

# **NENA Emergency Services IP Network Design for NG9-1-1 (NID)**



NENA Emergency Services IP Network Design for NG9-1-1

NENA 08-506, Version 1, December 14, 2011

Development Steering Council Approval Date, November 1, 2011

Standards Advisory Committee Approval Date, November 22, 2011

NENA Executive Board Approval Date, December 14, 2011

Prepared by:

National Emergency Number Association (NENA) VoIP/Packet Technical Committee – ESIND WG

Published by NENA

Printed in USA

**NENA**  
**INFORMATION DOCUMENT**

**NOTICE**

The National Emergency Number Association (NENA) publishes this document as an information source for the designers and manufacturers of systems to be utilized for the purpose of processing emergency calls. It is not intended to provide complete design specifications or parameters or to assure the quality of performance for systems that process emergency calls.

NENA reserves the right to revise this Information 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
- or to reflect changes in the design of network interface or services described herein.

It is possible that certain advances in technology 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.

Patents may cover the specifications, techniques, or network interface/system characteristics disclosed herein. No license expressed or implied is hereby granted. 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.

This document has been prepared solely for the use of E9-1-1 System Service Providers, network interface and system vendors, participating telephone companies, etc.

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 change to this document may be submitted to:

National Emergency Number Association

4350 North Fairfax Drive, Suite 750

Arlington, VA 22203-1695

800-332-3911

or: [commleadership@nena.org](mailto:commleadership@nena.org)

Acknowledgments:

The National Emergency Number Association (NENA) Technical Committee Chairs and ESIND WG developed this document.

NENA recognizes the following industry experts and their companies for their contributions in development of this document.

**Version 1, Approval Date, 12/14/2011**

Robert Walthall, CISSP - ESIND WG Leader	National Public Safety Solutions
Nate Wilcox, ENP - VoIP/Packet Technical Committee Chair	microDATA
Roger Marshall, VoIP/Packet Technical Committee Vice Chair	Telecommunication Systems
Armstrong, Michael	Verizon
Atkins, Richard, ENP	Tarrant County 9-1-1 District
Berryman, Marc	Digital Data Technologies Inc
Blackwell, Rick, ENP	Greenville Co 9-1-1
Brabant, Bernard	Brabant, Bernard Consultant 9-1-1
Carlson, Karen	Motorola Solutions Inc.
Dotson, Tim	Houston Galveston Area Council
Evans, Gary	Vision Net
Fletcher, Mark J, ENP	Avaya
Irwin, Dave	Washington Military Department, Emergency Management Division
Irons, Johnny	9-1-1 ACOG
Jones, Rick	NENA
Lamere, Jared	State of Vermont
Militeau, Christian	Intrado
Mongrain, Dan	Frequentis USA
Patel, Kantu	AT&T
Rohrer, Kevin	Commission on State Emergency Communications
Rosen, Brian	NeuStar
Schlesinger, Jerry, ENP, PMP	City of Portland Public Safety Revitalization Program
Stoffels, Paul	AT&T
Vislocky, Mike	Network Orange
Zeller, Victoria	Sprint



This committee would also thank Tom Breen Technical Committee Chair/Liaison, Tony Busam Technical Committee Vice-Chair/Liaison, Roger Hixson, Technical Issues Director; and Rick Jones, Operations Issues Director for their support and assistance. The committee/working group would also like to give a special thank you to Barbara Thornburg for her support & assistance.

**TABLE OF CONTENTS**

- 1 EXECUTIVE OVERVIEW .....7**
- 2 INTRODUCTION.....7**
  - 2.1 OPERATIONS IMPACTS SUMMARY .....7
  - 2.2 TECHNICAL IMPACTS SUMMARY .....7
  - 2.3 SECURITY IMPACTS SUMMARY .....7
  - 2.4 DOCUMENT TERMINOLOGY.....8
  - 2.5 REASON FOR ISSUE/REISSUE .....8
  - 2.6 RECOMMENDATION FOR ADDITIONAL DEVELOPMENT WORK.....8
  - 2.7 DATE COMPLIANCE.....8
  - 2.8 ANTICIPATED TIMELINE.....8
  - 2.9 COSTS FACTORS.....8
  - 2.10 FUTURE PATH PLAN CRITERIA FOR TECHNICAL EVOLUTION .....9
  - 2.11 COST RECOVERY CONSIDERATIONS.....9
  - 2.12 ADDITIONAL IMPACTS (NON COST RELATED) .....9
  - 2.13 INTELLECTUAL PROPERTY RIGHTS POLICY .....9
  - 2.14 ACRONYMS/ABBREVIATIONS.....10
- 3 EMERGENCY SERVICES IP NETWORK DESIGN.....13**
  - 3.1 OSI LAYER 1.....14
    - 3.1.1 *Copper*.....14
    - 3.1.2 *Coax Cable*.....15
    - 3.1.3 *3G/4G*.....15
    - 3.1.4 *Fiber*.....16
    - 3.1.5 *Microwave / Wireless Broadband*.....16
    - 3.1.6 *Satellite*.....17
  - 3.2 OSI LAYER 2.....17
    - 3.2.1 *HDLC (T1/T3)*.....17
    - 3.2.2 *Frame Relay*.....17
    - 3.2.3 *Asynchronous Transfer Mode*.....17
    - 3.2.4 *Metro Ethernet* .....19
    - 3.2.5 *Multiprotocol Label Switching*.....19



3.3 OSI LAYER 3.....20

    3.3.1 IP Addressing .....20

    3.3.2 Dynamic Routing Protocols .....21

        3.3.2.1 Open Shortest Path First (OSPF).....22

        3.3.2.2 Enhanced Interior Gateway Routing Protocol (EIGRP).....22

        3.3.2.3 Intermediate System –to-Intermediate System (IS-IS).....22

        3.3.2.4 Border Gateway Protocol (BGP).....22

3.4 AVAILABILITY AND RELIABILITY .....23

    3.4.1 Definitions and Equations .....23

    3.4.2 Achieving 5-9s Availability in 9-1-1 Networks.....26

    3.4.3 Network Availability and System Reliability in Legacy PSAPs.....26

    3.4.4 Defining Failure Metrics for an ESInet.....27

    3.4.5 Series and Parallel Reliability and Availability in ESInets.....27

3.5 NETWORK SECURITY.....29

    3.5.1 Session Border Controllers and Firewalls .....30

3.6 NETWORK MANAGEMENT AND MONITORING .....30

3.7 PERFORMANCE REQUIREMENTS .....31

    3.7.1 Packet Loss.....32

    3.7.2 Jitter.....32

    3.7.3 Latency .....32

3.8 HARDWARE/NETWORK ELEMENTS .....32

3.9 SERVICE LEVEL AGREEMENT .....33

3.10 LOCAL AREA NETWORK (LAN) ARCHITECTURE .....34

3.11 TRAFFIC ENGINEERING .....34

    3.11.1 Dimensioning ESInet Data Circuits .....34

    3.11.2 Traffic Policing.....35

    3.11.3 Traffic Shaping .....36

    3.11.4 Quality of Service (QoS).....36

3.12 NETWORK ARCHITECTURE.....37

3.13 CONCLUSION.....40

**4 RECOMMENDED READING AND REFERENCES .....41**



## 1 Executive Overview

Many 9-1-1 entities have built, are building, or will build in the near future an Emergency Services IP network (ESInet) to connect PSAPs and other public safety agencies within a region and provide interconnect to other ESInets and originating service providers within a region or state. The effort and expense required to build these facilities is significant. What steps can be taken today to ensure that these IP networks will be able to meet the requirements for the i3 core services (e.g. ECRF, ESRP, etc.)? What are some of the major design considerations that should be taken into account? What are some of the caveats, limitations, and advantages of the various technologies? What can network designers do to assure maximum availability in disaster circumstances? The purpose of this document is to answer these questions and provide network architects, consultants, 9-1-1 entities, and state authorities with the information that will assist them in developing the requirements for and/or designing ESInets today that will be capable of meeting the requirements of an NG9-1-1 system.

## 2 Introduction

### 2.1 Operations Impacts Summary

This is an informational document. As such the recommendations made throughout this document may be considered for use when designing and deploying ESInets. When implemented, some of the recommendations within this document may have significant operational impacts.

### 2.2 Technical Impacts Summary

This is an informational document. As such the recommendations made throughout this document may be considered for use when designing and deploying ESInets. When implemented, some of the recommendations within this document may have significant technical impacts.

### 2.3 Security Impacts Summary

ESInets are utilized to provide IP transport between a number of different agencies and resources including; PSAPs, regional host sites, and state-level i3 core services. Many of the agencies connected to the ESInet will also be connected to untrusted networks including the Internet. Given the operating environment that NG9-1-1 requires it seems likely that PSAPs, regional 9-1-1 entities, and state authorities will experience deliberate attacks on their systems. Maintaining high degrees of reliability and security in this new environment will require a fundamental change in the approach taken to both physical and cyber security. The NENA Security for NG9-1-1 standard (NENA 75-001) is applicable and recommended. Qualified security engineers should be consulted when designing and deploying ESInets.

## 2.4 Document Terminology

The terms "shall", "must" and "required" are used throughout this document to indicate required parameters and to differentiate from those parameters that are recommendations. Recommendations are identified by the words "should" or "preferably".

## 2.5 Reason for Issue/Reissue

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

Version	Approval Date	Reason For Changes
Original	12/14/2011	Initial Document

## 2.6 Recommendation for Additional Development Work

The VoIP/Packet technical committee recommends that some of the material in this document be further developed into a NENA recommended standard. Outage reports for ESInets and NG9-1-1 elements in the ESInet have not been standardized. There are no generally accepted mechanisms for reporting outages of such networks. ESIND recommends NENA undertake an effort to define standardized outage reporting mechanisms.

## 2.7 Date Compliance

All systems that are associated with the 9-1-1 process shall be designed and engineered to ensure that no detrimental, or other noticeable impact of any kind, will occur as a result of a date/time change up to 30 years subsequent to the manufacture of the system. This shall include embedded application, computer based or any other type application.

To ensure true compliance, the manufacturer shall upon request, provide verifiable test results to an industry acceptable test plan such as Telcordia GR-2945 or equivalent.

## 2.8 Anticipated Timeline

ESInets are already being designed and deployed.

## 2.9 Costs Factors

A number of the design considerations for ESInets including availability, technology, and bandwidth include costs as one of the parameters. This document does not take an authoritative position on cost factors for the solutions incorporated herein. Nevertheless, due to the pragmatic experience of the participants, the document tends to consider cost as one of the variables in making recommendations.

## **2.10 Future Path Plan Criteria for Technical Evolution**

In present and future applications of all technologies used for 9-1-1 call and data delivery, it is a requirement to maintain the same level or improve on the reliability and service characteristics inherent in present 9-1-1 system design.

New methods or solutions for current and future service needs and options should meet the criteria below. This inherently requires knowledge of current 9-1-1 system design factors and concepts, in order to evaluate new proposed methods or solutions against the Path Plan criteria.

Criteria to meet the Definition/Requirement:

1. Reliability/dependability as governed by NENA's technical standards and other generally accepted base characteristics of E9-1-1 service
2. Service parity for all potential 9-1-1 callers
3. Least complicated system design that results in fewest components to achieve needs (simplicity, maintainable)
4. Maximum probabilities for call and data delivery with least cost approach
5. Documented procedures, practices, and processes to ensure adequate implementation and ongoing maintenance for 9-1-1 systems

This basic technical policy is a guideline to focus technical development work on maintaining fundamental characteristics of E9-1-1 service by anyone providing equipment, software, or services.

## **2.11 Cost Recovery Considerations**

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

## **2.12 Additional Impacts (non cost related)**

ESInets provide the infrastructure upon which NG9-1-1 will be deployed. Transition to NG9-1-1 will have additional impacts. In many cases ESInets replace existing communications facilities for PSAPs.

## **2.13 Intellectual Property Rights Policy**

NENA takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights.

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 Road, Suite 500  
 Alexandria, VA 22314  
 800-332-3911  
 or: [admin@comments@nena.org](mailto:admin@comments@nena.org)

## 2.14 Acronyms/Abbreviations

Some acronyms/abbreviations used in this document have not yet been included in the master glossary. After initial approval of this document, they will be included. See NENA 00-001 - NENA Master Glossary of 9-1-1 Terminology located on the NENA web site for a complete listing of terms used in NENA documents.

<b>The following Acronyms are used in this document:</b>		
<b>Acronym</b>	<b>Description</b>	<b>** New (U)pdate</b>
<b>3G</b>	3rd Generation Mobile Telecommunications	
<b>4G</b>	4th Generation Mobile Telecommunications	
<b>ATM</b>	Asynchronous Transfer Mode	
<b>BCF</b>	Border Control Function	
<b>BGP</b>	Border Gateway Protocol	
<b>CBR</b>	Constant Bit Rate	
<b>CSMA/DA</b>	Carrier Sense Multiple Access / Collision Detect	
<b>CTFE</b>	Call Taker Functional Element	
<b>DDOS</b>	Distributed Denial of Service Attack	
<b>DS3</b>	Digital Signal 3	
<b>DSL</b>	Digital Subscriber Line	
<b>DSX</b>	Digital Cross Connect	
<b>E9-1-1</b>	Enhanced 9-1-1	
<b>ECRF</b>	Emergency Call Routing Function	
<b>EIGRP</b>	Enhanced Interior Gateway Routing Protocol	
<b>ESInet</b>	Emergency Services IP Network	
<b>ESRP</b>	Emergency Services Routing Proxy	
<b>EMI</b>	Electromagnetic Interference	
<b>EVDO</b>	Evolution-Data Optimized	
<b>FCC</b>	Federal Communications Commission	
<b>FE</b>	Functional Element	
<b>FLM150</b>	SONET Multiplexer	
<b>HDLC</b>	High-Level Data Link Control	
<b>IETF</b>	Internet Engineering Task Force	

<b>The following Acronyms are used in this document:</b>		
<b>IP</b>	Internet Protocol	
<b>IPv4</b>	Internet Protocol version 4	
<b>IPv6</b>	Internet Protocol version 6	
<b>ISP</b>	Internet Service Provider	
<b>IS-IS</b>	Intermediate System To Intermediate System	
<b>LAN</b>	Local Area Network	
<b>LNG</b>	Legacy Network Gateway	
<b>LTE</b>	Long Term Evolution	
<b>MIB</b>	Management Information Base	
<b>mS</b>	Millisecond	
<b>MPLS</b>	Multi-Protocol Label Switching	
<b>NAT</b>	Network Address Translation	
<b>NENA</b>	National Emergency Number Association	
<b>NIC</b>	Network Interface Card	
<b>OSI</b>	Open Systems Interconnection	
<b>OSPF</b>	Open Shortest Path First	
<b>PSAP</b>	Public Safety Answering Point	
<b>PVC</b>	Permanent Virtual Circuit	
<b>QoS</b>	Quality of Service	
<b>RFC</b>	Request For Comments	
<b>SBC</b>	Session Border Controller	
<b>SLA</b>	Service Level Agreement	
<b>SONET</b>	Synchronous Optical Networking	
<b>TCP</b>	Transport/Transmission Control Protocol	
<b>TDM</b>	Time Division Multiplexing	
<b>UBR</b>	Unspecified Bit Rate	
<b>VBR</b>	Variable Bit Rate	
<b>VCI</b>	Virtual Channel Identifier	
<b>VLAN</b>	Virtual Local Area Network	
<b>VoIP</b>	Voice Over Internet Protocol	
<b>VPI</b>	Virtual Path Identifier	
<b>VPN</b>	Virtual Private Network	
<b>WAN</b>	Wide Area Network	

<b>The following Terms and Definitions are used in this document:</b>		
<b>Term</b>	<b>Definition</b>	<b>** New (U)pdate</b>
<b>Authentication</b>	A security term referring to the process of reliably identifying an entity requesting access to data or a service.	

<b>The following Terms and Definitions are used in this document:</b>		
<b>Term</b>	<b>Definition</b>	<b>** New (U)date</b>
<i><b>Authorization</b></i>	A security term referring to the process of making a decision regarding what access rights an authenticated entity has to data or a service.	
<i><b>Code Point</b></i>	A code for a requested QoS action used in the Diffserv QoS mechanism on an IP network. The code point is sent in the TOS field of an IP packet.	
<i><b>Denial of Service Attack</b></i>	A type of cyber attack intended to overwhelm the resources of the target and deny the ability of legitimate users of the target the normal service the target provides.	
<i><b>Diffserv</b></i>	A quality of service mechanism for IP networks characterized by a code in a field of a Packet called a “Code Point” and a “Per hop Behavior”.	
<i><b>Emergency Call Routing Function (ECRF)</b></i>	A functional element in an ESInet which is a LoST protocol server where location information (either civic address or geocoordinates) and a Service URN serve as input to a mapping function that returns a URI used to route an emergency call toward the appropriate PSAP for the caller’s location or towards a responder agency.	
<i><b>Emergency Services IP Network</b></i>	An ESInet is a managed IP network that is used for emergency services communications, and which can be shared by all public safety agencies. It provides the IP transport infrastructure upon which independent application platforms and core functional processes can be deployed, including, but not restricted to, those necessary for providing NG9-1-1 services. ESInets may be constructed from a mix of dedicated and shared facilities. ESInets may be interconnected at local, regional, state, federal, national and international levels to form an IP-based inter-network (network of networks).	
<i><b>H.264</b></i>	A video codec, defined by ITU-T in common use today for real time two way video.	
<i><b>Originating ESRP</b></i>	The first routing element inside the ESInet. It receives calls From the BCF at the edge of the ESInet.	
<i><b>Session Border Control</b></i>	A commonly available functional element that provides security, NAT traversal, protocol repair and other functions to VoIP signaling such as SIP. A component of a Border Control Function.	
<i><b>Terminating ERSP</b></i>	The last ESRP for a call in an ESInet, and typically chooses a queue of call takers to answer the call.	

### 3 Emergency Services IP Network Design

ESInets are like other IP networks in that they are a collection of routers and links between routers in which there are multiple paths such that failures leave at least one path that the network can use. ESInets, however, must be designed to meet more stringent requirements for security and reliability service levels than most other IP networks.

Per NENA 08-003 and for the purposes of this document ESInet is defined as follows:

An ESInet is a managed IP network that is used for emergency services communications, and which can be shared by all public safety agencies. It provides the IP transport infrastructure upon which independent application platforms and core functional processes can be deployed, including, but not restricted to, those necessary for providing NG9-1-1 services. ESInets may be constructed from a mix of dedicated and shared facilities. ESInets may be interconnected at local, regional, state, federal, national and international levels to form an IP-based inter-network (network of networks).

This document covers the design of ESInets at OSI layers 1, 2, and 3. Network architecture options and methodologies for achieving recommended reliability and availability service levels are discussed. Performance requirements and other aspects of service level agreements for operators of ESInets are covered, as well as several aspects of network security. ESInets must deliver high priority traffic in the face of severe congestion. Traffic engineering strategies for achieving that goal are discussed. Network management and monitoring of ESInets is also covered.

The intended audience for this document includes network architects that are tasked with designing ESInets and 9-1-1 entities or state authorities that are working with consultants and service providers to procure an ESInet. One of the objectives of this document is to provide 9-1-1 entities and state authorities with the background information necessary to identify their requirements. Another objective is to define the concepts and vocabulary that will enable 9-1-1 entities and state authorities to guide their service providers and consultants to design solutions that meet their requirements. A number of the topics covered in this document are fields of study to which people devote their entire careers. The information contained in this document by itself does not provide all of the necessary details to properly design ESInets. It is a best practice to engage qualified IP network design engineers when designing ESInets.

A summary of the core requirements for an ESInet as summarized in the NENA 08-003 v 1.0 Detailed Functional and Interface Specification for the NENA i3 Solution – Stage 3 are as follows:

- The network between the PSAP and the ESInet will be a private or virtual private network based upon TCP/IP
- It will have scalable bandwidth to support new enhanced services.
- The Emergency Services IP Network shall be a conventional routed IP network
- MPLS or other sub-IP mechanisms are permitted as appropriate
- The PSAP should use redundant local area networks for reliability

- PSAP LAN to the ESInet must be resilient, secure, physically diverse, and logically separate
- The ESInet shall be engineered to sustain real time traffic, including data, audio, and video
- Connections between the PSAP and ESInet shall be secured TCP/IP connections
- ESInets should be capable of operating on IPv4 and IPv6 network infrastructures

### 3.1 OSI Layer 1

In this section we will discuss different types of physical cabling that are typically used to deliver services to a site that is connected to an ESInet, and some of the caveats and best practices utilized when designing the physical layer of an ESInet.

For the most part circuits are delivered to sites connected to an ESInet over one of the following:

- Copper
- Fiber
- Radio
- Satellite

There is a lot of emphasis on “no single point of failure” in 9-1-1, and while redundant physical circuits are sometimes ordered, for the most part PSAPs do not have dual entrance facilities. So the last mile (manhole to PSAP) is almost always in the same conduit/trench. Backhoe fade is a common cause of outages in the physical layer, but the cost of construction for dual entrance facilities is prohibitive.

There is some benefit to having multiple circuits even when they are in the same conduit/trench assuming different equipment is attached to the circuits (DSX-1, FLM150, etc). This is sometimes accomplished by ordering the redundant circuit from a separate service provider. However, care should be taken to ensure that the service provider for the redundant circuit is not purchasing/reselling service from the service provider that is delivering the primary circuit. A best practice when designing connections into an ESInet is to utilize as many technologies and service providers as is reasonable and economically feasible.

#### 3.1.1 Copper

Copper continues to be widely utilized for digital infrastructure in the United States. Services delivered over copper are frequently muxed onto fiber facilities at the Central Office, but in many cases the last mile of a 3 Mbps or smaller data circuit will be delivered over copper.

Advantages

- Repairs are relatively simple and fast
- Easier to troubleshoot and maintain

#### Disadvantages

- Limited capacity in terms of bandwidth
- EMI/Environmental
- Grounding issues

### 3.1.2 Coax Cable

DS3 circuits are delivered over coax cables. DS3 signals are rare except within buildings, where they are used for interconnections and as an intermediate step before being muxed onto a SONET circuit. This is because a T3 circuit can only go about 600 feet (180m) between repeaters. A customer who orders a DS3 usually receives a SONET circuit run into the building and a multiplexer mounted in a utility box.

### 3.1.3 3G/4G

Current network deployment of 3G/4G technologies is maturing for more densely populated areas and therefore most PSAPs would have above average coverage to utilize for data link capability.

Even before 4G network coverage is fully deployed, current deployment levels offer advantages to the PSAP for low-cost network connectivity.

#### Advantages to 3G/4G

- Adequate data bandwidth for 3G to support data (nominally ~10 Mbps up/down)
- Devices that offer 3G and 4G capabilities provide some amount of built in path redundancy between the respective built in technologies (e.g. EVDO/LTE).
- Additional bandwidth provided by 4G provides very good data throughput support
- The 4G transition to packet voice applications, 4G provides an adequate backup media path for limited voice communication
- Portable nature of 3G/4G mobile hotspot technology provides easy (though limited) scalability to support several call termination endpoints.
- Low cost
- Can scale to take advantage of multiple mobile hotspot devices
- Uses encrypted access path

#### Disadvantages

- Bandwidth is not guaranteed, but best effort, based on adjacent network capacity
- Shared public access network services

- Limited data transmission (caps), with significant data overage costs

### **3.1.4 Fiber**

Largely due to the advantages listed below, most of our nation's digital infrastructure is built on fiber optic circuits.

#### Advantages

- Fast Transmission Rates
- High BW
- Long Distance
- High Resistance to Interference/electromagnetic noise
- Low Maintenance
- EMI

#### Disadvantages

- Repairs are relatively difficult and slow.
- Cost

### **3.1.5 Microwave / Wireless Broadband**

Microwaves are electromagnetic wavelengths with frequencies between 300 Mhz and 300 Ghz. In 2002 the FCC designated the 4.9 GHz band for use in support of public safety. The FCC has also approved building wireless broadband networks for first responders in the 700 Mhz band. These microwave spectrums and others are being utilized to provide redundant WAN links to PSAPs. A best practice is to have radio links for ESInets engineered by professionals as it tends to significantly increase the reliability of the links.

#### Advantages

- Cost - significantly reduced to that of satellite
- Physical diversity - not in same conduit/trench as copper/fiber
- No cable(s) required between sites
- Microwave has multiple channels available for use
- Low power requirements for repeaters
- Easy implementation/installation into some areas
- Can be installed on existing support structures/masts

## Disadvantages

- Range is limited to approximately 25 miles
- Line of Sight
- Towers are expensive to construct/build
- Attenuation due to atmospheric conditions possible
- Tower maintenance can be problematic

### 3.1.6 Satellite

This is a topic for future study.

## 3.2 OSI Layer 2

Some of the most popular layer 2 protocols and technologies utilized to build ESInets are; HDLC (T1/T3), ATM, Metro Ethernet, and MPLS<sup>1</sup>. This section covers some of the advantages, disadvantages, caveats, and best practices utilized when designing the data link layer of an ESInet.

### 3.2.1 HDLC (T1/T3)

HDLC links have been utilized as the backbone for data networks for decades. These networks are highly reliable and have very low latency. Typically they are symmetric channels, with data rates in multiples of 1.54 Mbps. Multiple HDLC connections can be delivered to the same site to increase the aggregate capacity. HDLC links can be utilized for dedicated point to point connections where they are typically private (i.e. not shared).

### 3.2.2 Frame Relay

Frame-Relay was deployed in the early 1990s – approximately 10 years before VoIP was introduced to the commercial market. It was initially designed to transport data. After the advent of ATM, upgrades were made to Frame-Relay which enabled it to transport real-time data (i.e. voice and video). However, Frame-Relay is being phased out. So while it may be possible to design an ESInet based on Frame-Relay, it is not recommended.

### 3.2.3 Asynchronous Transfer Mode

There are a number of ESInets in operation today that rely on Asynchronous Transfer Mode (ATM) for transport. ATM is a cell-based switching technology that can guarantee deterministic QoS. It was

---

<sup>1</sup> MPLS and ATM are not strictly speaking layer 2 technologies. However they are included here because they are alternatives to true layer 2 technologies described in this section.

designed to transport real-time voice, data, and video. ATM service has been in demand in the US for over 10 years which has resulted the development of many very robust network architectures. ATM utilizes 3 main classes of service: Constant Bit Rate (CBR), Variable Bit Rate (VBR), and Unspecified Bit Rate (UBR).

The Constant Bit Rate (CBR) class of service was designed for applications that require a constant guaranteed bit rate between devices located across a Wide Area Network (WAN). CBR emulates Time Division Multiplexing (TDM) and requires more resources than the other classes of service. CBR is not as efficient or economical as other classes of service. Therefore, CBR is typically not recommended to build an ESInet.

The Variable Bit Rate (VBR) class of service is utilized by many companies throughout the world to transport a mix of real-time traffic such as voice and video, and traffic without real-time requirements (e.g., data). While it is technically possible to accommodate individual voice and video calls as individual circuits, practically, ESInets would be engineered to have all traffic on a single virtual circuit. It is a best practice to utilize VBR connections for ESInets.

Unspecified Bit Rate (UBR) is a best effort transport and it's typically used for IP services with no guaranteed bit rate. UBR is a common class of service for networks such as ESInets. However, the circuits must be over-provisioned / over-engineered in an attempt to prevent the best effort traffic from being dropped or delayed in the service provider's core network(s).

