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

One Nation 9-1-1 One Number

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, Suite750

Arlington, VA 22203-1695

800-332-3911

or: 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

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: admindoccomments@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.

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

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

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

The following Terms and Definitions are used in this document:		
Term	**Definition**	**** N)ew (U)pdate**
Authorization	A security term referring to the process of making a decision regarding what access rights an authenticated entity has to data or a service.	
Code Point	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.	
Denial of Service Attack	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.	
Diffserv	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".	
Emergency Call Routing Function (ECRF)	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.	
Emergency Services IP Network	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).	
H.264	A video codec, defined by ITU-T in common use today for real time two way video.	
Originating ESRP	The first routing element inside the ESInet. It receives calls From the BCF at the edge of the ESInet.	
Session Border Control	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.	
Terminating ERSP	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[1]. 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

[1] 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 that 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[2].

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 $3.4x10^{38}$). 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

[2] 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.[3] 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.[4] 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].[5]

[3] 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.

[4] 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.

[5] 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,

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

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.

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

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 provided 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.

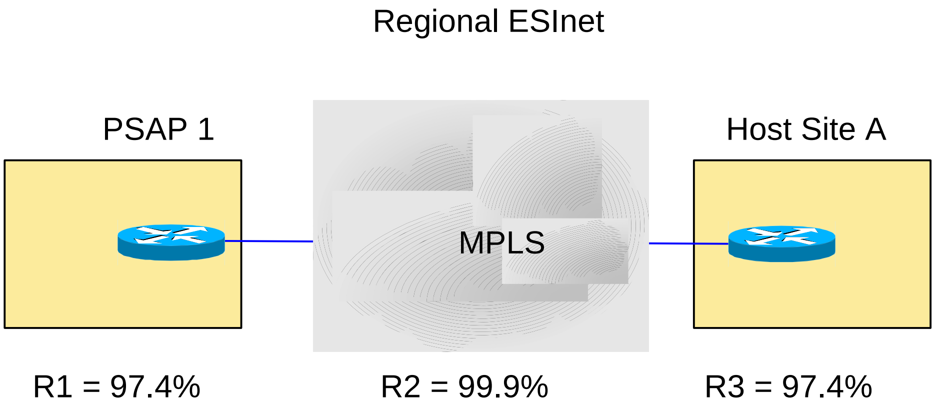
3.4.5 Series and Parallel Reliability and Availability in ESInets

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

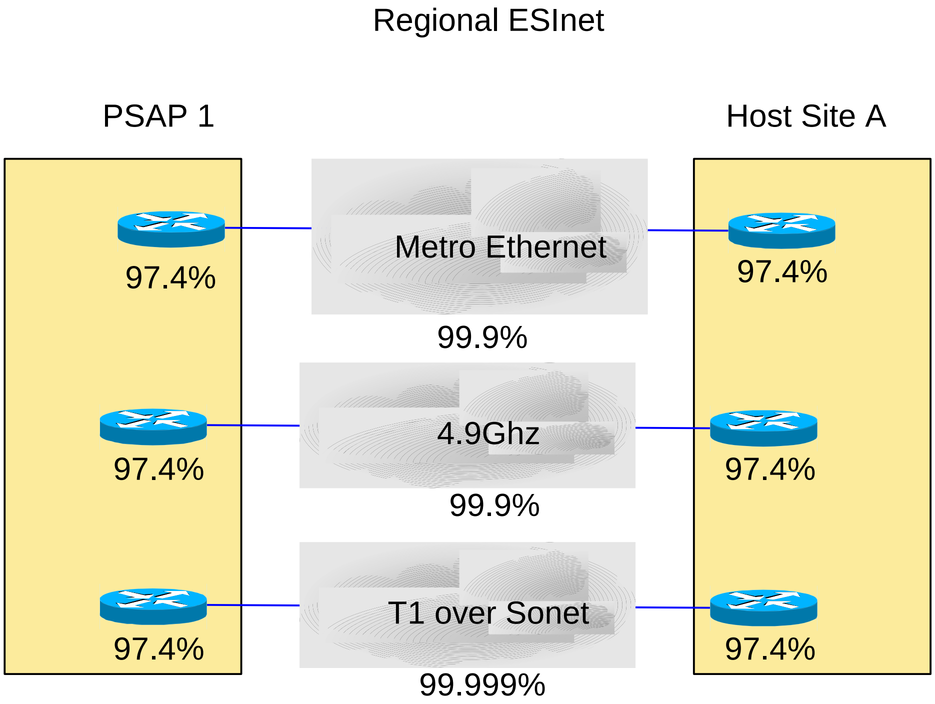
$$R_S = R_1 * R_2 * R_3$$

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:

$$R_P = 1 - ((1\text{-}Rs_1) * (1\text{-}Rs_2) * (1\text{-}Rs_3))$$

Where Rp = Parallel Reliability

and Rs1..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.

