Project Number: MQF-IQP 2821

IP-Enabled WAN EMS System

An Interactive Qualifying Project

Submitted to the Faculty of the

WORCESTER POLYTECHNIC INSTITUTE

in partial fulfillment of the requirements for the degree of
Bachelor of Science
by

Nick Algiere
Mechanical Engineering

André Guerlain
Computer Science

MIRAD Laboratory, April 30, 2013

Approved by:
Professor Mustapha S. Fofana, PhD, Advisor
Director of MIRAD Laboratory, Mechanical Engineering Department

Abstract

The purpose of this project is the investigation into and evaluation of the Emergency Medical Services (EMS) 911 communication infrastructure with the intent of discovering Internet Protocol (IP) enabled technologies that could create a new Emergency Network.

A detailed investigation will be to analyze both strengths and weaknesses of NG9-1-1 technology. The sections of the paper will examine, intellectually, the advantages and disadvantages of a heterogeneous system implementation for an EMS 911 system. There are several concerns, constraints and limitations addressed within this paper. Concerns of reliability stem from the dependence of IP networks on the power infrastructure as well as how reliably location can be determined. In addition, secure interconnectivity of wired and wireless devices in a metropolitan area is difficult to maintain, and impossible to ensure. Another challenge is facilitating interoperability of a geographically and technologically diverse system infrastructure and its operation. Such an infrastructure would require considerable maintenance and governance given its importance. User Interface (UI) matters such as personal identification and access of information and the security thereof; and protection of system resources against abuse, misuse, and disruption.

The specific use of this project is to prove that a workable and reliable IP based NG9-1-1 system can be formulated and is practical to serve a large area. This is accomplished by examining the strengths and limitations of existing NG9-1-1 technologies, and NG9-1-1 legislature and standards.

Table of Contents

List of Figures

List of Tables

Acknowledgements

We would like to thank Professor Fofana for his invaluable advice and counsel during the project. In addition, we would like to thank UMASS Memorial Emergency Medical Services for their assistance in figuring out and carrying out our project. Also, we would like to thank Blake Alberts for contributing his research over the course of the project.

Chapter 1: EMS Communications

1. Introduction

Within this project, it is our aim to research and discuss how EMS services can benefit by leveraging modern technologies and protocols, such as Metropolitan Area Networks (MANs), in order to supplement the existing 911 infrastructures. Specifically we desire to propose a novel heterogeneous system comprised of a harmony of old and new technologies to provide the most efficient, secure, and modern 911 systems that can be implemented given the advances of our age. The existing infrastructure is over 40 years old, meaning that it's uses are limited to what was practical then, rather than now. By leveraging the many technological advances that have come about since then, as we propose, access to emergency services, and therefore response time, could be significantly shorter, saving lives. Additionally, novel functional implementations could be integrated into the new heterogeneous infrastructure, which aid response personnel in ways the present system cannot. Specifically, the utilization of the transfer of audio/video data with greater ease could help EMS responders and the hospital personnel treat the patients quicker and more accurately.

The following chapters will build a foundation for our research and design ideas. Chapter 2 investigates, in depth, the present 911 infrastructures in order to garner a detailed understanding of its advantages and disadvantages. With these elements well defined and understood, we will expound on the specific limitations of the present system within the scope of topics our project addresses and seeks to improve. Simultaneously we will develop the technological, regulatory, legal, and logistical issues, which would be of concern in our proposed implementation. In order to keep the goals of this project concrete and manageable, a specific subset of technological implementations will be defined and focused on. While other matters will

be discussed, it is not possible to address each topic categorically within the scope of our work. The subset technologies and design techniques will then be researched into, and addressed in great detail.

Chapter 3 will present a feasibility study on next generation IP-Enabled 911 infrastructures. First the various limitations of the existing infrastructure and technologies will be discussed in order to create a basis for improvement. In addition, we will highlight specific constraints, which need to be met by a new infrastructure. We will in detail present solutions in order to meet the constraints of such a system. Their possible implementation will be discussed. This discussion will revolve around each technology and their advantages and disadvantages in the context of IPW-911.

Finally, in Chapter 4 remarks on the project and detailed descriptions of the difficulties we encountered and how they were overcome. The final results of the project are summed up and clearly analyzed. Continued discussion of the importance of the EMS communication system will finally move to the presentation of the possible future avenues of our work and assertion of the importance of improvement of the present system in the future.

Chapter 2: Present and Future 911 Infrastructure

2. Introduction

This chapter focuses on the background research of our project. The topics include, legislation, new implementations, legacy networks, and other proposals. These topics are analyzed in order to determine the weaknesses, limitations, and requirements of an IP-Enabled 911 network. These conclusions are then drawn upon in the following chapter where solutions are presented for constraint.

2.1 OSI Reference Model

Computer networks, regardless of their purpose, can be divided by their protocols into separate layers by functionality. Authors Kurose and Ross discuss the concept of defining a computer network into layers in "Computer Networking A Top-Down Approach" [2]. When a network is designed, the designers separate different functionality into separate layers in order to make the entire network uniform and therefore understandable. In order to understand the network or modify it, the protocols are all an innovator needs to understand in order to implement adaptations. Each layer provides a different functionality to the users of the network, as well as services to the layer above it so that the different layers can work together seamlessly. Each layer relies on the layer below it to provide it with usable data so that it can properly perform its purpose and pass on what the layer above it needs. Similarly, the user is the last layer. Even though they are not recognized as part of the network, the application layer passes on what the user needs in a human readable format, which is analogous to how the lower layers interact. This is certainly true for the public telephone network, and essential for discussing and understanding the existing and proposed emergency 911 infrastructures. The OSI reference

model is a generalized breakdown of the different layers a network can have. The public switched telephone network fits within this model.