ESInets built on ATM networks typically utilize Permanent Virtual Circuits (PVCs) to build connections between WAN sites. The PVCs are identified by using a Virtual Path Identifier (VPI) / Virtual Circuit Identifier (VCI). A primary benefit of the ATM technology is the ability to reroute PVCs around layer 1 and/or layer 2 network outages.

ATM circuits are typically purchased in bit delivery rates (bandwidth) anywhere from 1.5Mbps to 155Mbps. ATM is a proven technology, that is well suited for ESInets, but may not be available in every region of the country or by some service providers in a particular region. Additionally, it may be replaced by newer technologies such as MPLS.

#### Advantages

- High Bandwidth
- Dedicated PVCs
- Private
- Low Latency
- Scalable
- Deterministic Quality of Service

#### Disadvantages

- Regional Availability

- Efficiency
- End of Life

### 3.2.4 Metro Ethernet

There are ESInets in operation today which have been built on Metro Ethernet services. Metro Ethernet provides a scalable, high performance broadband platform that supports next-generation voice, data, and video.

Metro Ethernet is a technology that uses several classes of layer 2 technologies to provide a service that behaves much like an Ethernet (CSMA/CD) over a wide area. Unlike Frame Relay and ATM, where the standards largely defined the service offering and the terms used in describing the technology, Metro Ethernet services vary widely depending on the objectives of the service provider. Metro Ethernet services are sometimes marketed under something like Business Class Ethernet or Business Ethernet. Metro Ethernet services are typically provisioned over private networks managed and sometimes monitored by service providers. Symmetrical rates are available anywhere from 1Mbps to 1Gbps. Different classes of service may be supported, or it could be best effort.

It is a best practice to utilize a delay sensitive Class of Service for emergency 9-1-1 calls. Priority classes of service may be used for various data within ESInets.

#### Advantages

- High Bandwidth
- Low Cost
- Dedicated
- Private
- Low Latency
- Scalable
- Regional Availability

#### Disadvantages

- Wide variation in services and SLAs
- Complex Traffic Engineering
- Reliability (varies with service provider)

### 3.2.5 Multiprotocol Label Switching

The MPLS technology takes advantage of advancements in technology (high speed switching), industry trends such as the pervasive use of SONET, and builds upon the strengths of earlier layer 2 technologies to provide reliable transport of next generation voice, data and video.

In an MPLS network packets are labeled as they enter the network. Packets are forwarded thru the network based on the information contained in the label, and label(s) are striped off the packets as they leave the MPLS network.

Different classes of service are available on some MPLS based service offerings. Classes of service are not defined in the MPLS standards. The traffic engineers of each service provider utilize traffic trunks, resource allocation, and constraint based routing to implement traffic management within their MPLS network thereby defining the classes of service that will be supported. MPLS classes of service are typically based on some combination of the following; delay/jitter sensitive, high, medium, and/or low priority traffic. It is a best practice to utilize a delay/jitter sensitive class of service for emergency 9-1-1 calls delivered over an MPLS network.

It is not uncommon for service providers to offer an SLA of three nines (99.9%) for services based on MPLS technology. This is due in part to reluctance on the part of the service provider to compensate customers for downtime and may not be a true indication of the availability that is typically achieved on the MPLS networks.

MPLS was designed to replace existing IP transport technologies such as ATM and Frame-Relay, and in many regions of the country the industry is moving in that direction.

#### Advantages

- High Bandwidth
- Private
- Scalable
- Regional Availability
- Low Latency
- Efficiency

#### Disadvantages

- Limited Build-out
- SLAs

### 3.3 OSI Layer 3

This section covers some of the advantages, disadvantages, caveats, and best practices utilized when designing the network layer of an ESInet.

#### 3.3.1 IP Addressing

Devices that are connected to an ESInet will be configured with an IP address. Today 98% of all devices that are configured with an IP address are utilizing IP version 4 (IPv4). The pool of public/registered IPv4 addresses is rapidly approaching exhaustion<sup>2</sup>.

Researchers have been developing methods of extending the life of IPv4 addressing for decades. Two of the most commonly deployed methods are RFC 1918 Private Address Space and RFC 2663 the Network Address Translator (NAT). Among other things NAT enables devices that are configured with private IP addresses to be able to reach the Internet and/or visa versa (devices on the Internet able to reach devices configured with private IP address). In order to delay the transition to IPV6 some service providers are deploying IPv4 NAT within the core networks which results in multiple NATs between the caller and the PSAP. However, there is a limit to the effectiveness of these methods to extend the life of IPv4. For example, NATs generally don't know how to fix addresses that are embedded in protocols such as SIP.

Internet Protocol version 6 (IPv6) is a new version of the Internet Protocol which was designed to succeed IPv4. IPv6 is not all that much different from IPv4. It has a number of incremental improvements, yet can be summarized as IPv4 with 128 bit addresses. This allows for a practically unlimited number of IP addresses (about  $3.4 \times 10^{38}$ ). One of the challenges with IPv6 is that it is not backwards compatible with IPv4. In other words, a host with an IPv6 address cannot directly communicate with an IPv4 host.

The original intent of the developers of the IPv6 technology was that for a period of "transition" all end systems, ISPs and services would support both IPv4 and IPv6 simultaneously, and when the point was reached where this dual stack environment was universally deployed, IPv4 could be dropped and an IPv6 only version of the Internet would result.

At this time the IPv4 registered address pool is nearing exhaustion and IPv6 deployment is between 0.2 and 2% of the Internet. The organizations that assign IP addresses are expecting the effects of IPv4 address depletion to begin to be felt in 2011. Largely due to cost, complexity, and other more pressing issues, many organizations have put off IPv6 migration. At this time, it seems unlikely that the transition period will be short.

It is a best practice to design and deploy ESInets in a dual stack (IPv4 and IPv6) environment so as to allow for the interoperation of existing IPv4 devices and infrastructure with future emergency services devices and infrastructure that will be constrained to operate only with IPv6 addresses.

Services within the ESInet should be designed to use IPv6.

### 3.3.2 Dynamic Routing Protocols

---

<sup>2</sup> Private consultation with chief scientist ARIN 7/2010

Dynamic routing protocols are commonly used within ESInets to determine the best route/path to use to transport IP packets to their destination. Routing protocols dynamically discover and re-route around outages, and they simplify the configuration and maintenance of routing within an ESInet. It is a best practice to utilize a dynamic routing protocol within an ESInet where two or more paths to a destination exist. IPv6 uses the same types of routing protocols as IPv4, but with some slight modifications to account for specific requirements of IPv6. This section evaluates some of the routing protocols which are commonly used for ESInets.

One of the terms that will need to be understood when working with dynamic routing protocols is autonomous system (AS). An AS is a network or a group of networks that is controlled by a common network administrator (or group of administrators) on behalf of an entity (such as a regional 9-1-1 entity). It is a best practice to configure regional ESInets to be their own AS. Thus, routers at individual PSAPs should be configured to run an Interior Gateway Protocol (such as OSPF, IS-IS, etc.). State and national level ESInets should utilize Border Gateway Protocol (BGP) to route between autonomous systems.

### **3.3.2.1 Open Shortest Path First (OSPF)**

OSPF is a link-state routing protocol that was defined in RFC 2328 in 1998. It is one of the most widely used Interior Gateway Protocols (IGP). OSPF is frequently used in conjunction with BGP for MPLS networks. OSPF is used to route within a single routing domain (i.e. autonomous system (AS)) and BGP is used to interconnect autonomous systems. OSPF Version 2 is limited to IPv4. When utilizing OSPF for routing within a regional ESInet, it is a best practice to utilize OSPF Version 3 which includes support for IPv6.

### **3.3.2.2 Enhanced Interior Gateway Routing Protocol (EIGRP)**

EIGRP is a proprietary Interior Gateway Protocol developed by Cisco. EIGRP is very efficient and feature rich routing protocol that supports IPv6 and is appropriate for use within regional ESInets

### **3.3.2.3 Intermediate System –to-Intermediate System (IS-IS)**

IS-IS is a link-state routing protocol standardized by RFC 1142. IS-IS is an Interior Gateway Protocol which provides fast convergence, scalability, and is very efficient in its use of network bandwidth. It is commonly used in large service provider networks, supports IPv6, and is appropriate for use in regional ESInets.

### **3.3.2.4 Border Gateway Protocol (BGP)**

BGP (version 4) is an Exterior Gateway Protocol that is defined in RFC 4271. Unlike the previously discussed routing protocols which are used to find a specific network within an Autonomous System (AS), BGP is used to find the AS where the given network can be found. Since BGP requires peer authentication, a router that wants to share route information with a BGP router must first authenticate. BGP is also very flexible in terms of how routing updates are to be handled. BGP

routers can be configured to send specific route updates to specific peers and/or not receive updates from specific peers. These are only a few of the characteristics that make BGP the routing protocol of choice when connecting to untrusted networks. In many cases BGP is the only dynamic routing protocol supported by service providers when connecting to an MPLS network. It is a best practice to utilize BGP in state-level and national-level ESInets.

### 3.4 Availability and Reliability

Availability and reliability are key concerns for 9-1-1. It is well known that the availability objective for 9-1-1 service is five nines (99.999%). It is not well known that this standard typically has not been met in terms of network connections to the PSAPs in legacy 9-1-1 (i.e. CAMA trunks and ALI circuits). ESInets provide an opportunity for 9-1-1 entities to build to a higher standard, though the resources required to do so must not be assumed, and must be factored in the design phase.

In this section the definitions of reliability and availability are given.<sup>3</sup> The formulas used by reliability engineers to design and calculate the reliability and availability of systems are described; examples are given showing the application of each equation.<sup>4</sup> What it takes to achieve 5 – 9s availability on network connections is examined. And a description is given of how 5 – 9s availability for 9-1-1 service has been achieved in legacy 9-1-1 while operating on networks that are less than 5 – 9s is given. Failure metrics for ESInets are discussed. And finally the formulas used to calculate series and parallel availability and reliability are covered and applied to an ESInet.

#### 3.4.1 Definitions and Equations

The difference between reliability and availability is often misunderstood. High availability and high reliability often go hand in hand, but they are not interchangeable terms.

*Reliability is the ability of a system or component to perform its required functions under stated conditions for a specified period of time [IEEE 90].<sup>5</sup>*

---

<sup>3</sup> Call failures that occur before the call reaches the ESInet (P.01, Wireless Service, VoIP Service Provider networks, etc.) are outside the scope of this document.

<sup>4</sup> Reliability engineering is a science. Most of the sections in the document cover topics that could affect availability and reliability. It is a best practice to engage qualified engineers when designing highly available systems.

<sup>5</sup> IEEE 90 – Institute of Electrical and Electronics Engineers, IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries. New York, NY: 1990

For example, the primary goal of an airline is to complete the flights safely - with no catastrophic failures.

*Availability, on the other hand, is the degree to which a system or component is operational and accessible when required for use [IEEE 90].*

For example, if a lamp has a 99.9% availability, there will be one time out of a thousand that someone needs to use the lamp and finds out that the lamp is not operational either because the lamp is burned out or the lamp is in the process of being replaced.

An attribute of reliability is,

$$R_a = \frac{\text{Successes}}{\text{Attempts}}$$

where attempts = successes + failures

For example, if there were 99,999 calls completed to 9-1-1 out of 100,000 attempts, you could claim 99.999% reliability.

Mean Time Between Failure (MTBF) is a basic measure of a system's reliability. The higher the MTBF, the higher the reliability of the system. The equation below illustrates this relationship.

$$R = e^{-\left(\frac{\text{Time}}{\text{MTBF}}\right)}$$

where  $e$  = the mathematical constant  $e$  or 2.718281828459045...

and Time = time of the mission in hours

When time is set to 8760 hrs (1 yr), the formula above yields the following results.

Reliability	Time (hrs)	Required MTBF (hrs)
0.9	8760	83,143
0.99	8760	871,613
0.999	8760	8,755,619
0.9999	8760	87,595,620
0.99999	8760	875,995,620
0.999999	8760	8,759,995,620

Typical commercial grade routers often have an MTBF ranging from 240,000 to 340,000 hrs. (It should be noted that MTBF is often computed using methods that may not correlate to actual results.)

Thus depending on the methods used by the manufacturer to calculate the MTBF it may be necessary to reduce the MTBF by as much as half. )

Availability, in its simplest form, can be calculated as,

$$A = \frac{UpTime}{(UpTime + DownTime)}$$

Availability is often thought of in terms of downtime per year according to the following table:

Availability	Downtime
90% (1-nine)	36.5 days/year
99% (2-nines)	3.65 days/year
99.9% (3-nines)	8.76 hours/year
99.99% (4-nines)	52 minutes/year
99.999% (5-nines)	5 minutes/year
99.9999% (6-nines)	31 seconds/year

Mean Time to Repair (MTTR) is the time to recover from a component failure, a failed system upgrade, operator error, etc. The formula below illustrates how both MTBF and MTTR impact the overall availability of the system. As the MTBF goes up, availability goes up. As the MTTR goes up, availability goes down.

Inherent availability looks at availability from a design perspective:

$$Ai = \frac{MTBF}{(MTBF + MTTR)}$$

When an outage occurs, what's the probability that the redundant system will fail during the MTTR? If the MTTR is low (e.g. one hour), then the probability for redundant system failure during the outage is low. Repair and response times are key factors in achieving high availability for ESInets. It is a best practice to have a spares plan and SLAs on response time.

The procedure for software upgrades to the system must also be taken into account. If not properly designed, taking the system offline to upgrade the software may put the SLA in jeopardy. Another aspect of designing for 5-9s availability in an ESInet is the requirement that software upgrades can be installed without taking the system down, or require the system to be offline for a very short period of time.

Another consideration is that software upgrades sometimes fail. There must be a procedure to back out the change. So system repair procedures must include policies and procedures for software upgrades.

### **3.4.2 Achieving 5-9s Availability in 9-1-1 Networks**

Historically, telcos have strived to provide 5-9s availability on emergency 9-1-1 services (i.e. Selective Routers, DBMS, ALI, Dual Mated Tandems, etc) – which equates to 5 minutes downtime per year.

In order to achieve 5-9s availability using 2 fully independent systems, telcos implemented a strict set of technical and operational standards for their employees and central offices which include the following:

- Utilize NEBS Level 3 Compliant Equipment
- DC powered
- Redundant fans and power supplies
- Highly reliable components, tested at environmental extremes
- Installed in secure, environmentally controlled facilities
- Engineered to deal with a variety of common issues for failover and recovery
- Monitored by a NOC 24 x 7 x 365
- Spare parts available on site or within 1 hour
- Approval for use testing

### **3.4.3 Network Availability and System Reliability in Legacy PSAPs**

5-9s availability is a widely accepted standard for emergency 9-1-1. This objective is achieved for call completion within legacy 9-1-1 systems primarily thru the use of backup PSAPs and 10 digit numbers.

5-9s availability was rarely achieved at any individual PSAP largely due to limitations at the physical layer (i.e. a single entrance for facilities into each PSAP, CAMA trunks and ALI circuits in the same trench from CO to PSAP, etc).

The availability achieved by most legacy PSAPs for network is on the order of 2-9s. There are often outages caused by fiber/cable cuts, flood, power, etc. and the PSAP is offline for more than 8 hours. Availability varies by region, year, and service provider.

There are other mechanisms that can be used to achieve 5-9s (e.g. more redundancy). Calculating actual reliability is complex.

### 3.4.4 Defining Failure Metrics for an ESInet

One of the considerations that must be taken into account when designing and calculating an ESInet's availability and reliability is determining what constitutes a failure. A failure could be defined as one of the following:

- 1) The termination of the ability of the overall 9-1-1 system to perform its required function within a specific geographic region.
- 2) The termination of the ability of any individual PSAP to perform its required function but not the termination of the ability of the overall 9-1-1 system to perform within that specific geographic region.

For example, if all the circuits from the PSAP to an ESInet are all located in the same conduit, and there is a fiber cut, typically one of two things will happen:

1. NG9-1-1 Call handling system automatically routes calls to backup PSAP
2. Someone at the PSAP will take action on the management console which will reroute the 9-1-1 calls to a 10 digit number or back up PSAP.

The failure does not prevent 9-1-1 calls in that region from being completed. However the failure does prevent the calls from being delivered to the primary PSAP. Therefore, according to definition 1, this is not a failure, but according to definition 2, it is a failure.

9-1-1 entities should define what constitutes a failure within their system, and thereby determine how availability and reliability will be calculated.

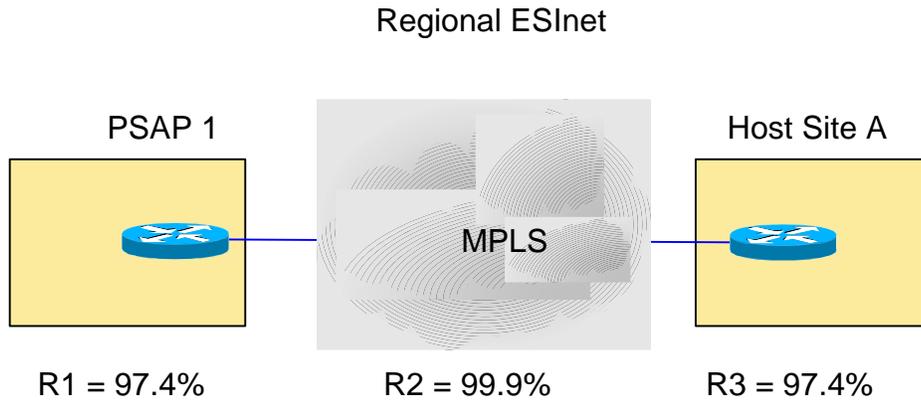
### 3.4.5 Series and Parallel Reliability and Availability in ESInets

Series and parallel reliability and availability are key components to the design of highly reliable ESInets. Series reliability is calculated as:

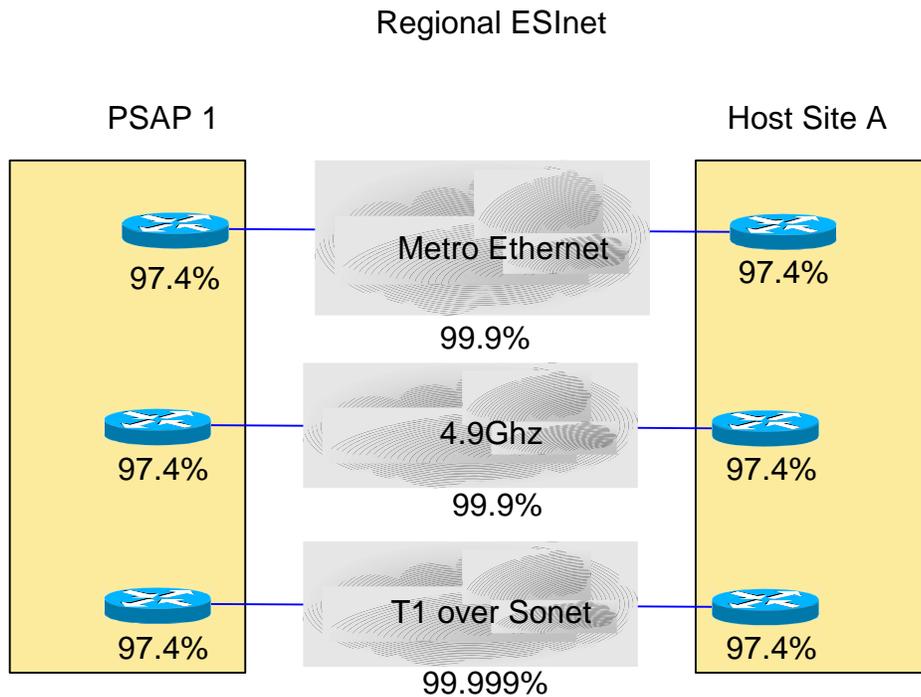
$$R_s = R_1 * R_2 * R_3$$

For example, the series reliability of the ESInet shown below is:

$$.9743 * .999 * .9743 = .948$$



An interesting property of series reliability is that it is always less than the least reliable component in the series. For example a 2-9s router connected to a 3-9s circuit yields an overall reliability of less than 2-9s. What would be the impact of adding 2 additional fully independent and physically diverse 94.8% links to the ESInet shown above?



Parallel reliability is calculated as:

$$R_p = 1 - ((1-R_{s1}) * (1-R_{s2}) * (1-R_{s3}))$$

Where  $R_p$  = Parallel Reliability

and  $R_{s1..3}$  = the series reliability of each independent link

So if the series reliability of each link is 94.8%, then the reliability for the 3 fully independent and physically diverse links in parallel is almost 4-9s.

$$R_p = 1 - ((1-.948) * (1-.948) * (1-.948)) = 1 - (0.052 * 0.052 * 0.052) = 0.99985$$

As shown below four fully independent and physically diverse links in parallel are required to achieve a reliability of 5-9s. (Note: In order to be fully independent and physically diverse, the links must not share any components in common (i.e. not in the same trench, not running thru the same Digital Cross Connect at the Central Office, routers not from the same vendor, etc.).)

$$\begin{aligned} R_p &= 1 - ((1-.948) * (1-.948) * (1-.948) * (1-.948)) \\ &= 1 - (0.052 * 0.052 * 0.052 * 0.052) \\ &= 0.9999927 \end{aligned}$$

In most cases higher overall reliability can be achieved by purchasing several physically diverse low cost links (i.e. Metro ethernet, T1 over Sonet, etc.) as opposed to a single high cost service. Surprisingly, series and parallel availability are calculated using the same formulas shown above for series and parallel reliability.

So assuming all of the necessary considerations have been taken into account (i.e. environmental considerations, operational and technical procedures are developed and adhered to, equipment is replaced as it reaches end of life, etc.) a PSAP connection to an ESInet that consists of 4 fully independent and physically diverse links that have a series reliability (taking routers into account) of at least 94.8% can expect to achieve 5-9s availability (5 minutes or less of downtime per yr) on that ESInet – every year.

### 3.5 Network Security

The NENA 75-001 Security for Next-Generation 9-1-1 Standard (NG-SEC) contains a number of sections which apply to ESInets including; Security Policies, Information Classification, Safeguarding Information Assets, Physical Security Guidelines, Network and Remote Access Security Guidelines, Change Control Documentation, Compliance Audits and Reviews. ESInets should be NG-SEC compliant.

The NENA 08-003 Detailed Functional and Interface Specification for the NENA i3 Solution – Stage 3 contains additional requirements for ESInets including encryption and authentication mechanisms. ESInets should comply with the 08-003 standard.

### **3.5.1 Session Border Controllers and Firewalls**

It is a best practice to utilize Session Border Controllers on ESInets to provide firewall-like security for call signaling and call media streams. In most cases it will be necessary to put a firewall in parallel with the SBC in order to be able to process all the different types of traffic. Logs and alerts from SBCs and firewalls should be continuously monitored to identify performance issues as well as successful and unsuccessful attacks.

SBCs and firewalls should be deployed to protect state-level i3 core services from attacks originating both from the access network and from the state-level ESInet. In order to contain virus outbreaks and/or intrusions, it is strongly recommended to deploy SBCs and firewalls at regional host sites. It is a best practice to deploy SBCs and firewalls at the individual PSAPs.

### **3.6 Network Management and Monitoring**

Critical circuits for E9-1-1 calls (i.e. PSAP trunks and ALI circuits) are monitored. Outages may be FCC reportable. By the same token ESInet(s), which provide transport for emergency 9-1-1 calls, should also be monitored. Although there are no reporting requirements in current regulation, discussion of such regulation is underway and 9-1-1 entities should be prepared to report ESInet outages to relevant authorities.

All data circuits and network components which comprise an ESInet should be monitored. All network components should provide SNMP traps to an approved management system. Vendors of all operational network components that form an ESInet should provide an SNMP MIB (management information base) for each component to organizations authorized to operate SNMP management systems. At least one SNMP based network monitoring system should be implemented by an organization with access to the resources necessary to perform effective network maintenance services.

Vendors of all non-network components such as NG9-1-1 application servers should also be encouraged to provide SNMP MIB's for their products. This would allow a network management system to monitor all of the network and applications components necessary for the reliable operation of NG9-1-1 on an ESInet. Companies that connect to the ESInet for the purpose of monitoring and/or management of devices should be NG-SEC compliant.

Effective network management requires:

- Proper/accurate documentation of the network
- Current network diagrams
- IP address range management/assignments

- Demarcation points
- Contact and Escalation lists – Vendor, Service Provider, NOC
- Near real time monitoring/alarming
- SLA benchmarks
- Capacity management / Trending Analysis
- Monitoring the state of element configuration (e.g.. QoS)
- Configuration Management / Change Control

Some of the methods above can be used to measure SLA metrics, but may not be reported to the end user.

The significance of the demarcation point is that it defines responsibility. When multiple service providers are involved (e.g. ECRF, ESRP, ESInet), it may be advantageous to have the service providers agree to forward SNMP traps and management alarms to a central network management system. Where appropriate, heartbeats can be used to verify the availability of network facilities.

Each participant within the ESInet should be responsible for ensuring that the appropriate tools and additional resources, including trained staff required to diagnose, test, and monitor traffic within their portion of the network are available and able to respond 24x7. Provisions should be made for capturing network traffic, generating alarms and producing other metrics for monitoring and troubleshooting outages on ESInets.

Monitoring packet data can be done in a variety of ways. This can be done both physically and virtually (through software using existing physical interconnections). The same access provisions may also be required for IDS and loggers. Provisions should be made for supporting access to the network or assuring the equipment is capable of supporting monitoring without degrading performance.

Active test equipment that can interrupt normal network activity should only be used on a case by case basis when needed to troubleshoot. Passive/monitoring test equipment should be treated differently than active (i.e. traffic generating) equipment. Active testing for FEs of NG9-1-1 beyond OSI layers 1-3 may help resolve outages.

During implementation and ongoing management of NG9-1-1, low-level packet analysis tools may be required for performance diagnostics and trouble resolution. These tools are equivalent replacement tools for the existing trunk monitoring techniques and tools that are used in legacy 9-1-1.

### **3.7 Performance Requirements**

There are a number of factors that affect the overall quality of multimedia traffic on an ESInet including packet loss, jitter, and latency. This section outlines some of the important properties of packet loss, jitter, and latency as pertaining to ESInets.

### 3.7.1 Packet Loss

Packets can be dropped by various devices in the network (e.g. routers, ATM and MPLS switches), or the packet may have been corrupted during transport and dropped at the destination. An overall (end to end) packet loss budget for maintaining intelligible voice transmission is about 5 %. Out of that 5% budget approximately ½ of the packet loss should be allocated for the ESInets with the remaining allocated for the origination network. It is a best practice to engineer ESInets to keep the packet loss budget under 2.5%. Audio media streams are the most sensitive to packet loss. ESInets should be designed without oversubscription. Packet loss of less than 1% should be achievable on such ESInets.

### 3.7.2 Jitter

A packet's delay varies with its position in the queues of the routers along the path between source and destination and this position can vary unpredictably. Arrival time of packets is ideally equal to the packetization period (i.e. sample rate times samples per packet). Because of the effects of queuing and because 2 sequential packets sent from the same source may not arrive via the same paths, variation in the actual arrival time of packets may occur. It is this variability in the delay that causes jitter. Jitter buffers are utilized to smooth out the variation. It is a best practice to design ESInets to maintain less than 20mS variation in the end point jitter buffers.

### 3.7.3 Latency

Latency is the amount of time it takes for a packet to reach its destination. The one-way transit delay (i.e. end to end, mouth to ear) for real-time media packets should not exceed 150mS. (ITU-T G.114).

