

NENA Standard for the Implementation of the Wireless Emergency Service Protocol E2

Abstract: This document clarifies the E2 interface defined in J-STD-036 and defines the content of parameters that are not fully defined therein.



NENA Standard for the Implementation of the Wireless Emergency Service Protocol E2

NENA-STA-018.2-2021 (originally 05-001)

DSC Approval: 12/17/2020

PRC Approval: 01/29/2021

NENA Board of Directors Approval: 02/17/2021

Next Scheduled Review Date: 06/02/2025

Prepared by:

National Emergency Number Association (NENA) 9-1-1 Core Services Committee, E2
Interface Working Group

Published by NENA

Printed in USA



© Copyright 2003-2021 National Emergency Number Association, Inc.

1 Executive Overview

This standard provides explicit protocols and parameters for interoperable operation of the E2 interface over TCP/IP¹. This interface is between the Mobile Positioning Center (MPC)/ Gateway Mobile Location Center (GMLC) and the Emergency Services Message Entity (ESME) as defined in ANSI/J-STD-036-C-2-2017 [5] (e.g., an Automatic Location Identification [ALI] system or a Legacy Network Gateway [LNG]). This current standard defines the methods that MPC/GMLC and ESME use to interact, allowing for the concept of geographically redundant nodes and the inherent link management. It defines how the TCAP (Transaction Capabilities Application Part)-based application protocol is to be encapsulated upon the TCP/IP stack.

While ANSI/J-STD-036-C-2-2017 [5] defined parameters for the E2 interface, it did not provide sufficient detail to allow vendors to implement the E2 interface and assure interoperability. This interface is required for the implementation of Wireless Phase 2, and, with the addition of the Location Description parameter, the necessary fall back to Phase 1 when Phase 2 data is unavailable. In addition, the Location Description parameter may contain address information associated with the caller's location, a nearby WiFi Access Point, etc.

This standard specifies implementation details not specified in ANSI/J-STD-036-C-2-2017 [5] down to explicit elements so that there can be no confusion regarding how parameters are to be implemented.

This standard is limited to clarifying the E2 interface defined in J-STD-036, including the content of parameters that are not fully defined therein. Changes from NENA 05-001 [9] include the incorporation of updates to J-STD-036 through ANSI/J-STD-036-C-2-2017 [5].

It is also noted that the interface between a VoIP Positioning Center (VPC) and an ALI database, known as the V-E2 interface and defined in NENA 08-001 [7], is out of scope for this document. Modifications to the E2 protocol described in NENA 08-001 [7] are associated with an architecture that was not implemented and are obsolete and are not included in this document.

¹ In this standard the use of the term E2 is in most ways synonymous with the defacto term E2+, although E2+ is not documented in ANSI/J-STD-036-C-2-2017.

Table of Contents

1 EXECUTIVE OVERVIEW	2
DOCUMENT TERMINOLOGY	6
INTELLECTUAL PROPERTY RIGHTS (IPR) POLICY	7
REASON FOR ISSUE/REISSUE	7
2 TECHNICAL OVERVIEW	8
3 TCP/IP PROTOCOL STACK	8
4 NETWORK ARCHITECTURE	9
4.1 SIMPLEX NODE.....	12
4.2 REDUNDANT NODE.....	12
4.3 FULL REDUNDANCY	13
5 SESSION ESTABLISHMENT	13
6 EMERGENCY SERVICE PROTOCOL (ESP) MESSAGES	13
6.1 HEARTBEATS	14
7 ESP QUERIES AND RESPONSES	14
8 EMERGENCY SERVICES PROTOCOL (ESP) MESSAGE FORMATS	19
8.1 EMERGENCY SERVICES POSITION REQUEST	20
8.2 EMERGENCY SERVICES POSITION REQUEST RESPONSE	21
8.3 EMERGENCY SERVICES POSITION REQUEST RESPONSE RETURN ERROR.....	21
8.4 EMERGENCY SERVICES POSITION REQUEST RESPONSE REJECT	22
9 EMERGENCY SERVICES PROTOCOL (ESP) MESSAGE ELEMENT DESCRIPTIONS	22
9.1 TRANSACTION PORTION INFORMATION ELEMENTS.....	23
9.1.1 <i>Package Type</i>	23
9.1.2 <i>Transaction ID</i>	23
9.2 COMPONENT PORTION INFORMATION ELEMENTS.....	24
9.2.1 <i>Component Sequence</i>	24
9.2.2 <i>Component Type</i>	24
9.2.3 <i>Component ID</i>	25
9.2.4 <i>Operation Code</i>	25
9.2.5 <i>Error Code</i>	26
9.2.6 <i>Problem Code</i>	26
9.2.7 <i>Parameter Set</i>	28
9.3 EMERGENCY SERVICES PROTOCOL (ESP) PARAMETERS.....	28
9.3.1 <i>ESME Identification</i>	28
9.3.2 <i>Position Request Type</i>	29
9.3.3 <i>Emergency Services Routing Key</i>	30
9.3.4 <i>Callback Number – Request</i>	32
9.3.5 <i>Callback Number – Request Response</i>	32
9.3.6 <i>Emergency Services Routing Digits – Request</i>	33

9.3.7	<i>Emergency Services Routing Digits – Request Response</i>	34
9.3.8	<i>Position Result</i>	34
9.3.9	<i>Position Information</i>	35
9.3.10	<i>Position Information Parameters</i>	35
9.3.11	<i>Generalized Time – ESRK Assignment</i>	44
9.3.12	<i>Mobile Identification Number</i>	45
9.3.13	<i>International Mobile Subscriber Identity</i>	45
9.3.14	<i>Mobile Call Status</i>	46
9.3.15	<i>Company ID</i>	47
9.3.16	<i>Location Description</i>	47
10	NENA REGISTRY SYSTEM	53
11	DOCUMENTATION REQUIRED FOR THE DEVELOPMENT OF A NENA XML SCHEMA	53
12	IMPACTS, CONSIDERATIONS, ABBREVIATIONS, TERMS, AND DEFINITIONS	53
12.1	OPERATIONS IMPACTS SUMMARY	53
12.2	TECHNICAL IMPACTS SUMMARY	54
12.3	SECURITY IMPACTS SUMMARY	54
12.4	RECOMMENDATION FOR ADDITIONAL DEVELOPMENT WORK.....	54
12.5	ANTICIPATED TIMELINE.....	54
12.6	COST FACTORS	54
12.7	COST RECOVERY CONSIDERATIONS	54
12.8	ADDITIONAL IMPACTS (NON-COST RELATED).....	55
12.9	ABBREVIATIONS, TERMS, AND DEFINITIONS	55
13	REFERENCES	58
14	EXHIBIT X	59
15	APPENDIX	59
	ACKNOWLEDGEMENTS	60



**NENA
STANDARD DOCUMENT
NOTICE**

This Standard Document (STA) is published by the National Emergency Number Association (NENA) as an information source for 9-1-1 System Service Providers, network interface vendors, system vendors, telecommunication service providers, and 9-1-1 Authorities. As an industry Standard it provides for interoperability among systems and services adopting and conforming to its specifications.

NENA reserves the right to revise this Standard Document for any reason including, but not limited to:

- Conformity with criteria or standards promulgated by various agencies,
- Utilization of advances in the state of the technical arts,
- Reflecting changes in the design of equipment, network interfaces, or services described herein.

This document is an information source for the voluntary use of communication centers. It is not intended to be a complete operational directive.

It is possible that certain advances in technology or changes in governmental regulations will precede these revisions. All NENA documents are subject to change as technology or other influencing factors change. Therefore, this NENA document should not be the only source of information used. NENA recommends that readers contact their 9-1-1 System Service Provider (9-1-1 SSP) representative to ensure compatibility with the 9-1-1 network, and their legal counsel, to ensure compliance with current regulations.

Patents may cover the specifications, techniques, or network interface/system characteristics disclosed herein. No license is granted, whether expressed or implied. This document shall not be construed as a suggestion to any manufacturer to modify or change any of its products, nor does this document represent any commitment by NENA, or any affiliate thereof, to purchase any product, whether or not it provides the described characteristics.

By using this document, the user agrees that NENA will have no liability for any consequential, incidental, special, or punitive damages arising from use of the document.

NENA's Committees have developed this document. Recommendations for changes to this document may be submitted to:

National Emergency Number Association
1700 Diagonal Rd, Suite 500
Alexandria, VA 22314
202.466.4911
or commleadership@nena.org



NENA: The 9-1-1 Association improves 9-1-1 through research, standards development, training, education, outreach, and advocacy. Our vision is a public made safer and more secure through universally-available state-of-the-art 9-1-1 systems and better-trained 9-1-1 professionals. Learn more at nena.org.

Document Terminology

This section defines keywords, as they should be interpreted in NENA documents. The form of emphasis (UPPER CASE) shall be consistent and exclusive throughout the document. Any of these words used in lower case and not emphasized do not have special significance beyond normal usage.

1. **MUST, SHALL, REQUIRED:** These terms mean that the definition is a normative (absolute) requirement of the specification.
2. **MUST NOT:** This phrase, or the phrase "SHALL NOT", means that the definition is an absolute prohibition of the specification.
3. **SHOULD:** This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
4. **SHOULD NOT:** This phrase, or the phrase "NOT RECOMMENDED" means that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
5. **MAY:** This word, or the adjective "OPTIONAL", means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option "must" be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option "must" be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

These definitions are based on IETF [RFC 2119](https://www.rfc-editor.org/rfc/2119).

Intellectual Property Rights (IPR) Policy

NOTE – The user’s attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, NENA takes no position with respect to the validity of any such claim(s) or of any patent rights in connection therewith. If a patent holder has filed a statement of willingness to grant a license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license, then details may be obtained from NENA by contacting the Committee Resource Manager identified on NENA’s website at www.nena.org/ipr.

Consistent with the NENA IPR Policy, available at www.nena.org/ipr, NENA invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard.

Please address the information to:
National Emergency Number Association
1700 Diagonal Rd, Suite 500
Alexandria, VA 22314
202.466.4911
or commleadership@nena.org

Reason for Issue/Reissue

NENA reserves the right to modify this document. Upon revision, the reason(s) will be provided in the table below.

Document Number	Approval Date	Reason For Issue/Reissue
NENA-05-001	12/02/2003	Initial Document
NENA-STA-018.2-2021	02/17/2021	Clarifies the E2 interface defined in J-STD-036 and incorporates updates through version ANSI/J-STD-036-C-2-2017 [5].

2 Technical Overview

While the ANSI/J-STD-036-C-2-2017 [5] Emergency Services Position Request and Response uses a Transaction Capabilities Application Part (TCAP) message format, this implies to some that SS7 is the transport and interconnection methodology. However, TCP/IP is a more appropriate transport protocol, and what is used today. The E2 interface connectivity is TCP/IP based, utilizing a TCAP-based application protocol.

The ESMEs (ALI systems and LNGs) normally operate in a redundant, geographically distributed configuration. In addition, the MPCs and GMLCs normally are configured as redundant nodes. The term MPC/GMLC is used throughout this document. This E2 interface MUST be able to handle queries and responses for these various network configurations. That is, both ESMEs MUST be capable of querying both MPCs in a network configuration where both operate as redundant nodes.

Note: The interface between a VoIP Positioning Center (VPC) and an ALI database, known as the V-E2 interface, is out of scope for this document. For details regarding the V-E2 interface see "NENA Interim VoIP Architecture for Enhanced 9-1-1 Services (i2) NENA 08-001 v2, August 11, 2010" [7]

3 TCP/IP Protocol Stack

Figure 1 replicates the TCP/IP protocol stack for the E2 interface described in Figure G-2 of ANSI/J-STD-036-C-2-2017 [5]. This figure illustrates the direct encapsulation of the TCAP ASN.1 encoded messages described in Chapter 7 of ANSI/J-STD-036-C-2-2017 [5] within TCP/IP packets, without additional layers of encoding. IP provides the capability to route the message, which replaces the need for the Signaling Connection Control Part (SCCP) portion of the standard SS7 message.

The intervening network elements (e.g., routers and firewalls) need only use IP to correctly route the session set up message and subsequent packets.

IP provides a connectionless, "best-effort" delivery service. IP's responsibilities include the transmission of a block of data received from upper layers as well as the message addressing. The combination of an IP header preceding a block of data constitutes a datagram. If a link layer failure occurs during datagram transmission, IP's behavior rules do not specify that the datagram be resent.

