TPS) and no further location updates are required.
- If the system is configured to obtain location updates from a Subnet LIS, the Needs Update flag is set for all Auto Update IP phones, requiring background relocation.

If the Call Server does not restart quickly enough, the IP phones also restart.

ESA call processing uses the best available location data for IP phones – the operational location data stored in the TN table.

IP phone restarts due to call server restarts

If an IP phone restarts:

- Location data cached on the phone itself is used until a location update is available.
  - Location data is cached in DRAM on the IP phone, and will survive a restart but not a power cycle.
- If the system is configured to obtain location updates from an External DM, the location update is provided in response to the IP phone connecting to the network. If the location update is provided before the phone registers with the call server, then the updated location is part of the normal registration message - otherwise an additional location update is required.
- If the system is configured to obtain location updates from a Subnet LIS, the Needs Update flag is set for the (Auto Update) IP phone in response to its registration, requiring a background relocation.

Switching to an alternate call server

Since no protected memory is synchronized to the Alternate Call Server, all dynamic data (for example, dynamic ELIN mappings) is lost. Otherwise, this is similar to a Call Server restart: if the switch to the Alternate Call Server is fast enough, the IP phones remain connected to their TPS - if not, the IP phones restart.

Survivability for geographic redundant systems

Manual Update phones have static location data.

Auto Update phones have dynamic location data (stored in the TN table) which is populated at regular intervals on the geographically redundant system. Registration and location determination occurs as normal except that a large number of sets will connect to the redundant server at the same time. Location data cached on the phone itself is used until a location update is available.

Survivability for signaling server restart

If the Signaling Server restarts, the connected IP phones also restart. Registration and location determination occurs as normal except that a large number of sets will connect at about the same time. Location data cached on the phone itself is used until a location update is available.

Survivability for Survivable Branch Office

A Survivable Branch Office or Survivable Call Server (for SMG and SSMG) provides local ESA service if it becomes isolated from the Main Office or Primary Call Server, as follows:

- The SBO/SMG/SSMG is essentially a standalone system (Local Mode).
- Branch User IP phones reconnect to the Branch Office TPS, and register to the SBO call processor.
- The SBO/SMG/SSMG must have its own ESA trunks defined for routing to a PSAP; otherwise, the ESA call must be terminated locally.

Geographical Redundancy or Survivable Branch Office uses GR N-Way data replication model, which means all of the CS including Main Office, Geographical Redundant Main Office and Branch Office have the same data stored. Any given Branch Office SIP phones a GR/ Survivable Branch Office uses GR N-Way data replication model, which means all of the CS including MO, GRMO and BO have the same data stored. Any given BO SIP phones should be able to register through BO, MO or GRMO depends on which failover case.

Geographical Redundancy or Branch Office SLG sends keep alive messages regularly and they are critical decision maker in case of any incoming registration or calls based on background keep-alive mechanism.

Survivability for Survivable Remote Gateway

A Survivable Remote Gateway (SRG) provides local emergency call handling similarly to a SBO:

- An SRG is essentially a stand-alone system.
- IP phones reconnect and register to the SRG.
- The SRG must have its own CO trunks to route to a PSAP.

The SRG does not support location management, which includes cached data on phone sets, interaction with the Subnet LIS, or an interface to the External DM. Therefore, emergency handling depends on statically configured data.

Survivability for External DM failure

If the External DM fails or otherwise loses connection with the TPS, the loss of connectivity is detected and system messages are printed. The TPS retains the last known (operational) location of the IP phones. This data is lost if a phone reconnects to a TPS, unless the location data is cached on the phone.

When communication is restored between the External DM and the TPS, the DM takes one of two approaches (depending upon the reason for the failure) as follows:

- If the failure of the DM was due to a restart then the DM will rediscover the connected IP phones and provide location updates upon completion of the restart. This activity may take an extended period of time depending on the number of connected IP phones.
- If the failure of the DM was due to a loss of communications, then the DM will detect any phones requiring location updates using the normal audit process and provide location updates for these phones only.
- The TPS also filters any duplicate location updates, to prevent unnecessary messages to the Call Server.

System Management

Element Manager (EM) can be used to manage the emergency services data contained in the System Configuration record, the Emergency Services Access (ESA) Data Block (LD 24), the Misdial Intercept Treatment in the Customer Data Block (CDB), the Subnet Location Information Service (LIS) table, the Dynamic Emergency Location Information Number (ELIN) table, and the Emergency Response Location (ERL) table.

To facilitate the management of this data, a new subsection called Emergency Services is added under the System section of the EM navigator. When expanded, the following links are displayed by the new Emergency Services subsection:

- Service Parameters
- Access Numbers and Routing
- Response Locations
- Subnet Information
- Dynamic Identification

Service Parameters (LD 17)

The Service Parameters link contains system wide timeout settings for LIS, ELIN, and the DM. The EM user interface allows the administrator to modify these parameters.

User interface

To access the Service Parameters page:

1. Select **System**.
2. Select **Emergency Services**.
3. Select **Service Parameters**.

The Service Parameters page is as shown in the following figure.

Figure 69: LD 17 - EM Service Parameters

There are three configurable parameters displayed on this page: LIS, DYNAMIC_ELIN_TIMEOUT, and DYNAMIC_ELIN_REUSE.

Acceptable LIS responses depend on the ESA Subnet LIS package (336) and the ESA External DM package (337).

The Dynamic ELIN prompts depend on the ESA Calling Number Mapping package (331).

In addition to these prompts:

- If the value for LIS is selected as “Internal Subnet Location Information Service” then another prompt with a check box for “Lookup Private IP Address for Subnet (SLIS_NAT_PRIV_IP)” is displayed.
- If the value for LIS is selected as “External Discovery Manager” then a prompt with an input box for “External Location Update Timeout (EXT_DM_UPDT_TIMEOUT)” is displayed.

Access Numbers and Routing (LD 24)

The Basic ESA Data Block (LD 24) contains call processing details for emergency calls, and are location specific. That is, the ESA Data Block defines a particular emergency call handling process for the local area serviced by a particular call server. An ESA Data Block should be configured for every individual customer site.

The EM user interface for Access Numbers and Routing allows the administrator to perform the following actions with regard to configuring the Basic ESA Data Block (LD 24):

- Creation of a new ESA Data Block.
- Deletion of an existing ESA Data Block.
- Modification of an existing ESA Data Block.
- Creation of additional ESDN entries.
- Listing of the currently configured ESDN entries.
- Modification of an existing additional ESDN entry.
- Deletion of an existing additional ESDN entry.

User interface

To access the Access Numbers and Routing page:

1. Select **System**.
2. Select **Emergency Services**.
3. **Access Numbers and Routing**.

The Access Numbers and Routing page displays all the configured ESA Data Blocks as shown in the following figure.

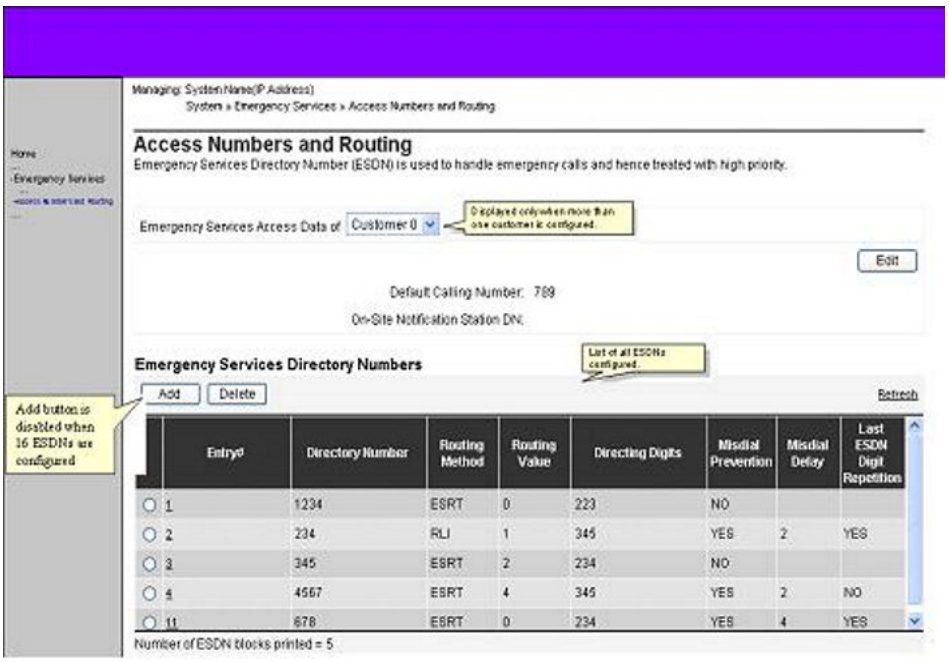


Figure 70: LD 24 - EM Access Numbers and Routing

The latest ESA Data Block (LD 24) information is displayed by the Refresh link by pulling it directly from the Call Server.

If there are no ESA Data Blocks are configured for the call server, a confirmation message is displayed that indicates this fact. The responses to this configuration message are detailed as follows:

- Clicking OK for this confirmation message causes the Customers page to be displayed, where a new customer may be added.
- If the **Cancel** button is clicked for this configuration message, the Home page is displayed.

If only one customer is configured but no ESA Data Block is configured as yet for that customer, The Add Customer (XX) Emergency Services Directory Number page is displayed after clicking the **Access Numbers and Routing** link in the navigator.

When there is more than one customer configured but no ESA Data Blocks are configured for any of those customers, the Add Customer (XX) Emergency Services Directory Number page is displayed after clicking the **Access Numbers and Routing** link in the navigator. By default, the customer displayed is the customer with lowest number. For example, if there are two customers configured, Customer 0 and Customer 1, the page displayed will be Add Customer 0 Emergency Services Directory Number.

When there are no routes or Route List Indexes (RLIs) configured for the customer, a confirmation message is displayed:

```
There are no routes configured for the customer! To add a new route click on [OK].
```

Responses to this confirmation message operate as follows:

- Clicking **OK** for the confirmation message causes the Customer (XX), New Route Configuration page to be displayed. After the successful configuration of ESA routing information, the Add Customer XX Emergency Services Directory Number page is displayed, along with the newly configured route data.
- Clicking **Cancel** for the confirmation message causes the Access Numbers and Routing page to be displayed with an empty table and all buttons disabled.

If ESA Data Blocks are configured for more than one customer, the ESA data displayed on the Access Numbers and Routing page is for the lowest customer number. ESA data for the other customers can be viewed by selecting the corresponding customer number from the Emergency Services Access Data of drop down list. If the ESA block for that particular customer is not configured, the Add Customer (XX) Emergency Services Directory Number page is displayed.

If there are no routes or Route List Indexes (RLIs) configured for the customer then the behavior is same as already described - the difference is that the Access Numbers and Routing page for the lowest customer number with an ESA block configured is displayed by clicking the Cancel button in the confirmation message or Customer (XX), New Route Configuration page.

The Access Numbers and Routing page has two sections.

Emergency Services Access data:

The configured Emergency Services Access data for the selected customer number is displayed in this area - common ESA data for the selected customer can be viewed in this section.

Clicking the **Edit** button in this section causes the Edit Customer (XX) Emergency Services Access data page to load for the customer number currently being viewed, allowing the customer's ESA data to be changed.

Emergency Services Directory Numbers:

A table is displayed in this section that contains the ESDN information, as configured for the customer number currently being viewed. The first ESDN entry displayed in the table is always the Primary ESDN (the ESDN with entry number 0), for which configuration is mandatory. The Emergency Services Directory Numbers table updates itself dynamically to reflect ESDN data for the currently selected customer.

An ESDN entry can be added for a customer by clicking the **Add** button. Additional ESDN entries can be edited by clicking on the Entry # hyperlinks contained in the table. The Add button is disabled when the maximum number of ESDN entries (16) has already been configured for the customer.

Additional ESDN entries can be deleted by selecting the radio button for the ESDN entry and then clicking on the Delete button. Deleting a customer's Primary ESDN (ESDN 0) will actually delete the entire ESA Data Block for that customer. A confirmation message is displayed if an attempt is made to delete a customer's Primary ESDN, as follows:

After clicking **OK** for the confirmation message, the selected customer's ESA Data Block is deleted, and the Access Numbers and Routing page is displayed, showing the ESA data of the next lowest available customer number. If no other customers are configured, a redirection is made to the Element Manager Home page.

Adding an ESDN

The Add Customer (XX) Emergency Services Directory Number page is displayed when the administrator clicks on the Access Numbers and Routing link and no ESA blocks are currently configured. The first ESDN added to each ESA Data Block is always the Primary ESDN (ESDN 0).

The Add Customer (XX) Emergency Services Directory Number page contains the following prompts:

1. Directory Number
2. Directing Digits
3. Default Calling Number (this is a common ESA parameter)
4. On Site Notification DN (this is a common ESA parameter)
5. Routing Method: Either ESA Route or ESA RLI can be configured.
    - When the routing method is selected as Route Number (by clicking on the radio button), the Route List Index field becomes inactive, and vice versa. Only the selected routing option is saved on the call server.

- Available routes configured for a particular customer are displayed in The Route Number select box - if the list exceeds 30 then the administrator can enter the route value in the select box itself.
- Available Route List Index (RLI) numbers are displayed in the Route List Index field selection box.
- If there are no ESA Route or ESA RLI data configured then the corresponding row is disabled and "Not Configured" is displayed in the dropdown list.

6. Misdial Prevention:
    - This option is used to enable or disable the Misdial Prevention feature. If there is a check in the check box, the Misdial Prevention feature is enabled – this means that any ESDN dialed with trailing digits will receive intercept treatment.
    - The Misdial Prevention feature is disabled by default.
    - If Misdial Prevention is enabled by selecting the check box, the following confirmation message is displayed:
    - Clicking OK for this confirmation message means that Misdial Prevention will be enabled (which means. therefore, that clicking Cancel disables Misdial Prevention). The default value of the confirmation message is Cancel.
7. Misdial Delay:
    - If Misdial Prevention is enabled, the Misdial Delay value is used as the time delay (in seconds) during which a misdialed ESDN may be intercepted. The default value is 2 seconds, with the option to specify a value between 1 and 4 seconds.
    - This prompt is displayed only if the Misdial Prevention feature is enabled.
8. Last ESDN Digit Repetition:
    - If Misdial Prevention is enabled, this option allows an emergency call to be placed, even if the last digit in the ESDN is repeated during dialing.
    - By default this prompt is enabled, but is only displayed if the Misdial Prevention feature is enabled.
    - The ESA Data Block is successfully configured if, after clicking the Save button, the Access Numbers and Routing page is loaded with the newly configured ESA data for the customer. Clicking the Cancel button aborts the present unsaved configurations and loads the Home page.

The following figure shows the page layout of Add Customer XX Emergency Services Directory Number. The page for the primary ESDN also contains the common ESA parameters.