$$R_P = 1\text{-}((1\text{-}.948) * (1\text{-}.948) * (1\text{-}.948)) = 1 – (0.052 * 0.052 * 0.052) = 0.99985$$

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.).)

$$R_P = 1 - ((1\text{-}.948) * (1\text{-}.948) * (1\text{-}.948) * (1\text{-}.948))$$

$$= 1 – (0.052 * 0.052 * 0.052 * 0.052)$$

$$= 0.9999927$$

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.

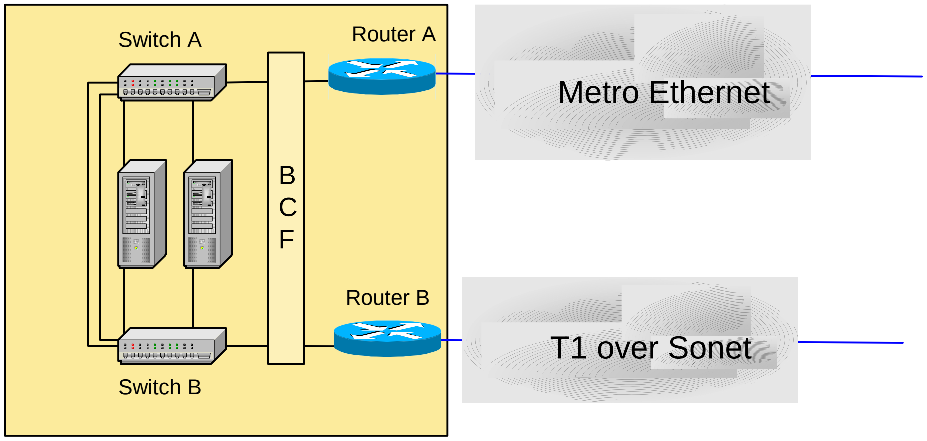
ESInets are complex and may involve management of SLAs from a number of different vendor/service providers. Best practices include:

- 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:

DSCP	**Use**	**PHB**
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

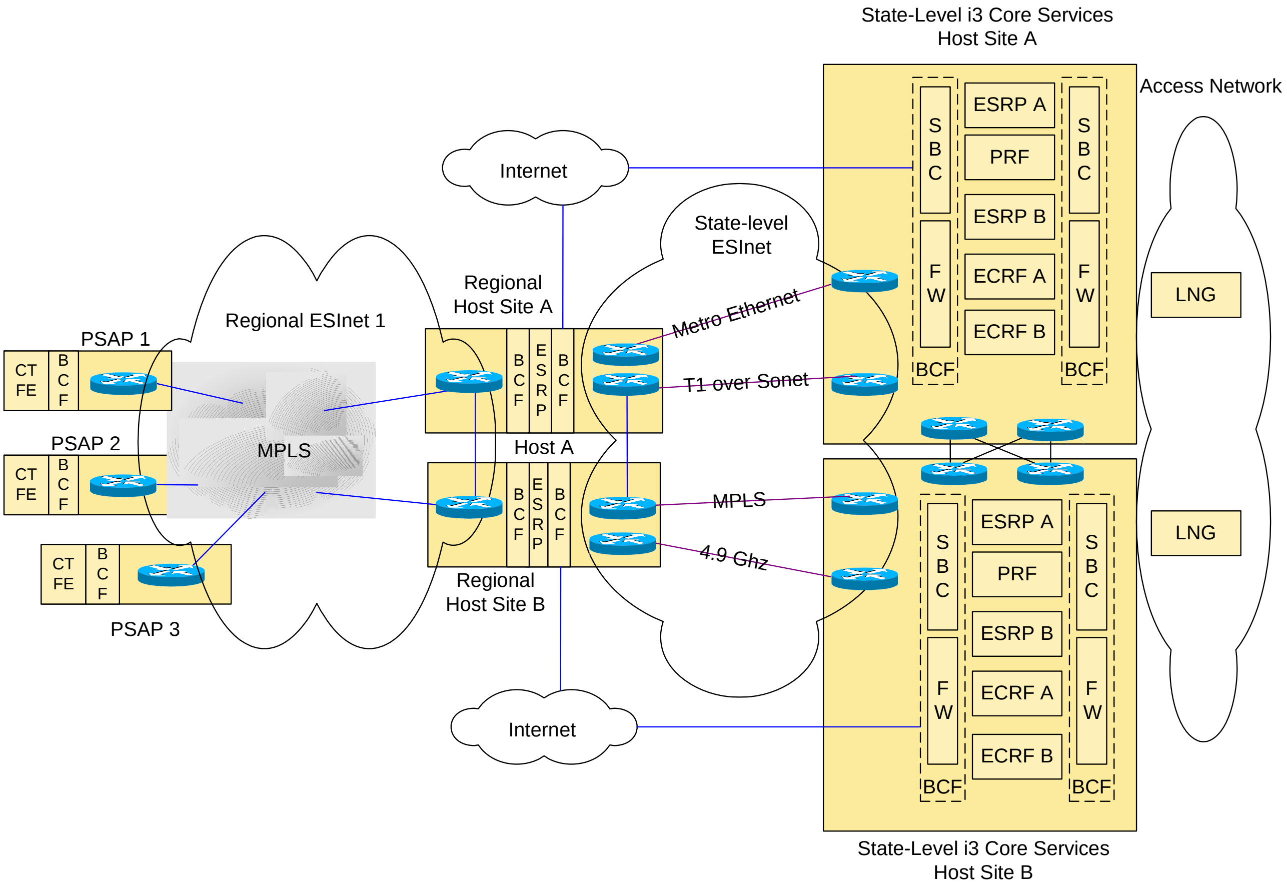
See RFC 2475 for a detailed description of DSCP and PHB mechanisms and functionality.