The transport layer (e.g., TCP) is responsible for this datagram retransmission functionality. TCP provides a reliable, connection-oriented, byte stream, transport layer service. It provides the reliability by performing the following functions:

1. Resizing application layer packets into the proper buffers for the network layer
2. Sending acknowledgments for each block of data received
3. Retransmitting unacknowledged data blocks

4. Making sure that the transmitted packets are received through the use of acknowledgement timers
5. Maintaining a checksum for the header and data
6. Discarding duplicate blocks of data
7. Providing flow control that prevents a faster host from overrunning a slower one

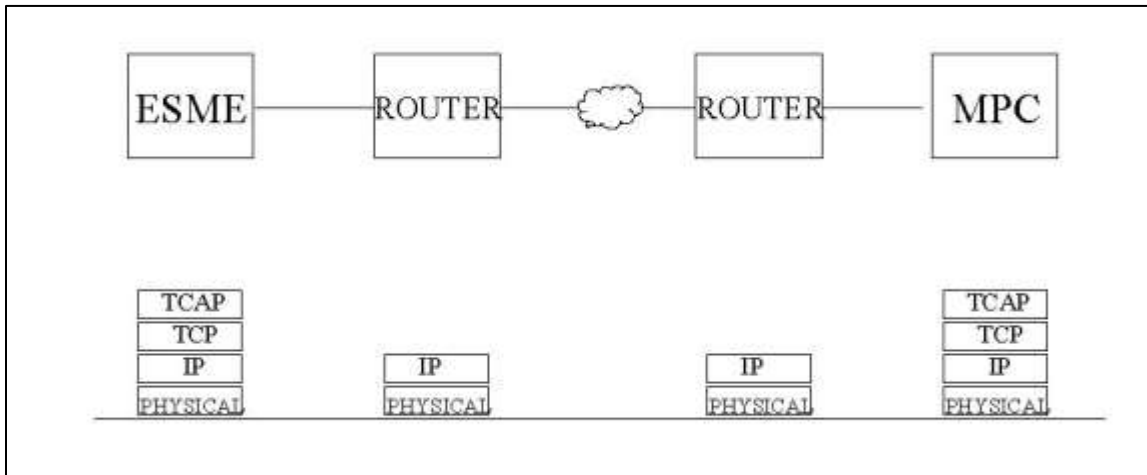


Figure 1 - TCP/IP protocol stack for the E2 interface

4 Network Architecture

Figure 2 below represents the data network architecture between the wireless network and the 9-1-1 Emergency Services Network to allow the caller's location to be returned to the Public Safety Answering Point (PSAP). Each PSAP has links to both of the mated, geographically distributed ESMs (ALI databases).

Figure 2 below represents the data network architecture between the wireless network and the ESMs (LNGs). The Legacy Network Gateway resides between the NG9-1-1 Emergency Services Network and the wireless network. (See NENA-STA-010.2-2016 [15] for further details).

This configuration allows the caller's location to be returned to the PSAP, as each PSAP has access to the LNGs via the NG9-1-1 network.

For the interconnection between the MPC/GMLC and ESME, three different configurations are possible:

- The first is the Simplex Node configuration. In this configuration the MPC/GMLC is a Simplex Node. Both ESMs connect to a high availability MPC/GMLC deployed in the

wireless network over Links A and C. Both ESMEs will steer queries to the single MPC/GMLC.

- The second is the Redundant Node configuration. In this configuration each ESME will have a companion MPC/GMLC with which it communicates (Links A and D). Each ESME will steer queries to its companion MPC/GMLC.
- The third is the Full Redundancy configuration. In this configuration, the ESME complex and the MPC/GMLC complex are fully connected (Links A, B, C, D). Therefore, each ESME has a logical TCP/IP connection to both MPC/GMLCs. The ESMEs will have an alternate destination to query if the query to the primary destination fails.

The network connection between the Emergency Service Provider and the Wireless Carrier is expected to be either a private packet-based network or a dedicated point-to-point environment.

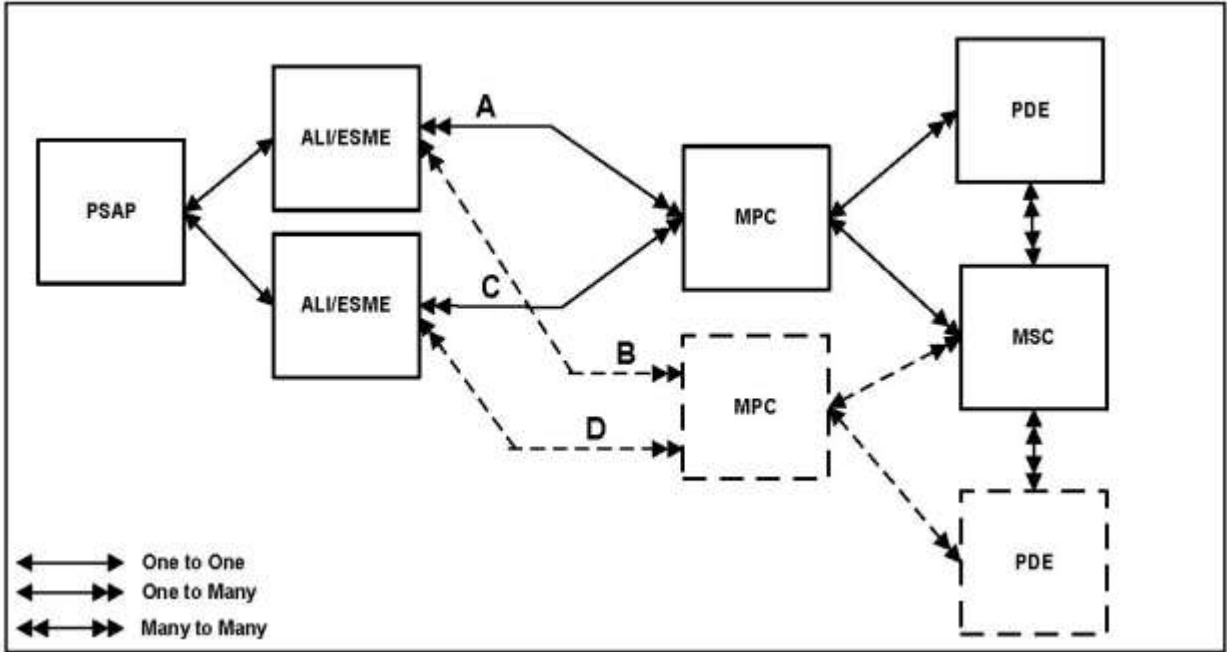


Figure 2 - Wireless E9 1 1 Entities Diagram

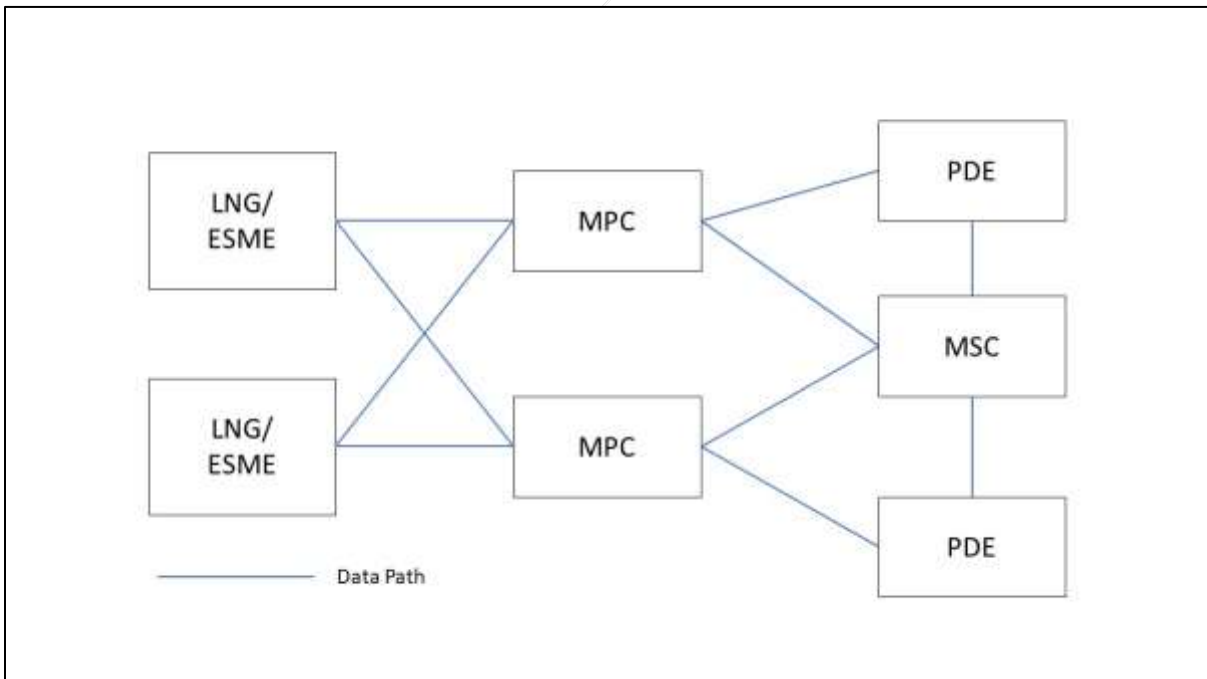


Figure 3 - NG Entities Diagram

4.1 Simplex Node

In the simplex node configuration (links A, C in Figure 2), the MPC/GMLC Node processes all origination requests from the MSC. It coordinates the process of locating the mobile subscriber through a sequence of messages to the PDEs. The ESMEs, always assumed to operate in a mated configuration, will have TCP/IP sessions to this MPC/GMLC Node.

As described in the call flows in Section 7, either one or both ESMEs will query this MPC/GMLC Node. If the query is for Selective Routing instructions, only one ESME may query the MPC/GMLC node. If the query is originated by a PSAP, both ESMEs may query the one MPC/GMLC. If a single MPC/GMLC receives the same query from two different ESMEs, the MPC/GMLC will either a) return the Position Information to the ESME that it received the query from first and ignore the second query, or b) process both queries as if they are separate requests. If the MPC/GMLC processes both queries as if they are separate requests, the PSAP may see duplicate responses.

In this configuration, if the MPC/GMLC is out of service, the ESMEs will not receive a response to their queries. If one link is out of service, and both ESMEs queried the MPC/GMLC Node, the ESME that receives the response will process it and the PSAP will receive a single response. If only one ESME attempts to query the MPC/GMLC Node and the link between it and the MPC/GMLC Node is not available, the ESME will receive no response. This will result in the PSAP not receiving the Position Information, or the Selective Router routing the call based on an ESRD.

4.2 Redundant Node

In the Redundant Node configuration (links A, D in Figure 2) the MPC/GMLC operates in a dual node configuration. The nodes may operate load sharing where they alternately service requests from the MSC or in an active-standby configuration where one MPC/GMLC Node services all requests from the MSC and the other node is activated only when there is a problem with the primary node. The ESMEs and MPC/GMLCs have a one-to-one relationship. ESME A is connected to MPC/GMLC A and ESME B is connected to MPC/GMLC B.

As described in the call flows in Section 7, either one or both ESMEs will query its companion MPC/GMLC Node. If the query is for Selective Routing instructions, only one ESME may query its companion MPC/GMLC Node. If the query is originated by a PSAP, both ESMEs may query their companion MPC/GMLC Node. If both MPC/GMLCs receive the same query, the MPC/GMLCs may negotiate to determine which MPC/GMLC will send the response to the query and that system returns the Position Information to the ESME, or both queries will be processed as separate requests.

In this configuration, if one MPC/GMLC Node is out of service, the ESME communicating with that node will not receive a response to its query. This is also true if the link between

the ESME and its companion MPC/GMLC Node is not available. If both ESMEs queried the associated MPC/GMLC Nodes, and only one node responds, the ESME that receives the response will process it. If only one ESME attempts to query the MPC/GMLC Node and the link between it and the MPC/GMLC Node is not available, the ESME will receive no response. This will result in the PSAP not receiving the Position Information or the Selective Router routing a call based on an ESRD.

4.3 Full Redundancy

In the Full Redundancy configuration (links A, B, C and D in Figure 2) there is a link between each ESME and each MPC/GMLC. The MPC/GMLC operates in a dual node configuration. The nodes may operate in a load-sharing configuration, where they alternately service requests from the MSC, or in an active-standby configuration, where one MPC/GMLC Node services all requests from the MSC and the other node is activated only when there is a problem with the primary node.