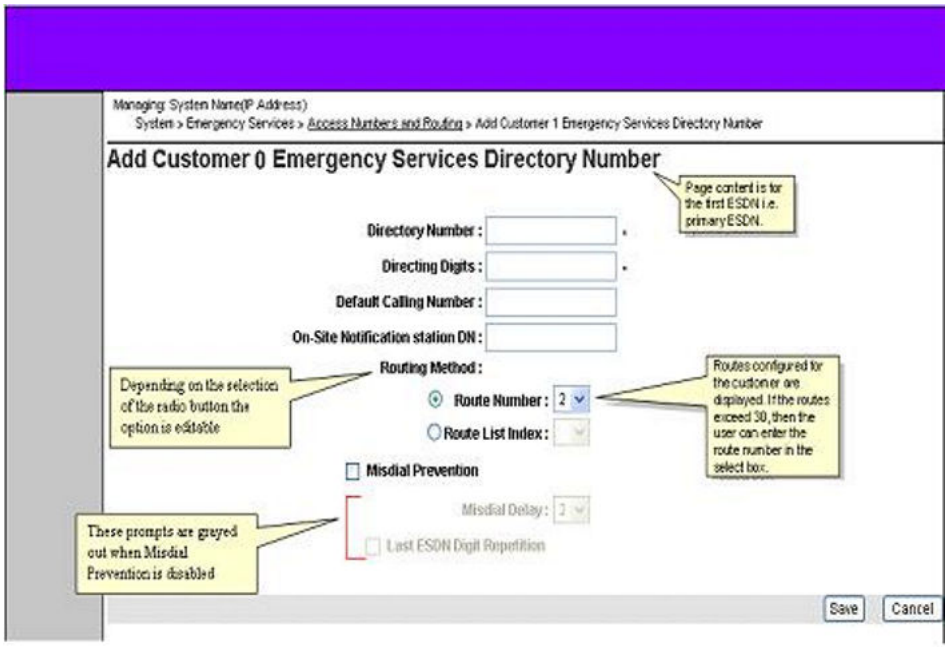


Figure 71: EM - Add Primary ESDN

Adding an additional Emergency Services DN

The Add Customer (XX) Emergency Services Directory Number page is displayed when the Add button is clicked on the Emergency Services Directory Numbers table. The page layout and prompts are as described by the following:

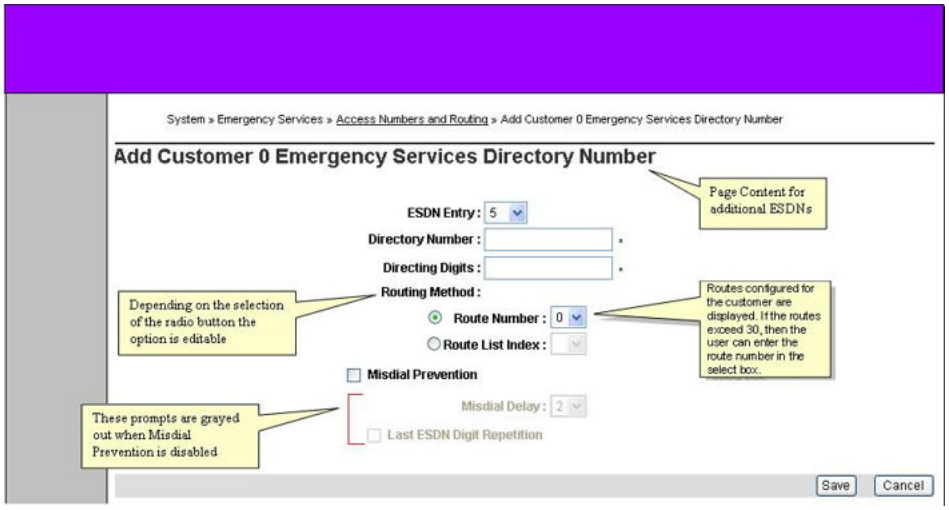


Figure 72: EM – Add additional ESDNs

This page contains the following prompts:

1. ESDN Entry
2. Directory Number
3. Directing Digits
4. Routing Method: Configuration is identical to that described for adding a single ESDN.
5. Misdial Prevention: Configuration is identical to that described for adding a single ESDN.
6. Misdial Delay: Configuration is identical to that described for adding a single ESDN.
7. Last ESDN Digit Repetition: Configuration is identical to that described for adding a single ESDN.

Editing an ESDN

The Edit Customer (XX) Emergency Services Directory Number page is displayed when the ESDN Entry # hyperlink is clicked on the Emergency Services Directory Numbers table.

The prompts listed on this page are the same as those listed on the Add Customer (XX) Emergency Services Directory Number page, except that the ESDN Entry field is not displayed on this page. The number for the ESDN entry currently being configured is updated on the page title.

Editing the common ESA data

The Edit Customer 0 Emergency Services Access Data page is loaded when the administrator clicks the Edit button in the Emergency Services Access Data section. The Edit Customer 0 Emergency Services Access Data page allows the configuration of the ESA data that is common to all ESDN entries (Default Calling Number and On-Site Notification DN).

Emergency Response Locations (LD 117)

The existing Branch Office Emergency Service Information page has been removed from the Zones section of Element Manager, and has been replaced with the new Emergency Response Locations page with its enhanced parameter list.

Also, the maintenance command PRT ZESA is removed from the Zone Diagnostic page.

The Emergency Response Locations page is as shown in the following figure:

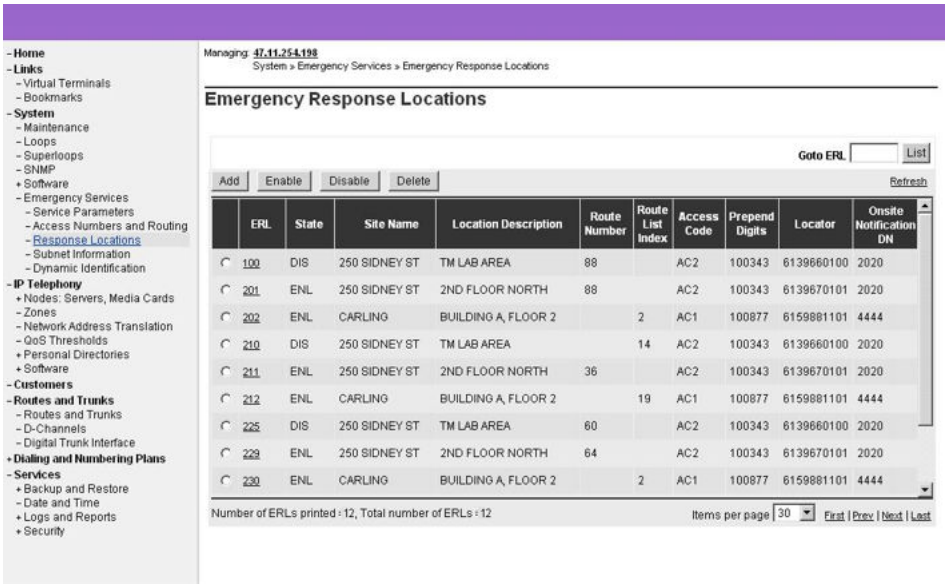


Figure 73: EM – Emergency Response Locations

The Emergency Response Locations (LD 117) user interface allows the administrator to perform the following actions:

- Create a new ERL.
- Delete an existing ERL.
- Modify an existing ERL.
- List configured ERLs.

User interface

To access the Emergency Response Locations page:

1. Select **System**.
2. Select **Emergency Services**.
3. Select **Response Locations**.

The Emergency Response Locations page lists every configured ERL in a table format. There is a paging mechanism in place to display the configured ERL records in sets of a specified amount (for example, 20 records at a time). This provides ease of navigation across the (potentially) many pages of configured ERLs.

To display a selected number of ERL records at a time:

- Click the Items per page drop down menu and select the number of simultaneous records to display.
- There are four record display types listed as links immediately to the right of the Items per page drop down menu. Depending on the desired display, choose one of the options, which are described as follows:
  - The first group of ERL records, in the amount specified using the Items per page drop down menu, is displayed using the **First** link, starting with the lowest ERL Entry number.
  - The previous set of ERL records, in the amount specified using the Items per page drop down menu, are displayed using the **Prev** link, ending at the first ERL record of the current list.
  - The next set of configured ERL records, in the amount specified using the Items per page drop down menu, is displayed using the **Next** link, starting with last ERL record of the current list.
  - The last group of ERL records, in the amount specified using the Items per page drop down menu, is displayed using the **Last** link.

It is also possible to display either a specific ERL record or a list of ERL records starting with a specific number, by entering a number in the Goto ERL text box and clicking on List button. If the ERL specified does not exist, the next group of configured ERL records is displayed, just as though the Next link was clicked.

ERL entries can be enabled, disabled or deleted by clicking the radio button for the desired ERL record and clicking on the corresponding button - Enable, Disable, or Delete - at the top of the Emergency Response Locations table.

The Add Emergency Response Location page, which allows the user to add a new ERL, is displayed by clicking the Add button on the Emergency Response Locations page. This page is shown in the following figure:

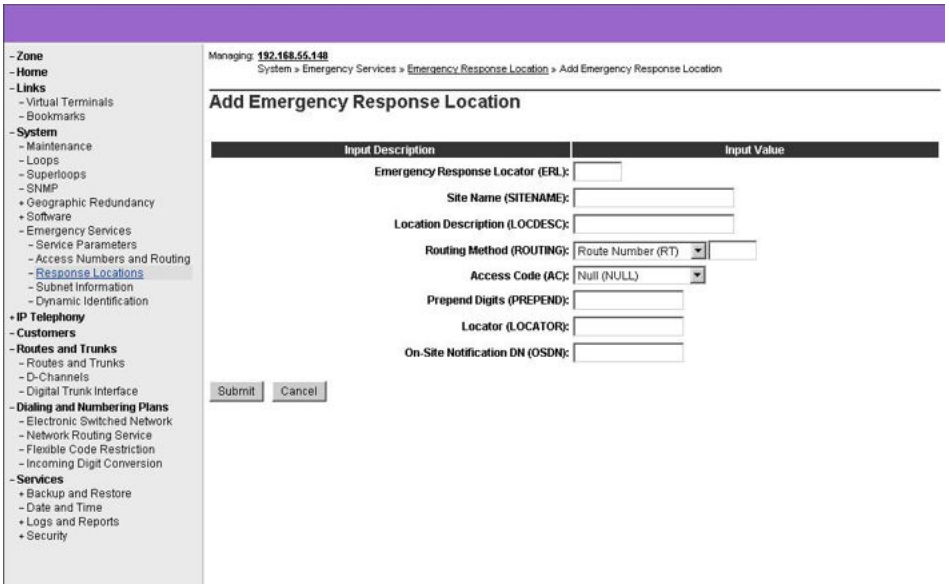


Figure 74: EM – Add Emergency Response Location

When the ERL entry hyperlink is clicked in the table on the Emergency Response Location page, the Edit Emergency Response Location page is displayed. This page allows the user to edit the data of the selected ERL.

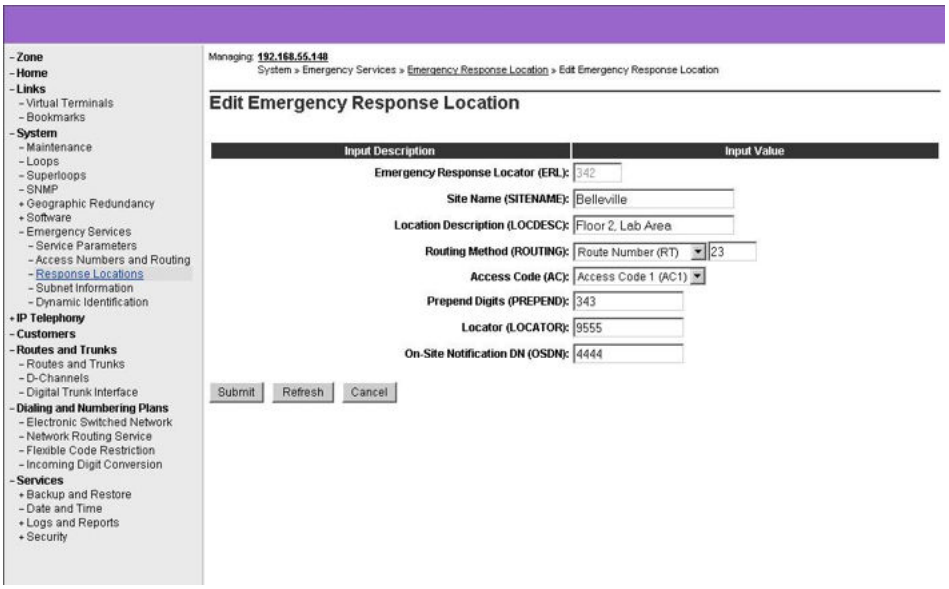


Figure 75: EM – Edit Emergency Response Location

Subnet Location Information Service (LD 117)

The Subnet Location Information Service (LIS) is an internal subnet lookup table, and is used in the Location Management of phones connected to the network. The subnet lookup table contains location data for every subnet entry.

The Element Manager user interface for the Subnet LIS (LD 117) allows the administrator to modify the information for any subnet, and is shown in the following figure. The IP Address and Mask fields are used to identify which subnet entry is to be modified.

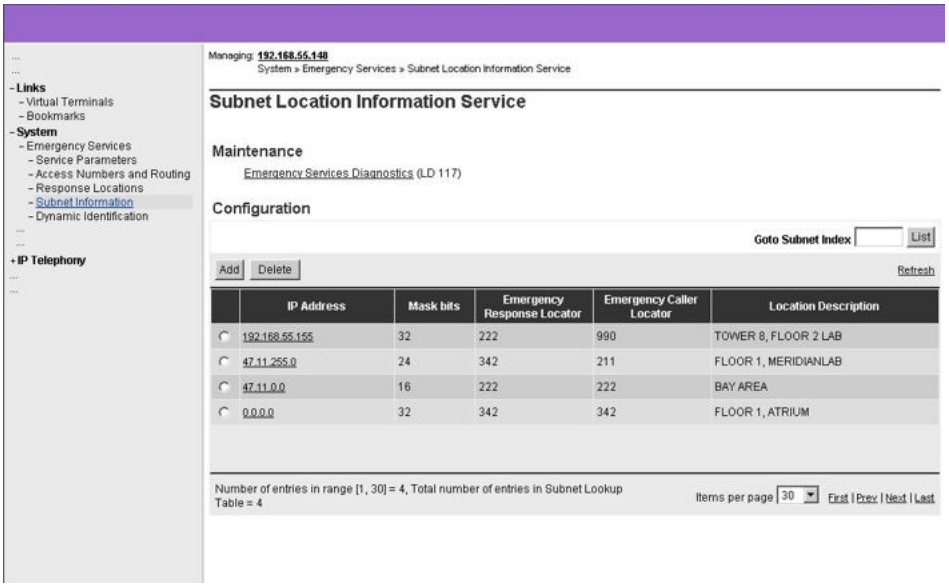


Figure 76: EM – Subnet Location Information Service

The Subnet LIS (LD 117) user interface allows the administrator to perform the following actions:

- Create a new subnet entry.
- Delete an existing subnet entry.
- Modify an existing subnet entry.
- Print configured subnet entries.

User interface

To access the Subnet LIS page:

1. Select **System**.
2. Select **Emergency Services**.
3. Select **Subnet Information**.

If the LIS is not set to SUBNET in the Emergency Services Configuration Record, then an indication of this is presented (by means of an alert message) whenever the subnet table is

updated. Subnet configuration and management using the Subnet LIS (LD 117) user interface is still allowed, however, regardless of whether the LIS is set to SUBNET or not.

The Subnet Location Information Service page contains two subsections - Maintenance and Configuration.

The Maintenance subsection contains a link to the Emergency Services Diagnostics page (to provide quick access to maintenance commands such as TEST SUBNETLIS).

The Configuration subsection lists every configured subnet entry in a table format. There is a paging mechanism in place to display the configured subnet entries in sets of a specified amount (for example, 20 entries at a time). This provides ease of navigation across the (potentially) many pages of configured subnet entries.

To display a selected number of subnet entries at a time:

- Click the Items per page drop down menu and select the number of simultaneous subnet entries to display.
- There are four preconfigured display types listed as links immediately to the right of the Items per page drop down menu. Depending on the desired display, choose one of the four options, which are described as follows:
  - The first group of subnet entries, in the amount specified using the Items per page drop down menu, is displayed using the **First** link.
  - The previous set of subnet entries, in the amount specified using the Items per page drop down menu, are displayed using the **Prev** link, ending at the first entry in the current list.
  - The next set of configured subnet entries, in the amount specified using the Items per page drop down menu, is displayed using the **Next** link, starting with last entry in the current list.
  - The last group of subnet entries, in the amount specified using the Items per page drop down menu, is displayed using the **Last** link.