In order to understand this system of network protocols and how they interact, it is important to have some understanding of both digital and analog signals and the method by which they are encoded on a physical medium such as a wire. Figure 1 shows the difference by which digital and analog signals are transmitted over a physical medium.

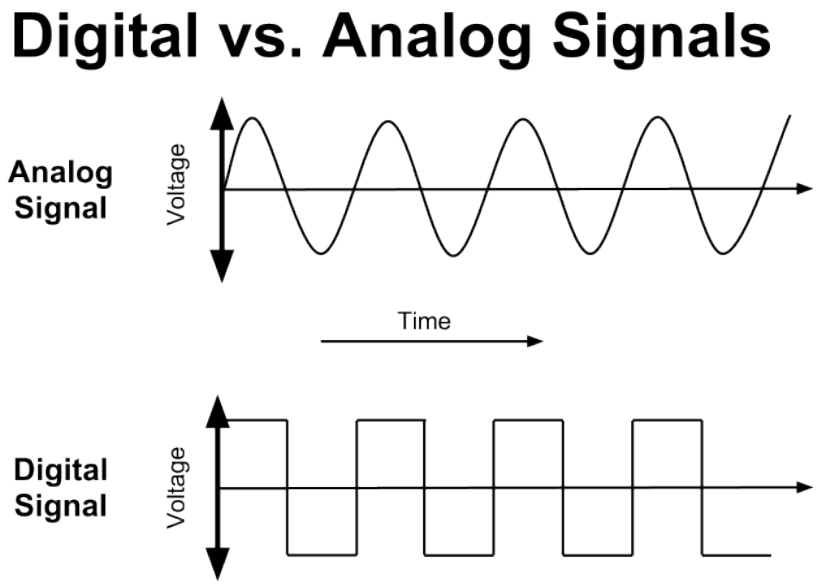


Figure 1: Digital vs. Analog Signals

Analog signals are a continuous sine wave and encoded on the wire by the changes in the amplitude, frequency or both. Digital signals use a variety of encoding schemes, where the voltage is constant for a set amount of time and changes in the voltage represent the bits, either 1 or 0. Analog is now very rarely used on the public switched telephone network, and only on the last mile loop. Digital transmissions are far more common and utilized by the rest of the infrastructure.

The OSI reference model contains all the same layers and corresponding functionality as the public switched telephone network. Figure 2 illustrates the OSI reference model and the relationship between the different layers within a network.

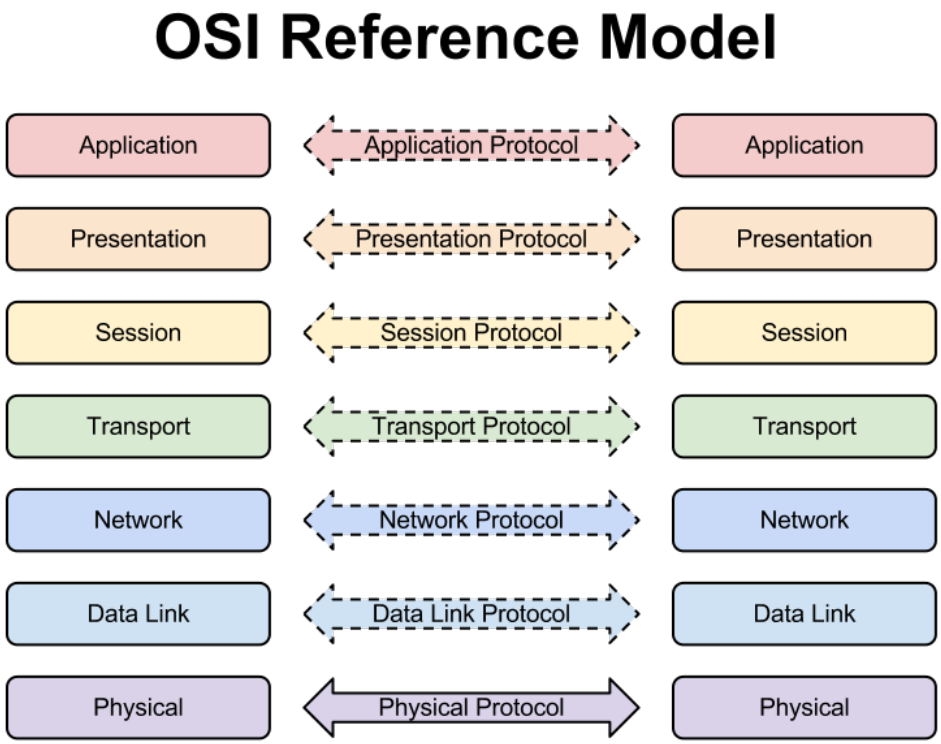


Figure 2: OSI Reference Model

On one end, the protocols are used to encode data that is going to be sent and then this data is passed down to the next layer to be processed. For example, the network layer contains the data necessary to route a packet through a network, yet it is not built with the functionality to handle synchronizing the packets in the case that they arrive in the wrong order. This case can occur due to network routing where the packets do not all follow the same route from the source to the destination, much like drivers do not always take the same roads between two different

cities due to traffic and other constraints. Since the network layer cannot handle this functionality, the data is passed onwards to the Data Link layer, which is built to handle synchronization. Eventually, the data is properly wrapped and is sent to the physical layer, which is the physical process of encoding the bits as ones and zeros, or an analog signal onto a wire or fiber optic cable. In order to provide a more detailed understanding of the current and possible future functionalities of this network, section 2.2 will go into further specifics about how the public switched telephone network fits into the OSI model.