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. [6]

Regional ESInet I

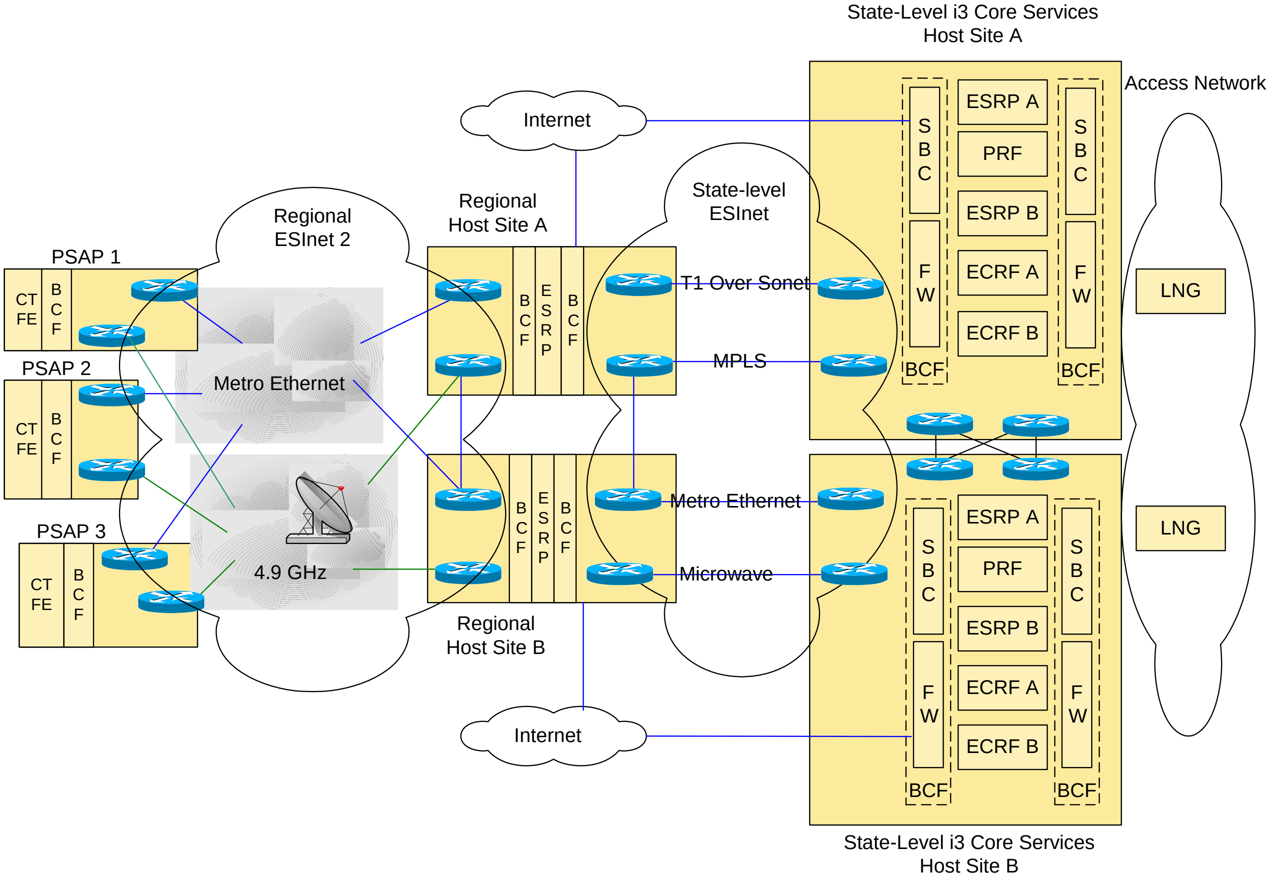
[6] In an effort to simplify the diagrams the physical connections within the sites (i.e. router to switch, switch to server, etc) are not shown.