By entering a Subnet index number into the Goto Subnet Index input box and clicking on the **List** button, a list of Subnet entries is displayed, starting with the specified Subnet index.

It is possible to delete a subnet entry from this page, by choosing the radio button beside the desired subnet entry and clicking the **Delete** button at the top of the table.

The latest subnet entry information, as stored on the call server, is displayed by clicking the **Refresh** link.

Clicking the IP address of a subnet entry listed in the table causes the Edit Subnet Location Information page to be displayed. This page allows the administrator to edit the subnet entry, and is shown by the following figure:

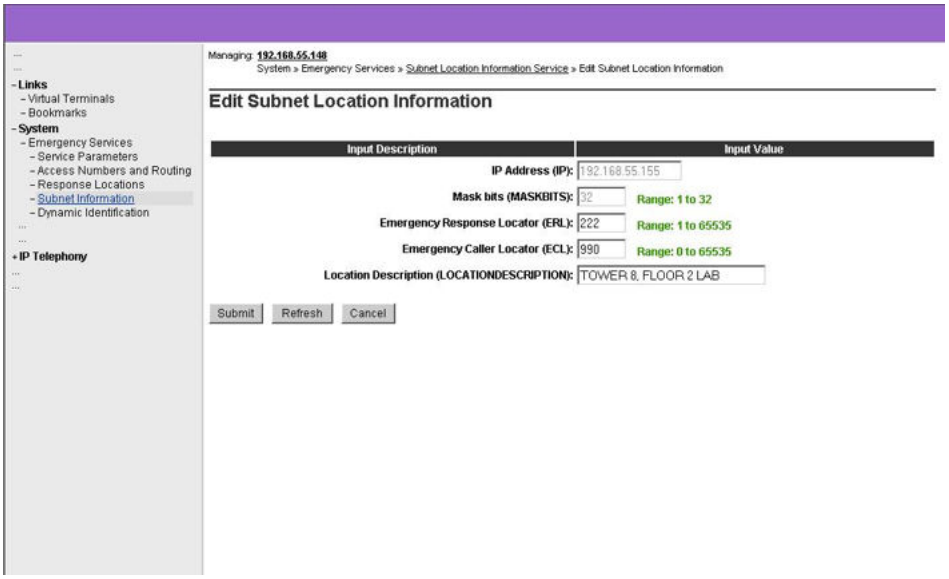


Figure 77: EM – Edit Subnet Location Information

Clicking the **Add** button at the top of the subnet entry table causes the Add Subnet Location Information page to be displayed, which allows the administrator to add a new subnet entry, as shown by the following figure:.

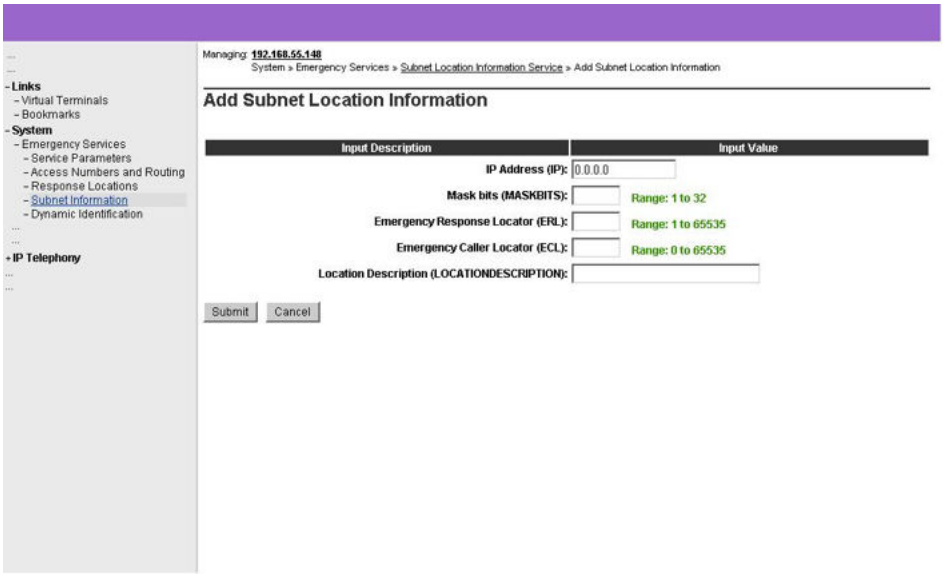


Figure 78: EM – Add Subnet Location Information

Dynamic Location Identification Number (LD 117)

The Dynamic ELIN table is required for the association or disassociation of a TN to an ERL, for the purpose of providing dynamic callback mapping to emergency callers who cannot use their DN as their CLID.

The Dynamic Location Identification Number user interface allows the administrator to perform the following actions:

- Add an ELIN (associate a TN to a specific ERL).
- Delete ELIN entries (disassociate a TN from a specific ERL).
- Print configured ELIN entries.

User interface

To access the Dynamic Location Identification Number page:

1. Select **IP Telephony**.
2. Select **Emergency Services**.
3. Select **Dynamic Identification**.

The Dynamic Location Identification Number page lists every configured Dynamic ELIN in a table format, and is shown in the following figure:

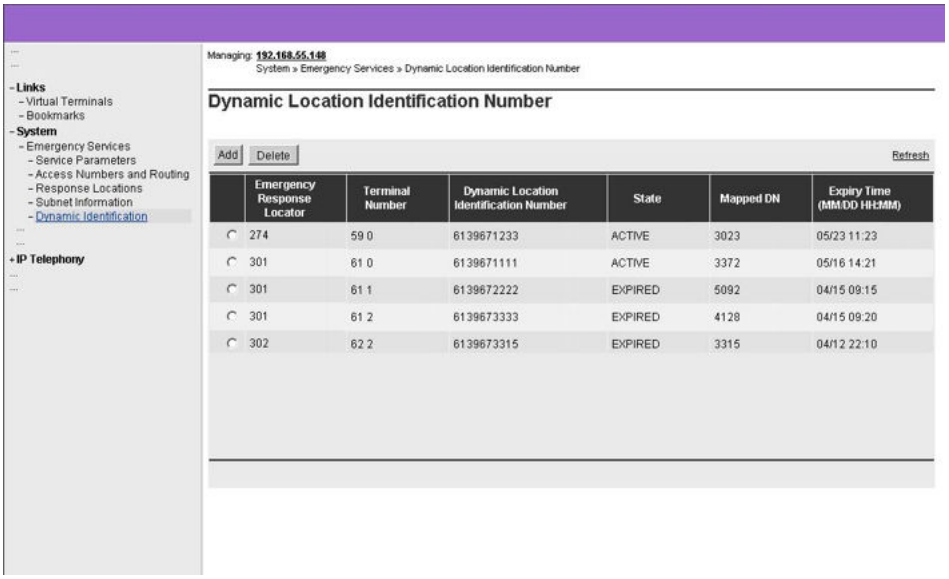


Figure 79: EM – Dynamic Location Identification Number

The administrator can delete an ELIN entry by selecting the radio button beside it and clicking the Delete button at the top of the table.

The latest ELIN configuration data, as stored on the call server, is displayed by clicking the **Refresh** link.

The Dynamic ELIN maintenance routines (including PRT) are accessed through the maintenance page .

Clicking the **Add** button causes the Add Dynamic Location Identification Number page to be displayed, which allows the administrator to add a new Dynamic ELIN entry. The Add Dynamic Location Identification Number page is shown by the following figure:

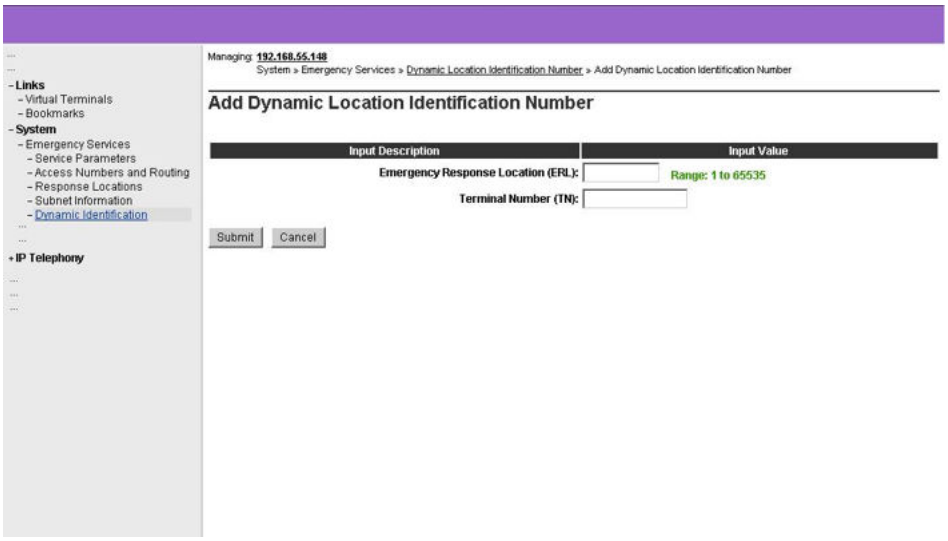


Figure 80: EM – Add Dynamic Location Identification Number

ESA maintenance commands (LD 117)

The emergency services maintenance commands are supported by Element Manager as a subsection of LD 117. This user interface allows the administrator to perform the following actions:

- Print an entire subnet table.
- Print subnet entries that match a specified IP address.
- Print subnet entries that match a specified ERL.
- Print subnet entries that match a specified ECL.
- Print the entire ERL table.
- Print a specified ERL.
- Print all configured Dynamic ELINs.
- Print all Dynamic ELINs for a specified ERL.
- Test the functionality of the Subnet LIS.
- Enable a specified ERL.

- Stat all configured Dynamic ELINs.
- Stat all configured Dynamic ELINs for a specified ERL.
- Stat all active Dynamic ELINs.
- Stat all active Dynamic ELINs for a specified ERL.
- Disable a specified ERL.

User interface

To access the Emergency Services Maintenance page:

1. Select **System**.
2. Select **Maintenance**.
3. Select **Emergency Services Diagnostics**.

From here, the administrator can select and execute each command with its respective parameters. Subsequent outputs are displayed in the text area.

The Emergency Service Maintenance page is shown in the following figure:

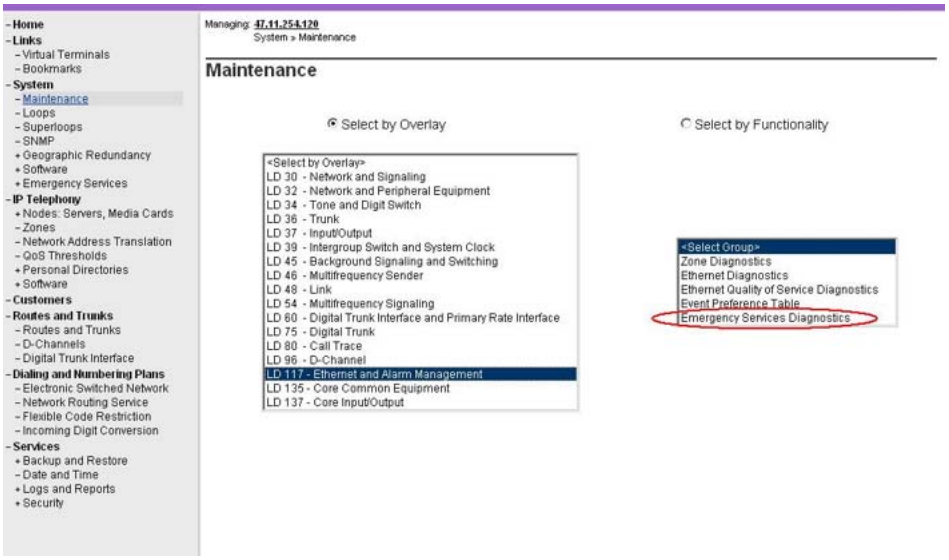


Figure 81: EM – Emergency Service Maintenance page

CLI commands

The ESA CLI commands are supported through the General Commands page for Servers and Media Cards. The General Commands user interface allows the administrator to execute the following commands:

- isetLocNeedUpdateShow – Returns a list of phones, connected to a specific Signaling Server, for which a location update is required.
- isetLocShow – Displays the location data of phones connected to a specific Signaling Server.

User interface

To access the new CLI commands:

1. Select **IP Network**.
2. Select **Maintenance and Reports**.
3. Select **General Commands**.

The administrator can select and execute each command with its respective parameters. Subsequent outputs are displayed in the text area.

The General Commands page is shown in the following figure:

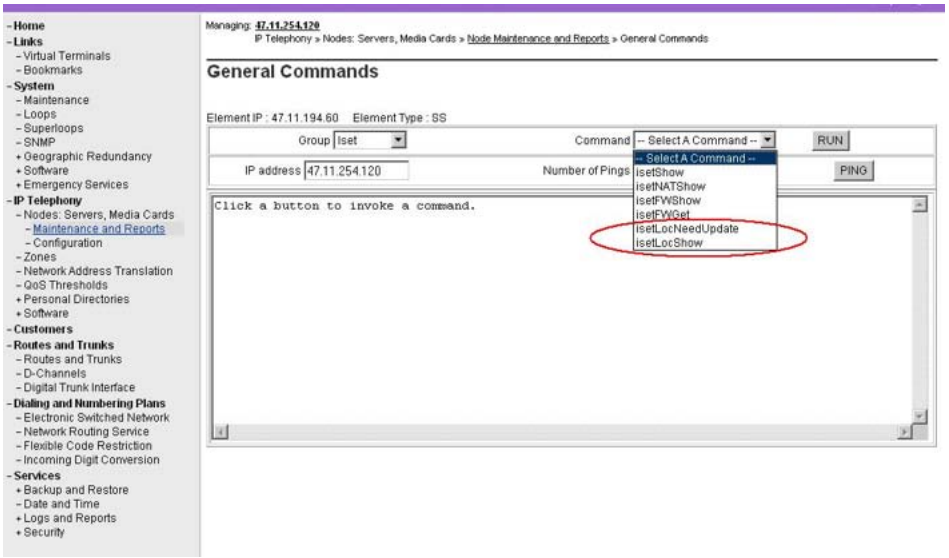


Figure 82: EM – General Commands page

Location Report (LD 117)

The IP Phone Location Report page provides a comprehensive location report for all IP phones currently listed in the TN Table. This includes IP phones that are currently connected and registered, and IP phones that have disconnected and unregistered since the last system restart (so long as their TN has not been reused).

The user interface allows the administrator to perform the following actions:

- Display location details in a table format.
- Create a Location Report using filtering based on the following predefined search criteria:
  - All IP Phones
  - Unregistered Sets
  - IP Phones on Roaming
  - IP Phones with Location Unknown
  - IP Phones configured as Manual Update
  - IP Phones that Need a Location Update
- In addition, the IP Phone Location Report provides filtering based on the following user defined search criteria, reporting IP phones that match the user specified value for:
  - Terminal Number
  - Prime DN
  - Terminal IP
  - Hardware ID
  - Emergency Response Location
  - Emergency Caller Location

When specifying a partial search value, all matching IP phones are displayed. A partial search value can only be specified for the TN, DN, IP or Hardware Id values.

The IP Phone Location Report can sort the reported data by column, and provides pagination of the data for easier viewing.