2.2 Public Switched Telephone Network

The public switched telephone network (PSTN) is the architecture through which traditional emergency communications first travels. Medhi and Ramasamy, authors of "Network Routing: Algorithms, Protocols, and Architectures" discuss the PSTN architecture and its functionality [1]. The PTSN is a network, where the data unit is a call. A call is a constant stream of voice data, which is routed from subscriber to another. At the end nodes of the network there are devices known as customer premise equipment, which can be a telephone, or in some cases a modem for data transfer. Each subscriber has a unique phone number which servers as a unique identifier. Phone numbers are defined under the E.164 addressing scheme, which is set up top down.

Telephone numbers, as well as the PSTN topology is described in depth by Bell Services West literature [3]. First a country code is used to identify the destination country, followed by an area code to further narrow down the location. The switches use these two numbers to quickly route the call. The remaining numbers, the number of which is decided by the country, are a number unique to each subscriber in the given area code. In terms of architecture, there are

nodes known as switches, which serve as intermediate hops between subscribers and route the traffic accordingly. Switches are connected via intermachine trunks, which are wired, physical connections between them. The first switch encountered by an outgoing call handles all of the traffic from one "last mile loop," which is a group of subscribers served by one single wire. This switch is known as a local central office, and makes an initial decision whether a call will be routed over the PSTN or the E911 network.

With regard to the OSI reference model, the public telephone network consists of the three lowest levels, as depicted in figure 3.

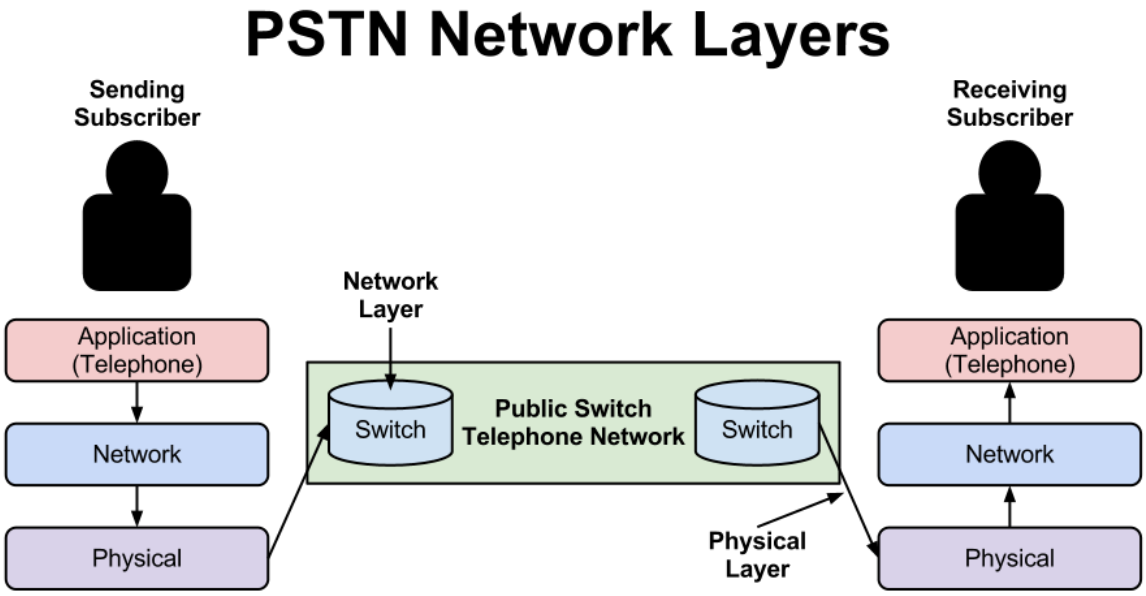


Figure 3: PSTN Network Layers

The physical, network and application layers are utilized to provide all of the necessary functionality. The other layers are unnecessary because the PSTN does not require their functionality. The physical layer consists of the intermachine trunks and well as the "last mile loop" which is the telephone wire that connects a loop of subscribers to the nearest switch. Both

of these physical mediums carry the necessary data between two nodes. Intermachine trunks now transmit exclusively digital data, since the network is a circuit-switched network and has completely done away with the original physical switches. The last mile loop however, may still be analog in certain areas, but for the most part has been converted for digital transmissions due to demand for DSL internet connections.

The switches within the PSTN provide networking services. The current network is a circuit-switched network, as opposed to a physical-switch network or mesh topology. Originally, an operator connected end users by creating a physical connection between two phones with a piece of wire. Then the operator was replaced by physical switches, which automatically connected two users to create a single wire between them. By creating the physical link, the two users had a dedicated physical medium by which analog voice data was transmitted. This means that there was a single wire connecting the two subscribers while a call is being made and that no other data could travel along that wire. In addition, the entire call was transmitted down that single physical connection. This system was replaced with a packet-switch network, which utilizes routing to more efficiently handle data flows.

Within the PSTN, calls are still given a dedicated link; however, it is not a physical link. A service model known as blocked-calls-cleared mode is used in order to establish these connections. This service model uses circuit switching. When an end user requests a call, the network attempts to set up a dedicated connection between the source and the destination. In order to establish a connection between multiple end users on the same physical link, specific bandwidths or data rates must be allocated to a single call at once. Each call is given 4 kilohertz on an analog circuit, or a 64 kbps data rate on a digital circuit. If an analog circuit has no available bandwidth available, or a digital circuit within the network cannot provide the 64kbps

data rate required for the call, the call is blocked and terminated. The exception to this rule is an emergency call, where the network recognizes the code, and automatically makes room for the call. The Federal Communications Commission (FCC) mandates this backup contingency plan to ensure emergency calls can be made regardless of call volume.