As described in the call flows in Section 7, either one or both ESMEs will query the MPC/GMLC Nodes. If the query is for Selective Routing instructions, only one ESME may query both MPC/GMLC Nodes. If the query is originated by a PSAP, both ESMEs may query both MPC/GMLC Nodes. If the MPC/GMLC responds on one link, the ESME that receives the response will respond to the PSAP. If both ESMEs receive responses, they will each respond with one response.

In the Full Redundancy configuration, if one MPC/GMLC Node is out of service, both ESMEs still have connections to the mated MPC/GMLC Node. Therefore, it would require two failures in the network before the ESME complex would not receive a response to a query.

5 Session Establishment

In this configuration, the TCP/IP address and port are agreed upon between the owners of the ESME and the MPC/GMLC. By convention, the ESME is the TCP/IP server and the MPC/GMLC is the TCP/IP client. The sessions are established via sockets where the MPC/GMLC establishes the connection to the ESME. Upon system start up, the ESME will listen to the designated port and the MPC/GMLC will initiate session set up to the designated TCP/IP address and port. Once the socket session is established, the application may begin the query and response handshake.

6 Emergency Service Protocol (ESP) Messages

The ESP query has two formats, identified here as Format A and Format B. For Format A, the Emergency Services Routing Key (ESRK) is passed in the query. For a Format B message, the Callback Number (CBN) and, optionally, the Emergency Services Routing Digits (ESRD) are passed. Parameters of ESME Identification and Position Request Type are

sent for both formats of messages. For the ESP response, the salient information is the CBN and Location. Once the ESME receives these, it will format them with a local ALI record associated with the ESRK/ESRD and return the information to the PSAP.

6.1 Heartbeats

In addition to query and response, there will be heartbeat messages between the ESME and the MPC/GMLC to verify the integrity of the links. These will be initiated by the ESME and responded to by the MPC/GMLC. The ESME will query with the PositionRequestType=4 (Test) and a zero-length EmergencyServicesRoutingKey. The MPC/GMLC should respond with the PositionResult=0A (Test).

These messages only will be sent during periods of inactivity of 60 seconds (a configurable parameter) on a link to verify the integrity of the application and socket connection.

The MPC/GMLC MUST monitor the connection for activity, including heartbeats. If the TCP connection is closed by the ESME, or if no activity from the ESME is detected for more than one heartbeat period, the MPC/GMLC SHOULD attempt to reestablish the connection to the ESME. It is necessary to monitor for the absence of activity because this is the only way to detect certain cases where the ESME has become disconnected without having properly closed the TCP connection.

7 ESP Queries and Responses

The MPC/GMLC may expect queries from the ESME for two situations. The first is when the Selective Router queries the ESME and the second is when the PSAP queries the ESME. Please note that the Selective Router (ESNE) interactions with the ESME (as shown in Figure 4) and described below may represent architectures that have not actually been implemented. These architectural concepts are maintained here for completeness and historical perspective.

Some ESME systems have specific software to aid the Selective Router in routing the call to the correct PSAP. In this situation, the ESME may query the MPC/GMLC for position prior to returning routing instructions to the Selective Router. The Selective Router treats the links to the mated ESME systems as active/standby. That is, the Selective Router only queries one ESME for routing instructions. Therefore, only the ESME that receives the request from the Selective Router may query the MPC/GMLC complex. The query may be either a Format A or Format B query, but the most likely case is a Format B query with both Callback Number and ESRD.

An example of this scenario is shown in Figure 4 below. The sequence of locating the Mobile Station (MS or handset) position is not shown in this flow. The MSC queries the MPC/GMLC with the Cell Site and Sector (CS&S) and Callback Number (CBN) to retrieve the Emergency Services Routing Digit (ESRD) associated with the Cell Site and Sector of where

the call originated (1). The MPC/GMLC returns the ESRD to the MSC (2). The MSC routes the call toward the Emergency Services Network Entity (ESNE or Selective Router) selected by the ESRD and passes CBN and ESRD (3). The ESNE queries one of the ESMEs (ESMEB) for routing instructions using CBN and ESRD (4). ESME B queries both MPC/GMLCs for which it has TCP/IP sessions established with a Format B query (CBN and ESRD) (5). One MPC/GMLC responds to ESME B with the Position Information (6). The ESME uses the Position Information to determine routing instructions for the ESNE and passes back to the ESNE an Emergency Service Number (ESN) (7). The ESNE delivers the call to the PSAP passing the CBN and potentially the ESRD (8). The PSAP queries both ESMEs with the CBN (9). ESME B, having the Position Information, returns it in the response to the PSAP.

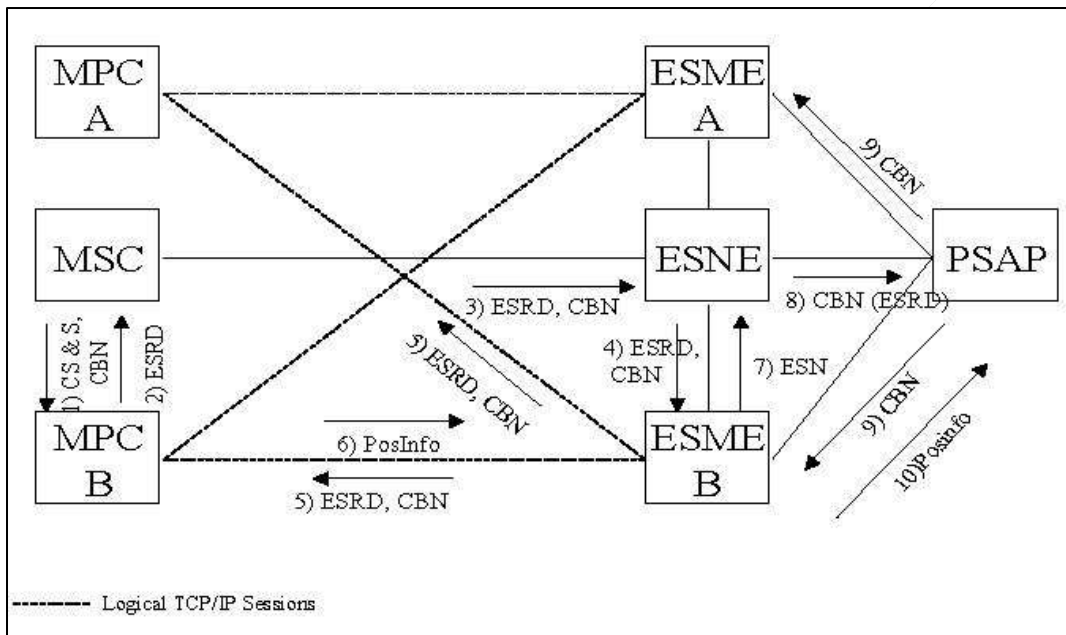


Figure 4 - Query for Selective Routing

The second situation is when the PSAP queries the ESME based upon the delivery of the Emergency Service Call to that PSAP. The PSAP queries the ESME and in turn the ESME queries the MPC/GMLC for the location data. The ESME may query the MPC/GMLC with either a Format A or Format B query depending upon what information is available to the ESME. For example, if the MSC sent both CBN and ESRD in the SS7 Initial Address Message (IAM) message to the ESNE, it is likely that the ESME will query the MPC/GMLC with both. If the MSC sent only ESRK in the call set up to the ESNE, the ESME will query with Emergency Service Routing Key (ESRK).

For the first query, called (initial) query, from the PSAP, the ESME will query the MPC/GMLC with request type of initial. If the ESME can discern that the PSAP has issued a repeat (update) query, the ESME will query the MPC/GMLC with either the request type of

“updated” or “updated or last”. The most likely case is “updated or last” to allow the PSAP to receive the last known location if an updated location cannot be provided by the location equipment.

An example of this flow is shown in Figure 5 below. The MSC queries the MPC/GMLC with the Cell Site and Sector (CS&S) and Callback Number (CBN) to retrieve the Emergency Services Routing Key (ESRK) assigned to this call (1). The MPC/GMLC returns the ESRK to the MSC (2). The MSC routes the call toward the PSAP via the ESNE selected by the ESRK (3). Using the ESRK as an index into static tables to determine routing, the ESNE routes the call to the PSAP (4). (These tables may be resident in the ESNE or the ESNE may query the ESME.) The ESNE passes only ESRK to the PSAP. The PSAP queries both ESMEs with the ESRK (5).

There are two options as to how the ESMEs query the MPC/GMLC Complex (6):

1. Both Mode. Both ESMEs query the MPC/GMLCs to which it has a TCP/IP session established (6). (Figure 5 **Error! Reference source not found.**)
2. Primary Mode. ESME A queries the MPC/GMLC to which it has a TCP/IP session established (6). (Figure 6 **Error! Reference source not found.**) If there is a failure, ESME A queries the other mated MPC/GMLC to which it has a TCP/IP session established (6).

There are three options for the MPC/GMLC to respond to the ESME with the Position information (7):

1. When both MPC/GMLCs receive queries from the ESMEs, the MPC/GMLCs may negotiate to determine which MPC/GMLC will send a single response to the queries and that system returns the Position Information to the ESME (7). The MPC/GMLCs acknowledge the other queries by responding with the PositionResult=07 (Inactive) (8). If the MPC/GMLCs do not negotiate then each MPC/GMLC will treat each query as a separate request (not shown in the figure).
2. When only one MPC/GMLC receives the query, the MPC/GMLC that receives the request from an ESME then responds with the Position Information to the ESME (7).
3. When a single MPC/GMLC receives the same query from two different ESMEs, the MPC/GMLC may return the Position Information to the first ESME from which it received the query. The MPC/GMLC acknowledges the query from the other ESME by responding with the PositionResult=07 (Inactive) (8). Alternatively, the MPC/GMLC may treat each request as a separate query and processes it as such.

In the example of Figure 5, the ESME that received the response from the MPC/GMLC returns the Position Information to the PSAP (9). If both ESMEs receive a Position Information response from an MPC/GMLC, there is a potential that both ESMEs may respond to the PSAP.

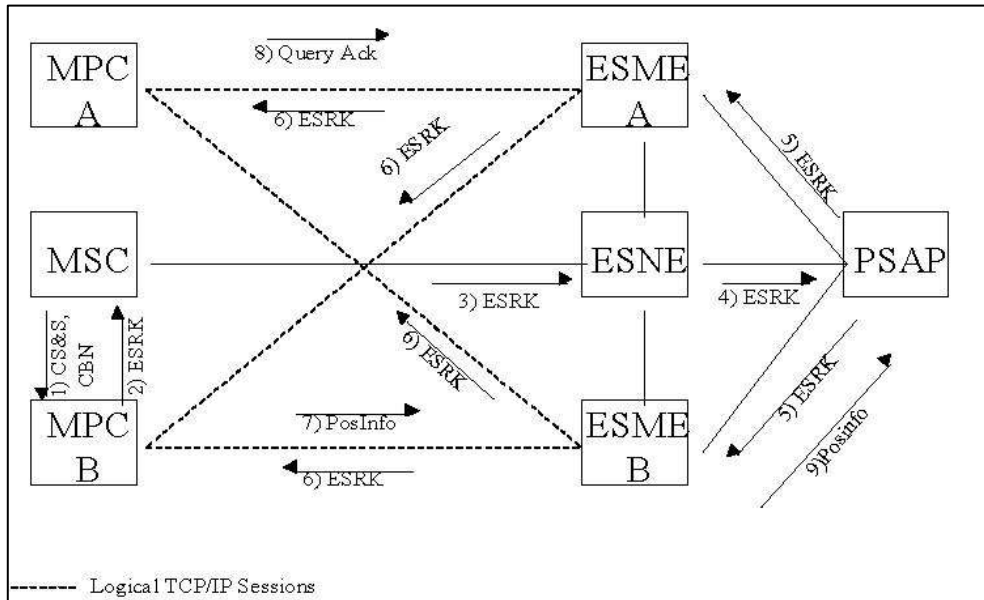


Figure 5 - Both Mode Query

An example of Primary Mode query is shown in Figure 6 below.