User interface

To access the IP Phone Location Report page:

1. Select **Tools**.
2. Select **Logs and reports**.
3. Select **IP Phone Location**.

The IP Phone Location Report page is shown in the following figure:

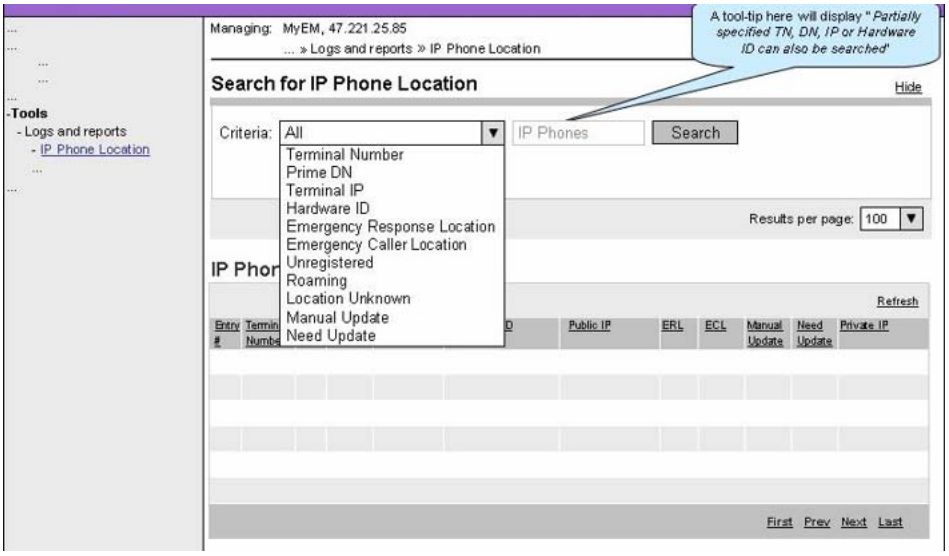


Figure 83: EM – IP Phone Location Report

The IP Phone Location Report page loads with the Search Criteria section collapsed (hidden). When the **Search** link is clicked, the Search Criteria section appears, and the Search link becomes Hide. In addition, the section title changes from Showing IP Phones with Search Criteria to Search for IP Phone Location.

If using All, Unregistered, Roaming, Location Unknown, Manual Update, or Need Update as search criteria, the input box is grayed out with the text IP Phones displayed in it.

If using Terminal Number, Prime DN, Terminal IP, Hardware ID, Emergency Response Location, or Emergency Caller Location as search criteria, the input box accepts values that coincide with these criteria.

The **Refresh** link causes the latest information, as stored on the call server, to be displayed. Clicking the column header links sorts the displayed data by that column heading.

ESA Configuration Task List

This section provides a configuration task list for the implementation of the Emergency Services Access feature. The configuration task list is as follows:

- Modify the customer CLID database to allow ESA calling number composition (LD 15).
- Configure CLID entries for all routes (LD 15).
- Configure a CLID entry for telephones to use (LD 10, LD 11).
- Configure terminal designator (DES) data telephones (LD 10, LD 11).
- Configure an OSN TTY output device (LD 17)
- Configure an IP or Digital OSN phone (analog not allowed) (LD 11).

- Configure outbound ESA trunk route (LD 16).
- Configure ESA data (LD 24).
- Configure ESA digit manipulation and call routing for NARS/BARS (LD 86).
- Configure ESA call recognition. This is to allow Access Code + ESDN dialing to be recognized and treated as an ESA call (LD 90).

ESA Feature Packaging

The following table describes the feature packages associated with the Emergency Services Access feature, as well as the functionality provided by each package.

Table 53: ESA feature packaging

Package Number	Mnemonic	Name	Description
329	ESA	Emergency Services Access	Defines an emergency number as being dialable without a prefix. Recognizes the emergency call and provides special treatment and routing to CAMA, PRI or other trunks. Provides flexible ANI number translation for DID numbers and sends out the ANI with the call to enable the PSAP to look up the caller. Includes Enhanced Routing functionality, Multiple ESDNs, and Misdial Prevention.
330	ESA_ SUPP	ESA Supplementary	Provides networking support by routing node-to-node ANI info for forwarding to a PSAP. Converts incoming ISDN to CAMA tandem to allow CLID forwarding via outpulsed CAMA Also provides On-Site-Notification (OSN) so that customer staff are aware of the call. This includes OSN phones per ERL.
331	ESA_CLMP	ESA Calling Number Mapping	Provides flexible ANI number translation for non-DID numbers (i.e. to translate non-DID numbers to DID

Package Number	Mnemonic	Name	Description
			numbers). This includes Dynamic ELIN functionality.
336	ESA_SUBNET_LIS	ESA Subnet LIS	Allows the use of an internal Subnet-Lookup Location Information Service to provide basic location determination for IP phones.
337	ESA_EXTERNAL_DM	ESA External DM Interface	Allows the use of an external Discover Manager (and corresponding LIS) to provide advanced location determination for IP phones. Additionally, the External Discovery Manager is charged separately.

Chapter 5: Emergency Services for Virtual Office

Contents

This section contains information about the following topics:

Introduction

The E911 for Virtual Office feature allows Virtual Office users to place an emergency (E911) call to the correct Public Safety Answering Point (PSAP) for their geographical location. It recognizes when a user dials an Emergency Services Directory Number (ESDN) and forces the Virtual Office IP Phone to log out of the Remote Call Server and redirect to the Home Call Server. Although this adds a small delay to call processing, the delay is almost imperceptible to the user.

No overlay changes are required because there are no configuration options.

Note:

Unless stated otherwise, all ESA functions (for example OSN, non-DID mapping to DID, and internetworking with partner solutions) continue to operate as previously described.

Virtual Office operation with feature not enabled

Upon Virtual Office login, without the E911 for Virtual Office feature enabled, the IP Phone de-registers with the Home Call Server and registers with the Call Server associated with the given User ID. This can be the same Call Server or another Call Server within the network. If it is another Call Server, then it might be in a different geographic area and use a different PSAP to handle emergency calls. Therefore, if a user places an emergency call using an IP Phone that is geographically distant from its registered Call Server, the emergency call is sent to the wrong PSAP and help might be delayed, go to the wrong location, or not arrive at all.

Note:

The basic ESA feature uses the premise that all the telephones connected to the Call Server are served by the same PSTN and the same PSAP. This assumption is acceptable for TDM telephones where the maximum length of the cable from the Call Server to the telephone is restricted to approximately 1000 feet. With IP Phones, it is possible for a telephone to be at a great distance from the Call Server.

Without the E911 for Virtual Office feature configured, ESA operates the same on a Virtual Office IP Phone as it operates on any other Call Server telephone, and the wrong PSAP may be used. This is considered fall back mode, which is compatible with older versions of the software or firmware.

Virtual Office operation with feature enabled

Upon Virtual Office login on a Remote Call Server with the E911 for Virtual Office feature enabled, the Home IP Line application stores the ESA configuration in the DRAM of the IP Phone before redirecting it to the Remote Call Server. This information tells the Remote Call Server that the Home Call Server is enabled and configured for ESA. The Remote Call Server uses this information to redirect the IP Phone to the Home Call Server to handle ESA calls.

Note:

The ESA configuration stored in the DRAM includes the Emergency Services DN (ESDN). This is implemented for future use, when the ESDN could differ on Call Servers.

When the redirected IP Phone starts the registration and Virtual Office login procedure at the Remote Call Server, the Remote IP Line application reads its DRAM and passes the ESA configuration to the Call Server. This lets the Call Server know that if the IP Phone user makes an ESA call, it must use the E911 for Virtual Office feature.

When the Virtual Office user dials the ESDN, then the E911 for Virtual Office feature is invoked on the Remote Call Server. The feature checks for a flag that indicates that the originating IP Phone can be redirected to the Home Call Server to process the ESA call. If this is the case,

then the Remote Call Server sends a message to the Remote IP Line application to write the request into the DRAM of the IP Phone and redirect it to the Home IP Line application.

Note:

The request to redirect the set to the Home IP Line application for the ESA call includes the dialed ESDN. This is implemented for future use, when the ESDN could differ on Call Servers.

A message is sent to the IP Phone's display alerting the user that the emergency call is in progress. Then, another message is sent to the IP Phone's display indicating that an emergency call is in progress. A final message causes the IP Phone to return to its Home IP Line application without the visible flashing of the light or clearing of the display.

When the IP Phone re-registers with the Home IP Line application, the Home IP Line application retrieves the DRAM and acts on the request for an ESA call. The Home IP Line application simultaneously refreshes the IP Phone's display with the correct keymap and sends a message to the Call Server indicating that an emergency call must be originated on the IP Phone's TN.

After the emergency call ends, the IP Phone remains registered to the Home IP Line application as a normal telephone, in case the PSAP makes a call back to the originator of the emergency call.

To prevent internetworking problems with external On Site Notification (OSN) data processing devices, OSN is not changed on the Home Call Server. If OSN is changed on the Remote Call Server, then care must be taken to not confuse external OSN data processing devices.

After the IP Phone is redirected to its Home Site, it is not allowed to initiate a new operation for five minutes. This prevents the user from accidentally dialing the emergency DN and hanging up. In this case, the emergency response personnel might call back to confirm the accidental call (and thus confirm that there is no emergency). If the phone is allowed to immediately resume a Virtual Office login to another site, it cannot receive the call back.

Operating parameters

The following are the minimum software and firmware requirements for the Emergency Services for Virtual Office feature:

- IP Phone firmware 1.5x
- Succession 3.0 Software

The ESA package must be enabled on the Home and Remote Call Servers. If either site does not have ESA enabled, the E911 feature operates the same with or without the feature enabled, and calls are placed to the PSAP of the user's home location.

The resources required to originate an emergency call should be blocked from use by normal call processing, and reserved for emergency calls. Because the E911 for Virtual Office feature

overrides access restrictions, it is possible to have resources that cannot be normally accessed, but can be accessed for an emergency call. In particular, the outbound trunks and DSP resources should be reserved in this manner.

The IP Phone may have a "red sticker" indicating the number to dial for emergency calls. This is only applicable when connected to the Local Call Server. A Virtual Office user, connected to a Remote Call Server, must dial the ESDN associated with the Remote Call Server (not necessarily the number indicated on the "red sticker"). It is up to the site to come up with a policy for this situation.

If the IP Phone does not have the correct firmware, the E911 for Virtual Office feature still redirects the IP Phone to the Home Site. However, the IP Phone appears to visually reset, which may cause the user to panic.

If the Home Call Server does not have ESA configured, ESA is not configured correctly, or the IP Line application does not have the correct software, then the feature operates in fallback mode.

If network problems prevent a redirected IP Phone from registering with the Home IP Line application (the Home IP Line application or Home Call Server might be out-of-service), the IP Phone goes into a server unreachable mode and resets. The IP Phone is out-of-service until it can connect to the Home IP Line application, and the data in the DRAM is lost and no emergency call originates.

If the maximum number of IP Phones is registered with the Home IP Line application, then no new telephones can register. Therefore, the Virtual Office IP Phone returning to the Home IP Line application cannot initiate an emergency call. The system should be engineered such that there are enough resources for additional IP Phones to register.

If the TN of the redirected IP Phone is used by another Virtual Office session, the IP Phone occupying the TN is preempted so the redirected IP Phone can access the TN to make an emergency call.

The IP network cannot be used to directly reach the PSAP, so the Call Server must have a TDM trunk to the PSTN for each PSAP. ESA does not support more than one PSAP for a given Call Server. The solution is to have a Call Server in each PSAP jurisdiction and to route the call to the appropriate Call Server based on the location of the originator of the emergency call.

If a user dials the ESDN on an IP Phone while logged onto a Remote Call Server using Virtual Office, it is not appropriate to have the Remote Call Server connect the call to its PSAP. It is better for the Remote Call Server to send the IP Phone to its Home Call Server (simulating a Virtual Office log out) along with a flag to let the Home Call Server know the reason the phone came home is to place an ESA call.

If the user changes between headset, handset, or handsfree operation between the time the final digit for the ESDN is pressed and the call is connected to the PSAP, that change will not be recognized by the Call Server. The call will be completed in all cases, but the user might not hear the PSAP if they expected the change to take effect and listened to the wrong device.

The Emergency Services for Virtual Office feature introduces error messages for the following situations:

- A remote IP Phone, that does not function with the feature, connects to the Call Server.
- A remote IP Phone, after generating the previous message, dials the emergency DN and is routed to the wrong PSAP.
- A TN without an active call is preempted due to an emergency call by a remote IP Phone.
- A TN with an active call is preempted due to an emergency call by a remote IP Phone.

Feature interactions

There are no feature interactions associated with this feature.

Feature packaging

The E911 for Virtual Office feature requires the following packages:

- Emergency Services Access (ESA) package 329
- Virtual Office (VO) package 382
- Virtual Office Enhancement (VOE) package 387

Feature implementation

There are no specific implementation procedures for this feature.

Feature operation

No specific operating procedures are required to use this feature.

E911 for VO

Background

The Virtual Office feature allows a user to login to an IP phone on a host call server using the DN (TN) provisioned for them on their home call server.

Without the availability of dynamic location data, however, ESA call processing for a VO user would mean that static location data at the home TN would be used to assign the ANI of the IP phone at the VO host site. Subsequently, ESA would route the emergency call as though the IP phone (logged into VO) was physically located at the home TN site. This routing behavior would be incorrect, obviously, as the VO user is actually placing the emergency call from an IP phone at a host site, which is at a different physical location entirely.

The E911 for VO feature provides a solution to this problem by causing a VO logged in phone to redirect back to its host call server for emergency call handling when an Emergency Services Directory Number (ESDN) is dialed. This allows ESA call processing to occur using accurate location data which reflects the VO logged in emergency caller as being physically located at the host call server site.

Overview

Virtual Office is a form of network wide mobility. With the ESA feature, a system administrator has the ability to assign device based location data using an enterprise wide location parameter, ERL. Therefore, a home call server can process a VO user just like any other network telephony client - an incoming emergency call made by a VO user can be tandem routed to a local gateway (the host call server, for example) instead of having to be blindly redirected. This guarantees that the home call server of the VO user can provide full emergency call handling by using an alternate call routing method if the VO host call server is found to be unreachable.

This E911 for VO functionality of the ESA feature requires that the host call server recognizes the location of the VO logged in IP phone. If the location of the VO phone is not recognized, then the home call server cannot handle the emergency call correctly. If Emergency Services Access is deployed throughout the entire enterprise, however, there is a low probability that a phone will be seen as being at an unknown location.

Operation

The ESA available flag is passed by the VO phone to the home call server of the VO user, and indicates whether the host call server has ESA provisioned.

If the VO phone has cached location data stored on it, then this is the location data the home call server uses until a location update is provided for the phone by either the Subnet LIS or the External. If the location specified by the cached location data is not recognized by the home call server, a system message is generated and null (unknown) location values are assigned to the VO phone.

If the VO user dials an ESDN at the host site, host call server will handle the call and may route the call back to the home call server to reach the PSAP

ESA must be configured on the home call server and on the host call server – a basic design condition of ESA is that, for true ESA coverage to exist throughout the entire enterprise network, every possible call location in the enterprise network must be defined. Furthermore, every call server on the enterprise network must have access to those location definitions, so that a call location can be recognized regardless of where it originates from. Therefore, if a VO phone routes to the home call server and its location is not recognized, ESA has not been truly implemented as it is intended to be, on every system in the enterprise network.

If ESA has been correctly implemented, then the host site location of the VO phone is recognized by the home call server and ESA call processing takes place normally – the home call server uses the ERL entry of the VO phone to assign a CLID and routes the call appropriately.

Although the home call server of the VO user will recognize the location of the VO phone at the host call server, it will not be configured handle the emergency call itself, directly, for phones at a different location. Therefore, the home call server will route the call either to another gateway (back to the host call server, for example) or else directly to the PSAP listed for the remote caller location. No system message is generated in either case.

In the event that ESA has not been implemented correctly and the location of the VO phone is not recognized, the home call server applies ESA call processing according to its own basic ESA Data Block (LD 24), as done under previous software releases. In this case, a system message is generated.

Manual Update TNs

To accomplish its basic function of allowing an IP phone on one call server to act as though it were actually located on another, Virtual Office must first break any current TN associations to an IP phone used for a VO login. Therefore, a TN that is Manual Update must be treated as Auto Update for the purposes of a VO login, so that the operational location data placed into the TN Table for that device is correct.