2.3 Public-Safety Answering Point

All emergency calls in North America are dialed to 911, which routes through the PSTN to a separate E911 network, as described by Bell Services West documentation [3]. When the local central office receives a 911 call, it is automatically routed over a dedicated local E911 intermachine trunk (IMT) to an E911 tandem central office (TCO). The TCO serves several local E911 IMTs, and therefore several local central offices. Each local central office has it's own dedicated E911 trunk, also called an interface, in order to communicate with the TCO. Each interface connects a single TCO and a local central office. Figure 4 illustrates the E911 network topology and the method by which it interacts with the PSTN architecture.

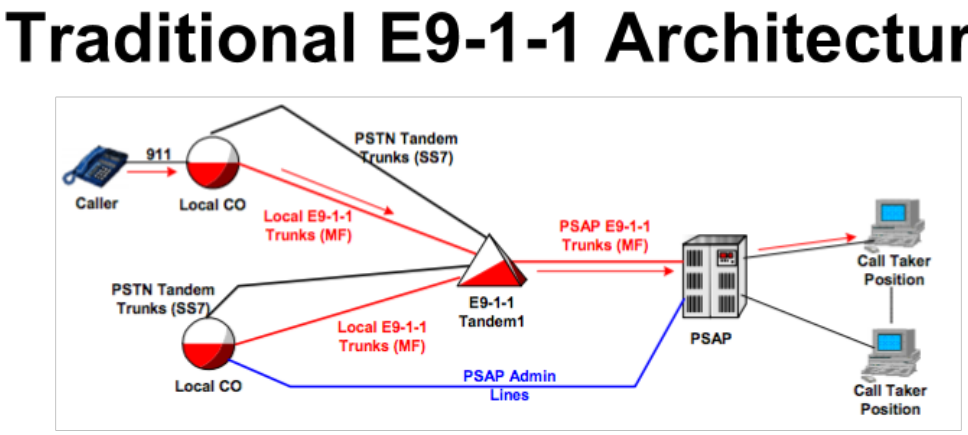


Figure 4: Traditional E9-1-1 Architecture [3]

Therefore, the E911 tandem central office must use the information of which interface the call was received on in order to determine where the call was placed, and where to route the call. From a tandem central office, the call is routed to the closest Public Service Answering Point (PSAP), where dispatchers wait to handle incoming calls and manage the available emergency responders in the area. Usually a tandem central office must make a choice where to route the call because it serves an area large enough that there are several PSAPs to choose from. Once the PSAP is chosen, it selects a call taker, at which point the caller's phone number is sent to the PSAP using multi-frequency digits. The PSAP then automatically looks up the caller's number in a local database, which stores landline numbers as well as their location. This process is unable to work all of the time when cell phones or VoIP calls are placed, and will be discussed in section 2.4. This algorithm within the infrastructure ensures that any emergency call made from within the PSTN is able to make it to the E911 network, is sent to a PSAP, and the location of the sender is verified.

With the advent of cell phones, new challenges were presented to this infrastructure. The database by which landline phones are located cannot be used, because cell phones can call from anywhere within a cell network. This means that the call enters the E911 network wherever the cell tower does. The call will be routed to the tandem central office, which will have little choice but to route to a regional PSAP, since answering points are hierarchical in nature. This may not provide the best service because if the victim is able to communicate their location, time is likely wasted waiting to be transferred to a closer PSAP, and if they are unable to communicate, then it is extremely hard to find them without location information. Unfortunately, the percentage of 911 calls from cell phones is now over seventy percent.

The FCC has mandated several improvements for finding caller's locations to help dispatchers and emergency personnel locate and assist them. The Consumer and Governmental Affairs Bureau lists these requirements online in their VoIP consumer advisory [4]. These requirements came in several phases to allow service providers time to implement them. The FCC requires all wireless service providers to:

1. **Basic 911 Rules:** Allow 911 calls and connect the caller to a PSAP, whether or not they have an active subscription with the carrier.
2. **Phase I Enhanced 911 Rules:** Supply the PSAP with the telephone number of the caller as well as the location of the cell site or base station, which is handling the call.
3. **Phase II Enhanced 911 Rules:** Supply precise location information to PSAPs. This information should include the latitude and longitude of the caller. Depending on the method by which the location is determined, the location must be within 50 to 300 meters of the victim.

The location precision varies because the service providers can use a variety of different methods to locate a caller including cell tower triangulation or GPS data. It is important to note that these rules only apply to calls, which are from outdoors due to the limitations of ascertaining the location of mobile devices while indoors. In addition, the FCC allows wireless providers to apply for exceptions in areas in which it is impractical or impossible to implement location services due to ecological or geographical features.

2.4 PSAP VoIP Limitations

Prusansky discusses adapting to VoIP and the challenges it presents in "VoIP and 911: Is Your Agency Prepared?" [6]. The Internet Protocol Suite consists of two protocols, the Internet

protocol (IP), and the Transmission Control Protocol (TCP) to form TCP/IP. These protocols are used in order to transfer data between computer networks. This technology can be leveraged to send any type of data, and as the ability to transmit data quickly over the Internet infrastructure increased, new applications were developed to exploit it. Voice over IP (VoIP) transmits voice data digitally over the Internet, similarly to the PSTN. Not only may users of VoIP applications talk to one another over an Internet connection, but by utilizing a connection between the PSTN and the Internet known as an "Internet exchange" or "Internet to PSTN gateway" subscribers can call any landline or cell phone as well.

VoIP introduces many new complications with meeting the FCC constraints for communication with the E911 infrastructure and PSAPs. The architecture by which a VoIP device establishes a connection with a PSAP is depicted in Figure 5.