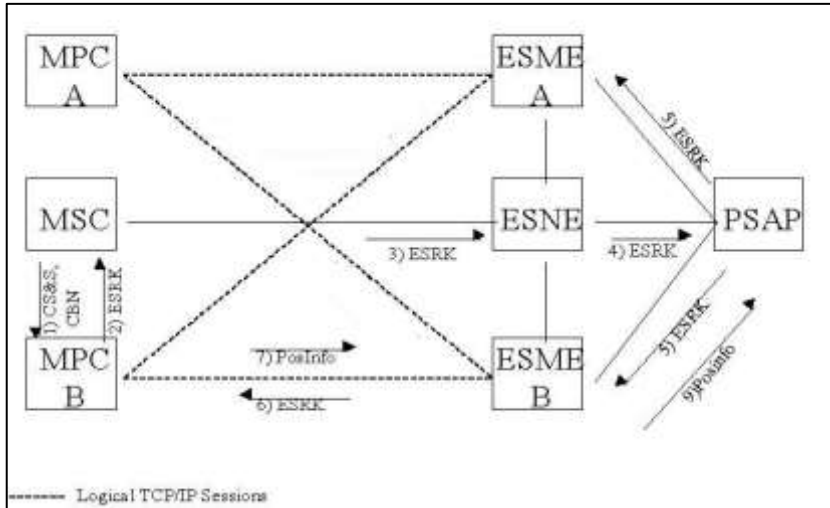


Figure 6 - Primary Mode Query

When installing Phase II functionality at the PSAP, the PSAP may request to test the path between the PSAP and the MPC/GMLC as well as having test coordinates returned from the MPC/GMLC to project on the PSAP's boundary map. The PSAP can do this by doing a manual query and sending the test ESRK to both ESMEs (1). The ESME will query the MPC/GMLC with Format A message with the ESMEIdentification, PositionRequestType=4 (test), and a test ESRK specifically configured on the MPC/GMLC for the PSAP.

If there is no query and response activity between the ESME and the MPC/GMLC for a period of time, the ESME will send a heartbeat over that link (session) and expect the MPC/GMLC to respond. This assures that, at the application level, the session is still established. A lack of heartbeat response will cause the ESME to take recovery action, such as forcibly closing the TCP connection.

An example of the heartbeat is shown in Figure 7 **Error! Reference source not found.** below. The ESME formats and sends an Emergency Services Protocol message with the PositionRequestType=4 and a zero-length EmergencyServicesRoutingKey (notated in the Figure as ESRK=0) (1). The MPC/GMLC response contains a PositionResult=0A(test)(2).

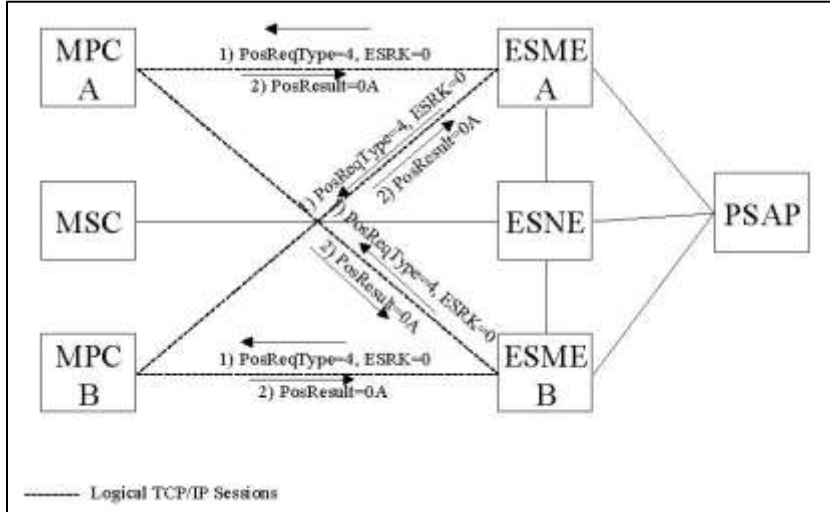


Figure 7 - Heartbeat Example

8 Emergency Services Protocol (ESP) Message Formats

ESP messages are formatted using many of the formatting principles of the ANSI TCAP protocol, as described in ATIS-1000114 [10], Chapters T1.114.1 – T1.114.4, with the following clarifications. The encoding of the Transaction Portion of an ESP message, which consists of the Package Type, Transaction ID, and Component Sequence, is as described in Chapter T1.114.3. The encoding of certain elements of the Component Portion, namely the Component Type, Component ID, Operation Code, and Parameter Set data elements are also formatted according to ANSI TCAP. However, the coding of the ESP parameters within the Parameter Set diverge from ANSI TCAP with regard to the coding of the various parameter identifiers. Although the Emergency Services Protocol uses identifiers from the National TCAP codespace, as defined in Chapter T1.114.3, the ESP parameters are not defined within the ANSI TCAP standard. Because of the potential for code conflicts between the ESP parameter identifier values and those assigned to existing or future TCAP data elements defined in ATIS-1000114 [10], caution should be exercised in using the ESP protocol with network nodes that also support the ANSI TCAP protocol.

The tables below define the sequence² of message elements and parameters within each ESP message type. Note that parameters in the Parameter Set may occur in any order.

² Although we present these elements as a sequence corresponding to the order that they appear in the binary representation, they exist within a hierarchical structure. That distinction is mostly unimportant for the limited messages described in this document, except that the length value of various elements depends on the elements contained within. The calculation of length is fully described in Section 9.

Other element ordering is mandatory. The elements and parameters themselves are described to the bit-level in section 9. The convention where bit 'A' is the least significant bit in an octet and bit 'H' is the most significant bit in an octet is used to match the convention in ATIS-1000114 [10].

It is intended that each message is sufficiently described herein such that an implementor can fully create or interpret all of the ESP messages in their binary representations. A more complete understanding of TCAP as described above may be helpful but should not be required.

Note: In the following tables, the Type M = Mandatory and O = Optional.

8.1 Emergency Services Position Request

This message is sent from the ESME to MPC/GMLC to request the initial, updated or last known position of an MS.

Element /Parameter	Reference	Type
Package Type = Query With Permission	9.1.1	M
Transaction ID	9.1.2	M
Component Sequence	9.2.1	M
Component Type = Invoke (Last)	9.2.2	M
Component ID	9.2.3	M
Operation Code = Private TCAP	9.2.4	M
Parameter Set	9.2.7	M
ESMEIdentification	9.3.1	M
PostionRequestType	9.3.2	M
EmergencyServicesRoutingKey (esprKey)	9.3.3	O
CallbackNumber (esprKey)	9.3.4	O
EmergencyServiceRoutingDigits (esprKey)	9.3.5	O

Please Note: The esprKey is a CHOICE of either the EmergencyServicesRoutingKey (ESRK), or the CallbackNumber and the optional EmergencyServiceRoutingDigit (ESRD). CallbackNumber is mandatory only if ESRK is not provided.

8.2 Emergency Services Position Request Response

This message is sent from MPC/GMLC to the ESME to inform the ESME interface of the position of the MS.

Element /Parameter	Reference	Type
Package Type = Response	9.1.1	M
Transaction ID	9.1.2	M
Component Sequence	9.2.1	M
Component Type = Return Result(Last)	9.2.2	M
Component ID	9.2.3	M
Parameter Set	9.2.7	M
PositionResult	9.3.8	M
PostionInformation	9.3.9	O
CallbackNumber	9.3.5	O
EmergencyServiceRoutingDigits	9.3.7	O
GeneralizedTime	9.3.11	O
MobileIdentificationNumber	9.3.12	O
InternationalMobileSubscriberIdentity	9.3.13	O
MobileCallStatus	9.3.14	O
CompanyID	9.3.15	O
Location Description	9.3.16	O

8.3 Emergency Services Position Request Response Return Error

This message is sent from the MPC/GMLC to the ESME to inform the ESME that the requested action was not performed. The Error Code contains the reason for the failure.

Element/Parameter	Reference	Type
Package Type = Response	9.1.1	M
Transaction ID	9.1.2	M
Component Sequence	9.2.1	M
Component Type = Return Error	9.2.2	M
Component ID	9.2.3	M
Error Code	9.2.5	M
Parameter Set	9.2.7	M

8.4 Emergency Services Position Request Response Reject

This message is sent from the MPC/GMLC to the ESME to inform the ESME that the Invoke message contains a Transaction Portion or Component Level protocol error. The problem code describes the nature of the protocol error.

Element/Parameter	Reference	Type
Package Type = Response	9.1.1	M
Transaction ID	9.1.2	M
Component Sequence	9.2.1	M
Component Type = Reject	9.2.2	M
Component ID	9.2.3	M
Problem Code	9.2.6	M
Parameter Set	9.2.7	M

9 Emergency Services Protocol (ESP) Message Element Descriptions

The TCAP elements used here begin with a single octet that identifies the element, followed by one or more octets that specify the length of the content in octets, and finally any content. The length does not include the identifier or the length indicator itself, and is represented as follows:

If the length of the content is 127 octets or less, the length value is expressed using a single octet with bit H = 0 and the low seven bits (A through G) representing the length of the content as a binary number.

If the length of the content is 128 octets or more, the length value is expressed using multiple octets with bit H = 1 in the first octet. The low seven bits (A through G) of the first octet represent the number of additional octets in the length field. These additional octets represent the length of content as an unsigned integer, with the most significant bit and byte first, using the fewest number of octets needed.

For elements having a fixed length, the length value is specified. For elements whose length is variable, or whose content consists of other elements that follow, the information to calculate the length is provided. Additionally, the Octet number is shown with a (+) to indicate that multiple bytes may be required to represent the length.

9.1 Transaction Portion Information Elements

9.1.1 Package Type

The Package Type is used to control the state of the transaction.

Octet	H	G	F	E	D	C	B	A
1	Package Type Identifier							
2(+)	Package Length							

The Package Type identifier is coded as defined in ANSI T1.114.3 – 1996, Section 3.1. The subset of Package Types that will be supported are shown below.

H	G	F	E	D	C	B	A	Hex	Meaning
1	1	1	0	0	0	1	0	E2	Query With Permission
1	1	1	0	0	1	0	0	E4	Response

The Package Length value includes all of the elements that follow (i.e., the entire message with the exception of the Package Type Identifier and the Package Length indicator itself).

9.1.2 Transaction ID

The Transaction ID used to identify messages that belong to the same transaction. It is unique for each transaction. The Transaction ID identifier is coded as defined in ATIS-1000114 [10], Chapter T1.114.3, Section 3.3. All TCAP messages require a Transaction ID

field. Each Transaction ID has a length of 4 octets. In messages that have a Package Type of Query with Permission, there is only one Transaction ID, which is the Originating Transaction ID. In messages that have a Package Type of Response there is a single Transaction ID, the Responding Transaction ID (which reflects the Originating Transaction ID).

Octet	H	G	F	E	D	C	B	A
1(=C7)	1	1	0	0	0	1	1	1
2	Transaction ID Length = 4							
3	Transaction ID (most significant octet)							
4	Transaction ID (octet 2)							
5	Transaction ID (octet 3)							
6	Transaction ID (least significant octet)							

9.2 Component Portion Information Elements

9.2.1 Component Sequence

The Component Sequence indicates that a sequence of one or more components follows. The Component Sequence Identifier is coded as in ATIS-1000114 [10], Chapter T1.114.3, Section 5.1. The Component Sequence Length is the length of all included components in the sequence, which is effectively all parts of the message that follow.

Octet	H	G	F	E	D	C	B	A
1(=E8)	1	1	1	0	1	0	0	0
2(+)	Component Sequence Length							

9.2.2 Component Type

The Component Type indicates the type of component that follows.

Octet	H	G	F	E	D	C	B	A
1	Component Type Identifier							
2(+)	Component Length							

The Component Type Identifier is coded as defined in A ATIS-1000114 [10], Chapter T1.114.3, Section 5.3. The subset of Component Types that will be supported are shown below.

H	G	F	E	D	C	B	A	Hex	Meaning
1	1	1	0	1	0	0	1	E9	Invoke (last)
1	1	1	0	1	0	1	0	EA	Return Result (last)
1	1	1	0	1	0	1	1	EB	Return Error
1	1	1	0	1	1	0	0	EC	Reject

The Component Length is the length of the entire component, which includes the Component ID, Operation Code, Error Code, Problem Code, and Parameter Set (as applicable).

9.2.3 Component ID

The Component ID is used to identify components within a transaction. The Component ID identifier is coded as defined in ATIS-1000114 [10], Chapter T1.114.3, Section 5.5. In the ESP, the Component ID Length is always 1, meaning that there is only one Component ID in the Component. Since the component in the Emergency Services Position Request is an Invoke component, and the Package Type is a query, this message will contain an Invoke ID. Since the Emergency Services Position Request Response contains a Return Result component, it will contain a Correlation ID (which reflects the Invoke ID).

Octet	H	G	F	E	D	C	B	A
1(=CF)	1	1	0	0	1	1	1	1
2	Component ID Length = 1							
3	Component ID							

9.2.4 Operation Code

The Operation Code defines the operation to be invoked in an Invoke component. The Operation Code identifier is coded as defined in ATIS-1000114 [10], Chapter T1.114.3, Section 5.8 and is Private TCAP. The Operation Code consists of 2 octets: the Operation Family and the Operation Specifier.