If a VO user invokes ESA by dialing an ESDN, it is possible (as explained previously) that they will be redirected by their home call server back to their host call server for emergency call handling. If the TNs on that host call server are configured to be Manual Update, then the VO phone also becomes Manual Update the instant they register back on the host call server. At this point, their location data comes from the host TN, which is correct.

Therefore, there is no need to deny VO logins from or to a Manual Update TN (VOLD or VOUD).

System messages

Just as there is no system message that indicates a VO user has been redirected to their originating call server for ESA call handling, there is also no system message that a VO user is handled directly at the home call server (meaning that the ESA call is routed).

Branch Users

The E911 for VO feature may redirect an IP phone to its provisioned S1 (its server configuration in flash memory), which may be a Survivable Branch Office or Survivable Remote Gateway or Secondary Call Server (SMG and SSMG). In this case, the SBO, SRG, or Secondary Call Server must provide local ESA service.

Active Call Failover

The Active Call Failover feature does not interact with E911 for VO redirection.

If there is another phone with an active VO login on the same host TN as the emergency caller, then the active VO login is preempted by E911 for VO operation, even if it is busy (on a call, for example) - its call is dropped and it is redirected to its own TN.

Chapter 6: Basic Emergency Service When VO Logged Out

Contents

This section contains information about the following topics:

Overview

Before the introduction of the Basic Emergency When VO Logged out feature, logged out phones could not be used for basic telephony function - making and receiving calls. The reason was that the basic telephony function was controlled by the central Call Server. The logged out phones were not registered with the Call Server and thus the user could not make and receive calls.

New functionality is introduced: to provide the ability for the logged out phone to make ESA calls and receive callbacks, temporarily register with the Call Server. The registration begins as the user tries to make a call from the logged out phone by going off hook or pressing the primary key, or using the handsfree or headset.

Making an ESA Call From a Logged Out Phone

The Call Server is provisioned with a pool of Emergency Terminal Numbers (TNs) referred to as Emergency Services Access Terminal Number (ESTN) in this document. The ESTN is allocated from this pool to register the logged out phone.

As the logged out phone registers with the Call Server using the allocated ESTN, the key presses are transmitted to the Call Server according to the existing operation, so the Call Server is fully responsible for initiating the call. The Call Server normally provides the dial tone and collects the digits.

The logged out phone can make ESA calls only. The configured ESTNs are fully restricted. As the Directory Number (DN) translation is complete, the Call Server checks the type of the DN and proceeds with the call only if an Emergency Services Access Directory Number (ESDN) or other locally routed emergency DNs as defined per ESA feature is dialed.

Scenario: Process Event In VO Logout State

1. This scenario begins when the user performs any action on the logged out phone.
2. The LTPS analyzes the event. The event is a key press. If the event received from the phone is not a key event (for example, accessory connect or disconnect), the LTPS silently ignores the event.
3. The LTPS analyzes the event. The event is a key press. If the event received from the phone is not a key event (for example, accessory connect or disconnect), the LTPS silently ignores the event.
4. The LTPS checks if the logged out phone is registered with the Call Server. If the phone is not registered with the Call Server, the scenario SYS_04: Register VO Logout Phone with Call Server.
5. If the logged out phone is registered with the Call Server, the LTPS processes all the key presses and sends them to the Call Server as per the existing functionality.
6. The Call Server receives the keys and processes them as per the existing functionality:
    - The Call Server allocates the call register and generates the dial tone when the user goes off-hook. See scenario SYS_04: Register VO Logout Phone with Call Server scenario to learn how the call can be originated in the Logout state.

- The Call Server processes dialing as per the existing functionality plus the new feature described in SYS_05:Accept Dialing Emergency Local Numbers on Call Server.
- As the DN translation is complete and the dialed number is an ESDN or one of the other two local emergency numbers, the Call Server makes the ESA call as per the ESA functionality. Otherwise, see “Scenario 0.2 The Dialed Number is not an ESDN Number”.
- The OSN treatment is provided for the ESA call as per the ESA functionality for ESDN number. That means the Name, DES and emergency DN configured for the corresponding ESTN are sent to the OSN phone/terminal.

7. As the ESA call originates, the ESAVOLO timer is stopped (see SYS_04: Register VO Logout Phone with Call Server for more information on why this timer is running).
8. As the user's ESA call is completed , the LTPS shows the Awaiting Callback text on the phone display. The Call Server reloads the ESAVOLO timer to the user defined value (20 minutes by default).
9. If the user hangs up without dialing a number before the 1 minute timer expires, no action is taken until the 1 minute timer times up and the set gets de-registered. This is to avoid subsequent attempt to reregister the phone in case of an unintentional disconnect.

Scenario: The Dialed Number is not an ESDN Number

If the dialed number is not an ESA number, the Call Server performs the overflow treatment as per the existing functionality:

- provides the overflow tone
- releases the call
- shows the Release and try again message on the phone.

The user has another chance to dial the ESDN number before the 1 minute timer expires (if it was the first attempt), or go back to “Await Callback” mode in other cases.

Scenario: Register VO Logout Phone with Call Server

- This scenario is a part of USER_01: Process Event in VO Logout State and begins if a key is pressed on a VO logged-out phone that is not registered with Call Server.
- The LTPS analyzes if the registration is pending for the logged-out phone. Suppose the registration is not started yet. Otherwise, see Scenario 0.1 The Registration is Pending for the VO Logout Phone.

  Registration pending means that the ESAVOLO Activity message (see section that follows) was sent to the Call Server, but no response from the Call Server is received. For example, some new ESAVOLORegPending flag can signal that the registration is pending. Originally, this flag is cleared, which is true in this main scenario.

- The registration is not started yet, and the LTPS analyzes the pressed key. One of the following keys can be used to originate the ESA call from the logged out phone:
  - OFFHOOK
  - PRIMARY KEY
  - HANDSFREE
  - HEADSET key or In-calls key for the 1150 phone.

  The following procedure is based on events if one of the previous is generated.
- The LTPS marks that the registration is pending (or started) for the logged out phone (sets the ESAVOLORegPending flag)
- The LTPS places the event in the dedicated ESAVOLO key buffer.
- The LTPS sends the new ESAVOLO Activity message to the Call Server. You need not define a new message, as you can use typedef command for the existing PBXOnline2 message, and reuse its fields. Only the new message type is defined, which is sufficient to distinguish between the ESAVOLOActivity message and PBXOnline2 message. The LTPS sends the new “ESAVOLO Activity” message to the Call Server.
- The Call Server receives the ESAVOLO Activity message and reviews the Emergency TN pool for the unused TN. If the Call Server does not find the unused TN, see Scenario 0.3 There are no unused Emergency TNs in the pool.
  - The Call Server marks the TN as used and copies the zone value from the original TN to VOLO TN.
  - The Call Server creates the ESAVOLO timer and executes the SYS_03: Reset ESAVOLO Timer scenario to reset the timer to one minute.
  - The Call Server sends the existing TN Status 2 message with the ESA TN Reserved reason to the LTPS. The TN and other parameters are filled as specified in the Emergency TN block.
- The LTPS receives the TN Status 2 message with the new ESA TN Reserved reason and performs the following tasks:
  - The LTPS saves the TN and other parameters received in the message.
  - The LTPS automatically generates the SSD messages corresponding to the key events contained in the ESAVOLO key buffer.
  - The LTPS requests the key map download.
- The key map download is processed according to the existing functionality. Because the only key that is configured on the Emergency TN is the primary DN, the phone display has the only primary DN label in its feature key area. The soft key and text areas (if applicable) are empty after the key map downloads.

Receiving ESA Callback

After the ESA call is complete (released by one of the parties), the logged out phone registers with the Call Server for a preconfigured period of time (20 minutes by default). During this time the phone continues to use the ESTN allocated for the ESA call.

The logged out phone can receive calls from any source during this period, which makes it possible to receive ESA callbacks from PSAP or local security service.

As the preconfigured time out is complete, the Call Server unregisters the phone. The phone moves to the original logged out state and the phone ESTN becomes available to other ESA calls from any other VO logged out phone.

1. This scenario begins when the call is terminates to the Emergency TN. The call can be from any source:
    - internal call
    - network call
2. The Call Server checks the emergency TN and finds the TN is registered. Otherwise, see Scenario: The Emergency TN is not registered with Call Server.
3. The call is terminated on the VO logged out phone if it is not busy and the ESAVOLO timer stops. If the phone is busy, see Scenario 0.2 VOLO phone is busy.
4. When the VOLO phone hangs up, ESAVOLO timer reloads again.

If an incoming call to the emergency TN is not used, the overflow treatment is provided for the call and the ERR_TBD1 message is displayed on the maintenance terminal.

If the VOLO Phone is Busy the Call Server sends back a busy signal and the other side has to disconnect and try again. A CFNA treatment is not provided to the caller if the VOLO phone does not answer the call, because the VOLO has no mailbox access.

ESA Call Processing

The ESA call from the logged out phone is processed in the same way as the ESA call from a normally registered phone. The information configured in the emergency TN block is provided to the OSN phone/terminal. This includes:

- Name: LoggedOut.
- CPND block: uses the English string VOLO and is automatically configured against the primary key of all the emergency TNs.
- DES: All the emergency TNs have the ESTN designator.
- DN: The emergency DN configured by administrator. The primary DN, that is configured by the administrator, is sent to the OSN phone/terminal, so that callback to this phone is possible.

CLID Composition

For ESA to identify the physical location of a logged out phone using its CLID, the Location Auto Update mechanism is required.

ESA VO Logout Timer

A special ESA VO Logout timer is created for every logged out phone with the emergency TN allocated. The emergency TN is released and the phone returns to the original logged out state when this timer expires.

The timer is created and set to 60 seconds as soon as the emergency TN is allocated. The timer stops only after the user is finished dialing the ESA number.

In other words, the user has a maximum of 1 minute to dial an ESA number. After the 1 minute, all key presses are lost and you must re-initiate the call. The ESA VO Logout Timer also includes the case when user dials a wrong number, in which they receive an overflow tone and Release and try again message on phone display.

The Release and try again message prevents the ESTN from abnormally remaining on the call server, for example, due to the accidental pressing the primary key or dropping the handset.

- The timer stops upon initiation of the ESA call (for example, while waiting for answer and connect phases).
- The timer restarts as the user's ESA call is completed. The timer is set to a preconfigured period (20 minutes by default) so the user can receive a callback during that period.
- The timer restarts again if the user makes another ESA call.
- If the timer expires but the phone is involved in a call, the time out event is ignored. When this call is finished, the 20 minute timer reloads.

Scenario: Reset ESAVOLO Timer

This scenario begins when the system needs to start the ESAVOLO timer to monitor the emergency TN. This happens in the following cases:

- The Emergency TN is just allocated, and you need to create the new ESAVOLO timer with the period of 60 seconds. This timer is necessary to guarantee that the Emergency TN is not busy because of some unnoticed user action, for example, accidentally dropping the handset from the Logged Out phone.
- The timer is stops upon origination of the ESA call.
- The ESA call is complete. In this case the timer resets to the period specified in LD 24 (20 minutes by default).
- If the timer does not exist, you must create it.
- Set the timer to the value specified by the system (either user defined value or 1 minute)

ESAVOLO Timer Expire

- This scenario begins when the ESAVOLO timer that is associated with every used emergency TN expires.
- The Call Server checks the associated emergency TN and finds it is not in a call. Otherwise, see Scenario: The Emergency TN is in a Call when the ESAVOLO Timer Expires.
- The Call Server marks the emergency TN as not used and destroys the emergency timer.
- The Call Server sends the existing TN Offline message with the new ESAVOLO Timeout reason to the LTPS.
- LTPS receives the TN Offline message with the new ESAVOLO Timeout reason and moves the phone to the initial VO logout state.
  - The display shows Emergency Calls Only label and the Virtual and Home soft keys.
  - The SSD channel is closed and all LTPS data is initialized according to the original VO Logout state.

If the Emergency TN is in a Call when the ESAVOLO Timer Expires, The time out event is ignored and no action occurs until the call finishes.

Provisioning, Administration and Maintenance

The Basic Emergency Services When VO Logged Out feature is provisioned as follows:

1. In LD 24, specify the number of emergency TNs in the pool and specify the range of the emergency pool.
2. In LD 11, configure emergency TNs.

   Enter the new VOLO response for the type prompt. Very limited information is prompted for the ESTN (basically, only the DN used for the call is required).

   The system saves the VOLO TNs in a new, fully-restricted data block similar to IP Phone 2001. Because these TNs are fully restricted to provide only one DN to access emergency numbers while the set is in VOLO state, Emergency TNs do not use up any user licences (ISMs).
3. Use LD 117 to print the used emergency TNs.
4. The *isetShow* command output is slightly modified to display if the logged out phone is registered with the Call Server, and uses emergency TN.
5. LD 32 *idu* command is modified to show a different type of TN (VOLO) when queried.
6. LD 80 *trak* command is modified to show a different type of TN (VOLO) when printing TN info.

Because the emergency TNs are stored with no features configured, the only primary key label downloaded to the logged-out phone is for making a call. The soft keys, feature keys, and information area of the display are emptied as the set registers.

Keeping Logged Out State

The remote user, who logged on to the TN that the emergency call was made from, may go back to its home TN during this time. According to the existing functionality, this forces the logged out phone to reregister with its home TN as well.

The use case Scenario: Keep Logged Out State provides the requirement to prevent the logged out phone registered with the Call Server for ESA from reregistering.

When this scenario occurs, the VOLO phone sustains its Awaiting Callback state until the ESAVOLO timer expires, and returns to i's original Logged Out state, to give you the chance to go back to normal registration by using the soft key provided.

Scenario: Keep Logged Out State

- This scenario begins when the logged in phone selects Virtual Office Logout from the menu.
- The logged in phone is registered back to the original TN.
- The Call Server checks if the logged out phone is connected to an emergency TN. If it is , the logged out phone is not reregistered with its home TN.

Configure ESA Data Block

Configure the VOLO BLOCK only for the lowest customer number. If you configure a low customer number after you configure the VOLO BLOCK for a higher customer, the number is not handled. The VO set cannot register as the configuration of the VOLO TN cannot occur in LD24 under such a situation. The VO set that tries to register in this case receives the prompt Service Not Available.

Scenario: Manage ESA Data

1. You start the scenario by entering overlay 24.
2. You create or change the existing ESA data block.
3. The customer number prompt appears and you enter the customer number.
4. The new VOLO_COUNT prompt appears after you enter OSDN.
5. You are prompted to enter the number of TNs in the emergency TN pool. Enter the number of VOLO TNs in the pool. The existing SCH0205 message is displayed and the input is not accepted if it is out of range.
6. The new VOLO_COUNT prompt is displayed after the you enter OSDN. You are then prompted to enter the number of TNs in the emergency TN pool. Enter the

number of VOLO TNs in the pool. The existing SCH0205 message is displayed and the input is not accepted if it is out of range.

7. The VOLO_FIRST_TN prompt is displayed if the number of ESTNs (VOLO_CNT value) is not 0. This marks the beginning of the continuous emergency TN pool.
8. As you enter the TN, the system checks if this TN and VOLO_COUNT -1 continuous virtual TNs are available in the system.
9. Continuous means that the TNs should occupy subsequent units and cards, starting from the TN specified in the VOLO_FIRST_TN prompt. For large systems it also means that it must be within one virtual loop.
10. If the continuous pool is not available, the input is not accepted and the new SCH2171 message is displayed.
11. The VOLO_CALBK_TIM prompt appears if VOLO_COUNT is not 0. You are prompted to enter the time the emergency TN is available after the ESA call is complete (default 20 minutes). Input must be an even number expressed in seconds. The allowable range is between 15 minutes and half an hour. The existing SCH0205 message is displayed and the input is not accepted if it is out of range.
12. When this prompt is accessible through EM, you are required enter the values in minutes instead of seconds to provide a more convenient user interface.