When latency exceeds 150 mS, turn taking is significantly impaired. Because the access network is outside the scope of the ESInet, and considerable latency may be incurred, the maximum acceptable delay for packets traversing the ESInet should be less than or equal to 35 mS. It is a best practice to design ESInets to operate with less than 15 to 20 mS of latency. This allows the original encode and decode and a conference bridge in the middle of the path and still achieve the maximum 35mS or less packet delay.

## 3.8 Hardware/Network Elements

Some of the equipment required to build an ESInet (i.e. routers, firewalls, session border controller(s), etc.) can be leased, other components will have to be purchased. It is a best practice to purchase and/or lease equipment that meets the following criteria:

- Is highly reliable
- Has a proven track record
- Has a warranty

- Has an abundance of qualified/trained engineers that can support it.
- Vendor provides 24/7 support
- Acceptable MTTR
- Is scalable

### 3.9 Service Level Agreement

A service level agreement is a mutually agreed upon formal document provided to the 9-1-1 entity from the vendor that defines the service level commitment the vendor is offering. The fundamental commitment in an SLA is the contracted availability metric for described service or system. This is typically represented in terms of uptime (e.g. 99.9%, 99.99%, 99.999%). Uptime metrics are typically described as three nines, four nines, five nines, etc.

The SLA typically describes where and how the measurement is made, and how often they are calculated and reported. For example, an SLA might be measured over a one month period, a one year period, or both. It is a best practice for 9-1-1 entities to ensure that there is some provision within the SLA that will require the service provider(s) to notify the 9-1-1 entity in the event of service affecting outages.

Service impact levels are typically used to define the severity of the outage denoted by some range of values (e.g.1 through 5). Failure to meet agreed upon service impact levels may result in pre-negotiated financial penalties to the vendor/service provider.

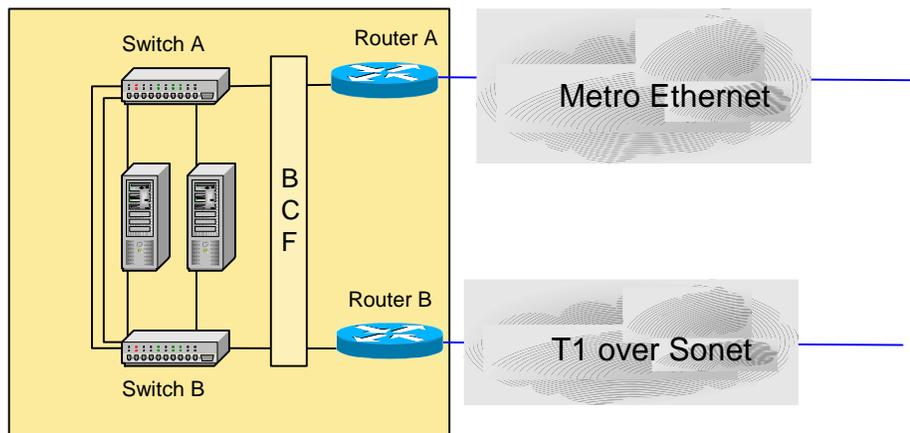
ESInets are complex and may involve management of SLAs from a number of different vendor/service providers. Best practices include:

- Where multiple service providers are involved, there should be a demarcation point that defines the boundaries of responsibilities as described in an agreement.
- Obtain or establish the MTTR for each piece of equipment used in an ESInet as well as an SLA for the network service. To maintain reliable service and ensure efficient testing, benchmarks should be established, documented, and periodically reviewed for accuracy.
- Contracted levels of service should be established to ensure adequate response times for repair.
- To minimize downtime critical hot spares should be identified, purchased, and maintained on site.
- Maintenance should include regularly scheduled audits of hardware revision levels and code compatibility (including firmware) with hardware revisions.
- Redundant systems should be regularly exercised by deliberate fail-over as part of routine maintenance.

- Escalation paths should be documented and known to the 9-1-1 entity so that responses to failures can be adequately addressed.

### 3.10 Local Area Network (LAN) Architecture

To some degree the ESInet requirements extend into the LAN within a PSAP. In many cases vendors of the IP enabled or NG9-1-1 call taking system will provide and configure the LAN switches. This is due in part to the large number of requirements that the IP enabled 9-1-1 call taking systems place on the LAN. It is a best practice to deploy at least 2 LAN switches at each site.



The workstations and/or servers shown above are typically equipped with dual Network Interface Cards (NICs). Each NIC is connected to a LAN switch. The switches are connected to each other and to the BCF (i.e. session border controller(s) and/or firewall(s)) that is attached to the ESInet router(s). It is a best practice to utilize managed switches in ESInets. Separate networks for different vendors are not recommended. In most cases the use of multiple VLANs can achieve sufficient isolation of network components in a shared infrastructure.

### 3.11 Traffic Engineering

ESInets should be designed to provide non-blocking service for high priority traffic. Bandwidth, Traffic Policing, Traffic Shaping and Quality of Service are some of the main design considerations which must be taken into account. This section describes some of the caveats to be avoided and best practices that should be observed with regard to traffic engineering in ESInets.

#### 3.11.1 Dimensioning ESInet Data Circuits

Traditionally, bandwidth sizing requirements for wide area networks are based on the bandwidth requirements of the applications being utilized on that network. One of the challenges of designing

ESInets today is that some of the applications that are expected to be implemented may be outside 9-1-1 and others are yet to be developed.

NENA 08-003, Section 4.8.1.2 requires support for video using the H.264 codec, baseline profile, levels 1-3. The maximum video bit rate for level 3 is 10Mbps. However, reasonable quality can be supported by less bandwidth given typical environments for emergency calls, which usually do not have rapid scene changes, and often have "talking heads." Further, while best practice for PSAP design would be to support all media at all positions, that does not necessarily imply that all positions must support the full level 3 bandwidth simultaneously. The bandwidth required is subject to some differences of opinion among practitioners. One possible formula is 2 Mbps per PSAP + 2 Mbps per call-center position equipped for video, but more (or less) bandwidth may be appropriate for a given ESInet. The actual bandwidth requirements for any individual installation should be properly designed by qualified network design engineers.

There is an expected update to the Americans with Disabilities Act due soon. Given the comments received, there is a possibility that the Department of Justice will require PSAPs to support video in NG9-1-1. However, no draft of new rules was available at the time this document was published. It is considered a best practice to always design and deploy ESInets that are scalable with regard to bandwidth allocation. This way, when bandwidth intensive applications are deployed, ESInets can be quickly scaled to meet these adjusted requirements. One concept that has been discussed and generally agreed to among the authors of this document is that the bandwidth requirements will expand over time, and will use up all available bandwidth capacity. Therefore, it is recommended that a fundamental best practice is to provision as much bandwidth capacity during the ESInet design phase as is reasonable for application use to cover a 2 year planning horizon, and that is economically feasible.

The circuits upon which Internet based emergency 9-1-1 calls will be delivered have some unique design considerations. The primary factor that drives the bandwidth requirement for these circuits is a Distributed Denial of Service Attack (DDOS). Per 08-003 these circuits must be terminated into a Border Control Function (BCF) which in this case would be a Session Border Controller (SBC). SBCs are programmed to recognize and thwart attacks, but the resources required to be able to receive an emergency 9-1-1 call via the Internet during a DDOS attack are significant. The ingress to the BCF should be designed to withstand the largest feasible attack. It is a best practice to engage qualified security professionals knowledgeable about current DDOS mitigation techniques to develop and implement strategies to protect ESInets against DDOS attacks.

### **3.11.2 Traffic Policing**

Some of the layer 2 technologies that can be utilized to provide transport for ESInets require that the traffic that is being sent into the network conform to a number of requirements including peak and sustainable cell/packet rate. Traffic that exceeds the rate purchased from the service provider may be discarded immediately, marked as non-compliant, delayed, or left as-is, depending on administrative policy and the characteristics of the excess traffic.

### 3.11.3 Traffic Shaping

Traffic shaping is commonly applied at the network edges to control traffic entering the network. Traffic shaping is frequently required when the port speeds exceed the amount of bandwidth purchased from the service provider. For example, assume a 10 Mbps Metro Ethernet service is purchased from a service provider. If the 100 Mbps Fast Ethernet port of a router is connected to that circuit, in many cases even though the data being transmitted over a period of 1 second is less than 10 Mega-bits, the router (transmitting at 100Mbps) will exceed the rates deemed acceptable by the service provider and packets will be dropped. When port speeds are not equal to the amount of bandwidth being purchased from the service provider, it is a best practice to configure traffic shaping on the routers to ensure that the traffic being transmitted is in compliance with the traffic contract.

### 3.11.4 Quality of Service (QoS)

Quality of service is the ability to give priority to different data flows. In ESInets QoS is implemented by configuring routers and other network elements to respect DiffServ Code Points (DSCPs) as defined in RFC 2475.

Per the Detailed Functional and Interface Standards for the NENA i3 Solution Version 1.0 (NENA 08-003)

- Functional Elements must mark packets they create with appropriate code points.
- The BCF must police code points for packets entering the ESInet.
- The following code points and Per Hop Behaviors (PHB) must be used on ESInets:

<b>DSCP</b>	<b>Use</b>	<b>PHB</b>
0	Routine Traffic	Default
1	9-1-1 Signaling	AF12
2	9-1-1 Text Media	AF12
3	9-1-1 Audio Media	EF
4	9-1-1 Video Media	AF11
5	9-1-1 Non human initiated Call	AF21
6	Intra ESInet Events	AF21
7	Intra ESInet Other 9-1-1 Traffic	AF22

See RFC 2475 for a detailed description of DSCP and PHB mechanisms and functionality.

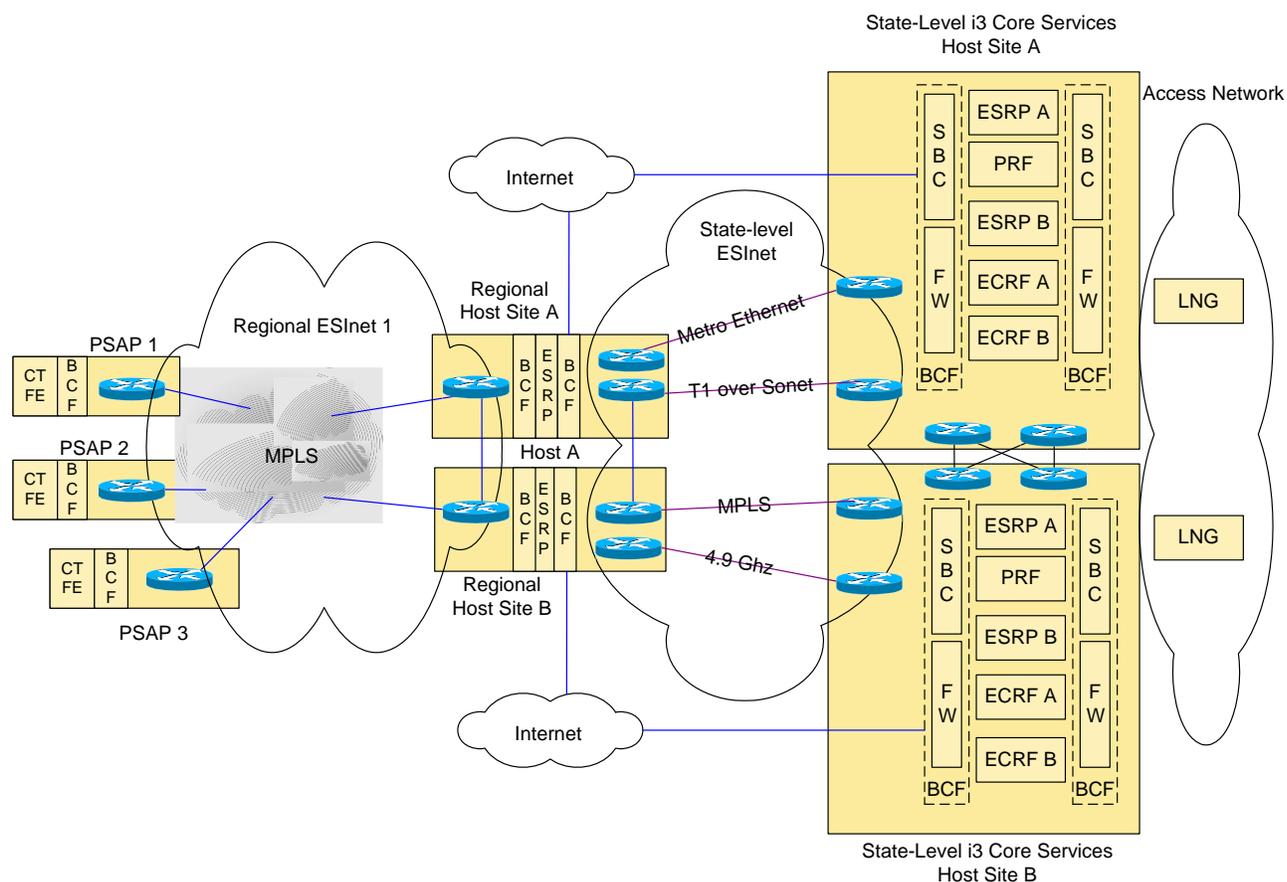
### 3.12 Network Architecture

This section covers some of the most commonly utilized ESInet architectures; some of their caveats, advantages, and disadvantages. Common objectives for ESInet architectures are to maximize availability and reliability within budgetary constraints. The diagram below shows a regional ESInet which is connected to state level i3 core services via a state-level ESInet. <sup>6</sup>

#### Regional ESInet I

---

<sup>6</sup> In an effort to simplify the diagrams the physical connections within the sites (i.e. router to switch, switch to server, etc) are not shown.

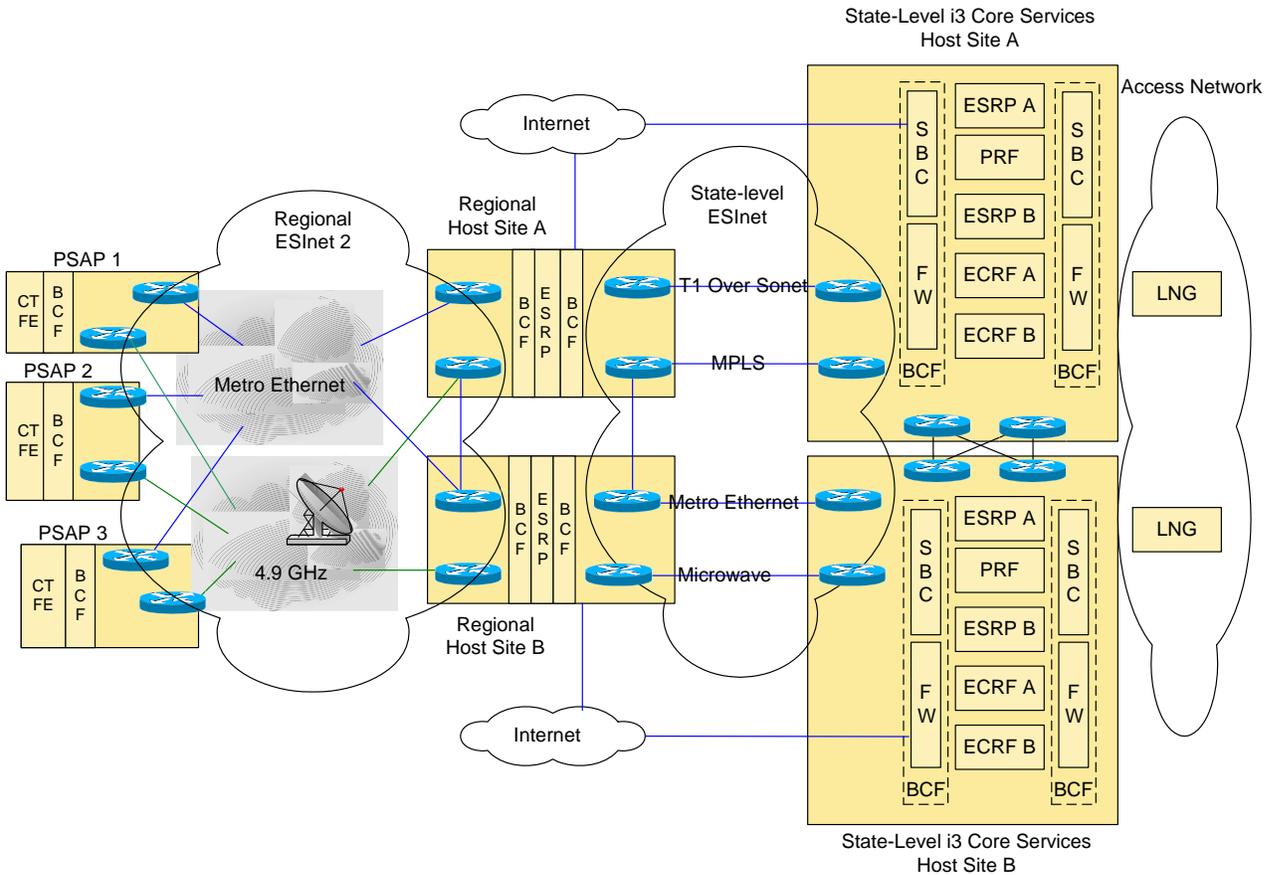


The state-level i3 core services are located at 2 geographically diverse sites – Host Site A and Host Site B. In order to assure high availability, redundant firewalls, Session Border Controllers (SBCs), ESRPs, and ECRFs are located at each of the state-level host sites. The i3 core services (e.g. ESRP, ECRF, and PRF) and the Legacy Network Gateways (LNGs) are outside the scope of the ESInet, but it was the consensus of the authors of this document that it would be advantageous to show how the i3 core services should be connected into an ESInet. It is a best practice to build state-level host sites and regional host sites in highly available data centers.

Regional ESInet 1 is comprised of an MPLS network. The PSAPs have a single entrance facility through which all circuits are delivered. A single router that provides connectivity into the regional ESInet is located in the backroom of each PSAP. Each PSAP has one or more call taker positions and a Border Control Function (BCF) which consists of a session border controller and a firewall. As discussed in section 3.4 reliability engineering calculations show the reliability and availability of Regional ESInet 1 to be on the order of 2-9s. PSAPs utilizing this solution must therefore rely on traditional methods (i.e. back-up PSAPs and 10 digit numbers) to achieve 5-9s availability for the overall 9-1-1 service in their region. The state-level ESInet, which transports call signaling message exchanges, call media streams which carry the call's audio, and data from the state-level i3 core

services to the regional host sites, is designed to achieve 5-9s availability. Connections to Internet border controllers from outside the ESInets are shown at both the regional hosts and state-level host sites. Among other things these connections could be utilized to support requirements to receive emergency 9-1-1 calls via the Internet and/or to support remote access requirements for monitoring and maintenance.

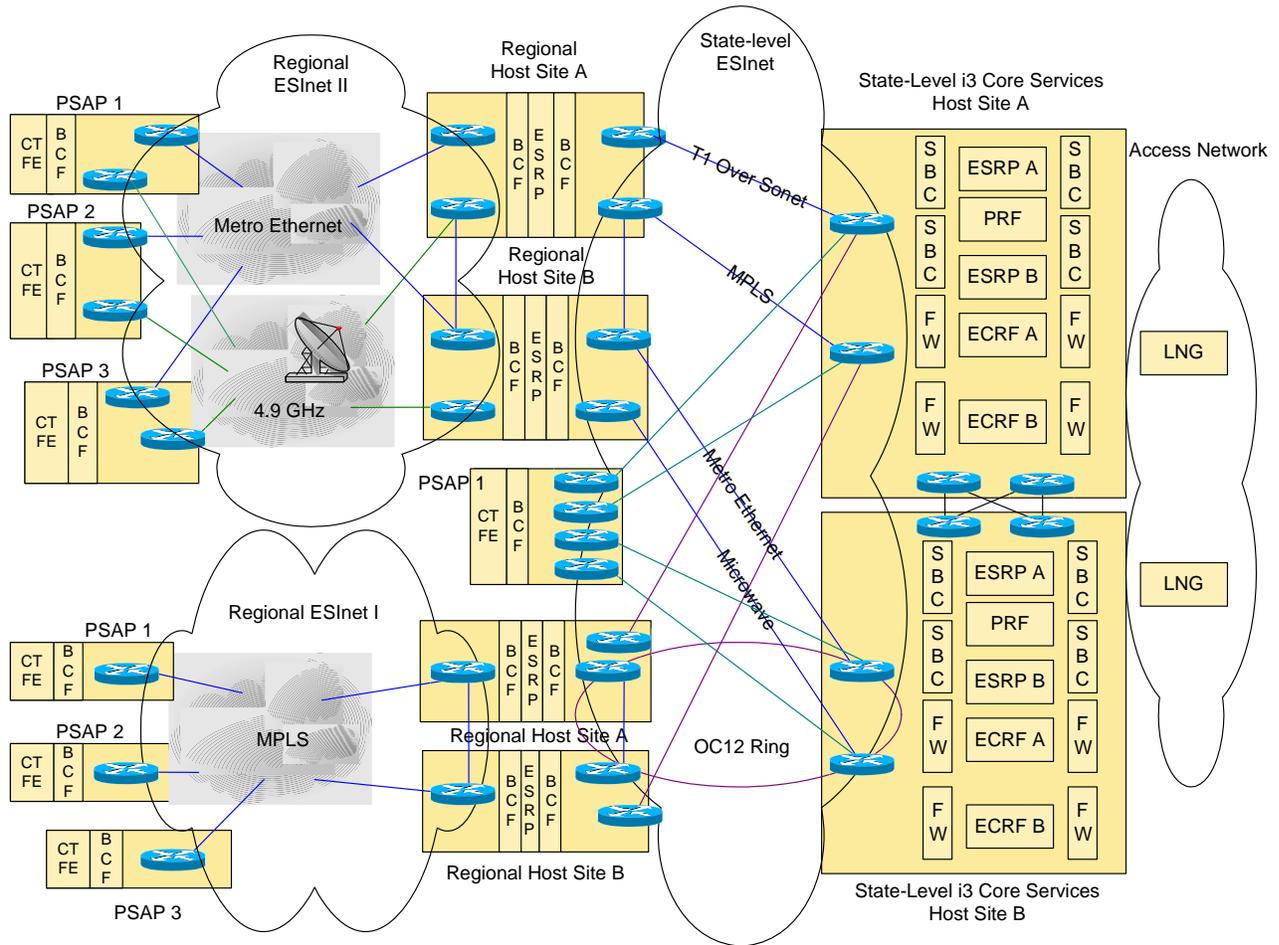
## Regional ESInet II



Regional ESInet II (above) is comprised of two physically diverse and independent networks; a Metro Ethernet and a 4.9 Ghz microwave network. Separate routers and entrance facilities are utilized for each of the layer 2 technologies. As described throughout this document there is a long list of other criteria which must be met, but assuming a typical PSAP environment, if properly designed and maintained, reliability engineering calculations show ESInet II to be capable of achieving 3-9s availability.

It is anticipated that many regional 9-1-1 entities and possibly individual PSAPs will connect into the state level i3 core services. The diagram below shows how the ESInets might be interconnected.<sup>7</sup> It is a best practice to design connections from regional host sites to state level i3 core services (i.e. state-level ESInets) to achieve 5-9s availability.

### Interconnecting Multiple ESInets



### 3.13 Conclusion

In this document many aspects underlying the design and construction of an ESInet supporting NG9-1-1 at OSI layers 1, 2, and 3 are addressed from both a technical and operational perspective. Given that resilient networks can be built using different approaches, a variety of network architecture options and methodologies for achieving recommended reliability and availability service levels are discussed throughout the document. In addition to the specific performance requirements that are

<sup>7</sup> Connections to the Internet are not shown.

included, operational requirements such as those that relate to service level agreements for operators of ESInets are discussed, as well as several aspects of network security. Further, since ESInets must deliver high priority traffic in the face of severe congestion, this document provides a variety of traffic engineering strategies for achieving these goals which are discussed alongside ESInet network management and monitoring.

After covering and reviewing the topics above and noting that a number of the topics covered in this document are fields of study to which people devote their entire careers, this working group has concluded that the information contained in this document by itself, although helpful and educational, does not provide all of the necessary details required to thoroughly design an ESInet supporting NG9-1-1. It is rather a best practice document, meant to stimulate discussion and provide background and overall guidance for qualified IP network design engineers tasked with designing ESInets supporting NG9-1-1.

#### **4 Recommended Reading and References**

- 1 Detailed Functional and Interface Specification for the NENA i3 Solution – Stage 3, National Emergency Number Association, [NENA 08-003](#)
- 2 NENA Master Glossary of 9-1-1 Terminology, National Emergency Number Association, [NENA 00-001](#)
- 3 NENA Security for Next-Generation 9-1-1 Standard (NG-SEC), National Emergency Number Association, [NENA 75-001](#)
- 4 Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, P. Ferguson, Internet Engineering Task Force, [RFC 2267](#)
- 5 Address Allocation for Private Internets, Internet Engineering Task Force, [RFC 1918](#)
- 6 IP Network Address Translator (NAT) Terminology and Considerations, Internet Engineering Task Force, [RFC 2663](#)

# NENA

## The 9-1-1 Association

1700 Diagonal Road | Suite 500 | Alexandria, VA 22314

### Understanding NENA's i3 Architectural Standard for NG9-1-1

Today, NENA takes a significant step toward achieving the vision of Next Generation 9-1-1 service. As we adopt Version 1.0 of NENA Technical Standard 08-003, *Detailed Functional and Interface Specification for the NENA i3 Solution – Stage 3*, we consider it important to explain how this standard relates to long-term efforts to modernize our nation's emergency communications systems.

This NENA standard intentionally describes an *end-state* NG9-1-1 architecture, rather than an immediate “build-to” specification for a complete NG9-1-1 system. Broadly speaking, 9-1-1 systems will reach the end-state envisioned by the i3 Standard only over the long term. In the interim, transitional steps must be taken to maintain support for legacy interfaces from originating service providers such as wireline and cellular telephone carriers, and to accommodate legacy PSAP equipment. At the same time, we recognize that state and local authorities will begin deploying ESInets and other core components of the i3 architecture as those components reach the market. Likewise, originating service providers and access network operators may begin deploying new network elements in support of longer-term NG9-1-1 services. The i3 architecture anticipates the existence of transitional states in origination services, access networks, and 9-1-1 systems and includes specifications for network elements that will be required to support a growing variety of “call” types as deployed systems evolve toward the end-state.

Critically, the i3 standard is not, by itself, the same thing as an NG9-1-1 system. The i3 standard describes *only* the network, components, and interfaces required to establish Next Generation 9-1-1 service. In order to deploy a fully-operational NG9-1-1 system, 9-1-1 authorities, equipment and software vendors, originating service providers, and access network providers will require detailed specifications for technical, operational, and human elements that are not described in the i3 standard. As the leading standards development organization for the 9-1-1 sector, NENA has already developed some of these specifications. Much work remains, however, and NENA is committed to developing the additional consensus standards needed to support fully-mature NG9-1-1 service systems.

It also will be necessary for NG9-1-1 systems to interwork with services and networks provided by the broader telecommunications and applications industries. NENA is aware of the evolution of the Internet Multimedia Subsystem (IMS) standard under development by ATIS, and our Technical Committee has designed the i3 architecture to support known characteristics of IMS. We are therefore pleased by the efforts of ATIS and others to develop detailed specifications for an interface between IMS-based originating services and the ESInets on which the i3 architecture operates. Version 1.0 of the i3 standard could not cover all aspects of the interface, however, because those efforts only recently began. Standards convergence in this area will be important to the success of NG9-1-1, and we look forward to more fully addressing the IMS/ESInet interface in concert with ATIS.

