



Nortel Communication Server 1000

Emergency Services Access Fundamentals

Document status: Standard
Document version: 01.01
Document date: 30 May 2007

Copyright © 2003-2007, Nortel Networks
All Rights Reserved.

Sourced in Canada.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

Nortel, the Nortel Logo, the Globemark, SL-1, Meridian 1, and Succession are trademarks of Nortel Networks.

All other trademarks are the property of their respective owners.

Revision History

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.

January 2007

Preliminary 00.08. Preliminary version of this document is released.

December 2006

Draft 00.06. This document is up-issued to incorporate items and restructuring resulting from documentation review.

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.

4 Revision History

Contents

New in this release	11
Features 11	
How to get help	13
Contents 13	
Getting help from the Nortel web site 13	
Getting help over the telephone from a Nortel Solutions Center 13	
Getting help from a specialist by using an Express Routing Code 14	
Getting help through a Nortel distributor or reseller 14	
About this document	15
Subject 15	
Applicable systems 15	
Intended audience 16	
Conventions 16	
Related information 17	
Emergency Services Access	19
Contents 19	
Introduction 20	
Background information 23	
Passing emergency caller information to the PSAP 23	
Routing to correct PSAP vs. delivering suitable ANI 24	
The ALI Record 25	
Enterprise wide mobility 26	
Data centralization 27	
Location based handling of emergency calls 27	
Location granularity 29	
Location granularity for WLAN E911 29	
Feature description 32	
System Components 34	
Location management 37	
Emergency Response Location (ERL) 38	
Emergency Caller Location (ECL) 39	
Architecture 40	

Location as a device attribute	40
IP Line application	41
Home Location data in the TN Block (TNB)	41
Storing location data in the TN Table	42
Location reporting	47
Subnet lookup table	52
Interworking with the DM	59
ERL table	66
Location management for non IP lines	71
Call Recognition	73
Calling Terminal Identification	76
Calling number composition	77
Dynamic ELIN	81
Background	81
Overview	81
Operation	82
Configuration considerations	83
Callback fallback	85
Overflow	86
Expired mappings	87
Emergency caller unregistrations	87
ELIN TN configuration	87
Administration	88
Maintenance	89
Configuration considerations	89
Dynamic ELIN audit	89
System messages	90
Multiple Appearance DNS	93
Survivability	93
System engineering	93
Digit translation examples	95
Call Routing	100
ESA enhanced routing	105
Emergency call routing	113
PSTN routing: Enhanced 911 versus Basic 911	113
Internal routing	114
On-Site Notification	115
OSN TTY	125
OSN phone display enhancement	126
OSN record / SNMP trap	130
On Site Notification	136
Tandem OSN	136
ESA Misdial Prevention	136

Overview	136
Operation	137
Administration	138
Multiple ESDNs	141
Overview	141
System configurations	151
Implementation and engineering considerations	162
Operating parameters	166
Non-networking feature interactions	169
Converged Desktop (CD)	171
Networking feature interactions	173
Feature packaging	177
Feature implementation	179
Feature operation	189
ESA call processing	193
Availability / survivability scenarios	202
Call Server restart / switchover	202
IP phone restart	203
Alternate Call Server	203
Geographic Redundancy	203
Signaling Server restart	204
Survivable Branch Office	204
Survivable Remote Gateway	205
External DM failure	205
System Management	206
Service Parameters (LD 17)	206
Access Numbers and Routing (LD 24)	207
Emergency Response Locations (LD 117)	212
Subnet Location Information Service (LD 117)	214
Dynamic Location Identification Number (LD 117)	216
ESA maintenance commands (LD 117)	216
CLI commands	217
Location Report (LD 117)	218

Emergency Services for Virtual Office

221

Contents	221
Introduction	221
Operating parameters	223
Feature interactions	225
Feature packaging	225
Feature implementation	225
Feature operation	225
E911 for VO	225
Background	225

Overview	226
Operation	226
Manual Update TNs	227
System messages	228
Branch Users	228
Active Call Failover	228
Basic Emergency Service When VO Logged Out	229
Contents	229
Overview	229
Configure ESA Data Block	237
Maintenance and Diagnostics	240
Warm Start	240
CLID Composition	241
Active Call Fail Over	241
Context Sensitive Soft Keys	242
Element Manager	242
Emergency Services M911 Networked Operation	247
Contents	247
Overview	247
Assumptions	248
Dependencies	249
Feature Description	249
Networked M911 operation	249
Configuration and Provisioning	259
Overlay 16	259
Overlay 14	260
Overlay 15	260
Overlay 23	260
Print Routines, Overlay 20	260
Print Routines, Overlay 21	260
Configuration examples for 911P trunks in RDB	261
Interactions / Interworkings	262
Feature Interactions	262
Emergency Services Access for Europe, the Middle East, and Africa	267
Contents	267
Introduction	267
Feature packaging	268
Emergency Services Access Configuration Audit	271
Contents	271
Feature description	271
Feature implementation	272

CLIDVER 284

New in this release

The following sections detail what's new in *Emergency Services Access Fundamentals (NN43001-613)* for Release 5.0:

Features

See the following sections for information about feature changes:

- [Emergency Services Access](#) contains new descriptions of functionality developed in Release 5.0.
- [Emergency Services M911 Networked Operation](#) describes new feature functionality.
- [Emergency Services for Virtual Office](#) describes new feature functionality.

How to get help

Contents

This section contains information on the following topics:

- Getting help from the Nortel web site
- Getting help over the telephone from a Nortel Solutions Center
- Getting help from a specialist by using an Express Routing Code
- Getting help through a Nortel distributor or reseller

Getting help from the Nortel web site

The best way to get technical support for Nortel products is from the Nortel Technical Support web site:

www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the telephone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support web site, and you have a Nortel support contract, you can also get help over the telephone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following web site to obtain the telephone number for your region:

www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

www.nortel.com

Getting help through a Nortel distributor or reseller

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

About this document

This document is a global document. Contact your system supplier or your Nortel 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 NTP contains information about systems, components, and features that are compatible with Nortel Communication Server 1000 Release 4.5 software. For more information on legacy products and releases, click the **Technical Documentation** link under **Support & Training** on the Nortel home page:

www.nortel.com

Applicable systems

This document applies to the following systems:

- Communication Server 1000S (CS 1000S)
- Communication Server 1000M Chassis (CS 1000M Chassis)
- Communication Server 1000M Cabinet (CS 1000M Cabinet)
- Communication Server 1000M Half Group (CS 1000M HG)
- Communication Server 1000M Single Group (CS 1000M SG)
- Communication Server 1000M Multi Group (CS 1000M MG)
- Communication Server 1000E (CS 1000E)
- Meridian 1 PBX 11C Chassis
- Meridian 1 PBX 11C Cabinet
- Meridian 1 PBX 51C
- Meridian 1 PBX 61C
- Meridian 1 PBX 81

- Meridian 1 PBX 81C

Note: When upgrading software, memory upgrades may be required on the Signaling Server, the Call Server, or both.

System migration

When particular Meridian 1 systems are upgraded to run CS 1000 Release 4.5 software and configured to include a Signaling Server, they become CS 1000M systems. [Table 1 "Meridian 1 systems to CS 1000M systems" \(page 16\)](#) lists each Meridian 1 system that supports an upgrade path to a CS 1000M system.

Table 1
Meridian 1 systems to CS 1000M systems

This Meridian 1 system...	Maps to this CS 1000M system
Meridian 1 PBX 11C Chassis	CS 1000M Chassis
Meridian 1 PBX 11C Cabinet	CS 1000M Cabinet
Meridian 1 PBX 51C	CS 1000M Half Group
Meridian 1 PBX 61C	CS 1000M Single Group
Meridian 1 PBX 81	CS 1000M Multi Group
Meridian 1 PBX 81C	CS 1000M Multi Group

For more information, see one or more of the following NTPs:

- *Communication Server 1000M and Meridian 1: Small System Upgrade Procedures (NN43011-459)*
- *CS 1000M and Meridian 1 Large System Upgrades Overview (NN43021-458)*
- *Communication Server 1000E Upgrades (NN43041-458)*

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

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

- Communication Server 1000M Chassis (CS 1000M Chassis)
- Communication Server 1000M Cabinet (CS 1000M Cabinet)
- Meridian 1 PBX 11C Chassis
- Meridian 1 PBX 11C Cabinet

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.

NTPs

The following NTPs are referenced in this document:

- *IP Phones Fundamentals (NN43001-368)*
- *Features and Services (NN43001-106)*
- *Branch Office Installation and Commissioning (NN43001-314)*

Online

To access Nortel documentation online, click the **Technical Documentation** link under **Support & Training** on the Nortel home page:

www.nortel.com

CD-ROM

To obtain Nortel documentation on CD-ROM, contact your Nortel customer representative.

Emergency Services Access

Contents

This section contains information about the following topics:

"Introduction" (page 20)

"Background information" (page 23)

"Feature description" (page 32)

"Location management" (page 37)

"Call Recognition" (page 73)

"Calling Terminal Identification" (page 76)

"Calling number composition" (page 77)

"Dynamic ELIN" (page 202)

"Digit translation examples" (page 95)

"Call Routing" (page 100)

"On-Site Notification" (page 115)

"ESA Misdial Prevention" (page 136)

"Multiple ESDNs" (page 141)

"System configurations" (page 151)

"Implementation and engineering considerations" (page 162)

"Operating parameters" (page 166)

"Non-networking feature interactions" (page 169)

"Networking feature interactions" (page 173)

"Feature packaging" (page 177)

"Feature implementation" (page 179)

"Feature operation" (page 189)

"Availability / survivability scenarios" (page 202)

"System Management" (page 206)

Introduction

The Emergency Services Access (ESA) is a feature that extends the type of emergency call handling found in residential 911 to telephony clients within an enterprise call environment. It will be appreciated by any customer who wants to route emergency calls in a special way, or who wants to be notified when a phone user makes an emergency call.

ESA introduces new implementation issues to be addressed by system administrators and craftspeople. For example, when making service changes to individual phones and DN's, changes to the ESA database (such as setting up the Calling Line Identification tables) have to be made at the same time. And when setting up the ESA database, ESA customer requirements must be considered, such as basic all DID cases, cases of mixed DID and non-DID, how and when to set up 7-digit and 10-digit Automatic Number Identification (ANI), when to use multiple area and office codes (NPAs and NXXs), and networking-specific requirements (because ESA applies to non-networking and networking environments).

The information in this document is geared to address these, and other, issues, as well as providing functional information about ESA.

Note: For Emergency Services Access on the Survivable Remote Gateway, refer to *Main Office Configuration for Survivable Remote Gateway 50 (NN43001-307)*.

Summary of capabilities provided by ESA

The Emergency Services Access (ESA) feature has been developed to respond to the needs of users who wish to manage emergency calls originating from within their call environment. These needs will depend on a number of factors, such as:

- current legislation in effect

- availability of access to the ALI database
- amount of administration
- the necessary response level for the type and location of the business

Emergency Services Access is flexible enough to be set up in different ways, depending on the requirements. Some examples follow:

- The customer wishes to uniquely identify every phone to the PSAP, either because effective legislation requires it or he wishes to do so for other reasons. The ability of the ESA feature to provide precise location data for an emergency caller (by provisioning location-based data fields against all connected telephone clients) enables the unique identification of phones to the PSAP when an emergency call is made.

This unique identification of individual DID phones requires that each DID phone have an accurate and up to date entry in the ALI database at the PSAP and further requires that the customer make ongoing updates to the ALI database every time that a DID phone change is made. Thus, it places heavy demands on the customer's administration staff, and puts the responsibility on them for ensuring that all databases are properly synchronized. It also requires that the ALI database owner permits, and provides facilities for, PBX administrators to access the ALI to make changes.

- The customer wishes outgoing emergency calls from their location to be handled by a local emergency responder - the Emergency Services Access feature can be configured to allow for the local termination of emergency calls as one of its routing options, and to provide detailed caller information to the local emergency responder when an emergency call is made. This scenario can happen in places where there is no legislation requiring every DID phone to be uniquely identified to the PSAP, or where the ALI database owner does not allow access for PBX administrators. There is obviously no non-DID mapping required, and the customer does not need to be sensitive about the quantity or distribution of his DID numbers.

This type of ESA implementation can potentially relieve the customer of a lot of administrative work, as the initial setup is simple and DID phone moves and changes can be made without major concern for ANI translation. However, the customer still needs to ensure that emergency calls made from these phones are configured to route to the appropriate dedicated or shared route.

- Several levels of intermediate approach can also be taken. A typical one would be to assign a single DID number (of an actual phone, or one which is unused) to a specific area on the business premises, such as a building, a floor, a wing, or a group of offices. An example would be 'B2F1T5', for 'Building number two, Floor number 1, Tower number

5' - this would comprise the location information for all phones in that particular area. This relatively small number of DIDs would be registered in the ALI database, and would not normally change (barring major reorganizations or building alterations). All phones within the specified area would be mapped to the corresponding DID number; thus calls from such phones would send the ANI of the DID number, and provide the respective location information. Local Notification would still provide details about the individual caller.

The PSAP and responding emergency team can identify the appropriate building, and so on, and can obtain more details from the customer using the Local Notification arrangements.

- The customer wishes to answer all emergency calls, either on a per-site or a network basis. This involves routing all emergency calls to an internal phone for a local emergency responder (such as a security desk), generally in conjunction with OSN. This configuration is covered later in the document, in the section "[Provisioning an ESA On-Site Notification phone](#)" (page 121).

References to "adjacent DID phones" can mean any of the previous, as required.

The focus of the ESA feature is to provide the following:

- The ability to provision location-based data fields against all connected telephone clients, including IP phones - these new fields allow the association of dynamic location data to every connected telephone client, providing current location information in the event that they make an emergency call. These dynamic location data fields assign location data as an attribute of the device - therefore, an emergency caller's location can be identified by means of the device used to place the call.
- Support for the ability to determine the physical location of telephone clients connected to the enterprise - either an internal Location Information Service (LIS), or an external Discovery Manager (DM) may be used in this capacity. These mechanisms are primarily implemented to allow location determination for IP phone clients (which can be highly mobile within an enterprise environment).
- A special ESA Directory Number access (such as 911) can be defined to access emergency services. This number can be dialed without having to first dial an ESN access code. The system recognizes that the dialed ESA DN is an emergency call, and provides special treatment. ESA has the capability of recognizing multiple configured Directory Numbers within a single enterprise environment.
- Functionality for a VO logged in phone that has dialed the Emergency Services Directory Number (ESDN) to be redirected back to its Host Call Server (where the emergency call can be handled using static TN data).

- Ability to route the emergency call to special trunks designated to handle ESA calls (either dedicated to handle only ESA calls, or shared to handle other types of calls as well). ESA also provides the capability to define alternate emergency call routes (by means of the Route List Indexing (RLI) architecture) and to define local terminations of emergency calls to an emergency responder within the enterprise.
- Flexible ANI number translation for non-DID numbers (and for DID numbers, if desired by the customer) - the ANI of the station making the emergency call is passed on to the PSAP, which can use it to determine the location of the emergency caller. ESA performs ANI number translation by means of either a statically configured Emergency Location Identification Number (ELIN) or a dynamically assigned Dynamic ELIN for phones that cannot use their DID number as their CLID. This feature applies to both IP and non IP phones.
- Support for the use of a Misdial Prevention feature, which provides system administrators the ability to recognize and block a call that might otherwise appear to be an ESA call. That is, if a call is dialed that includes digits which are the same as a configured ESDN, ESA Misdial Prevention recognizes those digits as being part of a larger dialed number and prevents an unintentional emergency call from being made.
- Support for a networking environment, that is, where the ESA call is originated on one node, and then routed across the network to another node for onward routing into the Public Network and the PSAP.
- On-Site Notification (OSN), so that the customer's staff know that an ESA call is in progress. The generated OSN information reflects specific location data for the emergency caller, based on their configured ERL.

Background information

Passing emergency caller information to the PSAP

When an emergency call is made, it is routed to a Public Safety Answering Point (PSAP) which responds to the call in a fashion appropriate to the nature of the emergency. For the PSAP to do this efficiently, it needs to be able to determine, as specifically as possible, the physical location of the emergency caller - this is accomplished by an interpretation of the caller information that is passed automatically to the PSAP at the time of the emergency call.

The only caller information passed on to the PSAP is the CLID (ANI) of the caller. The PSAP determines the location of the emergency caller by cross referencing the CLID against its Automatic Location Information (ALI) database, which brings up an ALI record containing a location description for that specific incoming CLID. The PSAP can also use the CLID to make

a call back to the emergency caller or another phone listed at the same location as the caller – this is useful if the caller cannot speak or if the call gets disconnected.

Because records in the PSAP ALI database are not updated in real time, the CLID must be provisioned before an emergency call is made. Therefore, it is required that the CLIDs for all potential emergency locations be preconfigured by the system administrator at the caller's location.

Routing to correct PSAP vs. delivering suitable ANI

Generally speaking, it is much better to route a call to an incorrect PSAP for the emergency caller than to not route to a PSAP at all, as the choice in this case is to either handle an emergency call (albeit less correctly) or to not handle it at all.

In the theoretical event, however, that a choice must be made between:

- routing an emergency call to the most correct PSAP (for the location of the caller) at the expense of the accuracy of the CLID information, or
- routing an emergency call to the less correct PSAP (for the location of the caller) in favor of preserving the accuracy of the CLID information,

there are several considerations that may be made.

First, if the emergency call is guaranteed to be routed to the most correct PSAP for the caller, then delivering the most accurate CLID is less important. In this case, the first of the two options can be considered as being acceptable.

In selecting the first option, however, the assumption is being made that the emergency caller is capable of communicating with the responding PSAP and can provide details of both the nature of the emergency and their location. If the caller cannot communicate this information, the PSAP (even the correct one) will be unable to accurately determine the location of the caller, as this determination would require a CLID to do so. In addition, should the emergency call be dropped or interrupted before the caller can provide this information, the PSAP cannot perform a callback either to the caller directly or to another phone at the same location.

Another consideration to be made when selecting the first option is that, without a correct CLID, it may not be possible to route to the correct PSAP or even any PSAP at all. For example, if the call must pass through a Selective Router before being sent to the PSAP, then a CLID is required to do so.

The argument for choosing the second option would be that if routing to the correct PSAP cannot be guaranteed then the CLID must be preserved to assure an effective emergency response from the PSAP responding to the

call. Also, if an entirely accurate CLID is provided to the responding PSAP, it would not matter if the caller cannot speak or if the call is disconnected, as the PSAP can determine the emergency caller's location using the CLID and perform a callback. Lastly, if there is a CLID to work from, there would be no issues with routing through a Selective Router, as the Selective Router can apply default routing to the emergency call. In short, if the location can be determined by the PSAP using a complete CLID, then routing to the most correct PSAP is not necessarily required.

In summary, it would seem reasonable to say that the emphasis should be placed on preserving the accuracy and completeness of the CLID rather than on simply routing to the most correct PSAP. A complete and accurate CLID can be used by any responding PSAP to determine the location of the caller, and provides a workaround for the possibility that the caller cannot communicate this information on their own.

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. **ALI:** 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 (per 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 managed - this is similar to existing processes used for managing CLID for groups of phones.

Enterprise wide mobility

Enterprise wide mobility is defined as being the ability of a telephone client (especially IP telephone clients) to change locations within an enterprise environment, from one Call Server to another, and is supported if every call server in the enterprise is configured with every defined ERL for the enterprise.

The Emergency Services Access feature is nodal in operational nature, and is not a network application. That is, ESA calls are not handled according to a central entity - each individual call server in the enterprise manages its own table of ERL references. As a result, each individual call server must be configured with the information required to effectively process emergency calls made by phones provisioned on every other call server within the enterprise.

The required information includes:

- knowledge of appropriate emergency call handling, or of where to send the call to be handled
- the ability to send the correct digits to satisfy the trunk far end (Central Office or tandem)
- knowledge of all other enterprise emergency areas (or the ability to provide default treatment for emergency calls routed from unknown areas).

For branch offices (SBO or SRG), the configuration of network wide data (ERL tables, for example) is not required, as IP phones only register to a branch office in a survival or local mode scenario, and in this case ESA calls can be routed using the basic ESA routing data configured at the branch office in the basic ESA Data Block (LD 24).

Also note that bandwidth management is not enterprise wide - the bandwidth zone of an IP phone is not automatically updated by Emergency Services Access. As a result, the bandwidth zone of an IP phone does not reflect changes in its location. Instead, the location-based emergency zone parameter, ERL, is used to identify changes of zone by a mobile IP client.

Data centralization

Emergency Services Access is nodal in operational nature. That is, ESA configuration data exists on each individual call server rather than on a centralized server.

It is still possible to use a centralized data repository (Common Nortel Database (CND), for example), and converge the administration of the following data:

- DHCP
- Subnet definitions
- ELINs (ALI management)
- ERL definitions

Although it is possible to centralize network wide ESA data (such as emergency routing / CLID data), this data must still exist on each call server because ideally there should not be a separate server in the critical path of an emergency call.

The solution is for every call server to maintain a local ERL table - this table could be synchronized with a central database in the future (although currently Call Server handling differences are allowed).

Location based handling of emergency calls

ESA divides an enterprise call environment into emergency zones (or emergency areas) for the purpose of more easily identifying the location of an emergency caller – the more zones an enterprise is divided into, the greater the location granularity provided and the more specifically the location of an emergency caller can be narrowed down.

More specific locations (such as a desk number) are assigned an ECL number, and more general locations (such as a floor number) are assigned an ERL number. Both ERL and ECL can be configured to contain any number of telephones, however, regardless of the size of the area being defined. In addition, due to the fact that every ERL table also contains ECS parameters, an ECL can be defined as a subdivision of location within an ERL - this provides both an additional layer of location information and also ease of management for a system administrator configuring the location parameters.

The ability of an ERL table to layer ECL location data within itself is useful in cases where an ECL location is found to be invalid - in this case, it would still be possible to determine an emergency caller's location by their defined ERL.

ERL and ECL are both used in constructing the ALI Record used at the PSAP in determining the physical location of a phone placing an emergency call. For more information, see ["The ALI Record" \(page 25\)](#).

Determination of caller location using ECL and ERL

A DID phone is assigned an ECL that identifies its location at a specific desk. If the DID phone has been moved from its originally provisioned location, however, (as specified by its originally assigned ECL) then the ECL is not valid, as it does not accurately reflect the true location of the phone. With ECL location data configured within a defined ERL, however, the location of the DID phone can still be determined (although it is less specific than that provided by a valid ECL).

When an enterprise environment is divided into emergency zones, each zone must be recognized network wide for location management to be effective. In other words, to achieve full network wide mobility for connected IP telephony clients, an emergency zone that has been defined on one call server in the enterprise must also be defined on every other call server in the enterprise. This enables an IP client to move from one zone to another throughout the entire enterprise environment and yet not lose the ability to have location information assigned (even as it moves between zones).

All phones in a given emergency zone receive the same emergency service treatment as defined for that location, even if a phone is a mobile IP client visiting that particular emergency zone (and their home call server is deemed to be remote from their current location). When a mobile IP phone makes an emergency call from a zone other than their originally provisioned zone, the emergency call is routed from their home call server to a call server or gateway local to the visited emergency zone. At this point, the call server in the visited zone can provide the appropriate emergency call handling service for that location.

An IP client visiting a zone other than the one on which it was originally defined must still dial the ESDN of its home call server to place an emergency call - this is the case even if the ESDN of their home emergency zone is different than that of the zone being visited.

A call server determined to be within the home ERL of the emergency caller can use the ESA parameters in the Basic ESA Data Block (LD 24) to route an emergency call; that is, the local ERL routing parameters in LD 117 (the ERL table) may be left blank and the call will still be routed as an emergency call so long as it is made within the home ERL.

A call server determined to be a remote ERL to the emergency caller must use the LD 117 (ERL table) routing parameters to reach a distant PSAP, either by a tandem route to a gateway in the area local to the PSAP or by routing through the PSTN using the PSAP public telephone number. An exception to this would be if the PSTN has an E911 Tandem and Selective Router - in this case, it may be possible to route to a remote PSAP based on the caller's ELIN, for which LD 24 parameters still suffice. However, E911 Tandems normally serve a limited geographical area, so this method cannot necessarily be used for every remote ERL.

Location granularity

Location granularity is defined as being the extent to which the physical location of a phone device can be specifically determined. The requirements for the level of location granularity on a PBX is a state legal matter – no standards currently exist. At present, there are location granularity laws in place that require the ability to locate an emergency caller within a 40000 square foot area (approximately 1 floor of large office building) or less.

Subnet mapping can provide a location granularity of 40000 square feet or better (the actual resolution achieved would depend on the network topology in place at the location). By using subnets to define location, for example, a single subnet could correspond to a floor, and several subnets could correspond to a building. A subnet created on a wireless network should have a location description that is more general, however, as it is a standard procedure to install WLAN access points on the same subnet.

Port mapping can provide a location resolution down to an RJ-45 wall jack – to specify an office or a cubicle, for example. If network hubs are used on the network, however, port mapping only identifies the L2 port to which they are connected. In the case of port mapping on WLAN, the location resolution can be scaled down to the area serviced by the closest access point to the device making the call.

The smallest unit of location resolution is a defined ECL (as in port mapping to an RJ-45 wall jack).

Location granularity for WLAN E911

If an internal LIS (Subnet Lookup Table) is being used within a WLAN environment, then an IP phone can only be located to a site (because all access points at the site are on the same subnet). Thus, the ERL location definition for the WLAN subnet (and the corresponding ALI record) should specify the location down to the site only and no further.

If using a port mapping LIS (an DM, for example), then a phone can only be located to the nearest wireless access point (which is the access point to which it connects to place the call). The achievable location resolution for WLAN E911 depends on the actual wireless technology in use and on the way that technology is deployed.

It is possible that the nearest access point to the caller is on another floor. The location description for the access point should take this into account, by specifying in the description that it is a wireless access point, for example.

A port mapping LIS recognizes mobility between wireless access points, so when an IP client roams between them, it results in a location update for the phone to the new nearest access point.

Residential vs. PBX services

ESA is primarily designed to provide a means of implementing (within an enterprise PBX environment) the type of emergency call handling service currently offered by residential (Private) 911 service.

When a call is made from a phone located on a PBX, the issue is more complex than with a residential call. Many PBXs only send the main Listed Directory Number (LDN) for the business - if the emergency caller cannot speak coherently, the PSAP operator can only dispatch assistance to the main entrance. When there, the guard or receptionist may be unaware that a 911 call has been made, and unaware of the exact site of the emergency.

Even for cases where the caller's full seven or 10-digit DID number can be sent with the call by the PBX, there is generally no entry in the ALI database information corresponding to the exact location of the caller (within a building), only the main business address. To date, there has not been a requirement for PBX owners to provide ALI database updates every time an internal phone move is made.

The solution is provided by a Private 911 service (such as Emergency Services Access feature). A Private 911 service sends out a unique number (ANI) with every call, which will identify the calling station by means of an ALI lookup - generally, this is done by prefixing the Directory Number (DN) of the phone by the specified three-digit office code (NXX). For DID numbers, this gives a unique seven-digit phone number that the PSAP can use to determine location. In addition, ALI database updates must be made corresponding to PBX service changes, so that all of the possible ANI combinations have valid and current ALI information available to the PSAP.

Non-DID DNs and number translation

Non-DID numbers pose a problem, because they cannot deliver an outgoing number to the PSAP: It is not valid to make a seven-digit number by prefixing the DN with the NXX (it is required that any Private 911 system send out only ANI numbers that are Part of the North American Numbering Plan (NANP), and that are valid DID numbers assigned to the customer by the serving Telco.)

For example, A PBX has an office code (NXX) of 962, and a DID range of 5000–5999. A phone within this DID range, for example, 5500, forms a Calling Number of 962-5500, which is valid and unique.

A non-DID phone, for example, DN 3000, would form a Calling Number of 962-3000 - because this is outside the DID range of 5000-5999, this number will have most likely been allocated by the phone company to a different subscriber, that could be many miles away from the PBX location.

Thus special arrangements need to be made for non-DID phones within the customer site. Non DID numbers usually have to be mapped to nearby DID numbers for the purposes of 911 calls. This involves some form of translation at the PBX before sending out the ANI.

As an example of non DID number translation, consider extension 3000, which is a non DID number, placing a 911 call. ESA recognizes that the extension is a non DID station and checks its translation table for the valid DID number to assign to the call. In this case extension 3000 will be replaced with a pre-determined station number of, say, 962-5500, which is a valid DID number (this station is located within the same physical area as extension 3000). The translated number, in this case 962-5500, can be used as a call-back number by the PSAP to provide location identification as close as possible to the caller who placed the call.

Note: DID numbers undergo a similar translation process, because they usually have to have their NXX office code prefixed. So, using the same example as previously, if extension 5500 (a DID number) makes a 911 call, ESA will 'translate' this into 962-5500, thus providing a unique North American Numbering Plan number to be used by the PSAP to determine accurate location information.

The capabilities originally provided by the ISDN CLID Enhancements feature are now enhanced to allow a great flexibility in setting up the required translations. (The section "[Digit translation examples](#)" (page 95) provides samples of common types of translations that are likely to be required, and how the customer can set up and use translation tables.)

Note: Although the ESA uses the translation capabilities provided by the ISDN CLID database, the ISDN package is not a prerequisite for

ESA functionality. Refer to "[A note on packaging](#)" (page 34) for more information about packaging and digit translation.

Note that a Private 911 environment requires that the customer deploy sufficient DID numbers so that all locations within the enterprise are close enough to a DID phone to be quickly found by the emergency response team. In the event that the caller could not be coherent about his exact location, the emergency services will arrive at the location of the phone with the DID number used as ANI. The location of any non-DID phones which have been mapped to the DID number must be close enough that the emergency response team can quickly locate the caller. This requirement might mean that additional DID numbers will have to be obtained, or those that are in use may have to be redistributed. This need is not specific to the system, but is of consequence to the concept of Private 911.

Feature description

Without configuration of the Emergency Services Access (ESA) feature, the system provides limited emergency 911 services to its users through the existing Automatic Number Identification (ANI) feature, where the ANI was output for callers dialing the public emergency services phone number (typically 911).

In this case, the use of ANI is limited to systems that use exclusively Direct Inward Dial (DID) numbers. Also, when a caller tries to access a Public Safety Answering Point (PSAP), an ESN Access Code would have to be dialed prior to dialing 911. In addition, this functionality applies only to a non-networking environment, and does not function within a networking environment.

With the introduction of ESA, the system has the capability of providing private 911 emergency services to all its users in both a non-networking and networking environment, on systems using DID and/or non-DID numbers, and without the need to dial an Access Code. Also, a calling terminal identification number can be delivered to the PSAP with the outgoing call.

Generally, the ESA feature functions as follows:

1. A user makes an emergency call by dialing the designated ESA DN (typically, 911) from a station. The system recognizes that this is an emergency call and prepares for special treatment - this involves creating a suitable ANI or Calling Line Identification, and routing the call to a trunk that has been designated to handle ESA calls (this trunk may be dedicated or shared).
2. An on-site alert of the ESA call is then given to a designated OSN phone or terminal. The OSN phone emits a buzzing when an ESA call is detected. This phone is also equipped with an OSN key lamp that flashes in case of an ESA call. By pressing this OSN key, the caller information is displayed on the phone. Also, the caller and calling

number information is created and printed on a designated display terminal as soon as the ESA call terminates onto an outgoing trunk.

3. The ESA call is then routed to a PSAP, or routed back to the system to be handled internally, depending on the particular ESA configuration for call handling.

There are five major components of ESA that provide the functionality described previously:

1. With 'ESA Location Management', it is possible to determine current location information for connected telephony clients, and is the component that enables true client mobility of IP telephony clients within an enterprise environment. That is, Location Management is the ESA component that enables effective emergency call handling for mobile clients - it is the concept that enables an IP client to make an emergency call using specific location data, and it encompasses any associated data fields and processing that enables this functionality.

The location information for a specific telephone client is used by ESA in its composition of calling numbers, in routing emergency calls appropriately to the correct PSAP or emergency responder, and in providing specific caller information for display on an OSN phone.

ESA Location Management occurs on an ongoing basis before an emergency call is made, and thus operates asynchronously with the remaining four ESA components.

2. With 'ESA Call Recognition' an Emergency Services Access DN (such as 911) can be configured on the system. When a caller dials the ESA DN (there is no need to first dial an Access Code), the system automatically recognizes the call as an Emergency Services Access call and sets up special treatment.
3. With 'ESA Call Routing' outgoing trunk routes may be designated to handle ESA calls. Available routing methods include a method based on Route List Index (RLI) architecture.
4. With 'ESA Calling Terminal Identification' the system composes an ESA calling number for outgoing ESA calls.
5. With On-Site Notification, a system output device (such as a terminal or a phone) may be configured to provide an on-site alerting capability for ESA calls. The last two capabilities allow emergency and security personnel to respond more promptly in the event of an ESA call.

These five components are described in detail in subsequent sections of this document.

A note about packaging

ESA is comprised of three different packages, which must be implemented separately (as defined in the section ["Feature implementation" \(page 179\)](#)), depending on the functionality that a customer desires.

The ESA package 329 provides ESA Call Recognition and ESA Call Routing. It also provides basic number translation, such as the addition of NXX and NPA (area and office) codes, but not non-DID to DID translation (this is provided by the ESA_CLMP package.) The ESA_SUPP package provides supplementary capabilities, such as networking capabilities (for example, incoming ISDN to CAMA number conversions), and about-Site Notification. The ESA_CLMP package provides translation of non-DID to DID numbers. Refer to the section ["Feature packaging" \(page 177\)](#) for more information.

A note about the Flexible Numbering Plan and ESA

Throughout this document, when examples are provided pertaining to Automatic Number Identification (ANI) which is being generated for ESA calls, the composed numbers are given to be either 7 or 10 digits in length. This assumes that the Flexible Numbering Plan (FNP) is not equipped on the system along with ESA. However, if FNP is equipped, then the ANI can be any length, up to a maximum of 16 digits. Refer to [Table 7 "Valid ESA calling number lengths" \(page 79\)](#) for an explanation of valid lengths for ESA calling number composition.

This also applies in cases where ISDN trunks are involved. However, because CAMA trunks are North-American specific, the ANI can only be 7 or 10 digits long.

Standards compliance

This feature is designed in accordance with the following standards:

- ANSI/T1.411-1995. "Interface between carriers and customer installations - analog voice-grade Enhanced 911 switched access using network-provided reverse-battery signaling." This standard describes CAMA signaling on analog CAMA trunks, but the same signaling is also used by this feature for digital CAMA trunks.
ISDN signaling uses standard ISDN CLID protocols.
- ANSI TIA/EIA 689. "PBX and KTS Support of Enhanced 911 Emergency Service Calling." This standard has been approved, but not yet printed and published, and is a supplement to ANSI EIA/TIA 464B-1995, the standard for PBX switching equipment.

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 port mapping 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).

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. Communication between the DM and the call servers is accomplished by means of the Zone Manager interface, which is used by the DM to query and update system data.

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 also contains 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" \(page 25\)](#).

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.

Only one ALI Manager may be configured per enterprise network - the ALI Manager can update multiple Call Servers using a common interface to query and update system data.

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 good idea 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.

Location management

Location Management is one of the central and driving components of the ESA feature, as it is the component that enables for unique location identifiers to be assigned to individual telephone devices within an enterprise network. Location Management is the functionality of ESA that provides support of emergency call handling for mobile telephone clients, most especially in the case of the client mobility associated with IP phones.

IP Phone clients present a unique challenge to the effective delivery of emergency call treatment, as they are subject to location ambiguity - IP phones are not required to be installed using static port assignments, and can connect to a call server from any active network port within an enterprise. For this reason, they are easily relocated within the network environment - the resulting challenge is that the specific current location of

a mobile IP Phone client cannot be assumed to remain constant, and this interferes with the delivery of efficient emergency call handling to these clients.

ESA Location Management provides a solution to this unique challenge, by providing the means to determine the current location of a connected IP phone device. This, in turn, enables effective emergency call treatment to be delivered to those clients, because their location can be determined in the event of an emergency call (regardless of possible client mobility). ESA Location Management, therefore, is the concept that enables a mobile IP phone client to make an emergency call using up to date location data, and it encompasses any associated data fields and processing that enables this functionality.

The necessity and challenge of determining current location applies only to IP phones - non-IP telephones also have a location-based data field assigned to them, but the values for these are static (as non-IP telephones are generally installed at a specific location and do not move, meaning that their current location remains constant). Non-IP telephones, therefore, are not subject to the same location ambiguity as IP phones, and do not require their current location to be determined.

Location management is separate from ESA call processing – it simply extends ESA call processing to IP phone clients by allowing those clients to make an ESA call using accurate and current location data. The Location Management functionality operates asynchronously with regular ESA call processing to determine and maintain current location data which ESA call processing requires for its effective operation.

The location-specific data parameters used by ESA to uniquely identify a specific device are **ERL** and **ECL**. These are described as follows:

Emergency Response Location (ERL)

Stored in the TNB, the ERL data field contains a value (within the range of 0 to 65535) that corresponds to a general location description for a telephone device. The ERL value points to an entry in the ERL table, and is used to determine the appropriate PSAP routing for an emergency call made from a specific telephone device. The ERL parameter can (optionally) be used in ELIN assignment for the telephone device to which it is associated.

If no Location Information Service (LIS) is configured on the network, a system message is printed to this effect.

By default, the ERL data field has a value of **zero**.

When the ERL value is zero:

- Indicates the phone is set to Auto Update.

- It is interpreted to mean that, in the case of an emergency call, the emergency route information to be used is that which is defined in the Basic ESA Data Block (LD 24).
- The ESA CLID for the phone is either defined in the TN Block (CLID table) or by the Default CLID (DFCL) as configured in the ESA Data Block (LD 24).
- If the Needs Update flag is set, it is interpreted to mean the phone is “not yet located”.
- If the Needs Update flag is clear, it is interpreted as meaning that the phone “could not be located”. This means that the LIS could not locate the phone device in its queries.

If the value configured for this data field does not point to a valid entry in the ERL Table, then the value is rejected.

The ERL is prompted when adding or changing a TN, and is displayed when the TN data is printed.

Note: ERL is only printed 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.

Emergency Caller Location (ECL)

The Emergency Caller Location (ECL) contains a value (within the range of 0 to 65535) that corresponds to a specific location, such as an office or desk.

The ECL value of a specific DID must be managed along with the ALI record associated with that specific DID.

The ECL value is used to define the specific location of a specific DID phone - by comparing the current ECL value of the phone (which is dynamically assigned by the Subnet LIS) with its home ECL value (which is manually provisioned by the system administrator in the phone's TN Block), it is possible to determine whether or not the phone is at its originally provisioned location (as specified in the ALI database).

If the Current ECL and Home ECL values are the same, then the DID phone is known to be at its originally provisioned location. The result of this evaluation determines whether or not the DID phone number can be used as the ESA CLID for that specific telephone device - if the Home and Current ECL values do not match, the DID phone number will not be used as the ESA CLID of the phone when making an emergency call, and the phone would be assigned a CLID based on the more generalized location descriptor of the ERL value.

ECL can be configured for Manual Update phones, but the value entered does not apply - this is due to the fact that, by definition, they are always at a static location (where they were originally provisioned).

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

The default value of the ECL data field is **zero**.

Note: ECL is only printed 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.

Architecture

The architecture and operational concepts of the Location Management functionality are described in the following sections:

Location as a device attribute

Location Management is concerned with providing accurate and specific location data for connected telephone devices. Therefore, a key to its functionality is the concept that location data is assigned as an attribute of the device itself.

Determining and maintaining the current location data for an IP phone client requires that updates to the location attributes of the device be made on an ongoing and consistent basis, to counter possible changes in location due to client mobility. As such, the current location data for an IP phone is stored in its registration record (in the Resource Locator Module table).

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

1. The location data is statically configured by the system administrator in the TN Block - that is, the location data is manually provisioned (which means that the IP phone is set to Manual Update).
2. The location data is determined and assigned by means of the Internal LIS (using a subnet lookup table): Current location data is dynamically determined when the IP phone registers itself on the network (which means that the IP phone is set to Auto Update). The location update process for a newly connected phone is delayed until background processing runs, as this process only occurs during idle system cycles.
3. The location data is determined by means of a DM: The current location of an IP phone is dynamically determined when the initial connection is made, even before registration with the Call Server (which means that the IP phone is set to Auto Update). Therefore, location determination for an IP phone using a DM enables for the location management of IP

phones that are connected but not registered (VO logged out phones, for example).

After the current location data of the IP phone device is determined and updated by one of these methods, ESA call processing uses the operational location data it can now find in the TN Table (in the event that an emergency call is made).

Except in the case of a statically configured TN, location data is not stored persistently for an IP phone – the LIS dynamically provides the necessary location data, as follows:

- If previous location data is cached on the IP phone device, it is used until a location update is available. Otherwise, location fields are initialized to “unknown” values. Telephone devices deemed to have an unknown location receive the default ESA treatment, as defined in the Basic ESA Data Block (LD 24).
- If an LIS is not configured or is not available, then the location data of the IP phone is not updated.

IP Line application

The IP Line application is an internal software component of the Signaling Server that handles initial IP phone connections. The IP Line application is required to provide an interface to the optional external DM.

Home Location data in the TN Block (TNB)

The location-based data fields found in the TN Block (TNB) contain static values provisioned by the system administrator (or, optionally, by the ALI Manager) to describe the Home (originally provisioned) location of a telephone device.