Because you can define the ESA data block for any customer, you can define the ESTN pool for any customer as well. The ESTN pool will only be required for customers that have access to the VO Login feature (lowest customer number for the time being).

Scenario: Manage ESTN Data

- This scenario begins when you enter LD 11 and create a new data block. The multiple TN is not supported for the VOLO TNs because they are based on the IP TN. The multiple TN configuration is supported only for an analog TN in Avaya Communication Server 1000. They are not supported for Digital TN or IP TN.
- The user enters “VOLO” as a response to the TYPE prompt.
- The TN prompt is displayed and you enter the emergency TN. The new SCH2182 message is displayed, and the input is not accepted if the TN is not in the range of the emergency pool configured in LD 24.
- The CUST prompt is displayed and you enter the customer number the emergency pool is configured for. The new SCH2190 message is displayed and the input is not accepted if the entered customer number is valid, but the customer has no emergency pool configured.
- The KEY prompt is displayed and you configure the primary key as SCR. If any other key number is entered, SCH0361 will be printed and the KEY prompt will be repeated. The CLID configuration is optional. It is strongly recommended you leave it blank to use the dynamic location management as introduced by ESA Client Mobility feature.
- No other prompts but those defined previously are displayed for the ESTN. After key 0 is entered the system saves the data with new VOLO type. It is similar to an IP phone 2001 with all the features restricted in addition to the conditions mentioned here:

    - for the IP Call Recording feature to be available, this CLS is set to ICRA.

- for the concurrent media security development, the default CLS Media Security Never (MSNV) should be used to prevent media encryption for this type of TN.
- The two new ERL and ECL prompts introduced by ESA for Client Mobility feature should be set to 0 to activate automatic location update.
- Both CLS for performing a VO login from this TN, or allowing another set to do a VOLO to this TN, are restricted.
- A multiple appearance DN is not allowed to be defined for this type of TN. It is to ensure that a call back from PSAP terminates to the original caller and nobody else.

• The ESTN is saved in the data block's designator DES field and VOLO in the CPND block of the primary SCR key

Sysload

Scenario: Load ESA VO Logout Settings

• This scenario begins when the system starts loading the configuration database from disk

• The ESA VO Logout data configured in the Manage ESA Data and Manage ESTN Data scenarios.

Maintenance and Diagnostics

• This scenario begins when you enter LD 117 and issue the new PRT STAT ESALO command.

• The used emergency TNs are displayed on the terminal.

Scenario: isetShow - Show Used Emergency TNs

• This scenario begins when you issue the isetShow command on LTPS.

• If the phone is in the Logged Out state and has the emergency TN allocated, the Emergency Service Access Logged Out (ESALO) string is appended to the phone's state. Thus, if the logged out phone is in an ESA call, the phone state is busy-ESALO. If the logged out phone is waiting for ESA callback (the phone is idle and uses an emergency TN), the phone state is Logout-ESALO.

Scenario: LD 32 idu Command

• This scenario begins when you enter LD 32 and issues the idu command, plus the TN of a ESA VOLO phone.

• When the TN is in use all the information related to that set is printed out with only the TN type changed to VOLO TN.

Scenario: LD 80 Trak Command

- This scenario begins when you make an emergency call using a VOLO phone.
- While on the call, the administrator enters LD 80 and issues a trak command with the TN of ESA VOLO phone on the call.
- All the information related to that set is printed out with only the TN type changed to VOLO

Warm Start

An active call to or from PSAP survives a warm start. In Awaiting Callback state, the VOLO set can register back to Call Server with the same VOLO TN. But because it will lose its VOLO timer, and it is not possible to distinguish between this situation and a first time registration, it is not possible to reload the timer. To avoid this scenario, the Signalling Server must deregister the phone and put it back to “Logged out” state.

CLID Composition

The Emergency Services Access feature composes a CLID that identifies the physical location of the logged phone. If a system is configured with an internal LIS server, the location update might not happen right after the set registers.

The call to PSAP occurs immediately after the set registers, requiring the correct location information; this is not desired. Special handling may be required, possibly by directly calling background LIS for the VOLO TN.

Active Call Fail Over

Interactions with Active Call Fail over can be considered under the following possible scenarios:

- ELAN failure happens for less than 10 minutes:
  - The ESA VOLO phone is on a call. The call must remain up because IP Line application keeps the set registered till 10 minutes. The TN synchronization after ELAN goes up must be completed without any errors.
  - ESA VOLO phone is in Waiting to Callback and Awaiting Callback status. The ESTN VOLO timer can expire during this period, causing the ESTN to be released. If the ELAN Signalling Server sends the TN online for the logged out phone with the TN previously used, that ESTN may already be assigned to another phone. The result can be unpredictable. To avoid this situation, the LTPS must move the phone to its

original logged out state, and allow the Call Server to release the ESTN and its associated timer.

- ELAN/TLAN failure happens for more than 10 minutes when:
  - The ESA VOLO phone is on a call. As a result, the ACF timer or PSAP will release the call register. In this case, the ESA VOLO timer should be removed. Nevertheless, the active call should survive. The phone returns to its original logged out state, but according to ACF feature, the IP Line application closes the audio path if the phone goes on-hook or you press the release button.
  - ESA VOLO phone is in Waiting to Callback status. This is the same as 2a case, when the phone loses its ESTN info after reregistering and goes back to its original logged out state. This needs additional implementation on Call Server to free up reserved ESTN and it's timer.

Context Sensitive Soft Keys

This works for the original soft keys that came from Call Server, but there are two extra callers and redial soft keys that are added on the IP Line application. It needs an extra check on the IP Line application to prevent these two soft keys on a VOLO set.

Element Manager

Avaya CS 1000 Element Manager supports the following configuration, provisioning and maintenance aspects of the Basic Emergency Services When VO Logged Out Feature.

- Configuration: Changes in ESA data block in Overlay 24.
- Diagnostics: A new command PRT ESALO is added in Overlay 117.

Scenario: Navigation Changes

1. Login to CS 1000 Element Manager with a valid user account.
2. In the navigation pane, expand **System** > **Emergency Services**.
3. A new link Virtual Office Phone is added.

Scenario: Virtual Office Phone Page Layout

1. Login to CS 1000 Element Manager with a valid user account.
2. In the navigation pane, expand **System** > **Emergency Services** and click the **Virtual Office Phone** link.
3. The Virtual Office Phone page is loaded. This page contains the list of Used Virtual Office TNs and Mapped Virtual Office TN Pools.
4. VOLO can be configured only for one customer. If VOLO is configured for a customer, in the table Mapped Virtual Office TN Pools, **Add** button is disabled and

Delete button is enabled. If VOLO is not configured for any customer, then **Add** is enabled and **Delete** button is disabled.

5. If there are no Used VOLO TNs, the **Trace** button in Used Virtual Office TNs table is disabled.

Scenario: Add Virtual Office Phone Configuration Page Layout

1. Login to CS 1000 Element Manager with a valid user account.
2. In the navigation pane, expand **System** > **Emergency Services** and click the **Virtual Office Phone** link.
3. Click on **Add** button in the Mapped Virtual Office TN Pools table.
4. You are navigated to the Add Virtual Office Phone Configuration page.
5. Customer Number is a select box containing the list of configured customers. By default, the Customer configured with the lowest number is selected.
6. The TN Pool block allows the user to configure Starting TN, Number of TNs in Pool and TN Reservation period.
7. When the number of TNs is 0, the Starting TN and the TN reservation period is disabled.

Scenario: Emergency Service for Virtual Office Phone Configuration for a Customer with ESA Block Configured

1. Login to CS 1000 Element Manager with a valid user account.
2. In the navigation pane, expand **System** > **Emergency Services** and click the **Virtual Office Phone** link.
3. Click on **Add** button in the Mapped Virtual Office TN Pools table.
4. Choose a listed customer
5. Enter a valid value for Starting TN
6. Change the Number of TNs in pool.
7. Enter the time in minutes for the TN Reservation period prompt.
8. Click on **Save** button.
9. New values are configured and Virtual Office Phone page is displayed with updated values.

Scenario: Emergency Service for Virtual Office Phone Configuration when there are no customers with ESA block configured

1. Login to CS 1000 Element Manager with a valid user account.
2. In the navigation pane, expand **System** > **Emergency Services** and click the **Virtual Office Phone** link.
3. A confirmation message is displayed.

4. When you click the **OK** button, you are redirected to Add Emergency Services Directory Number page.
5. When you click the **Cancel** button, the Virtual Office Phone page is displayed. The **Add** and **Delete** buttons in Mapped Virtual Office TN Pools table are both disabled.

Scenario: Edit Virtual Office Phone Configuration Page Layout

1. Login to CS 1000 Element Manager with a valid user account.
2. In the navigation pane, expand **System** > **Emergency Services** and click the **Virtual Office Phone** link.
3. Click on **Customer** hyperlink in the Mapped Virtual Office TN Pools table.
4. You are navigated to the Edit Virtual Office Phone Configuration page.
5. The fields are populated with the configured values.
6. Change some field values on this page and click on the **Save** button.
7. New values are configured and Virtual Office Phone page is displayed with updated values.

Scenario: Virtual Office Phone Details Page Layout

1. Login to CS 1000 Element Manager with a valid user account.
2. In the navigation pane, expand **System** > **Emergency Services** and click the **Virtual Office Phone** link.
3. Click on **Virtual Office TN** hyperlink in the Used Virtual Office TNs table.
4. You are navigated to the Virtual Office Phone Details page.
5. None of the fields are editable in this page.
6. Clicking on **Cancel** button takes you to the Virtual Office Phone page.

Scenario: Call Trace Diagnostics (Overlay 80)

1. Login to CS 1000 Element Manager with a valid user account.
2. In the navigation pane, expand **System** > **Emergency Services** and click the **Virtual Office Phone** link.
3. The Virtual Office Phone page is loaded.
4. Choose a VIrtual Office TN and click on the Trace button in the Used Virtual Office TNs table.
5. The Call Trace Diagnostics page is loaded with the command TRAC (trace calls for the specified TN).

   Enter the ESA VOLO TN which is on call in the input text box and click the **Submit** button.

6. The result in the output text area is the same as mentioned in screen capture of Scenario: LD 80 Trak command.
7. The same command can be accessed from the Maintenance page. In the navigation pane, expand **System**. Navigate to Maintenance page and choose **Select by Overlay** option.
8. Select **LD - 80 Call Trace**

Chapter 7: Emergency Services M911 Networked Operation

Contents

This document contains information about the following topics:

Overview

After the events of September 11, 2001, it has become apparent that survivability of a Public Safety Answering Point (PSAP) based on geographic distribution is the key to providing critical public safety services. The Networked M911 functionality of the Emergency Services Access (ESA) feature provides this survivability by allowing an emergency call to be redirected from one Avaya Communication Server 1000 Call Server to another within an MCDN environment and receive emergency call treatment.

In placing an emergency call, the caller dials a configured Emergency Services DN (ESDN) and the End/Tandem Office routes this call over 911E/T trunks to the Avaya CS 1000 (hereafter called Node A). The Emergency Services M911 Networked Operation feature allows the emergency call to be redirected to another CS 1000 (hereafter called Node B) by means of TIE trunks. The types of call redirection used to accomplish this redirection are Network ACD (NACD)/Network Skill Based Routing (NSBR) and Manual Call Transfer.

So that the call is correctly identified as being an emergency call and appropriate emergency treatment is provided for the call at Node B, a new trunk subtype is introduced for configuration exclusively on TIE trunks - this new trunk subtype is referred to as M911P or, more simply, as 911P trunks.

For the purposes of convention, Node A will be referred to as the tandem (originating) Node and Node B will referred to as the target (destination) node. Also, the Emergency Services M911 Networked Operation feature will simply be referred to as Networked 911

The Networked 911 feature provides support for the following requirements, in addition to the basic M911 functionality on an MCDN network:

- Network ACD/Network Skill Based Routing and Call Abandon feature.
- 10/20 digit ANI support.
- Malicious Call Trace.
- Centrex Hook Switch Flash capability over 911P to support call transfer on selective router.
- Networked 911 supports 911 calls made using PRI/PRI2 and IP Peer facilities.

Assumptions

This section outlines the assumptions made regarding the setup and configuration of the environment to which the Networked 911 feature is being installed.

The assumptions are as follows:

- The 911 End/Tandem Office is connected to the CS 1000 by means of Analog 911E/T trunks.
- In an MCDN network, 911 calls route over 911P trunks only. Non 911 calls route by means of non 911P trunks.
- Networked 911 supports the tandem transfer of 911 calls over an MCDN Peer to Peer TIE trunk network (MCDN TIE network) between two CS 1000 systems only - cascading of emergency calls over more than two CS 1000 systems is not supported as part of this feature. That is, the path between two CS 1000 systems must be direct and without any intermediate hops. MCDN network refers to the SL1 interface between the two systems.
- At the target node, if an emergency 911 call arrives on a non 911P trunk, the call is placed in a high priority ACD queue but no other emergency call treatment is provided. An error message is printed as part of the details of the call, indicating that the call is an emergency call that was routed in such a way that it has not been identified as an emergency call. If, on the other hand, a non emergency 911 call arrives by means of a 911P trunk, no emergency call treatment is provided for the call is provided and an error message is printed with the details of the call.
- Networked 911 supports the M2216 ACD, M2616, M3904 and M3905 telephone set types - support for Networked 911 operation on IP phone sets is not provided.
- The T301 timer must not be used concurrently with this feature.
- In LD 16, the NCRD and NCNA prompts must be set to YES for 911P routes to provide number and name display for the emergency call at the Target node.
- The NASA prompt must be set to YES to allow Network Attendant Service. The RCAP prompt must be set to ND2/ND3 for Network Name Display.

Dependencies

Prerequisites for the successful operation of Networked 911 are as follows:

- Both CS 1000 Call Server nodes involved in the transfer of the emergency call must have CS 1000 Release 5.0 or later installed - Networked 911 does not function in a mixed release environment.
- Loadware Changes must be made to support the new Emergency IE.
- To support Networked 911 using IP Peer facilities, a minimum of two Signalling Servers (SS) are required at both the Tandem and Target nodes - one SS (at each node) must be dedicated to handling call transfers over 911P trunks and the other for handling standard non 911 calls.

Feature Description

This section details the operation of Networked 911.

Networked M911 operation

The Networked M911 feature supports both NACD and Call Transfer of 911 calls within an MCDN environment. All 911 calls on the tandem node can be redirected to the target node by means of either NACD/NSBR or Manual Call Transfer. In order for the target node to recognize the call as an emergency call and provide subsequent emergency call treatment, redirection must occur using 911P trunks only. If all outgoing 911P trunks at the Tandem node are busy at the time the redirection is attempted, an error message (ERR0086) is printed to the TTY.

When a 911 call is made and is transferred to the target node by means of NACD, call modification using Network ACD occurs if no agents are logged in at the source ACD DN. This can also happen if all agents at the source ACD DN are busy at the time of the call transfer, and the ACD Day/Night table at the target is configured with available active targets. The Day/Night tables can define local or remote active targets that are available for the appropriate routing of 911 calls.

Note:

The final routing destination of a 911 call should be to an ACD DN only.

Note:

Do not configure the target node to provide RAN/IVR/MUSIC/FORCE DISCONNECT/FORCE BUSY/SILENCE - doing so can result in calls in the Emergency Queue to be terminated improperly at agent positions. RAN/IVR/MUSIC/FORCE DISCONNECT/FORCE BUSY/SILENCE should be applied only at the tandem node.

In the case of an emergency call redirection terminating on a Symposium Call Center Server (SCCS) controlled CDN at the Target node, the Symposium request for IVR/RAN/MUSIC/ FORCE DISCONNECT/FORCE BUSY/SILENCE causes an error to be reported (911 calls should not be given RAN/IVR/Music - see previous note).

Emergency calls can also be manually transferred to the target node by an agent on the tandem node.