Figure 5: VoIP to E911 Architecture [6]

When an emergency call is placed from a landline phone, the FCC standards are easily met by the physical infrastructure, and when cell phones were introduced, methods for physically locating a mobile device were developed and implemented. However, those experiencing an emergency are increasingly calling from VoIP phones, which leverage the Internet in order to place calls from outside the public and cell phone networks. It is very important to understand certain aspects of TCP/IP, which both provides benefits and adds limitations to its use.

The Consumer and Governmental Affairs Bureau released "FCC Consumer Advisory VoIP and 911 Service," which was a warning to consumers discussing the advantages and disadvantages of VoIP in terms of E911 [5]. VoIP provides many benefits to the customer and provider, creating many incentives for both. First, by utilizing an Internet connection rather than the PSTN, phone is incorporated into an already existing digital network rather than relying on an entirely different network. In addition, the Internet is designed to carry all types of data, not just voice. The implication is that the service can be provided for far less money, perhaps increasing the amount of people who can afford a phone service dedicated to their home. Secondly, VoIP allows their users to choose which area code they are in, and therefore which PSAP will receive their calls. This is achieved by setting up an Internet exchange, which can route traffic directly into the network covering each separate area code. Furthermore, the end user can add a variety of devices to connect with their VoIP phone. These devices can transmit any sort of data necessary to a receiver. Lastly, a VoIP-enabled device can make a call from anywhere that it can either be plugged in or connect to the Wi-Fi. This allows for a great deal of redundancy with the cellular network when a phone has VoIP compatibility as well. With these advantages, several drawbacks are also introduced within the process of interfacing with the PSTN and E911 infrastructures.

The ability to move a VoIP-enabled device from one place to another presents far more problems than it solves. It does allow subscribers to call from any Internet access point, however they are then routed to a PSAP where their number is registered when they call 911. This misdirection wastes time because the subscriber's local PSAP then has to re-route the call to a PSAP nearer to their location. Emergencies are urgent, and this is a significant waste of time. Plus the potential for human error in identifying the correct PSAP is introduced. In addition, a VoIP only device is unable to work when the power grid is knocked out because modems rely on the electrical grid to provide them with power and transmit and receive data. This is a significant issue when considering that there is a correlation between losing power and emergency situations. The economic advantages have allowed VoIP to persist on the market is becoming more prevalent, forcing policy makers to deal with this issue. In addition, our proposal in chapter 3 addresses these constraints.

2.5 Background Protocols and Technologies

There are several proposals and sources, which served as background material. These sources helped identify legal, social and technical constraints, which a new proposal for an IP-enabled Ubiquitous E911 Network must meet. The laws regarding emergency 911 liability and privacy concerns are an extremely important body of work. These documents provide the major non-technical constraints for our proposal. However, these non-technical constraints in many cases translate into technical constraints as well when the technologies and protocols used are taken into account. In addition to laws there are several sources, which discuss the actions taken by the government as well as government agencies in order to implement upgraded and modernized emergency 911 services. Also several publications are discussed which helped gain

insight into possible implementations and the physical and software components necessary for a ubiquitous, wireless and scalable emergency 911 infrastructure.

2.5.1 Wireless Communications and Public Safety Act of 1999

In 1999 members of the Unites States Congress expanded upon previous legislation to better protect citizens using alternatives to traditional wire line phones. This gave the government, and the FCC in particular, the authority to further regulate E911 services encompassing emerging mobile communication technologies. The stated goal of this bill is the "support of States in upgrading 9–1–1 capabilities and related functions, encouragement of construction and operation of seamless, ubiquitous, and reliable networks for personal wireless services, and for other purposes" [7]. This act first realized the potential problems posed by alternative telephone connections, and presented limited legislation to begin the process of modernizing the telephone architecture. The proposal presented in Section 3 is built with this and future additional legislation in mind as it would be under federal jurisdiction.

Not only did this act seek to fix current problems with the existing infrastructure in relation to the new expanding use of cellular and VoIP phones, but it also enacted that enhanced 911 be set up to leverage these technologies and provide optimal, best effort service. This act also gave wireless emergency communications the same standing as wired in the eyes of the law. This means that the same guarantees made by the law regarding wired 911 were extended to wireless, including reliability and liability. Legislators wrote the law with the understanding that it was not practical to expect wireless and VoIP phone providers to immediately have the technology to comply, but with language strong enough to begin promoting improvements. By allowing these new technologies the same standing as the wired PSTN connections, new ways of

collecting and transmitting data had to be incorporated, leading to many of the design constraints our proposal resolves.

2.5.2 FCC Takes Steps to Implement The WCPS Act

Immediately following the passage of the Wireless Communications and Public Safety Act, the FCC was assigned to enforcing and carrying out the newly established standards for establishing Enhanced 911 (E911). E911 encompasses all improvements made in order to give wireless and VoIP technologies as close to the same reliability as wire line emergency services as possible, and our proposal falls within this category. In response to the act, the FCC designated 911 as the universal emergency number for VoIP and Cellular, forcing these service providers to adopt it. They also recognized that during an emergency picking up a phone is often the first and most important means of communication, and that standardizing the number and the laws surrounding the E911 infrastructure would save lives. Initially, the FCC led an investigation in order to determine where 911 was not yet being used, and area specific limitations, in order to standardize the number. Following that action, they made an inquiry into how they could best serve the States in order to help them implement or upgrade their infrastructure in order to meet the new regulations.