The data values in the TNB do not reflect the current location values for a mobile IP phone, as these are dynamically determined and updated to the TN Table. Location Management never updates the static values of the TNB – any changes in the location of the telephone device are updated only to the dynamic TN Table.

The data fields in the TN Block are described by the following:

Station designator (DES)

- Is a data field that contains static data that can be used to provide a text-based description of the physical location of the telephone device.
- Can be used by Office Data Administration System (ODAS) to represent location.
- Printed on the On-Site Notification (OSN) phone and in the OSN record in the event that an emergency call is placed.

ERL

For more information, see ["Emergency Response Location \(ERL\)" \(page 38\)](#).

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 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 VO login is made on a Manual Update TN, the IP Phone used is treated as Auto Update.

ECL

For more information, see ["Emergency Caller Location \(ECL\)" \(page 39\)](#).

Storing location data in the TN Table

Location-based data fields in the TN Table contain current values, meaning that they are dynamically updated to reflect changes in the current location of a phone device as it changes location throughout the enterprise.

Static (provisioned) values are stored in the TN Block. See ["Home Location data in the TN Block \(TNB\)" \(page 41\)](#).

The data fields in the TN Table are described as follows:

ERL

For a phone device set to Auto Update, the value in the ERL data field of the TN Table is dynamically determined and assigned by the LIS.

For a phone device that is set to Manual Update, the ERL value in the TN Table is copied from the ERL field of the TN Block, to reflect a static (provisioned) location.

IP phones in a specific ERL can be queried through the TN Table, provided that they have a TN Table entry. The TN Table only reflects current location data, and so the IP phone must be either:

- currently registered on the network, or

- have been unregistered since the last system restart (only as long as their TN has not been reused by another device in the time since they unregistered).

ECL

For a phone device set to Auto Update, the value in the ECL data field of the TN Table is dynamically determined and assigned by the LIS.

For a phone device set to Manual Update, the value in the ECL data field of the TN Table is copied from the TN Block to reflect a static (provisioned) location.

IP phones in a specific ECL can be queried through the TN Table, provided that they have a TN Table entry. The TN Table only reflects current location data, and so the IP phone must be either:

- currently registered on the network, or
- have been unregistered since the last system restart (only as long as their TN has not been reused by another device in the time since they unregistered).

Location description

For a phone device set to Auto Update, the value of the Location Description data field in the TN Table is dynamically determined and assigned by the LIS.

For a phone device set to Manual Update, the value of the Location Description data field in the TN Table is copied from the ERL table.

When printed as part of the OSN record, the Location Description appears as **LOC**.

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 LIS

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

- Current ERL
- Current ECL
- Location description

Storing location data in the IP Line application

The IP Line application contains a copy of the current location data, as represented in the TN Table - subsequent updates to the location data on the occur asynchronously with phone registrations.

If the IP phone is not registered on the network, The IP Line application is the master copy of location data, as the TN Table reflects the location data of the phone for the last time it was registered.

If the IP phone is registered, the IP Line application and the TN Table are synchronized so that they reflect the same location data for the registered phone.

If the IP phone registers on the network and the TN is set to Manual Update, then the location data is defined by the entries provisioned for the phone in the TNB. If the phone then unregisters, the Manual Update flag persists on the IP Line application, as the location data is static and will not change when the phone registers again.

If the phone connects but does not register, the location data for the phone is as it is defined by the DM (if there is one). If there is no DM configured on the network, then the location of the phone remains unknown until it is registered.

Location data can be queried from the IP Line application.

Storing location data in the IP Phone

Some IP phone models can cache location data - this is useful in survivability scenarios and in the case of IP phones deployed in a Virtual Office (VO) environment.

Location data stored on an IP phone is a copy of the current location data, synchronized with the IP Line application – the IP phone device caches the location data in its DRAM (scratchpad memory), which is erased if the device is powered down.

If an IP phone can cache its location data, the cached location data is used in new phone registrations until a location update can be performed (the Needs Update flag will have been made active during this time, as no location update was done since registration).

Location data stored on the IP phone can be queried.

Selecting an LIS

A prompt in the system Config Record is used to specify which LIS configured on the network is to be used for location determination.

To configure the Subnet LIS, the ESA_SUBNET_LIS package (336) must be unrestricted.

To configure the external DM, the ESA_EXTERNAL_DM package (337) must be unrestricted.

If LIS=NONE, the system administrator should manually provision a value for the ERL of the IP phone - otherwise the location of the phone would be "unknown", as it will not be determined by an LIS. Also, if LIS=NONE all Auto Update IP phones will have their Needs Update flag set and a system message (OSN003) is generated during an emergency call to indicate that the location is unknown.

If the LIS is set to EXT/DM then an indication is being made that a DM will provide location updates. A DM is therefore required to be configured on the network - otherwise, all Auto Update IP phones will have their Needs Update flag set and a system message (OSN003) is generated during an emergency call to indicate that the location is unknown.

Use case: Subnet LIS

This following use case provides a functional description of IP Phones set to have their current location data assigned by the Subnet LIS. Included is a description of the effective architecture of this configuration.

A TN set to Auto Update is deemed to be at an unknown location until the Subnet LIS locates the phone during background processing. An exception to this is if there is cached location data that is stored on and read from the connecting IP phone itself.

Registration When an IP phone registers to an Auto Update TN, it uses the Subnet LIS to obtain its location information. This location data may be cached in the memory of the IP Phone or not, depending on the specific capabilities of the IP Phone model.

Location update

An IP phone that is mobile and using the Subnet LIS requires that the IP phone acquire a new IP address every time it moves to a new emergency zone in the enterprise. This requires the IP phone to reconnect and reregister whenever it moves from one emergency zone to another, in the same fashion as it would for a new registration.

Configuration changes

A change to the Subnet LIS configuration may cause a location update, which operates as follows:

1. For every TN impacted by the changes to the Subnet table, the Needs Update flag is set in the TN Table.
2. Later (during the ESA background locate), the Subnet LIS provides a location data update to the TN Table, in the ERL, ECL, and Location Description data fields.
3. The location data is synchronized to the IP Line application.
4. The IP Line application synchronizes the location data to the IP phone, which may be cached or not, depending on the capabilities of the IP phone.

Use case: Discovery Manager

This following use case provides a functional description of IP Phones set to have their current location data assigned by the DM. Included is a description of the effective architecture of this configuration.

If the DM is not available (For example, if the network is down, or the DM server is down) and an IP phone has moved, then no location updates are available for the IP phone at its new current location. In this case:

- Current operation location data is used (may be an unknown location or the last-known location of the IP Phone).
- ESA call processing generates a message that the location required updating.

If the DM does not receive registration traps (SNMP) which notify it of IP phone registrations, it still discovers phones that need a location update by means of its periodic query for those phones.

A TN that is set to Auto Update is deemed to be at an unknown location until a location update for that phone occurs - an exception to this is if there is cached location data that is stored on and read from the connecting IP phone itself.

Registration

In this Use Case, when an IP phone registers to an Auto Update TN, it uses the DM to obtain its location information. This location data may be cached in the memory of the IP Phone or not, depending on the specific capabilities of the IP Phone model.

Location update

A location update from the DM operates as follows:

1. The DM determines the current location data for the registered IP phone and copies it to the IP Line application.
2. The IP Line application synchronizes the newly current location data to the ERL, ECL, and Location Description data fields of the TN Table.
3. The IP Line application synchronizes the location data to the IP phone, which may be cached or not, depending on the capabilities of the IP phone.

Configuration changes

A configuration change to the location data on the DM may result in a forced location update. This operates in the same way as a normal location update.

Tracking IP phone mobility

The DM maintains current IP phone location in the TN Table (subject to a short delay between each location change). Thus, the system administrator can, at any time, determine the current location of any registered IP phone for which the DM provides location management.

While the current location of an IP Phone can be queried, however, there is no provision for the explicit (constant) tracking of IP phones on the network.

Location reporting

This section discusses location reporting for IP phones.

Location data in TNB

The location data in the TNB only applies to an IP phone set to Manual Update, but may be printed in the same way as other TN data, using LD 20.

LD 20 can be used to create a printout of the following TNB location data:

- Current ERL: Prints either the manually provisioned ERL value (for an IP phone set to Manual Update), or a blank value (if the IP phone was set to Auto Update, in which case the current ERL is found in the TN Table).
- Current ECL

Note: ERL and ECL are only printed if the ESA package (329) is unrestricted, regardless of whether an ESA data block configured.

Location data in LD 81

LD 81 generates a list or count of the IP phones matching the feature filters used with the query, by searching current data entries in the TN Table. The available feature filters are as follows:

- ERL: Lists or counts currently registered IP phones by their current ERL entries in the TN Table.
- ECL: Lists or counts currently registered IP phones by their current ECL entries in the TN Table.
- MANU: Lists or counts currently registered IP phones that are set to Manual Update.

LD 81 can use multiple feature filters concurrently to list or count the IP phones matching all filters chosen.

Because ERL values can be configured for Attendants or BRI set types, LD 81 includes Attendants and BRI sets when searching with the ERL feature filter.

The List (LST) command:

- Because DES configuration does not exist for an Attendant set, the DES field in the LD 81 output is always blank for Attendants.

The Count (CNT) command:

- The CNT header in the LD 81 output includes “ATT” and “BRI” for Attendants and BRI sets.
- The CNT header is common for all the CNT outputs, but if the feature filter used is not ERL then the count values are zero.

Note: The LD 81 List and Count commands are only available if the ESA package (329) is unrestricted.

LST/CNT by ERL The LST/CNT commands found in LD 81 include the functionality of listing or counting phones by their ERL values. Because these commands search the TNB, they only list manually provisioned ERL

information. Therefore, the LST/CNT commands are meant to be used primarily with Manual Update IP phones (and non IP telephones, which are configured at a static location).

An IP phone set to Auto Update does not have a manually provisioned ERL, and so the value contained in the ERL data field of the TNB is effectively zero. However, a TN set to Auto Update has its internal flag "Manual Update" clear (false), and so will not be reported when the LST/CNT commands are used.

The LST / CNT ERL commands can be made to apply to:

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

Current ERL data is stored in TN Table, and is not subject to the LST/CNT command functionality.

The output generated by the LST report includes the following:

- 'ERL' keyword
- Customer number
- Prime DN
- Emergency Response Location number
- Terminal Number
- Set type
- DES
- Date of last Service Change

LST/CNT by ECL The LST/CNT commands can be used to list or count phones by their ECL values. Because these commands search the TN blocks, they only list Home (provisioned) ECL values, as opposed to the Current ECL values (which are located in the TN Table). The home ECL field applies to IP phones only, as non-IP phones are manually configured with an ERL value for a static location (which provides more specific location information than the ECL value).

The LST / CNT ECL commands can be made to apply to:

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

The output generated by the LST report includes the following:

- 'ECL' keyword
- Customer number
- Prime DN
- Emergency Caller Location number
- Terminal Number
- Set type
- DES
- Date of last Service Change

LST/CNT IP phones that are MANU The LST/CNT commands can list or count phones set to be Manual Update - that is, they print those IP phone TNs for which the ERL value is statically configured (and the Manual Update flag is true). This command only applies to IP phone TNs.

The output generated by the LST report includes the following:

- 'MANU' keyword
- Customer number
- Prime DN
- Emergency Response Location number (Home ERL)
- Terminal Number
- Set type
- DES
- Date of last Service Change

Location data in LD 83

The Overlay 83 TNB command prints all TN Blocks. ERL and ECL are printed in the TN data, similarly to Overlays 10/11/20.

Location data in TN Table

The following commands print a comprehensive location report - the syntax is similar to the STIP (STAT IP) commands. These commands are executed using the Element Manager interface.

Because these commands search the TN Table, they only list IP phones that have an entry in the TN Table, which includes the following:

- IP phones that are registered.

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

IP Phones that are not yet registered have no TN Table entry. However if the phone is connected to an IP Line application then its location data may be queried on the IP Line application.

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

Note that commands in LD 117 can be abbreviated, as long as they still uniquely identify the command. For example, an administrator can shorten the command LOCRIPT MANUALUPDATE to LOC MANU.

If there are no IP phones matching the query then the command returns "No IP Phones found in RLM table".

The preceding table shows a sample LOCRIPT output, where:

- TN: Terminal Number of the IP phone
- Prime DN: Prime DN of the IP phone (Key 0, for example).
- Type: the IP phone type.
- State: Current registration state.
- HWID: Hardware Identifier of the IP phone.
- Signaling IP: the IP address and signal port of the IP phone. If the IP Phone is behind a NAT router, then the Private IP of the phone is printed below the Public IP (as with the currently existing STIP commands).
- 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 the IP phone is Manual Update.
- ND UPD: Indicates whether the IP phone requires a location updating.

Inventory Location Report

To provide a snapshot of the location data of all telephones connected to the enterprise network, in a fashion that is consistent with existing inventory reports, an Inventory Location Report is available.

Location data on IP Line application

Location data can be queried from a IP Line application (SS or VGMC).

Location data from IP phone

Location data can be queried from an IP phone.

Subnet lookup table

The subnet lookup table is an internal LIS. This location determination mechanism assumes that the data network architecture in place is implemented in such a way that it corresponds to geographical features of the enterprise environment. That is, the assumption is made that the subnet distribution for the enterprise is organized in such a way that each subnet describes, for example, floors within a building.

The second assumption being made is that IP addresses are assigned by means of a DHCP server, which is aware of the various subnets, and therefore assigns IP addresses by location. Thus, by performing a reverse DHCP lookup, the subnet of any given IP address can be determined, and the corresponding location deduced. For this to be possible, the subnet lookup table must mirror the enterprise DHCP configuration.

The subnet lookup table contains location data (ERL, ECL, Location Description) for each subnet entry in the enterprise network. Also, the subnet lookup table is not specific to any single call server, which means it can be synchronized to all call servers in the enterprise. For the location data contained in the subnet lookup table to be useful, however, ERL information must first be defined on all systems referenced by the subnet lookup table.

Operation

The subnet lookup table is used to determine the location of an IP phone in the following cases:

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

To detect changes in location for an IP phone client, the movement between defined subnet locations must result in a reregistration of the IP phone. While this is reasonably easy to accomplish for IP phones with a connection, changes in wireless IP phone location cannot be detected in this way, because they stay registered and maintain their IP addresses even as they change their association from one wireless access point to another.

Mobility of an IP phone due to a Virtual Office login is a scenario that is handled by the subnet lookup table, as there is a reregistration of the IP Phone every time a new login is processed.

The subnet lookup table determines the location of an IP phone by using its IP address as a search key - the IP address of the IP phone identifies which subnet location the phone is currently registered with.

When the subnet lookup table determines the location of an IP phone using its IP address, the location data from the subnet table is copied into the TN Table record for that phone. If the subnet lookup table searches for a

phone by IP address and no match is found, special “unknown” values are assigned to the TN Table record for that phone and a system message is generated to inform the system administrator.

The search for a phone by IP address can return matches for multiple subnets (depending on network mask) - subnet entries are stored in the subnet lookup table in such a way that the longest match is returned.

If a subnet lookup table search is done for the IP address 47.11.216.123, a match is returned for 47.11.216.0/24 instead of 47.11.0.0/16.

To verify that a Subnet LIS has been configured correctly, a command enables the administrator to do a test lookup for an IP phone (based on IP address).

Location data

The Subnet LIS is provisioned with location data for all subnets in the enterprise.

The combination of IP address and subnet mask is the address of either a subnet or of a host (a NAT router, for example).

Subnet masks are expressed in CIDR format, and are appended to the IP address. The CIDR format expresses the subnet mask as the number of bits in the IP address, counting from the most significant bit of the first IP address field. A complete IP address consists of 32 bits. Therefore, a typical CIDR format subnet mask is in the range from 9 to 30. For example, 24 bits corresponds to a subnet mask of 255.255.255.0, while 32 bits corresponds to a complete network address for a host.

ECL and ERL are the data fields that contain the current location information for an IP phone.

Location Description corresponds to the geographic area of the subnet. The value in this field is printed as LOC in the OSN record.

Note that a subnet could correspond to a DID phone's ECL (a floor number, for example), while multiple subnets could correspond to an ERL (representing a building number, for example).

VPN subnets may be entered into the subnet lookup table. However, because an IP phone with a VPN IP could be located anywhere in the world, the location data should be set to values indicating the location is unknown, so that default ESA treatment is given in case a VPN based IP phone makes an emergency call.

If the Subnet LIS cannot match an IP address, it returns an error status. A system message is generated to the system administrator, and data indicating an unknown location is assigned to the phone as follows:

- ERL = 0

- ECL = 0
- Location Description = "Unknown"

Alternately, the system administrator has the option to configure a universal fallback subnet, 0.0.0.0/0. Doing this allows for the assignment of particular ERL, ECL, and Location Description values, for an IP phone at an otherwise unknown location.

If an location update is performed for an IP phone at an unknown location, then a system message is generated indicating that the specified phone could not be located and will receive default ESA treatment. The Needs Update flag is cleared (because technically, the location update has occurred).

Under normal circumstances, the Subnet LIS should not assign ERL 0 to a phone.

NAT

A NAT router is used to map multiple private IP addresses to a single public IP address. An IP phone located behind a NAT router therefore 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 the public IP address of a NAT IP phone (the IP address of the NAT router itself), while in other cases it is better to perform a subnet lookup on the private IP address of NAT IP phone (the specific IP address of the IP phone itself). The Subnet LIS offers the option of which IP address to use in performing a subnet lookup for NAT IP phones, depending on the enterprise's NAT subnet distribution.

NAT_PRIV_IP = NO In this scenario, every phone behind the NAT router is assigned location data according to the NAT router's IP address (the public IP address of the NAT IP phone).

The subnet lookup table contains a host entry for the NAT router, which must therefore have a fixed IP address.

The advantage of assigning location data to IP phones in this way is that NAT domains can reuse IP addresses internally (192.168.x.x). That is, the IP phones under one NAT router can have the same private IP addresses assigned as IP phones under another NAT router on the enterprise, as the private IP addresses are not referenced by the subnet lookup table. The subnet lookup table is resolving only to the Public IP addresses of the NAT routers, which is different from one NAT router to the next.

The disadvantage of doing this is that there is a lack of location resolution, because a NAT router might cover a geographical area in the enterprise that is equal to several floors – and, therefore, all IP phones connected through it would only resolve to the same generalized location.

NAT_PRIV_IP = YES In this scenario, every phone behind the NAT router is assigned location data according to its private IP address. This allows for the configuration of different subnets on the NAT domain. The subnet lookup table would contain entries for all the subnets configured on the NAT router. The NAT router IP address (the public IP address of the IP phone) is not looked up by the Subnet LIS, as the NAT IP address would be listed in the subnet lookup table as a host IP to the subnets defined within it.

The advantage of this is that the resolution used in locating an IP phone is down to the subnet level, as it would be for everywhere else in the enterprise.

The disadvantage is that there is a requirement for more IP addresses to be available, as the private IP address of a phone on one NAT router must not be reused anywhere else within the enterprise (NAT domains must not overlap one another by means of the IP addresses contained in each).

Administration

The following sections detail the administration of subnet entries used by the Subnet LIS

Adding a subnet entry Adding a new subnet entry requires the use of the NEW SUBNET command (LD 117).

In adding an entry to the subnet lookup table, all fields are mandatory except the Location Description. If the Location Description is not specified in creating the subnet entry, then an IP Phone's Location Description (in its TN Table record) is retrieved from the ERL table instead.

Error checking is performed when adding a subnet entry, as follows:

- Duplicate subnet must not exist.
- The IP address and network mask specified must match – For example, if 47.11.216.123/24 is used, it returns an error, as this can be interpreted as either 47.11.216.0/24 or 47.11.216.123/32.
- The specified ERL and ECL values must be within the valid range (0-65535) for that data field.
- The ERL value must be fully defined (using LD 117), except in the case where ERL=0.
- The Location Description value entered must be in the form of an alphanumeric string up to 20 characters long. Spaces and punctuation

(except quotation marks and colons) may be used, provided the input is encapsulated in quotation marks.

Subnet entries are stored in the subnet lookup table in a sorted order that enables the return of the longest match, in the case of a multiple match during lookup. Each subnet entry is listed first by IP address and then by network mask.

As part of the NEW SUBNET command to add a new subnet entry, an audit is performed to determine if any currently registered IP phones are impacted by changes resulting from creation of the new subnet.

Deleting a subnet entry Deleting a subnet entry requires the use of the OUT SUBNET command (LD 117).

If an attempt is made to delete a subnet entry that does not exist, then an error message is returned.

As part of the OUT SUBNET command to delete a subnet entry, an audit is performed to determine if any registered IP phones are impacted by the deletion of the subnet.

The OUT SUBNET command reports the number of phones that were impacted by this change, due to the fact that they were currently located in the subnet that was deleted. Also, the corresponding NEW command to undo the deletion is printed.

Changing a subnet entry Making changes to the parameters of a subnet entry requires the use of the CHG SUBNET command (LD 117).

When a subnet entry has been created, only changes to the location fields (ERL, ECL, and Location Description) can be made.

To change the network definition of the subnet entry (IP Address and Mask Bits), the subnet entry must be removed entirely and then added back with the new network definition data.

In making changes to the subnet entry, all mandatory fields must remain defined. Error checking is performed to ensure this is so, as occurs for the NEW SUBNET command.

As part of the CHG SUBNET command, an audit is performed to determine if any registered IP phones are impacted by the changes made to the subnet, due to the fact that they were currently located in the subnet that was changed.

Maintenance

This section discusses the maintenance of subnet record entries.

There are no commands to enable or disable subnet entries. If a subnet entry exists, it is automatically active. Conversely, the only way to disable a subnet entry is to delete the entry entirely from the subnet lookup table.

Testing Subnet LIS To verify the Subnet LIS configuration, the TEST SUBNETLIS diagnostic command enables the system administrator to enter an specific IP address and verify its location mapping in the Subnet LIS. This command finds the best match for the specified IP in the subnet table, and then prints the associated location data for that entry.

If the Subnet LIS does not find a subnet match for the IP address specified, then the command returns “No match for (IP address specified) in Subnet Lookup Table”.

Note that commands in LD 117 can be abbreviated during usage, so long as they still uniquely identify the command. Therefore, for example, an administrator can shorten the command TEST SUBNETLIS to “TEST SUBNET” or even “T S”.

Subnet table changes

Subnet table changes using the NEW, OUT, or CHG SUBNET commands, may impact registered IP phones. As part of these change commands, an audit is performed to determine if any registered IP phones are impacted by the changes made to the subnet entry, due to the fact that they were currently located in the subnet that was changed.

The audit process for each of the Subnet entry change commands is described by the following:

- Adding a subnet table entry (NEW SUBNET):
 - All registered IP phones are compared against the new subnet.
 - Comparisons are done as part of the NEW command.
 - Impacted IP Phones are flagged for subsequent relocation. They may match a better subnet.
- Changing subnet table entries (CHG SUBNET):
 - Changes may only be made to the location data fields (ERL, ECL, and Location Description) of the subnet entry. All registered IP phones must be compared against the changed subnet entries.
 - Comparisons are done as part of the CHG command.
 - Impacted IP phones are flagged for subsequent relocation, by activating their Needs Update flags. Their TN Table location data will

then be updated with the newly entered location data, as reflected by the subnet entry.

- Deleting a subnet table entry (OUT SUBNET):
 - All registered IP phones that matched the old subnet must be relocated.
 - Comparisons can be done as part of the OUT command.
 - Impact IP phones are flagged for subsequent re-location. They may match a more general subnet entry, or their location may become unknown.

Relocation is performed in the background in the same way as a normal subnet lookup, and results in a synchronization message from the TN Table to the IP Line application.

Subnet LIS background processing

The Subnet LIS determines the location of IP phones in the background, during idle system cycles. This applies to both initial location determination, and subsequent relocations due to a subnet table configuration change.

System messages

The System Alarms and messages associated with Subnet LIS are illustrated in the table that follows:

Table 2
System Messages associated with Subnet LIS

Message Number	Severity	Event	Corrective Action	Output
SCH0099	Info	Invalid input		TTY
SCH1628	Info	ESA Subnet LIS package (336) is restricted	Provision the ESA Subnet LIS package (336) before using this feature.	TTY
SCH1631	Info	IP address and network mask do not match	Enter matching IP address and network mask.	TTY
SCH1632	Info	Entry not found in the Subnet table	Cannot reference undefined Subnet entry.	TTY
SCH1633	Info	Duplicate entry	Cannot add duplicate Subnet entry.	TTY

SCH1635	Info	Invalid Location Description	Enter valid Location Description.	TTY
SCH1654	Info	Invalid ECL	Enter valid ECL from 0 to 65535.	TTY
SCH1656	Info	ERL does not exist	Cannot reference undefined ERL.	TTY
SYS0143	Major	Error loading Subnet LIS database	Restore the Subnet database or contact your technical support group.	TTY, RPT, SNMP
ESA011	Minor	IP Phone TN <tn> was assigned unknown location (ERL 0) by Subnet LIS – will use ESA defaults	Consider adding phone's location to Subnet LIS.	TTY, SNMP
ESA012	Minor	IP Phone TN <tn> was not located by Subnet LIS – will use ESA defaults	Correct the Subnet LIS configuration.	TTY, SNMP
SRPT233	Critical	Failed to allocate protected heap memory	Contact your technical support group.	TTY, RPT, SNMP
TEMU019	Major	Error dumping Subnet LIS database	Contact your technical support group.	TTY, RPT, SNMP

System engineering

There is no limit to the number subnet entries that can be made in the subnet lookup table.

Interworking with the DM

This section describes interfacing with the external Discovery Manager (DM) - the DM communicates with the CS 1000 to monitor the connection of IP phones to the network and to update and maintain their operational location data.

Overview

Location data for an IP phone is treated as a device attribute and resides synchronously on the IP Line application and in the TN Table. The DM dynamically updates this location data by connecting to the IP Line application.

This section describes the CS 1000 interface that enables the interworking of the IP Line application with an external DM, which includes:

- The notification of IP phone connection events from the IP Line application to the DM.
- Audit queries made by the DM to the call server.
- Location updates made from the DM to the call server.

Web services interface for the external DM

The Web Service interface for DM utilizes Command Line Interface (CLI) commands on the servers running the IP Line application (Signaling Servers and Voice Gateway Media Cards). The commands are exposed as web methods by the Zone Manager using J2EE Web Services. This enables external clients such as the DM to access the commands in a platform and language independent way.

The Zone Manager web server hosts both the DM Web Services and the associated Web Services Definition Language (WSDL) document which 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 SUN's *wscompile* tool for Java clients. Using the generated client stub code, the DM can access the web methods as if they were local method calls, even though all calls go through the Web Services.

The commands used with the DM are a small portion of the Web Services interface that is exposed by the Zone Manager. Therefore, they benefit from the same security, logging, and other features that the Zone Manager Web Services interface provides for all services.

Connection events and SNMP traps

The DM uses SNMP traps from the IP Line application as its primary method for gathering the necessary information to track the location of an IP phone while it is mobile throughout the enterprise network.

When an IP phone makes its initial connection to the network, it does so by means of the IP Line application. The DM is notified of the IP phone connection event by means of the SNMP trap ITS5008, which is generated by the IP Line application to indicate a successful IP phone connection.

When an IP phone loses its connection to a IP Line application, an SNMP trap (ITS2008) is generated by the IP Line application to notify the DM of this.

Because SNMP traps are transmitted using User Datagram Protocol (UDP), their delivery is not guaranteed. Therefore, the DM performs periodic audits of phone status to ensure that it is aware of any missed IP phone connection events.

The DM only needs to be aware of the most recent connection event for a given IP phone. This handles the case of a Branch User phone initially connecting to the Branch Office IP Line application, then redirecting and reconnecting to the Main Office IP Line application.

Audit queries

The DM must perform periodic audits to ensure synchronization between its list of connected IP phones (for which location management is needed) and the same list of connected IP phones found on the call server. The DM and call server lists can become out of sync due to a missed connection event (an SNMP trap failed to transmit) or a system restart, for example.

To improve the efficiency of the DM queries, and to minimize the amount of data that the DM must audit and synchronize, query functions are provided with the ESA feature.

The DM issues these commands through the Zone Manager web methods. The DM directs these query commands to a particular target IP Line application by including the IP address of the Signaling Server on which the target IP Line application is operating. In this way, the Zone Manager is given the required information to direct the queries to the correct target IP Line application.

These commands report on all IP phones connected to a particular target IP Line application, and includes both registered and unregistered IP phones. An IP phone may be connected to the network and yet remain unregistered for any of the following reasons:

- The IP phone is VO logged out.
- There is an invalid TN configuration for the connected IP phone.
- The connected IP phone is using a duplicated TN configuration.

Query phones that need a location update The DM performs a query to determine which IP phones need location updates by means of the **isetLocNeedUpdateShow** CLI command. This command returns a list of any IP phone that requires a location update, and also their current location data.

Querying phone location data The CLI command **isetLocShow** provides current location data for the specified IP phone or, if none is specified, the current location data for all IP phones currently connected to the IP Line application. The DM uses this command in performing a full audit as it requires.

Location update function

When the DM has determined the current location of an IP phone (after an IP phone connection event), or has performed a location update, it sends location data to the IP Line application using the CLI command **isetLocUpdate**.

This command is not available to system administrators as a usable CLI command - only the DM can access this command function by calling it directly through Web Services.

The DM updates the following location data on the IP Line application:

- Current ERL, which corresponds to the general area of the IP phone (a floor number, for example).
- Current ECL, which corresponds to the specific area of the IP phone (an office or pillar number, for example).
- Location Description, which corresponds to the specific area of the IP phone (as described by the ECL).

The IP Line application validates the location data provided by the DM, confirming that the data conforms to valid format and range, as follows:

- the specified ERL and ECL values must be within the range of 0 to 65535
- the Location Description value must be in the form of an alphanumeric string up to 20 characters long. Spaces and punctuation (except quotation marks and colons) may be used, provided the input is encapsulated in quotation marks.

If the DM does not locate an IP phone then it performs a location update using null values, as shown by the following:

- ERL = 0
- ECL = 0
- Location Description = "Unknown"

If an unknown location update is performed then a system message is generated, indicating that the specified phone could not be located and will receive default ESA treatment.

The Needs Update flag is cleared in the case of an unknown location update (because, technically, the location update has occurred). Under normal circumstances, the DM should not assign ERL 0 to a phone.

If the DM assigns a phone to an undefined ERL, then a system message is generated and the phone is assigned unknown location data. The Needs Update flag is cleared as previously described.

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

Resynchronizations

Resynchronizations between the DM and the call server are required in various failure survivability scenarios.

If the DM is restarted:

- It must rebuild its location database from the time since it was last saved.
- It must perform a full audit on every IP Line application on the enterprise to list all connected IP phones (and their current locations).
- It must send location updates for all IP phones whose location data is out of date.

If the Call Server is restarted (warm or cold):

- If the restart is fast enough, the IP phones stay connected with the IP Line application. If IP phones stay connected to IP Line application (SS or VGMC), the DM keeps locations up to date, and there is no impact.
- If the restart is too lengthy, the IP phones restart – see section to follow.

If the IP Line application (Signaling Server or VGMC) restarts (warm or cold):

- The IP phones connected to it are restarted as well.
- The DM receives SNMP traps for all subsequent IP phone reconnections.
- The periodic query for IP phones that need a location update will update any phones for which the connection event (SNMP trap) is missed.

If IP phones restart:

- The DM receives SNMP traps for all IP phone reconnections.
- The periodic query for IP phones that need a location update will update any phones for which the connection event (SNMP trap) is missed.
- There is no impact due to Active Call Failover (ACF). With this feature, IP phones maintain their speech path, and only reboot when the call ends. After rebooting, IP phones connect to a IP Line application normally.

Login management

The DM communicates with the IP Line application in querying and updating the location data for an IP phone. All commands are made through Web Services in Zone Manager, however – therefore, the DM needs to login to the Zone Manager to execute its commands.

Package protection The CS 1000 must be equipped with the proper packages (ESA External DM package 337) and configuration (LD 17, LIS = EXT or DM) for the DM to establish a session with the Zone Manager and for the call server to accept location updates sent from the DM.

Presence management If a DM is configured but has not connected to the system within a preset time period to perform a location update or a periodic audit, then a system message is generated to indicate a probable fault with either the DM or its connection. This functionality is implemented by using an internal watchdog timer that is reset every time the DM communicates with the system in the form of a location update or a keep alive indicator message.

Also, if the timer is expired and an Auto Update phone makes an emergency call, then an OSN message (OSN003) indicates that the phone needed a location update.

The timeout value must be greater than the audit interval for the DM. For example, if the DM performs an audit every 15 minutes then the timeout value could be set to 20 minutes. This allows some flexibility in accommodating processing delay, yet would ensure that an alarm is generated shortly after the absence of the DM is detected (reducing the time window in which there is no coverage by the DM).

If the DM has not communicated with the call server within the configured time interval, a system message is generated. If the problem persists, then this alarm message is periodically generated at a frequency of two times the configured timeout value.

For example:

If the timeout value is configured at 15 minutes, then the first alarm message is generated 15 minutes from the last time the DM was known to be active. Therefore, an alarm message is generated periodically every 30 minutes, prompting the system administrator to take corrective action.

When the DM has been reconnected (when a DM update is successfully received), a system message is generated to inform the system administrator.

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

The timeout value of this watchdog timer is measured in minutes, and must be within the range of 5 - 1440 minutes. 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 DM timeout alarm. That is, no system alarm message is generated if the DM fails to connect to the system.

As indicated previously, this timeout value should be suitably configured to accommodate the audit interval of the DM (plus a reasonable amount of time to serve as a grace period in the event that system processing time is delayed).

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

System messages for interworking with the external DM

The error category **LIS** is created to inform the DM about errors in its operation. The outputs of the LISxxxx messages are sent to the TTY port.

Table 3
System messages for interworking with the external DM

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 – IP Line application has not been initialized.	Enable IP Line application, or wait until the IP Line application 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

Configuration

Ideally, the system should be configured to send SNMP traps to the DM upon IP phone connection to the IP Line application. Even without the benefit of SNMP traps, however, IP phone discovery still occurs on a delayed basis by means of the periodic audits initiated by the DM.

For the DM to be active on the network, the LIS must be configured to EXTERNAL.

ERL table

ESA configurations defining emergency areas within the enterprise are contained in the Emergency Response Location (ERL) table – where they are indexed by the ERL parameter.

Operation

To provide emergency call handling to phones that are mobile between emergency areas in the enterprise, the ERL table must contain a definition for every ERL defined in the enterprise network. In addition, the ERL table must be provisioned on every individual Call Server in the enterprise, to accommodate phone clients moving between one Call Server and another.

The ERL table can be used with all phone types, because all phones devices now have an ERL parameter assigned to them.

ERL 0 is not a valid entry for the ERL table - this value is reserved to indicate that basic ESA treatment is to be used, as defined in the ESA Data Block (LD24).

The system administrator must ensure that the ESA Data Block (LD24) for a phone is configured before defining entries for that phone in the ERL table. There is no automatic overlay check to confirm that this has been done.

It is possible to enable or disable an ERL. It is not advisable to do so, as ESA call processing will then automatically use the ESA Data Block (LD 24) parameters, which may result in less accurate emergency call routing to the PSAP and a less specific CLID assignment.

It is possible to assign a phone to a disabled ERL, but a warning message is generated in the event this is done. A system message is generated during ESA call processing if an emergency call is made from a phone with its ERL disabled.

The Site Name is printed in the SITE field of an OSN record. Although not required, it is expected that this be a familiar name for an enterprise location that corresponds to an MSAG (Master Street Address Guide) validated address within an ALI record.

If a phone is not assigned a Location Description by the LIS or DM (as is the case with IP phones set to Manual Update and with non-IP phones), the Location Description is printed as LOC in the OSN record.

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

Routing data is optional. ERL routing data includes:

- Route number
- Access Code
- Prepend Digits
- RLI number
- Access Code
- Prepend Digits

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

The configuration of the Locator value is optional:

- If Locator is not specified, then ESA call processing assigns the Default CLID (DFCL) contained in the ESA Data Block (LD24).
- A Locator must be specified for network wide mobility to be supported - the Locator is configured similarly in the ERL table of every call server in the enterprise, and can be shared by multiple ERLs..
- The Locator is used as a fallback to Dynamic ELIN

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

Administration

This section details the administrative functionality of the ERL table.

Adding an ERL entry Adding a new ERL entry requires the use of the NEW ERL command (LD 117).

A token specifies the route mechanism to use for each ERL.

System messages are generated when adding a new ERL entry, if any of the following errors are encountered:

- ERL number does not fall within the valid range for that value (1-65535).

- Entered ERL information is found to be a duplicate value to an ERL value already configured.

To specify null routing data for a new ERL entry, enter NULL as the input value for the following fields:

- Route Number or RLI Number
- Access Code
- Prepend Digits

To specify a null Locator value, enter NULL as the value for the Locator data field.

To specify a null OSDN value, enter NULL as the input value or leave blank.

A newly created ERL entry is enabled by default.

After adding an ERL entry, the number of currently provisioned ERL entries is printed.

The ERL entry must be created and defined before location strings can be assigned to it.

Site Name and Location Description are alphanumeric strings up to 20 characters long. Strings encapsulated in quotation marks may contain spaces and punctuation marks (with the exception of quotation marks and colons).

Changing the Location Description of an ERL causes all Manual Update IP phones to be relocated, and causes an update of their Location Description to occur in the TN Table.

Deleting an ERL entry Deleting an ERL entry requires the use of the OUT ERL command (LD 117).

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

The OUT ERL command is rejected if there are ELINs currently defined against it. Any Dynamic ELINs defined against the ERL entry must be deleted before the ERL entry itself can be deleted.

The OUT ERL command is rejected if the ERL entry specified for deletion is defined against a phone in either the TNB or TN Table, or is referenced in the subnet lookup table. Conversely, if an IP phone is assigned an ERL that no longer exists, then a system message is generated and the phone is assigned null (unknown) location data.

The administrator must ensure that the ERL to be deleted is not referenced by the DM.

After successful deletion of an ERL entry, the number of currently provisioned ERL entries is printed.

Changing an ERL entry Making changes to an existing ERL entry requires the use of the CHG ERL command (LD 117).

A token specifies the route mechanism to use for each ERL.

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

Optional parameters are specified the same way as for the NEW ERL command.

Printing ERL entries Printing one ERL entry or all ERL entries requires the use of the PRT ERL command (LD 117).

With the execution of the PRT ERL command, the number of currently provisioned ERL entries is printed.

Maintenance

Enabling and disabling an ERL entry requires the use of the ENL ERL and DIS ERL commands (LD 117), respectively.

System messages are generated if the specified ERL is out of range or does not exist, or (during ESA call processing) if the ERL of the emergency caller is disabled.

System messages related to ERL management (LD 117)

Table 4
System messages related to 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
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 999).	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 <conflict>.	Resolve the conflict before proceeding.	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, SNMP

Location management for non IP lines

This section discusses the way in which the Location Management functionality of the ESA feature can be applied to non IP telephones.

Incoming trunks

ESA call handling operates using the location based parameter, ERL. Trunks do not have an ERL parameter assigned to them (CS 1000E trunks function as assigned bandwidth zones, based on IPMG) - therefore, trunk-initiated ESA calls receive basic ESA treatment at the call server, as defined by the parameters configured in the ESA Data Block (LD 24). This causes a trunk-initiated ESA call to the call server to route using a configured set of default ESA parameters.

The ESA Data Block (LD 24) can also specify virtual trunk routing.

Non IP phones

The ERL parameter can be assigned to all phones in the enterprise, including non IP phones, to provide location information specific to each phone in the event of an emergency call. This results in easier management of the ESA feature due to a common enterprise wide configuration of caller locations by ERL. In addition, the assignment of ERL enables:

- flexible routing for remote cabinets (MCR and SIPE, for example).
- the use of Dynamic ELINs in CLID assignment (Dynamic ELINs are ERL based).

Data contained in the ERL data field of a non IP phone is statically configured, as a non IP phone is not deemed to be a mobile telephone client – it is assumed to always remain at its originally provisioned home location.

Because a non IP phone does not change locations, there is no need for a mechanism to determine its current (changing) location - the ERL value for a non IP phone is manually provisioned by the system administrator, and is always deemed represent the current location because the non IP phone does not move. This is similar to the ERL functionality of IP phones set to Manual Update.

Mobility of a non IP phone client (due to a wireless handset, for example) is not provided for by the ESA feature – if a non IP phone has the ability to move away from its phone base, then it should be configured using a less specific ERL value, that accommodates for its possible range of movement.

When configuring the ERL value for a non IP telephone by means of either the NEW or CHG commands, a value must be entered to identify it as a particular ERL entry, as follows:

- In the case of using NEW to configure a new ERL entry, the value must be within a valid range (1 to 65535). If the CHG command is used to alter the current ERL configuration of a given non IP telephone, the value is rejected if the ERL is not found to be currently defined.
- If the ERL value is left blank, then the value is interpreted to be zero. This indicates that basic ESA Data Block (LD 24) parameters are to be used in emergency call processing for the non IP phone, and that default emergency call treatment is to be provided. ESA call processing does not generate a system message for a non IP phone in ERL 0 - it is assumed that the system administrator intended for the phone to receive basic ESA treatment.

Non IP telephones in ERL 0 may still use CLID blocks to compose a specific ANI. If CLID blocks are used in this way, the ERL entry is only used for emergency route determination purposes. However, it is recommended that the definition of ANI be simplified by using the ERL table (Locator or Dynamic ELIN) in its composition, and not the CLID blocks.