Octet	H	G	F	E	D	C	B	A
1(=D1)	1	1	0	1	0	0	0	1

2	Operation Code Length = 2
3	Operation Family (= 1 decimal)
4	Operation Specifier = 1

The Operation Specifier value for Emergency Services Position Request is 1.

9.2.5 Error Code

The Error Code defines an Application Level error that occurred and is being returned in a Return Error component. The Error Code Identifier is coded as defined in ATIS-1000114 [10], Chapter T1.114.3, Section 5.11, and is Private TCAP.

Octet	H	G	F	E	D	C	B	A
1(=D4)	1	1	0	1	0	1	0	0
2	Error Code Length = 1							
3	Error Code							

The following table lists the values for Error Code and their meanings.

H	G	F	E	D	C	B	A	Hex	Meaning
0	0	0	0	0	0	0	1	01	System Failure
0	0	0	0	0	0	1	0	02	Unauthorized Request
0	0	0	0	0	0	1	1	03	Unexpected Data Value
0	0	0	0	0	1	0	0	04	Unrecognized Key

9.2.6 Problem Code

The Problem Code defines the reason that the Transaction or Component Portion of the message was rejected. The Problem Code identifier is coded as defined in ATIS-1000114 [10], Chapter T1.114.3, Section 5.14.

Octet	H	G	F	E	D	C	B	A
1(=D5)	1	1	0	1	0	1	0	1
2	Problem Code Length = 2							
3	Problem Type							

4	Problem Specifier
---	-------------------

The Problem Type is coded as defined in ATIS-1000114 [10], Chapter T1.114.3, Section 5.16.1. The subset of Problem Types that will be supported are shown below.

H	G	F	E	D	C	B	A	Hex	Meaning
0	0	0	0	0	0	0	1	01	General
0	0	0	0	0	0	1	0	02	Invoke
0	0	0	0	0	1	0	1	05	Transaction Portion

The Problem Specifier is coded as defined in ATIS-1000114 [10], Chapter T1.114.3, Section 5.16.2. The subset of Problem Specifiers for each Problem Type are shown below. Note that the Problem Specifier values have different meaning within each Problem Type.

Problem Type: General

H	G	F	E	D	C	B	A	Hex	Meaning
0	0	0	0	0	0	0	1	01	Unrecognized Component Type
0	0	0	0	0	0	1	0	02	Incorrect Component Portion
0	0	0	0	0	0	1	1	03	Badly Structured Component Portion
0	0	0	0	0	1	0	0	04	Incorrect Component Coding

Problem Type: Invoke

H	G	F	E	D	C	B	A	Hex	Meaning
0	0	0	0	0	0	0	1	01	Duplicate Invoke Id
0	0	0	0	0	0	1	0	02	Unrecognized Operation code
0	0	0	0	0	0	1	1	03	Incorrect Parameter

Problem Type Transaction Portion

H	G	F	E	D	C	B	A	Hex	Meaning
0	0	0	0	0	0	0	1	01	Unrecognized Package Type



0	0	0	0	0	0	1	0	02	Incorrect Transaction Portion
0	0	0	0	0	0	1	1	03	Badly Structured Transaction Portion
0	0	0	0	0	1	0	0	04	Unassigned Responding Transaction ID
0	0	0	0	0	1	0	1	05	Permission to Release Problem
0	0	0	0	0	1	1	0	06	Resource Unavailable

9.2.7 Parameter Set

The Parameter Set indicates that a set of zero or more parameters follows. The Parameter Set Identifier is coded as defined in ATIS-1000114 [10], Chapter T1.114.3, Section 5.17. The Parameter Set Length is the length of all included parameters.

Octet	H	G	F	E	D	C	B	A
1(=F2)	1	1	1	1	0	0	1	0
2(+)	Parameter Set Length							

9.3 Emergency Services Protocol (ESP) Parameters

The order of the parameters within the Parameter Set is not significant. Note that the Parameter Identifier value assignments provided in this document are not defined in ATIS-1000114 [10].

9.3.1 ESME Identification

This parameter identifies the ESME system initiating the request (i.e. ESME).

Octet	H	G	F	E	D	C	B	A
1(=C0)	1	1	0	0	0	0	0	0
2	ESME Identification Length is variable							
3	ESME Identification String (most significant octet)							
4								
5								

6	ESME Identification String	
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		ESME Identification String (least significant octet)

Max 15 alpha/numeric that defines the unique name of the ESME that is originating the query. As there is no officially maintained list of ESME identifiers, the content of this field should be set by mutual agreement of the MPC/GMLC providers and the ESME provider.

9.3.2 Position Request Type

This parameter indicates the type of position requested.

Octet	H	G	F	E	D	C	B	A
1(=C1)	1	1	0	0	0	0	0	1
2	Position Request Type length=1							
3	Position Request Type							

This table identifies the legal values for Position Request Type and their meanings.

H	G	F	E	D	C	B	A	Hex	Meaning
0	0	0	0	0	0	0	1	01	Initial
0	0	0	0	0	0	1	0	02	Updated
0	0	0	0	0	0	1	1	03	Updated or Last known
0	0	0	0	0	1	0	0	04	Test

Undefined values are treated as value 1 (Initial).

9.3.3 Emergency Services Routing Key

This parameter uniquely identifies an ongoing Emergency Services Call.

Octet	H	G	F	E	D	C	B	A
1(=C2)	1	1	0	0	0	0	1	0
2	Emergency Services Routing Key Length = 9 ¹							
3	Type of Digits (Routing Number)							
4	Nature of Number (National/International, No Presentation Restrictions)							
5	Numbering Plan (Telephony Numbering)				Encoding (BCD)			
6	Number of Digits							
7	Digit 2				Digit 1			
8	Digit 4				Digit 3			
9	Digit 6				Digit 5			
10	Digit 8				Digit 7			

¹When this parameter is used in a heartbeat message, the preferred representation is a "zero-length" parameter consisting only of the tag (0xC2) and length octets, with length = 0. Due to ambiguity in previous versions of this specification, some implementations may also accept other representations as valid.

This table identifies the legal values for Type of Digits and their meanings.

H	G	F	E	D	C	B	A	Hex	Meaning
0	0	0	0	0	0	0	1	01	Called Party Number
0	0	0	0	0	0	1	0	02	Calling Party Number
0	0	0	0	0	0	1	1	03	Caller Interaction
0	0	0	0	0	1	0	0	04	Routing Number
0	0	0	0	0	1	0	1	05	Billing Number

0	0	0	0	0	1	1	0	06	Destination Number
0	0	0	0	0	1	1	1	07	LATA
0	0	0	0	1	0	0	0	08	Carrier
0	0	0	0	1	0	0	1	09	Last Calling Party
0	0	0	0	1	0	1	0	0A	Last Party Called
0	0	0	0	1	0	1	1	0B	Calling Directory Number
0	0	0	0	1	1	0	0	0C	VMSR Identifier
0	0	0	0	1	1	0	1	0D	Original Called Number
0	0	0	0	1	1	1	0	0E	Redirecting Number
0	0	0	0	1	1	1	1	0F	Connected Number

This table identifies the legal values for Nature of Number and their meanings.

H	G	F	E	D	C	B	A	Hex	Meaning
0	0	0	0	0	0	0	0	00	National/No Presentation Restricted
0	0	0	0	0	0	0	1	01	International/No Presentation Restricted
0	0	0	0	0	0	1	0	02	National/Presentation Restricted
0	0	0	0	0	0	1	1	03	International/Presentation Restricted

This table identifies the legal values for Encoding scheme and their meanings.

D	C	B	A	Hex	Meaning
0	0	0	1	01	BCD
0	0	1	0	02	IA5

This table identifies the legal values for Numbering Plan and their meanings.



H	G	F	E	Hex	Meaning
0	0	0	1	01	ISDN Numbering
0	0	1	0	02	Telephony Numbering
0	0	1	1	03	Data Numbering
0	1	0	0	04	Telex Numbering
0	1	0	1	05	Maritime Mobile Numbering
0	1	1	0	06	Land Mobile Number
0	1	1	1	07	Private Numbering Plan

9.3.4 Callback Number – Request

This parameter is MDN/MSISDN that identifies the emergency service caller.

Octet	H	G	F	E	D	C	B	A
1(=C3)	1	1	0	0	0	0	1	1
2	Callback Number Length = 9							
3	Type of Digits (Calling Party Number)							
4	Nature of Number (National/International, No Presentation Restrictions)							
5	Numbering Plan (Telephony Numbering)				Encoding (BCD)			
6	Number of Digits							
7	Digit 2				Digit 1			
8	Digit 4				Digit 3			
9	Digit 6				Digit 5			
10	Digit 8				Digit 7			
11	Digit 10				Digit 9			

See Section 9.3.3 for how to encode type of digits, nature of number, numbering plan and encoding fields.

9.3.5 Callback Number – Request Response

This parameter is MDN/MSISDN that identifies the emergency service caller.

Octet	H	G	F	E	D	C	B	A
1(=C2)	1	1	0	0	0	0	1	0
2	Callback Number Length = 9							
3	Type of Digits (Calling Party Number)							
4	Nature of Number (National/International, No Presentation Restrictions)							
5	Numbering Plan (Telephony Numbering)				Encoding (BCD)			
6	Number of Digits							
7	Digit 2				Digit 1			
8	Digit 4				Digit 3			
9	Digit 6				Digit 5			
10	Digit 8				Digit 7			
11	Digit 10				Digit 9			

See Section 9.3.3 for how to encode type of digits, nature of number, numbering plan and encoding fields.

9.3.6 Emergency Services Routing Digits – Request

This parameter uniquely identifies a base station, cell site or sector.

Octet	H	G	F	E	D	C	B	A
1(=C4)	1	1	0	0	0	1	0	0
2	Emergency Services Routing Digits Length = 9							
3	Type of Digits (Routing Number)							
4	Nature of Number (National/International, No Presentation Restrictions)							
5	Numbering Plan (Telephony Numbering)				Encoding (BCD)			
6	Number of Digits							
7	Digit 2				Digit 1			
8	Digit 4				Digit 3			
9	Digit 6				Digit 5			
10	Digit 8				Digit 7			

Octet	H	G	F	E	D	C	B	A
11	Digit 10				Digit 9			

See Section 9.3.3 for how to encode type of digits, nature of number, numbering plan and encoding fields.

9.3.7 Emergency Services Routing Digits – Request Response

This parameter uniquely identifies a base station, cell site or sector.

Octet	H	G	F	E	D	C	B	A
1(=C3)	1	1	0	0	0	0	1	1
2	Emergency Services Routing Digits Length = 9							
3	Type of Digits (Routing Number)							
4	Nature of Number (National/International, No Presentation Restrictions)							
5	Numbering Plan (Telephony Numbering)				Encoding (BCD)			
6	Number of Digits							
7	Digit 2				Digit 1			
8	Digit 4				Digit 3			
9	Digit 6				Digit 5			
10	Digit 8				Digit 7			
11	Digit 10				Digit 9			

See Section 9.3.3 for how to encode type of digits, nature of number, numbering plan and encoding fields.

9.3.8 Position Result

This parameter indicates the type of position returned or the reason for not providing position information.

Octet	H	G	F	E	D	C	B	A
1(=C0)	1	1	0	0	0	0	0	0
2	Position Result length=1							
3	Position Result							

The table below identifies the legal values for Position Result and their meanings.

H	G	F	E	D	C	B	A	Hex	Meaning
0	0	0	0	0	0	0	1	01	Initial Position Returned
0	0	0	0	0	0	1	0	02	Updated Position Returned
0	0	0	0	0	0	1	1	03	Last known Position Returned
0	0	0	0	0	1	0	0	04	Req Position Not Avail
0	0	0	0	0	1	0	1	05	Caller Disconnected
0	0	0	0	0	1	1	0	06	Caller Has Handed Off
0	0	0	0	0	1	1	1	07	Inactive
0	0	0	0	1	0	0	0	08	Unresponsive
0	0	0	0	1	0	0	1	09	Refused
0	0	0	0	1	0	1	0	0A	Test

If undefined values are received, they are treated as value 4 was received.

9.3.9 Position Information

This parameter uses the constructor form and contains parameters representing the geographic position estimate of the mobile station and the time of the position determination. This parameter may also contain information regarding the method used to obtain the geographic position. The Length value is the total length of the included parameters which are listed in Section 9.3.10.