2.5.3 Enhancing SIP with Spatial Location for Emergency Call Services

Session Initiation Protocol (SIP) is the protocol used within VoIP to initiate, alter, or terminate a multimedia connection. Nokia researchers Costa-Requena and Tang proposed extending this protocol in order to carry additional data in “Enhancing SIP with Spatial Location for Emergency Call Services” [8]. SIP is an application protocol, meaning that it operates at either end of a TCP/IP connection, and is the protocol by which VoIP manages connections over

TCP/IP by maintaining a stream. SIP is highly extensible meaning that the design of the protocol leaves room for new functionality to be added, allowing the protocol to be customized for a variety of purposes. Importantly, SIP itself may encapsulate data using other protocols in order to handle significant constraints other than transportation provided by TCP/IP and stream management handled by SIP. One possibility is extending SIP functionality to include the use of Spatial Location (SLO) information. At the time of publication SIP could not support SLO, however researchers at Nokia have proposed a solution. Traditionally wrapped within a SIP packet is an SDP packet containing just audio and, if necessary, video data. They argue that to best meet the technical and social specifications for a ubiquitous VoIP architecture, SIP could replace it's traditional SDP packet with an SLO packet, allowing for additional special data to be included.

Spatial Location (SLO) is information regarding a user's location and can be embedded within SIP, but currently is not. SLO is an XML based data structure that is designed to handle far more than simply location verification. A SIP multimedia stream may be secured if a secure connection or protocol is being utilized above it, since it does not handle the transportation. Therefore, the connection may be insecure, meaning an adversary, someone who seeks to maliciously exploit a network or computing resource, may be able to monitor the connection. Therefore the Cellular Telecommunication Industry Association (CTIA) has a list of guidelines for reasonable security measures in order to prevent adversaries from gaining access to valuable data from subscribers. This will be further discussed in section 2.5.4.

These guidelines seek to ensure a measure of privacy with security measures robust enough that it is impossible for an adversary to gain meaningful information. Such security measures are measured in terms of how much effort needs to be exerted before they can be

circumvented and whether or not a reasonable adversary would attempt to do so as a result. Ultimately the goal of security is to make breaking the security policy cost so much that it outweighs the value of the information gained. SLO contains user information such as user identifiers, data regarding location and additional data. This data is sensitive if lost, therefore the protocol must provide security on that data, while the rest of the data may or may not be protected.

In addition to supporting SLO, the researchers' proposal utilizes SIP's extensibility to allow new data to be added in the future. Unmodified SIP has an architecture containing a user agent, a proxy server, a redirect server, a registrar server, and a location server. The user agent is the subscriber and their mobile device. The proxy redirect and registrar servers are important only as pieces of the network architecture. The purpose of the registrar server is to verify the registration status of the end user. If the subscriber is verified, their location data is decoded and sent to the location server. The location server is essentially part of the registrar server dedicated to managing user data. The location server interfaces with both the redirect and proxy servers in order to provide them with user information. The main change in this proposal is the addition of more data in order to keep track of not only location data associated with the device on the network, but also special data needed to determine the location of a victim using VoIP for an emergency call.

The SIP packet structures with both SDP and SLO embedded are detailed in Figure 6.

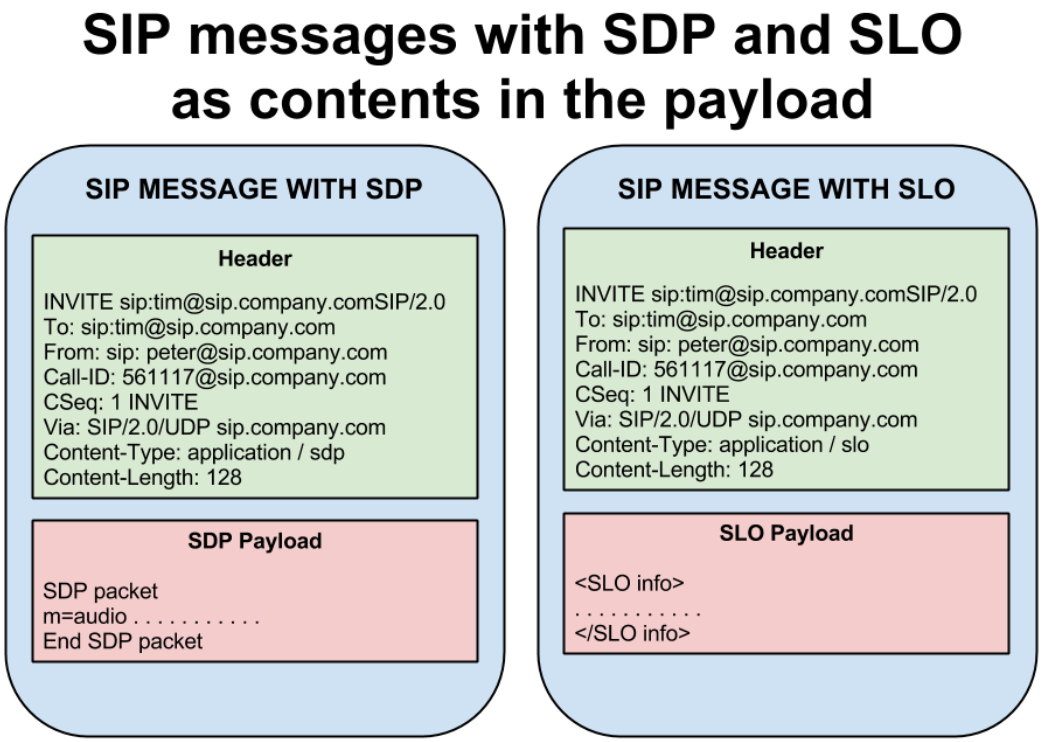


Figure 6: SIP Messages With SDP and SLO as Contents in the Payload

For both versions the packet starts with various header fields such as to, from and other relevant data. The only difference in terms of functionality is the application needed to decode the data in the Content-Type field. Following the header fields is the embedded packet utilizing the SDP and SLO protocols, respectively. The sole difference is the application needed to decode the data on the opposite side of the connection. It is important to note that when the SIP packet embeds SLO data with it, the encrypt option, which is not illustrated in the figure, would be used to protect the privacy of the spatial location data. By using the content type field, an application can tell what type of data it is receiving and decode it properly. Specifically the application must determine if an SIP packet is filled with data to maintain the connection, or filled with an SLO payload including spatial location data.