If a non IP phone is fully provisioned with an ERL entry, then its ESA parameters are contained in the ERL table, as is the case with IP phones.

ERL is only printed by the PRT TNB command if ESA is configured.

Automatic Set Relocation

ESA does not automatically update the ERL of the phone when Automatic Set Relocation (or Modular Telephone Relocation) is used. All location dependent data must be administratively updated following such a move. The data fields affected are as follows:

- Descriptor (DES)
- Zone
- ERL
- CLID entry or ALI update for DID mapping.

Data conversion

This section describes the assignment of ERL values during an upgrade from a previous software version of ESA.

As the ERL table is created automatically from the previous Zone (ZESA) table, the ERL parameter is converted automatically in the same way (as applicable) for non IP telephones, as described by the following:

- For a Non IP phone on a CS 1000E call server, the new ERL value is determined as follows:
 - $ERL = (VPNI \times 256) + IPMG \text{ Zone}$. This continues to allow location based ESA call treatment, as defined previous to the software upgrade. See also VPNI / ERL table on page 292.
 - As BRI phones did not previously receive ZESA call handling on CS 1000E, the ERL value assigned to BRI phones after the software update is 0.
- For a Non IP phone on a non CS 1000E call server, the ERL is assigned a value of 0 during the software upgrade. An ERL value of 0 indicates that basic ESA Data Block (LD 24) treatment for emergency calls is to be used, as before.

List phones by ERL

ESA enables the use of the LST/CNT commands (in LD 81) to list or count phones by ERL.

Call Recognition

The ESA Call Recognition function lets the system administrator configure an Emergency Services Directory Number (ESDN) in LD 24 (also used for Direct Inward System Access administration), on a customer basis. When a user dials the ESDN, the system recognizes the call as a public emergency services request, and immediately routes it to the public emergency services over trunks designated to handle ESA calls.

The ESDN can be up to four digits long, and can be the same number that a caller would use to request emergency services from home (in North America, this number is 911), unless the number conflicts with any other number in the dialing plan.

The configuration of a customer's ESDN is independent of the customer's ESN database, so that ESA calls can be routed to the PSAP as soon as the ESDN is dialed. There is no need to dial a BARS/NARS Access Code prior to dialing the ESDN. ESA calls also override any access restrictions placed on phones or trunks. Refer to ["Access Restrictions" \(page 169\)](#) of the feature interactions section for more details.

Guidelines for configuring the ESDN

The system does not check for conflicts between the digits used for the ESDN and digits used for Coordinated Dialing Plan steering codes, or for a BARS/NARS dialing plan. Therefore, the following guidelines should be followed when configuring the ESDN on the system:

- Do not configure internal DNs and CDP steering codes, that are the same length or longer than the ESDN, to have the same leading digits as the ESDN.

If there is any internal DN or steering code that is equal to or longer than the ESDN, and all the leading digits of that internal DN match the ESDN digits, then calls will not terminate on that internal DN or steering code, because ESA calls receive priority. For example, if the ESDN is 911, and there is a station DN or a steering code of 9112, then whenever someone dials the 9112 extension, or steering code, they are automatically routed to the PSAP as an ESA call.

In the event that a newly configured ESDN is found to be in conflict with a configured internal DN, error message SCH2225 is printed to indicate the conflict (as described previously, the ESDN will take precedence over the internal DN in a dialing scenario).

- Do not configure internal DNs or CDP steering codes, that are shorter than the ESDN, to have the same leading digits as the ESDN.

If there is any internal DN or steering code that is shorter than the ESDN, and all the leading digits of the ESDN match those of that internal DN or steering code, the callers may be prevented from making an ESA call. For example, if the ESDN is 911, and there is a station DN or steering code of 91, then whenever someone attempts to dial the 911 ESDN, they are presented as a call to that station, or routed out as a CDP steering code, rather than being routed to the PSAP as an ESA call.

- Do not configure a BARS/NARS dialing plan, (that is, Access Code (AC) + Location Code (LOC)/North American Planning Area Code (NPA)/Central Office Code (NXX)/Special Number (SPN)), that is the

same length or longer than the ESDN, to have the same leading digits as the ESDN.

If there is a BARS/NARS dialing plan, equal to or longer than the ESDN, and all the leading digits of that internal DN match the ESDN digits, then calls will not terminate on that dialing plan, because ESA calls receive priority. For example, if the ESDN is 911, and there is a BARS/NARS dialing plan having an access Code of 9 and a Special Number of 114, then whenever someone tries to dial 9114, they are automatically routed to the PSAP as an ESA call.

- Do not configure a BARS/NARS dialing plan (that is, Access Code (AC) + Location Code (LOC) / North American Planning Area Code (NPA) / Central Office Code (NXX) / Special Number (SPN), that is shorter than the ESDN, to have the same leading digits as the ESDN.

If there is BARS/NARS dialing plan, shorter in length than the ESDN, and all the leading digits of that internal DN match the ESDN digits, then callers may be prevented from making ESA calls. For example, if the ESDN is 911, and there is a BARS/NARS dialing plan having an access Code of 9 and a Special Number of 1, then whenever someone tries to dial 911, they are automatically routed out as a BARS/NARS Special Number.

- For customers using a BARS/NARS dialing plan, it is possible to configure their database such that the PSAP may be reached by either dialing only the ESDN, or an Access Code and then the ESDN. In order for the latter to be recognized as an ESA call by the system, the ESDN must be configured as a BARS/NARS Special Number in LD 90 (by entering the ESDN in response to the SPN prompt), and the Special Number be configured to use a local terminating route list index (by responding to the LTER prompt with YES in LD 86).

Table 5
System messages related to ESDN Configuration (LD 24)

Message Number	Severity	Event	Corrective Action	Output
SCH2225	Warning	ESDN conflicts with the existing DN.	Configure a different ESDN.	TTY

Originating an ESA call from a phone or attendant

Originating an ESA call from a phone

An ESA call may be made from an analog (500/2500-type) phone by simply going off-hook, waiting for dial tone, and dialing the ESDN. If there is another call already established on the phone, the caller may do a consultation, or invoke standard conference or call transfer by performing an off-hook flash, waiting for special dial tone, and then dialing the ESDN.

An ESA call can be made from a Meridian 1 proprietary phone by simply going off-hook, waiting for dial tone after pressing either the Single Call Ringing, Single Call Non-ringing, Multiple Call Ringing, Multiple Call Non-ringing, or Hotline (HOT) key, and then dialing the ESDN. If there is another call already established on the phone, the caller may do a consultation, or invoke standard conference or call transfer by pressing either the Transfer, Conference, No-hold Conference, or No-hold Conference Hotline key, waiting for dial tone, and then dialing the ESDN.

Originating an ESA call from an attendant console

An ESA call may be made from an attendant console by pressing an idle LOOP key, waiting for dial tone, and dialing the ESDN. If the attendant already has an established call on the source (SRC) side of an active LOOP key, an ESA call may be initiated on the destination (DEST) side of the active LOOP key.

Calling Terminal Identification

The ESA Calling Terminal Identification function lets the system compose an ESA calling number for outgoing ESA calls. The ESA feature modifies the functionality of the ISDN Calling Line Identification (CLID) Enhancements feature to compose the ESA calling number.

Note: The ESA Calling Terminal Identification function composes the calling number for ESA calls only. For non-ESA calls, the existing CLID composition remains in effect.

The ISDN CLID Enhancements feature lets up to 4000 CLID entries to be configured for a customer on a system equipped with the ISDN package 145. Each DN key for customer phones (analog (500/2500-type) phones, Meridian 1 proprietary phones, and ISDN BRI phones) may be assigned with a desired CLID entry (as stated, up to a maximum of 4000 CLID entries may be assigned for a customer). When an outgoing ISDN call is made, the appropriate CLID is composed for the originating DN based on the its CLID configuration (using LD 15, and, as required, LD 10, LD 11, and LD 27).

ESA does not require the ISDN package to define a CLID entry for a station DN. When an emergency services call is initiated, the Calling Terminal Identification function is automatically invoked by the system. This generates an Emergency Services Access calling number to identify the calling party requesting emergency services.

The calling number content is specified by the system administrator in LD 15, using the CLID entry prompt. This prompt has been modified to accept the following new responses for ESA. These new responses allow a customer to define how calling number digits are to be translated.

Refer to the section "[Digit translation examples](#)" (page 95) for examples of how the prompts (as defined in the following) may be applied to perform DID DN digit translation, and the type of translation required for non-DID digits.

- **ESA_HLCL** (ESA Home Local Code). This is the basic ANI that is generated. It is used as follows:
 - as a 3-digit home local office code for ESA DID calls that is being translated or
 - for non-DID calls, the full 7-digit translated number
- **ESA_INHN** (Insert Home National Code yes/no flag). If **ESA_INHN** is set to YES, then the ESA Home Local Code is translated to be prefixed by the Home National Code (area code). This is done when a 10-digit ANI is required. If **ESA_INHN** is set to NO, the ESA Home Local Code is not prefixed by the area code. This is done when a 7-digit ANI is required.
- **ESA_APDN** (Append DN yes/no flag). If **ESA_APDN** is set to YES, then the originating DN is translated to be appended to the ESA Home Local Code (**ESA_HLCL**). If **ESA_APDN** is set to NO, then the originating DN is not appended. The appending of the DN in this manner will be the typical treatment for DID numbers.

Note: **ESA_APDN** defaults to YES, and can only be changed to NO if the system is equipped with the Calling Number Mapping package (**ESA_CLMP**) 331.

On a system equipped with ESA, a CLID entry may be defined for trunk routes, on a per-route basis.

Calling number composition

The following sections provide tables that explain how a calling number is composed for DID digits, based on the digit translation done according to how the **ESA_HLCL**, **ESA_INHN**, and **ESA_APDN** prompts are defined. This is done for ESA calls initiated from a station phone, for ESA calls initiated from an attendant console, and for incoming trunk-initiated tandem ESA calls. Also, the section "[Digit translation examples](#)" (page 95) provides examples of how a customer might set up some digit translation configurations.

Note: In the tables that follow, for the sections pertaining to calling number composition, the composed numbers for ESA calls are said to be either 7 or 10 digits in length. As mentioned previously, if the Flexible Numbering Plan (FNP) is equipped, then the calling numbers can be any length, up to a maximum of 16 digits.

Also note that not all combinations of prompts shown in the tables are useful in an ESA environment. They have been included for completeness.

Calling number for station phone-initiated ESA calls

For ESA calls initiated from a station phone, the ESA calling number is composed based on the CLID entry for the DN key on which the call originates. [Table 6 "ESA calling number composition for station phone-initiated ESA calls" \(page 78\)](#) illustrates how the ESA calling number may be composed for station phone-initiated ESA calls, according to the CLID database.

Table 6
ESA calling number composition for station phone-initiated ESA calls

CLID entry configuration			ESA Calling Number composition (Typical use)	
HNTN	ESA_HLCL	ESA_INHN		
Does not matter	Defined	NO	YES	ESA_HCLCL + originating DN (7-digit ANI for a DID number)
Defined	Defined	YES	YES	HNTN+ESA_HLCL+originatingDN (10-digit ANI for a DID number)
Undefined	Defined	YES	YES	ESA_HLCL+originating DN (7-digit ANI for a DID number)
Does not matter	Undefined	NO	YES	originating DN (7-digit ANI for a DID number, if a 7-digit DID dialing plan is used.)
Defined	Undefined	YES	YES	HNTN+originating DN (10-digit ANI for a DID number, if a 7-digit DID dialing plan is used.)
Undefined	Undefined	YES	YES	Originating DN
Does not matter	Defined	NO	NO	ESA_HLCL (7-digit ANI for a non-DID number)
Defined	Defined	YES	NO	HNTN+ESA_HLCL (10-digit ANI for a non-DID number)
Undefined	Defined	YES	NO	ESA_HLCL
Does not matter	Undefined	NO	NO	Nothing
Defined	Undefined	YES	NO	HNTN
Undefined	Undefined	YES	NO	Nothing

Note: If the length of the resulting ESA calling number is invalid (refer to [Table 7 "Valid ESA calling number lengths" \(page 79\)](#) for valid lengths), then the ESA calling number is set to be the customer's Default ESA

Calling Number (as defined in response to the DFCL prompt in LD 24).
The DFCL is a number that is sent out if ANI is not used.

This also applies to the other cases of calling number composition in the sections that follow.

Table 7
Valid ESA calling number lengths

ESA Calling Number Length	ESA Calling Number Status	
	FNP Package Equipped	FNP Package Not Equipped
0	Invalid	Invalid
1-6	Valid	Invalid
7	Valid	Valid
8-9	Valid	Invalid
10	Valid	Valid
11-16	Valid	Invalid
More than 16	Invalid	Invalid

Calling number for attendant-initiated ESA calls

For ESA calls initiated from an attendant console, the ESA calling number is composed based on the CLID entry 0 (as per the ISDN CLID Enhancements feature functionality, when an attendant initiates a public numbering plan call, LDN0, as defined for the customer, is used as the originating DN).

[Table 8 "ESA calling number composition for attendant-initiated ESA calls" \(page 79\)](#) illustrates how the ESA calling number may be composed for attendant-initiated ESA calls, according to the CLID database.

Table 8
ESA calling number composition for attendant-initiated ESA calls

CLID entry configuration				ESA Calling Number composition (Typical use)
HNTN	ESA_HLCL	ESA_INHN	ESA_AP DN	
Does not matter	Defined	NO	YES	ESA_HLCL+LDN0 (7-digit ANI for a DID number)
Defined	Defined	YES	YES	HNTN+ESA_HLCL+LDN0 (10-digit ANI for a DID number)
Undefined	Defined	YES	YES	ESA_HLCL+LDN0 (7-digit ANI for a DID number)
Does not matter	Undefined	NO	YES	LDN0
Defined	Undefined	YES	YES	HNTN+LDN0

CLID entry configuration				ESA Calling Number composition (Typical use)
HNTN	ESA_HLCL	ESA_INHN	ESA_AP DN	
Undefined	Undefined	YES	YES	LDN0
Does not matter	Defined	NO	NO	ESA_HLCL (7-digit ANI if LDN0 is not to be used)
Defined	Defined	YES	NO	HNTN+ESA_HLCL (10-digit ANI if LDN0 is not to be used)
Undefined	Defined	YES	NO	ESA_HLCL
Does not matter	Undefined	NO	NO	Nothing
Defined	Undefined	YES	NO	HNTN
Undefined	Undefined	YES	NO	Nothing

Calling number for incoming non-ISDN trunk-initiated tandem ESA calls

For incoming non-ISDN trunk-initiated tandem ESA calls, the ESA calling number is composed based on the CLID entry used by the incoming trunk route. [Table 9 "ESA calling number for incoming trunk-initiated tandem ESA calls" \(page 80\)](#) illustrates how the ESA calling number may be composed for non-ISDN trunk-initiated tandem ESA calls, according to the various combinations of the CLID ESA configuration.

Table 9
ESA calling number for incoming trunk-initiated tandem ESA calls

CLID entry configuration				ESA Calling Number composition
HNTN	ESA_HLCL	ESA_INHN	ESA_AP DN	
Does not matter	Defined	NO	YES	ESA_HLCL+ACOD ¹
Defined	Defined	YES	YES	HNTN+ESA_HLCL+ACOD
Undefined	Defined	YES	YES	ESA_HLCL+ACOD
Does not matter	Undefined	NO	YES	ACOD
Defined	Undefined	YES	YES	HNTN+ACOD
Undefined	Undefined	YES	YES	ACOD
1. ACOD = Route access code of the incoming trunk.				

CLID entry configuration				ESA Calling Number composition
HNTN	ESA_HLCL	ESA_INHN	ESA_AP DN	
Does not matter	Defined	NO	NO	ESA_HLCL (7-digit ANI indicating the trunk route. This would allow the person who is receiving the DID call to at least know on what trunk the call originated.)
Defined	Defined	YES	NO	HNTN+ESA_HLCL (10-digit ANI indicating the trunk route)
Undefined	Defined	YES	NO	ESA_HLCL
Does not matter	Undefined	NO	NO	Nothing
Defined	Undefined	YES	NO	HNTN
Undefined	Undefined	YES	NO	Nothing

1. ACOD = Route access code of the incoming trunk.

Calling number for incoming ISDN trunk-initiated tandem ESA calls

For incoming trunk-initiated tandem ESA calls, the CLID that is tandemed in is tandemed out as the calling number. In rare cases, such as when no valid CLID is received, a CLID entry should be set up, in which case [Table 9 "ESA calling number for incoming trunk-initiated tandem ESA calls" \(page 80\)](#) applies.

Dynamic ELIN

Background

The only way to effectively communicate caller location to the PSAP at the time of an emergency call is to pass along an ANI (CLID) that corresponds to that location. Thus, a preconfigured ANI - that is, a static DID number or Emergency Location Identification Number (ELIN) - must be provisioned for all potential emergency locations within the enterprise network, so that those locations can be identified by the PSAP.

Overview

To allow for true network wide mobility, the ESA feature requires that every defined ERL on the enterprise network be defined on every individual call server – this ensures universal location recognition for every ERL by every call server, no matter where the ERL is physically located.

In turn, it is required that each ERL have a static ELIN (Locator) configured, which can be assigned to emergency calls for location recognition by the PSAP.

It is possible to assign a common static ELIN, or even a Default CLID (DFCL), to multiple ERL entries on the same call server. In this case, however, the static ELIN sent to the PSAP is associated with a static “zone phone” for the call server location (which is used for callback purposes), and not the actual phone of the emergency caller.

The Dynamic ELIN functionality of ESA allows a preconfigured static DID number (or ELIN) to be provisioned for each individual ERL. This means that, during an emergency call, ESA can dynamically (and temporarily) map this configured ELIN to a specific non DID phone anywhere in the ERL. This functionality provides the PSAP with a precise location description for the actual phone making the emergency call, allowing direct callback to the emergency caller location by the PSAP. This Dynamic ELIN functionality also applies to DID phones not at their originally provisioned location.

An ELIN can be assigned to an ERL so long as certain conditions are met, as follows:

- The ELIN allows emergency calls to route to the correct PSAP by means of a private or public network.
- The ELIN is valid in the ALI database associated with the ERL.
- When dialed from the PSTN, the ELIN (DID number) enables a direct callback to the call server to which it is associated. That is, the ELIN can be used for any ERL serviced by this call server.
- Multiple call servers providing local service to an ERL can have separate ELINs defined for that ERL.

The use of the Dynamic ELIN feature is optional. This enables an administrator to gradually perform data conversion after a software update, as there are initially no Dynamic ELINs defined.

The ALI Manager is expected to provide enterprise wide ELIN management. Otherwise, each individual ELIN defined for each individual ERL must be managed administratively.

Dynamic ELIN functionality applies to both IP phones and non IP telephones.

Operation

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

- ESA call processing assigns the Dynamic ELIN information to the emergency call, for routing to the PSAP and for location identification.
- ESA call processing configures call forward (CFW) on the ELIN to temporarily reflect the DN of the emergency caller.

- A system message is generated to log the ELIN mapping that has just taken place.

If a callback is made by the PSAP while the Dynamic ELIN is mapped, the subsequent call operation is as follows:

- The emergency operator calls back using the ELIN (DID number) information provided to them at the time of the call. The callback made by the PSAP which routes to the original call server.
- The Dynamic ELIN redirects the callback to the DN of the emergency caller, to which it has been temporarily assigned.
- The original emergency caller answers the call.

Repeat emergency calls

The case of a user making a repeat emergency call before the Dynamic ELIN mapping of the original emergency call has expired, is handled as follows:

- If the caller has not moved to a different location (and therefore has the same ERL as when the original emergency call was made) then they keep their assigned Dynamic ELIN. The expiry time of the Dynamic ELIN assignment is simply refreshed.
- If the caller has moved to a different location (to a new ERL) then a new Dynamic ELIN is assigned that corresponds to the new ERL, and the original ELIN remains assigned until it expires. This enables the PSAP to perform a callback to the original ELIN as well as the new ELIN, which provides the best possible emergency coverage. This dual assignment of ELIN information does consume additional resources, but has been implemented in the interest of providing the best emergency coverage under as many emergency call scenarios as possible. Placing a repeat emergency call using the same phone in two entirely different physical locations is not likely to be a common call scenario, and in any case will only apply to roaming callers making emergency calls. The Dynamic ELIN overflow behavior ensures that no denial of service situations can arise.

Configuration considerations

Virtual TNs and Phantom TNs can be used with the Dynamic ELIN functionality, and are detailed as follows:

- The functionality of Dynamic ELIN on a Virtual and Phantom TN is similar to the standard functionality, though engineering considerations differ.
- The administrator chooses which to use.
- The choice to use either a Virtual TN or a Phantom TN causes no inherent conflict in either the Dynamic ELIN or ERL tables.

- Can be defined and configured without concern for further associated hardware dependencies.
- Can be used to define DID directory numbers.
- If using a Virtual or Phantom TN, ESA CLID data must be configured so that an ELIN can be composed.
- The ALI records of the TN used must indicate its ERL location.
- The Virtual and Phantom TN types are reserved for emergency use.

The determination of the required number of Dynamic ELINs for each ERL depends on a number of considerations, as follows:

- The number of non DID phones, and the amount of DID mobility within the ERL - in making an emergency call, a DID phone uses its DID number as its ANI, and only requires the use of a Dynamic ELIN if it is not in its originally provisioned location.
- The amount of client mobility in the ERL – if there are only a few phones in the ERL that have the capability of being mobile telephony clients, then fewer Dynamic ELINs are required.
- The expected number of simultaneous emergency calls from this ERL - if the ERL is in a high risk environment, there is the potential of many emergency calls being placed at the same time. Consider provisioning extra numbers of Dynamic ELINs to accommodate.
- The emergency usage policies decided upon for the particular ERL environment – for example, whether delivering a PSAP callback directly to the emergency caller is deemed to be important or not.

Virtual TNs

If a Virtual TN is used, the system administrator must ensure that no IP phones will register themselves using it, as this can cause a call forward conflict and impact the operation of emergency services resources - a Station Control Password (SCPW) should therefore be configured to prevent IP phones from registering to the Virtual TN. In addition, Class of Service (CLS) Virtual Office User Denied (VOUD) should be configured so as to deny attempted Virtual Office logins over 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 so, the dynamic ELIN TN is rejected and an error message is generated. Another ELIN or the static ELIN (Locator) will be used instead.

Phantom TNs

If a Phantom TN is used, the system administrator must ensure that no IP phones will register themselves using it, as this can cause a call forward conflict and impact the operation of emergency services resources.

A Phantom TN must be configured with a Default Call Forward (DCFW) DN for times when the regular call forward is inactive (when the Dynamic ELIN is not mapped to it, for example).

A Phantom ELIN TN may be configured as 500 (PBX) sets on a phantom analog card or as 3904V (Taurus) sets on a phantom digital card.

Before mapping a 3904V dynamic ELIN TN, ESA call processing checks if there is a phone Virtual Office logged in to it. If so, the dynamic ELIN TN is rejected and an error is generated. Another ELIN or the static ELIN (Locator) will be used instead.

If the system is not configured with an IP ISM then a Phantom TN must be used for the configuring of Dynamic ELINs - in the event that this is the case, the Dynamic ELIN feature only applies to non IP phones.

Callback fallback

A callback from the PSAP is viewed and treated as any other incoming call, and could fail under certain conditions, as follows:

- The emergency caller's phone line is busy.
- The emergency caller does not answer.
- The emergency caller has unregistered or been preempted.
- The ELIN mapping to the emergency caller's phone has expired.

The following sections describe existing features which can be configured on the ELIN TN by the administrator as fallback call forward mechanisms, used to ensure that a PSAP callback succeeds.

Default Call Forward (DCFW)

This feature applies to Phantom TNs only.

If call forward is not active on the Phantom TN, meaning that an ELIN is not currently mapped to it, then all calls to the Phantom TN DN route to the configured Default Call Forward (DCFW) DN.

It is recommended that the DCFW DN be configured to reflect the static ELIN (Locator) of the ERL, or perhaps the Default CLID (DFCL) for the system. This ensures that the PSAP callback can still terminate if the ELIN mapping for the emergency caller's phone has expired.

Flexible Call Forward No Answer

This feature applies to Virtual TNs and Phantom TNs.

If the original emergency caller does not answer the PSAP callback attempt, Flexible Call Forward No Answer feature forwards the call to the Flexible Call Forward No Answer DN (FDN) configured on the ELIN TN.

It is recommended that the administrator configure the FDN to the static ELIN (Locator) for 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) enables an unanswered call to receive Call Forward No Answer (CFNA) treatment twice.

If this feature is configured, and the phone line of the emergency caller is busy, the PSAP callback may route to the hunt DN (to voicemail, for example), 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 Call Forward Save on Sysload system option is made active (by setting the CFWS prompt in LD 17 to YES), all phones will have their call forward status and reset to the state they were in as of the last successful data dump following a Sysload.

The Dynamic ELIN audit that occurs after a Sysload ensures that Dynamic ELIN mappings that are active are remapped, while mappings that are inactive are unmapped. This is only applicable if the Sysload occurs after the data dump and within the timeframe specified by the Dynamic ELIN Timeout value - otherwise any ELINs mapped at the time of the data dump will have already expired by the time the Sysload takes place.

Overflow

A system option specifies Dynamic ELIN overflow behavior if every Dynamic ELIN for an ERL are in currently in use and another emergency call occurs.

If the overflow option, DYNAMIC_ELIN_REUSE, is set to NO, the new emergency call will fall back to the Locator and the static ELIN (Locator) is used.

If the overflow option, DYNAMIC_ELIN_REUSE, is set to YES, then it is set to reuse oldest mapped ELIN, and the oldest mapped ELIN is remapped to the new emergency caller. In this case, a PSAP callback made to the phone

to which the ELIN was previously mapped will ring through to the phone making the new emergency call. Because both emergency call locations have sent the same CLID to the PSAP, this is similar to the case where the static ELIN (Locator) was used.

Expired mappings

A system configuration parameter, `DYNAMIC_ELIN_TIMEOUT`, specifies the time delay (in minutes) before a Dynamic ELIN mapped to a phone is unmapped so that it is made available for use in another emergency call.

Effectively, the time value configured in this parameter is the length of time the mapping of a Dynamic ELIN lasts.

A background procedure, the Dynamic ELIN audit, periodically checks for ELIN mappings that have expired and unmaps them.

A system message is generated to the log when an ELIN does not automatically unmap after it expires and needs to be unmapped by the Dynamic ELIN audit. No system message is generated if the unmapping of a Dynamic ELIN is due to a system restart. See also Emergency caller unregistrations, following.

Emergency caller unregistrations

If a caller becomes unregistered from the network after making an emergency call, the Dynamic ELIN mapping assigned to their phone becomes obsolete. Otherwise, a subsequent PSAP callback might route to an unregistered number or possibly to an incorrect user.

This functionality handles unregistrations caused by several cases, as follows:

- A Virtual Office user has logged out.
- Emergency caller was preempted by a VO login.
- Emergency caller has unregistered due to a connectivity problem.

A system message is generated to log this unmapping.

ELIN TN configuration

This section discusses the configuration of ELIN TNs.

To minimize system resources when using a Phantom TN, it is recommended that the most basic type of digital Phantom TN, the 3903V, be configured for Dynamic ELIN use.

To minimize system resources when using a Virtual TN, it is recommended that the most basic type of Virtual TN, the i2001, be configured for Dynamic ELIN use.

Administration

To associate a Dynamic ELIN with a specific ERL, the NEW ELIN command (LD 117) is used.

To define a Dynamic ELIN against an ERL, the ERL must be defined first.

The NEW command does not create a Dynamic ELIN, it only associates it with an ERL. The Dynamic ELIN must be fully provisioned before it can be associated to any ERL.

The administrator is responsible for ensuring that the Dynamic ELIN is associated to the correct ERL, as there is no process check in place to prevent an incorrect assignment – if the Dynamic ELIN is valid, it can be associated to any valid ERL, regardless of design intentions.

The NEW command reports the ESA CLID composed by the specified TN (according to its CLID block configuration). If the ESA CLID is invalid, the command is rejected.

To disassociate a Dynamic ELIN from its currently associated ERL, the OUT ELIN command (LD 117) is used, under the conditions as follows:

The OUT ELIN command is rejected if either the specified ERL or Dynamic ELIN entry does not exist.

The OUT ELIN command automatically makes any active mappings of the specified Dynamic ELIN obsolete, and generates a warning message that the mapping has been terminated. This is done to inform the administrator that emergency call handling for the mapped phone may have been interrupted by the administrative change (that is, a PSAP callback directly to the emergency caller's phone is no longer possible).

To print Dynamic ELIN information for either a specific ERL or for all ERLs, the PRT ELIN command (LD 117) is used.

The PRT command reports the CLID composed by each Dynamic ELIN. This ensures that configuration changes made to the Dynamic ELIN are reflected.

The DCFW number (if configured) is also printed.

Maintenance

The STAT ELIN command (LD 117) prints a report detailing the current status of all Dynamic ELINs on either a specific ERL or on all ERLs for the enterprise.

The STAT command reports the ELIN that is assigned per ERL, 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.

Configuration considerations

Because ERL data (Routing and DN information, for example) is configured for use with specific clients, the administrator must ensure that Dynamic ELIN data that is configured for use with a particular ERL is correctly associated to the ERL for which it was intended.

Error message ESA016 is generated during an ESA call if the information in an ELIN TN does not match that which is expected by the ESA caller.

Dynamic ELIN audit

The Dynamic ELIN audit is a procedure that runs in the background and checks if any currently mapped Dynamic ELINs have timed out and can be unmapped (freeing up the ELIN for reuse). The Dynamic ELIN audit 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 if the audit finds a Dynamic ELIN that it had to unmap.

System messages

The system messages associated with Dynamic ELIN are detailed in the table that follows:

Table 10
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
ESA005	Major	ERL 'x' is not configured.	Correct the ERL configuration.	TTY, SNMP

Message Number	Severity	Event	Corrective Action	Output
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. See previous ESA messages for reason.	TTY, SNMP
ESA016	Major	ESA caller customer number and ELIN customer number do not match <caller dn> <caller cust #> <elin dn> <elin cust num>	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

Message Number	Severity	Event	Corrective Action	Output
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 updated for ESA caller DN 'z'	Contact your technical support.	TTY, SNMP
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

Message Number	Severity	Event	Corrective Action	Output
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

Multiple Appearance DNs

It is possible that the target DN of a Dynamic ELIN mapping (for an emergency caller's phone) is a Multiple Appearance DN. In this case, a PSAP callback causes all instances of the DN to ring, so as to guarantee that the callback terminates.

Survivability

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

The 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 the ELIN table is only updated to include the last data dump).

System engineering Packaging

The call forward mechanism used is part of the base system software – no additional packages are required.

To use a Phantom TN, PHTN package (254) is required.

The Factory preset ISMs are set to the maximum values and cannot be orderable or incremental. Setting these ISMs to the maximum enables the functionality supported by these ISMs to be configured in software at any time to meet customer needs. Phantom TNs are factory preset (2500 on Small Systems / 32760 on Large Systems).

TN consumption and ISMs

Dynamic ELIN requires Virtual TNs or Phantom TNs (or a combination of both). Reserving Dynamic ELINs for emergency use reduces the overall system limits, such as the number of TNs available for other purposes. For example, a Phantom TN and a Virtual both use the same TN range in their operation. Therefore, the number of Phantom TNs on the network directly reduces the possible number of Virtual TNs that can be placed on the network. For this reason, system engineering guidelines regarding the use of Virtual TNs or Phantom TNs must be developed.

Using a Phantom TN is generally not as desirable as using a Virtual TN, because of the lower superloop density of the Phantom TN. However if a Phantom superloop is already provisioned on a system and unused phantom ports are already available, then it makes sense to utilize these for Dynamic ELIN.

A Virtual TN exists on a Virtual loop. Because an entire superloop must be configured as Virtual to provision a single virtual TN, then:

- Minimum 256 Virtual TNs on Small System (224 on SUPL 112).
- Minimum 1024 Virtual TNs on Large System

A Phantom TN exists on a Phantom loop. Because an entire superloop must be configured as Phantom, to provision a single Phantom TN, then:

- Minimum 128 Phantom TNs on Small System (112 on SUPL 112).
- Minimum 512 phantom TNs on Large System.

Also, additional ISMs may need to be provisioned for the Dynamic ELIN feature, as follows:

- If the Dynamic ELIN TN is configured as an Phantom TN:
 - The number of TNs on the system must be less than TNS.
 - The number of Phantom TNs on the system must be less than PHANTOM PORTS.
- If ELIN TN is configured as an i2001 phone:
 - Number of TNs on system must be less than TNS.
 - Number of i2001 phones on system must be less than BASIC IP USERS.
- If ELIN TN is configured as a non i2001 phone (for example, as i2004):
 - The number of TNs on system must be less than TNS.
 - The number of non i2001 phones on the system must be less than IP USERS.

Digit translation examples

This section provides examples about how a customer may set up digit translation for DID numbers, non-DID numbers, trunk routes, and attendants.

DID numbers

The only translation normally required by DID numbers is to add the NXX (office code), and possibly the NPA (area code). All DID numbers in the same NPA-NXX can share a single CLID table entry, unless there is a need for multiple entries for ISDN purposes.

Example 1

A customer has DID numbers in the ranges 5000–5999 and 8000–8499. The Office Code is 768 and the Area Code is 404.

Set up a CLID table entry number 7, and assign this CLID table number to all DID keys and phones.

The ESA data for entry 7 in LD 15 will be:

HNTN	404	Area code (NPA)
ESA_HLCL	768	Office code (NXX)
ESA_INHN	yes	Include NPA, if 10-digit ANI required
	no	No NPA if 7-digit ANI required
ESA_APDN	yes	Append the DN after ESA_HLCL

This will form the ANI in the following way:

- ANI will be set to 768.
- The DN will be appended at the end (for example, DN 5123 will form 7685123).
- If ESA_INHN is 'yes', the area code will be added on to the beginning, giving 4047685123.

Other DID numbers will be similarly formulated.

Example 2

A customer has DID numbers in the ranges 5000–5999 with Office Code 768, and 8000–8499 with Office Code 770. The Area Code is 404, but only 7-digit ANI is required.

Set up a CLID table entry number 7, and assign this CLID table number to all DID keys and phones in the 5000–5999 range.

The ESA data for entry 7 in LD 15 will be:

HNTN		Could be any valid value (may be needed for ISDN)
ESA_HLCL	768	Office code (NXX)
ESA_INHN	no	No NPA is required for a 7-digit ANI
ESA_APDN	yes	Append the DN after ESA_HLCL

This will form the ANI in the following way:

- ANI will be set to 768.
- The DN will be appended at the end (for example, DN 5123 will form 7685123).

Set up a second CLID table entry number 8, and assign this CLID table number to all DID keys and phones in the 8000–8499 range.

The ESA data for entry 8 in LD 15 will be:

HNTN		Could be any valid value (may be needed for ISDN)
ESA_HLCL	770	Office code (NXX)
ESA_INHN	no	No NPA is required for a 7-digit ANI
ESA_APDN	yes	Append the DN after ESA_HLCL

This will form the ANI in the following way:

- ANI will be set to 770.
- The DN will be appended at the end (for example, DN 8765 will form 7708765).

Example 3

A customer has DID numbers in the ranges 5000–5999 with NPA-NXX 404-768, and 8000–8499 with NPA-NXX 339-770. A 10-digit ANI is required to distinguish between the load area codes.

Set up a CLID table entry number 7, and assign this CLID table number to all DID keys and phones in the 5000–5999 range.

The ESA data for entry 7 in LD 15 will be:

HNTN	404	Area code (NPA)
ESA_HLCL	768	Office code (NXX)

ESA_INHN	yes	Include NPA, required by a 10-digit ANI
ESA_APDN	yes	Append the DN after ESA_HLCL

This will form the ANI in the following way:

- ANI will be set to 768.
- The DN will be appended at the end, for example DN 5123 will form 7685123.
- The area code will be added at the beginning, giving 4047685123.

Set up a second CLID table entry number 8, and assign this CLID table number to all DID keys and phones in the 8000–8499 range.

The ESA data for entry 8 in LD 15 will be:

HNTN	339	Area code (NPA)
ESA_HLCL	770	Office code (NXX)
ESA_INHN	yes	Include NPA, required by a 10-digit ANI
ESA_APDN	yes	Append the DN after ESA_HLCL

This will form the ANI in the following way:

- ANI will be set to 770.
- The DN will be appended at the end, for example DN 8765 will form 7708765.
- The area code will be added at the beginning, giving 3397708765.

7-digit DID numbers

This would be typical of a residential application, where the system is being used to deliver dial tone to apartment dwellers.

Example 4

An apartment complex has 7-digit dialing, and because of load area codes, requires to use 10-digit ANI. The 7-digit DNs encompass several NXXs.

A single CLID table entry will suffice to handle all such subscribers on a customer, unless there are multiple area codes involved, when there will need to be one entry per NPA.

Set up a CLID table entry number 6, and assign this CLID table number to all DID keys and phones.

The ESA data for entry 6 in LD 15 will be:

HNTN	404	Area code (NPA)
ESA_HLCL		leave blank
ESA_INHN	yes	Include NPA, if a 10-digit ANI required
ESA_APDN	yes	Append the DN after ESA_HLCL

This will form the ANI in the following way:

- ANI will be set to blank.
- The DN will be added onto the end, for example DN 7685123 will form 7685123.
- The area code will be added at the beginning, giving 4047685123.

Non-DID numbers

Non-DID numbers have to be mapped to individual DID numbers in most cases. As this mapping is not systematic, there will have to be at least as many CLID table entries as there are DID numbers that have non-DIDs mapped to them. If some DID numbers have no non-DIDs mapped, they will not need a unique entry, but can use a common one as in examples 1 and 2, described previously.

Example 5

A customer has DID numbers in the range 5000–5999, and has non-DID numbers in the range 3000-3999. The Office Code is 768, and NPA is not required. [Table 11 "CLID table configuration for non-DID numbers" \(page 98\)](#) illustrates part of the CLID table configuration that would be required:

Table 11
CLID table configuration for non-DID numbers

DN	3008	3009	3010	5704 (DID)
Mapped to DID	5199	5704	5704	5704
CLID table entry number	84	85	85	7
HNTN	-	-	-	-
ESA_HLCL	768 5199	768 5704	768 5704	768
ESA_INHN	no	no	no	no
ESA_APDN	no	no	no	yes
ANI formed	768 5199	768 5704	768 5704	768 5704

The non-DID keys and phones will have the corresponding table entries programmed in LD 10 and LD 11.

The DID number 5704 could equally well be mapped to itself (table entry 85), but it is easier for administration to map all DIDs to a common entry number (7 in this example).

Trunk Routes

Non-ISDN private network TIE trunk routes need to have an identifying DID number assigned. When a 911 call comes in over such a route, this number will be sent as the ANI to identify the originating location.

Example 6

The remote location is located in area code 339, and is within the Selective Routing capabilities from the hub node. The receptionist's DID DN at the remote node is 770-8700, and it is decided to use this number to identify the remote location.

Set up a CLID table number entry 5, and assign this CLID table number to the trunk route data block for the route.

The ESA data for entry 5 in LD 15 will be:

HNTN	339	Area code (NPA)
ESA_HLCL	7708700	Office area code (NXX)
ESA_INHN	yes	Include NPA, if a 10-digit ANI is used
ESA_APDN	no	Do not append the DN after ESA_HLCL

This will form the ANI in the following way:

- ANI will be set to 7708700.
- The area code will be added at the beginning, giving 3397708700.

ISDN trunk routes

Although the incoming CLID will be used as ANI on calls from an incoming ISDN TIE trunk route, a CLID entry should still be set up. This will be used as the ANI if no valid CLID is received. The data entry shown in Example 6 will apply for this case also.

Attendants

An entry is required to define the ANI to be sent when attendants originate a 911 call. Attendants default to CLID table entry 0, which uses the LDN0 as the DN to be used.

Example 7

Set up CLID table number entry 0, which will be used for all attendant consoles in the customer. The Office Code is 768, the Area Code is 404, and the LDN0 is 0100.

The ESA data for entry 0 in LD 15 will be:

HNTN	404	Area code (NPA)
ESA_HLCL	768	Office code (NXX)
ESA_INHN	yes	Include NPA, if a 10-digit ANI required
ESA_APDN	yes	Append the LDN0

This will form the ANI in the following way:

- ANI will be set to 768.
- The LDN0 will be appended at the end, giving 7680100.
- The area code will be added at the beginning, giving 4047680100.

If the Console Presentation Groups feature is being used, a different LDN0 can be programmed for each CPG. This will allow different ANIs to be constructed for each CPG, which will allow a distinct ALI record. Thus a different CPG Tenant with LDN0 of 4300 will generate an ANI of 4047684300.

If all attendants are to be mapped to the same LDN0 (single tenant and co-located) the LDN0, or any other desired DID DN, could be built into ESA_HLCL, and ESA_APDN set to 'NO.'

Call Routing

The ESA Call Routing function lets the system administrator configure an outgoing route to only handle ESA calls (using the ESRT prompt in LD 24).

Note: Although it is recommended that dedicated trunks be configured to handle only ESA calls, and generally a minimum of two, the designated trunk routes may be shared with other types of calls.