Octet	H	G	F	E	D	C	B	A
1(=E1)	1	1	1	0	0	0	0	1
2	Length of Position Information							

9.3.10 Position Information Parameters

9.3.10.1 Generalized Time (Mandatory)

This parameter contains time of position determination. This timestamp is specified in Universal Coordinated Time (UTC).

Octet	H	G	F	E	D	C	B	A	
1(=C0)	1	1	0	0	0	0	0	0	
2	Length of Generalized Time = 6								
3	Year – 2000								
4	Month								
5	Day of Month								
6	MSB		Time of Day						LSB
7									
8									

9.3.10.2 Geographic Position (Mandatory)

Latitude and longitude of the wireless caller's position are carried in this parameter. The format and coding of the elements in the shape description are described in the sub clauses. The shape description used MUST correspond with the Type Of Shape value, and the resulting Length is as follows:

1. Ellipsoid Point, Length = 8
2. Ellipsoid Point with Uncertainty, Length = 10
3. Ellipsoid Point with altitude and uncertainty, Length = 13

The ellipsoid point with altitude and uncertainty is intended to represent a three-dimensional volume of uncertainty that can be described as spheroid, centered on a point at an altitude above or below the WGS84 ellipsoid, and having the axis of revolution aligned vertically (perpendicular to the surface of the WGS84 ellipsoid). This shape may also be described as an ellipsoid with two equal semi-diameters in the horizontal plane. The length of the horizontal semi-diameter corresponds to the uncertainty code, and the length of the vertical semi-axis corresponds to the altitude uncertainty code.

Note that only one confidence value is included in the shape parameters; the horizontal and vertical uncertainties of a given position MUST therefore be delivered to or converted by the GMLC to representations having the same confidence, prior to being encoded into the E2 parameter set.

Octet	H	G	F	E	D	C	B	A
-------	---	---	---	---	---	---	---	---

1(=C1)	1	1	0	0	0	0	0	1
2	Length of Geographic Position							
3	Spare				LPRI		Screening	
4	Ext	Type of Shape						
5	Shape description							
6								
N								

The following codes are used in the sub fields of Geographic Position parameter:
Location Presentation Restricted Indicator (LPRI)

D	C	Hex	Meaning
0	0	00	Presentation Allowed
0	1	01	Presentation Restricted
1	0	02	Location not Available
1	1	03	Spare

Screening Indicator (Screening)

B	A	Hex	Meaning
0	0	00	User provided, not verified
0	1	01	User provided, verified and passed
1	0	02	User provided, verified and failed
1	1	03	Network provided

Extension Indicator (Ext)

H	Hex	Meaning
0	00	Info continues thru the next octet
1	01	Last octet

Type of Shape

G	F	E	D	C	B	A	Hex	Meaning
---	---	---	---	---	---	---	-----	---------

0	0	0	0	0	0	0	00	Ellipsoid Point
0	0	0	0	0	0	1	01	Ellipsoid Point with Uncertainty
0	0	0	0	0	1	0	02	Ellipsoid Point with Altitude and Uncertainty

Shape Descriptions:

1. Ellipsoid Point

	H	G	F	E	D	C	B	A
5	Lat sign	MSB						
6	Degrees of Latitude							LSB
7								
8	MSB							LSB
9	Degrees of Longitude							
10								

These values are further defined in ATIS-1000628.2000(R2015) [3] as:

i) Lat Sign

0 North
1 South

ii) Degrees of latitude

The relation between the binary coded number N and the range of latitudes X ($0 \leq X < 90$), where X is in degrees but not necessarily an integral number of degrees it encodes, is described by the following equation:

$$N \leq \frac{2^{23}}{90} X < N + 1$$

except for $N=2^{23}-1$, for which the range is extended to include N+1

iii) Degrees of longitude

The longitude, expressed in the range (-180, +180) is coded as a number between -2^{23} and $2^{23}-1$, coded in 2's complement binary. The relation between the binary coded number N and the range of longitudes X ($-180 \leq X < 180$), where X is in degrees but not necessarily an integral number of degrees it encodes, is described by the following equation:



$$N \leq \frac{2^{24}}{360} X < N + 1$$

2. Ellipsoid point with uncertainty

	H	G	F	E	D	C	B	A
5	Lat sign	MSB						
6	Degrees of Latitude							LSB
7								
8	MSB							
9	Degrees of Longitude							LSB
10								
11	Spare	Uncertainty code						
12	Spare	Confidence						

These values are further defined in ATIS-1000628.2000(R2015) [3] as:

- i) Lat Sign
Same as above
- ii) Degrees of latitude
Same as above
- iii) Degrees of longitude
Same as above
- iv) Uncertainty code
The uncertainty r , expressed in meters (in the range 1m to ≈ 1800 km), is mapped from the binary number K , with the following formula:

$$r = C((1 + x)^K - 1)$$

with $C = 10$ and $x = 0.1$.

Valid values of K are integers between 1 and 127, inclusive. To represent an ellipsoid point with zero uncertainty, use shape type = 0 (Ellipsoid Point) shown previously.

- v) Confidence

The confidence by which the location is known to be within the shape description, C (expressed as a percentage) is directly mapped from the binary number K, except for K=0 which is used to indicate 'no information', and $100 < K \leq 127$ which are not used.

3. Ellipsoid Point with altitude and uncertainty

	H	G	F	E	D	C	B	A	
5	Lat sign	MSB							
6	Degrees of Latitude							LSB	
7									
8									MSB
9									
10	LSB								
11	Spare	Uncertainty code							
12	Alt sign	MSB							LSB
13	Altitude								
14	Spare	Altitude Uncertainty code							
15	Spare	Confidence							

These values are further defined in ATIS-1000628.2000(R2015) [3] as:

- i) Lat Sign
Same as above
- ii) Degrees of latitude
Same as above
- iii) Degrees of longitude
Same as above
- iv) Uncertainty code
Same as above, applies to horizontal position only
- v) Alt Sign
0 Above the ellipsoid

1 Below the ellipsoid

vi) Altitude

The relation between the binary coded number N and the range of altitudes a (in meters) it encodes is described by the following equation:

$$N \leq a < N + 1$$

except for $N=2^{15}$ for which the range is extended to include all greater values of a .

vii) Altitude uncertainty code

Altitude uncertainty h , expressed in meters (in the range 0m to ≈ 1000 m), is mapped from the binary number K , with the following formula:

$$h = C((1 + x)^K - 1)$$

with $C = 45$ and $x = 0.025$.

viii) Confidence

Same as above; applies to both uncertainty (horizontal) and altitude uncertainty

Notes regarding Uncertainty and Confidence:

Points with uncertainty and confidence are approximations intended to reflect the probability that the true location will be found within the shape described. Depending on the techniques used to measure position, other shapes may better represent the actual distribution of true positions. However, the E2 protocol is limited to the representations herein. The methods for calculating the most appropriate values to send over E2 are beyond the scope of this document.

Although the E2 protocol allows for uncertainty to be communicated at any chosen level of confidence, it is desirable for uncertainty to be presented at the PSAP in a consistent manner – ideally at a uniform level of confidence. Guidance may be found in RFC 7459.

The E2 protocol does not include a method for indicating the Probability Density Function (PDF) related to the uncertainty, nor does it require that a specific PDF be used or assumed. Without knowledge of the PDF, it is not possible to properly compute an equivalent uncertainty at a different level of confidence than the value that was originally provided. It is also improper to assume that the point at the center of the shape has any more or any less significance than the rest of the shape.

Therefore, unless information regarding the PDF is known via another mechanism, recipients of E2 geographic position data SHOULD NOT attempt to convert or modify the uncertainty and confidence for the sake of consistency. Additionally, when uncertainty and

confidence data are provided, recipients SHOULD NOT rely only upon the ellipsoid point for further processing, analysis, or display.

However, providers of position data SHOULD seek to provide uncertainty values at a consistent level of confidence for all provided locations, and this level of confidence SHOULD be consistent among all providers. This document makes no recommendation regarding the specific value of confidence that should be used.

It is recognized that a GMLC may receive position information containing an ellipse in two dimensions or an ellipsoid in three dimensions, each having individual major and minor uncertainty values in the horizontal plane. Because the E2 Standard supports point with uncertainty or point with altitude and uncertainty shape types, encoding of the E2 shape is typically done using the major axis of the original elliptical shape as the horizontal uncertainty in this situation.

9.3.10.3 Position Source (Optional)

This parameter specifies how particular position information was obtained to help assess its credibility.

Octet	H	G	F	E	D	C	B	A
1(=C2)	1	1	0	0	0	0	1	0
2	Length of Position Source=1							
3	Value of Position Source							

The table below identifies the legal values for Position Source and their meanings.

H	G	F	E	D	C	B	A	Hex	Dec	Meaning
0	0	0	0	0	0	0	0	0	0	unknown
0	0	0	0	0	0	0	1	1	1	networkUnspecified ³
0	0	0	0	0	0	1	0	2	2	networkAOA
0	0	0	0	0	0	1	1	3	3	networkTOA
0	0	0	0	0	1	0	0	4	4	networkTDOA
0	0	0	0	0	1	0	1	5	5	networkRFFingerprinting
0	0	0	0	0	1	1	0	6	6	networkCellSector
0	0	0	0	0	1	1	1	7	7	networkCellSectorWithTiming

³ Use only if the Network source type is not described by any of the other Network Position Sources



NENA Standard for the Implementation of
the Wireless Emergency Service Protocol E2
NENA-STA-018.2-2021 (originally 05-001), February 17, 2021

H	G	F	E	D	C	B	A	Hex	Dec	Meaning
0	0	0	1	0	0	0	0	10	16	handsetUnspecified ⁴
0	0	0	1	0	0	0	1	11	17	handsetGPS
0	0	0	1	0	0	1	0	12	18	handsetAGPS
0	0	0	1	0	0	1	1	13	19	handsetEOTD
0	0	0	1	0	1	0	0	14	20	handsetAFLT
0	0	0	1	0	1	0	1	15	21	handsetEFLT
0	0	0	1	0	1	1	0	16	22	handsetGNSS
0	0	0	1	0	1	1	1	17	23	handsetAGNSS
0	0	0	1	1	0	0	0	18	24	handsetOTDOA
0	0	0	1	1	0	0	1	19	25	handsetTBS
0	0	0	1	1	0	1	0	1A	26	handsetWi-Fi
0	0	0	1	1	0	1	1	1B	27	handsetBluetooth
0	0	1	0	0	0	0	0	20	32	hybridUnspecified
0	0	1	0	0	0	0	1	21	33	hybridAGPS_AFLT
0	0	1	0	0	0	1	0	22	34	hybridCellSector_AFLT
0	0	1	0	0	0	1	1	23	35	hybridNetworkTDOA_AOA
0	0	1	0	0	1	0	0	24	36	hybridNetworkTDOA_AGPS
0	0	1	0	0	1	0	1	25	37	hybridTDOA_AGPS_AOA
0	0	1	0	0	1	1	0	26	38	hybridAGPS_OTDOA
0	0	1	0	0	1	1	1	27	39	hybridAGNSS_OTDOA
0	0	1	0	1	0	0	0	28	40	hybridDeviceBased
0	0	1	0	1	0	0	1	29	41	hybridAGPS_RFPatternMatch
0	0	1	0	1	0	1	0	2A	42	hybridAGPS_Wi-Fi
0	0	1	1	0	0	0	0	30	48	cosUnspecified
0	0	1	1	0	0	0	1	31	49	cosWRLS – E9-1-1 Phase I only deployment. No positioning fix available.
0	0	1	1	0	0	1	0	32	50	cosWPH1 – E9-1-1 Phase I fallback for Phase II deployment.
0	0	1	1	0	0	1	1	33	51	cosWPH2 – E9-1-1 Phase II with caller's location.
0	0	1	1	0	1	0	0	34	52	cosTEXT – Text message sent to "911"

⁴ Use only if the Handset source type is not described by any of the other Handset Position Sources



H	G	F	E	D	C	B	A	Hex	Dec	Meaning
0	0	1	1	0	1	0	1	35	535	cosFIXD – Call originating from a small, semi-static wireless cell site.
0	0	1	1	0	1	1	0	36	545	cosRESA – Static wireless device at a residential address.
0	0	1	1	0	1	1	1	37	55	cosWCVC – E9-1-1 civic location
0	0	1	1	1	0	0	0	38	56	cosWDL1 – E9-1-1 medium level quality dispatchable civic location
0	0	1	1	1	0	0	1	39	57	cosWDL2 – E9-1-1 highest level quality dispatchable civic location

Exception handling:

- Undefined values in the range 1 (0x1) – 15 (0xF) are treated as value 1 (Network Unspecified)
- Undefined values in the range 16 (0x10) – 31 (0x1F) are treated as value 16 (Handset Unspecified)
- Undefined values in the range 32 (0x20) – 47 (0x2F) are treated as value 32 (hybridUnspecified)
- Undefined values in the range 48 (0x30) – 63 (0x3F) are treated as value 48 (cosUnspecified)
- Other undefined values are treated as if value 0 (unknown)

9.3.11 Generalized Time – ESRK Assignment

This parameter contains time of ESRK assignment. This timestamp is specified in Universal Coordinated Time (UTC).