Note:

If the 911 call terminates on an Individual Directory Number (IDN) at the Target Node (by means of any call redirection or call modification), no emergency treatment is provided for the call.

Operation of the M911P trunk subtype

Networked M911 exclusively uses the M911P trunk subtype in its redirection of 911 calls over an MCDN Network. The M911P prompt in the Route Data Block (RDB) is used to configure the M911P trunk subtype on TIE trunks only - if the prompt is set to YES, the indication is made that the TIE trunks associated with a specific route are configured for use as M911P trunks.

All incoming emergency calls to the tandem CS 1000 node are redirected to the target CS 1000 node by means of these defined M911P trunks.

Operation of the 911 Emergency Call Control IE

The 911 Emergency Call Control IE (in the ISDN SETUP message) is used exclusively for 911 calls - it identifies emergency calls made on the tandem node and carries ANI information for the call to the target node during a Networked 911 redirection.

If the 911 Emergency Call Control IE is redirected with the emergency call to Target node by means of a non M911P trunk, the associated 911 call is placed in a high priority ACD queue but no other emergency call processing is provided - an error message is printed on the TTY. So that the agent receiving the transfer knows that the call should have received emergency call treatment, however, their telset display for the call is appended with a "911" tag to notify that the call is an emergency call even though it arrived on a non 911P trunk.

NACD and Call Transfer of 911 calls over M911P trunks

Network ACD over M911P

The Source ACD DN at the tandem node can have Day/Night Tables configured to allow the Network ACD of 911 calls over 911P trunks. All incoming 911 calls are sent to the Source ACD DN are put into the high priority ACD queue.

Because 911 calls will only receive emergency call handling if they are routed by means of 911P trunks, the NACD of 911 calls should be configured to redirect using 911P trunks only.

Therefore, when selecting a trunk for an outgoing emergency call to the target node it is important that the NACD Day/Night tables are only configured with remote targets associated with M911P routes. If an NACD table is configured with targets associated with non M911P routes, it can result in emergency calls trying to seize non M911P routes. If an emergency call tries to seize a non M911P route, the NACD redirection of the call is blocked at the tandem node and the call remains queued to the Source ACD DN. In the event that this occurs, error messages are printed on the TTY. In view of this, it is recommended that the Source ACD DN employed for NACD be a dedicated ACD DN equipped to handle emergency calls only.

The administrator should take care of these considerations while configuring NACD for use by the Networked M911 feature. Doing so will allow the best usage of M911P trunks.

Note:

During NACD/NSBR, if a 911 caller is listening to any form of IVR at the Tandem node when the Target agent becomes available, the IVR is removed and the 911 call is queued to the agent set.

Call Transfer/Conference over M911P

Emergency calls answered by an agent at the tandem node can redirected to the target node by means of Call Transfer or Call Conference. In such cases, the agent should be aware of the established dialing plans and DNs used to transfer the call over the M911P trunks. It is recommended that autodial numbers be configured on the agent's telephone, so that it is easier for the agent to transfer the call appropriately. Trunk priority is maintained for all emergency calls transferred or conferenced over M911P trunks.

The agent can transfer or conference the 911 call over a non M911P trunk as well, but these emergency calls are treated as a normal call at the target node. If redirection of a non emergency call is attempted over a M911P trunk by means of Call Transfer or Call Conference, the transfer or conference is blocked and an appropriate error message is printed.

As previously detailed, an emergency call is provided emergency treatment at the target node only if the call is redirected to an ACD DN at the target node using Call Transfer or Call Conference over an M911P trunk.

ANI display for transferred 911 calls

The trunk group name displayed for all transferred emergency calls (if this is displayed at the Target node) is the name configured for the incoming trunk group at the Tandem node. In case of Consultative Transfer, this display is applicable only after the transfer has been completed.

If an emergency call is redirected to the target node by means of a non M911P trunk, it is put in a high priority ACD queue but no other emergency call processing is provided. An error message is printed on the TTY to indicate that this has occurred. However, to allow the agent to know that this call should have been a networked 911P call, the agent telset display is appended with a 911 tag to notify that the call is an emergency call (even though it arrived on a non 911P trunk).

When an agent at either the Tandem or Target node drops out of the conference, 911 ANI display for the emergency call is provided on the phone of the active agent.

Call Redirections for Networked 911

A Summary of the various call redirection scenarios that can be encountered in the operation of Networked 911 is as follows:

- If an emergency call tries to route from the tandem node by means of a non M911P route, then NACD of the call is not allowed (blocked at the tandem node) and the call remains queued to the Source ACD DN.
- Although it is possible to transfer/conference the 911 call over non M911P routes, it is not recommended that this be done, as the emergency call would treated as a normal call at the target node.
- Non emergency calls are not allowed to NACD to the target node over 911P routes - NACD redirection of the call is blocked. Similarly, non emergency calls cannot be redirected to the target node by means of Call Transfer or Call Conference over M911P routes - the transfer or conference of the 911 call is blocked.

Transport and Display of ANI over M911P trunks

8 digit ANI on M911P trunks

Networked 911 redirects the ANI of an emergency call to the target Node (using M911P trunks) in the same format (KP + NPD/ID + ANI + ST) as it was received from 911E/911T trunks. KP, ST and STP tones sent from the 911 End Office/tandem office are converted on the tandem node to their respective hexadecimal formats and then propagated over the M911P trunks as part of the 911 Emergency Call Control IE passed along with the emergency call - hexadecimal conversion is required for the format of the received digits to be recognized at the target node.

Unlike 911E/T routes, M911_NPID_FORM and NPID_TBL_NUM (in the Route Data Block) are not prompted for M911P routes. This is because the ANI translation (from 8 digit to 10 digit, accomplished by accessing the NPID table) would have already taken place at the tandem node in the case of 911T routes. With Networked 911, the target node always receives the ANI of an emergency call from the Emergency Call Control IE, and so these prompts are not required for calls routed using M911P routes (as only emergency calls are routed over M911P).

The ANI contained in the 911 Emergency Call Control IE is decoded and stored at the target node. The length of the ANI is then determined and the display on the telephone set of the target agent is handled accordingly. The trunk name, if displayed at the telephone set, would be the name configured for incoming trunk group (911E/T) at the Tandem node for all 911 calls.

10/20 digit ANI on M911P Trunks

All ANI information received for an incoming emergency call over a 911E/911T trunk is propagated to the target node over 911P trunks by means of the 911 Emergency Call Control IE (present in the ISDN Setup message).

As with 8 digit ANIs, the KP, ST and STP tones sent from the 911 End Office/Tandem Office are converted on the tandem node to their respective hexadecimal formats, which are then propagated over the M911P trunks as part of the 911 Emergency Call Control IE (passed along with the emergency call). Hexadecimal conversion is required for the format of the received digits to be recognized at the target node.

The trunk name if displayed at the telephone set would be the name configured for 911E/T trunks at the Tandem node, on which the 911 call arrived.

M911_NPID_FORM and NPID_TBL_NUM is not prompted in the RDB.

ANI display is handled based on the length of the digits received from the 911 Emergency Call Control IE.

At the target node, the M911_PANI prompt in the Customer Data Block determines whether or not to display PSEUDO ANI on the answering digital set - a PSEUDO ANI is loosely defined as being the cell site or sector information of a wireless caller. M911_PANI is only prompted if the M911_ENH_PKG 249 is equipped, and its default value is set to NO.

Even in the case where the M911_ENH_PKG 249 package is equipped, and the M911_PANI prompt is left at the default value of NO, the PSEUDO ANI is still displayed for a moment before being replaced with meaningful CPND information. If no CPND information is available then the line containing the PSUEDO ANI information is kept blank. This is done because the PSEUDO ANI information is a critical piece of data in performing ALI lookup.

If the M911_ENH_PKG 249 package is unequipped then the PSEUDO ANI is not displayed at all. This means that no indication is given that the emergency call is being placed from a wireless phone.

SCCS interactions:

In the event that an emergency call is redirected to a Symposium Call Center Server (SCCS) controlled CDN, 10/20 digit ANI information should be sent over the Application Module Link (AML). The length of the IE in the following messages are changed to accommodate all 20 digits in the ANI:

- ICC
- PCI
- USM Active
- USM Hold
- USM Ringing
- USM Unringing
- USM Transfer Initiate
- USM Conference Initiate
- USM Restore
- USM Conference to Simple
- USM Transfer Complete
- USM Disconnect
- Call Abandon and CALLANS

The various IEs changed in these messages to accommodate the 20 digit ANI are as follows.

- Originating DN IE H.30 in the ICC message
- Calling Party DN and Transfer DN IE H.4C in the PCI message
- Other Party DN IE H.39 in the USM Active, USM Hold, USM Ringing, USM Unringing, USM
- Transfer Initiate, USM Conference Initiate, USM Restore, USM Conference to Simple and USM Transfer Complete messages.
- Transfer DN IE H.4C in the USM Ringing, USM Active and USM Disconnect message.
- Other Party DN IE H.39 in the CALLANS message.
- Orig DN IE H.30 in the Call Abandon message.
- If the agent telset display is controlled by SCCS, it is overridden to make sure that the standard 911 display is shown on an agent set for a 911 call.
- Along with support of NACD for 911 calls, Network Skill Based Routing for 911 calls incoming at the tandem node is supported.

Network Skill Based Routing for 911 calls:

As part of the regular setup of NSBR on the Call Servers, the SCCS at each node is connected to the CS 1000 using an ELAN connection. Therefore, the SCCS of one node can be connected to an SCCS of a different node by means of its data network. CS 1000 Call Servers themselves are connected together by means of the CS 1000 MCDN network, so that an incoming 911 call from the tandem node can be routed to the target node and answered by a reserved agent.

For the sake of convention, the SCCS at the tandem node is referred to as the Tandem SCCS, the SCCS at the target node is referred to as Target SCCS, and the agent at the target node is referred to as remote agent in the explanations that follow.

The tandem SCCS can issue the Network Skill Routing Call request to reserve an agent (in idle state) from the target node. When the agent is reserved, the tandem node routes the 911 call to the target node over the CS 1000 MCDN network. When the remote agent answers the Network Skill Based Routing call, USM Offhook and USM Active AML messages are sent to the target SCCS and an ISDN Connect message is returned to the tandem node.

When the ISDN CONNECT message is received at the tandem node, an AML Call Answer message is sent to the tandem SCCS to notify that the Network Skill Based Routing call has been answered by the remote agent. Now, if the remote agent releases the Network Skill Based Routing call, the target node would send an ISDN DISCONNECT message to the tandem node. Also, USM Onhook and USM Disconnect AML messages are sent to the target SCCS to notify that the call has been released from the remote agent. When the ISDN DISCONNECT message is received at the Tandem node, it sends an AML Call Disconnect message to the tandem SCCS.

If a 911 caller abandons the call, Call Abandon Treatment is given to the 911 call. Refer to Call abandon treatment for 911 calls connecting to 911P trunks.

Do not script to give RAN/IVR/MUSIC/FORCE DISCONNECT/FORCE BUSY/SILENCE at target node. This will cause calls in Emergency Queue to be terminated improperly at agent

positions. All give RAN/IVR/MUSIC/FORCE DISCONNECT/FORCE BUSY/SILENCE should be applied only at the tandem node.

In case of any call redirections that terminate the 911 call on a SCCS controlled CDN at the Target node, the Symposium request on the target node for IVR/RAN/MUSIC/FORCE DISCONNECT/FORCE BUSY/SILENCE is returned with an appropriate error (911 call should not be given RAN/IVR/Music).

ANI Failure

In 911E/T configurations, if an ANI failure occurs it is indicated on the answering set with “0000000”. At the tandem node, if the call is received with ANI failure, the 911 Emergency Call Control IE passed with the emergency call over the 911P trunks holds zeroes. At the target node, call is terminated but zeroes are displayed on the answering set.

Some of the scenarios which can be considered as ANI failure at the tandem node are the following:

- Single digit ANI is interpreted as ANI failure based on the NPID table.
- If timeout occurs on the trunk signalling protocol while waiting for ANI receipt.
- MF tones are unrecognizable at the tandem node.
- An 8 digit ANI is received at the tandem node with a normal NPD followed by 911-0YYY. For such cases, the display at the target node is inline with that at the tandem node.

Refer to *Avaya Features and Services Fundamentals, NN43001-106* for more information.

Call abandon treatment for 911 calls connecting to 911P trunks

When the 911 caller abandons the call, a disconnect notice is received at the tandem node. For NACD or NSBR, this message is not sent to the target node, to hold the 911P trunks until the call taker at the Target node releases the call. A new Operation ID is introduced as part of the NAS Service Invoke Identifiers in FACILITY IE and is sent to the target node to indicate that the call has been abandoned. A timer, ABTR (configured in overlay 16 (RDB)) is started at the tandem node, upon receiving the FACILITY ACK success from the target Node, to keep the 911P trunks busy until either the call taker releases the call at the target node or the timer expires. The timer is given a default value of 15 minutes and can be configured from a range of 0-30 minutes with increments of 1 minute. If the FACILITY ACK success is not received then the FACILITY IE is retransmitted after an interval of 4 seconds. Only two retransmissions are allowed.

If the call is answered at the target node, an ISDN CONNECT message is sent to the tandem node and the SCCS at the tandem node is informed of the same by the AML CALLANS message. The timer (ABTR) is disabled when the ISDN CONNECT is received at the tandem node.

An AML CALLDIS message is sent to the tandem SCCS when an ISDN Disconnect message is received at the tandem node. If the call is not answered at the target node and the timer expires, then the blocked ISDN Disconnect is tandem transferred to the target node. An AML Call abandon message is then sent across to the SCCS at the tandem node, and the trunks are released.

If a 911 call is abandoned it is still at the tandem node, the ISDN FACILITY IE is sent to the target node. This occurs only after the ISDN ALERT/CALL PROCEEDING is sent to the tandem node from the target node.

When an abandoned 911 call over 911P trunk is answered, the call Abandon treatment given to the call is the same as the Call Abandon treatment given to a call arriving on 911E/911T trunks. This includes appending of the ABAND tag to the ANI display as well as providing a six second continuous cadence tone (if configured) to the call taker.

The Call Abandon treatment applies only for those calls which are not answered. Therefore this treatment applies only to NACD/NSBR redirections and not for Transfer/Conference.

The Call Abandon treatment is not provided in case of a call with ANI failure.

Support of Centrex Hook Switch Flash over 911P

The Trunk Hook Flash (THF) sent by the CS 1000 over certain non ISDN trunks is used by Centrex Switchhook Flash, Malicious Call Trace (MCT), and other CS 2000 or CS 2100 features. The THF can be accessed through tandem MCDN TIE trunks for MCT by the CS 1000. The Networked M911 feature provides the CS 1000 station users the ability to generate a switchhook flash signal towards Central Office (CO) when they are on a call established using CO. This signal is interpreted by the Central Office as a request for the activation of one of the services offered by the public switch itself (conference or call transfer, for example). The user can operate on these services by sending further information (digits) directly from the telephone set (End to End Signaling).

As part of the Networked M911 feature, a new Operation ID introduced as part of NAS Service Invoke Identifiers in FACILITY IE is sent to the tandem node to indicate the initiation of the feature at the target node. This results in the tandem node generating a switchhook flash signal towards CO. A new CLS NHFA/NHFD (Network Hook Flash Allowed/Denied) is introduced in LD 14 to allow/deny the Trunk Hook Flash feature over 911P trunks.

Support of Malicious Call Trace over 911P

Malicious Call Trace (MCT) allows users of selected telephones to activate a call trace that results in a printed report of the calling and called parties. The report is generated on all system TTYs designated as maintenance terminals. If the caller has to be traced, while a 911 call is in progress, the agent can activate this feature (if an appropriate key is defined on the selected telephone), and identify the offending trunk.

End to End Signalling is allowed on a 911P trunk during talk state to support MCT.