Naming within the SDP packet is illustrated in Figure 6 by the contents of the “to” and “from” fields. SIP queries DNS servers or LDAP in order to find destination addresses and route the packets, in the same way TCP/IP does. The first part of the to and from fields is a specific person while the second part is the name to be looked up in order to find the IP. This second part of the address could be represented by a network address, removing the need for a domain name lookup.

SLO is a protocol for encoding and decoding location data in Extensible Markup Language (XML). Location data encoded in XML using SLO is depicted below in Figure 7.

Example SLO Spatial Location Data

```
<SLO-info>
  <TID>
    urn: username@company.com, owner=jose,
    id=2342112, email=Jose.Costa-Requena@nokia.com,
    pstn=+358405201816
  </TID>
  <Signature: aZWQAd22aFg& "£4/>
  <Time-to-Live: 3000 sec/>
  <Type-of-Device: mobile/>
  <Location-description>
     I am sitting in a terrace on the second floor of Eiffel Tower
  </Location-description>
  <Coordinates-calculation: Enable/>
  <SLO-data>
    <Accuracy: 5m/>
    <Coordinates>
      Geographical coordinates x,y,z
    </Coordinates>
    <Date: 22.11.2000/>
    <Speed: 20ms/>
  </SLO-data>
</SLO-info>
```

Figure 7: Example SLO Spatial Location Data [8]

XML encodes data by using tags, which have an opening ‘<’ symbol, a value and then a closing ‘>’ symbol. Tags are in pairs, meaning that any text between tags ‘<example>’ and

‘</example>’ is associated with those tags. The forward slash indicates the end of what a tag contains. Tags may contain other tags as shown, allowing for complex data structures to be easily represented in the layout.

The researchers propose that all of this data be contained within an SIP packet and transmitted to give emergency personnel more in depth data. The mandatory and non-mandatory data that SLO can encode is shown in Table 1.

SLO Possible Data Fields

Datum	- WGS84	Mandatory
Coordinate	- Latitude - Longitude - Altitude above WGS84 reference ellipsoid - Altitude above mean sea level	Mandatory Mandatory Optional Optional
Location Accuracy	- Horizontal accuracy, by radius of a circle from the positioned point - Altitude accuracy, by range from the positioned point	Optional Optional
Time	- Real time of the measurement /fix	Mandatory
Speed	- Ground speed - Vertical speed	Optional Optional
Direction	- Direction of movement	Optional
Course	- Direction from the current position to a defined destination	Optional
Orientation	- Horizontal orientation – Vertical orientation (pitch)	Optional
Un-specified Attributes	- Attributes enabling some extensibility	Optional

Table 1: SLO Possible Data Fields [8]

SLO supports a much larger variety of location data than simply longitude and latitude. SLO can include ground speed and altitude, which requires the data to be generated by the transmitted device and sent. The implication is less work needs to be done on the receiving end in terms of what needs to be calculated based on periodic spatial location data.

This approach to providing spatial location data to the PSAP depends on several factors, which make it unfeasible with relation to legacy hardware. Firstly, this solution depends on the

user's device to have the functionality to calculate or obtain location data wherever it is. It is possible to accomplish this goal with an embedded GPS device or a mechanism for signal strength calculations, however this may not always be possible inside buildings where signals are often distorted or blocked. In addition, routers and other Internet access points do not necessarily have the ability to provide this kind of data to the subscriber's device.

2.5.4 CTIA Guidelines

The CTIA provides guidelines [11] for location-based services, which attach a location to a user ID, phone number or other means of personal identification. These guidelines do not apply to information, which was transmitted under the following circumstances:

1. As authorized or required by applicable law (e.g., to respond to emergencies, E911, or legal process);

2. To protect the rights and property of LBS Providers, users or other providers of location information;

3. For testing or maintenance in the normal operation of any network or LBS; or

4. In the form of aggregate or anonymous data.

Therefore, the information sent in the case of an emergency is not covered under these guidelines. However, it is still important to keep these guidelines and make a best effort attempt to maintain the privacy of those using VoIP in order to prevent malicious agents from compromising the proposed E911 architecture.

2.6 E911 Legislation

Any changes made to the way the current 911 infrastructure operates must first coincide with the laws and regulations put forth by The Federal Communications Commission (FCC) as

well as any standards and laws individual states may have. The Federal Communication Commission regulates international and interstate communications by radio, television, wire, cable, and satellite in every US state and Territory, including the District of Columbia. The Federal Communications Commission was established in 1934 by the Communications Act and operates as an independent government agency overseen by the US congress. The structure and responsibilities of the Federal Communication Commission is outlined in the Federal Code of Regulations under Title 47- Telecommunications; Chapter 1 – Federal Communications Commission. Thus far the Federal Communications Commission has made great strides in increasing the efficiency and flexibility of the 9-1-1 system, more so in the past few years working on the transition to a Next Generation 9-1-1 emergency system.