# NENA

## The 9-1-1 Association

1700 Diagonal Road | Suite 500 | Alexandria, VA 22314

In addition to technical and operational standards, a detailed policy framework must be created to enable and support the transition to NG9-1-1. Critical policy decisions such as how NG9-1-1 deployments will be funded and how system costs should be allocated are beyond the scope of the i3 technical standard. Those decisions must be made, however, and NENA will support policymakers at all levels of government as they wrestle with these issues.

We also wish to emphasize that the i3 standard is not intended to fully address the issues involved in transitioning from legacy 9-1-1 and E9-1-1 systems to end-state NG9-1-1. In 2006, NENA created a working group focused on transitional matters, such as network, data, and operational issues. That group has since completed work on Version 1.0 of a transition plan, covering mostly network issues. That group is now working on Version 2.0, covering data and operational issues. As the group continues its work, we expect that it will soon produce an integrated, consensus-based plan covering all essential elements of the transition to NG9-1-1 with sufficient specificity to allow 9-1-1 system administrators, vendors, access network operators, and originating service providers to confidently deploy capital in support of the transition.

Much work remains to be done, but our adoption of the i3 standard establishes a clear vision for the future and a foundation on which successful transitions to Next Generation 9-1-1 service can be built. As work continues, NENA stands ready to lead the cooperative efforts needed to ensure smooth transitions and to achieve the ultimate vision of NG9-1-1 as a service accessible anytime, anywhere, on any device.

*For the Executive Board,*



Stephen F. O'Connor, ENP  
*President*

# Detailed Functional and Interface Specification for the NENA i3 Solution – Stage 3



NENA Detailed Functional and Interface Standards for the NENA i3 Solution (TSD)

NENA 08-003 v1, June 14, 2011

Standards Advisory Board approval date, February 16, 2011

NENA Executive Board approval date, June 14, 2011

Prepared by:

National Emergency Number Association (NENA) Technical Committee Chairs

Published by NENA

Printed in USA



## NENA TECHNICAL STANDARD DOCUMENT

### NOTICE

The National Emergency Number Association (**NENA**) publishes this document as a guide for the designers and manufacturers of systems to utilize for the purpose of processing emergency calls. It is not intended to provide complete design specifications or to assure the quality of performance of such equipment.

NENA reserves the right to revise this TSD 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
- or to reflect changes in the design of equipment or services described herein.

It is possible that certain advances in technology will precede these revisions. Therefore, this NENA TSD should not be the only source of information used. **NENA** recommends that readers contact their Telecommunications Carrier representative to ensure compatibility with the 9-1-1 network.

Patents may cover the specifications, techniques, or network interface/system characteristics disclosed herein. No license expressed or implied is hereby granted. 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.

This document has been prepared solely for the use of E9-1-1 Service System Providers, network interface and system vendors, participating telephone companies, etc.

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 Technical Committee has developed this document. Recommendations for change to this document may be submitted to:

National Emergency Number Association

4350 N Fairfax Dr, Suite 750

Arlington, VA 22203-1695

800-332-3911

or: [techdoccomments@nena.org](mailto:techdoccomments@nena.org)

**Acknowledgments:**

The National Emergency Number Association (NENA) VoIP/Packet Technical Committee Long Term Definition Working Group developed this document.

NENA recognizes the following industry experts and their companies for their contributions in development of this document.

**Version 1, Approval Date, 06/14/2011**

<b>Members</b>	<b>Company</b>
Brian Rosen –Work Group Leader and Technical Editor	NeuStar
Nate Wilcox – VoIP/Packet Technical Chair	microDATA
Richard Atkins	Tarrant County 9-1-1 District
Delaine Arnold	Arnold 9-1-1 Consulting
Wayne Ballantyne	Motorola
Deborah Barclay	Alcatel Lucent
Marc Berryman	DDTI
Tom Breen	AT&T
Gary Brown	NENA Utah Chapter Member
Pete Eggimann	Metropolitan Emergency Services Board
Randall Gellens	Qualcomm
Casimer M (Duke) Kaczmarczyk	Verizon
Marc Linsner	Cisco
Roger Marshall	TeleCommunication Systems, (TCS)
Kathy McMahon-Ruscitto	APCO International
Theresa Reese	Telcordia
Greg Schumacher	Sprint
Robert Sherry	Intrado
Michael Smith	DSS
Hannes Tschofenig	Nokia Siemens Networks
Mike Vislocky	Network Orange

This committee would also thank Tom Breen, Technical Committee Chair and Roger Hixson, Technical Issues Director for their support and assistance.



## TABLE OF CONTENTS

<b>1 EXECUTIVE OVERVIEW .....</b>	<b>14</b>
<b>2 INTRODUCTION .....</b>	<b>17</b>
2.1 OPERATIONAL IMPACTS SUMMARY .....	17
2.2 SECURITY IMPACTS SUMMARY .....	17
2.3 DOCUMENT TERMINOLOGY .....	17
2.4 REASON FOR ISSUE/REISSUE.....	18
2.5 RECOMMENDATION FOR ADDITIONAL DEVELOPMENT WORK .....	18
2.6 DATE COMPLIANCE .....	20
2.7 ANTICIPATED TIMELINE .....	21
2.8 COSTS FACTORS .....	21
2.9 FUTURE PATH PLAN CRITERIA FOR TECHNICAL EVOLUTION.....	21
2.10 COST RECOVERY CONSIDERATIONS .....	22
2.11 ADDITIONAL IMPACTS (NON COST RELATED).....	22
2.12 INTELLECTUAL PROPERTY RIGHTS POLICY .....	22
2.13 ACRONYMS/ABBREVIATIONS/DEFINITIONS .....	23
<b>3 GENERAL CONCEPTS.....</b>	<b>38</b>
3.1 IDENTIFIERS.....	38
3.1.1 Agency Identifier.....	38
3.1.2 Agent Identifier .....	38
3.1.3 Element Identifier.....	38
3.1.4 Call Identifier.....	38
3.1.5 Incident Tracking Identifier .....	38
3.2 TIMESTAMP .....	39
3.3 EVENTS COMMON TO MULTIPLE FUNCTIONAL ELEMENTS .....	39
3.3.1 Security Posture .....	39
3.3.2 Element State.....	40
3.3.3 Service State.....	42
3.4 LOCATION REPRESENTATION.....	43
3.5 vCARDS.....	44
3.6 EMERGENCY SERVICES IP NETWORKS .....	44
<b>4 INTERFACES.....</b>	<b>45</b>
4.1 SIP CALL.....	45
4.1.1 Minimal Methods needed to handle a call .....	46
4.1.1.1 INVITE (initial call).....	46

4.1.1.2	REFER (transfer)	49
4.1.1.3	BYE (call termination)	49
4.1.2	<i>Methods allowed to be initiated by caller which must be supported by i3 elements</i>	49
4.1.2.1	CANCEL (cancel call initiation)	49
4.1.2.2	UPDATE (update parameters)	50
4.1.2.3	OPTIONS (option negotiation)	50
4.1.2.4	ACK (acknowledgement)	50
4.1.2.5	PRACK (reliable message acknowledgement)	50
4.1.2.6	MESSAGE (text message)	50
4.1.2.7	INFO	51
4.1.3	<i>Methods used within the ESInet</i>	51
4.1.3.1	REGISTER (Call Taker to PSAP “login”)	51
4.1.3.2	SUBSCRIBE/NOTIFY (Events)	51
4.1.3.3	PUBLISH (update of presence information to presence server)	51
4.1.4	<i>Headers assumed supported at the interface to the ESInet</i>	51
4.1.5	<i>Headers Accepted and also used internally</i>	53
4.1.6	<i>Resource Priority</i>	54
4.1.7	<i>History-Info and Reason</i>	55
4.1.8	<i>Media</i>	55
4.1.8.1	Audio	55
4.1.8.2	Video	55
4.1.8.3	Real-Time Text	55
4.1.8.4	TTY (Baudot tones)	55
4.1.9	<i>Instant Messaging</i>	56
4.1.10	<i>Non-human-initiated calls</i>	57
4.1.11	<i>Bodies in messages</i>	58
4.1.12	<i>Transport</i>	58
4.1.13	<i>Routing</i>	59
4.1.14	<i>Originating network Interface</i>	59
4.1.15	<i>PSAP Interface</i>	59
4.1.16	<i>Element Overload</i>	60
4.2	LOCATION	60
4.3	PROVISIONING	61
4.4	POLICY	62
4.4.1	<i>Policy Store Web Service</i>	62
4.4.2	<i>Policy Syntax</i>	69



4.4.2.1	Condition Elements.....	69
4.4.2.2	Actions.....	72
4.4.2.3	LoSTServiceURN Action.....	72
4.4.2.4	Examples.....	72
4.4.2.5	Namespace.....	74
4.5	LoST.....	74
4.5.1	<i>Emergency Call Routing using LoST</i> .....	75
4.5.1.1	LoST Call Routing Messages.....	75
4.5.1.2	Call Routing Scenarios.....	93
4.5.2	<i>Location Validation</i> .....	95
4.6	EVENT NOTIFICATION.....	95
4.7	SPATIAL INFORMATION FUNCTION LAYER REPLICATION.....	96
4.7.1	<i>Web Feature Service</i> .....	96
4.7.2	<i>Atom Protocol and GeoRSS</i> .....	96
4.8	CAD.....	96
4.9	DISCREPANCY REPORTING.....	97
4.9.1	<i>DiscrepancyReport</i> .....	98
4.9.2	<i>StatusUpdate</i> .....	100
4.9.3	<i>DiscrepancyResolution</i> .....	101
4.9.4	<i>LVF Discrepancy Report</i> .....	102
4.9.5	<i>Policy Discrepancy Report</i> .....	103
4.9.6	<i>LoST Discrepancy Report</i> .....	103
4.9.7	<i>ECRF Discrepancy Report</i> .....	104
4.9.8	<i>BCF Discrepancy Report</i> .....	104
4.9.9	<i>Log Discrepancy Report</i> .....	104
4.9.10	<i>PSAP Call Taker Discrepancy Report</i> .....	104
4.9.11	<i>Permissions Discrepancy Report</i> .....	104
4.9.12	<i>GIS Discrepancy Report</i> .....	104
<b>5</b>	<b>FUNCTIONS.....</b>	<b>104</b>
5.1	BORDER CONTROL FUNCTION (BCF).....	104
5.1.1	<i>Functional Description</i> .....	104
5.1.2	<i>Interface Description</i> .....	108
5.1.2.1	CallSuspicion.....	109
5.1.3	<i>Roles and Responsibilities</i> .....	109
5.1.4	<i>Operational Considerations</i> .....	109
5.2	EMERGENCY SERVICE ROUTING PROXY (ESRP).....	109



5.2.1	<i>Functional Description</i> .....	109
5.2.1.1	Overview .....	109
5.2.1.2	Call Queuing .....	110
5.2.1.3	QueueState Event Package .....	111
5.2.1.4	DequeueRegistration Event Package .....	113
5.2.1.5	Policy Routing Function .....	114
5.2.1.6	ESRPnotify Event Package .....	116
5.2.1.7	Processing of an INVITE transaction .....	118
5.2.1.8	Processing a BYE Transaction .....	119
5.2.1.9	Processing a CANCEL transaction .....	119
5.2.1.10	Processing an OPTIONS transaction .....	119
5.2.2	<i>Interface Description</i> .....	119
5.2.2.1	Upstream Call Interface .....	119
5.2.2.2	Downstream Call Interface .....	120
5.2.2.3	ECRF interface .....	120
5.2.2.4	LIS Dereference Interface .....	121
5.2.2.5	Additional Data Interfaces .....	121
5.2.2.6	ESRP, PSAP and Call Taker State Notification and Subscriptions .....	121
5.2.2.7	Time Interface .....	122
5.2.2.8	Logging Interface .....	122
5.2.3	<i>Data Structures</i> .....	122
5.2.4	<i>Policy Elements</i> .....	122
5.2.5	<i>Provisioning</i> .....	123
5.2.6	<i>Roles and Responsibilities</i> .....	123
5.2.7	<i>Operational Considerations</i> .....	123
5.3	EMERGENCY CALL ROUTING FUNCTION (ECRF) .....	123
5.3.1	<i>Functional Description</i> .....	124
5.3.2	<i>Interface Description</i> .....	124
5.3.2.1	Routing Query Interface .....	124
5.3.2.2	Data Source Interface .....	129
5.3.2.3	Time Interface .....	129
5.3.3	<i>Data Structures</i> .....	129
5.3.3.1	Data to Support Routing Based on Civic Location Information .....	129
5.3.3.2	Service Boundaries .....	132
5.3.3.3	Routing Data – URI Format .....	133
5.3.3.4	Other Data .....	133
5.3.4	<i>Recursive and Iterative Query Resolution</i> .....	134



5.3.5 *Coalescing Data and Gap/Overlap Processing* ..... 135

5.3.6 *Replicas*..... 136

5.3.7 *Provisioning*..... 137

5.3.8 *Roles and Responsibilities*..... 137

5.3.9 *Operational Considerations*..... 137

5.4 LOCATION VALIDATION FUNCTION ..... 138

5.4.1 *Functional Description* ..... 139

5.4.2 *Interface Description* ..... 139

5.4.2.1 *User Endpoint interaction* ..... 139

5.4.2.2 *LIS Interaction* ..... 140

5.4.2.3 *Provisioning Interaction*..... 140

5.4.3 *Interface Description* ..... 140

5.4.3.1 *Validation query interface:*..... 140

5.4.3.2 *Validation response interface*..... 141

5.4.3.3 *LVF Provisioning/synchronization* ..... 142

5.4.3.4 *Alternative Address Interface*..... 142

5.4.3.5 *Time Interface*..... 142

5.4.3.6 *Logging Interface*..... 143

5.4.4 *Data Structures* ..... 144

5.4.5 *Roles and Responsibilities*..... 144

5.4.6 *Operational Considerations*..... 145

5.5 SPATIAL INFORMATION FUNCTION ..... 146

5.5.1 *Layers*..... 146

5.5.2 *MSAG Conversion Service (MCS)* ..... 147

5.5.3 *Geocode Service (GCS)*..... 149

5.5.4 *Operational Considerations*..... 150

5.6 PSAP..... 151

5.6.1 *SIP Call interface*..... 151

5.6.2 *LoST interface* ..... 151

5.6.3 *LIS Interfaces*..... 151

5.6.4 *Bridge Interface* ..... 152

5.6.5 *ElementState*..... 152

5.6.6 *SIF*..... 152

5.6.7 *Logging Service*..... 152

5.6.8 *Security Posture* ..... 153

5.6.9 *Policy* ..... 153



5.6.10 *Additional Data dereference* ..... 153

5.6.11 *Time Interface* ..... 153

5.6.12 *Test Call* ..... 153

5.6.13 *Call Diversion* ..... 153

5.6.14 *Incidents* ..... 154

5.7 BRIDGING ..... 154

5.7.1 *Bridge Call Flow* ..... 154

5.7.1.1 *Creation of a Conference Using SIP Ad-Hoc Methods* ..... 155

5.7.1.2 *Primary PSAP Asks Bridge to Invite the Caller to the Conference* ..... 156

5.7.1.3 *Secondary PSAP is Invited to the Conference* ..... 157

5.7.1.4 *Primary PSAP Drops Out of Conference; Secondary PSAP Completes Transfer* ..... 160

5.7.2 *Passing data to Agencies via bridging* ..... 161

5.8 TRANSFER INVOLVING CALLING DEVICES THAT DO NOT SUPPORT REPLACES ..... 161

5.8.1 *B2BUA in the Border Control Function* ..... 162

5.8.2 *Bridging at the PSAP Using Third Party Call Control in the Call Taker User Agent* ..... 166

5.8.2.1 *Call Taker Creates a Conference* ..... 167

5.8.2.2 *Call Taker Asks the Bridge to Invite the Transfer Target to the Conference* ..... 169

5.8.2.3 *Primary PSAP Drops; Transfer Target Completes Transfer* ..... 171

5.8.2.4 *Transfer Target Terminates Session with Caller* ..... 173

5.8.3 *Answer all calls at a bridge* ..... 174

5.8.3.1 *Call Established Between Caller and Primary PSAP Via Bridge; Primary PSAP Asks Bridge to Invite the Secondary PSAP to the Conference* ..... 174

5.8.3.2 *Bridge Invites the Secondary PSAP to the Conference* ..... 176

5.8.3.3 *Secondary PSAP Terminates the Call* ..... 177

5.8.4 *Recommendations* ..... 178

5.9 LOCATION INFORMATION SERVER (LIS) ..... 178

5.10 CALL INFORMATION DATABASE (CIDB) ..... 179

5.11 INTERACTIVE MEDIA RESPONSE SYSTEM (IMR) ..... 180

5.12 LOGGING SERVICE ..... 180

5.12.1 *Interfaces* ..... 180

5.12.1.1 *LogEvent* ..... 181

5.12.1.2 *RetrieveLogEvent* ..... 183

5.12.1.3 *ListEventsByCallId* ..... 183

5.12.1.4 *ListEventsByIncidentId* ..... 183

5.12.1.5 *ListCallsbyIncidentId* ..... 184

5.12.1.6 *List IncidentsByDateRange* ..... 184

5.12.1.7 *ListIncidentsByLocation* ..... 184



5.12.1.8	ListIncidentsByDateAndLocation .....	184
5.12.1.9	ListCallsByDateRange .....	185
5.12.1.10	ListAgenciesByCallId .....	185
5.12.1.11	ListAgenciesByIncidentId.....	185
5.12.2	<i>Instant Recall Recorder</i> .....	185
5.12.3	<i>Roles and Responsibilities</i> .....	186
5.12.4	<i>Operational Considerations</i> .....	186
5.13	FOREST GUIDE.....	186
5.13.1	<i>Functional Description</i> .....	186
5.13.2	<i>Interface Description</i> .....	187
5.13.3	<i>Data Structures</i> .....	187
5.13.4	<i>Roles and Responsibilities</i> .....	187
5.13.5	<i>Operational Considerations</i> .....	187
5.14	DNS .....	187
5.15	AGENCY LOCATOR .....	188
5.16	POLICY STORE .....	188
5.16.1	<i>Functional Description</i> .....	188
5.16.2	<i>Interface Description</i> .....	188
5.16.3	<i>Roles and Responsibilities</i> .....	188
5.17	TIME SERVER.....	188
5.18	ORIGINATION NETWORKS AND DEVICES .....	188
5.18.1	<i>SIP Call Interface</i> .....	188
5.18.2	<i>Location by Reference</i> .....	189
5.18.3	<i>Call Information Database</i> .....	189
<b>6</b>	<b>SECURITY</b> .....	<b>189</b>
6.1	IDENTITY .....	189
6.2	PSAP CREDENTIALING AGENCY .....	189
6.3	ROLES.....	190
6.4	AUTHENTICATION.....	191
6.4.1	<i>Trusting Asserting and relying parties</i> .....	192
6.5	AUTHORIZATION.....	193
6.6	INTEGRITY PROTECTION .....	193
6.7	PRIVACY .....	193
<b>7</b>	<b>GATEWAYS</b> .....	<b>193</b>
7.1	LEGACY NETWORK GATEWAY (LNG).....	194



7.1.1	<i>Protocol Interworking Function (PIF)</i> .....	196
7.1.1.1	MF Trunk Interface .....	196
7.1.1.2	SS7 Interface .....	197
7.1.1.3	Internal Interface to the NIF Component .....	199
7.1.2	<i>NG9-1-1 specific Interwork Function (NIF)</i> .....	201
7.1.2.1	1.1.2.1 NIF Handling of INVITE from PIF.....	201
7.1.2.2	NIF Handling of Location Information from the LIF.....	202
7.1.2.3	SIP Interface to the ESInet.....	202
7.1.3	<i>Location Interwork Function (LIF)</i> .....	204
7.2	<b>LEGACY PSAP GATEWAY</b> .....	206
7.2.1	<i>Protocol Interworking Function (PIF)</i> .....	207
7.2.1.1	Traditional MF Interface .....	208
7.2.1.2	Enhanced MF (E-MF) Interface .....	211
7.2.2	<i>NG9-1-1 Specific Interwork Function (NIF)</i> .....	213
7.2.2.1	Handling of Emergency Calls with Non-NANP Callback Information.....	214
7.2.2.2	Special Handling Indication .....	214
7.2.2.3	Internal Interface to the PIF Component .....	215
7.2.2.4	Support for Emergency Call Transfer .....	219
7.2.2.5	Alternate Routing Invocation and Notification .....	224
7.2.3	<i>Location Interwork Function (LIF)</i> .....	225
<b>8</b>	<b>DATA ASSOCIATED WITH CALL/CALLER/LOCATION/PSAP</b> .....	<b>225</b>
8.1	ADDITIONAL DATA ASSOCIATED WITH A CALL (NENA 71-001) .....	226
8.2	ADDITIONAL DATA ASSOCIATED WITH A LOCATION (NENA 71-001) .....	226
8.3	ADDITIONAL DATA ASSOCIATED WITH A CALLER (NENA 71-001) .....	227
8.4	ADDITIONAL DATA ASSOCIATED WITH A PSAP (NENA 71-001) .....	227
<b>9</b>	<b>3RD PARTY ORIGINATION</b> .....	<b>227</b>
9.1	3 <sup>RD</sup> PARTY CLIENT IS REFERRED TO PSAP; PSAP ESTABLISHES CONFERENCE .....	228
9.2	3 <sup>RD</sup> PARTY CALL AGENT AND CALLER ADDED TO CONFERENCE .....	232
<b>10</b>	<b>PSAP MANAGEMENT</b> .....	<b>235</b>
<b>11</b>	<b>TEST CALLS</b> .....	<b>235</b>
<b>12</b>	<b>NRS CONSIDERATION</b> .....	<b>236</b>
12.1	URN REGISTRY.....	236
12.1.1	<i>Name</i> .....	236
12.1.2	<i>Information required to create a new value</i> .....	236
12.1.3	<i>Management Policy</i> .....	237
12.1.4	<i>Content</i> .....	237

---

12.1.5	Initial Values .....	237
12.2	“SERVICE” URN SUBREGISTRY .....	237
12.2.1	Name .....	237
12.2.2	Information required to create a new value.....	237
12.2.3	Management Policy.....	238
12.2.4	Content.....	238
12.2.5	Initial Values .....	238
12.3	URN:NENA:SERVICE:SOS .....	238
12.3.1	Name .....	238
12.3.2	Information required to create a new value.....	238
12.3.3	Management Policy.....	239
12.3.4	Content.....	239
12.3.5	Initial Values .....	239
12.4	URN:NENA:SERVICE:RESPONDER.....	239
12.4.1	Name .....	239
12.4.2	Information required to create a new value.....	240
12.4.3	Management Policy.....	240
12.4.4	Content.....	240
12.4.5	Initial Values .....	240
12.5	ELEMENTSTATE REGISTRY .....	240
12.5.1	Name .....	240
12.5.2	Information required to create a new value.....	240
12.5.3	Management Policy.....	241
12.5.4	Content.....	241
12.5.5	Initial Values .....	241
12.6	SERVICESTATE REGISTRY .....	241
12.6.1	Name .....	241
12.6.2	Information required to create a new value.....	241
12.6.3	Management Policy.....	241
12.6.4	Content.....	241
12.6.5	Initial Values .....	241
12.7	SECURITYPOSTURE .....	241
12.7.1	Name .....	242
12.7.2	Information required to create a new value.....	242
12.7.3	Management Policy.....	242

12.7.4	<i>Content</i> .....	242
12.7.5	<i>Initial Values</i> .....	242
12.8	EXTERNALEVENTCODES REGISTRY .....	242
12.8.1	<i>Name</i> .....	242
12.8.2	<i>Information required to create a new value</i> .....	242
12.8.3	<i>Management Policy</i> .....	242
12.8.4	<i>Content</i> .....	243
12.8.5	<i>Initial Values</i> .....	243
12.9	ESRPNOTIFYEVENTCODES REGISTRY .....	243
12.9.1	<i>Name</i> .....	243
12.9.2	<i>Information required to create a new value</i> .....	243
12.9.3	<i>Management Policy</i> .....	243
12.9.4	<i>Content</i> .....	243
12.9.5	<i>Initial Values</i> .....	244
12.10	ROUTECAUSE REGISTRY .....	244
12.10.1	<i>Name</i> .....	244
12.10.2	<i>Information required to create a new value</i> .....	244
12.10.3	<i>Management Policy</i> .....	244
12.10.4	<i>Content</i> .....	244
12.10.5	<i>Initial Values</i> .....	245
12.11	LOGEVENT .....	245
12.11.1	<i>Name</i> .....	245
12.11.2	<i>Information required to create a new value</i> .....	245
12.11.3	<i>Management Policy</i> .....	245
12.11.4	<i>Content</i> .....	245
12.11.5	<i>Initial Values</i> .....	245
12.12	AGENCYROLES.....	245
12.12.1	<i>Name</i> .....	245
12.12.2	<i>Information required to create a new value</i> .....	245
12.12.3	<i>Management Policy</i> .....	246
12.12.4	<i>Content</i> .....	246
12.12.5	<i>Initial Values</i> .....	246
12.13	AGENTROLES .....	246
12.13.1	<i>Name</i> .....	246
12.13.2	<i>Information required to create a new value</i> .....	246



12.13.3 *Management Policy*..... 246  
12.13.4 *Content*..... 246  
12.13.5 *Initial Values*..... 246  
**13 REFERENCES**..... **247**  
**APPENDIX A – MAPPING OF PIDF-LO TO LEGACY PSAP ALI** ..... **256**  
**APPENDIX B – GIS LAYER DEFINITIONS**..... **265**

**LIST OF TABLES**

Table 4-1 – LoST <findService> Message Attributes and Elements..... 76  
Table 4-3 – LoST <location> Element Attributes and Elements..... 79  
Table 4-5 PIDF <civicAddress> Element Attributes and Elements ..... 82  
Table 4-7 – LoST <findServiceResponse> Message Attributes and Elements ..... 84  
Table 4-9 LoST <mapping> Element Attributes and Elements..... 85  
Table 4-11 – LoST <errors> Message Attributes and Elements..... 87  
Table 4-12 – LoST "Error Type" Element Attributes ..... 89  
Table 4-13 – LoST <redirect> Message Attributes and Elements..... 90  
Table 4-14 – LoST Protocol Message Elements and xmlns Attribute Common Namespaces ..... 91  
Table 4-16 - GML and geoShape Elements and srsName Attribute Common URNs..... 92  
Table 5-1 LVF Specific Location Data Elements..... 144

**1 Executive Overview**

This specification builds upon prior NENA publications including i3 requirements [1] and architecture [101] documents. Familiarity with the concepts, terminology and functional elements described in these documents is a prerequisite. While the requirements and architecture documents describe high level concepts, the present document describes only the detailed functional and external interfaces to those functional elements. If there are discrepancies between the requirements or architecture documents and this document, this document takes precedence. This document provides a baseline to other NG9-1-1 related specifications.

The i3 solution supports end-to-end IP connectivity; gateways are used to accommodate legacy wireline and wireless origination networks that are non-IP. NENA i3 introduces the concept of an Emergency Services IP network (ESInet), which is designed as an IP-based inter-network (network of networks) that can be shared by all public safety agencies that may be involved in any emergency. The i3 Public Safety Answering Point (PSAP) is capable of receiving IP-based signaling and media for delivery of emergency calls conformant to the i3 standard.