As soon as an ESA call is made, the system identifies the call as being an ESA call (based on the ESA Call Recognition function.) The system then seizes the first available trunk designated as an ESA emergency services trunk, and routes the call over that trunk. If no ESA emergency services trunk is available, then the call will overflow to the alternate route (as configured in LD 16 in response to the STEP prompt).

The following trunk route types can be designated to handle ESA emergency calls only:

- Centralized Automatic Message Accounting (CAMA)

- Central Office (COT)
- Direct Inward Dial (DID)
- Foreign Exchange (FEX)
- TIE
- Wide Area Telephone Service (WATS)

Note: An NI-2 Call By Call or Integrated Services Access (ISA) service route may be configured as an ESA emergency call route, as long as it is one of the previously detailed types.

Because it is important for ESA calls to terminate on the outgoing trunk designated to handle ESA emergency calls, ESA calls override any access restrictions placed on outgoing trunks (refer to ["Access Restrictions"](#) (page 169) of the feature interactions section for more details.)

Calling and called number information for ESA calls routed to a CAMA trunk

This section describes the called number information for ESA calls routed to a Centralized Automatic Message Accounting (CAMA) trunk. A CAMA trunk is a trunk type that is mostly used to provide Private 911 services by the system.

For a system to PSAP connection, or in a system to Central Office to PSAP connection, the use of CAMA trunks between the system and the PSAP, or between system and the CO, is recommended by the FCC.

Whenever an ESA call is routed to an outgoing CAMA trunk, a called number and calling number information are sent using Multifrequency (MF) signaling.

Called number information

The called number information for outgoing ESA calls over CAMA trunks consists of, in order, a Key Pulse (KP) signal, the called number signals, and a Start (ST) signal.

As per the existing Enhanced 911 (E911) Switch Access requirements, the called number to access emergency services is in North America is expected to be either 911, 11, or 1. It is up to the E911 provider to specify the digits that the system is to output as the called number. This outputted number may be different than the ESDN. Using prompt DDGT in LD 24, the system administrator may configure "ESA Directing Digits." For ESA calls terminating on CAMA trunks, these DDGT digits are outputted as the called number rather than the ESDN.

Note: Enhanced 911 refers to the delivery of calling party numbers to the PSAP with 911 calls.

Calling number information

The calling number information for outgoing ESA calls over CAMA trunks consists of, in order, a Key Pulse (KP) signal, an information digit signal, the calling number signals, and a Start (ST) signal.

As per the existing E911 requirements, the information digit for ESA calls must be either '0' if the calling number is transmitted by the system, or '2' if the system does not know and cannot transmit the calling number.

The ESA feature sets the outgoing calling number to be one of the following:

- For a station phone to CAMA trunk ESA call, the outgoing calling number is the ESA calling number that has been composed for the station phone (refer to [Table 6 "ESA calling number composition for station phone-initiated ESA calls" \(page 78\).](#))
- For an attendant console to CAMA ESA call, the outgoing calling number is the ESA calling number that has been composed for the attendant console (refer to [Table 8 "ESA calling number composition for attendant-initiated ESA calls" \(page 79\).](#))
- For a trunk to CAMA tandem ESA call, the outgoing calling number is as follows:
 - On a system not equipped with the ESA_SUPP package, the outgoing calling number is the ESA calling number composed for the incoming trunk route (refer to [Table 9 "ESA calling number for incoming trunk-initiated tandem ESA calls" \(page 80\)](#)), regardless of whether an ANI/CLID is passed in by the incoming trunk.
 - On a system equipped with the ESA_SUPP package, if a valid ANI/CLID is passed in by the incoming trunk (such as an ISDN trunk, M911 trunk, or Feature Group D trunk), the outgoing calling number is set by the ESA feature to be the incoming ANI/CLID. If the incoming trunk does not pass on an ANI/CLID, or if the ANI/CLID is invalid, then the ESA feature sets the outgoing calling number to be the ESA calling number that has been composed for the incoming trunk route. Refer to [Table 9 "ESA calling number for incoming trunk-initiated tandem ESA calls" \(page 80\).](#)

Note: Refer to ["A note on the Flexible Numbering Plan and ESA" \(page 34\)](#) when viewing these tables.

Table 12 "Calling number for incoming trunk-initiated tandem ESA call" (page 103) describes the resulting calling number that is sent.

Table 12

Calling number for incoming trunk-initiated tandem ESA call

Length of incoming ANI/CLID	Length of ESA calling number for the incoming trunk	Resulting calling number
7 or 10	Does not matter	Incoming ANI/CLID
Other than 7 or 10	7 or 10	ESA calling number for the incoming trunk
Other than 7 or 10	Other than 7 or 10	Null

Note: As per E911 requirements, the calling number for North America is expected to be 7 or 10 digits.

When the outgoing calling number is identified, the resulting calling number information that is outpulsed is described in [Table 13 "CAMA Multi frequency Compelled format of the calling number information" \(page 103\)](#).

Table 13

CAMA Multi frequency Compelled format of the calling number information

Calling number length	Calling number information
0	KP_2_ST
7	KP_0_7 digit calling number_ST
10	KP_0_10 digit calling number_ST

Calling and called number information for ESA calls routed to an ISDN trunk

This section describes the called number information for ESA calls routed to an ISDN trunk. For a system to system to Central Office (optional) to PSAP tandem scenario, the use of ISDN trunks (either PRI or ISL) is recommended. This is to allow the appropriate ESA calling number to be composed by the originating node and to be passed on by the system tandem node(s).

Called number information

When an ESA call is routed to an outgoing ISDN trunk, the ESDN is sent as the called number in the SETUP message using the existing ISDN protocol. The values for Numbering Plan Identification (NPI) and the Type of Number (TON) are defined in the called number Information Element as shown in [Table 14 "TON and NPI for the ESA called number" \(page 104\)](#).

Table 14
TON and NPI for the ESA called number

Outgoing ISDN trunk type	Numbering Plan	Type of Number	Outgoing ISDN trunk type
TIE	Private	Unknown	TIE
Others	E163 for a Lucent ESS4/ESS5 interface	Local	Others
	E.164 for all other interfaces		

Calling number information

When an ESA call is routed to an outgoing ISDN trunk, the outgoing CLID is set to be one of the following:

- For a station phone/attendant console to non-ISDN trunk ESA call, the outgoing calling number is the ESA calling number that has been composed for the station phone (refer to [Table 6 "ESA calling number composition for station phone-initiated ESA calls" \(page 78\)](#)) or attendant console (refer to [Table 8 "ESA calling number composition for attendant-initiated ESA calls" \(page 79\)](#).)
- For a trunk to ISDN tandem ESA call, the outgoing calling number is as follows:
 - If no ANI/CLID is passed in by the incoming trunk, then the outgoing calling number is set to be the ESA calling number composed for the incoming trunk route (refer to [Table 9 "ESA calling number for incoming trunk-initiated tandem ESA calls" \(page 80\)](#).)
 - If ANI/CLID is passed in by the incoming trunk, then the outgoing calling number is set to be the incoming ANI/CLID.

When the ESA outgoing calling number is identified, it is sent as the CLID in the SETUP message using the existing ISDN protocol. The values for Numbering Plan Identification (NPI) and the Type of Number (TON) are defined in the calling number Information Element as shown in [Table 15 "TON and NPI for the ESA calling number"](#) (page 105).

Table 15
TON and NPI for the ESA calling number

Calling number length	Numbering Plan	Type of Number
1-9	E163 for a Lucent ESS4/ESS5 interface	Local
	E.164 for all other interfaces	
10 or more	E163 for a Lucent ESS4/ESS5 interface	National
	E.164 for all other interfaces	

Calling and called number information for ESA calls routed to all other outgoing trunks

This section describes the called number information for ESA calls routed to all other types of outgoing trunks.

Called number information

When an ESA call is routed to any other outgoing trunk, the ESDN is sent as the called number. It is up to the far end to recognize the called number and to process it accordingly.

Calling number information

When an ESA call is routed to any other outgoing trunk, the ESA feature does not transmit a calling number, because these trunks cannot carry calling number information.

ESA enhanced routing

Background

In previous software releases, the only specification made for routing an ESA call was the ESRT (Emergency Services Route), which is configured in either the ERL table (LD 117), or from the ESA Data Block (LD 24). If the route failed then ESA would try the STEP route configured against it.

The use of ESRT to define routes for emergency calls has several limitations, as follows:

- The ESA Data Block cannot adequately define routing over IP Peer trunks, because there is no way to specify prepended routing digits to the ESDN sent across these trunks. These prepended routing digits are required for NRS resolution to a particular gateway.

- An ESA call cannot step to an Integrated Services Access (ISA) route, limiting ESA routing options in the event of ESRT failure.
- An ESA call cannot step between some route types (for example, PRI to IP Peer, and vice-versa).
- There is no way to locally terminate an ESA call without using loopback trunks.

Overview

In addition to the ESA basic routing method, an ESA advanced routing method based on the Route List Index (RLI) architecture is available. The RLI routing functionality depends on the use of packaging for Electronic Switched Network (ESN) packaging, although the configuration of Network Alternate Route Selection (NARS) / Basic Alternate Route Selection (BARS) is not required.

With RLI, a list of possible ESA routes is created. The RLI number is then specified in the basic ESA Data Block (LD 24) or the ERL table (LD 117). At this point, the system administrator can specify multiple alternate routes for ESA calls, should the main configured route fail for any reason. ESA advanced routing also removes a number of the limitations of ESA basic routing, as described previously in this section.

The basic ESA Data Block (LD 24) and the ERL table (LD 117) are mutually exclusive – one is used to the exclusion of the other. The system administrator can choose to use either one to specify RLI and ESRT based routing options, as these are made available in both.

The ESA feature implements Local Termination and Digit Manipulation (for Called Number) for use in ESA call handling. This offers an increased flexibility of routing options for use in ESA call treatment.

Digit Manipulation is required for the proper functionality of multiple ESDNs, when support for these is implemented.

There is no cascading between ESRT and RLI routing definitions. One suggestion that can be used to overcome this is to configure the last route entry in an RLI to be the same as the default ESRT route entry. Another suggestion is to make the last entry in the RLI a local termination. If both of these configuration suggestions fail, and the ESA fails to terminate, then the emergency caller receives intercept treatment.

ESA basic routing

With ESA basic routing, ESN packages and configuration are not required.

ESA enhanced routing

The alternate RLI routing facility is an advanced configuration that provides additional functionality that enables for managed alternate routing of ESA calls across different route types. This is a significant advantage over the existing ESRT / STEP route mechanism.

The routes specified in the RLI could be on different trunk types (IP Peer, PRI, and CAMA, for example). When an ESA call needs to be routed, these are stepped through until an unallocated trunk is found. This overcomes limitations imposed on STEP routing, especially the inability of configuring an ISA route as a STEP route.

Digit manipulation through Digit Manipulation Index (DMI) configurations is a supplementary functionality that can be used to modify the Called Party number to suit the needs of the network. Using this feature the digits can be either modified or completely replaced. This is useful for:

- inserting routing digits (Prepend Digits) for IP Peer routes.
- replacing the called number with the administrative number of the PSAP (for calling it directly).
- specifying DDGT for a CAMA route.
- specifying a DN for local termination.
- handling multiple ESDNs.

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

LD 86 is used to configure a list of routes into an RLI.

After an RLI has been configured with entries for all the available routes, it can be associated with an ESA block (LD 24 or LD 117).

Alternate route operation One of the main motivational factors for the implementation of the ESA enhanced routing feature is the apparent limitation of the STEP routing option to spill over calls which cannot be routed by means of the first choice ESA route specified.

ESA enhanced routing extends the option of utilizing a Route List Index (RLI) to specify a list of alternate available routes. The list also specifies the sequence of priority in which these available routes are to be used.

For example, in the 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 (that is, all the trunks in the PRI route are currently in use), the ESA call spills over to the second routing choice (IP peer route, in this example).

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

- All trunks of the preferred routing type are either busy or 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, rendering them useless for ESA routing.

A system message is generated if the actual route selected for use is not the route identified in the RLI as the first choice (RLI entry 0). The system message is a warning that the emergency call may not go to the right PSAP.

Local termination

With RLI routing, it is possible to specify that ESA calls are to be sent to an internal security desk. This may be the first and only choice available for routing in the particular enterprise environment, or the last choice in a long list of route options. Note that alternate routing does not proceed beyond a specified local termination – from a routing standpoint, the local termination is assumed to always succeed, regardless of whether it is actually successful or not.

It is recommended to locally terminate emergency calls to an ACD DN. This allows correct operation if there are multiple security agents or if they cannot immediately answer the emergency call (as might be the case with a large number of incoming emergency calls, for example).

Administration

To utilize the ESA routing flexibility provided by the RLI, all relevant configuration of RLI data and DMI (Digit Manipulation Index) data is a prerequisite.

Configuring RLI in ESA Data Block To configure an RLI in a new basic ESA Data Block (LD 24), enter no value for the ESRT prompt and enter the RLI number at the RLI prompt. This ensures that only the RLI is in effect.

Changing RLI in ESA Data Block To modify the RLI currently being referenced by the basic ESA Data Block (LD 24), enter no value for the ESRT prompt and enter the new RLI number at the RLI prompt.

To retain the current configuration, enter no value for both the ESRT and RLI prompts.

Changing RLI to ESRT in ESA Data Block To stop using an RLI in favor of an ESRT, configure the basic ESA Data Block (LD 24) with the appropriate 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 in further configurations of the basic ESA Data Block. This ensures that only ESRT is in effect.

If the ESRT is left blank and the RLI is deleted (using response 'X'), an SCH message is generated and a prompt for route information is again presented, starting with the option to enter ESRT. This functionality enables the system administrator to recover from a data entry error made when configuring ESA routing information.

Note: It is mandatory to have valid route information in the ESA Data Block. Therefore, either ESRT or RLI must be configured.

Configuring ESRT in ESA Data Block To configure an ESRT in a new basic ESA Data Block (LD 24), enter the route number for ESRT when prompted to do so. With a valid route entered at the ESRT prompt, the RLI prompt is not displayed. This ensures that only the ESRT is in effect.

Changing ESRT in ESA Data Block To modify the ESRT data existing in the basic ESA Data Block (LD 24), enter the new route number at the ESRT prompt. With a valid route entered at the ESRT prompt, the RLI prompt is not displayed. To retain the current configuration, enter no value at both the ESRT and RLI prompts.

Changing ESRT to RLI in ESA Data Block To change from an ESRT to an RLI in the basic ESA Data Block (LD 24), enter 'X' at the ESRT prompt (to remove the ESRT), and enter the RLI number at the RLI prompt. This ensures that only the RLI is in effect.

If the RLI is left blank and the ESRT is deleted (using response 'X'), an SCH message is generated and a prompt for route information is again presented, starting with the option to enter ESRT. This functionality enables the system administrator to recover from a data entry error made when configuring ESA routing information.

Note: It is mandatory to have valid route information in the ESA Data Block. Therefore, either ESRT or RLI must be configured.

Printing ESA Data Block When printing the basic ESA Data Block (LD 24), only data for the currently configured ESA route type is displayed. For example, if ESRT is defined in the basic ESA Data Block, then the RLI prompt is not displayed, and vice versa.

Configuring route in ERL table To configure a route number in the ERL table (LD 117), use the RT token in the NEW ERL command.

Configuring RLI in ERL table The token RL is added to the NEW ERL command to specify a Route List Index number in the ERL table (LD 117).

The Prepend Digits specified in this command applies to all routes specified in the RLI. All called number manipulations made by means of the DMI take effect only after the prepending of these digits occurs.

The keyword NULL may be specified in the Prepend Digits, to indicate that no routing digits are used.

Any entry in the RLI can make use of a Digit Manipulation Index (DMI) to modify the called number.

1. ESDN is set to '911'.
2. Prepend Digits adds '343' to the ESDN – the called number is now '343911'.
3. DMI removes 3 leading digits – the called number is now '911'.

The token RLI is added to the NEW ERL command, and is used to specify in the ERL table (LD 117) that RLI based routing is to be used. The Prepend Digits specified in this command applies to all routes specified in the RLI. All called number manipulations made by means of DMI take effect only after this.

Printing ERL table The PRT ERL output has columns for both ESRT and RLI. Because these fields are mutually exclusive, only one of the fields is displayed for each ERL being printed.

Changing ERL table To change an ERL from route number to RLI number, or vice-versa, enter the new values for the ERL.

System messages

SCH or ESA messages are generated if the administrator makes an error in the configuration of an ESA routing type or if there is a processing error.

Table 16
System alarms and messages for ESA 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

Message Number	Severity	Event	Corrective Action	Output
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
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	Correct the ESA routing configuration.	TTY, SNMP

Data conversion

In switching from ESRT to RLI, no data conversion is performed.

Routing behavior functions as previously.

To use the new ESA Advanced Routing functionality, the system administrator must configure new RLI and DMI entries, and switch over to these manually.

CLIDVER

The CLIDVER report is used to allow RLI routing information to be displayed. The route used in the CLIDVER report is the first route configured in the RLI that would be used to perform ESA routing. CLIDVER does not take into consideration the dynamic availability of trunks or other network resources, and therefore reports only the configuration it finds.

The called number reported is the actual number composed by the DMI for that route entry.

Determining the Called Number displayed in the CLIDVER report

For:

- ESDN: 911
- Prepend Digits: 888
- DMI Configuration: DEL 0, INS 77

If both Prepend Digits and a DMI are applied to a route with the preceding configuration, the final called number would be "888-77-911".

The CLIDVER report in its short form is similar to the existing CLIDVER output. To make the reported route data more informative, however, an additional token is reported as follows:

- 'I' means that the indicated route is from Route List Index (LD 24 or LD 117).
- 'R' means that indicated route is from ESRT (LD 24) or Route (LD 117).
- 'L' means Local Termination - there is no route to report.

The CLIDVER report in its long form includes all routing details.

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, and the ability to reach an endpoint are not considered by CLIDVER.

Changes to CLIDVER output in both the long and short forms, as discussed in the preceding sections, relates only to RLI. CLIDVER output for ESRT is unchanged in both the long and short forms.

System engineering

Configuration To make use of the ESA enhanced routing functionality, the configuration of additional RLI and DMI resources may be required, depending on the nature of each particular enterprise network.

Theoretically, every ERL entry in the ERL table (LD 117) can be provisioned with its own RLI and DMI resources. It is assumed, however, that many ERLs will share the same configured RLI and DMI resources. For example, a single remote site may have several ERL entries defined, as dictated by the size and layout of the site. All emergency calls made from any ERL at that site, however, will most likely share the same set of outgoing ESA routing options, as each individual ERL will not likely have specific trunks dedicated for its exclusive use. Therefore, as the trunks are shared commonly, so too are the RLI and DMI resources that govern ESA routing using those trunks.

Nonetheless, care must be taken to ensure that sufficient RLI and DMI resources are provisioned, and so resource usage must be monitored while configuring ESA enhanced call routing (to ensure that required ESA routing takes place as needed).

Packaging The ESN package is required for ESA enhanced routing, and may be configured with either the Basic Alternate Route Selection (BARS) or Network Alternate Route Selection (NARS) routing algorithm. The valid RLI and DMI value ranges for each of these routing algorithms is as follows:

- Using Basic Alternate Route Selection (BARS), RLI values can range from 0 to 127 and DMI values can range from 1 to 255.
- Using Network Alternate Route Selection (NARS) without the Flexible Number Plan (FNP) package, RLI values can range from 0 to 255 and DMI values can range from 1 to 255.
- Using Network Alternate Route Selection (NARS) with the Flexible Number Plan (FNP) package equipped, RLI values can range from 0 to 999 and DMI values can range from 1 to 999.

Emergency call routing

A Call Server can be configured to provide emergency call handling service to IP phones across multiple emergency jurisdictions. As a matter of best practice, the emergency call should be routed to a service at the phone's current location, as the PSAP for that location would be the most appropriate one to respond.

An emergency call should be handled by the designated means for the current phone location – it may be routed internally (to be handled by an internal responder, for example, such as a designated security desk) or externally (routed directly to the external PSAP).

PSTN routing: Enhanced 911 versus Basic 911

With Enhanced 911 (E911), multiple emergency service zones are connected by an E911 Tandem system. When an emergency call is made from any of these emergency service zones, it is routed by the PSTN to the E911 Tandem, which contains a Selective Router.

The Selective Router looks up the caller ANI in its Selective Routing database (which is synchronized with the ALI database at the PSAP) to determine the correct PSAP for the emergency caller. The emergency call is then routed to the appropriate PSAP using PSTN. The emergency call, can be routed to any Central Office in the correct E911 Tandem area - the Selective Router automatically routes the call to the appropriate PSAP based on the ANI of the caller.

In call environments that only support Basic 911, the route to the PSAP is determined by the PSTN access point, and the emergency call must be routed to the Central Office nearest the caller.

With ESA, system administrators can specify a PSTN route for each configured ERL, which meets the more stringent requirement of Basic 911. In areas where there is support for Enhanced 911, system administrators have more flexibility in specifying how emergency calls are routed to the PSTN.

Internal routing

Currently, there is no industry standard in place that governs the routing of an emergency call to a PSAP (or for delivering an ANI). The approach used by ESA involves tandem routing an emergency call originating from a remote IP phone to a gateway local to the caller's location. This gateway may be a Call Server, Branch Office, or other enterprise PSTN gateway, and is defined as being local if it is in the same E911 Tandem area or PSAP Emergency Service Zone as the emergency caller.

If there is a gateway located in the same emergency jurisdiction as the caller, then the emergency call can be internally routed by tandem to that gateway. Upon reaching the gateway, the incoming ESA call can be routed over the local emergency trunk to the PSAP. In this way, the emergency call is routed to a trunk that connects to the PSTN in the correct emergency jurisdiction (which can route to the PSAP nearest the caller).

If there is a single call server or gateway providing emergency handling for the current location of the emergency caller, then the call should be tandem routed to that call server or gateway.

In the case of there being multiple call servers or gateways local to the caller's location, the emergency call can be routed to any of them, as they should all be configured to handle emergency calls in a similar fashion (for that location).

On-Site Notification

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 Meridian 1 proprietary phone with display. The maintenance device and OSN phone are independent of one another, and can be configured together, or one without the other (MTC is entered in response to the USER prompt in LD 17).

When an emergency call is placed, the On-Site Notification function automatically broadcasts an On-Site Notification call record to the output devices. If the History File (ADAN = HST in LD 17) is configured as a maintenance device, then the OSN call record will be saved in the History File.

On-Site Notification output device print

Call record for a station phone-initiated ESA call

Figure 2 "OSN call record print for an attendant console-initiated ESA call" (page 118) illustrates the call record printed on the OSN output device for a station phone-initiated ESA call. See Table 17 "Description of call record fields" (page 116) for a description of call record fields.

Note: This output can be used by third-party vendors to create a PC application that would filter out any data not pertaining to ESA. In turn, this application could then be run on a system equipped with the ESA feature.

Figure 1
OSN call record print for a station phone-initiated ESA call

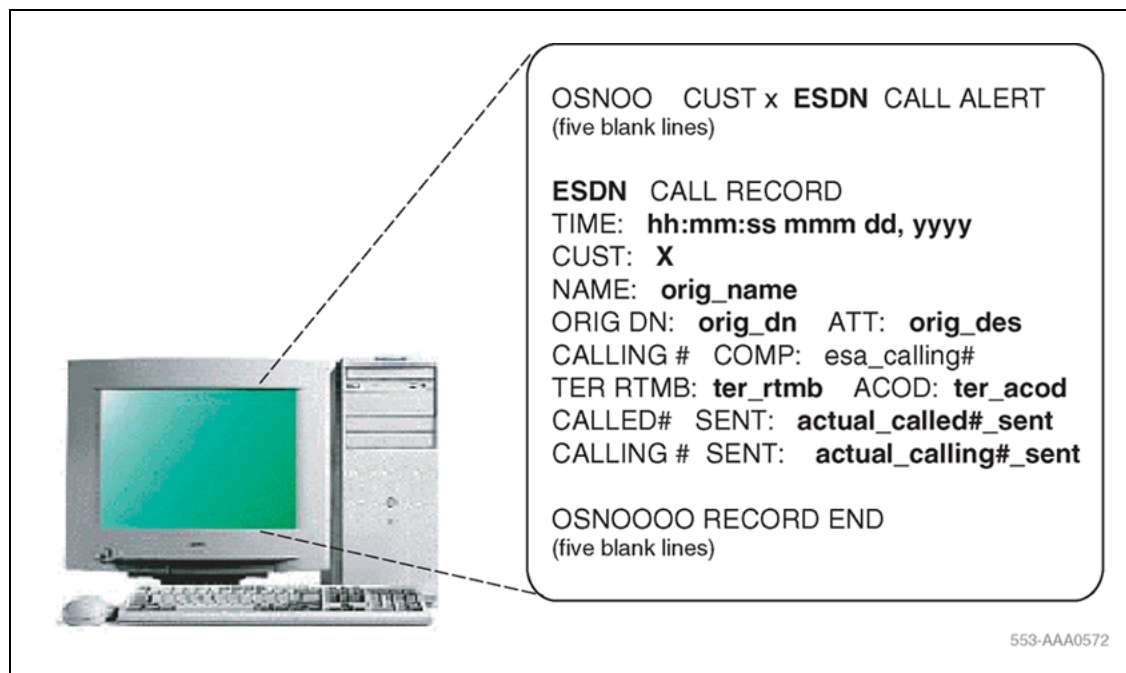


Table 17
Description of call record fields

Field	Description
X	The customer number, as defined using the CUST prompt in LD 10, LD 11, or LD 27.
ESDN	The customer Emergency Services Access DN, as defined using the ESDN prompt in LD 24.
hh:mm:ss	The 24-hour time stamp of when the call was made (hour, minute, and second).
mmm dd yyyy	The date stamp of when the call was made (month, day, and year).
orig_name	The name associated with the originating DN ¹ , as defined using the NAME prompt in LD 95.
orig_dn	The DN associated with the originating phone.
1. The system must be equipped with the Calling Party Name Display (CPND) package 95 to print the originating name. 2. The system must be equipped with the Office Date Administration System (ODAS) package 20 to print the phone designator.	

Field	Description
esa_calling#	The calling number composed by the ESA Call Termination Identification function, for the originating station phone.
orig_des	The phone designator ² of the originating station phone.
ter_rtmb	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	The route access code of the outgoing trunk on which the ESA call terminated.
actual_called#_sent	The called number that was sent.
actual_calling#_sent	The calling number that was sent.
1. The system must be equipped with the Calling Party Name Display (CPND) package 95 to print the originating name. 2. The system must be equipped with the Office Date Administration System (ODAS) package 20 to print the phone designator.	

Call record for an attendant console-initiated ESA call

Figure 2 "OSN call record print for an attendant console-initiated ESA call" (page 118) illustrates the call record printed on the OSN output device for an attendant console-initiated ESA call. Table 18 "Description of call record fields" (page 118) shows a description of call record fields.

Figure 2
OSN call record print for an attendant console-initiated ESA call

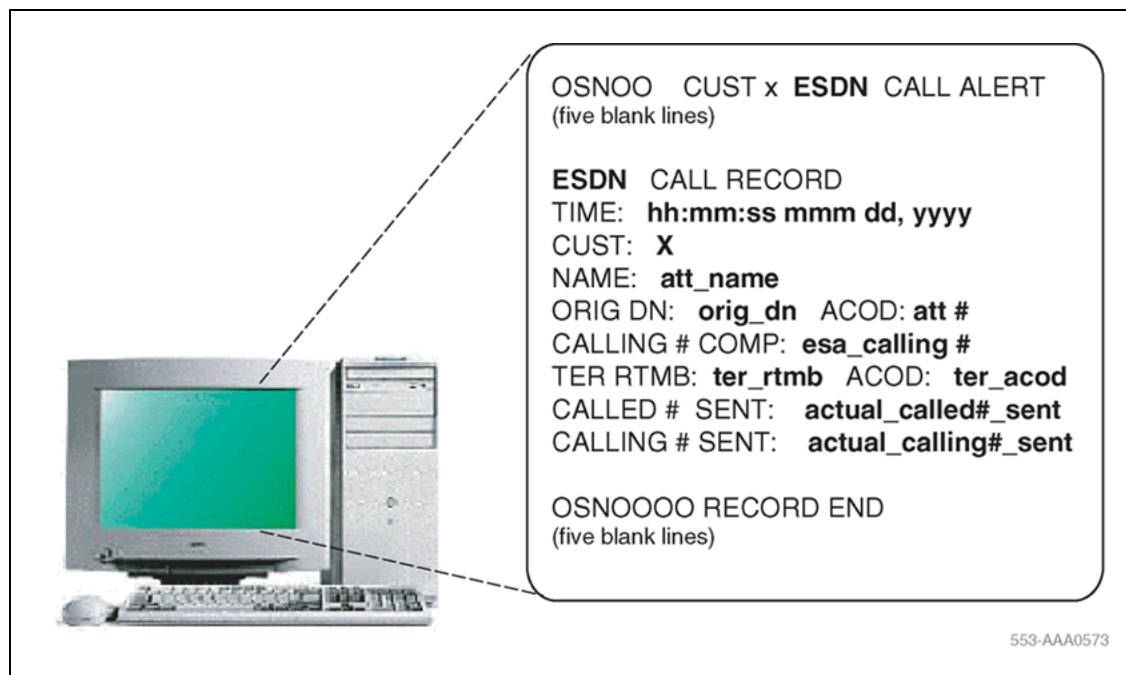


Table 18
Description of call record fields

Field	Description
X	The customer number, as defined using the CUST prompt in LD 12.
ESDN	The customer Emergency Services Access DN, as defined using the ESDN prompt in LD 24.
hh:mm:ss	The 24-hour time stamp of when the call was made (hour, minute, and second).
mmm dd yyyy	The date stamp of when the call was made (month, day, and year).
att_name	The name associated with the attendant DN ¹ , as defined using the NAME prompt in LD 95.
orig_dn	The attendant DN, as defined using the ATDN prompt in LD 15.
attn#	The attendant number, as defined using the ANUM prompt in LD 12.
1. The system must be equipped with Calling Party Name Display (CPND) package 95 to print the originating name.	

Field	Description
esa_calling#	The calling number composed by the ESA Call Termination Identification function, for the originating attendant console.
ter_rtmb	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	The route access code of the outgoing trunk on which the ESA call terminated.
actual_called#_sent	The called number that was sent.
actual_calling#_sent	The calling number that was sent.
1. The system must be equipped with Calling Party Name Display (CPND) package 95 to print the originating name.	

Call record for an incoming trunk-initiated tandem ESA call

Figure 3 "OSN call record print for an incoming trunk-initiated tandem ESA call" (page 120) illustrates the call record printed on the OSN output device for an incoming trunk-initiated tandem ESA call. Table 19 "Description of call record fields" (page 120) shows a description of call record fields.

Figure 3
OSN call record print for an incoming trunk-initiated tandem ESA call

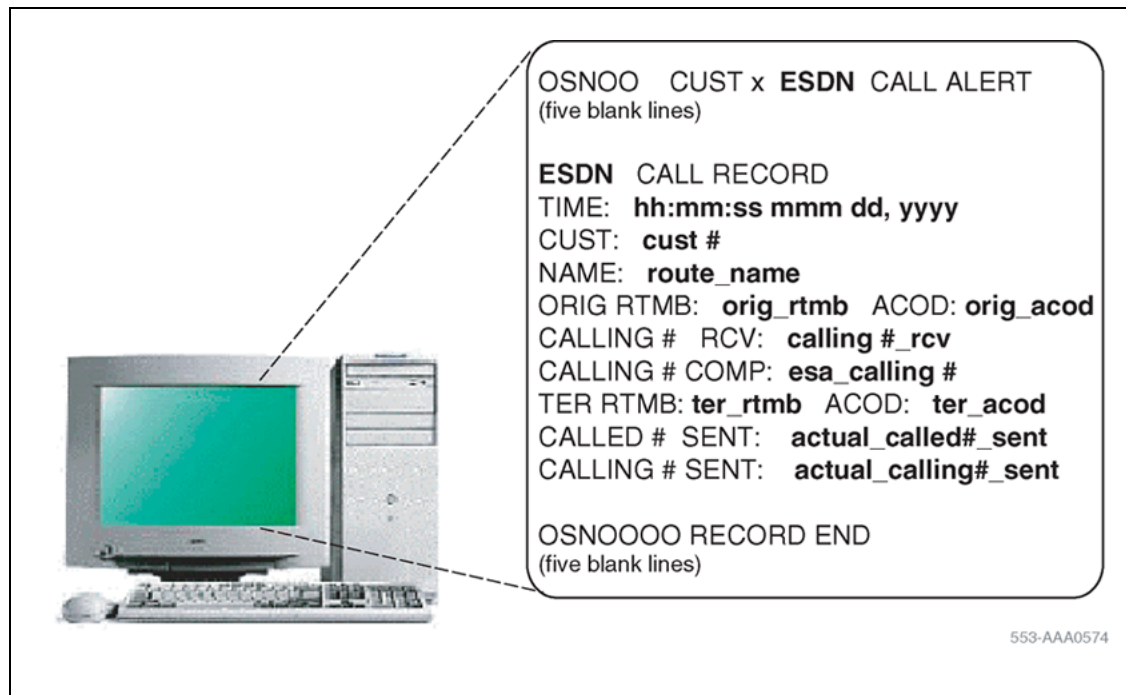


Table 19
Description of call record fields

Field	Description
X	The customer number, as defined using the CUST prompt in LD 12.
ESDN	The customer Emergency Services Access DN, as defined using the ESDN prompt in LD 24.
hh:mm:ss	The 24-hour time stamp of when the call was made (hour, minute, and second).
mmm dd yyyy	The date stamp of when the call was made (month, day, and year).
route_name	The name associated with the incoming trunk route ¹ , as defined using the NAME prompt in LD 95.
orig_rtmb	The route and member number of the incoming trunk, as defined using the RTMB prompt in LD 14.
1. The system must be equipped with the Calling Party Name Display (CPND) package 95 to print the originating name.	

Field	Description
orig_acod	The route access code of the incoming trunk on which the ESA call was initiated, as defined using the ACOD prompt in LD 16.
calling#_rcv	The calling number that was received from the incoming trunk.
esa_calling#	The calling number composed by the ESA Call Termination Identification function, for the incoming trunk route.
ter_rtmb	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	The route access code of the outgoing trunk on which the ESA call terminated, as defined using the ACOD prompt in LD 16.
actual_called#_sent	The called number that was sent.
actual_calling#_sent	The calling number that was sent.
1. The system must be equipped with the Calling Party Name Display (CPND) package 95 to print the originating name.	

Provisioning an ESA On-Site Notification phone

A Meridian 1 proprietary display phone may be designated as an On-Site Notification phone (only one OSN phone can be configured per customer). The phone is provisioned with an On-Site Notification (OSN) key, using the KEY prompt in LD 11. The OSN key can only be used to display ESA caller information. It cannot be used to make or receive a call.

A single appearance station DN on the OSN phone is designated as the customer's On-Site DN using the OSDN prompt on LD 24. This OSDN is used by the On-Site Notification function to locate and alert the OSDN phone that an ESA call has taken place.

The following events also take place when an ESA call is detected:

- The caller information is copied into a separate memory block (call register).
- The OSN key lamp begins to flash.
- The OSN buzzing is activated for 10 seconds.

OSN phone considerations

The OSN phone display feature is intended for small installations, where cost is a major factor, and 911 calls are likely to be infrequent. Accordingly, the following limitations should be noted:

- Only one OSN Phone can be defined per customer.

- Only one ESA call can be handled at a time. Calls cannot be queued for the OSN Phone. The second and subsequent simultaneous calls will not be notified, even if the first call information is cleared while the second call is in progress.
- ESA information must be cleared off the OSN phone manually, before another ESA call information can be presented. This is to prevent successive (often related) emergency calls from "rippling" across the phone before the operator has a chance to properly process them.

ESA Call Answering

The OSN function does not answer the ESA call; the call continues to the ESA trunk and the PSAP normally. Similarly, the OSN phone operator cannot monitor the call directly.

If call monitoring is required, and allowed, the OSN phone can dial the originating 911 caller's number and perform an override. This will form a conference between the caller, the PSAP, the OSN phone, and a warning tone.

Note: Some jurisdictions do not allow this kind of conference, and many public safety officials disapprove of it, so check carefully before implementation.

It is also possible to route the outgoing trunks back into the system and answer them internally, rather than routing to the PSAP. Refer to the section "[Standalone configuration \(on-site call answering\)](#)" (page 160) for details. It is also possible to combine the answering phone with the OSN function. This will, however, require the OSN phone user to be careful in his operating procedures to avoid losing the ESA information. It is definitely not recommended in large installations; in these, the SDI Port output would form the basis of OSN display.

The following sections contain information pertaining to the OSN phone displays. For details about OSN phone operation (how to view and discard the caller information) and key lamp states, refer to the section "[Feature operation](#)" (page 189).

OSN phone displays

OSN phone display for a station phone-initiated ESA call

[Figure 4 "OSN phone display for a station phone-initiated ESA call"](#) (page 123) illustrates the OSN phone display for a station phone-initiated ESA call. [Table 20 "Description of call record fields"](#) (page 123) shows a description of call record fields.

Figure 4
OSN phone display for a station phone-initiated ESA call

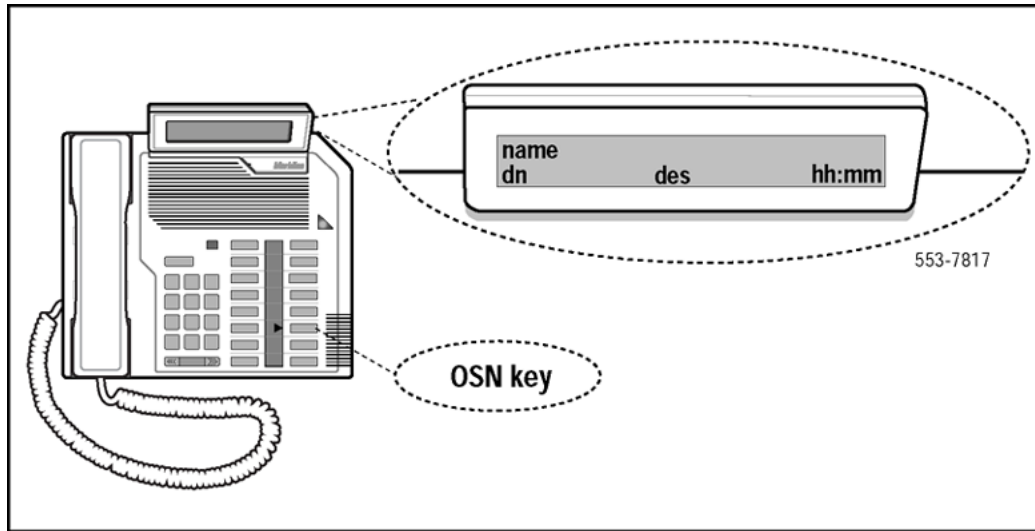


Table 20
Description of call record fields

Field	Description
name	The name (as defined using the NAME prompt in LD 95) associated with the originating DN ¹ .
dn	The originating DN.
des	The phone designator ² of the originating phone (as defined using the DES prompt in LD 10, LD 11, or LD 27).
hh:mm	The 24-hour time stamp of when the ESA call was made.
1. The system must be equipped with the Calling Party Name Display (CPND) package 95 to display the originating name. 2. The system must be equipped with the Office Data Administration System (ODAS) package 20 to display the phone designator.	

OSN phone display for an attendant-initiated ESA call

Figure 5 "OSN phone display for an attendant console-initiated ESA call" (page 124) illustrates the OSN phone display for an attendant-initiated ESA call. A description of the fields follows. Table 21 "Description of call record fields" (page 124) shows a description of call record fields.

Figure 5
OSN phone display for an attendant console-initiated ESA call

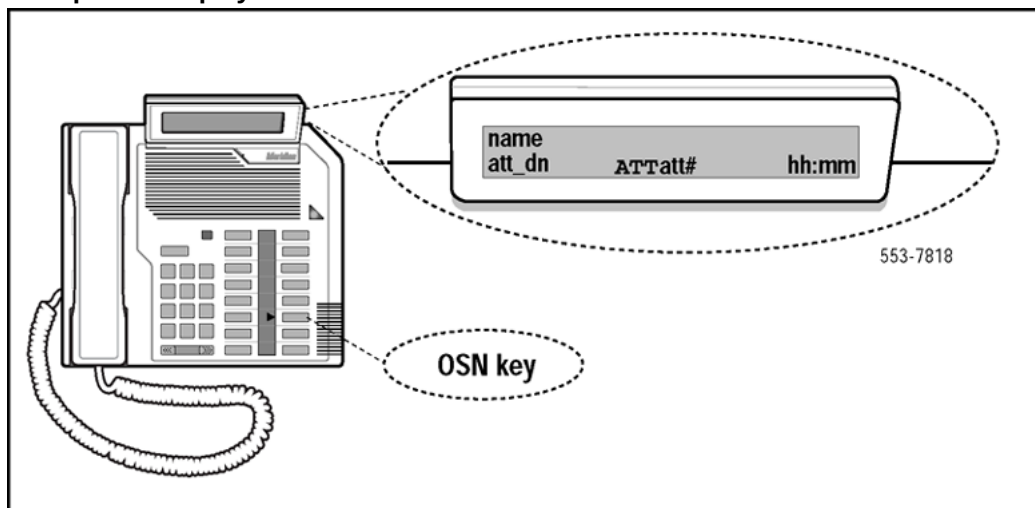


Table 21
Description of call record fields

Field	Description
name	The name (as defined using the NAME prompt in LD 95) associated with the attendant DN ¹ .
attn_dn	The attendant DN (as defined using the ATDN prompt in LD 15).
ATTatt#	The attendant number of the originating attendant console (as defined using the ANUM prompt in LD 12).
hh:mm	The 24-hour time stamp of when the ESA call was made.
1. The system must be equipped with the Calling Party Name Display (CPND) package 95 to display the originating name.	