Support for Network Time Synchronization over 911P

The Network Time Synchronization functionality ensures that all time stamps in a network are synchronized from one source. One switch becomes the master for this purpose.

In a private network environment, each switch in the network has an individual system clock. These system clocks can, under certain conditions, lose or gain time, causing inaccurate timestamps for different features. The issue of inaccurate timestamps is made more pronounced by the fact that, in a private network, it is possible for several switches to be located in different time zones. As features become more centralized in a network environment; it is useful to have time stamps based on one time zone. To provide Time Synchronization on a network-wide basis, MCDN nodes can request Time Synchronization from another node, using D-channel messages.

The Network Time Protocol is widely used to synchronize computer clocks in the global network. The NTP client (that is, the CS 1000 system) gets its time from an authoritative NTP server using its ELAN connectivity, and then distributes the time across its different components like Signalling Server, Symposium, CallPilot. NTP allows the system to

synchronize with a customer’s own NTP Server not only for the purpose of accuracy between the two nodes but also for security reasons. The Networked M911 feature ensures that the time on two separate CS 1000 Call Servers (connected by 911P trunks) are synchronized.

Support of Networked M911 feature on IP Peer facilities

To support this feature on IP Peer facilities (H.323 and SIP), each node (Tandem and Target) requires a minimum of two SS. Current IP Peer does not have the intelligence to route calls based on the trunk type. There can be situations when a 911 call arrives on a 911P trunk at the Tandem SS but at the Target SS it may take a non-911P trunk. This may result in the 911 call being treated as a normal call. To avoid such scenarios and to give emergency treatment to a 911 call, a dedicated SS for 911P trunks, a fixed dialing plan and dedicated ACD DNs are required at both the Tandem and Target nodes.

For IP Peer network, if UDP/CDP configuration is used, a unique ACD DN must be defined exclusively for 911 calls at the Target and Tandem nodes. When defining the remote targets in the NACD table or configuring the ADL keys on the agent set, these unique ACD DNs must be used for routing of 911 calls. At the NRS, care must be taken to configure the ACD DN to terminate on a SS dedicated for 911P trunks. In case of non 911 calls another ACD DN must be defined.

Note:

The ACD DNs (for UDP or CDP) defined should be unique and used for 911 calls only. It should not conflict with any other ACD DN configurations. To support Least Cost Routing (LCR), the alternate routes must terminate on a SS dedicated for 911P trunks.

911P route entry on the NRS must never be configured as default route.

Modification of CPDC feature

Called Party Disconnect Control (CPDC) allows a CS 1000 system to control the disconnection of calls on Central Office (CO), Foreign Exchange (FX), Common Control Switching Arrangement (CCSA), Direct Inward Dialing (DID), TIE, Wide Area Telephone Service (WATS), modem, and Centralized Automatic Message Accounting (CAMA) trunks. With Called Party Disconnect Control, an incoming trunk call answered on a CS 1000 Call Server is not disconnected until the call taker goes onhook. If the calling party goes onhook, the connection is held, allowing the call to be traced in emergency situations.

The CPDC feature is applicable only for 911 calls which are established to an ACD agent.

The Networked M911 feature provides support for use of the CPDC feature over TIE trunks with trunk subtype M911P.

Configuration and Provisioning

Overlay 16

Prompts and Responses

A trunk subtype is included in the Route Data Block, exclusively for TIE trunks. All the prompts specific to 911 in the RDB are made applicable when the TKTP prompt value is TIE. In case of TIE trunks, the M911_TRK_TYPE prompt does not appear and is replaced by the newly introduced prompt, M911P. The M911_ANI, M911_NPID_FORM and NPID_TBL_NUM are not prompted.

If M911P prompt is set to YES:

- A new prompt ABTR is prompted. This prompt has a default value of 15 minutes.
- DTRK prompt is set to YES and is non-configurable.
- IFC prompt is set to SL1 and is non-configurable.

Note:

If the DTI and PRI2 packages are restricted and the VTRK prompt is set to NO, SCH2160 is printed on the TTY and VTRK is re-prompted. This is because only PRI/PRI2 is supported for 911P routes and if DTI and PRI2 packages are restricted, VTRK should not be set to NO.

System/Alarm Messages

An error message (SCH0765) is used for an invalid response for M911P prompt. In addition, two additional errors are used, in the cases as follows:

- .SCH1980 is used to handle cases when DGTP prompt in the Route Data Block is set to any value other than PRI/PRI2.
- .SCH2160 is used to handle the case when the DTI and PRI2 packages are restricted and the VTRK prompt is set to NO.

Overlay 14

The Class of Service NHFA/NHFD (Network Hook Flash Allowed/Denied) is introduced in overlay 14 to allow/deny the support Trunk Hook Switch Flash feature over 911P trunks.

Overlay 15

As per the 10/20 digit ANI feature, M911_PANI is prompted in the Customer data block if M911_ENH_PKG 249 is equipped.

Overlay 23

The Source ACD DN at the tandem node should be configured such that it is a dedicated ACD queue serving 911 calls only. Non-911 calls should not be allowed to land on this ACD DN.

While configuring the NACD table, it should be noted that all the remote targets are associated with 911P routes only. This can be done by associating the RLI for the remote active targets with 911P routes.

Print Routines, Overlay 20

Overlay 20 is used to print the TN block, including NHFA/NHFD as configured in Overlay 14.

Print Routines, Overlay 21

Overlay 21 is used to print the route data block, including the prompts and responses for Meridian 911P routes. The 911 related prompts, M911_ABAN, M911_TONE, M911P and ABTR are printed in the RDB. Other 911 prompts like, M911_TRK_TYPE, M911_ANI, M911_NPID_FORM and NPID_TBL_NUM are not printed.

Configuration examples for 911P trunks in RDB

New RDB for PRI/PRI2 with trunk sub-type M911P

1. Load Overlay 16.
2. Create “NEW” Route Data Block
3. Set TKTP to TIE
4. M911P prompt is output. Set it to YES.
5. M911_ABAN prompt is output. Set it to YES.
6. M911_TONE prompt is output. Set it to YES.
7. ABTR prompt is output. Set a value between 0-30.
8. VTRK prompt is output. Set it to NO. (Default value is NO).
9. DTRK prompt set to YES is output.
10. BRIP prompt set to NO is output.
11. Set DGTP to PRI/PRI2.
12. IFC prompt set to SL1 is output.

New RDB with trunk sub-type M911P and DGTP set to DTI/DTI2

1. Steps 1 to 10 as mentioned in Scenario 1.0 (previous)
2. Set DGTP to DTI/DTI2.
3. Error. DTI/DTI2 not supported over 911P trunks.

CHG RDB (non-M911 route) with trunk type TIE

1. Load Overlay 16.
2. “CHG” existing Route Data Block
3. M911P prompt is output. Set it to YES.
4. Error (.SCH5675). Cannot change a non-M911 route to a M911 route.

CHG RDB (M911 route) with trunk type TIE

- Load Overlay 16.
- “CHG” existing Route Data Block
- M911P prompt is output. Set it to NO.
- All the M911P prompts are skipped.

New RDB for IP Peer with trunk sub-type M911P

1. Load Overlay 16.
2. Create “NEW” Route Data Block
3. Set TKTP to TIE.
4. M911P prompt is output. Set it to YES.
5. M911_ABAN prompt is output. Set it to YES.
6. M911_TONE prompt is output. Set it to YES.
7. ABTR prompt is output. Set a value between 0-30.
8. VTRK prompt is output. Set it to YES.
9. NODE prompt is output. Give the NODE ID associated with the SS (dedicated for 911P trunks)
10. DTRK and DGTP are not prompted.
11. IFC prompt set to SL1 is output

Interactions/Interworkings

Feature Interactions

Calling Party Privacy

If an incoming call with a Privacy Indicator terminates on a system switch configured with M911, the ANI information (if it exists) is still sent to the Meridian 911 application. The Privacy Indicator is ignored on all 911 calls propagated over 911P trunks.

Called Party Disconnect Control

The Called Party Disconnect Control feature is modified to allow called party disconnect control over tandem connections of trunk identified as M911 911T or 911E and trunk sub-type M911P. Ability to hold tandem trunk connection until the termination call taker releases the call. This applies to calls that are established to an ACD agent.

Transfer/Conference

Emergency treatment is provided to all 911 calls transferred/conferenced by means of 911P trunks. The same applies to No Hold conference calls. Abandoned 911 calls cannot be transferred/conferenced.

The trunk priority is maintained for all 911 calls transferred/conferenced by means of 911P trunks.

Display of Calling Party Denied

An incoming M911 call with Automatic Number Identification (ANI) information always displays ANI digits on the terminating set regardless of the calling party's DPD Class of Service.

Malicious Call Trace

Malicious Call Trace feature is supported over tandem trunk connection by means of MCDN 911P trunks.

Basic Rate Interface (BRI)

Answering positions are not supported on BRI sets.

Dialed Number Identification Service

Dialed Number Identification Service is not supported on 911P trunks.

Incoming Digit Conversion (IDC)

IDC name, if configured, is overridden by the name configured for the 911E/T trunks at the Tandem Node.

Calling Party Name Display

The Calling Party Name Display feature can be used to configure and display the incoming 911 route name.

Night Call Forward

If the ACD DN at the tandem node has NCFW defined to a valid destination at the target node, the 911 call is sent to the NCFW destination. The NCFW destination should be a valid ACD DN which is defined at the target node. This is supported for 911P trunks.

Interflow

911 calls can interflow to a valid ACD DN defined at the target node. This is supported for 911P trunks.

Overflow

911 calls can overflow just like any other ACD calls within the tandem node. Overflow DN is always an ACD DN.

Call Force

Abandoned 911 calls can be call forced.

Not Ready

Abandoned calls that are being presented to an agent at the target node are put back into the queue when the NRD key is pressed, but no RAN or music is provided which is consistent with existing 911 operation. If an agent is established on an abandoned call and presses the Not Ready Key, the call is dropped.

Supervisor Observe

On abandoned 911 calls, because there is no speech path between the ACD agent and the caller, the supervisor observe feature is blocked. The supervisor can still press the OBV key on his set to observe an agent active on an abandoned call, but he hears silence.

Night Service Key (NSVC)

If the calls reach Target node by way of NSVC key operation on Tandem node, the Emergency Treatment for 911 calls is provided at the Target node. However, if the 911 call is redirected to another node from the Target node, the Emergency Treatment is not supported.

ACD C-Reports

The ACD-C reports printed at the target node remains consistent with the existing format of the reports printed at the tandem node.

For the ACD-C reports, the CALLS ANSWD field only accounts for real calls; the ABANDONED field accounts for abandoned calls that are answered, assuming that all abandoned calls are eventually answered by an agent. Consequently the CALLS ACCPTD field is equal to the CALLS ANSWD field plus the ABANDONED field (number of calls entering queue = number of real calls + number of abandoned ones). This way the Average or Total Call-Processing (DCP) Time accurately reflects the amount of time an agent spent on real calls, because answering an abandoned call requires little amount of time. The work that the agent does for an abandoned call is more accurately reflected in the DN OUT and OUT TIME fields, which mean total number of outgoing calls and total time of all outgoing calls respectively. Because the agent must hang up the abandoned call and call back to see what the condition is, the outgoing call that he makes is more valuable for reporting his work.

Controlled Directory Number Ceiling

The CDN ceiling feature returns busy tone to calls arriving at the CDN while it is in default mode. If a 911 call should arrive while these conditions are true, the 911 call does not hear busy tone, but is linked into the default destination ACD DN’s queue. Therefore, the setting of the ceiling value is irrelevant if only 911 calls are expected at the CDN. The ceiling value, is still applied to non-911 calls arriving at the CDN. This is supported for 911P trunks.

Delay Night RAN

Delay Night RAN is not given to a 911 call in case NACD/NSBR as all 911 calls are emergency calls.

IP Trunks

H.323 trunks over ITG are not supported as part of this feature.

Trunk Anti Tromboning (TAT)

There are no interactions with this feature. However, if the call returns back to the Tandem node by way of any call modifications or call redirections, it is not treated as an emergency call.

Trunk Optimization Before Answer (TRO-BA)

Because this feature operates between two nodes, there are no interactions with TRO-BA (no intermediate hops).

Trunk Optimization Call Modification (TRO-CM)

Because this feature operates between two nodes, there are no interactions with TRO-CM (no intermediate hops).

ISL Trunks

ISL trunks on PRI/PRI2 are not supported as part of this feature.

Chapter 8: Emergency Services Access for Europe, the Middle East, and Africa

Contents

This document contains information about the following topics:

Introduction

ESA has been designed extensively in U.S. and Canada for both Enterprise and Carrier markets using North American standards based CAMA (Centralized Automatic Message Accounting) and ISDN trunks.

ESA for EMEA applies to Europe, the Middle East, and Africa (EMEA). For Europe, it applies to European countries that are members of the European Union (EU). EU members are under obligation to adopt the directive for the universal adoption of single emergency response number 112. ESA for EMEA supports 112 or any other single emergency response number in use prior to the EU directive.

Note:

EMEA markets do not support the use of CAMA trunks.

The EMEA trunking protocols supported are limited to:

- BRIE (Basic Rate Interface – ETSI based)
- PRI 2.0 (Primary Rate Interface per Euro ISDN)
- QSIG on PRI
- DPNSS
- IP tandem trunks to ISDN

Public network operators provide the location information for both fixed and mobile callers making 112 calls. Where private networks are involved, the private network gateway must provide the location information.

Feature packaging

This section identifies the software packages that the ESA for EMEA feature requires. ESA is comprised of three software packages (329, 330, and 331) that are explained in detail in sections to follow .

The software packages are listed according to the defined type of functionality.

Total functionality

Emergency Services Access (ESA) is package 329 and provides the following functions:

- ESA Call Recognition
- ESA Call Routing to Primary Rate Interface (PRI), or other trunks
- Basic number translations such as NXX and NPA, but excluding non-Direct Inward Dialing (DID) translations
- ESA Call Termination Identification
- Emergency Services Access (ESA) package 329 has the following dependencies:
    - Automatic Number Identification (ANI) package 12
    - Office Data Administration System (ODAS) package 20
    - Calling Party Name Display (CPND) package 95
    - Integrated Services Digital Network (ISDN) package 145

Emergency Services Access Supplementary (ESA_SUPP) is package 330 and provides the following functions:

- Networking conversions such as incoming ISDN conversions
- On-Site notification

Emergency Services Access Calling Number Mapping (ESA_CLMP) is package 331 and provides the translation of non-Direct Inward Dialing (non-DID) numbers.

Partial functionality

ESA Call Recognition requires Emergency Service Access (ESA) package 329.

ESA Call Termination Identification requires the following packages:

- Emergency Service Access (ESA) package 329
- Emergency Service Access Calling Number Mapping (ESA_CLMP) package 331 (required if the customer desires translation of non-DID numbers to DID numbers)

ESA Call Routing requires the following packages:

- Emergency Services Access (ESA) package 329
- Emergency Services Access Supplementary (ESA_SUPP) package 330 (required if the customer is to offer ISDN tandem ESA calls and wants to allow the Calling Line Identification (CLID) from the incoming ISDN trunk to be converted for outpulsing as the calling number)
- Integrated Services Digital Network (ISDN) package 145 (required if the ESA calls are transported over outgoing ISDN trunks)

ESA On-Site Notification requires the following packages:

- Emergency Services Access (ESA) package 329
- Emergency Services Access Supplementary (ESA_SUPP) package 330
- Calling Party Name Display (CPND) package 95 (required to provide the originator's name on the call record, and to display the originator's name on the On-Site Notification [OSN] set)
- Office Data Administration System (ODAS) package 20 (required to provide the originator's DES information on the call record and to display the originator's DES information on the OSN set)

Note:

The ESA On-Site Notification (OSN) function notifies local security personnel that an emergency call has occurred. This notification can be provided by a maintenance device or a digital telephone with display.