Octet	H	G	F	E	D	C	B	A
1(=C4)	1	1	0	0	0	1	0	0
2	Length of Generalized Time = 6							
3	Year – 2000							

⁵ NENA has not adopted specific Classes of Service for Position Sources 53 (FIXD) and 54 (RESA) as recommended by TIA/ATIS. Refer to NENA-STA-015.10-2018 (originally 02-010) [8] for further discussion.



4	Month
5	Day of Month
6	MSB Time of Day
7	
8	
LSB	

9.3.12 Mobile Identification Number

Octet	H	G	F	E	D	C	B	A
1(=C5)	1	1	0	0	0	1	0	1
2	Mobile Identification Number Length = 9							
3	Type of Digits (Not Used)							
4	Nature of Number (International, No Presentation Restrictions)							
5	Numbering Plan (Not Applicable)				Encoding (BCD)			
6	Number of Digits							
7	Digit 2				Digit 1			
8	Digit 4				Digit 3			
9	Digit 6				Digit 5			
10	Digit 8				Digit 7			
11	Digit 10				Digit 9			

See Section 9.3.3 for how to encode type of digits, nature of number, numbering plan and encoding fields.

9.3.13 International Mobile Subscriber Identity

Octet	H	G	F	E	D	C	B	A
1(=C6)	1	1	0	0	0	1	1	0
2	IMSI Length = 12							
3	Type of Digits (Not Used)							
4	Nature of Number (International, No Presentation Restrictions)							

Octet	H	G	F	E	D	C	B	A
5	Numbering Plan (Land Mobile Numbering)				Encoding (BCD)			
6	Number of Digits							
7	Digit 2				Digit 1			
8	Digit 4				Digit 3			
9	Digit 6				Digit 5			
10	Digit 8				Digit 7			
11	Digit 10				Digit 9			
12	Digit 12				Digit 11			
13	Digit 14				Digit 13			
14	Filler				Digit 15			

See Section 9.3.3 for how to encode type of digits, nature of number, numbering plan, and encoding fields.

9.3.14 Mobile Call Status

This parameter identifies the validation status of the MS' subscription or the access status of an MS for a particular call origination.

Octet	H	G	F	E	D	C	B	A
1(=C7)	1	1	0	0	0	1	1	1
2	Length of Mobile call status = 1							
3	Authorization				Authentication			

The table below identifies the legal values for Authentication and their meanings.

D	C	B	A	Hex	Meaning
0	0	0	0	00	Authentication not performed
0	0	0	1	01	Authentication successful
0	0	1	0	02	Authentication failure

The table below identifies the legal values for Authorization and their meanings.

H	G	F	E	Hex	Meaning
0	0	0	0	00	Authorization not performed
0	0	0	1	01	Authorization successful
0	0	1	0	02	Invalid Electronic Serial Number
0	0	1	1	03	Unassigned Directory Number
0	1	0	0	04	Duplicate Unit
0	1	0	1	05	Delinquent Account
0	1	1	0	06	Stolen Unit
0	1	1	1	07	Not Authorized for MSC
1	0	0	0	08	Unspecified
				09-15	Reserved. Treat the same as value 0. Authorization not performed.

9.3.15 Company ID

This parameter carries a unique identifier for the wireless service provider.

Octet	H	G	F	E	D	C	B	A
1(=C8)	1	1	0	0	1	0	0	0
2	Company ID Length is Variable (up to 15 octets)							
3	Company ID String (most significant octet)							
4								
							
n-1								
N	Company ID String (least significant octet)							

9.3.16 Location Description

This parameter provides descriptive location information to the PSAP. This parameter will be used to provide general location information of the caller. It can also be used to deliver Phase I data if the Phase II information is not available.

Octet	H	G	F	E	D	C	B	A
1(=CE)	1	1	0	0	1	1	1	0
2(+)	Location Description Length is Variable (up to 512 octets)							
3	Location Description (most significant octet)							
4								
							
n-1								
N	Location Description (least significant octet)							

Due to legacy implementation considerations, the data in this field may be in either of two similar (but not interchangeable) formats. To achieve full interoperability, implementations may need to send or accept both formats.

9.3.16.1 Full XML

The "Full XML" format is the nominal format for this field and is an XML 1.0 fragment consisting of one or more of the XML elements defined below. Each of the elements may appear zero or one time, in any order. Although this document does not create a formal schema, the list of elements is analogous to the XML schema definition of 'all' within a complexType.

While the fragment is not an XML document, does not have an enclosing root element, and does not include an XML declaration, it MUST otherwise follow the "well-formedness constraints" of the XML standard [14] so that conforming XML processors can parse the data. Note that violations of these constraints are fatal errors as specified in the XML standard [14] and "the processor MUST NOT continue normal processing". However, special consideration is given below.

9.3.16.2 Pseudo XML

The "Pseudo XML" format is the same as the Full XML format, except that it does not follow all of the "well-formedness constraints" of the XML standard [14]. Specifically, escape sequences are not used, and the ampersand (&) may appear unescaped. Several additional constraints are imposed as a direct consequence. The rules for using this format are as follows:

- Escape sequences, including numeric character references, MUST NOT be used.
- The ampersand character MAY appear in literal form in values.
- The left angle bracket MUST NOT appear except as a markup delimiter.

- The string “]]>” MUST NOT appear in the content of elements.
- Attribute values MUST NOT contain both single and double quotes, and an attribute value which contains either a single or a double quote MUST be delimited with the other.
- Those items which are disallowed cannot be represented using escape sequences, and therefore MUST be removed from any input data.

9.3.16.3 Compatible Parsing

Implementations MAY use a conforming XML processor to parse the Pseudo XML format by replacing any ampersands with the escape sequence “&#amp;#x26;” prior to submitting the data to the XML processor. However, this substitution MUST NOT be applied to data in the Full XML format. A conforming XML processor will successfully parse Pseudo XML data without modifications, if that data does not contain an ampersand, but will experience a fatal error if an ampersand is present. An implementation MAY use this to distinguish between the formats, and only perform the described substitution if the attempt to parse the unmodified data fails.

9.3.16.4 Characters Permitted

In order to support the use of XML in the Location Description, it is necessary to deviate from J-STD-036 [5] which defines the content of this field as an ASN.1 PrintableString. The PrintableString definition excludes a number of characters required for the expression of XML such as angle brackets, the ampersand, and the semicolon. In place of the J-STD-036 [5] definition, this document defines the Location Description content to be text that MUST be encoded as UTF-8 and is further restricted to the character range described in section 2.2 of the XML standard [14]. Note that ASCII characters encoded as 8-bit bytes with the most significant bit set to zero are a subset of UTF-8. Various “extended ASCII” schemes are not compatible with UTF-8 and MUST NOT be used without the appropriate conversion to UTF-8. The Unicode byte order mark (BOM) SHOULD NOT be used.

It is intended that this definition is compatible with existing implementations based on the ASCII character set without requiring changes to the implementations. However, those implementations may not be able to correctly receive UTF-8 characters beyond the ASCII set. Senders (MPCs) SHOULD use ASCII only unless they have previously verified UTF-8 with their intended recipients.

9.3.16.5 XML Elements

The element names listed below were originally defined in a now-obsolete version of NENA 02-010 and subsequent updates to NENA version 4 XML schemas are not compatible with the names or usage here. It is therefore necessary for the following element definitions to be normative for use within the E2 location description. The elements have no namespace.

The MPC MAY include other elements that are not defined here, and the ESME MUST ignore elements that it does not recognize. Type values are: A=Alphabetic, N=Numeric, V=Variable Length.

Name	Tag	Max Chars	Type	Description
Cell ID	<CEL>	6	ANV	Identification number indicating a geographic region of wireless coverage. i.e., the cell site where the call is received.
Class of Service	<CLS type="x">	1	AN	The single character code for a class of service as described in section 18 of NENA STA-015.10-2018 [8]. The code "x" appears as the value of the "type" attribute, and the element value is left empty.
Comments	<CMT>	30	ANV	Optional notes which may be displayed at a PSAP.
Company ID 1	<CPF>	5	ANV	NENA registered Company Identification code for Service Provider providing wireline or wireless service to the customer.
County ID	<COI>	5	ANV	County Identification Code
Customer Name	<NAM	32	ANV	Subscriber Name
Emergency Medical Service Responder	<EMS>	25	ANV	Name of Emergency Medical Service Responder associated with the ESN of the caller.
Emergency Services Number	<ESN>	5	ANV	Emergency Service Number associated with the House Number and Street Name and Community Name. <i>Note: The Service Provider, providing the E9-1-1 Selective Routing will assign ESN's.</i>

Name	Tag	Max Chars	Type	Description
Fire Department Service Responder	<FIR>	25	ANV	Name of Fire Department Service Responder associated with the ESN of the caller.
House Number	<HNO>	10	ANV	House Number
House Number Suffix	<HNS>	4	ANV	House Number Extension (e.g., 1/2)
Law Enforcement Service Responder	<LAW>	25	ANV	Name of Law Enforcement Service Responder associated with the ESN of the caller.
Location	<LOC>	60	ANV	<p>Additional location information (free formatted) describing the exact location of the Calling Party Number. (e.g., "Apt 718" or "cell sector A") Emergency Response Location (ERL) - A Location to which a 9- 1-1 emergency response team may be dispatched.</p> <p>Alternatively, this element may contain sub-address data structured as described by ATIS-0700028.002 (see below).</p> <p>The location should be specific enough to provide a reasonable opportunity for the emergency response team to quickly locate a caller anywhere within it. <i>This information may be displayed at the PSAP</i></p>
MSAG Community	<MCN>	32	AV	Valid service community name as identified by the MSAG
Post Directional	<POD>	2	AV	Directional Trailing street direction suffix. Valid Entries: N S E W NE NW SE SW



Name	Tag	Max Chars	Type	Description
Prefix Directional	<PRD>	2	AV	Directional Leading street direction prefix. Valid Entries: N S E W NE NW SE SW
Sector ID	<SEC>	2	AN	Sub set/section of a cell.
State	<STA>	2	A	Alpha U.S. state or Canadian province abbreviation, i.e., TX (Texas), ON (Ontario)
Street Name	<STN>	60	ANV	Valid service address of the Calling Party Number
Street Name Suffix	<STS>	4	AV	Valid street abbreviation, as defined by the U S Postal Service Publication 28. (e.g. AVE)
Type of Service	<TYS type="x">	1	AN	The single character code for a type of service as described in section 9 of NENA STA-015.10-2018 [8]. The code "x" appears as the value of the "type" attribute, and the element value is left empty.
Postal or Zip Code	<ZIP>	10	ANV	The postal code or Zip code associated with the location.

ATIS-0700028.v002:2018 [12] was developed to align with the FCC requirements for improved location accuracy and uses the concepts of the Location Description parameter defined above to pass location information across the E2 interface. It extended the addressing concepts by defining sub-address attributes in the Location field of the Location Description parameter. The table below (extracted from Table 8-5 of ATIS-0700028.v002 [12]) illustrates the sub address attributes.

Attribute	Location Description Field	Example
Building (BLD)	LOC (60)	<LOC> BLD A FLR 5 UNIT 12</LOC>
Additional Location Information	LOC (60)	<LOC> LOC West Wing</LOC>



Attribute	Location Description Field	Example
(LOC)		
Floor (FLR)	LOC (60)	<LOC>BLD A FLR 5 UNIT 12</LOC>
Unit (UNIT)	LOC (60)	<LOC>FLR 5 UNIT 12 </LOC>
Room (ROOM)	LOC (60)	<LOC>FLR 5 ROOM 102 SEAT 23</LOC>
Seat (SEAT)	LOC (60)	<LOC>FLR 5 ROOM 102 SEAT 23 </LOC>
Place Type (PLC)	LOC (60)	<LOC> PLC MTS</LOC>

The priority of mapping sub-address attributes to the LOC element in the E2 Location Description parameter is as follows:

BLD | FLR | UNIT | ROOM | SEAT | MP | LOC | LMK (or LMKP) | PLC | UBP
where Uncompensated Barometric Pressure (UBP) is defined as an Integer between 30,000 and 115,000 in units of Pascals.