OSN phone display for an incoming trunk-initiated tandem ESA call

Figure 6 "OSN phone display for an incoming non-ISDN trunk-initiated tandem ESA call" (page 125) illustrates the OSN phone display for an incoming trunk-initiated tandem ESA call. Table 22 "Description of call record fields" (page 125) shows a description of call record fields.

Figure 6
OSN phone display for an incoming non-ISDN trunk-initiated tandem ESA call

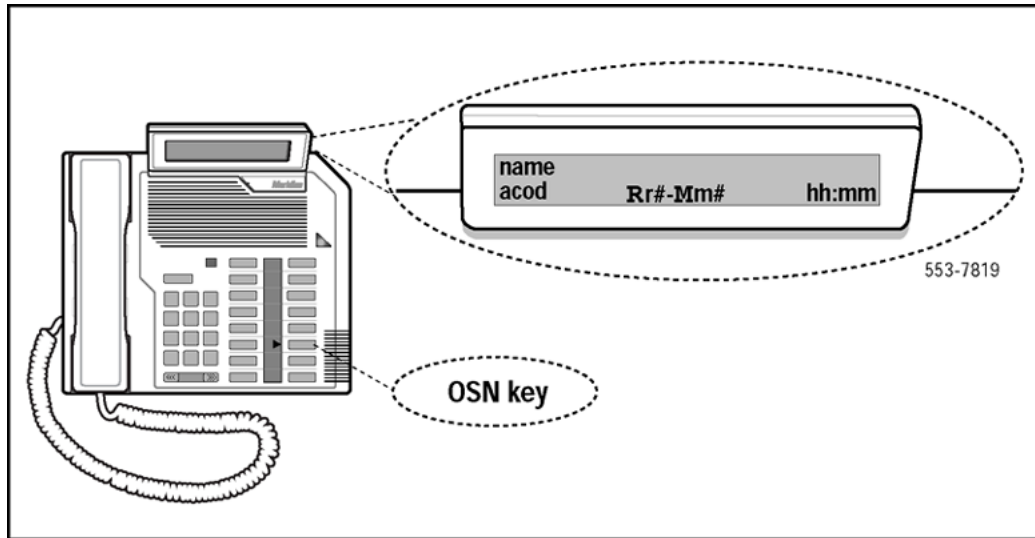


Table 22
Description of call record fields

Field	Description
name	The name (as defined using the NAME prompt in LD 95) associated with the attendant DN ¹ .
acod	The route access code of the incoming trunk (as defined using the ACOD prompt in LD 16).
Rr#-Mm#	The route and member number of the incoming trunk (as defined using the RTMB prompt in LD 14).
hh:mm	The 24-hour time stamp of when the ESA call was made.
1. The system must be equipped with the Calling Party Name Display (CPND) package 95 to display the originating name.	

OSN TTY

The ESA feature prints OSN system messages by means of the TTY output message type, **OSN**.

With ESA, it is practical to have a dedicated output device (a printer, for example) to handle generated OSN messages. A dedicated OSN TTY may alleviate the requirement for OSN phones, and may also increase the performance of a third party OSN alerter, as this will no longer have to parse other (irrelevant) message types.

ESA related processing errors (ESAx) are printed only on MTC terminals. It is reasonable that these are not printed to the OSN terminal, because they indicate a problem at the system level (configuration problems, for example), which only a system administrator should be aware of. Security personnel only need to be made aware of alerts directly relating to emergency calls, and so should not be alerted every time an administrative alert is generated. Therefore, printing ESA related processing errors only on MTC terminals prevents unnecessary alerts from being sent to the security personnel, and also keeps system level messages more private than the OSN terminal might otherwise be.

Multiple TTYs can be configured to display OSN outputs generated by the system - this enables for the deployment of TTYs at remote locations. If multiple TTYs are configured on a system, they will all print OSN messages that the system generates. That is, if an emergency call is placed anywhere within the system, it is reported on every TTY installed on that system, remote or otherwise – this potentially increases system wide awareness of an emergency in a more efficient and automated fashion.

Note: An OSN TTY is deployed independently of an OSN phone, and will function in different way. The key functional difference between the two is that an OSN TTY prints all OSN system messages, while OSN phones may display only those events that occur in their associated location .

Data conversion

To maintain functionality from earlier system versions, data conversion for OSN TTY occurs as detailed by the following:

- All TTYs that had output message type MTC acquire output message type OSN. The system administrator can remove output message type OSN later from the original MTC TTYs, if desired.
- All HST TTY that had output message type MTC will be data converted to OSN + MTC.

OSN phone display enhancement

Background

A Meridian or Succession display phone may be configured to function as an On Site Notification (OSN) phone. In doing so, the display phone is provisioned with an OSN key that is used to display ESA caller information. The caller information itself is displayed according to which ESA call type is being made - there are three possible ESA call types, as follows:

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

There are only two lines available on the phone display to use in presenting ESA caller information. Therefore, the presented ESA caller information is designed to be compact in appearance, as well as informative enough to allow on site emergency personnel to identify the emergency caller.

In the case of an incoming trunk initiated (tandem routed) ESA call, however, the incoming trunk information is displayed on the OSN phone, and is not very useful in identifying the specific emergency caller and, worse, may even confuse the emergency staff.

A common type of incoming trunk initiated ESA call is one from a Branch User registered at the Main Office. In this case, the ESA call is routed back to the Branch Office so that it can then be sent to the PSAP serving the Branch Office. To display the caller information in this case, the OSN phone at the Branch Office must be in Local Mode, as the emergency call is ultimately routed to the PSAP by the local call server at the Branch Office.

Network wide phone mobility scenarios, including Virtual Office, also results in an incoming trunk initiated (tandem routed) ESA call.

Overview

For the displayed emergency caller information to be useful for the on site personnel, it must be useful in identifying the emergency caller - therefore, the OSN phone display for trunk initiated emergency calls includes the emergency caller's name and CLID, which are displayed instead of trunk information.

The display character restrictions imposed on the OSN phone display are as described as follows:

- Name can be as many as 16 characters, and will be truncated if necessary.
- ESDN can be as many as 7 characters.
- CLID can be as many as 16 characters.
- RTMB can be as many as 9 characters
- DES is up to 6 characters.
- ATT is set to 5 characters.
- HH:MM is set to 5 characters.

Operation

First line of display If the emergency caller's name (CPND Name), composed at the originating node, is carried across the trunk, then it is printed in the first line of the display. The emergency caller's ESDN is presented in the first line as well, beside the caller's name. If these are not available, then the incoming trunk route name is printed instead.

Note: In a Branch User / Main Office scenario, the caller's name is configured on the Main Office. It is the system administrator's responsibility to maintain the Main Office and Branch Office user configurations, so that the correct caller name is displayed.

If neither the caller name nor the trunk route name are available then a language-specific string "Not Available" is printed. This is to notify the on-site personnel that there is no valid name data available. (Previously, nothing was printed. (The language is selected on a Meridian / Succession telephone by means of its options menu.)

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

1. Emergency caller's name, or
2. Incoming trunk route name, or
3. "Not Available".

The caller's name or trunk route name is displayed on the OSN phone even if the CPND package (95) is restricted. In this case, however, the OSN record does not display name.

The OSN CPND display overrides the CPND package restriction and the DDGD (DN display on other set Denied) class of service on the emergency caller's phone.

DPNSS trunks The following describes the behavior of emergency call handling over a DPNSS trunk.

In order for an emergency call to be placed over a DPNSS trunk, it is required that an Originating Line Identity (OLI) string (the caller's CLID) be sent along with the call, otherwise emergency call handling fails.

To ensure proper treatment of the emergency call, the originating node uses the caller's DN as the OLI string if no ESA CLID is composed. In the event that the caller's DN is used as the OLI string (instead of the ESA CLID), a system message (ERRxxxx) is generated to report this configuration error.

Because the originating node passes along the emergency call with a valid OLI (CLID), it is passed through directly to the PSAP or local security desk responder when it reaches the tandem node. If the OLI (CLID) for the call is the caller's DN, however, then it may not be a valid PSTN number (which is used for determining route, for ALI lookup, and for PSAP callback). Subsequently, if the emergency call is routed to the PSTN, then the OLI (CLID) will not be recognized and default PSAP routing will be used for the emergency call. If the emergency call routes to a security desk (instead of directly to the PSAP), then the attendant may be unable to automatically identify the caller.

In the end, the second line of the OSN phone display for an emergency call on a DPNSS trunk shows (in order of preference):

1. Emergency caller's CLID, or
2. Emergency caller's DN.

The rest of the second line display functionality for the OSN phone is unchanged.

Note: The lack of an ESA CLID reflects a scenario in which ESA has not been configured as intended by the feature design. Emergency call handling as just described, therefore, is not the optimal scenario for emergency call handling, but is better than the emergency call receiving an intercept treatment, as it does route the emergency call to either the PSAP or security desk responders. Ideally, an ESA CLID should be generated for the emergency call to provide the best call handling possible.

OSN record The OSN record for a trunk-initiated ESA call automatically prints the caller's name instead of the trunk route information, as on the OSN phone.

Supported trunks

This enhancement prints Caller Name and Caller CLID for any incoming trunk-initiated ESA call where the trunk carries CPND and CLID. This includes:

- PRI and PRI2 (ISDN).
- DPNSS (CLID only).
- H.323 virtual trunk.
- SIP virtual trunk.
- CAMA (Caller ANI only).

The following route types are valid for ESA calls:

- TIE
- Autovon (ATV)
- Centralized Automatic Message Accounting (CAMA)
- Central Office (COT)
- Direct Inward Dial (DID)
- Foreign Exchange (FEX)
- Wide Area Telephone Service (WATS)
- Integrated Digital Access (IDA)

OSN record / SNMP trap

Background

SNMP traps generated from the Call Server use the *commonMIBAlarmData* variable binding to describe the event. This variable binding contains both a general and detailed description and can contain up to 750 bytes of data. The *commonMIBErrCode* variable binding will contain "OSN000" for these traps.

For more information on the Common Trap MIB format refer to the *Communication Server 1000 Fault Management - SNMP NTP* (NN43001-719).

Operation

All emergency call events are presented using specific caller location data and are carried by means of the variable binding contained within the SNMP trap. ESA call record and SNMP traps divide the event descriptions into two parts – one for the general description of the event, and the other for more detailed information with which the event can be more specifically analyzed to identify the calling party. As described previously, the general and the detailed description of the emergency call event is carried by the *commonMIBAlarmData* variable binding.

The general description part of the ESA record is presented to avoid any ambiguity in understanding the nature of the emergency call event - the emergency responder must be able to read the general description record and understand that an immediate response is required.

The detailed description of the ESA call provides specific calling party information, which allows the caller's location to be more easily determined.

The OSN record does not display ECL information, which could be used to look up a detailed location record on the DM. It is suggested, therefore, that the ANI be used instead when looking up caller location, as would be done by the PSAP.

Other notifications Other emergency event notification methods such as strobes, pagers, email, and IM, may be provided by a 3rd party external application such as Telident Site Alert. The actual event notification capabilities depend on the particular software used.

Site Alert processing is triggered by the OSN record generated on the CS 1000. Site Alert can possibly look up additional caller or location data based on the provided OSN data.

OSN record for a station phone initiated ESA Call

This section provides a description of the OSN record for an emergency call initiated by a station phone, as shown by the following:

Table 23

OSN000 commonMIBAlarmData for a station phone initiated ESA call

```
CUST cust# esdn CALL ALERT
TIME: hh:mm:ss mmm dd, yyyy
NAME: orig_name
ORIG DN: orig_dn
SITE: orig_site
LOC: orig_loc
;;
DES: orig_des
SET: orig_set
ERL: erl
TER RTMB: ter_rtmb ACOD: ter_acod
CALLED#: called#_dialed
CALLING#: calling#_sent
OSN000 RECORD END
```

Where:

- 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. This is taken from the ERL table, if the ERL is not set to zero - otherwise, orig_site is blank.
- orig_loc is the Location Description of the caller, taken from the TN Table if the phone is set to Auto Update IP. If the phone is not set to Auto Update, orig_loc provides the ERL description of the caller, taken from the ERL table, if the ERL is not set to zero - otherwise, orig_loc is blank.
- orig_des is the telephone designator of the originating station phone taken from its TNB.
- orig_set is the phone type of the emergency caller taken from LD 10, 11, 12, or 27.

- erl is the 16 bit number that corresponds to the ERL of the phone.
- 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 is call terminated.
- called#_dialed is the number that was actually dialed by the emergency caller.
- calling#_sent is the calling number actually sent.

OSN record for an attendant console initiated ESA call

The section provides a description of the OSN record for an emergency call initiated by an attendant console, as shown in the table that follows:

Where:

Table 24

OSN000 commonMIBAlarmData for an attendant console initiated ESA call

CUST cust# esdn CALL ALERT TIME: hh:mm:ss mmm dd, yyyy ORIG DN: orig_dn NAME: att_name SITE: orig_site LOC: orig_loc ;; ATT: att# ERL: erl TER RTMB: ter_rtmb ACOD: ter_acod CALLED#: called#_dialed CALLING#: calling#_sent OSN000 RECORD END
--

- att_name is the name associated with the attendant DN, as defined using the NAME prompt in LD 95.
- att# is the attendant number, as defined using the ANUM prompt in LD 12.

OSN record for an incoming trunk initiated ESA call

The section provides a description of the OSN record for an incoming trunk initiated ESA call, in the table that follows:

Table 25

OSN000 commonMIBAlarmData for an incoming trunk initiated ESA call

```
CUST cust# esdn CALL ALERT
TIME: hh:mm:ss mmm dd, yyyy
NAME: caller_name
ORIG RTMB: orig_trmb ACOD: orig_acod
CALLING# RCV: calling#_rcv
;;
CALLING# COMP: esa_calling#
TER RTMB: ter_rtmb ACOD: ter_acod
CALLED#: called#_dialed
CALLING#: calling#_sent
OSN000 RECORD END
```

Where:

- 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. This is an existing functionality.
- calling#_rcv is the ANI (CLID) of the original caller, as received from the incoming trunk.
- esa_calling# is the calling number composed for the originating station phone by the ESA Call Termination Identification function.
- 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.

Note 1: If there is a calling number received from the incoming trunk (calling#_rcv) and it is valid, then this 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 2: 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 be locally terminated using ESA enhanced routing. The commonMIBAlarmData variable binding of the OSN record identifies this scenario, as in the following:

Table 26**OSN000 commonMIBAlarmData for a locally terminated ESA call**

<pre>;; DES: orig_des SET: orig_set ERL: erl LTER DN: lter_dn</pre>

Where:

- lter_dn is the DN to which the ESA call locally terminates, as specified by the RLI and DMI.

Configuration

There is no configuration that can be used to control the OSN record.

The OSN record is printed to all TTYs with output message type “OSN”.

The OSN000 SNMP trap is sent to all hosts specified by the OPEN_ALARMS parameter on the Call Server (LD 117).

If the CPND package (95) is restricted, then the Caller Name and the Route Name are not displayed. In this case, the OSN phone does display Name.

OSN phone per ERL

As part of the functionality of the EAS feature, multiple OSN phones can be defined on a single system by the configuration of OSN phone per ERL, giving the system administrator more flexibility in emergency call notification setup.

A summary of OSN phone functionality and rules of use are as follows:

- The OSN function does not answer an incoming ESA call, and an OSN phone operator cannot monitor the emergency call directly.
- When a DN has been designated as the OSN Directory Number (OSDN), it is up to the system administrator to maintain the database so that the OSDN remains valid.
- Only a Meridian 1 / Succession proprietary display phone can be an OSN phone.

- The OSDN must be a valid single appearance internal DN that belongs to a Meridian 1 / Succession proprietary telephone, which is configured with an OSN key.
- ESA calls cannot be queued for the OSN phone.
- ESA information displayed on the OSN phone must be cleared manually, before information for another ESA call can be displayed.

Operation

The ERL table allows the configuration of an optional OSN Phone DN (OSDN) for each individual ERL. That is, each ERL can now specify a particular OSN phone on which to display caller information for any emergency call made from that ERL.

When an emergency call is made, the emergency caller's ERL data is retrieved from either their TN Table record (if an IP phone) or their TNB (if a non IP phone). If an OSDN has been configured for the indicated ERL, in either the ERL table (LD 117) or the Basic ESA Data Block (LD 24), then the configured OSDN is used for the display of the emergency call information.

If an OSDN is not configured in either the ERL table or ESA Data Block then no particular OSN phone is signaled.

Configuration

The OSDN configured in the ESA Data Block (LD 24) is retained for default or fallback OSN phone display purposes. Some scenarios in which the default or fallback OSDN will be used include the following:

- Operation after the upgrade is configured to be the same as before the upgrade (this is the situation immediately after the upgrade has occurred and new configurations have not been made, for example).
- The system administrator has not configured an OSDN for a particular ERL.
- The location of the IP phone is unknown, or is configured as ERL 0.
- The emergency call is a trunk initiated (tandem) ESA call.

Configuring OSDN against each ERL is optional and is done through LD 117. The OSDN in the Basic ESA Data Block is still provisioned through LD 24.

System messages

Existing OSN and ERR messages are printed for ERL information as the error condition is met. The ERL number is printed only when it is applicable.

OSN001 When ESA call information is linked onto the OSN key, no other call information can be linked onto the OSN key until the current one is discarded.

If the call information cannot be linked onto the OSN key because another call information is linked to it, a warning message, OSN0001, is generated.

OSN002 If the call information cannot be linked onto the OSN key because the OSN phone is found to be disabled, a warning message OSN0002 is generated.

OSN005 During an emergency call, if an invalid DN is designated to be the OSDN for an ERL, then the call information is not linked and the error message OSN005 is generated.

OSN006 During an emergency call, if the phone specified by the OSDN is not configured with an OSN key then the call information is not linked and the error message OSN006 is generated.

On Site Notification

All call servers involved in handling an emergency call can print OSN data, including:

- Originating Call Server
- Tandem Call Server(s), if any, and
- Terminating Call Server (or Trunk Gateway).

Multiple OSN TTYs can be configured to provide remote notification.

OSN phone per ERL can be used for remote notification.

Tandem OSN

A Branch User (registered at the Main Office) making an ESA call results in a tandem ESA call at the Branch Office (so that the call can go to the PSAP serving the BO).

Alternatively, put the OSN phone for the ERL at the Branch Office (registered at the Main Office). The OSN phone will then provide indication of the ESA call.

ESA Misdial Prevention

Overview

The ESA Misdial Prevention feature provides system administrators the ability to prevent ESA calls being accidentally misdialed. For example, if an ESDN is dialed with extra trailing digits, the normal assumption would be that the caller was trying to dial a different number than the ESDN, and therefore

would not be handled appropriately as an emergency call. With the ESA Misdial Prevention feature, however, an ESDN is recognized for what it is, even if it is dialed with trailing digits. When a misdialled ESDN is identified, it is intercepted by the Misdial Prevention feature, but is not routed to the PSAP – instead, the caller receives 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 an indication of an ESA misdial.

Implementation of the ESA Misdial Prevention feature has the direct consequence of delaying all normally dialed emergency calls prior to being routed to the PSAP. The default value of this enforced delay is 2 seconds. Pressing the octothorpe key (“#”) after dialing the ESDN, however, results in the call being routed immediately, without a delay. For example, if the ESDN is set to 9-1-1, then dialing 9-1-1- # results in the call being placed without delay.

There are three types of ESA calls:

1. Station phone initiated ESA call.
2. Attendant initiated ESA call.
3. Incoming trunk (ISDN & non-ISDN) initiated (that is, tandem) ESA call.

The ESDN dialing delay is only applicable to station phones making an ESA call - no dialing delay occurs for attendant initiated ESA calls, BRI set initiated ESA calls, or for non ISDN and ISDN trunk initiated ESA calls at the tandem node.

The ESA Misdial Prevention feature is configurable per ESDN entry.

Operation

ESA call

When a recognized ESDN is dialed, a configurable delay timer (2 seconds by default) is started. If the delay timer expires and no additional digits have been entered, then the call is processed as an ESA call and is routed to the appropriate PSAP. Also, if the octothorpe key (“#”) is pressed within the delay period then the call is immediately processed as a normal ESA call.

Misdialed call

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

The intercept treatment provided for the misdialled ESA call is configured by the system administrator.

On Site Notification

When an ESA call is intercepted, the On Site Notification (OSN) telephone is alerted as it would be with an actual ESA call. The assumption should be made that a call intercepted by the ESA Misdial Prevention feature could be an actual emergency and should be followed up by local emergency personnel.

A Misdialed Call Alert message (OSN004) is printed on all system OSN terminals for each intercepted call. This message is similar to the OSN000 Call Alert message that is used for notification in the case of an actual emergency call.

The actual intercept treatment applied to the misdialled ESA call is identified in the OSN004 record. The possible intercept treatments are as follows:

- OVERFLOW
- BUSY
- ATTENDANT
- RAN ROUTE xxx

When the emergency call is routed after the configured delay (or if the octothorpe is pressed during the delay period), the regular Call Alert message (OSN000) is printed on all OSN terminals, system wide.

Allow Last Digit Repeat

Allow Last Digit Repeat is an additional functionality provided with the ESA Misdial Prevention feature. Each individual ESDN entry includes a specific option to either enable or disable this feature.

The Allow Last Digit Repeat functionality permits 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 ESDN digit is accidentally dialed again, but also to process the call immediately. For example, dialing 9-1-1-1 would be the same as dialing 9-1-1-#, if the Allow Last Digit Repeat functionality is enabled.

Administration**Feature control**

The operation of the ESA Misdial Prevention feature is controlled by prompts in the Basic ESA Data Block (LD 24). The prompts are detailed as follows:

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

If the MISDIAL_PREVENTION option is set to YES then the ESA Misdial Prevention feature is enabled. That is, anytime an ESDN is dialed with trailing digits (other than the octothorpe) it receives the configured intercept treatment.

A banner is printed to warn the administrator of the potential outcome of the feature. A second level confirmation prompt, "ARE YOU SURE?", is made 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. Either YES or NO must be entered for this prompt. Otherwise, SCH0703 is generated and "ARE YOU SURE?" is prompted again.

If the MISDIAL_PREVENTION option is set to NO then the ESA call recognition feature continues to behave as it did previously and the next entry (ENTR) is prompted.

If no value is entered for the MISDIAL_PREVENTION prompt during a CHG ESA block configuration, then the previously entered 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 for any of the ENTR (meaning that YES was entered for both the MISDIAL_PREVENTION and "ARE YOU SURE?" prompts). In the case of a CHG ESA block configuration, 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 time value of 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 misdialled ESA call. The allowable delay values are 1, 2, 3 or 4, with a default value of 2 seconds.

SCH0030 is generated if any alpha character is entered, and 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. If no value is entered then the default value (YES) 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 causes the ESA call to be processed immediately, as in the case of dialing the octothorpe key ("#") immediately after the ESDN. If

the ALLOW_LAST_DIG_REPEAT is set to NO, then a repeated last ESDN digit is handled as a misdialled ESA call. This is a configurable option for each individual ESDN.

The Misdial Prevention configuration can be printed through Overlay 24.

Intercept treatment

A customer specific option specifies the type of intercept treatment provided to the misdialled caller. If RAN treatment is configured as the intercept treatment for a misdialled ESA call, then it is suggested that a message be provided to the caller that indicates both the cause of the intercept and a corrective action. For example, "You have incorrectly dialed an emergency number, and your call has been intercepted. Please hang up and try again".

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

The valid inputs for the ESAM prompt are:

- OVF or OVFL (indicates that overflow treatment will be used)
- BSY or BUSY (indicates that busy treatment will be used)
- RAN (indicates that recorded announcement treatment will be used)
- ATT (indicates that the misdialled ESA call will intercept to an attendant)

The default value of the ESAM prompt is Overflow (OVF). SCH0111 is generated if an invalid input is entered.

If the RAN intercept treatment is entered for this prompt then the sub prompt RRT is displayed, which indicates the preconfigured RAN route to be used in this intercept treatment. The valid range for this sub prompt is 0-127 for a small system and 0-511 for a large system. SCH0030 is generated if any alpha character is entered, and SCH0481 is generated if a numeric value beyond the allowable range is entered. If a non RAN route number is entered, SCH0406 is generated.

The intercept treatment configuration can be printed using LD 21, if the ESA package (329) is unrestricted.

System messages

This system alarms / messages associated with the ESA Misdial Prevention functionality are detailed in the following table:

Table 27
System alarms / messages for ESA Misdial Prevention

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

Configuration considerations

Some useful considerations to make in configuring the ESA Misdial Prevention feature are as follows:

- 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 – a blind transfer when the emergency number is misdialled will intercept the original emergency caller, especially with Misdial Prevention enabled.

Multiple ESDNs Overview

This feature allows for the recognition of multiple ESDNs on an enterprise telephony network.

It is assumed that all ESDNs are to be used for emergency calls only, which allows all configured ESDNs to be treated at the same high priority level.

ESDNs can be either public external numbers or local directory numbers.

To support network wide client mobility (including Virtual Office), all recognized ESDNs configured on the enterprise telephony network should be configured on every individual call server. This allows any given call server to recognize the ESDN of any other call server – this, in turn, allows a user to dial their home ESDN from any location within the connected enterprise network.

The global ESA configuration parameters common to every configured ESDN are as follows:

- LD 17 Config Record ESA block:
 - LIS –
 - SLIS_NAT_PRIV_IP –
 - DYNAMIC_ELIN_TIMEOUT –
 - DYNAMIC_ELIN_OVERFLOW –
 - EXTERNAL_DM_TIMEOUT –
- LD 117 ERL table –
- LD 117 Subnet table –
- LD 117 Dynamic ELIN table –

Location specific ESA parameters are defined in the Basic ESA Data Block (LD 24). The functionality and rules governing the configuration of ESDNs (using LD 24) are as follows:

- It is mandatory to configure a Primary ESDN.
- Up to 15 additional ESDNs may be optionally configured.
- Each ESDN can be up to 7 digits long.
- Duplicate ESDN entries are not allowed.
- Any new ESDN cannot conflict with an existing ESDN. For example:
 - If ESDN 1234 exists, then ESDN 123 cannot be configured. Any attempt to do so causes the error message “SCH1685 Duplicate ESDN or shorter ESDN already exists” to be displayed.
 - If ESDN 123 exists, then ESDN 1234 cannot be configured. Any attempt to do so causes the error message “SCH1685 Duplicate ESDN or shorter ESDN exists” to be displayed.
- Each configured ESDN specifies its own routing parameters: ESRT or RLI, and Directing Digits (DDGT).
 - Used for local and tandem (trunk initiated) emergency calls.

- Remote calls use ERL table – every ESDN routes to same remote gateway.
- Every ESDN uses the same Default CLID (DFCL).
- Every ESDN uses the same OSN phone DN (OSDN).

Access codes

The use and configuration of Access Codes (ACs) with ESDN is detailed by the following:

- ESDN configuration is independent of the ESN configuration. It is not required to dial AC1/AC2 to dial an ESDN.
- General guidelines for configuring an ESDN:
 - Do not configure any internal DN or Steering Code (for CDP numbering) that conflicts with any ESDN configured in the Basic ESA Data Block (LD 24).
 - Do not configure any BARS/NARS DN (AC1/AC2 + LOC/NPA/NXX/SPN) that conflicts with any ESDN configured in the Basic ESA Data Block (LD 24).

An ESDN can be dialed as AC+ESDN. Other rules governing the use of an access code with ESDN include the following:

- To dial any ESDN as AC1+ESDN or AC2+ESDN, 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.

Alternately, it is possible to configure an SPN (Special Number) to use an RLI and DMI to terminate on a new DN (or ACD/IVR), or to route to another system. However, if this is done then ESA features are unavailable – this includes OSN (On Site Notification), call prioritization (class of service override) or ANI composition (including ELINs).

Administration

- Configuration of Entry 0, the Primary ESDN, is mandatory.
 - An error (SCH1683) is displayed if Entry 0 is not configured.
- Entries 1-15, which are for additional ESDN entries, are optional. Configuration of these additional entries is as follows:
 - An error (SCH1638) is displayed for invalid entry number.

- An error is printed when no more entries can be configured.
- Entering a Null value at the ENTR prompt indicates that no further entries are to be made.
- Each entry must fully specify required ESDN information, as follows:
 - An error (SCH0703) is displayed if ESDN is not configured.
 - An error (SCH1685) is displayed if the ESDN entered conflicts with another shorter ESDN.
 - An error (SCH1685) is displayed if the ESDN entered conflicts with another longer ESDN.
 - An error (SCH0212) is displayed if the ESDN entered is invalid.
- Each ESDN entry must specify routing information using ESRT or RLI. An error is displayed if ESRT or RLI are not configured (SCH1982).
- Each entry must specify Directing Digits (DDGT). An error is displayed if DDGT is not configured (SCH0703).
- Each ESDN entry also has optional Misdial Prevention parameters.
- All the ESDN entries share a common Default CLID (DFCL). A warning is displayed if DFCL is not configured (SCH1979).
- All the ESDN entries share a common OSN Phone DN (OSDN). An error is displayed for invalid OSDN (SCH0278).

ESDN Entry 0, the Primary ESDN, cannot be added to an existing ESA Data Block, as it must already be configured if the ESA Data Block exists. An error (SCH1640) is displayed when an attempt is made to add the Primary ESDN.

ESDN Entries 1-15, used for defining additional ESDNs, can be added. An error is printed for invalid entry number (SCH1638) and Null input for ENTR means end of entries.

Each entry must fully specify required ESDN information, as follows:

- An error (SCH0703) is displayed if ESDN is not configured.
- An error (SCH1685) is displayed if the ESDN entered conflicts with another shorter ESDN.
- An error (SCH1685) is displayed if the ESDN entered conflicts with another longer ESDN.
- An error (SCH0212) is displayed if the ESDN entered is invalid.

Each ESDN entry must specify routing information using ESRT or RLI. An error is displayed if ESRT or RLI are not configured (SCH1982).

Each entry must specify Directing Digits (DDGT). An error is displayed if DDGT is not configured (SCH0703).

Each entry also has Misdialed Prevention parameters.

DFCL cannot be added here, because this data is not specific to a particular ESDN entry.

OSDN cannot be added here, because this data is not specific to a particular ESDN entry.

Any ESDN entry, including Entry 0 (the Primary ESDN), can be changed.

- An error (SCH1638) is displayed for invalid entry number.
- An error (SCH1647) is displayed if an attempt is made to change a non-existent entry.
- The ESDN can be changed, with restrictions as follows:
 - An error (SCH1685) is displayed if the ESDN entered conflicts with another shorter ESDN.
 - An error (SCH1685) is displayed if the ESDN entered conflicts with another longer ESDN.
 - An error (SCH0212) is displayed if the ESDN entered is invalid.
- ESRT or RLI information can be changed.
- The DDGT can be changed.
- The optional Misdialed Prevention parameters can be changed.

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

- An error (SCH1647) is displayed if an attempt is made to remove the Primary ESDN.
- An error (SCH1668) is displayed if an attempt is made to remove a non-existent ESDN entry.

New ESDN entries cannot be added here.

ESA data common to every ESDN (DFCL and OSDN, for example) cannot be changed here.

Entering a Null value at the ENTR prompt indicates that no further entries are to be made.

Inputs made to the ENTR prompt need not be prefixed with 'x'.

Any ESDN entry, with the exception of Entry 0 (the Primary ESDN), can be deleted.

- An error (SCH1638) is displayed for invalid entry number.

- An error (SCH1647) is displayed if an attempt is made to remove the Primary ESDN.
- An error (SCH1668) is displayed if an attempt is made to remove a non-existent entry.

A new ESDN entry cannot be added here.

An existing ESDN entry cannot be modified here.

The ESA Data Block (LD 24) cannot be deleted with this command.

Entering a Null value at the ENTR prompt indicates that no further entries are to be made.

- The whole ESA Data Block can be deleted without deleting ESDN entries first.
 - An error (SCH0282) is displayed if an attempt is made to remove an ESA Data Block that is not configured.
 - Any ESDN entry, including Entry 0 (the Primary ESDN), can be changed.
 - An error (SCH1638) is displayed for invalid entry number.
 - An error (SCH1647) is printed if trying to change a non-existent entry.
 - The ESDN can be changed, with restrictions as follows:
 - An error (SCH1685) is displayed if the entered ESDN value conflicts with another shorter ESDN.
 - An error (SCH1685) is displayed if the entered ESDN value conflicts with another longer ESDN.
 - An error (SCH0212) is displayed if the entered ESDN value is invalid.
 - The ESRT or RLI information can be changed.
 - The DDGT can be changed.
 - The optional Misdialed Prevention parameters can be changed.
 - Any ESDN entry, other than Entry 0 (the Primary ESDN), can be deleted.
 - An error (SCH1638) is displayed for an invalid entry number.
 - An error (SCH1647) is displayed if an attempt is made to remove the Primary ESDN.
 - An error (SCH1668) is displayed if an attempt is made to remove a non-existent ESDN entry.
 - A new ESDN entry cannot be added here.
-

- ESA data common to every ESDN (DFCL and OSDN, for example) cannot be changed here.
- Entering a Null value at the ENTR prompt indicates that no further entries are to be made.
- DFCL is common for all the ESDN entries and can be modified. A warning (SCH1979) is printed if DFCL is not configured.
- OSDN is common for all the ESDN entries and can be modified. An error (SCH0278) is printed for an invalid OSDN.
- An error message (SCH0282) is displayed if the ESA Data Block (LD 24) is not configured.
- ESDN entries are printed as part of ESA Data Block (LD 24).
- Each ESDN entry also has optional Misdialed Prevention parameters.
- An error message (SCH1630) is printed if the ESA Data Block (LD 24) is not configured.
- An error (SCH1638) is printed for an invalid ESDN entry number.
- An error (SCH1647) is printed if trying to change a non-existent ESDN entry.
- Only one ESDN 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 ESDN entries it contains.
- Common ESA Data Block parameters (DFCL and OSDN) are not printed in the output.

ESA VO redirection

An IP phone VO logged in to its home call server can be redirected back to its host call server when an emergency call is made. However, there might be a mismatch between the ESDN configured on the home call server and the ESDN configured on the host call server – an ESDN on the home call server might actually be an unknown number on the host call server (or vice versa) and this would result in a redirected ESA call being unrecognized when it is redirected back to the host call server.

To avoid this situation:

- All call servers must have a Primary ESDN configured (for example, 911 for North America, 112 for Europe) - this is a mandatory configuration.
- The VO ESA call is routed from the home call server. If the ESA call has to be rerouted to the Host CS, then:
 - The home ESDN (as dialed by the VO user) is passed along to the host call server through the DRAM of the IP phone.

- If the host call server finds the home ESDN entry to be configured in its ESA Data Block (LD 24), the call is routed accordingly to the emergency responder.
- If the host call server does not have the home ESDN entry configured in its ESA Data Block, then it uses its own configured Primary ESDN and routes the call accordingly. A system message is generated to notify that the ESA call has been routed using the Primary ESDN of the host call server instead of the caller's home ESDN.

Shared RLIs / DMIs

If the situation allows it, an emergency RLI can be shared by multiple ESDNs and yet still allow different call treatments for each ESDN. Digit manipulation performed by the DMI (configured in the RLI) can make the Called Number ESDN specific.

Prepend Digits, specified in either the ERL table or by a DMI, can route to different endpoints. For example, the Prepend Digits 343 can route to either "343-911" or "343-311".

Through the careful DN management, different ESDN calls can terminate locally on different DNs. A call using an ESDN of 911, for example, could terminate on extension 5911, while calls made using an ESDN of 311 could terminate on extension 5311.

A full (10 digit) PSAP number can be specified if a DMI is used to delete all digits and inserts the full PSAP number, but this would apply to all emergency calls made using the related RLI (and thus would not be ESDN specific).

OSN Telephone

The OSN Phone identifies the Emergency Services DN (ESDN) that was used to make the emergency call (911, for example). Refer to the Called # in the OSN Record to see any digit manipulation.

If an emergency call is trunk initiated (that is, on the terminating node in a tandem scenario) and any ESDN translation took place, then the OSN Phone may display a different ESDN than on the originating system. However, this is still the ESDN used to invoke the emergency call on this system.

The ESDN is printed on the first line of the display, along with the Caller Name, as follows:

- The maximum length of the Caller Name (or the Incoming Route Name, if this is used) is 27 characters.
- The maximum length of the ESDN string is 7 characters.

- Depending on the display capabilities of the phone type in use, the Caller Name (or Incoming Route Name) is truncated, if required, in favor of allowing the full ESDN to be displayed.
 - The IP Phone 2002 can display 23 characters per line.
 - The IP Phone 2004 can display 24 characters per line.
- Truncation of the Caller Name (or Incoming Route Name) to display full ESDN information applies to both the originating node OSN Phone (for a set originated ESA call) and the tandem node OSN Phone (for a trunk initiated ESA call).

OSN Record

With the implementation of the Multiple ESDN functionality, the dialed ESDN is printed in the header line of the OSN Record. In addition, the OSN Record display of CALLED# behaves as follows:

- For CAMA trunks, CALLED# prints the DDGT configured for the dialed ESDN.
- For all other call types, the actual Called Number that goes out in the messages is displayed by CALLED#.
- In the case of Local Termination, the CALLED# is not displayed.

Data conversion

If an ESA Data Block was configured for use with the previous release, then data conversion during a version upgrade behaves as follows:

1. The previously configured ESDN, ESRT and DDGT become the data used in building the Primary ESDN (ENTR 0).
2. No additional ESDN entries exist.
3. The configured DFCL and OSDN values (common to all ESDN entries) 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 the Multiple ESDNs feature.

System messages

The following new system messages are identified for the implementation of this feature.

Table 28
System alarms and messages for Multiple ESDNs

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

Message Number	Severity	Description	Corrective Action	Output
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

System configurations

The following sections describe the most common system configurations that are possible with ESA. Samples are provided to show typical non-networking and networking configurations. Also, a standalone configuration, where ESA calls are answered on the business premises, rather than being forwarded to the PSAP, is presented at the end of the section.

Note 1: In the diagrams, CAMA trunks are depicted as handling ESA calls. However, ISDN trunks are equally applicable.

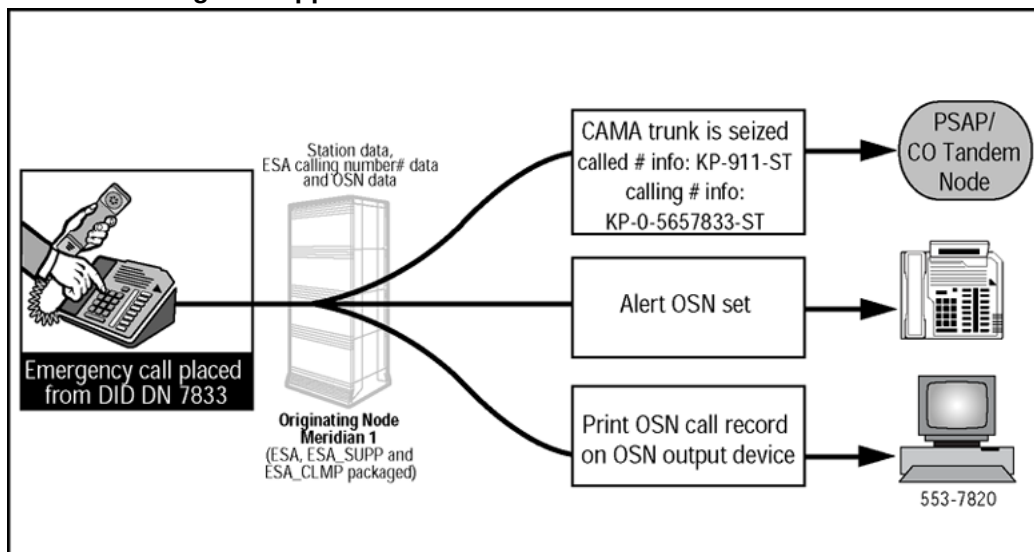
Note 2: Note that, as discussed in the section Different applications on page REFERENCE, there are variations to how ESA may be configured.

Non-networking ESA configurations

Sample configuration for a DID DN ESA call

Figure 7 "Non-networking ESA application for a DID DN call" (page 152) illustrates a system with the ESA feature handling a DID DN ESA call.