Getting to the i3 solution from where we are today means that we will have to go through a transition from existing legacy originating network and 9-1-1 PSAP interconnections to next



generation interconnections. This document describes how NG9-1-1 works after transition, including ongoing interworking requirements for IP-based and TDM-based PSAPs and origination networks<sup>1</sup>. It does not provide solutions for how PSAPs, origination networks, selective routers and ALI systems evolve. Rather, it describes the end point where conversion is complete. At that point, selective routers and existing ALI systems are decommissioned and all 9-1-1 calls are routed by the ECRF and arrive at the ESInet via SIP. The NENA NG9-1-1 Transition Planning Committee (NGTPC) will produce documents covering transition options and procedures.

This document supports IP-based and legacy TDM-based PSAPs.

TDM-based PSAPs are connected to the ESInet via a gateway (the Legacy PSAP Gateway). The definition of the Legacy PSAP Gateway is broad enough that both primary and secondary PSAPs that have not been upgraded may be served by this type of gateway.

Similarly, the scope includes gateways for legacy wireline and wireless origination networks (the Legacy Network Gateway) used by origination networks who cannot yet create call signaling matching the interfaces described in this document for the ESInet. It is not envisioned that legacy origination networks will evolve to IP interconnect in all cases, and thus the Legacy Network Gateways will be needed for a very long time. The document considers all wireline, wireless, and other types of networks with IP interfaces, including IMS [64] networks, although the document only describes the external interfaces to the ESInet, which a conforming network must support. This document describes a common interface to the ESInet, to be used by all types of origination networks or devices. How origination networks, or devices within them, conform is not visible to the ESInet and is out of scope. NENA has endeavored to define this interface to be sufficiently aligned with the major types of originating networks, as defined by the prevalent SDOs (such as 3GPP, 3GPP2, IETF), that they are able to conform without significant modification to their architectures. However, it is recognized that IMS design has evolved in parallel with development of this document, and that further SDO convergence work will be required to align the details between i3 and related origination network 9-1-1 interfaces. The results of this convergence work will be documented in a future edition of this document. Further, regulatory policies will affect how this standard will evolve.

This specification defines a number of Functional Elements (FEs), with their external interfaces. An implementation of one or more FEs in a single indivisible unit (such as a physical box, or software load for a server) is compliant with this specification if it implements the functions as defined, and the external interfaces as defined for the assembly of FEs. Internal interfaces between FEs which are not exposed outside the implementation are not required to meet the standards herein, although it is recommended that they do.

---

<sup>1</sup> “Origination networks” include service providers who send calls to ESInets.

This document describes the “end state” that has been reached after a migration from legacy TDM circuit-switched telephony, and the legacy E9-1-1 system built to support it, to an all IP-based telephony system with a corresponding IP-based Emergency Services IP network. To get to this “end state” it is critical to understand the following underlying assumptions:

1. All calls entering the ESInet are SIP based. Gateways, if needed, are outside of, or on the edge of, the ESInet. IP services that are not native SIP based, have protocol interworking to SIP prior to being presented to the ESInet.
2. Access Network Providers (e.g.: DSL providers, fiber network providers, WiMax providers, Long Term Evolution (LTE) wireless carriers, etc.) have installed, provisioned and operated some kind of location function for their networks. Location functions are critical for 9-1-1 calls originating on an IP network because it provides a 9-1-1 valid location to IP clients that bundle their location in the SIP signaling to the ESInet.
3. All calls entering the ESInet will normally have location (which might be coarse, e.g., cell site/sector) in the signaling with the call.
4. 9-1-1 authorities have transitioned from the tabular MSAG and ESNs to GIS based Location Validation Function (LVF) and Emergency Call Routing Function (ECRF).
5. 9-1-1 authorities have accurate and complete GIS systems, which are used to provision the LVF and ECRF. A change to the 9-1-1 Authority’s GIS system automatically propagates to the ECRF and LVF and immediately affects routing.
6. Civic location will be validated by the access network against the LVF prior to an emergency call being placed. This is analogous to MSAG validation.
7. Periodic revalidation of civic location against the LVF is also needed to assure that location remains valid as changes in the GIS system that affect existing civic locations are made.
8. Since the legacy circuit-switched TDM network will very likely continue to be used for the foreseeable future (both wireline and wireless,) the i3 architecture defines a Legacy Network Gateway (LNG) to interface between the legacy network and the ESInet.
9. Transition to i3 is complete when the existing Selective Router and ALI are no longer used. Even after that time, some PSAPs may not have upgraded to i3. The i3 architecture describes a Legacy PSAP Gateway (LPG) to interface between the ESInet and a legacy PSAP. The LPG supports the origination of an emergency call through the ESInet to a legacy PSAP as well as the transfer of an emergency call from/to an i3 PSAP to/from a legacy PSAP.
10. Federal, State and local laws, regulations and rules may need to be modified to support NG9-1-1 system deployment.
11. While NG9-1-1 is based on protocols that are international, and are designed to allow visitors and equipment not of North American origin to work with NG9-1-1, the specific protocol mechanisms, especially interworking of legacy telecom and ESInet protocols is North American-specific and may not be applicable in other areas.

## 2 Introduction

### 2.1 Operational Impacts Summary

This standard will have a profound impact on the operation of 9-1-1 services and PSAPs. New data formats, more rigid data structure requirements, new functions, new databases, new call sources, new media types, new security challenges and more will impact the operation of 9-1-1 systems, PSAPs, their contractors and access and origination networks.

Nevertheless, the basic function, and the fundamental processes used to process calls will not change substantially. NENA Operations committees are working diligently to provide appropriate procedures to match this specification.

### 2.2 Security Impacts Summary

This document introduces many new security mechanisms that will impact network and PSAP operations. The most significant changes to current practice are:

- All transactions must be protected with authentication, authorization, integrity protection and privacy mechanisms specified by this document
- Common authentication (single sign-on) and common rights management/authorization functions are used for ALL elements in the network.
- Of necessity, PSAPs will be connected, indirectly through the ESInet, to the Internet to accept calls. This means that PSAPs will likely experience deliberate attack on their systems. The types of vulnerabilities that NG9-1-1 systems must manage and protect against will fundamentally change and will require constant vigilance to create a secure and reliable operating environment. NG9-1-1 systems must have robust detection and mitigation mechanisms to deal with such attacks.

### 2.3 Document Terminology

The terms "shall", "must" and "required" are used throughout this document to indicate required parameters and to differentiate from those parameters that are recommendations. Recommendations are identified by the words "desirable" or "preferably".

This document uses the word "call" to refer to a session established by signaling with two way real-time media and involves a human making a request for help. We sometimes use "voice call", "video call" or "text call" when specific media is of primary importance. The term "non-human-initiated call" refers to a one-time notification or series of data exchanges established by signaling with at most one-way media, and typically does not involve a human at the "calling" end. Examples of non-human-originated calls include a burglar alarm, an automatically detected HAZMAT spill or a flooding sensor. The term "call" can also be used to refer to either a "Voice Call", "Video Call", "Text Call" or "Data-only call", since they are handled the same way through most of NG9-1-1. The term "Incident" is used to refer to a real world occurrence for which one or more calls may be received.

The term Location Information Server as listed in the NENA Master Glossary includes functions out of scope i3. This document only uses those functions of a LIS described in Sections 4.2 and 5.9.

**2.4 Reason for Issue/Reissue**

This document is issued to define a specification describing the functionality supported by elements associated with an ESInet and the interconnection of these functional elements. This version (Issue 1.0) of the Functional and Interface Standards for the NENA i3 Solution is intended to be used in SDO liaisons, and Request for Information (RFI)-like processes. The NENA LTD Working Group plans to release subsequent versions of the Standard as new work items are identified and resolved.

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

Version	Approval Date	Reason For Changes
Original	[MM/DD/YYYY]	Initial Document

**2.5 Recommendation for Additional Development Work**

This is the first edition of this document. There are several sections where it is noted that further work is needed, and future editions will cover topics in more depth. The following table lists sections in this document that refer to possible future work.

<u>Section</u>	<u>Reference to future work</u>
1	Further SDO convergence work will be required to align the details between i3 and related origination network 9-1-1 interfaces. The results of this convergence work will be documented in a future edition of this document.
4.1.1.3	There is a requirement to allow PSAPs to control disconnect. There are no standards, which describe how this is accomplished in SIP signaling, but discussion on the subject is ongoing in the IETF ecrit work group. A future edition of this document is expected to describe how PSAP control of disconnect is implemented.
4.1.9	There is considerable flux in standardized Instant Messaging protocols. It is anticipated that there may be additional IM protocols supported by NG9-1-1 in the future, specifically XMPP. If such protocols are adopted, a future edition of this document will describe the ESInet interface.
4.3	A future edition of this document will contain descriptions of the Provisioning Service Objects (PSOs) defined for standard functions.
4.5	A future edition of this document will remove some of the informative text on LoST and highlight the normative text.



4.5.1.1.1	It is presently an error to request location validation for a geodetic coordinates-based location in RFC5222. This may be changed in a future edition to allow validation of a geodetic location; for example, how far off shore services can be provided may determine if an off shore location is valid for 9-1-1 purposes.
4.5.1.2	Further examples of call routing will be provided in a future edition of this document.
4.5.1.2.2	Examples of geodetic coordinates-based call routing in the LoST interface will be provided in a future edition of this document
4.7.1	A standard NENA schema for WFS as used in the i3 SIF layer replication protocol will be provided in a future edition of this document.
4.7.2	A future OGC specification, or a future edition of this document, will describe the SIF layer replication protocol definitively.
4.8	The CAD interface will be defined in a future edition of this standard, or a reference to another NENA document that defines it will be provided.
5.2.1.6	A list of the parameters contained in the notification of the ESRPnotify Event Package will be provided in a future edition of this document
5.2.2.7	CANCEL of a call should result in notification to the intended PSAP. This will be provided for in a future edition of this document
5.2.2.8	The specifics of the log service entries will be provided in a future edition of this document.
5.2.4	Specific policy document structures will be specified for each of the policy instances defined for the ESRP in a future edition of this document.
5.2.7	Operational Considerations for the ESRP will be provided in a future edition of this standard.
5.4.3.4	The ability to have alternative addresses returned, as supported within an i2 VDB, is currently out-of-scope for this document, and is left for future consideration.
5.5.3	The IETF geopriv working group is considering the definition of a geocoding protocol/service. If such a standardization effort is undertaken, and if the resulting work is suitable, it will replace this NENA-only interface in a future edition of this document.
5.6.1	While all i3 PSAPs must handle all media, a legacy PSAP behind an LPG would only handle voice media and TTY. There is no mechanism by which a caller could discover what media the PSAP supports. This will be covered in a future edition of this document.
5.9	How long a location reference must be valid beyond the duration of the call is a topic for future study, as well as the privacy considerations.

5.10	Extension of SIP to allow the data contained in an Additional Data about a Call structure to be included by value in the signaling is for future study.
5.12.1.1	A mechanism to discover the logger associated with an agency will be provided in a future edition of this document
5.12.1.1	It may be desirable to log other messages that are part of the INVITE transaction, such as the ACK. This will be covered in a future edition of this document.
5.12.4	Operational Considerations for the logging service will be supplied in a future edition of this standard.
5.15	The definition of an Agency Locator service will be provided in a future edition of this document.
6.2	The PCA CP/CPS must be in conformance with minimum standards to be provided in a future edition of this document.
6.3	Specific definitions of the roles enumerated in this section will be defined in an OID to be referenced in a future edition of this document.
6.7	A future edition of this standard will specify more precise key storage requirements to maintain privacy
7.1	Note: The LNG must log all significant events. Log record formats for this purpose will be provided in a future edition of this document.
7.1.2.3	This version does not describe interworking between SIP/HELD and E2/MLP for location conveyance and updates. This will be covered in a future edition of this document.
7.2	Note: The LPG must log all significant events. Log record formats for this purpose will be provided in a future edition of this document.
8.2	The xml data structure for Additional Data associated with a location will be defined in future work.
10	PSAP Management interface will be provided in a future edition of this document.
12.13	Roles will be defined in an OID to be referenced in a future edition of this document.

## 2.6 Date Compliance

All systems that are associated with the 9-1-1 process shall be designed and engineered to ensure that no detrimental, or other noticeable impact of any kind, will occur as a result of a date/time change up to 30 years subsequent to the manufacture of the system. This shall include embedded application, computer based or any other type application. To ensure true compliance, the

manufacturer shall upon request, provide verifiable test results to an industry acceptable test plan such as Telcordia GR-2945 or equivalent.

## **2.7 Anticipated Timeline**

As this is a major change to the 9-1-1 system, adoption of this standard will take several years and is also dependent on the pace of change and evolution of origination and access network providers. Experience with the immediately prior major change to 9-1-1 (i.e., Phase II wireless) suggests that unless consensus among government agencies at the local, state and federal levels, as well as network operators, vendors and other service providers is reached, implementation for the majority of PSAPs could take a decade. The Long Term Definition (LTD) Working Group chose technology commensurate with a 2-5 year implementation schedule.

## **2.8 Costs Factors**

This is an all-new 9-1-1 system; the cost of everything will change. At this time it is difficult to predict the costs of the system and more work will be needed by vendors and service providers to determine the impact of the changes on their products and operations. If implemented at a regional (multi-county) or state level, the cost of the new system may be significantly less than the cost of the existing system, although in the transition from the existing system to the new one, duplicate elements and services will have to be maintained at a higher overall cost. It also may be that costs are not reduced, but the improved service to the public justifies these costs. Note that the charge to the LTD Working Group was to NOT make costs a primary consideration in making technical decisions. Nevertheless, due to the pragmatic experience of the participants, the document tended to consider cost as one of the variables in making choices. Estimating the cost to deploy the entire NG9-1-1 system is the purview of other groups within and outside NENA.

## **2.9 Future Path Plan Criteria for Technical Evolution**

In present and future applications of all technologies used for 9-1-1 call and data delivery, it is a requirement to maintain the same level or improve on the reliability and service characteristics inherent in present 9-1-1 system design.

New methods or solutions for current and future service needs and options should meet the criteria below. This inherently requires knowledge of current 9-1-1 system design factors and concepts, in order to evaluate new proposed methods or solutions against the Path Plan criteria.

Criteria to meet the Definition/Requirement:

1. Reliability/dependability as governed by NENA's technical standards and other generally accepted base characteristics of E9-1-1 service
2. Service parity for all potential 9-1-1 callers
3. Least complicated system design that results in fewest components to achieve needs (simplicity, maintainable)
4. Maximum probabilities for call and data delivery with least cost approach

5. Documented procedures, practices, and processes to ensure adequate implementation and ongoing maintenance for 9-1-1 systems.

This basic technical policy is a guideline to focus technical development work on maintaining fundamental characteristics of E9-1-1 service by anyone providing equipment, software, or services.

## **2.10 Cost Recovery Considerations**

Traditionally, much of the cost of the existing E9-1-1 Service Provider infrastructure has been supported through the collection of fees and surcharges on wireline and wireless telephone service. Changes in the telecommunications industry has caused the basis on which the fees and surcharges are collected to be modified, and the architecture described in this document further sunders the assumptions on which the current revenue streams are based. It should be noted that the costs associated with operating the 9-1-1 environment envisioned within this document are no longer accurately predicted by the number of originating network subscribers residing in a given service area. This document does not make recommendations on how funding should be changed. See the NG Partner Program Funding Policy paper [142] for more on this subject.

## **2.11 Additional Impacts (non cost related)**

This effort is a part of the over-all Next Generation 9-1-1 project. There are far reaching impacts to the entire 9-1-1 system and public safety policies engendered by the changes in networks, databases, devices, interfaces and mechanisms this document describes. See the NG Partner Program Policy Guidelines documents for more on these areas [143]. It is expected that originating networks will ultimately evolve, but i3 assumes this evolution to take place over time and in stages by use of supporting gateways to allow existing interfaces from originating networks to be supported until such time as the originating network provider is ready to migrate to IP. Nearly all systems in a PSAP must (eventually) evolve. All databases change, some are eliminated, some new ones created, others are modified. New relationships between agencies must be established, for example, to facilitate answering of calls out of area.

Some of the more significant impacts are the methods and procedures to migrate the current 9-1-1 system to Next Generation 9-1-1. The NG9-1-1 Transition Planning Committee is developing documents that describe transition. This document only describes external interfaces to a PSAP. The internal PSAP subsystems and the interconnection between those subsystems must change. This is the responsibility of the NENA NG9-1-1 PSAP Working Group.

## **2.12 Intellectual Property Rights Policy**

NENA takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights.

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:

Version 1, June 14, 2011

Page 22 of 282

National Emergency Number Association

4350 N Fairfax Dr, Suite 750

Arlington, VA 22203-1695

800-332-3911

or: [techdoccomments@nena.org](mailto:techdoccomments@nena.org)

### 2.13 Acronyms/Abbreviations/Definitions

This is not a glossary. See NENA 00-002 - NENA Master Glossary of 9-1-1 Terminology located on the NENA web site for a complete listing of terms used in NENA documents.

**The following Acronyms are used in this document:**

<i>Acronym</i>	<i>Description</i>	<i>**New (U)pdate</i>
<b>3GPP</b>	3 <sup>RD</sup> Generation Partner Project	
<b>3GPP2</b>	3 <sup>rd</sup> Generation Partnership Project 2	
<b>AAA</b>	Authorization, Admission and Accounting	N
<b>ABNF</b>	Augmented Backus-Naur Form	N
<b>ACK</b>	Acknowledgement	N
<b>ACM</b>	Address Complete Message	N
<b>AES</b>	Advanced Encryption Standard	
<b>AIP</b>	Access Infrastructure Provider	
<b>AMR</b>	Adaptive Multi Rate (codec)	N
<b>AMR-WB</b>	Adaptive Multi Rate (codec) – Wide Band	N
<b>ANI</b>	Automatic Number Identification	
<b>ANS</b>	American National Standard	
<b>ANSI</b>	American National Standards Institute	
<b>AoR</b>	Address of Record	
<b>APCO</b>	Association of Public Safety Communications Officials	
<b>ATIS</b>	Alliance for Telecommunications Industry Solutions	
<b>ATIS-ESIF</b>	Alliance for Telecommunications Industry Solutions – Emergency Services Interconnection Forum	N
<b>B2BUA</b>	Back to Back User Agent	
<b>BCF</b>	Border Control Function	

<b>BISACS</b>	Building Information Services and Control System	N
<b>CA</b>	Certificate Authority	U
<b>CAD</b>	Computer Aided Dispatch	
<b>CAMA</b>	Centralized Automatic Message Accounting	
<b>CAP</b>	Common Alerting Protocol	N
<b>CERT</b>	Community Emergency Response Team	N
<b>cid</b>	Content Indirection	N
<b>CIDB</b>	Call Information Database	
<b>CPE</b>	Customer Premises Equipment	
<b>CRL</b>	Certificate Revocation List	
<b>CS</b>	Circuit Switched	N
<b>CSCF</b>	Call Session Control Function	
<b>CSP</b>	Communication Service Provider	
<b>DHCP</b>	Dynamic Host Control Protocol (i2) Dynamic Host Configuration Protocol	
<b>DNS</b>	Domain Name Server (or Service or System)	
<b>DoS</b>	Denial of Service	
<b>DSL</b>	Digital Subscriber Line	
<b>E9-1-1</b>	Enhanced 9-1-1	
<b>ECRF</b>	Emergency Call Routing Function	
<b>Ecrit</b>	Emergency Context Resolution In the Internet	
<b>E-CSCF</b>	Emergency Call Session Control Function	
<b>EDXL</b>	Emergency Data eXchange Language	N
<b>EISI</b>	Emergency Information Services Interface	
<b>EPAD</b>	Emergency Provider Access Directory	
<b>ESIF</b>	Emergency Services Interconnection Forum	
<b>ESInet</b>	Emergency Services IP Network	
<b>ESMI</b>	Emergency Services Messaging Interface	
<b>ESNet</b>	Emergency Services Network	
<b>ESN</b>	Emergency Service Number, Electronic Serial Number, Emergency Service Network	

<i>ESNI</i>	Emergency Services Network Interfaces	
<i>ESQK</i>	Emergency Services Query Key	
<i>ESRK</i>	Emergency Services Routing Key	
<i>ESRP</i>	Emergency Services Routing Proxy	
<i>ESZ</i>	Emergency Services Zone (Same as ESN)	
<i>EVRC</i>	Enhanced Variable Rate Narrowband Codec	
<i>EVRC-WB</i>	Enhanced Variable Rate Wideband Codec	
<i>FCC</i>	Federal Communications Commission	
<i>GDP</i>	Generic Digit Parameter	
<i>Geopriv</i>	Geolocation and Privacy	
<i>GeoRSS</i>	Geodetic Really Simple Syndication	N
<i>Geoshape</i>	Geodetic Shape	N
<i>GML</i>	Geographic Markup Language	
<i>GSM</i>	Global Standard for Mobile Communication	
<i>GUID</i>	Globally Unique Identifier	
<i>HELD</i>	HTTP-Enabled Location Delivery Protocol	
<i>HSS</i>	Home Subscriber Server	
<i>IAM</i>	Initial Address Message	
<i>IANA</i>	Internet Assigned Numbers Authority	
<i>IDP</i>	Identity Provider	N
<i>IETF</i>	Internet Engineering Task Force	
<i>IM</i>	Instant Messaging	
<i>IMS</i>	IP Multimedia Subsystem	
<i>IP</i>	Internet Protocol	
<i>IP-CAN</i>	IP Connectivity Access Network	
<i>IP-PBX</i>	Internet Protocol Private Branch Exchange	
<i>IPsec</i>	Internet Protocol Security	
<i>ISDN</i>	Integrated Services Digital Network	
<i>ISUP</i>	Integrated Services Digital Network User Part	N
<i>ISP</i>	Internet Service Provider	

<b>ISUP</b>	Integrated Services Digital Network User Part	
<b>KP</b>	Key Pulse	
<b>LAN</b>	Local Area Network	
<b>LDAP</b>	Lightweight Directory Access Protocol	
<b>LIF</b>	Location Interwork Function	N
<b>LIS</b>	Location Information Server	
<b>LO</b>	Location Object	
<b>LoST</b>	Location to Service Translation	
<b>LRF</b>	Location Retrieval Function	
<b>LTD</b>	Long Term Definition	
<b>LVF</b>	Location Validation Function	
<b>MDN</b>	Mobile Directory Number	
<b>MEP</b>	Message Exchange Pattern	
<b>MF</b>	Multi-Frequency	
<b>MIB</b>	Management Information Base	
<b>MPC/GMLC</b>	Mobile Positioning Center/ Gateway Mobile Location Center	
<b>MSC</b>	Mobile Switching Center	
<b>MPLS</b>	Multi-Protocol Label Switching	
<b>MSAG</b>	Master Street Address Guide	
<b>MSC</b>	Mobile Switching Center	
<b>MSRP</b>	Message Session Relay Protocol	N
<b>MTP</b>	Message Transfer Point	
<b>NAT</b>	Network Address Translation	
<b>NCIC</b>	National Crime Information Center, National Crime Enforcement Center	
<b>NENA</b>	National Emergency Number Association	
<b>NG9-1-1</b>	Next Generation 9-1-1	
<b>NGES</b>	Next Generation Emergency Services	
<b>NGN</b>	Next Generation Network	
<b>NIF</b>	NG9-1-1 Specific Interwork Function	N

<b>NMC</b>	9-1-1 Malicious Content	N
<b>NPD</b>	Numbering Plan Digit	
<b>NRS</b>	NENA Registry System	N
<b>NTP</b>	Network Time Protocol	
<b>OASIS</b>	Organization for the Advancement of Structured Information Standards	
<b>OGC</b>	Open Geospatial Consortium	N
<b>OLIP</b>	Originating Line Information Parameter	U
<b>PAI</b>	P-Asserted-Identity	N
<b>P-CSCF</b>	Proxy Call Session Control Function	
<b>PCA</b>	PSAP Credentialing Agency	
<b>PDA</b>	Personal Digital Assistant	
<b>PHB</b>	Per Hop Behaviors	N
<b>PIDF</b>	Presence Information Data Format	
<b>PIDF-LO</b>	Presence Information Data Format – Location Objects	
<b>PIF</b>	Protocol Interworking Function	N
<b>PKI</b>	Public Key Infrastructure	
<b>PRF</b>	Policy Routing Function	
<b>PSP</b>	Provisioning Service Provider	N
<b>PSAP</b>	Public Safety Answering Point or Primary Public Safety Answering Point	
<b>PSO</b>	Provisioning Service Object	N
<b>PSTN</b>	Public Switched Telephone Network	
<b>PTSC</b>	Packet Technologies and Services Committee (ATIS Standards Committees)	
<b>QoS</b>	Quality of Service	
<b>RA</b>	Requesting Authority	N
<b>RBAC</b>	Role Based Access Control profile	
<b>RDF</b>	Routing Determination Function	
<b>REL</b>	Release (message)	N
<b>REST</b>	Representational State Transfer	

<b>RFC</b>	Request for Comments	
<b>RG</b>	Response Gateway, Routing Gateway	
<b>RLC</b>	Release Complete (message)	N
<b>ROHC</b>	Robust Header Compression	N
<b>RTCP</b>	Real Time Control Protocol	
<b>RTP</b>	Real Time Transport Protocol	
<b>RTSP</b>	Real Time Streaming Protocol	
<b>RTT</b>	Real Time Text	N
<b>S-CSCF</b>	Serving Call Session Control Function	
<b>SAML</b>	Security Assertion Markup Language	
<b>SBC</b>	Session Border Control	
<b>SCTP</b>	Session Control Transport Protocol	
<b>SDES</b>	Session Description protocol Security Descriptions	N
<b>SDO</b>	Standards Development Organization	
<b>SDP</b>	Session Description Protocol	
<b>SHA</b>	Secure Hash Algorithm	
<b>SIF</b>	Spatial Information Function	N
<b>SIO</b>	Service Information Octet	
<b>SIP</b>	Session Initiation Protocol	
<b>SMS</b>	Short Message Service	
<b>SOA</b>	Service Oriented Architecture	
<b>SOAP</b>	Simple Object Access Protocol	
<b>SPML</b>	Service Provisioning Markup Language	
<b>SR</b>	Selective Routing, Selective Router [a.k.a., E9-1-1 Tandem, or Enhanced 9-1-1 (E9-1-1) Control Office]	
<b>SRTP</b>	Secure Real Time Protocol	N
<b>SRV</b>	Service (a DNS record type)	
<b>SS7</b>	Signaling System 7	
<b>TCP</b>	Transport/Transmission Control Protocol	
<b>TDM</b>	Time Division Multiplexing	