A string longer than 60 characters will be truncated right to left (left justified). A space is inserted between each element. All strings (except UBP) will be preceded by a descriptor that contains the name of the CLDXF element (e.g., BLD).

10 NENA Registry System

Not applicable

11 Documentation Required for the Development of a NENA XML Schema

Not applicable.

12 Impacts, Considerations, Abbreviations, Terms, and Definitions

12.1 Operations Impacts Summary

This document is a revision to a legacy standard that includes minimal changes. Existing systems may continue to be used without modification, in which case there will be no operational impact. Alternatively, updated systems will be able to better present location data and will be less likely to encounter interoperability issues that may impede successful delivery of location data to the PSAP.

12.2 Technical Impacts Summary

The revisions contained in this document are intended to clarify aspects of the E2 protocol that were not sufficiently described in the previous version, clarify and enhance the ability to communicate civic location data, and to align with ANSI/J-STD-036-C-2-2017 [5]. Details added regarding the Location Description parameter provide a clear path for resolving compatibility issues in existing implementations due to differing interpretations of the previous standard. Unmodified ESME implementations will continue to function but may not fully recognize new position source or civic location elements.

Implementors will find this document to be a more complete description of the E2 protocol, reducing the difficulty of producing interoperable systems and gateways during the transition to NG9-1-1.

12.3 Security Impacts Summary

The E2 protocol communicates over TCP/IP in the clear and includes no provision for authentication, privacy, or verification of message integrity. Modifying the protocol to include these features would require modification of the underlying standards and is beyond the intended scope of changes for this revision. Existing implementations use sufficient mechanisms to protect E2 communications at the underlying network layers, and new implementers should likewise employ such mechanisms.

12.4 Recommendation for Additional Development Work

E2 is a legacy protocol that will be made fully obsolete by NG9-1-1 location services. No further work is recommended at this time.

12.5 Anticipated Timeline

Systems implementing the E2 protocol are widely deployed. The time required to modify implementations to include the changes in this revision should be less than one year. However, no specific timeline for deployment can be anticipated due to widely varying constraints and business requirements regarding legacy systems.

12.6 Cost Factors

Enhancements to implementations based on the content of this document will require software changes. Although these changes are generally limited, the associated costs may vary significantly depending on the stage of the software development life cycle of any given implementation.

12.7 Cost Recovery Considerations

Normal business practices shall be assumed to be the cost recovery mechanism.

12.8 Additional Impacts (non-cost related)

The effort to update this document has resulted in the submission of an issue statement to ATIS seeking study and possible changes related to the use of the Position Source parameter and the desire to communicate separate methods of location determination for both geodetic and civic locations. This submission may or may not result in additional standards development work and changes to the E2 protocol.

No additional impacts are anticipated beyond the technical and operational impacts discussed above.

12.9 Abbreviations, Terms, and Definitions

See NENA Master Glossary of 9-1-1 Terminology, NENA-ADM-000 [1], for a complete listing of terms used in NENA documents. All abbreviations used in this document are listed below, along with any new or updated terms and definitions.

Term or Abbreviation (Expansion)	Definition / Description
ALI (Automatic Location Identification)	The automatic display at the PSAP of the caller’s telephone number, the address/location of the telephone and supplementary emergency services information of the location from which a call originates.
CBN (Call Back Number)	A number used by the PSAP to re-contact the location from which the 9-1-1 call was placed. The number may or may not be the number of the station used to originate the 9-1-1 call.
E2, E2+ (E2 Interface)	An industry standard interface (defined in J-STD-036) used between a Mobile Positioning Center (MPC/GMLC) and an ALI database server.
ESME (Emergency Services Message Entity)	Routes and processes the out-of-band messages related to emergency calls. This may be incorporated into selective routers (also known as Routing, Bridging and Transfer switches) and Automatic Location Identification (ALI) database engines.
ESN (Emergency Service Number)	A 3-5 digit number that represents one or more ESZs. An ESN is defined as one of two types: Administrative ESN and Routing ESN.
ESNE (Emergency Services Network Entity/Element)	A network element of TIA/EIA/J-STD- 036. The ESNE routes and processes the voice band portion of the



Term or Abbreviation (Expansion)	Definition / Description
	emergency call. This is composed of selective routers (also known as Routing, Bridging and Transfer switches).
ESP (Emergency Service Protocol)	A telecommunications protocol defined by J-STD-036 for the exchange of data through the E2 interface.
ESRD (Emergency Services Routing Digit)	A 10-digit North American Numbering Plan number that uniquely identifies a base station, cell site, or sector that is used to route wireless emergency calls through the network. The ESRD may also be used by the PSAP to retrieve the associated ALI data.
ESRK (Emergency Services Routing Key)	A 10-digit North American Numbering Plan number that uniquely identifies a wireless emergency call, is used to route the call through the network, and used to retrieve the associated ALI data.
IP (Internet Protocol)	The method by which data is sent from one computer to another on the Internet or other networks.
LNG (Legacy Network Gateway)	An NG9-1-1 Functional Element that provides an interface between a non-IP originating network and a Next Generation Core Services (NGCS) enabled network.
MPC/GMLC (Mobile Positioning Center/ Gateway Mobile Location Center)	A Functional Entity that provides an interface between the wireless originating network and the Emergency Services Network. The MPC/GMLC retrieves, forwards, stores and controls position data within the location services network. It interfaces with the location server (e.g., Position Determining Entity [PDE]) for initial and updated position determination. The MPC/GMLC restricts access to provide position information only while an emergency call is active.
PDE (Position Determining Entity)	Determines the precise position or geographic location of a wireless terminal when the MS starts a call or while the MS is engaged in a call. Each PDE supports one or more position determining technologies. Multiple PDEs may service the coverage area of an MPC and multiple PDEs may serve the same coverage area of an MPC utilizing different positioning determining technologies. (PDE is synonymous with Location Determination Technology [LDT])



Term or Abbreviation (Expansion)	Definition / Description
PSAP (Public Safety Answering Point)	An entity responsible for receiving 9-1-1 calls and processing those calls according to a specific operational policy.
SCCP (Signaling Connection Control Part)	The protocol used at the transport layer for TCAP-based services such as freephone (toll free services), calling card, local number portability, wireless roaming, and personal communication services (PCS). SCCP also provides the means by which an STP can perform global title translation (GTT), a procedure by which the destination signaling point and subsystem number (SSN) is determined from digits (i.e., the global title) present in the signaling message.
TCAP (Transaction Capabilities Application Part)	An application protocol used to connect to an external database, perform a query of the database and retrieve information. The information or data retrieved is then sent back in the form of a TCAP message to the signaling point that requested it. It may reside upon the SS7 protocol stack or TCP/IP stack.
TCP (Transmission Control Protocol)	A communications protocol linking different computer platforms across networks. TCP/IP functions at the 3rd and 4th levels of the Open System Interconnection (OSI) model.
TCP/IP (Transmission Control Protocol/Internet Protocol)	A communications protocol linking different computer platforms across networks. TCP/IP functions at the 3rd and 4th levels of the Open Systems Interconnection model.
V-E2 Interface (Voice over Internet Protocol E2 Interface)	VPC to ALI DB. The V-E2 interface uses the E2+ protocol as defined in NENA-STA-018.2, with modifications required for support of i2.
VPC (VoIP Positioning Center)	The element that provides routing information to support the routing of VoIP emergency calls and cooperates in delivering location information to the PSAP over the existing ALI DB infrastructure. The VPC supports access to the routing data in the ERDB.



13 References

- [1] National Emergency Number Association. *Master Glossary of 9-1-1 Terminology*. [NENA-ADM-000.023-2020](#). Alexandria, VA: NENA, approved April 13, 2018.
- [2] Alliance for Telecommunications Industry Solutions. *Signaling System Number 7 (SS7) – Transaction Capabilities Transaction Part (TCAP)*. [ATIS 1000114.2004\(S2019\)](#). Washington, DC: ATIS, approved September 1, 2004.
- [3] Alliance for Telecommunications Industry Solutions. *Emergency Calling Service*. [ATIS 1000628.2000\(R2015\)](#). Washington, DC: ATIS, approved May 1, 2000.
- [4] Telecommunications Industry Association. *Cellular Radiotelecommunications Intersystem Operations*. [TIA/EIA-41-D](#), November 13, 1997.
- [5] Telecommunications Industry Association (TIA) and Alliance for Telecommunications Industry Solutions. *ATIS Joint Standard – Enhanced Wireless 9-1-1 Phase II*, [ATIS J-STD-036-C-2-2017](#), approved June 19, 2017.
- [6] National Emergency Number Association. *Standards for Recommended Formats & Protocols For Data Exchange*. [NENA 02-010](#). Alexandria, VA: NENA, approved February 2002. (Archived)
- [7] National Emergency Number Association. *Interim VoIP Architecture for Enhanced 9-1-1 Services (i2)*. [NENA 08-001 v2](#). Alexandria, VA: NENA, approved August 11, 2010.
- [8] National Emergency Number Association. *Standard Data Formats for E9-1-1 Data Exchange & GIS Mapping*. [NENA STA-015.10-2018 \(originally 02-010\)](#). Alexandria, VA: NENA, approved August 12, 2018.
- [9] National Emergency Number Association. *NENA Standard for the Implementation of the Wireless Emergency Service Protocol E2 Interface*. [NENA 05-001](#). Alexandria, VA: NENA, approved December 2, 2003.
- [10] Alliance for Telecommunications Industry Solutions. *Signaling System Number 7 (SS7) – Transaction Capabilities Transaction Part (TCAP)*. [ANSI T1.114-2000](#). Washington, DC: ATIS, approved June 1, 2000.
- [11] Internet Engineering Task Force (IETF). *Representation of Uncertainty and Confidence in the Presence Information Data Format Location Object (PIDF-LO)*. M. Thomson and J. Winterbottom. [RFC 7459](#), February 2015.
- [12] Alliance for Telecommunications Industry Solutions. *Location Accuracy Improvements for Emergency Calls (version 2)*. [ATIS-0700028.V002:2018](#). Washington, DC: ATIS, approved December 2018.
- [13] Internet Engineering Task Force. *XML Media Types*. H. Thompson and C. Lilley. [RFC 7303](#), July 2014.
- [14] World Wide Web Consortium (W3C). *Extensible Markup Language (XML) 1.0 (Fifth Edition)*. T. Bray, J. Paoli, C.M. Sperberg-McQueen, E. Maler and F. Yergeau. <https://www.w3.org/TR/2008/REC-xml-20081126/>, 26 November 2008.

- [15] National Emergency Number Association. *NENA Detailed Functional and Interface Standards for the NENA i3 Solution*. [NENA-STA-010.2-2016](#). Alexandria, VA: NENA, approved September 10, 2016.

14 Exhibit X

Not Applicable

15 Appendix

Not Applicable

ACKNOWLEDGEMENTS

The National Emergency Number Association (NENA) 9-1-1 Core Services Committee, E2 Interface Working Group developed this document.

NENA Board of Directors Approval Date: **02/17/2021**

NENA recognizes the following industry experts and their employers for their contributions to the development of this document.

Members	Employer
Stephen O’Conor, 9-1-1 Core Services Committee Co-Chair	Next Generation 9-1-1 Consulting Services, LLC
Theresa Reese, 9-1-1 Core Services Committee Co-Chair, Technical Editor	Ericsson Inc
Dan Banks, Working Group Chair	Digital Data Technologies Inc
Tom Breen-ENP	Comtech Telecommunications Corporation
Victor Burton	Comtech Telecommunications Corporation
Nicole Graves-ENP	911 Datamaster Inc
Tom Hsu	Nokia
Roger Marshall	Comtech Telecommunications Corporation
Fondra Marshall-ENP	Bandwidth
Glen Roach-ENP	Emergency Public Safety Communications Consultants

Special Acknowledgements:

Delaine Arnold, ENP, Committee Resource Manager, has facilitated the production of this document through the prescribed approval process.

The E2 Interface Working Group is part of the NENA Development Group that is led by:

- Wendi Rooney, ENP, and Jim Shepard, ENP, Development Steering Council Co-Chairs
- Brandon Abley, ENP, Technical Issues Director
- April Heinze, ENP, PSAP Operations Director