Figure 7
Non-networking ESA application for a DID DN call



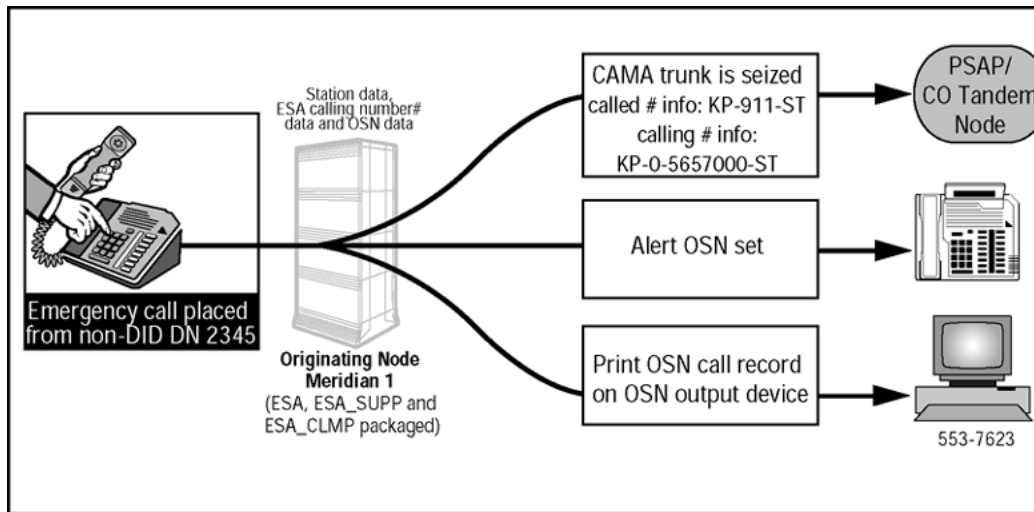
In [Figure 7 "Non-networking ESA application for a DID DN call" \(page 152\)](#), an emergency call is placed at the originating node from DID DN 7833 (by dialing the ESDN 911). The following call processing takes place:

- An outgoing CAMA trunk is seized at the originating node.
- 911 is outpulsed as the CAMA trunk directing digits (911 is entered against the DDGT prompt in LD 24) by means of MF signaling.
- The appropriate calling number information for the DID DN is composed and outpulsed by means of MF signaling. Refer to the section ["Calling number for station phone-initiated ESA calls" \(page 78\)](#).
- The OSN phone is alerted by ESA.
- The OSN call record is printed on the output device. Refer to [Figure 2 "OSN call record print for an attendant console-initiated ESA call" \(page 118\)](#).

Sample configuration for a non-DID DN ESA call

[Figure 8 "Non-networking ESA application for a non-DID DN call" \(page 153\)](#) illustrates a system with the ESA feature handling a non-DID DN ESA call.

Figure 8
Non-networking ESA application for a non-DID DN call



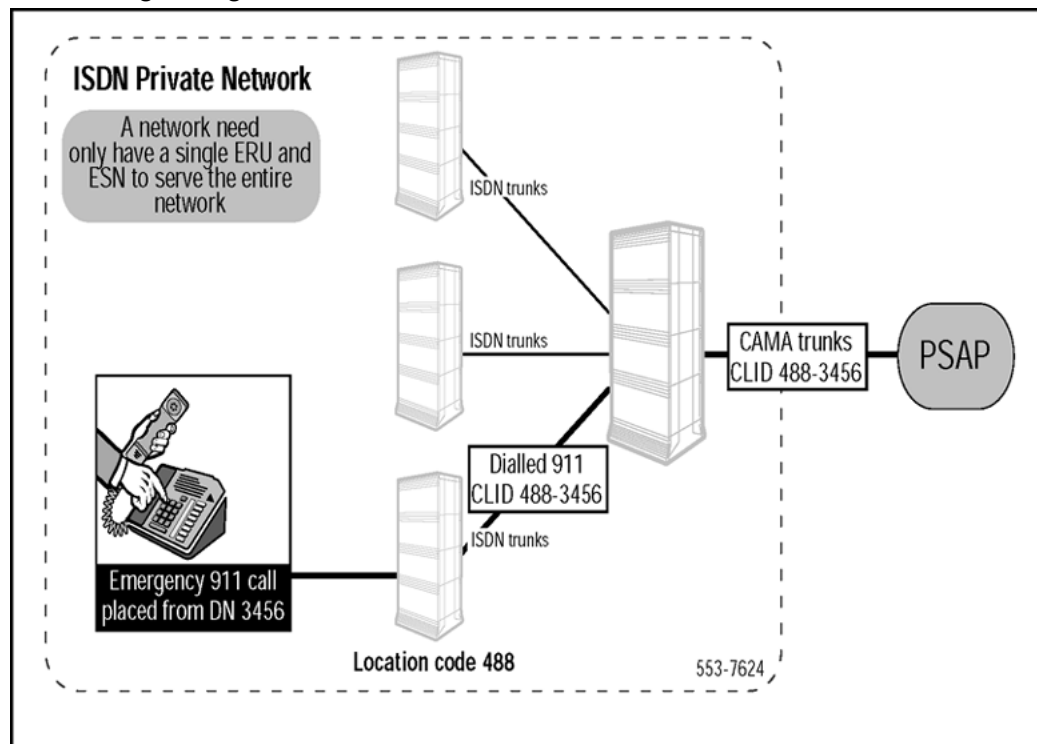
In Figure 8 "Non-networking ESA application for a non-DID DN call" (page 153), an emergency call is placed at the originating node from non-DID DN 2345 (by dialing the ESDN 911.) The following call processing takes place:

- An outgoing CAMA trunk is seized at the originating node.
- 911 is outpulsed as part of the called number using MF signaling.
- The appropriate calling number information for the non-DID DN is composed and outpulsed using MF signaling Refer to the section "Calling number for station phone-initiated ESA calls" (page 78).
- The OSN phone is alerted by ESA.
- The OSN call record is printed on the output device. Refer to Figure 2 "OSN call record print for an attendant console-initiated ESA call" (page 118).

Networking ESA configuration

This configuration, as shown in Figure 9 "Networking configuration" (page 154) will appeal to users who normally route all of their outgoing calls through a single hub location, as well as those with a more complex configuration. Callers can still dial 911 at remote locations, and have their calls routed automatically across the private network to the hop-off point. At that point, they are routed to the PSAP. All locations would typically be running ESA, with the same ESDN at each node.

Figure 9
Networking configuration



Configuration guidelines

This arrangement is not satisfactory if such network calls can be overflowed to the public network or to non-ISDN links. In these cases, the overflow mechanism should be a direct local CO connection, which would still allow 911 calls to be completed, albeit without the benefits of the ANI.

Thought should also be given to the engineering of the ISDN links if this arrangement is adopted. It is important to ensure that a trunk is always available, and it is recommended that a route of one or two channels in the PRI link be dedicated to 911.

If the network links are not ISDN, it will only be possible to identify the location, and not the individual station. The trunk route can be programmed to provide a single unique number that is sent as the ANI.

Before planning this configuration, care should also be taken that calls will route to the correct PSAPs. The public 911 tandem network usually provides a feature known as Selective Routing, which will route a 911 call to the correct PSAP based on the ANI. However, this generally only works within a limited area, and it might not be possible for the hub's 911 connection to correctly route calls from some distant locations. The

customer should always check with the Telco or Public Safety agency before committing to this arrangement, and plan additional 911 access at locations where routing might be a problem.

How to set up the ESA networking requirements

At the remote nodes, the following configuration is required:

- Set the outgoing trunk routes to be dedicated or shared.
- Ensure that the outgoing ESDN is the same as the ESDN outputted at the hub.
- Set up OSN.

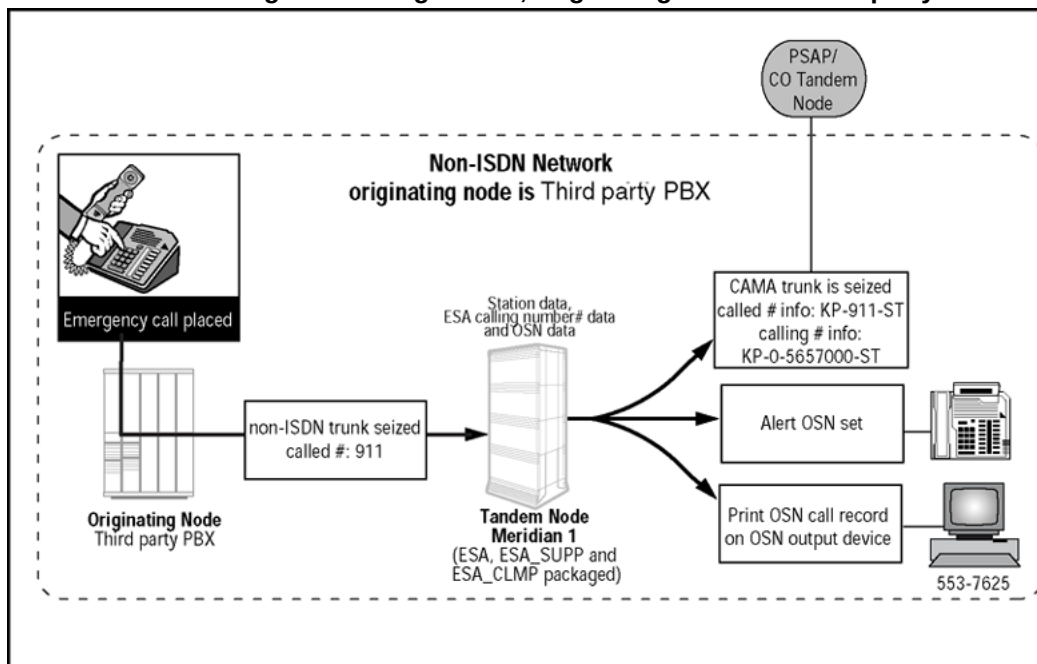
At the hub, no special set up is required, because the CLID delivered by the ISDN link is used (the ANI from the hub is ignored).

Sample ESA networking configurations

Non-ISDN network, originating node is third party PBX Figure 10

"Non-ISDN networking ESA configuration, originating node is a third-party PBX." (page 155) illustrates a non-ISDN network ESA configuration, where the originating node is a third party PBX.

Figure 10
Non-ISDN networking ESA configuration, originating node is a third-party PBX.

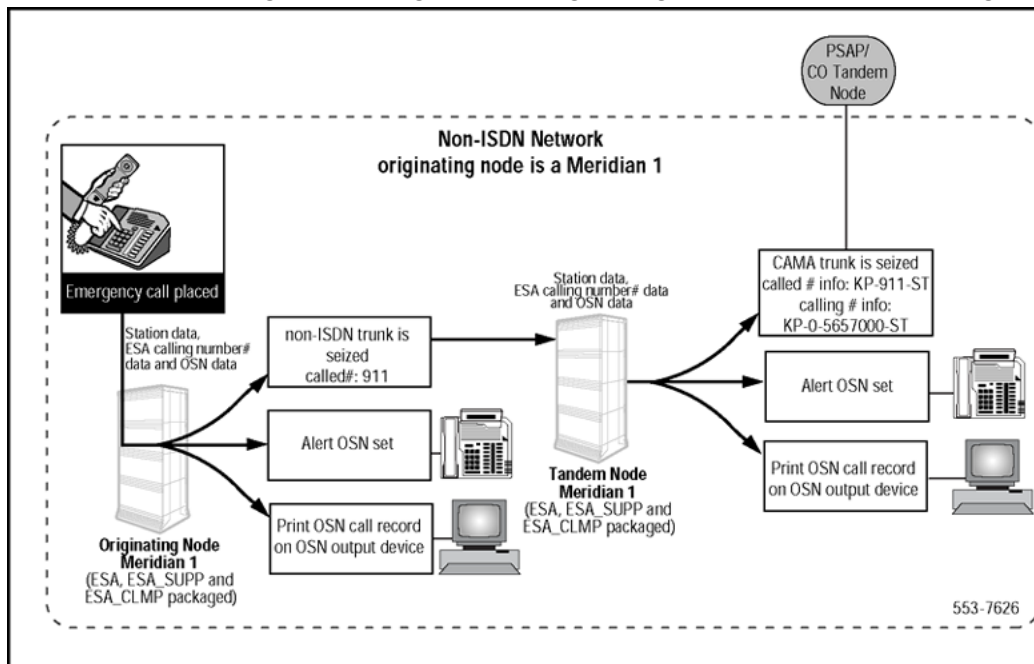


In Figure 10 "Non-ISDN networking ESA configuration, originating node is a third-party PBX." (page 155), an emergency call is placed from the originating node over a non-ISDN trunk to a tandem system. At the tandem system, the following call processing takes place:

- An outgoing CAMA trunk is seized.
- 911 is outpulsed as part of the called number using MF signaling.
- The appropriate calling number information for the incoming non-ISDN trunk is composed and outpulsed using MF signaling. Refer to the section "Calling number for incoming non-ISDN trunk-initiated tandem ESA calls" (page 80).
- The OSN phone is alerted by ESA.
- The OSN call record is printed on the output device. Refer to Figure 3 "OSN call record print for an incoming trunk-initiated tandem ESA call" (page 120).

Non ISDN network, originating node is a Meridian 1 Large System Figure 11 "Non-ISDN networking ESA configuration, originating node is a Meridian 1 Large System" (page 156) illustrates a private non-ISDN network ESA configuration. In this case, the originating node is a Meridian 1 Large System, which can output display information.

Figure 11
Non ISDN networking ESA configuration, originating node is a Meridian 1 Large System



In Figure 11 "Non-ISDN networking ESA configuration, originating node is a Meridian 1 Large System" (page 156), an emergency call is placed from the originating node, where the following call processing occurs:

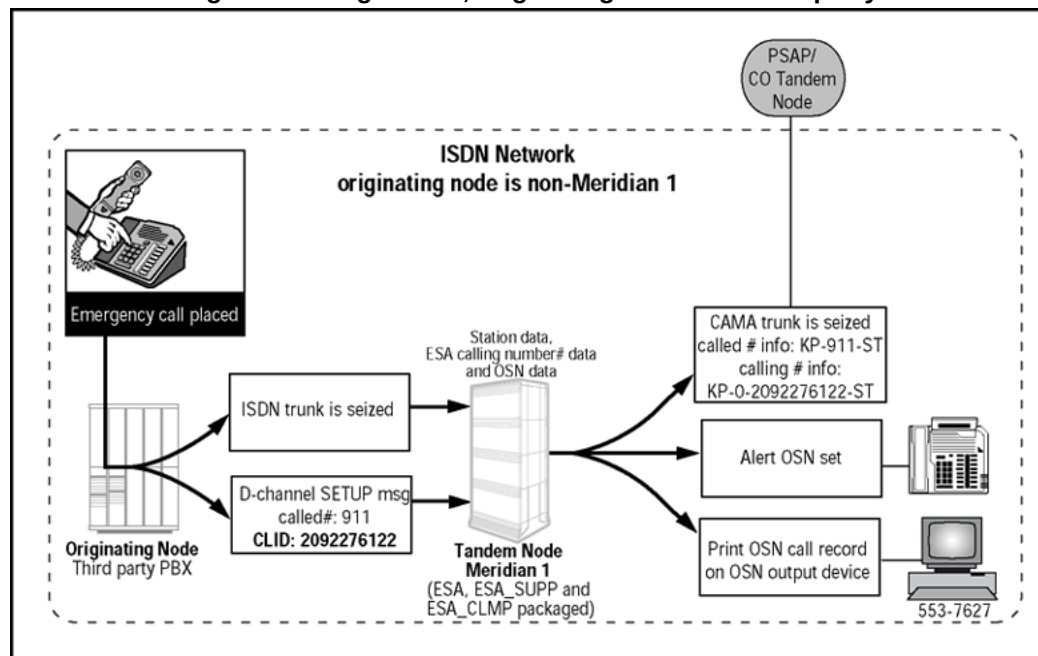
- An outgoing system non-ISDN trunk is seized.
- 911 (which has been defined as the ESDN in LD 24) is outputted as part of the called number.
- The OSN phone is alerted by ESA.
- The OSN call record is printed on the output device. Refer to Figure 3 "OSN call record print for an incoming trunk-initiated tandem ESA call" (page 120).

At the tandem node, the following call processing takes place:

- An outgoing CAMA trunk is seized.
- 911 is outputted as part of the called number by means of MF signaling.
- The appropriate calling number information for the incoming non-ISDN trunk is composed and outputted by means of MF signaling. Refer to the section "Calling number for incoming non-ISDN trunk-initiated tandem ESA calls" (page 80).
- The OSN phone is alerted by ESA.
- The OSN call record is printed on the output device. Refer to Figure 3 "OSN call record print for an incoming trunk-initiated tandem ESA call" (page 120) Figure 3 "OSN call record print for an incoming trunk-initiated tandem ESA call" (page 120).

ISDN network, originating node is a third party PBX Figure 12 "ISDN networking ESA configuration, originating node is a third-party PBX" (page 158) on Figure 12 "ISDN networking ESA configuration, originating node is a third-party PBX" (page 158) illustrates a non-private ISDN network ESA configuration. In this example, the originating node is a third party PBX.

Figure 12
ISDN networking ESA configuration, originating node is a third-party PBX



In Figure 12 "ISDN networking ESA configuration, originating node is a third-party PBX" (page 158), an emergency call is placed from the originating node, where the following call processing occurs:

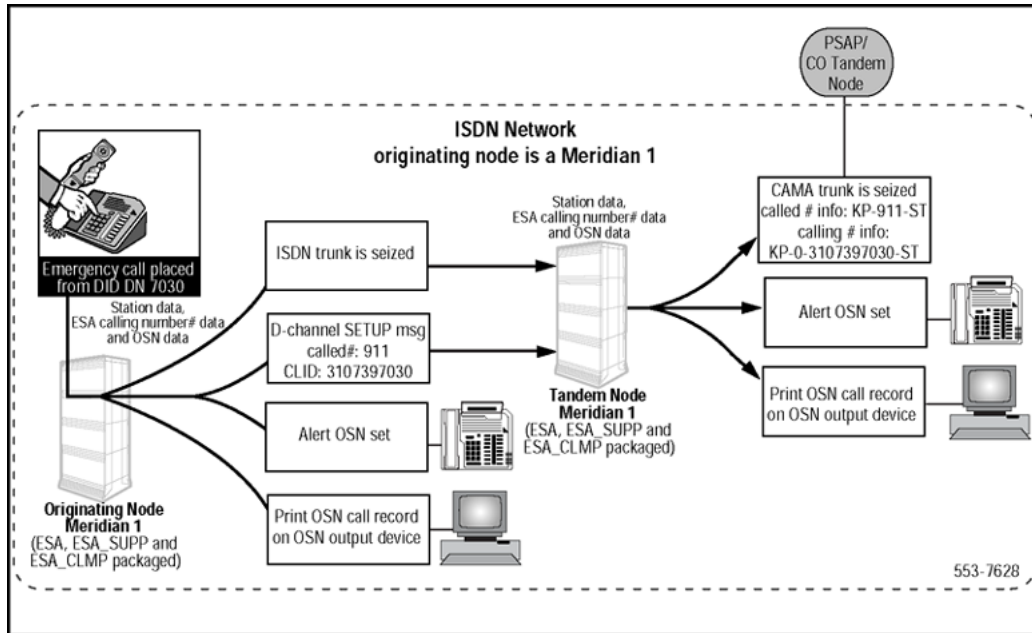
- An outgoing system ISDN trunk is seized.
- 911 (which has been defined as the ESDN in LD 24) is outpulsed as part of the called number using ISDN messaging.
- The appropriate calling number is composed for the ISDN trunk (refer to the section "Calling and called number information for ESA calls routed to an ISDN trunk" (page 103)), and passed on to the tandem node by means of CLID messaging.

At the tandem node, the following call processing takes place:

- An outgoing CAMA trunk is seized.
- 911 is outpulsed as the called number using MF signaling.
- The CLID received from the incoming trunk is retrieved and outpulsed as the calling number, using MF signaling.
- The OSN phone is alerted by ESA.
- The OSN call record is printed on the output device. Refer to Figure 3 "OSN call record print for an incoming trunk-initiated tandem ESA call" (page 120).

ISDN network, originating node is a Meridian 1 Large System Figure 14 "Meridian 1 ESA stand-alone configuration using CAMA trunks" (page 160) illustrates a private ISDN network ESA configuration, where the originating node is a system equipped with ESA.

Figure 13
ISDN networking ESA configuration, originating node is a Meridian 1 Large System



In Figure 14 "Meridian 1 ESA stand-alone configuration using CAMA trunks" (page 160) on Figure 14 "Meridian 1 ESA stand-alone configuration using CAMA trunks" (page 160), an emergency call is placed from the originating node, where the following call processing occurs:

- An outgoing system ISDN trunk is seized.
- 911 (which has been defined as the ESDN in LD 24) is outputted as the called number using ISDN messaging.
- The appropriate calling number is composed for the ISDN trunk (refer to the section "Calling and called number information for ESA calls routed to an ISDN trunk" (page 103)), and passed on to the tandem node using CLID messaging.

At the tandem node, the following call processing takes place:

- An outgoing CAMA trunk is seized.
- 911 (which has been defined as using the DDGT in LD 24) is outputted as the called number using MF signaling.
- The CLID received from the incoming trunk is retrieved and outputted as the calling number, using MF signaling.

- The OSN phone is alerted by ESA.
- The OSN call record is printed on the output device. Refer to [Figure 3 "OSN call record print for an incoming trunk-initiated tandem ESA call"](#) (page 120).

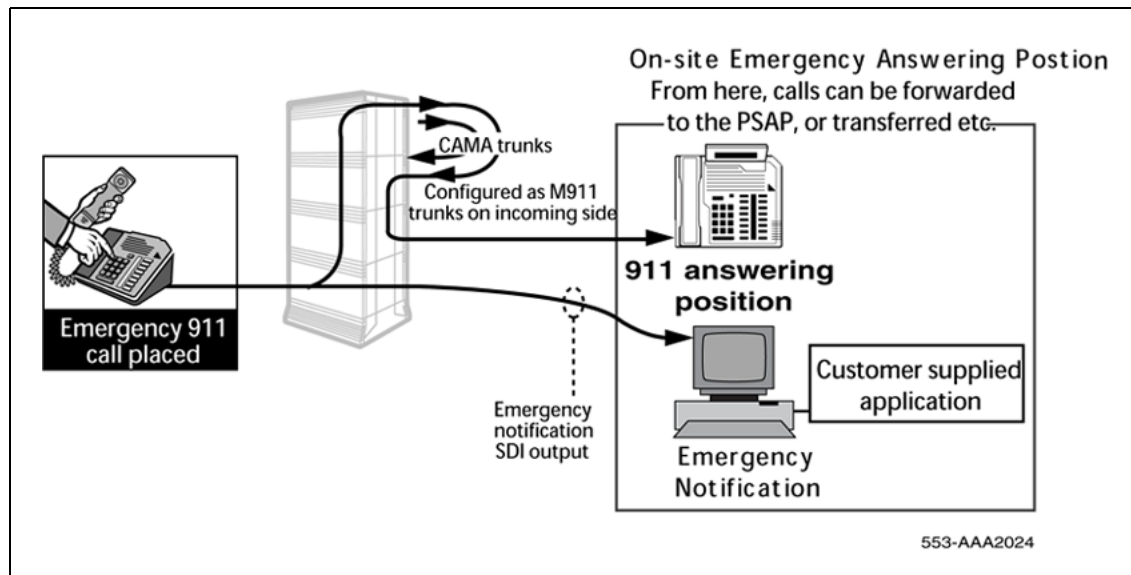
Standalone configuration (on-site call answering)

A standalone configuration is one where ESA calls are answered on the business premises, rather than being forwarded to the PSAP. The calls, however, can then be redirected to the PSAP, if required.

The configuration is illustrated by [Figure 14 "Meridian 1 ESA stand-alone configuration using CAMA trunks"](#) (page 160) (using CAMA trunks) and by [Figure 15 "ESA stand-alone configuration using ISDN trunks"](#) (page 162) (using ISDN trunks).

Note: This configuration does not provide what the legislation requires. However, in jurisdictions where no legislation yet exists, there are requirements for it. If it is used, you should be aware that later legislation may require you to reconfigure.

Figure 14
Meridian 1 ESA stand-alone configuration using CAMA trunks



The two CAMA trunks which normally go to the PSAP or 911 tandem are fed back into the system. They must be configured as "Meridian 911" trunks at the system, and invoke the Meridian 911 feature. Meridian 911 is a feature which is designed to be used when a system is being used as a PSAP, and is used here to simulate a customer-owned PSAP.

Meridian 911 allows E911 CAMA trunks to bring incoming 911 calls into the system, and route them to either an ACD operation, or to single or multiple appearance phones. Refer to *Features and Services (NN43001-106)* for a more detailed description of Meridian 911.

Configuration guidelines

If the use of single or multiple appearance phones is preferred over ACD, it will still be necessary to set up an ACD operation, and use the default ACD number for the Control DN (CDN) required by Meridian 911. The ACD queue should then be Night Call Forwarded to the desired single or multiple appearance DN. Note that this is the only way that emergency calls can be automatically forwarded out of the system to the Public Safety Answering Point if internal answering is not being used at any time.

The Emergency Notification computer (if one is used) will be co-located with the Meridian 911 phone, so that the call can be answered and the screen information made available at the same time.

To transfer calls to the public 911 service, use the No-Hold Conference (or Transfer) capabilities, to ensure that the caller is not disconnected while waiting for the connection. Note, however, that if the same customer is used to both originate and answer a call, the ESDN cannot be used, because the call would simply loop around another CAMA trunk back to the same phone. It is recommended that ESN translation be used to ensure that the transferred call correctly exits the system on a trunk route to the Central Office and the PSAP. Similar consideration apply for Call Forward No Answer and Call Forward All Calls. You might want to consider putting the public 911 number into a No-Hold Conference Hotline key, to simplify such transfers.

It is not recommended that this configuration be used if the answering position is likely to be unattended. However, if the Meridian 911 customer is set up as indicated previously for non-ACD operation, the phone can be forwarded (Call Forward All Calls (preferred) or Call Forward No Answer) to the public network by means of ESN.

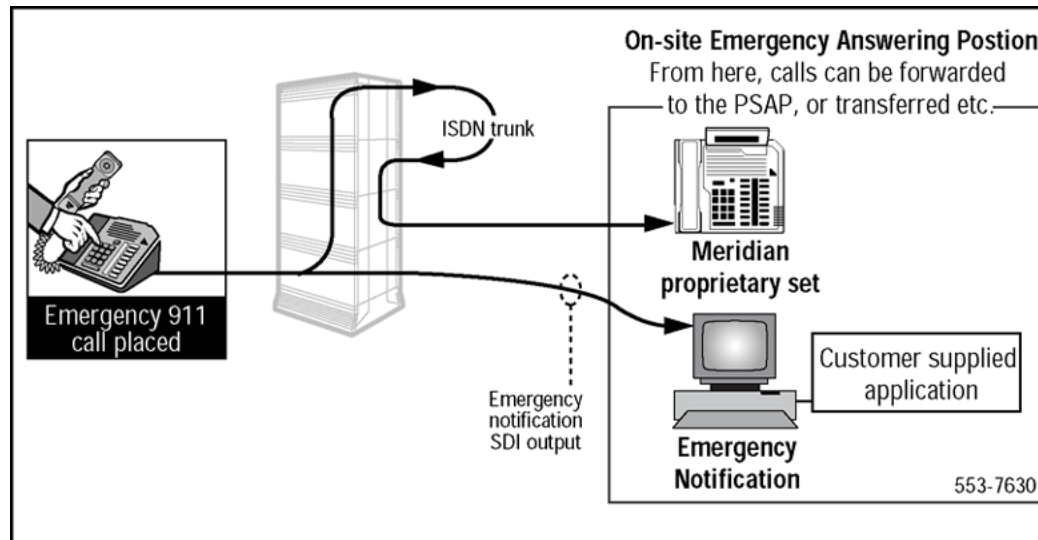
The answering phone should be set to 'Forward-No-Answer' to the public 911 service, in case the attendant inadvertently omits to set call forward when away. However, relying on CFNA like this will put a delay into the call answer, and is to be avoided. The phone should always be forwarded when unattended, even if momentarily.

Any configuration that allows unattended operation must be thoroughly tested before being put into service. If there is any doubt that all 911 calls will be properly routed, the position should be continuously staffed.

Note: If ISDN trunks are being used, they are not configured as Meridian 911 trunks. They are fed out and routed back in as ISDN

trunks, as shown in [Figure 15 "ESA stand-alone configuration using ISDN trunks"](#) (page 162). As mentioned in the section ["On-Site Notification output device print"](#) (page 115), a third-party application may be used to view the screen information.

Figure 15
ESA stand-alone configuration using ISDN trunks



Because the ESDN is always sent out as the directing number on ISDN ESA calls, care must be taken to ensure that the incoming loop call does not loop straight back out again. This may happen if the same customer is used, unless Autotermination or Incoming Digit Conversion is used on the incoming portion of the ISDN trunk loop.

Implementation and engineering considerations

The following items are required to implement ESA between the system and the Public Safety Answering Point (PSAP). Contact your service provider at an early date, to establish if there are any other requirements.

Note: These requirements have been largely based on U.S. practice, but broadly similar conditions will apply to other jurisdictions. A number of steps may not apply, or apply to a lesser extent if the ESA feature is being used for other than full functionality (as described in the section [Different applications](#)).

General considerations

- All buildings are required to have an address approved by the 911 emergency services provider, as these are the only ones that can be entered in the ALI database. You should verify with your 911 service provider or Telco that the addresses you propose to use are acceptable.

Addresses may vary from building to building, especially in a campus environment.

- Each phone station user's location will require a designation, such as a floor and room number, or pillar number. These designations should be consistent in design and clearly visible, as this information will be entered in the ALI database, as well as ENS. The proposed designations should be discussed and agreed with your 911 service provider or Telco. The database typically has a field for 20 alphanumeric characters.
- Phones should be clearly marked with the digits that must be dialed to initiate a 911 call.
- The primary routing for 911 calls will be using CAMA or ISDN trunks, to deliver phone station user information (usually ANI) to the emergency services dispatcher. Alternate 911 routing should be established by means of regular central office trunk lines, to provide backup and overflow capabilities, even though ANI is not available on these routes.
- Determine the number of trunks needed to handle the 911 traffic volume. The Telco or service provider's 911 contact can assist in determining the number of CAMA or ISDN trunks required: two would be the recommended minimum. You then need to order these trunks and arrange an installation date.
- Analyze your system to determine your additional hardware and software requirements, if any.
- Analyze your DID numbers to see if you have a sufficient number, and if they are distributed appropriately. Order additional numbers if necessary.
- Determine how close you want to map DNs to actual locations on your premises (adjacent DID phones). For example, one small group of desks or workstations may share one DID number, or one DID number may be designated per floor. This DID number may be real or fictitious. This DID number will be used to track down the point of origin in the case of an emergency call.
- Map all non-DID numbers to appropriately adjacent DIDs. Refer to "[Digit translation examples](#)" (page 95). Collect all location information for all phones on the system, along with other pertinent details.
- Program the required changes to the system.
- A personal computer for operation of the ALI database software (if provided by your Telco or service provider) may be required, but it does not need to be a dedicated computer for this function. This PC is used for maintaining the addresses and phone user database information, and to download it to the ALI database. A POTS line is also required for the PC's modem.

DID numbers

ESA deals effectively with non-DID numbers, by mapping them to nearby DID numbers. (Refer to "[Digit translation examples](#)" (page 95) for information). This means that large numbers of non-DID numbers can be used, but it also means that there needs to be a reasonable number of DID numbers to map them to. These DID numbers need to be strategically scattered throughout the organization, so that all non-DID numbers are reasonable close to a DID number.

Thought, therefore, needs to be given to whether there are enough DID numbers, and whether the distribution is satisfactory.

Trunk service (CAMA, ISDN) from Telco

It will be necessary to contact your local phone service provider to obtain CAMA or ISDN trunk service, and a service agreement will have to be drawn up, based on applicable tariffs. CAMA trunks would typically be new service, while ISDN trunks would normally already be in use.

System hardware considerations

NTAG26 is a MF Receiver card that is required to support the Meridian 911 feature in the standalone configuration. XUT trunk appearances are also required to be configured as incoming Meridian 911 trunks.

Database considerations**Data Management - general**

When Private 911 is first implemented, a great deal of information may need to be gathered, concerning the locations and DNs of phones, and the names of the users. When the information is gathered, careful record-keeping will be required, and all changes must be properly recorded and made in all databases (including system) at more or less the same time. This additional effort needs to be planned for.

Also, an agreement must be made with the agency maintaining the ALI database about the content and format of the location information, as well as updating procedures. Typically the content will include:

- street address of the building, and location information and access methods, if necessary
- the floor number
- location on the floor (for example, NW corner, room number, pillar number, or something similar)
- name of the principal user of the phone, if appropriate

This information must be provided when the PBX is first installed or configured for Private 911 service, and also on an ongoing basis as service activity for Adds, Moves and Changes are carried out.

ALI database updating

When Private 911 is in use, it is required that all changes to station phones be registered in the external ALI database. This will be required not only at initial service time, but every time that a change is made to a station's location, DN, or user name. The Telco will have procedures in place to allow this to be done, and should be consulted at an early stage.

ALI database maintenance will be performed as a separate activity from the system service change, and strict procedures will be necessary to ensure consistency of the external ALI database with the system. The Telco may offer one or more of the following methods to do this updating:

- a PC utility to post ALI updates by means of a modem
- mailing in changes
- faxing changes
- other arrangements

As changes are made to the DNs and locations of the phones in the switch, changes should be made to the ANI translation tables needed to provide the correct ANI (not always necessary, but should be checked), as well as the 'DES' and the external ALI.

The previously detailed issues pertaining to the ALI database updating are not part of the ESA feature, but an essential part of what the user has to do.

Special database considerations

Activities that can possibly cause inconsistencies are:

- Automatic Set Relocation and Modular Telephone Relocation. These are features where the user can move his/her own phone simply by dialing appropriate codes, and then picking up the phone and moving to another location. It is recommended that the 'CSC' USER type be enabled in LD 17, so that messages can be printed and history file records generated for such moves. This will allow procedures to be put into place to make appropriate ALI updates.
- Attendant and Phone-based Administration. Phones can be configured, changed, and removed, and DNs can be changed by persons other than the official administration staff. Again, CSC messages should be enabled, to allow ALI updates to be made.
- It is also important to note that undocumented moving of phones by means of building wiring changes (such as would perhaps happen in a departmental move) must not occur. Any activity that causes the physical location of a DN to change must be reflected in an ALI update.

ESA equipment engineering

Many jurisdictions recommend dedicated trunks to handle 911 calls, and generally a minimum of two. It is important to determine how many channels will be needed to handle the maximum number of 911 calls that will be in progress simultaneously, and provide as many trunks as needed to handle the traffic. As each business is different, it is not possible to provide definitive guidelines for how many channels will be needed, but an average figure for a normal business might be two dedicated trunks serving up to 5000 lines. The 911 calls should overflow onto Central Office (CO) trunks, thus ensuring that no calls get blocked. However, such overflowed calls cannot provide the ANI to the PSAP, so Enhanced 911 service would not be given.

Operating parameters**ESA Call Recognition**

As per existing system operation, when a TN is service changed by means of load administration or attendant administration, or disabled using maintenance loads, then all calls on the TN, including ESA calls, are force disconnected.

Up to four digits (0-9) can be defined as the customer's ESDN. The symbols '#', '*' are rejected as invalid.

The system administrator must define the customer's ESDN as a BARS/NARS Special Number (defined by responding with SPN to the TYPE prompt in LD 90) in order for an Access Code + ESDN call to be recognized as an ESA call.

The system administrator must define a local terminating route list index for the SPN (defined by responding with YES to the LTER prompt in LD 86) in order for an Access Code + ESDN call to be recognized as an ESA call.

If an ESA route is accessed by dialing the Access Code of the ESA route, the call is not recognized as an ESA call. It is recommended that, to prevent non-911 calls from direct access to ESA routes, some means of access control be implemented (such as Trunk Group Access Restriction).

ESA Calling Terminal Identification

When a CLID entry has been assigned to a station phone or to a route, it is up to the system administrator to maintain the database so that the CLID entry remains valid.

If an undefined CLID entry is being referenced when the system is trying to compose the ESA calling number, then the ESA calling number is set to the Customer's Default Calling Number (DFCL). The following error message is provided as an indication:

`ERR9009 cust# dn clid_ent#`

After the ESA calling number has been composed for an ESA or tandem ESA call, the number of digits in the ESA calling number is validated by the system. If the ESA calling number is found to contain an unexpected number of digits, then the ESA calling number is set to the Customer's Default Calling Number (DFCL). The following error message is provided as an indication:

ERR9012 *cust# clid_ent# calling#*

ESA Call Routing

Only the following routes can be used as an ESA route:

- Centralized Automatic Message Accounting (CAMA)
- Central Office (COT)
- Direct Inward Dial (DID)
- Foreign Exchange (FEX)
- TIE
- Wide Area Telephone Service (WATS)

Note: An NI-2 Call-By-Call or Integrated Services Access (ISA) service route can be configured as an ESA emergency call route, as long as it is one of the previously detailed types.

When a route is designated as an ESA route, it is up to the system administrator to maintain the database so that the ESA route remains valid.

As per existing operation, when a call terminates onto an outgoing CAMA trunk, the call may be dropped if the far end cannot respond to the CAMA MF signaling.

If all trunks in the Emergency Service Route (ESRT) and the alternate route defined for the ESRT (using the STEP prompt in LD 16) are unavailable, then the Access Denied intercept treatment (defined using the ACCD prompt in LD 15) is given.

After the ESRT has been configured in LD 24, there is no cross checking by the system for subsequent route database administration in LD 16 to ensure that the route that is designated as the ESRT remains valid. Therefore, during call processing, if the ESRT is found to be configured with an invalid route (for example, undefined), then the customer's ACCD treatment is given. The following error message is provided as an indication:

ERR9006 CUST: *cust#* ESA RT: *esrt#*

When ESA Call Routing tries to route an ESA call to the step route configured for the ESRT, if the step route is not valid for ESA calls, then the customer's ACCD treatment is given. The following error message is provided as an indication:

ERR9006 CUST:*cust#* ESA RT: *esrt#* STEP: *step_rt#*

For a CAMA outgoing trunk, in the event that a customer's DFCL is to be used as the ESA calling number and the DFCL is not configured, then KP-2-ST is outpulsed as the calling number.

For a CAMA outgoing trunk, if the composed number is not a 7-or-10 digit number, the DFCL is not sent. KP-2-ST is outpulsed as the calling number instead. There is no error message provided.

For an ISDN-to-ISDN tandem ESA call, if no CLID is passed in by the incoming ISDN trunk, then the Customer's Default Calling Number (DFCL) is sent as the CLID. If the DFCL is not configured, then no CLID is sent over the outgoing trunk.

ESA On-Site Notification

Only a Meridian 1 proprietary display phone can be an OSN phone.

Only a single appearance station DN on the OSN phone can be used as the customer's On-Site Notification DN (defined using the OSDN prompt in LD 24).

When an ESA caller information is linked onto the OSN key, no other ESA caller information can be linked onto the OSN key until the current one is discarded.

When a DN has been designated as the OSDN, it is up to the system administrator to maintain the database so that the OSDN remains valid.

As soon as an ESA call terminates onto an outgoing trunk, an OSN call record is printed, and an alert is initiated to the OSN phone. If an ESA call terminates onto an outgoing trunk that is configured with wink start arrangement (defined by setting the STRO prompt to WNK in LD 14), in the event that wink is not returned, the ESA call steps to the next available trunk, as per the existing trunk termination operation. When this occurs, the ESA OSN function treats the call as a new call, prints a separate OSN record and attempts to notify the OSN phone again.

Whenever an ESA call receives the customer's ACCD intercept treatment, it is indicated in the OSN call record with the following line:

911 CALL INTERCEPTED

As per existing operation, whenever ringing is removed from a Meridian 1 proprietary phone, buzzing (including the OSN buzzing) ends.

If the DN that is designated as the customer's On-Site Notification DN (OSDN) is invalid (for example, vacant, or multiple appearance), the caller information will not be linked. The following error message is provided as an indication:

ERR9007 *cust#*

If the station phone specified by the OSDN is not configured with an OSN key, then the caller information is not linked. The following error message is provided as an indication:

ERR9008 *cust#*

The caller information is not linked onto the OSN key if it already has a caller information linked to it. The following warning message is provided as an indication:

OSN001 *cust#* OSN SET IS NOT NOTIFIED - OSN KEY IS BUSY

The caller information is not linked onto the OSN key if the phone is found to be in the disable state. The following warning message is provided as an indication:

OSN002 *cust#* OSN SET IS NOT NOTIFIED - OSN SET IS UNAVAILABLE

If a customer has more than one phone configured with an OSN key, then only the OSN phone that has a DN key that matches the customer's OSDN is linked with the ESA caller information.

If more than one OSN key is defined on a phone, then the ESA caller information is linked to the first OSN key on the phone.

When an OSN phone is service changed using load administration or attendant administration, or disabled using maintenance loads, then all call registers linked to the phone, including that on the OSN key, are discarded.

Non-networking feature interactions

Access Restrictions

Class of Service Restriction

ESA calls override any system Class of Service restrictions, such as: Unrestricted Service (UNR), Conditionally Restricted (CUN), Conditionally Toll Restricted (CTD), Toll Restricted (TLD), Semi-restricted (SRE), and Fully Restricted (FRE).

Code Restriction

The ESA feature lets outgoing ESA calls override code restrictions.

Trunk Group Access Restriction

The ESA feature lets outgoing ESA calls override Trunk Group Access Restriction (TGAR).

Attendant Administration

Attendant Administration is not supported by the ESA feature.

As per existing operation, when an analog (500/2500 type) phone is service changed using Attendant Administration, all calls on that phone, including ESA calls, are force disconnected.

As per existing operation, when a Meridian 1 proprietary phone is service changed using Attendant Administration, all call registers linked to that phone, including those on the On-Site Notification (OSN) key, are discarded.