<b><i>TLS</i></b>	Transport Layer Security	
<b><i>TN</i></b>	Telephone Number	
<b><i>TOPS</i></b>	Technology and Operations Council	N
<b><i>TRD</i></b>	Technical Requirements Document	
<b><i>TTY</i></b>	Teletypewriter (a.k.a. TDD, Telecommunications Device for the Deaf and Hard-of-Hearing)	
<b><i>UA</i></b>	User Agent	
<b><i>UAC</i></b>	User Agent Client	
<b><i>UAS</i></b>	User Agent Service	
<b><i>UDDI</i></b>	Universal Description, Discovery and Integration	
<b><i>UDP</i></b>	User Datagram Protocol	
<b><i>UE</i></b>	User Element	
<b><i>URI</i></b>	Uniform Resource Identifier	
<b><i>URISA</i></b>	Urban and Regional Information Systems Association	
<b><i>URL</i></b>	Uniform Resource Locator (location sensitive)	
<b><i>URN</i></b>	Uniform Resource Name (location insensitive)	
<b><i>USPS</i></b>	United States Postal Service	
<b><i>UTC</i></b>	Universal Coordinated Time	
<b><i>VEDS</i></b>	Vehicle Emergency Data Sets	
<b><i>VF</i></b>	Validation Function	
<b><i>VoIP</i></b>	Voice over Internet Protocol	
<b><i>VPN</i></b>	Virtual Private Network	
<b><i>VSP</i></b>	VoIP Service Provider	
<b><i>WFS</i></b>	Web Feature Service	
<b><i>WSDL</i></b>	Web Service Definition Language	
<b><i>WSS</i></b>	Web Services Security	
<b><i>WTSC</i></b>	Wireless Technologies and Systems Committee	
<b><i>XACML</i></b>	eXtensible Access Control Markup Language	
<b><i>XML</i></b>	eXtensible Markup Language	
<b><i>XMPP</i></b>	eXtensible Messaging and Presence Protocol	N

<b>XSD</b>	W3C XML Schema Definition	
------------	---------------------------	--

The following Terms and Definitions are used in this document:		
<b>Term</b>	<b>Definition</b>	<b>** N)ew (U)pdate</b>
<b><i>g.711 a-law</i></b>	An ITU-T Recommendation for an audio codec for telephony in non-North American regions	N
<b><i>g.711 mu-law</i></b>	An ITU-T Recommendation for an audio codec for telephony in the North American region	N
<b><i>9-1-1 Authority</i></b>	The local agency responsible for overall operation of, and data for the 9-1-1 system	?
<b><i>AdditionalAgency Event</i></b>	A log entry indicating another agency’s involvement with a call or incident, which may have log records for that call or event in their own log.	N
<b><i>Additional Data</i></b>	Data associated with a call for which a URI is sent with the call or retrieved from the ECRF, for example, Additional Call Data, Additional Caller data and Additional Location Data	N
<b><i>Agency Identifier</i></b>	A domain name for an agency used as a globally unique identifier.	N
<b><i>Authentication</i></b>	A security term referring to the process of reliably identifying an entity requesting access to data or a service.	
<b><i>Authorization</i></b>	A security term referring to the process of making a decision what access rights an authenticated entity has to data or a service	
<b><i>B2BUA</i></b>	A back to back user agent is a SIP element that relays signaling mechanisms while performing some alteration or modification of the messages that would otherwise not be permitted by a proxy server.	N
<b><i>Bridging</i></b>	Connecting two or more parties with a conference bridge	N
<b><i>BYE transaction</i></b>	A SIP transaction used to terminate a session	N

The following Terms and Definitions are used in this document:		
<i>Term</i>	<i>Definition</i>	<i>** N)ew (U)pdate</i>
<i>Call</i>	A session established by signaling with two way real-time media and involves a human making a request for help. We sometimes use “voice call”, “video call” or “text call” when specific media is of primary importance. The term “non-human-initiated call” refers to a one-time notification or series of data exchanges established by signaling with at most one way media, and typically does not involve a human at the “calling” end. The term “call” can also be used to refer to either a “Voice Call”, “Video Call”, “Text Call” or “Data-only call”, since they are handled the same way through most of NG9-1-1.	
<i>Call Detail Record (CDR)</i>	A record stored in a database recording the details of a received or transmitted call	
<i>Call Identifier</i>	An identifier assigned by the first element in the first ESInet which handles a call. Call Identifiers are globally unique.	U
<i>Call-Info Header</i>	A SIP header which contains a URI referring to some kind of data relevant to a call, and a “purpose” parameter describing what the URI refers to. Used to carry URIs to such entities as Additional Call and Caller data, and call/Incident Tracking Identifiers	N
<i>CANCEL transaction</i>	A SIP transaction which is used to cancel an INVITE transaction which has not yet completed	N

The following Terms and Definitions are used in this document:		
<i>Term</i>	<i>Definition</i>	<i>** N)ew (U)pdate</i>
<b><i>CAP MESSAGE</i></b>	A notification using the Common Alerting Protocol. CAP is used within the ESInet to send alerts from automated systems to PSAPs, and is also used to communicate data between agencies without a call.	N
<b><i>Catypes</i></b>	A component of a civic address in a PIDF-LO such as a Street Name or House Number, which has a code used to identify what kind of component.	N
<b><i>Code Point</i></b>	A code for a requested QoS action used in the Diffserv QoS mechanism on an IP network. The code point is sent in the TOS field of an IP packet.	N
<b><i>Denial of Service Attack</i></b>	A type of cyber attack intended to overwhelm the resources of the target and deny the ability of legitimate users of the target the normal service the target provides.	N
<b><i>Dereference</i></b>	The act of exchanging a reference to an item by its value. Used primarily with a Location URI. The dereference operation uses a protocol such as SIP or HELD to obtain a location value (PIDF-LO).	N
<b><i>Diffserv</i></b>	A quality of service mechanism for IP networks characterized by a code in a field of a Packet called a “Code Point” and a “Per hop Behavior”	N
<b><i>Domain (or Domain Name)</i></b>	The domain name (hostname) of an agency or element in an ESInet. See Domain Name System (DNS)	N
<b><i>Element Identifier</i></b>	A logical name used to represent physical implementation of a functional element or set of functional elements as a single addressable unit. The form of an element identifier is a hostname.	N
<b><i>Emergency Call Routing Function (ECRF)</i></b>	A functional element in an ESInet which is a LoST protocol server where location information (either civic address or geo-coordinates) and a Service URN serve as input to a mapping function that returns a URI used to route an emergency call toward the appropriate PSAP for the caller’s location or towards a responder agency.	U

The following Terms and Definitions are used in this document:		
<i>Term</i>	<i>Definition</i>	<i>** New (U) pdate</i>
<b><i>Emergency Event</i></b>	An asynchronous communications notification which is a single communication message to a PSAP that results in a defined action by a call taker but does not have a human at the origination end and where no two way media streams are established.	N
<b><i>Emergency Services IP Network</i></b>	An ESIInet is a managed IP network that is used for emergency services communications, and which can be shared by all public safety agencies. It provides the IP transport infrastructure upon which independent application platforms and core functional processes can be deployed, including, but not restricted to, those necessary for providing NG9-1-1 services. ESIInets may be constructed from a mix of dedicated and shared facilities. ESIInets may be interconnected at local, regional, state, federal, national and international levels to form an IP-based inter-network (network of networks).	N
<b><i>From Header</i></b>	A SIP header that describes the caller's notion of its own identity (Address of Record). From is generally not treated as reliable unless it is protected by an Identity header	N
<b><i>geoShape Element</i></b>	One of a list of shapes defined originally by the IETF and standardized by the Open Geospatial Consortium that can be found in a PIDF-LO. Includes point, circle, ellipse, arc band, polygon and 3D versions of same	N
<b><i>H.264</i></b>	A video codec, defined by ITU-T in common use today for real time two way video	N
<b><i>HELD</i></b>	A protocol defined by the IETF to deliver location using HTTP transport	N
<b><i>IANA Registry</i></b>	A registry maintained by the Internet Assigned Number Authority, usually at the behest of the IETF	N
<b><i>Incident</i></b>	A real world occurrence such as a heart attack, car crash or a building fire for which one or more calls may be received.	N
<b><i>Incident Tracking Identifier</i></b>	An identifier assigned by the first element which declares an incident. Incident Tracking Identifiers are globally unique.	U
<b><i>INFO</i></b>	A SIP transaction used to pass information from the caller to the called party	N
<b><i>Instant Messaging (IM)</i></b>	A method of communication generally using text where more than a character at a time is sent between parties nearly instantaneously	N
<b><i>INVITE</i></b>	A SIP transaction used to initiate a session	N

The following Terms and Definitions are used in this document:		
<i>Term</i>	<i>Definition</i>	<i>** N)ew (U)pdate</i>
<b>Legacy PSAP Gateway</b>	An NG9-1-1 Functional Element which provides an interface between an ESInet and an un-upgraded PSAP	N
<b>Location</b>	In the context of location information to support IP-based emergency services: The physical position of an end-point expressed in either civic or geodetic form. A spot on the planet where something is; a particular place or position. Oxford Dictionary, Oxford University Press, 2009.	U
<b>Location Interwork Function (LIF)</b>	The functional component of a Legacy Network Gateway which is responsible for taking the appropriate information from the incoming signaling (i.e., calling number/ANI, ESRK, cell site/sector) and using it to acquire location information that can be used to route the emergency call and to provide location information to the PSAP. In a Legacy PSAP Gateway, this functional component takes the information from an ALI query and uses it to obtain location from a LIS.	N
<b>Location URI</b>	A URI which, when dereferenced, yields a location value in the form of a PIDF-LO. Location-by-reference in NG9-1-1 is represented by a Location URI.	N
<b>Mapping</b>	The act of determining a value in one domain from a value in another domain. For example, mapping a location to the URI of a PSAP that serves that location using the LoST protocol.	N
<b>MESSAGE</b>	A SIP method which passes information, often an Instant Message, between endpoints in the body of the SIP message	N
<b>NG9-1-1 Specific Interwork Function (NIF)</b>	The functional component of a Legacy Network Gateway or Legacy PSAP Gateway which provides NG9-1-1-specific processing of the call not provided by an off-the-shelf protocol interwork gateway.	N
<b>Next Hop</b>	The next element in a routing path. For example, the next router in an IP network, or the next SIP proxy server in a SIP signaling path.	N
<b>Notifier</b>	An element in an asynchronous event notification mechanism that transmits events	N
<b>NOTIFY</b>	A SIP method used to send a notification to a subscriber of the occurrence of an asynchronous event.	N
<b>OPTIONS</b>	A SIP method used to request the SIP protocol options supported by an endpoint.	N

The following Terms and Definitions are used in this document:		
<i>Term</i>	<i>Definition</i>	<i>** New (U)pdate</i>
<b><i>Originating ESRP</i></b>	The first routing element inside the ESInet. It receives calls from the BCF at the edge of the ESInet.	N
<b><i>Per Hop Behaviors (PHB)</i></b>	The action a router takes for a packet marked with a specific code point in the Diffserv QoS mechanism in IP networks	N
<b><i>Policy Routing Function (PRF)</i></b>	That functional component of an Emergency Services Routing Proxy that determines the next hop in the SIP signaling path using the policy of the nominal next element determined by querying the ECRF with the location of the caller.	U
<b><i>Policy Store</i></b>	A functional element in the ESInet that stores policy documents.	N
<b><i>PRACK</i></b>	A SIP message used to reliably acknowledge receipt of an otherwise unreliable message transmission.	N
<b><i>Protocol Interworking Function (PIF)</i></b>	That functional component of a Legacy Network Gateway or Legacy PSAP Gateway that interworks legacy PSTN signaling such as ISUP or CAMA with SIP signaling.	N
<b><i>Provisioning Service provider (PSP)</i></b>	The component in an ESInet functional element that implements the provider side of a SPML interface used for provisioning	N
<b><i>PSAP Credentialing Agency (PCA)</i></b>	The root authority designated to issue and revoke security credentials (in the form of an X.509 certificate) to authorized 9-1-1 agencies in an ESInet.	N
<b><i>Real Time Text (RTT)</i></b>	Text transmission that is character at a time, as in TTY.	N
<b><i>REFER</i></b>	A SIP method that is used as part of a transfer operation to refer a call to another endpoint	N
<b><i>REFER/Replaces</i></b>	Use of the SIP REFER method together with a Replaces header as part of a transfer operation to indicate that a new leg is to be created that replaces an existing call leg.	N
<b><i>REGISTER</i></b>	A SIP method that is used to communicate the availability and address of an endpoint to the proxy server that directs incoming calls.	N
<b><i>reINVITE</i></b>	A SIP INVITE transaction within an established session used to change the parameters of a call.	N
<b><i>RequestURI</i></b>	That part of a SIP message that indicates where the call is being routed towards. SIP Proxy servers commonly change the Request ID (“retargeting”) to route a call towards the intended recipient.	N
<b><i>Resource Priority</i></b>	A header used on SIP calls to indicate priority that proxy servers give to specific calls.	N

The following Terms and Definitions are used in this document:		
<i>Term</i>	<i>Definition</i>	<i>** New (U)pdate</i>
<b><i>ReverseGeocode</i></b>	The process of converting a geo form of location (X,Y) to a civic (street address) form.	N
<b><i>Rights Management</i></b>	Specifying the access rights by an entity (agent or agency) to a particular document, data element, or service	N
<b><i>Scheme</i></b>	The part of a URI that indicates the protocol. For example, the scheme in the URI sip:john@example.com is “sip”	N
<b><i>Security Posture</i></b>	An event that represents a downstream entity’s current security state (normal, under attack, ...).	N
<b><i>Service Boundary</i></b>	A polygon in a GIS system, SIF, ECRF or other ESInet element that indicates the area a particular agency or element serves.	N
<b><i>Service Uniform Resource Name (Service URN)</i></b>	A URN with “service” as the first component supplied as an input in a LoST request to an ECRF to indicate which service boundaries to consider when determining a response. A service URN is also used to mark a call as an emergency call.	N
<b><i>Session Border Control</i></b>	A commonly available functional element that provides security, NAT traversal, protocol repair and other functions to VoIP signaling such as SIP. A component of a Border Control Function	N
<b><i>Smart Cards</i></b>	A credit-card-like object that contains a processor and memory, and is typically used to carry credentials for an agent in an authentication system. A smart card may be one factor in a 2 or 3 factor authentication system and is “something you have”	N
<b><i>SOS URN</i></b>	A service URN starting with “urn:service:sos” which is used to mark calls as emergency calls as they traverse an IP network.	N
<b><i>SUBSCRIBE/NOTIFY</i></b>	The two actions in an asynchronous event notification system. The subscription is the request to receive notifications of the events. The Notify is the notification of the event itself. Also refers to the SIP methods used for this purpose.	N
<b><i>Subscriber Database (SDB)</i></b>	A database operated by a carrier or other service provider which supplies the “Additional Call” data object. The SDB dereferences the URI passed in a Call-Info header and returns the AdditionalCall XML object.	N
<b><i>SubjectAltName</i></b>	A field in an X.509c digital certificate which typically contains identifying information for the entity issued the certificate. In an ESInet, SubjectAltName contains an agent or agency ID	N

The following Terms and Definitions are used in this document:		
<i>Term</i>	<i>Definition</i>	<i>** N)ew (U)pdate</i>
<b><i>Terminating ESRP</i></b>	The last ESRP for a call in an ESInet, and typically chooses a queue of call takers to answer the call	N
<b><i>Token</i></b>	A physical device that displays a multidigit number used as part of an authentication system (“something you have”). Also, a set of bits that represent some data, permission or state which is meaningful to the recipient, but not necessarily the sender.	N
<b><i>Transcoding</i></b>	Translating a media stream from one codec to another. For example, translating Baudot tones detected in a G.711 encoded audio stream to T.140 real time text	N
<b><i>UPDATE</i></b>	A SIP method used to update parameters in a call not yet established	N

## 3 General Concepts

### 3.1 Identifiers

To enable calls to be handled in an interconnected ESInet, identifiers are standardized as follows:

#### 3.1.1 Agency Identifier

An Agency is an organization that is a client of a database or service, which is represented by a domain name (hostname from STD013 [106]). Agencies must use one domain name consistently in order to correlate actions across a wide range of calls and incidents. Any domain name in the public DNS is acceptable so long as each distinct agency uses a different domain name. This implies that each agency ID is globally unique. An example of an agency identifier is [psap.allegheny.pa.us](http://psap.allegheny.pa.us).

#### 3.1.2 Agent Identifier

An agent is a person employed by or contracted by an agency. An agent identifier is a user name, using the syntax for “Dot-string” in RFC2821 (that is, the user part of an email address, without the possibility of a “Quoted-String”). Usernames must be unique within the domain of the agency, which implies that the combination Agent and Agency IDs is globally unique. Examples of this include [tom.jones@psap.allegheny.pa.us](mailto:tom.jones@psap.allegheny.pa.us) and [tjones.atroop@state.vt.us](mailto:tjones.atroop@state.vt.us).

#### 3.1.3 Element Identifier

A logical name used to represent physical implementation of a functional element or set of functional elements as a single addressable unit. (Section 4.1.2) The external interfaces of the element must adhere to the standards in this document. Elements are addressable via a hostname that must be globally unique. An example of an element identifier is [esrp.state.pa.us](http://esrp.state.pa.us).

#### 3.1.4 Call Identifier

The term “call” is defined in Section 2.3 and includes voice calls, video calls, text calls and non-human-initiated calls. The first element in the first ESInet which handles a call assigns the Call Identifier. The form of a Call Identifier is a URI consisting of the string “\_CI\_”, a unique string, the “@” character, and the domain name of the element that first handled the call. For example: “\_CI\_a56e556d871@bcf.state.pa.us”. The unique string must be unique for each call the element handles over time. The length of the unique string must be between 10 and 30 characters. One way to create the unique string is to use a timestamp with a suffix that differentiates multiple calls if they could be created by the element in the same instant. Implementations using multiple physical devices to implement a redundant element may need an additional component to guarantee uniqueness.

#### 3.1.5 Incident Tracking Identifier

A real world occurrence such as a heart attack, car crash or a building fire for which one or more calls may be received is an Incident. Examples include a traffic accident (including subsequent secondary crashes), a hazardous material spill, etc. Multiple Calls may be associated with an Incident. An Incident may include other Incidents in a hierarchical fashion. The form of an Incident

Tracking Identifier is a URI consisting of the string “\_II\_”, a unique string, the “@” character, and the domain name of the entity that first declared the incident. For example: “\_II\_a564w443112z@bcf.state.pa.us”. The unique string must be unique for each Incident the element handles over time. One way to create the unique string is to use a timestamp with a suffix that differentiates multiple Incidents if they could be created by an element in the same instant. Implementations using multiple physical devices to implement a redundant element may need an additional component to guarantee uniqueness. Incident Tracking Identifiers are globally unique. By definition, there is an Incident associated with every call. As a practical matter, there is at least one call associated with every Incident, except those incidents declared by an agent (such as a policeman observing a traffic incident). Incident Tracking Identifiers may be assigned to a call prior to determining what real world incident it actually belongs to. See Section 5.2.2.2

### 3.2 Timestamp

Any record that must be marked with when it occurred (especially a log record, see Section 5.12) includes a timestamp. A timestamp is represented by an ISO 8601 [115] time point. Time must include seconds, and, if two or more timestamps could be generated by the same element within one second where the order of events matter, the seconds element must include sufficient decimal places in the seconds field to differentiate the time stamps. An example of a timestamp is 2015-08-21T12:58.03.01+05. All time within the ESInet is represented as local time with offset to UTC. The offset is a required component of a timestamp.

### 3.3 Events common to multiple functional elements

Events are described in Section 4.1.3.2. The following events may be implemented in any functional element. Also see the Logging service interface in Section 5.12, which is implemented by any element that handles a call.

#### 3.3.1 Security Posture

SecurityPosture is an event that represents a downstream entity’s current security state. This document creates a NENA Registry System (NRS) registry of allowed values. The initial defined values are:

- Green – The entity is operating normally
- Yellow – The entity is receiving suspicious activity, but is able to operate normally
- Orange – The entity is receiving fraudulent calls/events, is stressed, but is able to continue most operations
- Red – The entity is under active attack and is overwhelmed

**Event Package Name:** nena-SecurityPosture

**Event Package Parameters:** None

**SUBSCRIBE Bodies:** standard RFC4661 + extensions filter specification may be present

**Subscription Duration** Default 1 hour. 1 minute to 24 hours is reasonable.

**NOTIFY Bodies:** MIME type application/vnd, nena.SecurityPosture+xml

Parameter	Condition	Description
Posture	Mandatory	Enumeration of current security posture from NRS SecurityPosture registry

### Notifier Processing of SUBSCRIBE Requests

The notifier consults the policy (securityPosture) to determine if the requester is permitted to subscribe. It returns 603 (Decline) if not acceptable. If the request is acceptable, it returns 202 (Accepted).

### Notifier Generation of NOTIFY Requests

When the security posture of the element changes, a new NOTIFY is generated, adhering to the filter requests.

### Subscriber Processing of NOTIFY Requests

No specific action required.

### Handling of Forked Requests

Forking is not expected to be used with this package

### Rate of Notification

Posture state normally does not change rapidly. Changes may occur in minutes if attacks start and stop sporadically.

### State Agents

No special handling is required.

### 3.3.2 Element State

ElementState is an event that indicates the state of an element either automatically determined, or as determined by management. This document creates an NRS registry (ElementState) of allowed values with initial defined states of:

- Normal: The element is operating normally, accepting calls and events
- Unmanned: (applies to PSAPs only) The PSAP has indicated that it is not currently answering calls.
- ScheduledMaintenance: The element is undergoing maintenance activities and is not processing calls

- **ServiceDisruption:** The element has significant problems and is unable to answer calls
- **MajorIncidentInProgress:** The element is operating normally, but is handling a major incident and may be unable to accept some kinds of calls
- **Overloaded:** The element is completely overloaded
- **GoingDown:** The element is being taken out of service
- **Down:** The element is unavailable
- **ComingUp:** the element is being put back in service

Note that when an implementation provides redundant physical implementations to increase reliability, usually the set of physical boxes is treated as a single element with respect to the rest of the ESInet and there is only one element state

**Event Package Name:** nena-ElementState

**Event Package Parameters:** None

**SUBSCRIBE Bodies:** standard RFC4661 + extensions filter specification may be present

**Subscription Duration** Default 1 hour. 1 minute to 24 hours is reasonable.

**NOTIFY Bodies:** MIME type application/vnd.nena.ElementState+xml

Parameter	Condition	Description
State	Mandatory	Enumeration of current state from NRS ElementState registry

### Notifier Processing of SUBSCRIBE Requests

The notifier consults the policy (elementState) to determine if the requester is permitted to subscribe. It returns 603 (Decline) if not acceptable. If the request is acceptable, it returns 202 (Accepted).

### Notifier Generation of NOTIFY Requests

When the state of the element changes, a new NOTIFY is generated, adhering to the filter requests.

### Subscriber Processing of NOTIFY Requests

No specific action required

### Handling of Forked Requests

Forking is not expected to be used with this package

## Rate of Notification

State normally does not change rapidly. Changes may occur in tens of seconds if the network or systems are unstable.

## State Agents

No special handling is required.

### 3.3.3 Service State

ServiceState is an event that indicates the state of service either automatically determined, or as determined by management. This document creates an NRS registry (ServiceState) of allowed values with initial defined states of:

- Normal: The service is operating normally
- ScheduledMaintenance (down): The service is undergoing maintenance activities and is not accepting service requests
- ScheduledMaintenance (available): The service is undergoing maintenance activities, but will respond to service requests, possibly with reduced reliability
- ServiceDisruption: The service has significant problems and is unable to respond
- Slow: The service is operating normally, but is handling a larger than normal number of requests, responses may be slow.
- GoingDown: The service is being taken out of service
- Down: The service is unavailable
- ComingUp: The service is being put back in service

Note that one or more elements may implement a service. Each element would have its own element state, the service would have an independent state.

**Event Package Name:** nena-ServiceState

**Event Package Parameters:** None

**SUBSCRIBE Bodies:** standard RFC4661 + extensions filter specification may be present

**Subscription Duration** Default 1 hour. 1 minute to 24 hours is reasonable.

**NOTIFY Bodies:** MIME type application/vnd.nena.ServiceState+xml

Parameter	Condition	Description
Service	Mandatory	Name of Service
State	Mandatory	Enumeration of current state from NRS ServiceState registry

### **Notifier Processing of SUBSCRIBE Requests**

The notifier consults the policy (serviceState) to determine if the requester is permitted to subscribe. It returns 603 (Decline) if not acceptable. If the request is acceptable, it returns 202 (Accepted).

### **Notifier Generation of NOTIFY Requests**

When the state of the service changes, a new NOTIFY is generated, adhering to the filter requests.

### **Subscriber Processing of NOTIFY Requests**

No specific action required.

### **Handling of Forked Requests**

Forking is not expected to be used with this package.

### **Rate of Notification**

State normally does not change rapidly. Changes may occur in tens of seconds if the network or systems are unstable.

### **State Agents**

No special handling is required.

## **3.4 Location Representation**

Location in NG9-1-1 is represented by validated content in the PIDF-LO<sup>2</sup> (RFC4119, updated by RFC5139 and RFC5491) with field use for the United States as documented in the NENA Civic Location Exchange Format [109]. Fields in the PIDF-LO must be used as defined; no local variation is permitted. A service (PIDFLOtoMSAG) is provided in this document for translating PIDF-LO to

---

<sup>2</sup> In the IETF, location information is a subset of Presence information. While NG9-1-1 uses PIDF and the IETF mechanisms that are described in the Presence service, no other parts of presence are used.

a NENA standard MSAG representation for backwards compatibility. All geodetic data in i3 uses WGS84 as the datum.

### 3.5 vCards

In many interfaces defined in this and related NG9-1-1 documents, a common need is to provide contact information. For example, in the Additional Caller Data, the identity and contact information is part of the data structure. When contact data is needed, i3 specifies the use of a **vCard** as defined in RFC2426 [124]. It is recognized that an XML format of this information would be desirable, but until one is standardized, it is felt using the recognized RFC2425 standard is appropriate.

### 3.6 Emergency Services IP Networks

ESInets are private, managed, and routed IP networks. An ESInet serves a set of PSAPs, a region, a state, or a set of states. The ESInet has a service area, defined by a (set of) polygon(s). ESInets are interconnected to neighboring ESInets so that traffic can be routed from any point in the ESInet to any point in any other ESInet. States may have a backbone ESInet either directly connecting to all PSAPs in the state, or interconnected to all county or regional ESInets. Neighboring states or regions may interconnect their ESInets. It is desirable to have a backbone national ESInet to optimize routing of traffic between distant state ESInets. Each PSAP must be connected to an ESInet, possibly through a Legacy PSAP Gateway.

ESInets must accept and route IPv4 and IPv6 packets. All services must support IPv4 and IPv6 interfaces. IPv6 is recommended for use throughout the ESInet, but cannot be assumed.

The ESInet must be connected to the Internet through the Border Control Function (BCF) to accept calls. This Internet interconnect is recommended at the state ESInet level. Origination networks should be connected to any ESInet they regularly deliver volume traffic to via a private connection, through the BCF of that ESInet. Connection through the Internet is acceptable, preferably through a VPN.

Access to ESInets must be controlled. Only public safety agencies, their contractors and service providers should be connected directly to the ESInet. However, for security reasons, the ESInet should not be assumed to be a “walled garden”.

For QoS reasons, IP traffic within an ESInet must implement DiffServ (RFC2475). Routers must respect code points, functional elements must mark packets they create with appropriate code points. The BCF must police code points for packets entering the ESInet. The following code points and Per Hop Behaviors (PHB) must be used on ESInets:

<b>DSCP</b>	<b>Use</b>	<b>PHB</b>
0	Routine Traffic	Default
1	9-1-1 Signaling	AF12
2	9-1-1 Text Media	AF12

3	9-1-1 Audio Media	EF
4	9-1-1 Video Media	AF11
5	9-1-1 Non-human-initiated Call	AF21
6	Intra ESInet Events	AF21
7	Intra ESInet Other 9-1-1 Traffic	AF22

All elements in an ESInet should have a publicly addressable IP address. Network Address Translations (NATs) should not be used within an ESInet. Although NAT use within an ESInet is not recommended, NATs may be needed in specific deployments, and therefore all network elements must operate in the presence of NATs.