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 to 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.

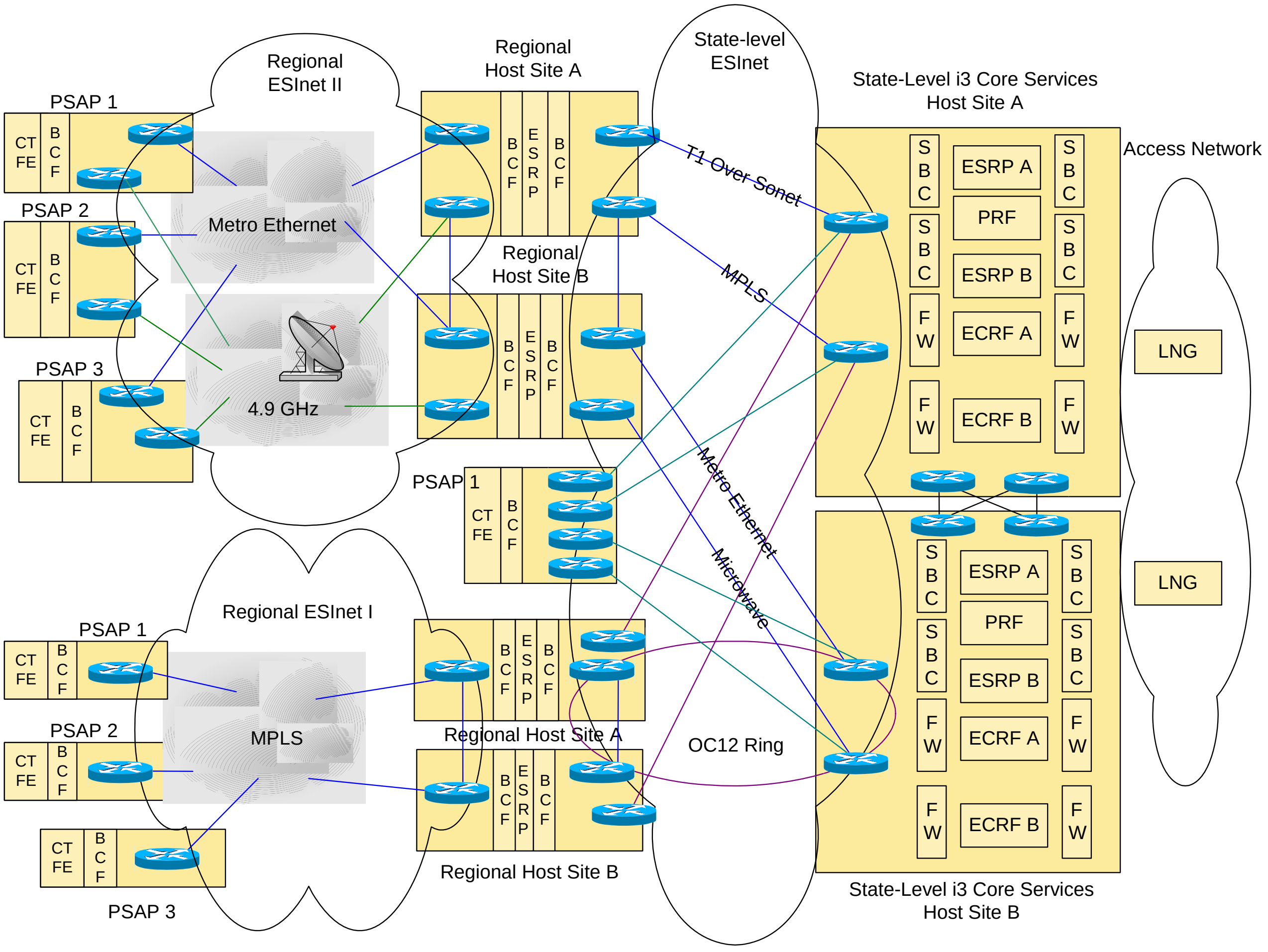
Regional ESInet
II



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.[7] 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

[7] 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