Attendant Barge-In

The ESA feature does not restrict Attendant Barge-In on ESA calls.

Attendant Break-In

The ESA feature does not restrict an attendant from breaking into ESA calls.

Automatic Call Distribution

When an ESA call is initiated by an ACD agent using Call Transfer or Conference and the transfer/conference is against the ACD key on the agent phone, the CLID entry associated with the ACD key is used for composing the ESA Calling Number.

When an ESA call is initiated by an ACD agent using Call Transfer or Conference and the transfer/conference is against an Individual DN (IDN) key on the agent's phone, the CLID entry associated with the IDN key is used for composing the ESA Calling Number.

There is no CLID entry for a PBX ACD DN. The CLID entry associated with the PBX DN is used for the PBX ACD DN when a Call Transfer/Conference is initiated by an ACD agent on an analog (500/2500-type) phone.

Conference

No Hold Conference

The ESA feature does not restrict an Attendant Console or a phone from initiating an ESA call using Conference. The ESA feature does not restrict conference completion of an ESA call that is initiated using Conference/No Hold Conference.

When a Meridian 1 proprietary phone initiates an ESA Call using Conference/No Hold Conference, the ESA Calling Terminal Identification function composes the ESA Calling Number based on the key against which

the conference is activated. If this key is not a DN key, the ESA Calling Number is set to the Customer's Default Calling Number (DFCL). The DFCL is a number that is sent out if ANI is not used. In rare cases, the number that is sent is the customer's Listed Directory Number.

Call Hunt

For all three cases of redirection previously detailed, the ANI of the originating phone overrides the ANI of the redirecting phone. This means that it is the ANI of the originating phone that is sent out with the call, and that appears on the OSN phone-type or terminal-type display, and not that of the redirecting phone.

Call Transfer

The ESA feature does not restrict an Attendant Console or a phone from initiating an ESA call using Call Transfer. The ESA feature does not restrict transfer completion of an ESA call that is initiated using Call Transfer.

When a Meridian 1 proprietary phone initiates an ESA call using Call Transfer, the ESA Calling Terminal Identification function composes the ESA Calling number based on the key against which the transfer is activated. If this key is not a DN key, the ESA Calling Number is set to the Customer's default ESA Calling Number (DFCL).

Converged Desktop (CD)

In Converged Desktop mode, a phone set registered to a CS 1000 will receive emergency call treatment as with any other ESA call. Location data that may have been entered for the MCS client will not apply, however - only the location data configured for the CS 1000 phone set applies.

An ESA call cannot be initiated from the soft client (registered to MCS) using **click to call**, as this functionality is not supported through the AML mechanism.

Emergency Services for Virtual Office

For information about Emergency Services for Virtual Office functionality, refer to the chapter ["Emergency Services for Virtual Office" \(page 221\)](#).

Flexible Incoming Tone

The Flexible Incoming Tone (FIT) feature does not apply to the OSN buzz. The OSN buzz is a 10 - second continuous buzz, regardless of whether or not the OSN phone has FIT configured.

When the OSN phone receives the OSN buzz at the same time the FIT buzz is being given for another key, the FIT buzz resumes after the OSN buzz times out.

Group Call

ESA calls cannot be made using the Group Call feature.

History Files

All ESA records are saved into the History File if USER = MTC in LD 17.

Hotline

If the terminating/target DN of a Hotline phone/key is programmed with the ESDN, an ESA call is originated whenever the Hotline phone goes off-hook or whenever the Hotline key is pressed to initiate a new call.

Intercept Treatment

When an ESA call cannot be completed because of invalid route configuration or unavailable trunk, it receives the Customer's access denied (ACCD) intercept treatment. As per existing operation, the ACCD intercept treatment can be defined to route the intercepted call to a Recorded Announcement (RAN), route the intercepted call to the attendant, provide the caller with overflow tone, or provide the caller with busy tone.

Meridian 1 Attendant Console Enhancements

The ESA feature is dependent on the ISDN CLID Enhancements feature. As per existing ISDN CLID Enhancements functionality, for attendant initiated calls, Attendant Consoles use CLID entry 0 and LDN 0 as the originating DN.

Due to the ESA feature's dependency on the ISDN CLID Enhancement, the MACE feature determines whether LDN 0 should be replaced with an appropriate value.

One Plus Dialing

When One Plus Dialing is defined in the CLID entries, the calling number for North America can be 8 or 11 digits. However, E911 standard requires that ESA calls sent over CAMA trunks must have a 7 or 10 digit calling number. Therefore, whenever the calling number is 8 or 11 digits and the leading digit is a "1," the leading digit "1" is truncated and the KP-0-7/10 digit calling number-ST is outpulsed. If the calling number is anything other than 7 or 10 digits, the KP-2-ST is outpulsed.

Pretranslation

Pretranslation, when configured, occurs before the dialed digits are verified to determine whether or not the call is an ESA call.

Privacy Override

The ESA feature allows ESA calls to be overridden by the Privacy Override feature.

Private Line

The ESA feature does not support calls that are initiated by a Private Line phone or key.

Trunk Barring

Trunk Barring provides the option of allowing or denying a direct or modified connection between customer-defined routes. For direct connection, the ESA feature allows outgoing ESA calls to override Trunk Barring. For modified connection, the ESA feature does not allow outgoing ESA calls to override Trunk Barring.

Networking feature interactions**Attendant Break-In**

When an ESA call and an attendant are on different nodes, if Network Attendant Service (NAS) is provisioned, the ESA feature does not restrict the attendant from breaking into the ESA call.

Basic Alternate Route Selection (BARS)/Network Alternate Route Selection (NARS)

A BARS/NARS dialing plan that is the same length or longer than the ESDN, should not have the same leading digits as the ESDN. If there is a BARS/NARS dialing plan equal to or longer than the ESDN, and all the leading digits of that internal DN match the ESDN digits, then calls do not terminate on that dialing plan, because ESA calls receive priority.

Similarly, a BARS/NARS dialing plan that is shorter than the ESDN, must not have the same leading digits as the ESDN. If there is a BARS/NARS dialing plan, shorter in length than the ESDN, and all the leading digits of that internal DN match the ESDN digits, then callers may be prevented from making ESA calls.

The system administrator must define ESDN as a BARS/NARS SPN, to ensure that AC+ESDN calls are recognized as ESA calls.

The system administrator must define a local terminating route list index for the SPN that is configured with the ESDN, to ensure that AC+ESDN calls are recognized as ESA calls. For example, no ESA Calling Number or On-Site Notification is composed.

**Basic Rate Interface Phone Calling Line Identification Restriction
CLIR Phone to ISDN trunks**

When a CLIR phone initiates an ESA call, the ESA feature overrides the BRI Set CLIR feature. Therefore, the calling number and Calling Party Name Display (CPND) presentation indicators are set to display allowed.

CLIR Phone to CAMA or other trunks

As per existing operation, the Basic Rate Interface (BRI) Phone Calling Line Identification Restriction (CLIR) feature applies to CLIR Phone to ISDN trunk calls only.

Calling Party Privacy

Display of Calling Party Denied

Both Calling Party Privacy and Display of Calling Party Denied have the potential to mark a call as 'Private', and set the Presentation Restriction indicators or outpulse a Privacy code (for example *67). The ESA feature overrides all such privacy indications, except in the case of an incoming ISDN Tandem trunk (the assumption is that the originating system will have already set the indicator to 'Presentation Allowed' because it is an emergency call).

If the source of the call, either phone, console, or trunk, has a privacy indicator set, [Table 29 "Privacy indication" \(page 174\)](#) indicates the status of the privacy indication on the outgoing trunk for ESA calls.

Table 29
Privacy indication

TO FROM	CAMA trunk	ISDN trunk	Other trunk
Phone or console	No privacy indication possible	No privacy indicator sent	No privacy indicator sent
ISDN trunk	No privacy indication possible	Incoming privacy indicators are tandemed	Privacy indicator (DTPI/DPPI in LD 16) sent
Non-ISDN trunk	No privacy indication possible	No privacy indicator sent	No privacy indicator sent

Coordinated Dialing Plan

When an Internal DN or Coordinated Dialing Plan (CDP) steering code is equal to or longer than the ESDN and all of the leading digits of such an Internal DN match with those of the ESDN, then calls do not terminate onto these Internal DNs or CDP steering codes, as ESA calls are given priority. Conversely, if there is any Internal DN that is shorter than the ESDN and all of the leading digits match those of the Internal DN, then it may prevent callers from placing ESA calls.

Direct Inward System Access

An incoming trunk that has obtained system access using a DISA DN can initiate a tandem ESA call. When a tandem ESA call is initiated using DISA, it is treated in the same manner as any other tandem ESA call.

Feature Group D

The Feature Group D (FGD) route cannot be defined as the Customer's outgoing Emergency Services Route (ESRT).

For an FGD-to-CAMA tandem ESA call:

- If no FGD Automatic Number Identification (ANI) is passed in, then as FGD is a non-ISDN trunk, the ESA Calling Number, composed for the incoming FGD trunk, is outpulsed as the calling number using CAMA MF signaling over the outgoing CAMA trunk.
- If FGD ANI is passed in and the system does not have the ESA_SUPP package equipped, the FGD ANI is ignored and the ESA Calling Number, composed for the incoming trunk, is outpulsed as the calling number using CAMA MF Signaling over the outgoing CAMA trunk.
- If FGD ANI is passed in and the system has the ESA_SUPP package equipped, the FGD ANI is outpulsed as the calling number using CAMA MF Signaling over the outgoing CAMA trunk.

For an FGD-to-ISDN tandem ESA call:

- If no FGD ANI is passed in, then as FGD is a non-ISDN trunk, the ESA Calling Number, composed for the incoming FGD trunk, is sent as the CLID over the outgoing ISDN trunk.
- If FGD ANI is passed in and the system does not have the ESA_SUPP package equipped, the FGD ANI is ignored and the ESA Calling Number is sent as the CLID over the outgoing ISDN trunk.
- If FGD ANI is passed in and the system has the ESA_SUPP package equipped, the FGD ANI is sent as the CLID over the outgoing ISDN trunk.

The ESA feature overrides the FGD ANI display suppression functionality if it is configured for the incoming FGD trunk (SHAN = NO in LD 19).

In-Band ANI

For a non-ISDN-to-CAMA tandem ESA call:

- If no In-Band ANI is passed in, then as the incoming trunk is a non-ISDN trunk, the ESA Calling Number, composed for the incoming trunk, is outpulsed as the calling number using CAMA MF signaling over the outgoing CAMA trunk.

- If In-Band ANI is passed in and the system does not have the ESA_SUPP package equipped, then the In-Band ANI is ignored, and the ESA Calling Number is outpulsed as the calling number using CAMA MF signaling over the outgoing CAMA trunk.
- If In-Band ANI is passed and the system has the ESA_SUPP package equipped, then the In-Band ANI is outpulsed as the calling number using CAMA MF signaling over the outgoing CAMA trunk.

For a non-ISDN-to-ISDN tandem ESA call:

- If no In-band ANI is passed in, then as the incoming trunk is a non-ISDN trunk, the ESA Calling Number composed for the incoming trunk is sent as the CLID over the outgoing ISDN trunk.
- If In-Band ANI is passed in and the system does not have the ESA_SUPP package equipped, then the In-Band ANI is ignored and the ESA Calling Number is sent as the CLID over the outgoing ISDN trunk.
- If In-Band ANI is passed in and the system has the ESA_SUPP package equipped, then the In-Band ANI is sent as the CLID over the outgoing ISDN trunk.

Incoming Trunk Programmable CLID

The Incoming Trunk Programmable CLID feature allows incoming non-ISDN trunk routes to be provisioned for a programmable billing number when the incoming non-ISDN trunk is tandemed onto an outgoing ISDN trunk. For a non-ISDN trunk initiated ESA call, the ESA feature takes precedence over the Incoming Trunk Programmable CLID feature. Therefore, the ESA Calling Number, composed for the incoming non-ISDN trunk, is sent as the CLID over the outgoing ISDN trunk.

ISDN CLID Enhancements

With the ESA feature, the ISDN package 145 restriction is removed for the ISDN CLID Enhancements feature. Also, ISDN CLID Enhancements is modified to allow the configuration of ESA data within each CLID entry. If the call is identified as an ESA call, the CLID ESA configuration is referenced for ESA Calling Number composition.

ISDN Enbloc Dialing

ESA Call Processing takes precedence over the ISDN Enbloc Dialing feature. As soon as the ESDN is dialed, if the outgoing trunk for the ESA call is an ISDN trunk, the call is initiated for call termination.

ISDN Network Attendant Service

When an ESA call is intercepted to the local attendant, CLID/ANI is unavailable. If the ESA call is routed to a network attendant through NAS routing, this call is not treated as an ESA call by the NAS feature, and the existing NAS feature constructs the appropriate CLID.

Meridian 911

An incoming Meridian 911 (M911) call cannot tandem out of the system. Therefore, there is no interaction between the M911 and ESA features.

Network Call Redirection

As per existing Network Call Redirection (NCRD) operation, when a call is redirected, a NOTIFY message is sent to the originating and/or terminating node to request the connected party number. Upon receiving the NOTIFY message, the connected party number is composed and then sent by the existing ISDN CLID Enhancements feature. The ESA Calling Terminal Identification function is not invoked to compose the connected party number.

Virtual Network Services

Virtual Network Services (VNS) trunks are treated in the same manner as ISDN trunks.

Feature packaging

The ESA feature requires the following software packages, according to the type of functionality define:

Total functionality

Emergency Services Access (ESA) is package 329 and provides the following functions:

- Emergency Services Access Call Recognition
- Emergency Services Access Call Routing to CAMA, 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
- 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 to CAMA conversions
- On-Site Notification

Emergency Service Access Calling Number Mapping (ESA_CLMP) is package 331 and provides the following function:

- Translation of non-Direct Inward Dialing (non-DID) numbers

Emergency Service Access Subnet LIS (ESA_SUBNET_LIS) is package 336 and provides the following function:

- Allows the use of an internal Subnet-Lookup Location Information Service to provide basic location determination for IP phones.

Emergency Service Access External DM Interface (ESA_EXTERNAL_DM) is package 337 and provides the following function:

- 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.

Partial functionality

ESA Call Recognition:

- Access (ESA) is package 329

ESA Call Termination Identification:

- Emergency Services 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:

- Emergency Services Access (ESA) package 329
- Emergency Services Access Supplementary (ESA_SUPP) package 330 (required if the customer is to offer ISDN-to-CAMA tandem ESA calls, and wants to allow the CLID passed in by the incoming ISDN trunk to be converted to be outpulsed as the CAMA calling number)
- Automatic Number Identification (ANI) package 12 (required for CAMA MF outpulsing, if CAMA trunks are used for outgoing ESA calls)
- Integrated Services Digital Network (ISDN) package 145 (required if the ESA calls are transported over outgoing ISDN trunks)

ESA On-Site Notification:

- 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 originator's name to be displayed on the OSN phone)
- Office Data Administration System (ODAS) package 20 (required to provide the originator's DES information on the call record, and the originator's DES information to be displayed on the OSN phone)

Feature implementation

Task summary list

The following steps are required to implement ESA:

1. LD 15 – Modify the customer CLID database to allow ESA calling number composition, using LD 15.
2. LD 16 – Configure CLID entries for non-ISDN routes, so that when an incoming non-ISDN trunk initiates a tandem ESA call, the ESA Calling Terminal Identification function composes an ESA calling number to identify the incoming trunk. This is done using LD 16.
3. LD 14 – Configure the ESA trunk type using LD 14. Only the following trunk types may be used to handle ESA calls:
 - Centralized Automatic Message Accounting (CAMA)
 - Central Office (COT)
 - Direct Inward Dial (DID)
 - Foreign Exchange (FEX)
 - TIE
 - Wide Area Telephone Service (WATS)
4. LDs 10, 11 and 27– Configure a CLID entry for analog (500/2500 type) phones, Meridian proprietary phones, and BRI phones, using LD 10, LD 11, and LD 27 respectively.
5. LD 17– Configure an OSN output device.
6. LD 11 – Configure an OSN phone.
7. LDs 10, 11, and 27– Configure terminal designator (DES) data for analog (500/2500-type) phones, Meridian 1 proprietary phones, and BRI phones.
8. LD 24 – Configure ESA data.
9. LD 16 – Configure ESA route data.

10. LD 86 – If BARS/NARS is used, configure ESA digit manipulation and call routing
11. LD 90 – Configure ESA call recognition. This is to allow Access Code + ESDN dialing to be recognized and treated as an ESA call.

LD 15 Modify the customer CLID database to allow ESA calling number composition.

Prompt	Response	Description
REQ:	CHG	Change
TYPE:	NET	Networking data
CUST		Customer number
	0-99	Range for Large System, Call Server 1000E, and Media Gateway 1000E
	0-31	Range for Small System, CS 1000S system, Media Gateway 1000B, and Media Gateway 1000T
...		
CLID	YES	Configure Calling Line Identification (CLID) options.
- SIZE	0-4000	Specify the maximum number of CLID entries required.
- INTL	1-4	Country code (1 to 4 digits).
- ENTRY	0-(1)-3999	CLID entry to be configured.
		CLID entries must be between 0 and the value entered at the size prompt - 1. ENTRY is repeated until a <cr> is entered.
- HNTN	x...x	National code for home national number (1 - 6 digits). Precede with 'X' to delete digits.
- ESA_HLCL	x...x	Home local code for Emergency Service Access call. Up to 12 digits are accepted. Precede with 'X' to delete entry.
- ESA_INHN	(NO) YES	Do not insert HNTN in front of ESA_HLCL. Insert HNTN in front of ESA_HLCL.
- ESA_APDN	(YES) NO	Append the originating DN after ESA_HLCL. Do not append the originating DN after ESA_HLCL.
...		
- ENTRY	xx	Configure another CLID entry. ENTRY is repeated until a <cr> is entered.

LD 16 Configure CLID entries for a non ISDN route.

Prompt	Response	Description
REQ	CHG	Change
TYPE	RDB	Route Data Block

Prompt	Response	Description
CUST	xx	Customer number as defined in LD 15.
ROUT		Route number
	0-511	Range for Large System, Call Server 1000E, and Media Gateway 1000E
	0-127	Range for Small System, CS 1000S system, Media Gateway 1000B, and Media Gateway 1000T
...		
TKTP	aaa	Trunk type where: aaa = CAM, COT, DID, FEX, TIE, WAT
ISDN	NO	Route is not an ISDN route.
...		
- ISAR	NO	Route is not an ISA service route.
...		
ACOD	x...x	Route Access Code.
		It must not conflict with numbering plan. Up to 4 digits (7 digits if the DN Expansion package equipped.)
CLEN	0-(1)-3999	Calling Line Identification entry number. Configured in LD 15. CLEN will not be prompted for NI-2 CBC or ISA master routes.

LD 14 Configure the ESA trunk type.

Prompt	Response	Description
REQ	NEW	Add new data.
TYPE	aaa	Trunk type, where aaa can be one of the following: CAM = Centralized Automatic Message Accounting COT = Central Office DID = Direct Inward Dial FEX = Foreign Exchange TIE = TIE WAT = Wide Area Telephone Service
TN		Terminal Number
	l s c u	Format for Large System, Call Server 1000E, and Media Gateway 1000E, where l = loop, s = shelf, c = card, u = unit
	c u	Format for Small System, CS 1000S system, Media Gateway 1000B, and Media Gateway 1000T, where c = card and u = unit
RTMB		Route number and Member Number

Prompt	Response	Description
	0-511 1-4000	Range for Large System, Call Server 1000E, and Media Gateway 1000E
	0-127 1-4000	Range for Small System, CS 1000S system, Media Gateway 1000B, and Media Gateway 1000T

Note: While LD 10 is loaded, you may want to configure the terminal designator data required for On-Site Notification configuration for analog (500/2500-type) phones. Refer to ["LD 10 – Configure terminal designator \(DES\) data for Analog \(500/2500 type\) phones."](#) (page 184).

LD 10 Configure a CLID entry for analog (500/2500 type) phones.

Prompt	Response	Description
REQ:	NEW CHG	Add, Change
TYPE:	500	Phone type
TN		Terminal Number
	l s c u	Format for Large System, Call Server 1000E, and Media Gateway 1000E, where l = loop, s = shelf, c = card, u = unit
	c u	Format for Small System, CS 1000S system, Media Gateway 1000B, and Media Gateway 1000T, where c = card and u = unit
...	...	...
DN	xxxx (0)-N	DN and CLID entry. N = CLID SIZE-1 (where SIZE is defined in LD 15).

Note: While LD 11 is loaded, you may want to configure the OSN phone (refer to ["LD 11 – Configure the On-Site Notification phone."](#) (page 184)) and terminal designator data required for On-Site Notification configuration for Meridian 1 proprietary phones (refer to ["On-Site Notification Configuration"](#) (page 183))

LD 11 Configure Calling Line Identification for Meridian 1 proprietary phones.

Prompt	Response	Description
REQ:	NEW CHG	Add, Change
TYPE:	xxxx	Phone type
TN		Terminal Number
	l s c u	Format for Large System, Call Server 1000E, and Media Gateway 1000E, where l = loop, s = shelf, c = card, u = unit

Prompt	Response	Description
KEY	c u aa bbb yyyy (0)-N	Format for Small System, CS 1000S system, Media Gateway 1000B, and Media Gateway 1000T, where c = card and u = unit Directory Number, where: aa = key number. bbb = key type or function; one of the following: SCR, SCN, MCR, MCN, or HOT. yyyy = DN. (0)-N = CLID entry, where N = SIZE-1 (SIZE is defined in LD 15).

Note: While LD 27 is loaded, you may want to configure the terminal designator data required for On-Site Notification configuration for BRI phones. Refer to ["On-Site Notification Configuration" \(page 183\)](#).

LD 27 Configure Calling Line Identification for Basic Rate Interface phones.

Prompt	Response	Description
REQ	NEW CHG	Add, Change
TYPE	TSP	Administer the Terminal Service Profile on the Digital Subscriber Loop.
DSL	l s c dsl c dsl	Digital Subscriber Loop address (Large System) Small System
...		
DN	xxxx (0)-N	DN and CLID entry. N = CLID SIZE-1 (where SIZE is defined in LD 15).

On-Site Notification Configuration

LD 17 Configure an OSN output device.

Prompt	Response	Description
REQ	CHG	Change
TYPE	ADAN	Action Device and Number
- ADAN	CHG bbb x	Change Action Device and Number where: bbb = TTY, or PRT x = Port number
...		
USER	MTC	Maintenance output device.

Note 1: Only one OSN phone can be configured for a customer.

Note 2: After the OSN phone has been defined, an Equipment Datadump (EDD command in LD 43) must be performed so that the On-Site Notification Directory Number (OSDN) can be programmed in LD 24, as defined on "[Emergency Services Access Configuration.](#)" (page 185)

LD 11 Configure the On-Site Notification phone.

Prompt	Response	Description
REQ:	NEW CHG	Add, Change
TYPE:	xxxx	Phone type
TN		Terminal Number
	l s c u	Format for Large System, Call Server 1000E, and Media Gateway 1000E, where l = loop, s = shelf, c = card, u = unit
	c u	Format for Small System, CS 1000S system, Media Gateway 1000B, and Media Gateway 1000T, where c = card and u = unit
...		
CUST	xx	Customer number as defined in LD 15.
...		
KEY	aa bbb yyyy (0)-N	Directory Number, where: aa = key number. bbb = key type or function; one of the following: SCR, SCN, MCR, MCN, or HOT. yyyy = DN. (0)-N = CLID entry, where N = SIZE-1 (SIZE is defined in LD 15).
KEY	xx OSN	Key number and the On-Site Notification key mnemonic.

LD 10 Configure terminal designator (DES) data for Analog (500/2500 type) phones.

Prompt	Response	Description
REQ:	NEW CHG	Add, Change
TYPE:	500	Phone type
TN		Terminal Number
	l s c u	Format for Large System, Call Server 1000E, and Media Gateway 1000E, where l = loop, s = shelf, c = card, u = unit
	c u	Format for Small System, CS 1000S system, Media Gateway 1000B, and Media Gateway 1000T, where c = card and u = unit

Prompt	Response	Description
...	...	...
DES	d...d	Office Data Administration System Station Designator.

LD 11 Configure terminal designator (DES) data for Meridian 1 proprietary phones.

Prompt	Response	Description
REQ:	NEW CHG	Add, Change
TYPE:	xxxx	Phone type
TN		Terminal Number
	l s c u	Format for Large System, Call Server 1000E, and Media Gateway 1000E, where l = loop, s = shelf, c = card, u = unit
	c u	Format for Small System, CS 1000S system, Media Gateway 1000B, and Media Gateway 1000T, where c = card and u = unit
...		
DES	d...d	Office Data Administration System Station Designator.

LD 27 Configure terminal designator (DES) data for Basic Rate Interface phones.

Prompt	Response	Description
REQ	NEW CHG	Add, Change
TYPE	TSP	Administer the Terminal Service Profile on the Digital Subscriber Loop.
DSL	l s c dsl c dsl	Digital Subscriber Loop address (Large System) Small System
...		
DES	d...d	Office Data Administration System Station Designator.

Emergency Services Access Configuration.**LD 24 Configure Emergency Services Access Data.**

Prompt	Response	Description
REQ	NEW CHG	Add, Change
TYPE	ESA	Emergency Services Access
CUST	xx	Customer number as defined in LD 15.
ESDN	x...x	Emergency Services Directory Number (for example 911). Up to 4 digits are accepted.

Prompt	Response	Description
ESRT	0-511 0-127	ESA route number For Large Systems For Small Systems The trunk type can be CAM, COT, DID, FEX, TIE, or WAT
DDGT	xxxx	Emergency Services Directing Digits (for example 1, 11, 911, and so on). Up to 4 digits are accepted. The DDGT digits are output as the called number if the ESA call terminates onto an outgoing CAMA trunk. Otherwise, the ESDN is output.
DFCL	x....x	Default Calling Line Identification. The input must be of the following length: - On a system that is not FNP packaged, the input must be nothing, or 7 or 10 digit. If nothing is entered, KP-911-ST is output. - On a system that is FNP packaged, any number of digits, up to 16, are allowed to be entered.
OSDN	x....x	On-Site Notification Directory Number. The input must be a valid single appearance internal DN that belongs to a Meridian 1 proprietary phone configured with an OSN key. This DN must be the same as the OSDN configured for the OSN phone in LD 11. Refer to " LD 11 – Configure the On-Site Notification phone. " (page 184).

LD 16 Configure Emergency Services Access Route Data.

Prompt	Response	Description
REQ	NEW CHG	Add, Change
TYPE	RDB	Route Data Block
CUST	xx	Customer number as defined in LD 15.
ROUT		Route number
	0-511	Range for Large System, Call Server 1000E, and Media Gateway 1000E
	0-127	Range for Small System, CS 1000S system, Media Gateway 1000B, and Media Gateway 1000T
...		

Prompt	Response	Description
TKTP	aaa	Trunk type where: aaa = CAM, COT, DID, FEX, TIE, WAT
...		
STEP	0-511 0-127	ESA alternate route number. For Large Systems For Small Systems

Access Code + Emergency Services Directory Number

For customers using Basic Automatic Route Selection (BARS) or Network Automatic Route Selection (NARS), the following configuration is recommended to allow Access Code (AC) + Emergency Services Directory Number (ESDN) Dialing to be recognized and treated as an emergency call.

LD 86 Configure Emergency Service Access Digit Manipulation for AC + ESDN dialing.

Prompt	Response	Description
REQ	NEW CHG	Add, Change
CUST	xx	Customer number as defined in LD 15.
FEAT	DGT	Digit Manipulation
...		
DMI	1 - 999	Digit Manipulation Table numbers.
		Note: Do not use digit manipulation Table 0, as it results in the incorrect call termination treatment.

LD 86 Configure Emergency Service Access call routing for AC + ESDN dialing.

Prompt	Response	Description
REQ	NEW CHG	Add, Change
CUST	xx	Customer number as defined in LD 15.
FEAT	RLB	Route List Block
...		
RLI	xxx	Route List Index to be accessed.
ENTR	xxx	Entry number for NARS/BARS Route list.

Prompt	Response	Description
LTER	YES	Local Termination entry. This allows the AC+ESDN call to be recognized as an Emergency Services Access call.
DMI	1 - 999	Digit Manipulation Table. Use the table configured in LD 86. This allows the digits after the AC to remain in the call register as a called number. Note: Do not use digit manipulation Table 0, as it results in the incorrect call termination treatment.

LD 90 Configure Emergency Service Access call recognition for AC + ESDN dialing.

Prompt	Response	Description
REQ	NEW CHG	Add, Change
CUST	xx	Customer number as defined in LD 15.
FEAT	NET	Network translation tables
TRAN	aaa	Access code type where aaa: AC1 = Access Code 1 (BARS/NARS) AC2 = Access Code 2 (NARS)
TYPE	SPN	Special code translation data block
- SPN	911	AC+ESDN is recognized as an Emergency Services Access call.
- RLI	xxx	Route List Index. Use Route List Index configured in LD 86.

Example The following is an AC + ESDN configuration example:

1 Configure DMI

```
> ld 86
REQ new
CUST 0
FEAT dgt
DMI 3
```

2 Configure RLB

```
> ld 86
REQ new
CUST 0
FEAT rlb
RLI 2
ENTR 0
LTER yes
DMI 3
```

3 Configure SPN for AC1

```
>ld 90
REQ new
CUST 0
FEAT net
TRAN ac1
TYPE spn
SPN 911
RLI 2
```

4 Configure SPN for AC2

```
> ld 90
CUST 0
FEAT net
TRAN ac2
TYPE spn
SPN 911
RLI 2
```

Feature operation

This section explains how to view and discard caller information on an OSN phone. Also, [Table 30 "OSN key operation" \(page 191\)](#) on [Table 30 "OSN key operation" \(page 191\)](#) summarizes the various events on the OSN phone that may affect the operation of the OSN key.

OSN Phone operation

The purpose of the OSN Phone is to provide basic information about a 911 caller at the time of the call. It does this by linking certain information into the digit display of an Meridian 1 digital phone. This phone must have a single key-lamp pair for the OSN function, as well as other standard keys. For greatest flexibility, it should also be equipped with a DISP (display) key.

Key-lamp states

- If the OSN lamp is dark, there is no ESA information waiting to be displayed.
- If the OSN lamp is flashing, there is information waiting to be displayed.
- If the OSN lamp is steadily lit, there is ESA information being displayed, or in some circumstances can be redisplayed.

To display OSN data

The user can display the ESA information in one of the following two ways:

- Press the DISP key, followed by the OSN key. This leaves the ESA information in a waiting state, which has the advantage of allowing it to be repeatedly re-displayed interspersed with other phone operations. The OSN lamp remains flashing to indicate this.

This operation can be carried out with another call active on the phone, and new calls can be initiated or answered without permanently losing the ESA information. If some of these other operations change the display, the ESA information can be restored by either of the methods described here. You can repeatedly toggle between ESA information and display information for other calls by using this method.

- Press the OSN key only. The OSN lamp changes to steadily lit to indicate that the ESA information is now active on the phone.

Note: Whenever the OSN lamp is steadily lit, any of the following phone operations permanently discard the ESA operation:

- to go on-hook or Release
- initiate or answer another call
- take a call off hold
- any other action that makes the phone active on a non-OSN function

Note: If it is still important, ensure that the ESA information is written down before carrying out one of these operations.

An incoming call can be presented to the phone, but will not overwrite the ESA information. The DISP key, followed by the incoming DN key, allows the incoming call information to be seen, without losing the ESA information. To restore the ESA information, use DISP + OSN.

Operating the OSN key in this fashion does not work if there is another call active on the phone. Release or put on hold all such active calls first.

Note: Any call taken off hold at this point will lose the ESA information.

The ESA information cannot be put "On Hold."

Clearing OSN display

ESA information must be cleared from the OSN phone manually, before another ESA call information can be presented. This is to prevent successive (often related) emergency calls from rippling across the phone before the operator has a chance to properly process them.

To remove the ESA information from the phone, and thus permit the information for another ESA call to come in, make the ESA information active (OSN lamp steadily lit) and then perform one of the following:

- Go on-hook.
- Press the Release (RLS) key.
- Answer an incoming call, make a new call, or return to a previously established call by going off-hook or pressing an appropriate key.

OSN key operation and lamp state

Table 30 "OSN key operation" (page 191) describes the various events on the OSN phone that can affect the operation of the OSN key.

Table 30
OSN key operation

Event	Current OSN Key Lamp State		
	Dark There is no ESA caller information to be displayed.	Flashing An ESA caller information is waiting to be displayed.	Lit An ESA caller information is being displayed.
A new ESA call is presented to the OSN phone.	OSN buzzing is given to the OSN phone. The OSN key lamp changes to flashing, and the caller information is linked to the OSN key.	The new caller information is not linked as there is a caller information already linked to the OSN key. The OSN key lamp remains flashing, and the previous caller information remains linked to the OSN key.	The new caller information is not linked as there is a caller information already linked to the OSN key. The OSN key lamp remains lit, and the previous caller information remains linked to the OSN key.
The Display (DISP) key is pressed, and then the OSN key.	No ESA caller information is displayed. The DISP key lamp changes to dark. The OSN key lamp remains dark.	The caller information that is linked to the OSN key is displayed. The DISP key lamp changes to dark. The OSN key lamp remains flashing, and the caller information remains linked to the OSN key.	The caller information that is linked to the OSN key is redisplayed. The DISP key lamp changes to dark. The OSN key lamp remains lit, and the caller information remains linked to the OSN key.
The OSN key is pressed when the OSN phone is not in idle state.	The operation is ignored. The OSN key lamp remains dark.	The operation is ignored. The OSN key lamp remains flashing, and the caller information remains linked to the OSN key.	The operation is ignored. The OSN key lamp remains lit, and the caller information remains linked to the OSN key.

	Current OSN Key Lamp State		
The OSN key is pressed when the OSN phone is in idle state.	The operation is ignored. The OSN key lamp remains dark.	The caller information linked to the OSN key is displayed. The operation is ignored. The OSN key lamp changes to lit, and the caller information remains linked to the OSN key. The OSN buzzing ends, if it has not already timed out. While the OSN key lamp remains lit, the OSN phone is in active state, with the OSN key being the active key.	The operation is ignored. The OSN key lamp remains lit, and the caller information remains linked to the OSN key.
A new ESA call is presented to the OSN phone.	The new call is presented as per normal operation. The OSN key lamp remains dark.	The new call is presented as per normal operation. The OSN key lamp remains flashing, and the caller information remains linked to the OSN key.	The new call is presented to the OSN phone. The phone display continues to show the existing ESA caller information; it is not replaced by the new caller information. The OSN key lamp remains lit, and the caller information remains linked to the OSN key.

	Current OSN Key Lamp State		
A new ESA call is presented to the OSN phone. The Display (DISP) key is pressed, and then the DN key on which the new call has been presented.	The caller information associated with the new call is displayed. The OSN key lamp remains dark.	The caller information associated with the new call is displayed. The OSN key lamp remains flashing, and the caller information remains linked to the OSN key.	The ESA caller information that was being displayed is replaced by the new caller information. The OSN key lamp remains lit, and the caller information remains linked to the OSN key. <i>Note: To redisplay the previous caller information, press the DISP key and then the OSN key.</i>
The OSN phone user goes on-hook, or presses the RLS key.	The OSN key lamp remains dark.	The OSN key lamp remains flashing, and the caller information remains linked to the OSN key.	The OSN phone is returned to the idle state. The OSN key lamp changes to dark, and the caller information is erased.
The OSN phone user makes a new call, returns to a previously established call, or answers an incoming call.	The OSN key lamp remains dark.	The OSN key lamp remains flashing, and the caller information remains linked to the OSN key.	The OSN key lamp changes to dark, and the caller information is erased.

ESA call processing

ESA Call Processing is the feature component that selects the appropriate emergency route and composes an appropriate CLID for the emergency caller.

ESA call processing applies to both IP phones and non IP phone, as well at Attendants and incoming trunks (for tandem ESA calls, for example).

ESA call processing is separate from location management. Location management is the ESA feature functionality that allows for the determination and maintenance of current location data for an IP phone client.

ESA call processing uses the operational location data taken from either the TN Table (for IP phones) or the home location data (for non IP lines).

ESA call processing is compatible with ESA configuration from previous software releases.

ERL 0

ERL 0 is a special value that indicates that basic ESA Data Block (LD 24) parameters are to be used. It is used with specific telephony client types and configurations, as follows:

- Non IP telephones (which are statically provisioned).
- Manual Update IP phones (which are statically provisioned).
- Auto Update IP phones not yet located (an error condition).
- Auto Update IP phones that could not be located (an error condition).

Under normal circumstances, an Auto Update IP phone should not be assigned to ERL 0 by either the Location Information Service (LIS) or DM location determination mechanisms.

The behavior of IP phones and non IP phones set with ERL 0 is detailed in the following table:

Just as phones configured to use ERL 0, phones in a disabled ERL also receive emergency service according to the basic ESA Data Block (LD 24). See also ERL table on page 127.

Operational characteristics of ERL 0 are as follows:

- There is no Site Name and no Location Description (in the OSN record).
- No dynamic ELINs can be configured for ERL 0.
- Emergency route is per basic ESA Data Block (LD 24).
- If CLID ESA data is configured for the phone, use it. Otherwise, calling number is DFCL per the basic ESA Data Block (LD 24).
- OSN DN is per basic ESA Data Block (LD 24).

Route selection

ESA routes are configured in both the basic ESA Data Block (LD 24) and, optionally, the ERL table (LD 117).

ESA uses the ERL (Emergency Response Location) parameter to denote location for all phone types. This is used to reference routing data in the ERL table – except in the case of an ERL value of 0, which is a reserved value signifying that the routing data in the basic ESA Data Block (LD 24) should be used.

A comparison of route selection is shown in the table that follows.

If a route is not specified in the ERL table then ESA call processing uses ESA Data Block (LD 24) route parameters.

Calling number composition

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

ESA configuration is now common for all phone types in the enterprise.

All phone types have an ERL (Emergency Response Location) parameter that is used to denote their location. This is used to reference CLID data in the ERL table – except for ERL 0, which is a reserved value signifying that the basic ESA Data Block should be used.

In addition to the ERL parameter, IP phones also have an ECL (Emergency Caller Location) parameter to denote more specific location. This is also used for DID phones, which can use their DID as CLID if they are at their provisioned location (that is, the current ECL of the DID phone is the same as the home ECL).

The mechanisms used in composing the calling number for a phone, in order of precedence, are as follows:

1. 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 locations.
2. Dynamic ELIN, as defined for the ERL (optional).
3. Locator (static ELIN), as defined for the ERL.
4. Default CLID (DFCL in LD 24).

A more detailed description of the operation of these calling number generation mechanisms is provided in the following table:

If DFCL is assigned (rather generating than a calling number) then a system message is generated.

If no Calling Number is composed then a system message is generated.

Trunk-initiated ESA call The calling number composition for a trunk initiated ESA call is described as follows:

- If a valid CLID is passed in by the trunk, it is used as the calling number for the emergency caller. Otherwise, the calling number is composed locally using the CLID blocks for the route.

- Trunk initiated emergency calls are routed as configured in the basic ESA Data Block (LD 24).
- There is no Site Name and no Location String (in the OSN record), as the Basic ESA Data Block (LD 24) does not have these configured.

Non 7/10 digit calling numbers When CAMA trunks are used for ESA, a valid ANI can be either 7 or 10 digits.

Previously, it was possible to configure a non 7/10 digit Default CLID (DFCL) only if FNP was set to YES. Now, if FNP is set to NO, a warning message is generated instead of rejecting the non 7/10 digit length DFCL. This is because it has been recognized that the non 7/10 digit length DFCL may actually be valid on a non CAMA trunk. The warning message is also generated during emergency call processing, but only when the ANI package (12) is unrestricted.

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 FNP cannot be checked (as static ELIN information 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 is sent to the PSAP.

System messages System alarms and messages associated with CLID composition are detailed in the following table:

Client / network scenarios

The following sections detail the operation of ESA call handling for various client / network scenarios. For the purposes of the scenarios described, conventions are made as follows:

- Statically provisioned phones are understood to include the following phone types:
 - Non IP telephones – whether Analog, Digital, Attendant consoles, or BRI phones.
 - IP phones set to Manual Update – for example, all IP phones immediately after a software version upgrade.
- Auto Update phones are understood to include the following phone types:

- Desktop IP phones – that is, IP phones that have a wired connection and are not wireless handsets.
- IP Softphones – these may be wireless.
- Mobile IP phones – IP phones that are mobile because they make use of WLAN handsets.

A Local Gateway is defined as being the point of connectivity to the PSAP, located in the same E911 Tandem area as the caller IP phone.

The following scenarios apply to all phone types, both IP and non IP.

Local ERL This Client / Network Scenario is described as having the telephony client making an emergency call from a location that has an ERL defined for a location with an onsite call server. Functional client examples covered by this scenario include the following:

- Any phone located at a main call processing site.
- Any telephone mobility within the main call processing site.
- Location data can be static or automatically assigned.

Key configuration assumptions for this scenario:

- If a phone is set to Auto Update, then a location determination mechanism (LIS or DM) determines its current location.
- Optionally, the Dynamic ELIN functionality may be used in assigning caller numbers for phones making emergency calls.

The following is a description of ESA Call Handling under this scenario:

- A CLID is composed using any of the mechanisms previously described.
- The emergency call is routed to the local PSAP – the routing parameters used are located in either the ERL table (LD 117) or the Basic ESA Data Block (LD 24).