It is recommended that elements connected to the ESInet not be referred to by their IP address but rather through a hostname using DNS. Use of statically assigned IP addresses should be limited, and should never be used with IPv6 addresses. DHCP must be implemented on all network elements to obtain IP address, gateway, and other services. Many ESInet services depend on discovery of services via DHCP.

There must be no single point of failure for any critical service or function on the ESInet. Certain services designated as non-critical may be exempt from this requirement. These must not include the BCF, internal ECRF, ESRP, logging service and security services. Services must be deployed to survive disaster, deliberate attack and massive failure.

## 4 Interfaces

### 4.1 SIP Call

The i3 call interface is SIP [12]. All calls presented to the ESInet must be SIP signaled. Calls are potentially multimedia, and can include one or more forms of media (audio, video and/or text<sup>3</sup>). See Section 4.6 for a discussion of "non-human-initiated calls" which can be used for non-human-initiated requests for help where there is no human caller. SIP is also the protocol used to call a 9-1-1 caller back, and for calls between agents within the ESInet.

SIP is a complex protocol defined in a large number of standards documents. All NG9-1-1 elements which process calls must implement all of the standards listed in Section 3 (Core Standards) in the

---

<sup>3</sup> All ESInet elements support all forms of media described in this document. Any given origination network or device may not support all media types, and support of specific media types by origination networks and devices may be subject to regulation.

"Hitchhiker's Guide to SIP" [11]. Implementations are cautioned to be "strict in what you send, and liberal in what you accept" with respect to such standards. It is generally unacceptable to drop a 9-1-1 call just because it doesn't meet some standard detail if it's reasonably possible to process the call anyway.

There are three primary entities in a SIP protocol exchange:

1. The User Agent Client, which is the initiator of a "transaction" within SIP. In the origination of a 9-1-1 call, the calling party's end device is the UAC
2. The User Agent Server, which is the target of a transaction within SIP. In the origination of a 9-1-1 call, the call taker's end device is the UAS.
3. A Proxy Server, which is an intermediary that assists in the routing of a call. Proxy servers are in the signaling path of a call, but not in the media path. A call may traverse several proxies. In a typical 9-1-1 call, the calling party's carrier may have two or more proxies. The ESInet has at least one proxy (an Emergency Services Routing Proxy) and typically has more than one.

SIP message exchanges are defined in transactions, which are explicit sequences of messages. The transaction is named by the "method" in the SIP message that starts the transaction. For example, the SIP transaction that creates a call (termed a "session" in SIP) is the INVITE transaction.

#### **4.1.1 Minimal Methods needed to handle a call**

The only method absolutely required to handle a 9-1-1 call is the INVITE. The REFER method (defined in [23]) should also be supported to conference and transfer calls. Call takers (and thus bridges that they use) must be able to generate the BYE transaction to terminate the call.

NG9-1-1 elements that process 9-1-1 calls must accept calls that do not strictly follow the SIP standards. So long as the messages can be parsed, and the method discerned, at least the first SIP element (the BCF) must be able to accept the call and forward the call onward (see Section 5.1).

##### **4.1.1.1 INVITE (initial call)**

The INVITE method is used to initiate a call. The standard INVITE/OK/ACK sequence must be followed, with allowance for intermediate (1XX) responses. It is generally unacceptable to refuse an INVITE request unless the PSAP is under active attack and cannot respond.

An emergency call has a Route header obtained from the ECRF based on the location of the call, and a Request URI containing a Service URN. Nominally, the Service URN should be urn:service:sos. In most jurisdictions, urn:service:sos.police, urn:service:sos.fire and urn:service:sos.ambulance would route to the primary PSAP.

The external (outside the ESInet) ECRF returns a "PSAP URI" which would be the Route header when the call enters the ESInet. The content of this URI can vary depending on the policy of the 9-1-1 Authority. One strategy is simply to use a general URI that leads to a state level ESRP, for example [911@sos.tx.us](mailto:911@sos.tx.us). The state ESRP would query the internal (within the ESInet) ECRF with a mapped (from the incoming service URN in the Request URI) service urn, for example urn:nena:service:sos.psap and would receive the next hop route for the call. Alternatively, the

external ECRF could return a more specific URI, for example, [harris.county@sos.tx.us](mailto:harris.county@sos.tx.us). This URI would still route to the same state-level ESRP, which would perform the same ECRF query. However, failures at the state ESRP (for example, a failure to obtain a route from the ECRF) may be able to be mitigated by using the information in the Route header.

Every call received by the ESInet gets some form of "call treatment". Minimal call treatments defined include:

1. Queue a call for answering by a call taker
2. Return Busy (600 Busy Everywhere)
3. Answer at an Interactive Multimedia Response system
4. Divert to another PSAP.

The ESRP determines, by evaluating PSAP policy, which treatment a call gets.

All calls that will go to a call taker are queued; however, the time in queue may be negligible.

The PSAP should normally only return a 183 In Progress intermediate response when a 9-1-1 call is queued for answer. It is recommended that no other 1XX response be used due to uneven implementations of these responses. 183 In Progress should be repeated at approximately 3 second intervals if the call is not answered. When placing a call back, elements must accept any 1XX intermediate response and provide an appropriate indication to the caller. UACs within the ESInet must generate an appropriate audible and in most cases a visual ring indication.

The normal response to an answered call is 200 OK.

9-1-1 calls are usually not redirected, and thus 3XX responses are normally not used; however 3XX may be used for calls within the ESInet. NG9-1-1 elements that initiate calls within the ESInet should appropriately respond as defined in RFC 3261 [12]. A 9-1-1 call may be so malformed that the BCF cannot parse the message.

Errors typically encountered in a SIP call should be handled as follows:

<b>SIP INVITE Response Codes from ESRP</b>	<b>Description</b>
183 (Ringing)	A 9-1-1 call is queued for answer. It is recommended that no other 1XX response be used due to uneven implementations of these responses. 183 Ringing should be repeated at approximately 3 second intervals if the call is not answered.
200 (OK)	Normal response to an answered call
3XX	9-1-1 calls are usually not redirected, and thus 3XX responses are normally not used. 3XX may be used for calls within the ESInet. NG9-1-1 elements that initiate calls within the ESInet should appropriately respond as defined in RFC 3261 [12].

400 (Bad Request)	A 9-1-1 call is so malformed that the BCF cannot parse the message.
401	Should never occur for a 9-1-1 call, but proxy authorization is required for all calls originated by entities within an ESInet.
402	Should never occur for a 9-1-1 call or an internal call
403 (Forbidden)	Normally, 403 (Forbidden) should not occur, but if the BCF passes a malformed INVITE which downstream devices cannot handle, they may have no choice but to return 403.
404 (Not Found)	404 (Not Found) would normally not occur for a 9-1-1 call, but may be used within the ESInet.
406 (Not Acceptable)	The 406 (Not Acceptable) should not occur for a 9-1-1 call because the INVITE should not have an Accept header that is unacceptable to the PSAP. If it does, 406 is the correct response.
408 (Request Timeout)	May be issued in an unplanned circumstance. Normally, this should never happen to a 9-1-1 call.
413 (Request Entity too Large)	The BCF should accept any Request URI, but downstream elements may return 413 (Request Entity Too Large).
414 (Request-URI Too Long)	The BCF should accept any Request URI, but downstream elements may return 414 (Request-URI Too Long).
416 (Unsupported URI Scheme)	The BCF should accept any Request URI, but downstream elements may return 416 (Unsupported URI Scheme).
486 (Busy Here)	PSAPs may limit the number of test calls, and if that limit is exceeded, the response shall be 486 Busy Here.
600 (Busy Everywhere)	If the BCF detects an active attack, it should respond with 600 (Busy Everywhere), rather than another 4XX response.

Once a call is established, it may be necessary to modify some of the parameters of the call. For example, it may be necessary to change the media session parameters. In this case, an INVITE transaction on an existing session is used. This is termed a “reINVITE” in SIP. Re-INVITES may be used on any call within the ESInet, including a 9-1-1 call. ReINVITE may be initiated from

either end of the call. Note that when the reINVITE is initiated by the called party, it becomes the UAC and the calling party becomes the UAS.

#### **4.1.1.2 REFER (transfer)**

The REFER method is used with the ESInet for two purposes:

- to transfer a call
- to conference additional parties to a call.

Actually, these two use cases are related, because the ESInet transfer operation involves a bridge so that the caller is never put on hold.

REFER is defined in [23]. The REFER method indicates that the recipient (identified by the Request-URI) should contact a third party using the contact information provided in the Refer-To header of the request. The recipient of the REFER request sends an INVITE to the URI in the Refer-To header.

REFER creates an implicit subscription [17] to a REFER event package. As with all SIP subscriptions the recipient of the REFER sends an immediate notify confirming instantiation of the subscription. When the INVITE is answered or fails, another NOTIFY is sent with success or failure of the REFER operation.

REFER is sometimes used with the Replaces header, which is dubbed “REFER/Replaces”. This is used to replace a call leg with another call leg, an example being replacing a two way call between the caller and call taker with a leg between the caller and the bridge, with another transaction used to create the leg between the call taker and the bridge.

If the calling device supports REFER, the REFER can be sent to the calling device to transfer a call. Section 5.8 discusses the problem of a calling device that is unable to support a REFER transaction.

#### **4.1.1.3 BYE (call termination)**

The BYE method is used to terminate a call. BYE may be initiated from either end. PSAPs must accept a BYE request and honor it.

Note: There is a requirement to allow PSAPs to optionally control disconnect. There are no standards that describe how this is accomplished in SIP signaling, but discussion on the subject is ongoing in the IETF ecrit work group and appropriate work in other SDOs will be required. A future edition of this document is expected to describe how PSAP control of disconnect is implemented.

### **4.1.2 Methods allowed to be initiated by caller which must be supported by i3 elements**

#### **4.1.2.1 CANCEL (cancel call initiation)**

An attempt to create a call with INVITE may be cancelled before it is completed with a CANCEL method. CANCEL is used before the session is created (call establishment), BYE is used after the session is created. Of course, race conditions exist between the signaling of the session and the attempt to cancel it. These conditions are discussed in RFC 3261 [12]. CANCEL would be the

signaling used to abandon a call, and ESInet elements must treat a CANCELLED call as such, including logging requirements.

#### **4.1.2.2 UPDATE (update parameters)**

UPDATE is defined in RFC3311 [18] and is sometimes used during call establishment if needed to change the parameters of the call. UPDATE is usually not used on calls that are already established, which typically requires a reINVITE. UPDATE may be used on any call within an ESInet (including 9-1-1 calls).

#### **4.1.2.3 OPTIONS (option negotiation)**

Options may be used by an external caller, or inside the ESInet to determine the capabilities of the destination UA. All endpoints within the ESInet must be capable of responding to an OPTIONS request, as defined in RFC3261. It would be unusual, but not improper, for an external caller to query the PSAP with OPTIONS before placing an emergency call.

An OPTIONS transaction is the preferred mechanism for maintaining a “keep alive” between two SIP elements. Periodic OPTIONS transactions must be used between ESRPs which normally pass calls between themselves, between the ESRP and the PSAPs and LPGs it normally serves, and between the PSAP and the bridge it normally uses. The period between OPTIONS used for keep-alive should be provisioned, and default to 1 minute (which must be less than the TLS timeout period) intervals during periods of inactivity. Since OPTIONS requires an exchange of messages, only one member of a pair of “adjacent” SIP elements need initiate OPTIONS towards the other.

#### **4.1.2.4 ACK (acknowledgement)**

The ACK request is used to acknowledge completion of a request. Strictly speaking, there are two cases of ACK, one used for a 2XX series response (which is actually part of a three way handshake, typically INVITE/200 (OK)/ACK) and a non-2XX response, which is a separate transaction. All endpoints in an ESInet will use ACK.

#### **4.1.2.5 PRACK (reliable message acknowledgement)**

The PRACK method is used within systems that need reliable provisional responses (non 100). “Provisional” responses are part of the 1XX series responses, except the general 100 (Trying) response. As an example of when an ESInet SIP element may see a PRACK, see the example in RFC3311 [21] where PRACK is sent by the UAS to reliably send an SDP “offer” to a UAC in an 18X response.

#### **4.1.2.6 MESSAGE (text message)**

The MESSAGE method, an extension to SIP, allows the transfer of Instant Messages and is also used to carry a Common Alerting Protocol (CAP) message. Since the MESSAGE request is an extension to SIP, it inherits all the request routing and security features of that protocol. MESSAGE requests carry the content in the form of MIME body parts. MESSAGE requests do not themselves initiate a SIP dialog; under normal usage each Instant Message stands alone, much like pager messages. MESSAGE requests may also be sent in the context of a dialog initiated by some other

SIP request, for example in a multi-media call. For more information on MESSAGE please refer to RFC 3428 [21]. MESSAGE is part of the SIP/SIMPLE presence and messaging system.

#### **4.1.2.7 INFO**

The INFO method is used for communicating mid-session signaling information along the signaling path for a call. INFO is not recommended for use within the ESIInet.

#### **4.1.3 Methods used within the ESIInet**

##### **4.1.3.1 REGISTER (Call Taker to PSAP “login”)**

As defined in RFC 3261 [12], any PSAP UA must register with a SIP registrar server within their domain to ensure that emergency calls can be delivered to them.

##### **4.1.3.2 SUBSCRIBE/NOTIFY (Events)**

Subscribe/Notify is a mechanism to implement asynchronous events notification between two elements. The mechanism is used in i3, for example, to request current state and updates to state from a remote element. SUBSCRIBE requests should contain an "Expires" header. This “Expires” value indicates the duration of the subscription. In order to keep subscriptions effective beyond the duration communicated in the "Expires" header, subscribers need to refresh subscriptions on a periodic basis using a new SUBSCRIBE message on the same dialog. The subscription also expires in the origination network when the associated SIP dialogue is terminated with a BYE

NOTIFY messages are sent to inform subscribers of changes in state to which the subscriber has a subscription. Subscriptions are typically put in place using the SUBSCRIBE method; however, it is possible for other means to be used. A NOTIFY message does not terminate its corresponding subscription. A single SUBSCRIBE request may trigger several NOTIFY requests.

For further information refer to RFC3265 [17] Section 7.1

##### **4.1.3.3 PUBLISH (update of presence information to presence server)**

PUBLISH is a SIP method for publishing event state. The PUBLISH method allows the user to create, modify and remove state in another entity which manages this state on behalf of the user. The request URI of a PUBLISH request is populated with the address of the resource for which the user wishes to publish event state. The body of a PUBLISH request carries the PUBLISH event state. For more information refer to RFC 3911 [41].

#### **4.1.4 Headers assumed supported at the interface to the ESIInet**

All SIP elements within an ESIInet should support Robust Header Compression (ROHC) [145]. BCF’s must support ROHC.

Note: The phoneBCP document referenced in this section contains text normative on devices and service providers. The i3 document considers only the interface between an origination network and the ESIInet. References to phoneBCP in this document are limited to requirement ED-63, the details of signaling for an emergency call. Accordingly, it shall be explicitly understood that all requirements referenced from the IETF phoneBCP document, regardless of wording and context in that document, shall apply only to the ESIInet interface and shall in no way constrain or limit the

signaling and procedures used by end devices, access networks, and originating networks when not interacting with the ESInet.

<b>Header</b>	<b>Defined In</b>	<b>See Section (or Phonebcp)</b>	<b>Notes</b>
To	RFC3261 Section 8.1.1.2 & 20.39	ED63 2.	Usually sip:911 or urn:service:sos
From	RFC3261 Section 8.1.1.3 & 20.20	ED63 3.	Content cannot be trusted unless protected by an Identity header
Via	RFC3261 Section 8.1.1.7 & 20.42	ED63 4.	Occurs multiple times, once for each SIP element in the path
CSeq	RFC3261 Section 8.1.1.5 & 20.16		Defines the order of transactions in a session
Call-Id	RFC3261 Section 8.1.1.4 & 20.8		NOT the NG9-1-1 call id
Contact	RFC3261 Section 8.1.1.8 & 20.10	ED63 6.	Usually a “globally routable user agent URI” (gruu)
Content-Length	RFC3261 Section 20.14		
Content-Type	RFC3261 Section 8.2.3 & 20.15		Used in, for example, in RFC4119 and RFC4566 <sup>4</sup>
Geolocation	draft-sipcore-location-conveyence	ED63 9.	
History-Info	RFC4244		Indicates call has been retargeted
P-Asserted-Identity Reason	RFC3325 RFC3326		When present, overrides From  Used with History Info to specify why a call was retargeted
Route Supported	RFC3261 Section 20.34 RFC3261 Section 8.1.1.9 &	ED63 5. ED63 8.	Usually ESRP/PSAP URI

<sup>4</sup> Examples may include application/pidf+xml to indicate a PIDF-LO in the body of the message and application/sdp to indicate use of Session Description Protocol (SDP) in the body of the message.

Replaces	20.37 RFC3891	5.7	Used with transfer
----------	------------------	-----	--------------------

#### 4.1.5 Headers Accepted and also used internally

Header	Defined In	Section	Notes
Max-Forwards	RFC3261 20.22		Specifies the maximum number of SIP elements that may be traversed before assuming a routing loop has occurred
Accept	RFC3261 20.1		
Content-Encoding	RFC3261 20.12		
Accept-Encoding	RFC3261 20.2		
Content-Language	RFC3261 20.13		
Accept-Language	RFC3261 20.3		
Content-Disposition	RFC3261 20.11		
Record-Route	RFC3261 20.30		
Allow	RFC3261 20.5		
Unsupported	RFC3261 20.40		
Require	RFC3261 20.32		
Proxy Require	RFC3261 20.29		
Expires	RFC3261 20.19		
Min-expires	RFC3261 20.23		
Subject	RFC3261 20.36		
Priority	RFC3261 20.26		
Date	RFC3261 20.17		
Timestamp	RFC3261 20.38		
Organization	RFC3261 20.25		
User-Agent	RFC3261 20.41		
Server	RFC3261 20.35		
Authorization	RFC3261 20.7		
Authentication-Info	RFC3261 20.6		
Proxy-Authenticate	RFC3261 20.27		
Proxy-Authorization	RFC3261 20.28		
WWW-Authenticate	RFC3261 20.44		

Warning	RFC3261 20.43	
Call-Info	RFC3261 20.9	Used to carry URIs to Additional Call/Caller data
Error-Info	RFC3261 20.18	
Alert-Info	RFC3261 20.4	
In-Reply-To	RFC3261 20.21	
MIME-Version	RFC3261 20.24	
Reply-To	RFC3261 20.31	
Retry-After	RFC3261 20.33	
RAck	RFC3262 7.2	
RSeq	RFC3262 7.1	
Event	RFC3265 7.2.1	
Allow Events	RFC3265 7.2.2	
Subscription-State	RFC3265 7.2.3	
Resource	RFC4412 3.1	
Priority	Section 4.1.6	

#### 4.1.6 Resource Priority

The resource priority header (RFC4412) is used on SIP calls to indicate priority that proxy servers give to specific calls. All SIP user agents that place calls within the ESInet must be able to set Resource Priority. All SIP proxy servers in the ESInet must implement Resource Priority and process calls in priority order when a queue of calls is waiting for service at the proxy server and, where needed, pre-empt lower priority calls<sup>5</sup>. BCFs must police Resource Priority for incoming SIP calls. Calls that appear to be 9-1-1 calls must be marked with a provisioned Resource Priority, which defaults to esnet.1. PSAP callbacks during handling of an incident use esnet.0. Callbacks outside of an incident are not marked. ESInets normally use the esnet namespace. The use of the namespace in an ESInet is defined as:

esnet.0	Calls which relate to an incident in progress, but whose purpose is not
---------	---

<sup>5</sup> Mechanisms such as DiffServ are likely to be sufficient to assure that high priority traffic gets through an ESInet. Preemption is unlikely to be needed, even for very high priority responder traffic, and should not be used for 9-1-1 calls. However, if responders need resources, lower priority traffic may have to be cleared to provide such resources. Preemption is considered a necessary prerequisite to getting police and fire responders on an ESInet. Originating network operators have expressed concerns over preemption especially for 9-1-1 calls.



	critical
esnet.1	9-1-1 calls traversing the ESInet
esnet.2	Calls related to an incident in progress which are deemed critical
esnet.3- esnet.7	not defined

#### 4.1.7 History-Info and Reason

When a call is not sent to the originally intended destination: for example, when it is diverted by the ESRP to another PSAP, the final destination must have the ability to know why it got the call. For this reason, SIP elements in the ESInet must support the History-Info header (RFC4244 [44]) and the associated Reason header (RFC3326 [22]). Elements which retarget a call must add a History-Info header indicating the original intended recipient, and the reason why the call was retargeted. ESInet elements must be prepared to handle a History-Info (and its associated Reason header) added by an element outside the ESInet before presentation to the 9-1-1 system.

#### 4.1.8 Media

All call handling elements must support media using RTP (RFC3550 [13]). Each SIP session initiation message or response should describe the media the User Agent is capable of supporting using Session Description Protocol (SDP) (RFC4566 [14]) in the body of the message. Support of any type of media (e.g., voice, video, text) in originating networks is based on regulatory requirements or business decisions. All elements in the ESInet support all media if offered, except that a legacy PSAP on a Legacy PSAP Gateway may only support audio and TTY.

##### 4.1.8.1 Audio

All User Agents in the ESInet must support g.711 mu-law and a-law. A-law support is required in the case that devices manufactured primarily for non-North American markets is used within North America. It is recommended that AMR, AMR-WB, EVRC[138], EVRC-B[139], EVRC-WB[140], and EVRC-NW[141] also be supported.

##### 4.1.8.2 Video

All User Agents in the ESInet must support H.264/MPEG-4 Version 10 video. The Baseline profile must be supported. Scalable baseline profile support is recommended. At least levels 1-3 must be supported.

##### 4.1.8.3 Real-Time Text

All call handling elements in the ESInet must support Framework for Real-Time Text over IP Using the Session Initiation Protocol (SIP) (RFC5194 [117]).

##### 4.1.8.4 TTY (Baudot tones)

NG9-1-1 anticipates that deaf and hard of hearing callers will migrate from TTY to other forms of communication including real time text devices and various forms of relay. Although use of TTY is

expected to decline, it cannot be assumed that TTY will be completely gone by the time transition to NG9-1-1 is complete. Therefore, PSAPs must be capable of receiving calls from TTYs.

It is possible to have a transcoder in the path of every voice call which would recognize baudot tones, and replace them with RFC4103 [118] real time text on incoming (with respect to the ESInet) RTP media, and terminate RFC4103 real time text and synthesize baudot tones for outgoing RTP. If an ESInet can assure that ALL calls, including diverted calls, calls transferred from another ESInet and all calls from any origination network will pass through the transcoder, such an architecture is acceptable. The transcoder must be compliant with RFC5369 [119]. Where all calls are answered at a bridge, the bridge can provide the transcode service. It may be practical to place a transcoder at the edge of a PSAP to serve all endpoints inside that PSAP.

For ESInets where it cannot be assured that all audio calls will transit such a transcoder, the PSAP User Agents, conference bridges, Interactive Media Response units, etc. will need to recognize baudot tones and display text, as well as accept typed text and generate baudot tones.

#### 4.1.9 Instant Messaging

Text-based communications for NG9-1-1 by all call handling elements of an NG9-1-1 system, is supported in two ways: Real-Time Text (RTT) and Instant Messages (IM) with location and the ability to support location updates.

Note: there is considerable flux in standardized Instant Messaging protocols. It is anticipated that there may be additional IM protocols supported by NG9-1-1 in the future, specifically XMPP. At this time, the only standardized IM protocol fully specified for supporting emergency IMs within or presented to an ESInet is SIP/SIMPLE.

All call handling elements within the ESInet must support Session Initiation Protocol (SIP) Extension for Instant Messaging (RFC3428 [21]), Indication of Message Composition for Instant Messaging (RFC3994 [120]), The Message Session Relay Protocol (MSRP) (RFC4975 [121]) and Relay Extension for the Message Session Relay Protocol (MSRP) (RFC4976 [122])<sup>6</sup>. PSAPs must be prepared to handle IM as a series of individual MESSAGE transactions as well as a message session via MSRP. MESSAGES received from the same caller within a configurable time (2-3 minutes nominally) should be considered part of the same “call”, and must be routed to the same PSAP (and the same call taker), regardless of movement of the caller while texting. If the origination network/device supports non session mode IM to NG9-1-1, it must assure that all messages from the same caller within this time frame is sent to the same ESInet (same ECRF query results). If the network/device cannot guarantee this, it must use session mode. The ESRP in the

---

<sup>6</sup> All ESInet elements support instant messaging using the specifications in this document. Any given origination network or device may not support instant messaging, and support of instant messaging by origination networks and devices may be subject to regulation.

ESInet will also maintain a timer for this function and assure that all messages from the same caller that route to an ESInet will route to the same PSAP.

Location must be included in a geolocation header in the MESSAGE method or the initiation of the MSRP session as with any other “call” to 9-1-1.

Other Instant Messaging protocols such as XMPP may be supported by an originating network, but must be interworked to SIP IM for presentation to the ESInet. For example, draft-saintandre-sip-xmpp-im-01 [110] describes interwork between XMPP and SIP IM.

#### 4.1.10 Non-human-initiated calls

Non-human-initiated calls presented to an ESInet are signaled with a SIP MESSAGE method containing a Common Alerting Protocol (CAP) [95] message, possibly wrapped in an Emergency Data eXchange Language – Distribution Element (EDXL-DE) [111] wrapper<sup>7</sup>. The <area> element of the CAP message is copied, in PIDF-LO form, in a Geolocation header in the MESSAGE container. The CAP message is in the body of the MESSAGE, with MIMEtype **application/common-alerting-protocol+xml**.

The MESSAGE should contain a Call-Info header with a URI of an Additional Data about a Call object.

The <identifier> in the CAP message is not the same as the Call Identifier assigned in the ESInet, but the log contains the record that relates the two.

The <sender> should be the same as the From header in the MESSAGE.

If included, the <addresses> element should contain “urn:service:sos”, the same as the Route header for the Message.

An <info> element must be included. The element must contain an <event code>. The <valueName> may be some externally defined namespace, but in many cases is expected to be “NENA”. This document defines a NRS registry of allowed values for “NENA-ExternalEventCodes” which registers values that may be used in an <event code> where <valueName> is “NENA”. The initially defined values in the registry (which become the <value> contents in the <event code> element) are VEDS and BISACS, representing the standard Vehicle Emergency DataSet, and the NIST Building Information and Control System messages.

If an <area> element is included, at least one <polygon> or <circle> element must be included. Any <areaDesc> and <geocode> elements will not be used by the routing elements, although destination

---

<sup>7</sup> All ESInet elements support non-human-initiated calls using the specifications in this document. Any given origination network or device may not support non-human-initiated calls, and support of non-human-initiated calls by origination networks and devices may be subject to regulation.

agencies may be able to make use of them. The Geolocation header in the MESSAGE must have the PIDF-LO equivalent of the <polygon> or <circle> element(s). If <altitude> and <ceiling> is provided, they will be used for routing if the ECRF is provisioned with 3D data.

A digital signature should be included in the CAP message. The CAP message should not be encrypted. Transport Layer Security (TLS) may be used on the SIP MESSAGE transmission to encrypt the message.