Optionally, if a Dynamic ELIN is provisioned for the local ERL, then it is used as CLID and mapped to the emergency caller. When the emergency call is routed to the local PSAP, the Dynamic ELIN conveys location information to the PSAP that allows a direct callback to the emergency caller's phone. See Dynamic ELIN on page 159.

This Client /Network Scenario is illustrated by the following diagram:

CS (call server) A maps an ELIN to the emergency caller, as illustrated by the following:

CS (call server) A then routes the call over a local CO trunk to PSAP A, according to the ERL table:

Because the ERL is local, the routing parameters in the ERL table are optional – falling back to the routing parameters contained in the Basic ESA Data Block (LD 24) is acceptable.

In this case, the static ELIN (Locator) is not used, because an ELIN was assigned.

The emergency caller can be called back directly by the PSAP, using the Dynamic ELIN mapped to the caller's phone.

Remote ERL with gateway This Client / Network Scenario is described as being where the client is making an emergency call from a remote location that has an ERL defined. There is a gateway call server local to the caller's physical location, but when the emergency call is made it goes to a different call server (the caller's home call server) for ESA call handling.

Functional client examples covered by this scenario include the following:

- A Desktop phone located at an integrated remote Survivable Branch Office (SBO) or Survivable Remote Gateway (SRG).
- A Desktop phone at an independent remote location – an office not directly serviced by their provisioned call server, for example.
- Mobility to a different site within the enterprise, including:
 - VO logs in at a recognized location
 - Branch Users.
 - Phones that have been picked up and moved temporarily to a different site within enterprise network.

Key configuration assumptions for this scenario:

- If a phone is set to Auto Update, then a location determination mechanism (LIS or DM) determines its current location.

The following is a description of ESA Call Handling under this scenario:

- When the emergency call reaches the caller's home call server, the home call server ERL table (LD 117) is used to specify an ELIN for the emergency caller's phone (at its remote location). This can be a Dynamic ELIN if the home call server has a way to route calls directly back to the caller at the remote location, but otherwise the ELIN assigned to the caller's phone should be static (that is, the DID DN of the zone phone at the caller's physical location).

- The ERL table (LD 117) at the caller's home call server specifies a route to a tandem gateway in the phone's area. The emergency call is then routed back to the remote gateway (call server).
- The remote call server then reprocesses the ESA call as a trunk initiated ESA call and gives local treatment as specified in the ESA Data Block (LD 24). The call is routed to the remote location's registered PSAP, using the CLID assigned by the home call server. Generally speaking, this CLID references the "zone phone" at the remote location, and this is where any PSAP callbacks will go.

A Branch User registered to a Main Office is a prime example of this scenario.

A VO user whose location is recognized can also be handled this way.

This Client /Network Scenario is illustrated by the following diagram:

In the diagram, CS B is the gateway local to ERL 5.

CS A assigns an ELIN to the emergency call, according to its ERL table.

CS A routes the call over a tandem trunk to CS B, according to its ERL table as shown by the following:

On CS B, the tandem (trunk-initiated) ESA call is handled as a "local ERL", which uses LD 24 (basic) ESA parameters to route an emergency call:

- CS B processes trunk-initiated ESA call.
- CS B routes the call over a local trunk to PSAP B, according to its basic ESA Data Block.

CS B simply passes the CLID through to the PSAP.

The emergency caller cannot be called back directly. Instead, the zone phone receives any callbacks.

Remote ERL without gateway This Client / Network Scenario is described as being where the client is making an emergency call from a remote location that has an ERL defined for it, but no gateway at the caller's physical location. When the emergency call is made it goes to a remote call server (the caller's home call server, on which they are registered from their remote location) for ESA call handling.

Functional client examples covered by this scenario include the following:

- A phone at a known off network location. – An enterprise user working from home, for example, and registered with their home call server from their remote location. The user's phone is set to Manual Update and has statically provisioned location data.

- A Branch Office without PSTN trunks (or no PSTN trunks available) – phones at this location are set to Auto Update, and an LIS or DM is in place to assign current location data.

The following is a description of ESA Call Handling under this scenario:

If the emergency caller is registered to a system but there is no enterprise gateway at their location, then a static ELIN is used as a CLID for the caller's phone and the emergency call is routed to their local PSAP. The static ELIN refers to another (fixed) phone at the same location that can be called back over the PSTN (this is not a phone registered on the enterprise network, but might be a home phone in the case of the enterprise user working from their home). Subsequent PSAP callbacks will go to the static, non enterprise phone.

The **Remote ERL without gateway** Client /Network Scenario is illustrated by the following diagram:

CS (call server) A assigns a static ELIN (Locator) to the emergency caller's phone, according to its ERL table.

CS (call server) A routes the call to PSAP C directly through the PSTN using the public telephone number of the PSAP , according to its ERL table.

The emergency caller cannot be called back directly, as this would require the callback to be passed through the remote call server. Instead, the defined zone phone at the caller's location receives any subsequent PSAP callbacks.

Unknown location This Client / Network Scenario describes the situation where the client is making an emergency call from a phone in a location that is deemed to be unknown. Some typical examples of this scenario are as follows:

- An IP phone (set to Auto Update) before it is located by LIS / DM, including
 - New registration (when using Subnet LIS).
 - New connection (when using DM).
 - VO login when phone cannot cache location.
 - E911 for VO redirection when phone cannot cache location.
- Location cannot be determined, including:
 - Calls made from an unrecognized off enterprise site – the most common situation where this can occur is when a caller is connected to the enterprise network using VPN access, which does not specify

the location where it is in use. Specific examples of this include the following:

- Road Warrior (caller is off enterprise in an arbitrary location, such as a hotel room).
 - The user is working from home. This work at home situation is different from the one described under the Remote ERL without gateway scenario because, in this case, work at home is not their usual work arrangement.
- The caller's IP phone is at enterprise site before full deployment (provisioning of the LIS or ERL is incomplete).
 - The call is placed from a Virtual Office location that is unrecognized by the VO user's home call server.
 - Branch User in Local Mode.
 - The DM is offline or otherwise unavailable.

Key configuration:

- All phones are set to be Auto Update - for whatever reason, however, the Subnet LIS or DM cannot normally determine their location.

The following is a description of ESA Call Handling under this scenario:

- If the caller is a Virtual Office user, and their host call server has ESA configured, the home call server redirects the call back to the host call server for emergency call handling. See E911 for VO on page 143.
- The Basic ESA Data Block (LD 24) at the host call server then sends the emergency call to the local PSAP by means of the default route. The CLID specified for the emergency caller is the DFCL (the security desk or operator for the host call server).
- A system message is generated to indicate that the emergency caller location was unknown and that default emergency call handling was handling was given.

Callbacks

This section describes the behavior of PSAP callbacks under various CLID submission scenarios, as detailed by the following:

DID phone If a an emergency call is placed from a phone that submits the DID number of the phone was used as the CLID sent to the PSAP:

- If the PSAP performs a callback it goes directly to the emergency caller. If the emergency caller does not answer the PSAP callback or the line is busy, the callback may forward to voicemail.

Static ELIN (Locator) If an emergency call is placed from a phone that submits a static ELIN (Locator) as the CLID sent to the PSAP:

- The PSAP callback is performed using the static ELIN, which is the number of a fixed phone at the emergency location. The ELIN may also be configured in the following ways:
 - May be DFCL (such as billing number), used for entire system (site).
 - May be non-enterprise phone (such as a home phone or a hotel front desk).

Dynamic ELIN If an emergency call is placed from a phone that submits a Dynamic ELIN (Locator) as the CLID:

1. The PSAP callback is performed using the Dynamic ELIN, which is call forwarded directly to the emergency caller's phone.
2. If the emergency caller does not answer the PSAP callback or the line is busy, DCFW or SFNA can provide alternate number for callback fallback.

Availability / survivability scenarios

It is essential that reasonable ESA call handling be provided even during a system failure scenario, as efficiently as the capabilities of the remaining resources will allow. Degraded performance, particularly in determining the current location of mobile clients, is acceptable, so long as emergency calls are completed in the best manner available.

Call Server restart / switchover

Full service is eventually restored after a call server restart or call processor switchover (whether graceful or ungraceful). New location updates for connected telephony clients may be delayed, but the location data cached in either the phones or in the IP Line application remains available until the LIS or DM can again start providing the necessary location updates.

The TN Table is stored in unprotected memory, and as such must be rebuilt after a restart or switchover. This happens when the IP phones reregister on the network.

If the Call Server restarts quickly enough, the currently connected IP phones will remain connected to their IP Line application.

- Location data is copied from the IP Line application to rebuild the TN Table as the IP phones reregister themselves on the network.
- If the system is configured with an external DM, the Needs Update flag is preserved by the IP Line application. The DM will perform the subsequent location updates for all phones for which it finds an active Needs Update flag.

- If the system is configured to use the Subnet LIS, the Needs Update flag is set for all Auto Update IP phones. The Subnet LIS performs the required background relocation in the course of its normal operation.

If the Call Server does not restart quickly enough, the IP phones will also restart. See IP phone restart, to follow.

ESA call processing uses the best available location data for IP phones – this is the operational location data for the IP phones, stored in the TN Table.

IP phone restart

If an IP phone restarts, the location data cached on the IP phone itself is used until a location update is available – the stored location data on the IP Phones is cached in DRAM, which survives a restart but is lost during a full power cycle.

If the system is configured to use a DM, a location update is provided in response to the reconnection of the IP phone 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 message is required.

If the system is configured to use the Subnet LIS, the Needs Update flag is set for an Auto Update IP phone in response to its registration, indicating that a background re-location is required.

Alternate Call Server

Because no protected memory is synchronized to the Alternate Call Server, all dynamic data is lost, (including, for example, any active Dynamic ELIN mappings). Otherwise, this is similar to a Call Server restart. The behavior of IP phones making a switchover to an Alternate Call Server is as follows:

- If the switch to the Alternate Call Server is fast enough, the IP phones will remain connected to their IP Line application.
- If the switch to the Alternate Call Server is not fast enough, the IP phones will restart and reconnect.

Geographic Redundancy

Manual Update phones have static location data, which is provisioned by the system administrator.

Auto Update phones have dynamic operational location data, stored in the TN Table, which is populated on the redundant system when the phones reconnect and reregister to it. Registration and location determination

occurs as normal except that a large number of phones will be connecting at the same time. Location data cached on the phone itself is used until a location update is performed.

Signaling Server restart

If the Signaling Server (or VGMC) restarts, 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.

Survivable Branch Office

If a Survivable Branch Office becomes isolated from the Main Office, It provides local ESA service as follows:

- It is essentially a stand-alone system (Local Mode).
- Branch User IP phones reconnect to the Branch Office IP Line application, and register themselves with the SBO call processor.
- The SBO must have its own ESA trunks to route emergency calls to a PSAP - alternatively, ESA calls can be configured to terminate locally.

A Survivable Branch Office has several options for determining location while in Local Mode (and for local phones), as follows:

- If statically configured location data is to be used, the configuration requirements and operational characteristics are as follows:
 - CLID blocks must be provisioned for ANI composition. Otherwise, the DFCL is used as configured in the basic ESA Data Block (LD 24).
 - Emergency route information must be provisioned in the basic ESA Data Block (LD 24).
 - No provisioning of the ERL table is required – all phones default to ERL 0, which indicates basic ESA handling, the same as previous software releases.
- If location determination by Subnet LIS is to be used, the configuration requirements and operational characteristics are as follows:
 - The Subnet lookup table must be provisioned.
 - The ERL table must be provisioned.
 - If isolated from the NRS and/or required gateways, routing to PSAP requires local PSTN trunks.
- If location determination by DM is to be used, the configuration requirements and operational characteristics are as follows:
 - The ERL table must be provisioned.

- If isolated from the DM, location updates for the phones is not possible. If available, location data cached on the phones is used. Otherwise ESA call processing uses basic ESA Data Block (LD 24) for ANI composition and routing.
- If isolated from the NRS or required gateways, routing to PSAP requires access to local PSTN trunks.

The ERL table at the Survivable Branch Office does not require full network wide data, as default handling is provided for any undefined ERL. For example, if an IP phone re-registers at the SBO (either by VO ESA redirection or by fallback to Local Mode), ESA call processing is applied as follows:

- If the local TN is provisioned as Manual Update, then the phone is assigned static location data and receives basic ESA call processing (as defined in the basic ESA Data Block).
- If the local TN is provisioned as Auto Update, then any cached location data stored in the phone is rejected if found to be undefined locally, and unknown location values are assigned. Unknown location indicates default (basic) emergency processing (per LD 24), which is acceptable for a small branch.

Survivable Remote Gateway

A Survivable Remote Gateway provides local emergency call handling in a similar fashion to a Survivable Branch Office:

- It 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.

Although similar to the Survivable Branch Office, the Survivable Remote Gateway does not support location management - this includes data cached in sets, the use of a Subnet LIS or an interface to a DM. As a result, emergency handling for a Survivable Remote Gateway depends entirely on statically configured data.

External DM failure

In the event that the DM fails or otherwise loses connection with the IP Line application (with which it connects using the Zone Manager), the loss of connectivity is detected and system messages are printed. The IP Line application retains the last known location of the IP phones - this data is lost if an IP phone reconnects to an IP Line application, unless it has cached location data.

When communication is restored between the DM and the IP Line application (using the Zone Manager), the DM does one of two things depending upon the nature of the failure:

- If the failure was due to a restart of the DM, then it rediscovers any connected IP phones and provides location updates. This activity may take an extended period of time, as it depends on the actual number of connected IP phones that the DM must go through.
- If the failure was due to a loss of communication between the DM and the IP Line application, then the DM detects any phones requiring location updates using the normal audit process and subsequently provides location updates for these phones only.
- The IP Line application also filters any duplicate location updates, to prevent unnecessary messages from being 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:

Step	Action
------	--------

- | | |
|---|------------------------|
| 1 | Select System . |
|---|------------------------|
-

2 Select **Emergency Services**.

3 Select **Service Parameters**.

—End—

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:

Step	Action
------	--------

- | | |
|---|-------------------------------------|
| 1 | Select System . |
| 2 | Select Emergency Services . |
| 3 | Access Numbers and Routing . |

—End—

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** 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 checkbox, 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 checkbox, 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 misdialled 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.

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 follows:

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 (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:

Step	Action
------	--------

- | | |
|---|------------------------------------|
| 1 | Select System . |
| 2 | Select Emergency Services . |
| 3 | Select Response Locations . |
-

—End—

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.

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.

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. The IP Address and Mask fields are used to identify which subnet entry is to be modified.

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:

Step	Action
------	--------

- | | |
|---|------------------------------------|
| 1 | Select System . |
| 2 | Select Emergency Services . |
| 3 | Select Subnet Information . |
-

—End—

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.

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.

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:

Step	Action
1	Select IP Telephony .
2	Select Emergency Services .
3	Select Dynamic Identification .
—End—	

The Dynamic Location Identification Number page lists every configured Dynamic ELIN in a table format.

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.

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:

Step	Action
1	Select System .
2	Select Maintenance .
3	Select Emergency Services Diagnostics .
—End—	

From here, the administrator can select and execute each command with its respective parameters. Subsequent outputs are displayed in the text area.

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:

Step	Action
1	Select IP Network .
2	Select Maintenance and Reports .
3	Select General Commands .
—End—	

The administrator can select and execute each command with its respective parameters. Subsequent outputs are displayed in the text area.

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:

Step	Action
1	Select Tools .
2	Select Logs and reports .
3	Select IP Phone Location .
—End—	

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.

Emergency Services for Virtual Office

Contents

This section contains information about the following topics:

"Introduction" (page 221)

"Operating parameters" (page 223)

"Feature interactions" (page 225)

"Feature packaging" (page 225)

"Feature implementation" (page 225)

"Feature operation" (page 225)

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 existing 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, the emergency call is routed to the home call server for emergency call handling. The home call server then decides to either redirect the phone back to the originating host call server or apply emergency call handling itself, directly.

ESA has not been implemented correctly if it is configured on the home call server but not 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. In this case, the SBO or SRG 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.

Basic Emergency Service When VO Logged Out

This document contains information about the following topics:

Contents

- "Overview" (page 229)
 - "Making an ESA Call From a Logged Out Phone" (page 230)
 - "Receiving ESA Callback" (page 233)
 - "ESA Call Processing" (page 234)
 - "CLID Composition" (page 234)
 - "ESA VO Logout Timer" (page 234)
 - "Provisioning, Administration and Maintenance" (page 236)
 - "Keeping Logged Out State" (page 237)
 - "Configure ESA Data Block" (page 237)
 - "Sysload" (page 239)
 - "Maintenance and Diagnostics" (page 240)
 - "Warm Start" (page 240)
 - "Emergency Services For Client Mobility" (page 241)
 - "Active Call Fail Over" (page 241)
 - "Context Sensitive Soft Keys" (page 242)
 - "Element Manager" (page 242)

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

Step	Action
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 <i>SYS_04: Register VO Logout Phone with Call Server</i> .
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.

—End—

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.

Step	Action
1	This scenario begins when the call 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 <i>Scenario: The Emergency TN is not registered with Call Server</i>.

- 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.

—End—

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:

Step	Action
1	First, specify the number of emergency TNs in the pool and specify the range of the emergency pool in overlay 24.
2	Second, go to overlay 11 and 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 Overlay 117 to print the used emergency TNs.
4	The <i>isetShow</i> command output is slightly modified to display if the logged out phone is registered with the Call Server, and uses emergency TN.
5	Overlay 32 idu command will be modified to show a different type of TN (VOLO) when queried.
6	Overlay 80 trak command will be modified to show a different type of TN (VOLO) when printing TN info.

—End—

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 its 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

Step	Action
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.

—End—

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 CS1K. 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 its 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

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

Step	Action
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.
—End—	

Scenario: Virtual Office Phone Page Layout

Step	Action
1	Login to CS 1000 Element Manager with a valid user account.
2	In the navigation pane, expand 'System' > 'Emergency Services' and click on <i>Virtual Office Phone</i> 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.

—End—

Scenario: Add Virtual Office Phone Configuration Page Layout

Step	Action
1	Login to CS 1000 Element Manager with a valid user account.
2	In the navigation pane, expand 'System' > 'Emergency Services' and click on <i>Virtual Office Phone</i> 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.

—End—

Scenario: Emergency Service for Virtual Office Phone Configuration for a Customer with ESA Block Configured

Step	Action
1	Login to CS 1000 Element Manager with a valid user account.
2	In the navigation pane, expand 'System' > 'Emergency Services' and click on 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.

—End—

Scenario: Emergency Service for Virtual Office Phone Configuration when there are no customers with ESA block configured

Step	Action
------	--------

- | | |
|---|--|
| 1 | Login to CS 1000 Element Manager with a valid user account. |
| 2 | In the navigation pane, expand 'System' > 'Emergency Services' and click on 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 of Cancel button, the Virtual Office Phone page is displayed. The Add and Delete buttons in Mapped Virtual Office TN Pools table are both disabled. |

—End—

Scenario: Edit Virtual Office Phone Configuration Page Layout

Step	Action
------	--------

- | | |
|---|--|
| 1 | Login to CS 1000 Element Manager with a valid user account. |
| 2 | In the navigation pane, expand 'System' > 'Emergency Services' and click on 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.

—End—

Scenario: Virtual Office Phone Details Page Layout

Step	Action
1	Login to CS 1000 Element Manager with a valid user account.
2	In the navigation pane, expand 'System' > 'Emergency Services' and click on 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.

—End—

Scenario: Call Trace Diagnostics (Overlay 80)

Step	Action
1	Login to CS 1000 Element Manager with a valid user account.
2	In the navigation pane, expand 'System' and 'Emergency Services'. Click on 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 <i>TRAK - Trace calls for the specified TN</i> for the small systems and <i>TRAC - Trace calls for specified TN</i> for large systems is pre-selected.
6	Enter the ESA VOLO TN which is on call in the input text box and click the Submit button.
7	The result in the output text area is the same as mentioned in screen capture of Scenario: LD 80 Trak command.

- 8 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.
- 9 Select LD - 80 Call Trace

—End—

Emergency Services M911 Networked Operation

Contents

This document contains information about the following topics:

["Overview" \(page 247\)](#)

["Feature Description" \(page 249\)](#)

["Configuration and Provisioning" \(page 259\)](#)

["Interactions/Interworkings" \(page 262\)](#)

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 CS 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 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 be 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 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 1: The final routing destination of a 911 call should be to an ACD DN only.

Note 2: 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 and 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 be 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 be 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 *Features and Services (NN43001-106)*, section *ANI Failure*) 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.

VNS

VNS over MCDN is not supported as part of this development.

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.

Emergency Services Access for Europe, the Middle East, and Africa

Contents

This document contains information about the following topics:

["Introduction" \(page 267\)](#)

["Feature packaging" \(page 268\)](#)

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 in the first deployment is be 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. For more information about OSN, see ["On-Site Notification" \(page 115\)](#).

Emergency Services Access Configuration Audit

Contents

This document contains information about the following topics:

"Feature description" (page 271)

"Feature implementation" (page 272)

"CLIDVER input" (page 272)

"CLIDVER output" (page 273)

"CLIDVER report types" (page 274)

"CLID composition for Media Gateway 1000B-initiated calls" (page 284)

"CLID composition for CS 1000E systems" (page 284)

Feature description

The Emergency Services Access (ESA) Configuration Audit feature generates a report for both ESA call processing based on the ESA parameters configured on the Call Server, and for non-ESA Calling Line Identification (CLID) sent for each ESN call type listed in [Table 31 "ESN call types" \(page 272\)](#).

The ESA Configuration Audit feature provides administrators with CLID Verification (CLIDVER) reports that determine how an emergency call is routed, without actually routing the call. These reports include the following details:

- ESA CLID
- ESA Route
- ESA Called Number

- non-ESA CLID sent for each ESN call type (see [Table 31 "ESN call types"](#) (page 272))

Table 31
ESN call types

Abbreviation	Call Type
NATL	National
INTL	International
LOC/UDP*	Location Codes
CDP	Coordinated Dialing Plan
*The Location Codes call type is referenced as UDP in CLIDVER output, instead of the common LOC abbreviation.	

The CLID identified in the reports is the Automatic Number Identification (ANI) sent out of the switch for the ESA call.

This feature does not alter or enhance current ESA functionality, and does not perform call processing. To compose the calling number, information is extracted from the various tables already available on the system, based on the input parameters supplied by the user.

The ESA Configuration Audit feature works in conjunction with the ESA for Europe, the Middle East, and Africa (EMEA) feature to introduce emergency services for enterprises in the EMEA markets. For information about the ESA for EMEA feature, see ["Emergency Services Access for Europe, the Middle East, and Africa"](#) (page 267).

Feature implementation

CLIDVER input

The following overlay table shows a sample series of prompts used to generate a CLIDVER report in LD 20.

LD 20 Generate a CLIDVER report.

Prompt	Response	Description
REQ	PRT	Print
TYPE	CLIDVER	CLID Verification
SORTBY	(DN) TN	The output/report is sorted based on this flag. If the response is DN, the overlay prompts the user to enter the DN, and the output is sorted by the DN. If the response is TN, the overlay prompts the user to enter the TN, and the output is sorted by the TN.

Prompt	Response	Description
ESA_ONLY	(YES) NO	Flag used to decide if the report should contain information for ESA call type only or for all call types. If the ESA package is restricted, this input prompt does NOT appear. The report contains non-ESA data only.
SHORT	(YES) NO	Flag to decide if the output report should be a Short report or a Detail Report.
TN		Terminal Number
	l s c u	Format for Large System and CS 1000E system, where l = loop, s = shelf, c = card, u = unit
	c u	Format for Small System, CS 1000S system, Media Gateway 1000B, and Media Gateway 1000T, where c = card and u = unit
CUST	xx	Customer number as defined in LD 15.
DN	x...x	Directory Number. If no value is entered, the report includes all supported Directory Numbers.
DATE	dd mmm yyyy	Date
PAGE	(NO) YES	Data printed on a per page basis
DES	d...d	Designator

The generated report is based on the responses provided, giving the flexibility of a report based on Directory Numbers, Terminal Numbers, or customers.

CLIDVER output

Table 32 "CLIDVER report input/output combinations" (page 273) shows the various input combinations and corresponding outputs of the CLIDVER report.

Table 32
CLIDVER report input/output combinations

CUST	SORTBY	DN	TN	OUTPUT
<CR>	DN	<CR>	N/A	CLID for all DNs of all Customers - by DN
<CR>	TN	N/A	<CR>	CLID for all TNs of all Customers - by TN
xx	DN	<CR>	N/A	CLID for all DNs of this Customer - by DN
xx	TN	N/A	<CR>	CLID for all TNs of this Customer - by TN
<CR>	DN	Yes	N/A	CLID for all DNs of all Customers - by DN
<CR>	TN	N/A	Yes	CLID for this TN of all Customer - by TN
xx	DN	Yes	N/A	CLID for this DN of this Customer - by DN
xx	TN	N/A	Yes	CLID for this TN of this Customer - by TN

CUST	SORTBY	DN	TN	OUTPUT
<CR>	<CR>	<CR>	N/A	CLID for all DNs of all Customers - by DN
<CR>	<CR>	Yes	N/A	CLID for this DN of all Customers - by DN
xx	<CR>	<CR>	N/A	CLID for all DNs of this Customer - by DN
xx	<CR>	Yes	N/A	CLID for this DN of this Customer - by DN

CLIDVER report types

The following CLIDVER reports are generated based on the responses provided at the ESA_ONLY and SHORT prompts:

- "Short Version ESA-Only" (page 274)
- "Short Version ESA and non-ESA (All)" (page 276)
- "Detailed Version ESA-Only" (page 278)
- "Detailed Version ESA and non-ESA (All)" (page 280)

Note: The ESA_ONLY prompt appears only if ESA package 329 is unrestricted.

Short Version ESA-Only

This CLIDVER report is generated in the Short Version ESA-Only format for the combinations of ESA_ONLY and SHORT prompts shown in [Table 33](#) "ESA_ONLY and SHORT prompts combinations" (page 274).

Table 33
ESA_ONLY and SHORT prompts combinations

ESA_ONLY	SHORT	OUTPUT format
<CR>	<CR>	Short Version ESA-Only
Yes	<CR>	Short Version ESA-Only
Yes	Yes	Short Version ESA-Only

Note: Each line of a Short Version report is a maximum of 80 characters in length. This output format provides support for standard TTY terminals.

The following overlay table shows a series of prompts and responses used to generate a Short Version ESA-Only report.

LD 20 Generate a Short Version ESA-Only report

Prompt	Response	Description
REQ	PRT	Print
TYPE	CLIDVER	CLID Verification

Prompt	Response	Description
SORTBY	TN	The output/report is sorted based on this flag.
ESA_ONLY	YES	Note: If the ESA package is restricted, this input prompt does not appear. The report only contains non-ESA data.
SHORT	YES	Short Version report
TN		Terminal Number
	I s c u	Format for Large System and CS 1000E system, where I = loop, s = shelf, c = card, u = unit
CUST	xx	Customer number as defined in LD 15.

Table 34 "Sample Short Version ESA-Only report output" (page 275) shows a sample Short Version ESA-Only output report for CLIDVER.

Table 34
Sample Short Version ESA-Only report output

CUST 0								
TN	KEY	DN	ZN	CTY P	CLID	R T	CALLED #	
001 0 00 00	00 SCR	7100	---	911	D 6139660100	2	911	
001 0 00 00	01 SCR	7101	---	911	C 0000012345710123	2	911	
001 0 00 00	02 SCR	7102	---	911	C 7717102	2	911	
061 0 00 00	00 SCR	7000	010	911	Z 7077097007	2	444911	
061 0 00 00	01 SCR	7001	010	911	Z 7077097007	2	444911	
061 0 00 00	02 SCR	7003	010	911	C Z 7077097007	2	444911	

Where:

- TN = Terminal Number
- KEY = keys on the set
- DN = Directory Number
- ZONE = Zone number that the set is residing on. Applicable only for telephones on CS 1000E systems or any IP Phones.
- CTYP = call type
- CLID = Calling Line ID
 - "C" indicates that a CLID table entry composes the CLID.
 - "D" indicates that the Default Calling Line Identification (DFCL) composes the CLID.

— "Z" indicates that the LOCATOR in the ZESA table composes the CLID. This also applies to telephones on CS 1000E systems.

- ESRT = route taken by the call
- CALLEDNUMBER = out-pulsed digits

Short Version ESA and non-ESA (All)

This CLIDVER report is generated in the Short Version ESA and non-ESA format for the combinations of ESA_ONLY and SHORT prompts shown in [Table 35 "Input for Short Version ESA and non-ESA" \(page 276\)](#)

Table 35
Input for Short Version ESA and non-ESA

ESA_ONLY	SHORT	OUTPUT format
No	<CR>	Short Version ESA and non-ESA
No	Yes	Short Version ESA and non-ESA

The report is printed in the Short format if the user entered YES or an empty response at the SHORT prompt, and entered NO at the ESA_ONLY prompt.

The following overlay table shows a series of prompts and responses used to generate a Short Version ESA and non-ESA report.

LD 20 Generate a Short Version ESA and non ESA report

Prompt	Response	Description
REQ	PRT	Print
TYPE	CLIDVER	CLID Verification
SORTBY	DN	The output/report is sorted based on this flag.
ESA_ONLY	NO	Note: If the ESA package is restricted, this input prompt does not appear. The report contains non-ESA data only.
SHORT	YES	Short Version report.
CUST	xx	Customer number as defined in LD 15.
DN	7000-7003	Print for Directory Number

Table 36 "Sample Short Version ESA and non-ESA report output" (page 277) shows a sample Short Version ESA and non-ESA output report for CLIDVER. Note that this report is extended to provide information about both ESA and non-ESA call types.

Table 36
Sample Short Version ESA and non-ESA report output

CUST 0									
DN	KEY	TN	ZN	CTYP	CLID	RT	CALLED #		
700 0	00 SCR	061 0 00 00	0 10	911	C 0000012345700 0	0 01	911		
				NATL	00000666				
				INTL	1100000666				
				UDP	5557000				
				CDP	5557000				
700 1	01 SCR	061 0 00 00	0 10	911	C 616967	0 01	911		
				NATL	6166167001				
				INTL	116166167001				
				UDP	3547001				
				CDP	7001				
700 3	02 SCR	061 0 00 00	0 10	911	D 6139660100	0 01	911		

Where:

- TN = Terminal Number
- KEY = keys on the set
- DN = Directory Number
- ZONE = Zone number that the phone is residing on. Supported only for IP Phones or telephones on CS 1000E systems.
- CTYP = call type
- CLID = Calling Line ID
 - "C" indicates that a CLID table entry composes the CLID.
 - "D" indicates that the Default Calling Line Identification (DFCL) composes the CLID.
 - "Z" indicates that the LOCATOR in the ZESA table composes the CLID. This also applies to telephones on CS 1000E systems.

— ESRT = route taken by the call

- CALLEDNUMBER = out-pulsed digits

Detailed Version ESA-Only

Correlating the CLID configuration, Zone configuration, and the ESA configuration to the TN and DN is a time consuming process. The Detailed Version of the CLIDVER report includes data that simplify this process.

In addition to the information provided in the Short Version of the report, the Detailed Version contains the data configured in the CLID table, the DFCL, and data configured for the Zone.

In the Detailed Version ESA-Only report, CLID configurations pertaining to ESA are reported for each given DN. The output appears in print overlay format.

The CLIDVER report is generated in the Detailed Version ESA-Only format for the combinations of ESA_ONLY and SHORT prompts shown in [Table 37 "ESA_ONLY and SHORT prompts combinations"](#) (page 278).

Table 37
ESA_ONLY and SHORT prompts combinations

ESA_ONLY	SHORT	OUTPUT format
<CR>	NO	Detailed Version ESA-Only
Yes	NO	Detailed Version ESA-Only

The following overlay table shows a series of prompts and responses used to generate a Detailed Version ESA-Only report.

LD 20 Generate a Detailed Version ESA Only report

Prompt	Response	Description
REQ	PRT	Print
TYPE	CLIDVER	CLID Verification
SORTBY	TN	The output/report is sorted based on this flag.
ESA_ONLY	NO	Note: If the ESA package is restricted, this input prompt does not appear. The report only contains non-ESA data.
TN		Terminal Number
	I s c u	Format for Large System and CS 1000E system, where I = loop, s = shelf, c = card, u = unit

Prompt	Response	Description
	c u	Format for Small System, CS 1000S system, Media Gateway 1000B, and Media Gateway 1000T, where c = card and u = unit
CUST	xx	Customer number as defined in LD 15.

Table 38 "Sample Detailed Version ESA-only report output" (page 279)
shows a sample Detailed Version ESA-Only output report for CLIDVER.

Table 38
Sample Detailed Version ESA-only report output

CUST 0
DES C2168AB
TN 061 0 00 00
TYPE I2004
ESA
ESDN 911
ESRT 10
DFCL 6139660100
CALLEDNUMBER 444911
OSDN 7000
ZONE
ZONE 11
ZESA ENL
ZBRN YES
ROUTE 2
AC NONE
PRE DGT 444
LOCATOR 7077097007
KEY 00 SCR 7000
NAME DN7000
CLID ENTRY 0
HNTN 613
ESA_HLCL 967
ESA_INHN YES
ESA_APDN YES
DIDN YES
CLID VERIFICATION
CTYP CLID ESRT CALLEDNUMBER
911 Z 7077097007 10 444911

```

KEY 02 SCR 7003
NAME DN7003
CLID ENTRY 10
HNTN 514
ESA_HLCL 5150123
ESA_INHN YES
ESA_APDN NO
DIDN NO
CLID VERIFICATION
CTYP CLID          ESRT CALLEDNUMBER
911   Z 7077097007 10    444911

CUST 1
DES COSETA
TN 01 0 00 00
TYPE 2616
ESA
ESDN 911
ESRT 10
DFCL 6139660100
CALLEDNUMBER 911
OSDN

KEY 00 SCR 7100
NAME DN7100
CLID ENTRY 11
HNTN
ESA_HLCL 771
ESA_INHN YES
ESA_APDN YES
DIDN YES
CLID VERIFICATION
CTYP CLID          ESRT CALLEDNUMBER
911   Z 7717100    10    911

```

Detailed Version ESA and non-ESA (All)

In the Detailed Version ESA-Only and non-ESA report, the CLID configurations pertaining to ESA, as well as non-ESA, is reported for each given DN. The output appears in print overlay format.

The CLIDVER report is generated in the Detailed Version ESA and non-ESA format for the combinations of ESA_ONLY and SHORT prompts shown in [Table 39 "ESA_ONLY and SHORT prompts combinations" \(page 280\)](#).

Table 39
ESA_ONLY and SHORT prompts combinations

ESA_ONLY	SHORT	OUTPUT format
NO	NO	Detailed Version ESA and non-ESA

The report is printed in the Short format if the user entered NO at the SHORT prompt and entered NO at the ESA_ONLY prompt.

The following overlay table shows a series of prompts and responses used to generate a Detailed Version ESA and non-ESA report.

LD 20 Generate a Detailed Version ESA and non ESA report

Prompt	Response	Description
REQ	PRT	Print
TYPE	CLIDVER	CLID Verification
SORTBY	TN	The output/report is sorted based on this flag.
ESA_ONLY	NO	Note: If the ESA package is restricted, this input prompt does not appear. The report contains non-ESA data only.
TN		Terminal Number
	l s c u	Format for Large System and CS 1000E system, where l = loop, s = shelf, c = card, u = unit
	c u	Format for Small System, CS 1000S system, Media Gateway 1000B, and Media Gateway 1000T, where c = card and u = unit
CUST	xx	Customer number as defined in LD 15.

Table 40 "Sample Detailed Version ESA and non-ESA report output" (page 281) shows a sample Detailed Version ESA and non-ESA output report for CLIDVER.

Table 40
Sample Detailed Version ESA and non-ESA report output

CUST 0
DES C2168AB
TN 061 0 00 00
TYPE I2004
ESA
ESDN 911
ESRT 10
DFCL 6139660100
CALLEDNUMBER 911
OSDN 7000
ESRT 15
ZONE
ZONE 11
ZESA ENL
ZBRN YES
ROUTE 2
AC NONE
PRE DGT 444

```
LOCATOR 7077097007
KEY 00 SCR 7000
NAME DN7000
CLID ENTRY 0
  HNTN 613
  ESA_HLCL 967
  ESA_INHN YES
  ESA_APDN YES
  HLCL 968
  DIDN YES
  HLOC 343
  LSC
  CLASS_FMT DN
CLID VERIFICATION
  CTYP CLID      ESRT  CALLEDNUMBER
  911  Z 077097007  10      444911
  CDP 7000      NATL 9675000
  INTL 6139675000
  UDP 7000
KEY 02 SCR 7003
NAME DN7003
CLID ENTRY 10
  HNTN 514
  ESA_HLCL 5150123
  ESA_INHN YES
  ESA_APDN NO
  HLCL 5150123
  DIDN NO
  HLOC 444
  LSC
  CLASS_FMT DN
CLID VERIFICATION
  CTYP CLID      ESRT  CALLEDNUMBER
  911  Z 7077097007  10      444911
  CDP 7003
  NATL 9675000
  INTL 6139675000
  UDP 7003
CUST 0
DES COSETAB
TN 01 0 00 00
TYPE 2616
ESA
  ESDN 911
  ESRT 10
  DFCL 6139660100
  CALLEDNUMBER 911
  OSDN KEY 00 SCR 7100
  NAME DN7100
```

```

CLID ENTRY 11
HNTN 613
ESA_HLCL 967
ESA_INHN YES
ESA_APDN YES
HLCL 968
DIDN YES
HLOC 343
LSC
CLASS_FMT DN
CLID VERIFICATION
CTYP      CLID      ESRT CALLEDNUMBER
911 D      6139677100 10    911
CDP 7100
NATL 9677100
INTL 6139677100
UDP 7100
KEY 01 SCR 7101

```

ESA CLID composition for set-initiated calls routed to ISDN or Centralized Automatic Message Accounting (CAMA)

For set-initiated ESA calls routed to an ISDN or CAMA trunk, the CLIDVER report relies on the ESA Calling Terminal Identification functionality. This functionality allows the Call Server to compose an ESA calling number for outgoing ESA calls. The calling number content (both ESA and non-ESA) is specified by the system administrator using the CLID entry prompt in LD 15. Currently, up to 4000 CLID entries can be configured.

For the Short Version ESA-Only report, the information entered for the prompts shown in the following overlay is extracted.

LD 15 ESA prompts for each CLID entry in the Customer Data Block

Prompt	Response	Description
ESA_HLCL	x...x	Home Local Code for Emergency Services Access (up to 12 digits).
ESA_INHN	YES NO	Insert/Do not Insert Home National Code in front of ESA_HLCL.
ESA_APDN	YES NO	Append/Do not append DN after ESA_HLCL.

A customer can have up to 4000 CLID entries. The report uses the CLID-based values configured for each customer from the following fields:

- ESA_HLCL
- ESA_INHN
- ESA_APDN

The CLID displayed in the report is the ANI data sent to the Public Safety Answering Point (PSAP).

If the DN does not have a CLID entry associated with it, then the CLIDVER report displays the Default ESA Calling Number (DFCL) as the CLID, in response to the DFCL prompt in LD 24. The CLIDVER report indicates that DFCL information is being displayed by prefixing the CLID with a "D" as shown by the following.

[Table 41 "Sample Short Version ESA and non-ESA report output" \(page 284\)](#) shows a sample Detailed Version ESA and non-ESA output report for ISDN or CAMA trunks.

Table 41
Sample Short Version ESA and non-ESA report output

CUST 0							
TN	KEY	DN	ZN	CTYP	CLID	RT	CALLED #
001	00 SCR	7100	---	911	D 6139660100	2	911

CLID composition for Media Gateway 1000B-initiated calls

ESA processing for Media Gateway 1000B platforms is different from ESA processing for a non-Media Gateway 1000B scenario. See *Branch Office Installation and Commissioning (NN43001-314)* for details.

CLID composition for CS 1000E systems

A CS 1000E system that has analog (500/2500-type) and digital telephones on Media Gateway 1000E platforms receive zone-based ESA service, similar to IP Phones. In this case, the zone number of the Media Gateway 1000E is displayed.

The CLIDVER command correctly displays ESA data for analog (500/2500-type) and digital telephones on a CS 1000E system. See *Branch Office Installation and Commissioning (NN43001-314)* for more information.

CLIDVER

The output of the PRT CLIDVER command (LD 20) is enhanced to reflect the following changes:

- IP phones now receive ESA treatment based on ERL, not Zone.
- Non IP telephones now receive ESA treatment based on ERL.
- There are new fields in the ERL table (for CLIDVER long format).

Enhancements to the CLIDVER report to display Dynamic ELIN information:

- The short format prints the actual Dynamic ELIN that would have been selected for an emergency call. The ELIN is differentiated from the other CLID types by the character 'E'.
- The character 'S' is printed to identify the CLID as a Static ELIN (that is, as Locator).

Nortel Communication Server 1000

Emergency Services Access Fundamentals

Copyright © 2007, Nortel Networks
All Rights Reserved.

Publication: NN43001-613
Document status: Standard
Document version: 01.01
Document date: 30 May 2007

To provide feedback or to report a problem with this document, go to www.nortel.com/documentfeedback.

Sourced in Canada.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

Nortel, the Nortel logo and the Globemark are trademarks of Nortel Networks.

All other trademarks are the property of their respective owners.