The CAP message may be enclosed in an EDXL-DE wrapper. If it is, the body of the SIP MESSAGE will contain a section application/emergency-data-exchange-language+xml.

Non-human-initiated calls are routed and handled the same as voice, video or text calls throughout the NG9-1-1 system. The routing mechanisms can route non-human-initiated calls differently from voice calls in the same way they can route video calls differently from voice calls. The parameters in the CAP message are available to the routing function as inputs to direct calls with specified characteristics to specific entities.

Note that in this edition, there is no mechanism specified to handle an APCO/CSAA 2.101.1-2008 Alarm within the ESInet, although a PSAP could have an interface to such an alarm.

#### **4.1.11 Bodies in messages.**

All SIP elements in an ESInet must support multipart MIME as defined in RFC2046 [123]. For example, location and SDP may be present in a message body. All SIP elements must allow additional body content (for example, images, vcards, etc) to pass to the PSAP. Note that the typical length of a SIP INVITE is around 1300 bytes including around 200 bytes for the SIP Header overhead. If, for example, a SIP INVITE contains a complete header, and a body containing both an SDP and a civic PIDF-LO, it is likely this SIP message may be too big for UDP; and may require the use of TCP.

#### **4.1.12 Transport**

SIP signaling within the ESInet must be TCP with TLS. Fallback to UDP is allowed. However emergency call messages have many large elements, for example, a PIDF-LO, and are more likely to be fragmented when carried in UDP. Fragmentation and reassembly must be supported by all ESInet elements. If TLS establishment fails, fallback to TCP/UDP without TLS is allowed. If fallback with TLS is allowed, additional security weaknesses occur, and implementations must be prepared to deal with the security risks engendered when TLS protection is not available. Known attacks on incomplete fragmentation/reassembly implementations are another concern which must be addressed by all elements in the ESInet. Persistent TLS connections between elements that frequently exchange SIP transactions should be deployed. Media streams for voice, video and text must be carried on RTP over UDP. All endpoints in an ESInet must implement media security with SRTP as defined in RFC3711 [125] and SDES as defined in RFC4568 [126]. SRTP Security must be requested in all calls originated within an ESInet. Since media is routinely logged, the logger must be given the keys to enable it to decode the SRTP. RTCP as defined in RFC3550 [13] and SRTCP as defined in RFC3711 [125] must be supported within the ESInet and it is highly recommended that all calls presented to the ESInet provide RTCP.

PSAPs must detect the presence of RTP streams so they can distinguish RTP failure from real silence by the caller. User Agents who detect the loss of RTP should attempt to reestablish the streams by reINVITING the other party. If that fails, the device should indicate a failure and require the user (call taker in most cases) to take action such as initiating disconnect. In no circumstances should a call be automatically taken down just because RTP streams fail. For example a multimedia stream which loses one of several streams would not be terminated, except by call taker action.

PSAPs should supply audible ring as (early) media for devices that do not perform local audible ring or its equivalent.

#### **4.1.13 Routing**

All SIP elements must support routing of SIP messages per RFC3261 [12] and RFC3263 [15]. Note particularly that URIs will often have the domain of the destination following the ‘@’ rather than the hostname of a sip server, and thus SRV records [107] will need to be consulted to determine the hostname of the sip server for that domain.

#### **4.1.14 Originating network Interface**

The originating call interface to the ESInet is a SIP call interface as described above in section 4.1. All calls are presented to the correct ESInet by routing via an ECRF or equivalent as described in Section 5.3. Location must be included in the Geolocation header, civic or geo, by reference or value. The location used to query the routing function must be included in the Geolocation header of the outgoing INVITE message. The call must be routed, using normal RFC 3261 [12] procedures to the URI obtained from the routing function using the “urn:service:sos” service URN. A callback address must be included in the outgoing INVITE message, with an immediate device callback in the Contact header and an address of record for later callback in either the From header (protected by the Identity header) or a P-Asserted-Identity.

A call from an unauthenticated device shall populate the P-Preferred-Identity header field in the INVITE request with an equipment identifier as a SIP URI and no P-Asserted-Identity shall be provided.

A Call-Info header must be included in the incoming INVITE message to the ESInet that contains a URI that refers to an Additional Data associated with a Call ([127][144]) structure, and marked with an “emergencyCallData” purpose. A Call-Info header may be included which contains a URI which refers to an Additional Data associated with a Caller (NENA 71-001) structure, marked with an “emergencyCallerData” purpose.

#### **4.1.15 PSAP Interface**

The PSAP call interface is a SIP call interface as described in section 4.1. All calls will be presented to the PSAP based on the terminating ESRP’s Policy Routing Function (Section 5.2.1.5). Geolocation header, Call-Info headers and other headers should be the same as above (Section 4.1.14). The call will be routed, using normal RFC 3261 [12] procedures to the URI obtained from the ESRP’s PRF. See Section 5.6.1 for other information on the PSAP interface.

#### 4.1.16 Element Overload

Any SIP element may encounter a condition in which it is asked to process more calls than it can handle. SIP element overload has been extensively studied [114]. Simple mechanisms to handle overload are insufficient. Elements must not return 503 Busy Here unless it is certain, by design and configuration that the upstream element can reliably cope with the error. This standard specifies specific methods to avoid overload of calls to specific agencies using the routing rule and queue mechanisms, but a given SIP element may still encounter overload. To cope with such overload, all SIP elements must implement the overload control mechanisms described in [79]

#### 4.2 Location

Location is fundamental to the operation of the 9-1-1 system. Location is provided outside the ESInet, and the generic functional entity which provides location is a Location Information Server (LIS). Since the LIS is external to the ESInet, and not provided by the 9-1-1 Authority, the LIS is out of scope for i3. However, the entities inside the ESInet must interact with a source of location and thus the interfaces to that function are in scope. For the purposes of this document, the only functions a LIS provides that are relevant to i3 are:

- a) A dereference function defined below for location by reference
- b) A validation function which uses the i3 LVF for civic addresses

Any element that provides either or both of these two functions is considered a LIS within i3. Although a LIS is defined as a “server”, as with all elements defined in this document, there may not be a physical server, and indeed, a LIS for some networks may only be a protocol interwork function to some other element in the network.

The NG9-1-1 system supports location included by value in a Geolocation header [10] of a SIP message. It also supports location by reference. All elements in an ESInet that use location by reference must implement SIP and HTTP Enabled Location Delivery (HELD) dereferencing protocol. A Location Information Servers (LIS)<sup>8</sup> must implement one or both of these protocols.

Location by reference using SIP is an implied subscription to Presence (RFC3856). An element needing location that has a SIP location URI must issue a SIP SUBSCRIBE (RFC3265) to the location URI. The use of filters (RFC4661 [128], rate control [113] and loc-filters [129]) may be used to control notification.

An element needing location that has a HELD URI must dereference per draft-winterbottom-geopriv-deref-protocol [78].

---

<sup>8</sup> A LIS, if it implements the SIP Subscribe/Notify mechanisms for location dereferencing, implements these portions of Presence server as defined in the IETF for the purposes of returning the location information only.

An access network that provides location by reference must supply either a SIP or a HELD location reference URI per section 4.2. Networks that use other protocols must interwork to SIP or HELD. Elements in the ESInet which receive a location reference and forward location in SIP signaling to another element must pass the reference, and not any value it determines by dereferencing (although the value should be logged). Each element must do its own dereference operation, supplying its credentials to the LIS. It is recommended that LISs cache location values and supply the cached values if multiple dereferences occur in quick succession, such as when a call is being routed.

The LIS must accept the ESRP and PSAP credentials traceable to the PSAP Credentialing Authority (PCA) to deliver location with the required confidence/uncertainty.

Other than the above, the implementation used within the origination and access networks for support of location is out of scope of i3<sup>9</sup>.

### 4.3 Provisioning

The i3 standard provisioning mechanism is Service Provisioning Markup Language, Version 2.0 (SPML 2.0 [91]).

In i3, the SPML roles and definitions are applied and associated with functional entities as follows:

**Target:** Each i3 service (including each BCF, ESRP, ECRF and LVF) would be a Provisioning Service Target (PST or Target) and is identified by a TargetID.

**Provider:** the software component included by each service on an ESInet that is responsible for processing SPML requests.

**Requesting Authority (RA):** the requestor in i3 is typically controlled by a PSAP, 9-1-1 Authority or state/county authority) that issues a SPML request to a Provisioning Service Provider (PSP).

**Provisioning Service Provider (PSP):** controlled by functional entity service provider and listens for a well-formed SPML request, processes the request, and returns the results to the RA. It provisions Targets.

**Provisioning Service Object:** A data entity or an information object on a target.

**Note:** A future edition of this document will contain descriptions of the Provisioning Service Objects (PSOs) defined for standard functions.

The transport for SPML is SOAP/XML. PSOs are identified by PSOIdentifiers.

---

<sup>9</sup> The roles of the access and origination networks in obtaining location for routing and delivery with an emergency call, and interactions between such networks is out of scope and subject to SDO work outside NENA as well as regulatory policy.

Most Providers are expected to use the SPMLv2 XSD Profile. Providers and Requestors must be capable of handling synchronous and asynchronous operations. Batch capability must be supported on all Providers and Requestors.

In SPML, RequestID sent from Requestor to Provider is optional for a synchronous request using transports such as SOAP/XML who have mechanisms to match requests with responses. However, for NG9-1-1, most provisioning requests will be logged, and the RequestID is used in the log entry. Therefore, all requests must contain a unique RequestID.

TargetIDs and PSIdentifiers must use a Globally Unique IDs (GUIDs).

#### **4.4 Policy**

Policy is stored into and retrieved from the Policy Store using a web service. This section describes the "Policy Store Web Service" in Section 4.4.1 that allows to upload and to retrieve policies. Policies are named by the function that defines the policy, i.e., the DownstreamRoutingPolicy for an ESRP. A specific policy set is known by that name and the agency whose policy is being stored or retrieved. The authentication to the web service identifies the agency storing or retrieving policy sets in the store.

The store only accepts or delivers complete policy sets, not individual rules within a policy set. The policy store may reduce the size of the chunk returned if it is unable or unwilling (by local policy) to serve a chunk as large as the requester specifies. The policy retrieved is valid until the expiration time. If the policy is needed for use after expiration, it must be retrieved again from the policy store. The response may not return the policy requested. Instead, it may return a referral to another policy store that may have the policy.

The standard i3 data rights management system can limit which agencies, agents or functions are permitted to retrieve policies for another agency. The rights management policy can also allow an agency to store policies on behalf of another agency. The interface includes a chunking mechanism that can be used by either the client or the server to limit the size of an individual transaction.

##### **4.4.1 Policy Store Web Service**

This web service has the following functions:

**RetrievePolicy:** retrieves a policy set from the common policy store. The function's parameters include the policy name, the identity of the agency whose policy is needed, and an indication of the maximum size of the return. The response is the policy set, if it is smaller than the indicated maximum size, or the first chunk of the policy set if it is large, plus an identifier that can be used with **MoreRetrievePolicy** to obtain more chunks of a large policy set if the policy is too large to send in the response, and an expiration time. The policy store may reduce the size of the chunk returned if it is unable or unwilling (by local policy) to serve a chunk as large as the requester specifies. The policy retrieved is valid until the expiration time. If the policy is needed for use after expiration, it must be retrieved again from the policy store. The response may not return the policy requested. Instead, it may return a referral to another policy store that may have the policy.

RetrievePolicyRequest

Parameter	Condition	Description
policyName	Mandatory	The name of the policy
agency	Mandatory	The agency whose policy is requested. Must be a domain name or URI that contains a domain name
maxChunkSize	Optional	Maximum size of a chunk accepted, in bytes. If not specified, responder may choose the size.

RetrievePolicyResponse

Parameter	Condition	Description
policyDataChunk	Optional	All or part of a policy, limited to the maxChunkSize, or smaller
TTL	Optional	The expiration time of the policy
nextChunkId	Optional	Id to be used with MoreRetrievePolicy. Must be present if policyDataChunk is returned, but is not the complete policy
Referral	Optional	URI of another policy store that may have this policy.
errorCode	Optional	Error Code if no policy or referral is returned

Error Codes

- 100    Okay    No error (optional to return)
- 501    Unknown or bad Policy Name
- 502    Unknown or bad Agency Name
- 503    Not available here, no referral available

504 Unspecified Error

**MoreRetrievePolicy:** retrieves another chunk of a large policy set. The request includes the identifier returned to the requester in a **RetrievePolicy** or prior **MoreRetrievePolicy** operation and an indication of the maximum size of the return. The response is the next chunk of the policy set, plus an identifier that can be used on a subsequent invocation of **MoreRetrievePolicy**. The policy store may reduce the size of the chunk returned if it is unable or unwilling (by local policy) to serve a chunk as large as the requester specifies. The policy store must be able to accept and respond to a request it has already sent (that is, the identifiers may be used repeatedly, in case of error). The identifiers can be expired in a reasonable time period (perhaps 30 minutes).

**MoreRetrievePolicyRequest**

Parameter	Condition	Description
nextChunkId	Mandatory	ChunkId returned from <b>RetrievePolicy</b>
maxChunkSize	Optional	Maximum size of a chunk accepted, in bytes. If not specified, but maxChunkSize was specified in <b>RetrievePolicy</b> , use that size. If neither specified, responder may choose size.

**MoreRetrievePolicyResponse**

Parameter	Condition	Description
policyDataChunk	Mandatory	Remainder or part of a policy, limited to the maxChunkSize, or smaller
nextChunkId	Optional	Id to be used with <b>MoreRetrievePolicy</b> if not the last chunk
errorCode	Optional	Error Code if no policy or referral is returned

Error Codes

- 100 Okay No error (optional to return)
- 504 Unspecified Error
- 505 Bad chunkId

**StorePolicy:** initiates the storage of a policy set in the policy store. This function’s parameters include the name of the policy, the agency whose policy is being stored, the size of the entire policy set, the expiration time, and the maximum chunk size the sender is willing to send. If the name of the agency is omitted, the sender’s identity is used. The response contains the maximum size of the initial chunk, which must be no larger than the sender’s maximum chunk size, and an identifier to be used with the MoreStorePolicy function.

**StorePolicyRequest**

<b>Parameter</b>	<b>Condition</b>	<b>Description</b>
policyName	Mandatory	The name of the policy
agency	Mandatory	The agency whose policy is being stored. Must be a domain name or URI that contains a domain name
policySize	Mandatory	Size of the entire policy in bytes
TTL	Mandatory	The expiration time of the policy
maxChunkSize	Optional	Maximum size of a chunk to be sent, in bytes. If not specified, responder may choose the size.

**StorePolicyResponse**

<b>Parameter</b>	<b>Condition</b>	<b>Description</b>
maxChunkSize	Optional	Maximum size of a chunk accepted, in bytes. If not specified, sender may choose the size up to the maxChunksize specified in the request.
nextChunkId	Optional	Id to be used with MoreStorePolicy.
errorCode	Optional	Error Code

**Error Codes**

- 100    Okay    No error (optional to return)
- 501    Unknown or bad Policy Name
- 502    Unknown or bad Agency Name

- 504 Unspecified Error
- 506 Policy Too Large
- 507 Bad TTL

MoreStorePolicy: sends a chunk of the policy set to the store. Its parameters include the identifier returned from StorePolicy or a prior invocation of MoreStorePolicy, and a chunk of the policy set. The response contains the maximum size of the next chunk (which must be no larger than the maximum chunk size indicated by the sender on the original StorePolicy invocation) and an identifier to be used on a subsequent MoreStorePolicy to send the next chunk. Identifiers may be reused, but if they are, any later chunks are discarded by the store and must be re-sent. Identifiers may be expired in a reasonable time (perhaps 30 minutes).

MoreStorePolicyRequest

Parameter	Condition	Description
nextChunkId	Mandatory	ChunkId returned from RetrievePolicy
policyDataChunk	Mandatory	All or part of a policy, limited to the maxChunkSize, or smaller

MoreStorePolicyResponse

Parameter	Condition	Description
maxChunkSize	Optional	Maximum size of a chunk accepted, in bytes. If not specified, but maxChunkSize was specified in the StorePolicyRequest, use that size. If neither is specified, responder may choose size.
nextChunkId	Optional	Id to be used with MoreRetrievePolicy if not the last chunk
errorCode	Optional	Error Code if no policy or referral is returned

Error Codes

- 100 Okay No error (optional to return)

- 504 Unspecified Error
- 505 Bad chunkId
- 508 Chunk Too Big

EnumeratePolicies: returns a list of policy names available in the store for a specific agency. The parameters of the request include the name of the policy set and the name of the agency. The response includes a list of the policy names in the store, the last date they were stored, expiration time, and the size of the policy. The enumeration includes only those policies that are actually stored in this specific instance of the policy store.

EnumeratePoliciesRequest

Parameter	Condition	Description
policyName	Mandatory	The name of the policy. May be "*" for all policy names
Agency	Mandatory	The agency of interest. Must be a domain name or URI that contains a domain name or "*" for all agencies

EnumeratePoliciesResponse (may be repeated for each policy)

Parameter	Condition	Description
policyName	Mandatory	The name of the policy.
Agency	Mandatory	The agency of interest. Must be a domain name or URI that contains a domain name
policySize	Mandatory	Size of the entire policy in bytes
TTL	Mandatory	The expiration time of the policy
lastModification	Mandatory	Date/Time of last modification
errorCode	Optional	Error Code if no policy

Error Codes

- 100 Okay No error (optional to return)

- 501 Unknown or bad Policy Name
- 502 Unknown or bad Agency Name
- 504 Unspecified Error

The policy store is replicated and distributed. There is a single authoritative master store for a given policy, and there may be one or more replicas of that policy in other policy stores. To create a replica, the master policy store is provisioned with a list of replicas that are authorized. The replica uses the RetrievePolicy function to get policies from the master policy store, and refreshes them automatically when they expire. EnumeratePolicies can be used to determine which agency’s policies are stored in the policy store.

As an optimization, the replica can make use of the UpdatedPolicy function:

UpdatedPolicies: returns a list of policies updated in the Policy Store since a given time. The request includes a timestamp. The response is a list of policy names and agencies whose policy has been updated since the timestamp in the request.

UpdatedPoliciesRequest

Parameter	Condition	Description
policyName	Mandatory	The name of the policy. May be “*” for all policy names
agency	Mandatory	The agency of interest. Must be a domain name or URI that contains a domain name or “*” for all agencies
updatesSince	Mandatory	Earliest time desired in the response

UpdatedPoliciesResponse (may be repeated for each policy)

Parameter	Condition	Description
policyName	Mandatory	The name of the policy.
agency	Mandatory	The agency of interest. Must be a domain name or URI that contains a domain name
policySize	Mandatory	Size of the entire policy in bytes
TTL	Mandatory	The expiration time of the policy

lastModification	Mandatory	Date/Time of last modification
errorCode	Optional	Error Code if no policy

Error Codes

- 100     Okay    No error (optional to return)
- 501     Unknown or bad Policy Name
- 502     Unknown or bad Agency Name
- 504     Unspecified Error

UpdatedPolicies can be used as a poll to keep a more up to date replica, rather than waiting for expiration times. Use of UpdatedPolicies is recommended for replicas of policies that may reasonably be changed unexpectedly, such as in a disaster situation.

The EnumerateAgencies function is also useful to maintain a referral service to distribute the policy store. Policy stores may refer queries to another policy store. To do so, they maintain a map of which policy stores have what policies. The mapping may be provisioned or learned via the EnumerateAgencies function (with a list of other policy stores provisioned in a specific policy store).

**4.4.2 Policy Syntax**

This section summarizes the syntax and semantic of the policy language used for making call routing decisions. Policy is represented in an RFC4745 [147] compliant common policy schema.

A policy document is an XML document, formatted according to the schema defined in RFC 4745. This document inherits the MIME type of common policy documents, namely application/auth-policy+xml. As described in RFC4745, this document is composed of rules that contain three parts - conditions, actions, and transformations. The condition statement may either evaluate to 'true' or 'false'. If it evaluates to 'true' then the action, and the transformation part of the rule is executed. In order to deal with the case where multiple condition parts evaluate to 'true' a conflict resolution mechanism is described to avoid conflicting actions to be executed. Common Policy described a conflict resolution and this document extends Common Policy with a priority based mechanism whereby each rules has a priority value associated that indicates the relative importance of the specific rule with the semantic that a higher value gets precedence over a rule with a lower value. The transformations part of a rule is not used by this application.

**4.4.2.1 Condition Elements**

This section describes the additional enhancements of the conditions-part of the rule. This document inherits the Common Policy functionality, including <validity>. The <identity> and <sphere> condition is not used by this version of the document.



#### 4.4.2.1.1 Time Period Condition

The <time-period> element allows a rule to make decisions based on the time, date and time zone. It defines an extended version of the <validity> element. The <time-period> element may contain the following attributes:

dtstart: Start of interval (timestamp, see Section 3.2). This attribute is mandatory.

dtend: End of interval (timestamp). This attribute is mandatory.

timestart: Start of time interval in a particular day. It is of the TIME data type as mentioned in Section 4.3.12 of RFC 2445. Time is local time at the PSAP, including daylight savings. This attribute is optional. The default value is 000000.

timeend: End of time interval in a particular day. It is of the TIME data type as mentioned in Section 4.3.12 of RFC 2445. Time is local time at the PSAP, including daylight savings. This attribute is optional. The default value is 235959.

byweekday: List of days of the week. This attribute is optional.

The <time-period> is based on the description in CPL but with a reduced feature set.

The "dtstart" and "dtend" attributes are formatted as i3 timestamps.

The "timestart" specifies a time value to indicate the beginning of every day. The default value is 000000 representing the beginning of the day.

The "timeend" specifies a time value to indicate the end of every day. The default value is 235959 representing the end of the day.

The "byweekday" attribute specifies a comma-separated list of days of the week. "MO" indicates Monday, "TU" indicates Tuesday, "WE" indicates Wednesday, "TH" indicates Thursday, "FR" indicates Friday, "SA" indicates Saturday, and "SU" indicates Sunday. These values are not case-sensitive.

Here is an example of the time-period element.

```
<time dtstart="20070112T083000+05"  
      timestart="0800"  
      timeend="1800"  
      byweekday="MO,TU,WE,TH,FR"  
      dtend="20080101T183000+05"/>
```

The following aspects need to be considered:

1. By default, if all the OPTIONAL parameters are missing, <time-period> element is valid for the whole duration from 'dtstart' to 'dtend'.

2. The 'byweekday' attribute comes into effect only if the period from 'dtstart' till 'dtstart' is long enough to accommodate the specified values, else they are just neglected.
3. If the values of the 'byweekday' attribute values do not correspond to the expected domain, they are simply ignored.
4. Only a single 'byweekday' attribute MUST be listed in a <time> element.

#### 4.4.2.1.2 SIPHeader Element

Any header in a SIP message, such as the From, To, Contact etc., can be used to perform actions on incoming messages. The <SIPHeader> element has three child elements, namely <header>, <operator> and <content>. Currently, only a single operator is defined, namely an equality match. The defined value is "equal" in the <operator> element.

The semantic of this field is to compare the content of a specific header field with a pre-defined content.

#### 4.4.2.1.3 MIME Body List Condition

The <mime-list> element contains one or more child <mime> child elements. Any mime type listed in the <mime> element is compared with the content of the incoming message.

The <mime-list> condition element evaluates to TRUE if any of its child elements evaluate to TRUE, i.e., the results of the individual child element are combined using a logical OR.

#### 4.4.2.1.4 Location Conditions

This document re-uses the location-based condition elements from ietf-geopriv-policy [146].

#### 4.4.2.1.5 Call Suspicion Condition

This document allows the spam-score header of the SIP message to be evaluated. The <callsuspicion> element has one child element, <score>: which indicates the spam score in the attributes "from" and "to".

#### 4.4.2.1.6 SecurityPosture Condition

The <SecurityPosture> element expressed carries a "domain" attribute where "domain" is a hostname, or a URI. If a URI is specified, the domain function is used to extract the domain from the URI. The domain must be that of an agency or element that the ESRP can subscribe to the SecurityPosture package for.

#### 4.4.2.1.7 QueueState Condition

The <QueueState> element carries a "queue" attribute, where "queue" is the name of a queue. The value of the <QueueState> element can either be:

- Active: one or more entities are actively available or are currently handling calls being enqueued
- DiversionRequested: a queue designated for diversion (i.e., not the normal call path) is having calls enqueued on it.

- Inactive: no entity is available or actively handling calls being enqueued
- Disabled: The queue is disabled by management action and no calls may be enqueued

#### 4.4.2.2 Actions

As stated in [RFC4474], conditions are the 'if'-part of rules, whereas actions and transformations form their 'then'-part. The actions and transformations parts of a rule determine which operations the proxy server MUST execute on receiving a connection request attempt that matches all conditions of this rule. Actions and transformations permit certain operations to be executed.

##### 4.4.2.2.1 Priority

Each rule has to contain an unsigned integer value to indicate its priority in the <priority> element. When the conditions of two rules evaluate to 'true' then the rule with the higher priority value wins, i.e., the actions of that rule will be executed. Every rule MUST have a unique priority value.

##### 4.4.2.2.2 Route Action

The action supported in this section is forwarding of SIP messages to a specific URL. The <route> element contains two child elements namely <recipient> and <causes>, where <recipient> contains a URI that will become the Route header for the outgoing SIP message (the Request URI is normally a service urn), and the <causes> contains the value used with the Reason header associated with a History-Info header. The <recipient> element is mandatory, and the <causes> element is optional.

##### 4.4.2.3 LoSTServiceURN Action

The <LoSTServiceURN> element carries the Service URN (either urn:service:... or urn:ena:service:...) as the value. The resulting URI is a variable called "NormalNextHop", available to the rule evaluation system.

##### 4.4.2.3.1 Busy Action

The <busy> element returns 600 Busy Everywhere to the caller.

##### 4.4.2.3.2 Notify Action

The <notify> element has several child elements (<recipient>, <eventCode>, <urgency>, <severity>, and <certainty>) and sends a NOTIFY message containing a CAP message to any entity subscribing to the Normal-NextHop's ESRPnotify event for that reason code. This may be used, for example, to advise other entities that calls are being diverted, etc. If the <recipient> is a service urn, the CAP message is wrapped in a SIP MESSAGE and is routed via the ECRF to the proper recipients. All indicated child elements provide information on how to populate the CAP message.

##### 4.4.2.4 Examples

```
<?xml version="1.0" encoding="UTF-8"?>
<ruleset xmlns="urn:ietf:params:xml:ns:common-policy"
  xmlns:ena="urn:ena:policy-v1"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

```
; Call is probably spam.
<rule id="AA56i12">
<conditions>
  <na:callsuspicion>
    <na:score from="70" to="100"/>
  </na:callsuspicion>
</conditions>
<actions>
  <priority>7</priority>
<na:route>

<na:recipient>sip:special-treatment@psap.foo-bar.com
  </na:recipient>
</na:route>
</actions>
<transformations/>
</rule>

; Rule for handling a SIP msg contain a CAP payload.
<rule id="AA56i11">
<conditions>
  <na:mime-list>

<na:mime>application/common-alerting-protocol+xml</na:mime>
  </na:mime-list>
</conditions>
<actions>
  <priority>6</priority>
<na:route>
  <na:recipient>sip:psap@home.foo-bar.com
  </na:recipient>
</na:route>
</actions>
<transformations/>
</rule>

; Rule consider time and queue state.
<rule id="AA56i10">
<conditions>
  <na:QueueState>Active</na:QueueState>
```