The Federal Communication Commission has been seeking to improve the effectiveness and reliability of wireless 9-1-1 emergency services since the Wireless Communications and Public Safety Act of 1991 also called the 9-1-1 Act. Under the 9-1-1 Act, the Federal Communication Commission made 9-1-1 the universal number for all telephone services. The Federal Communication Commission also ensures that carriers and public safety entities upgrade the 9-1-1 network regularly resulting in innovation such as automatically reporting the telephone number and location from where a call was made. These capabilities are now called Enhanced 9-1-1.

The regulations set forth by Federal Communication Commission to improve the efficiency of wireless Enhanced 9-1-1 services include the wireless Enhanced 9-1-1 program which is separated into two phases which was part of the ENHANCE 911 Act of 2004. Phase one requires carriers to provide the Public Safety Answering (PSAP) point with the telephone number and locations from where the wireless 9-1-1 call originated. The carriers have six months

to complete phase one once requested by the PSAP. Phase two requires carriers to provide more precise information, such as latitude and longitude, to the PSAP. This information must be within 300 meters, the Federal Communication Commission's standards for E9-1-1 accuracy. This again must be completed within six months of a valid request by a PSAP. For E9-1-1 deployment, The Federal Communication Commission requires coordination amongst both Public and Private Entities for the development of new technology and upgrades to local PSAP and E9-1-1 services. The ENHANCE 911 act also addressed concerns about deployment of 911 services in rural areas and was another step forward in the transition to the NG911 system.

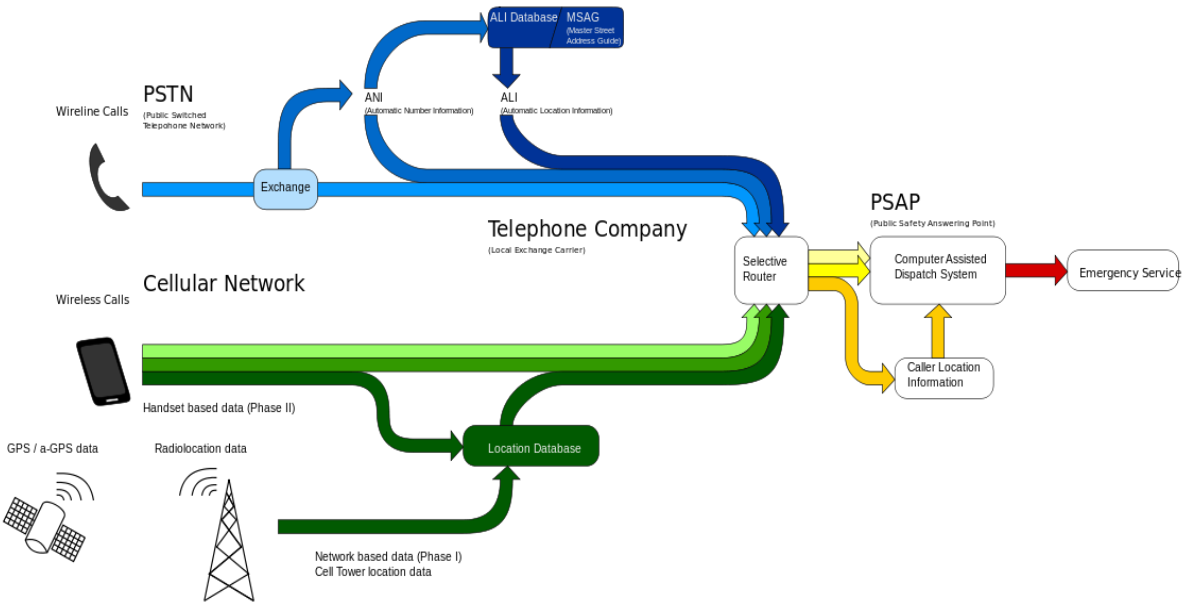


Figure 8: Emergency Flowchart of the Current Public Safety Telephone Network

In 2008, Congressed established the New and Emerging Technologies 911 Improvement Act (NET 911 Act) in hopes of furthering the countries progression toward the NG911 system. The NET 911 Act solidified the Federal Communications Commission's authority to regulate

Voice over Internet Protocols (VoIP) 9-1-1 emergency system, which is a technology not based on the current switchboard system. As of 2005, the Federal Communications Commission adopted a new set of rules which require providers of interconnected VoIP services to adapt the technology too supply emergency 9-1-1 capabilities to customers. These VoIP services allow one to both make and receive calls on the current telephone network and under the rules set by the Federal Communications Network, must deliver all 9-1-1 calls to a local emergency call center, deliver the customers call back number and locations information, and inform the customer of the capabilities and limitations of the VoIP 9-1-1 service.

VoIP 9-1-1 service also touches upon the Next Generation 9-1-1 Initiative, a government program that helps in the research and development of system architecture and plans to establish an Internet Protocol based delivery system for multimedia 9-1-1 calls. The Federal Government has recognized that in a world with ever increasing mobile and dynamic communications has increased the demand for connection to 9-1-1 Emergency services. The current infrastructure and equipment of PSAPs are of an analog-based system from 1968 and cannot process calls using new technology such as Internet Protocol access networks nor efficiently transfer calls when the volume of calls exceeds the available resources. To help the transition the Next Generation 9-1-1 Initiative provides some incentives for those at state and local levels to pursue their own developments in accordance with this next generation system.

In continueing transition to a next generation 9-1-1 emergency system the Next Generation 9-1-1 Advancement Act of 2012 outlines roles of the Federal, State, and local government in traditional 9-1-1 and Next Generation 9-1-1 (NG911) Governance. The Federal Communications Comission has recently made efforts in the transition to NG911. “In the National Broadband Plan, the Comission made several recommendations to “bridge the gap” to

NG911".[9] As of December 2012 the Federal Communications Comission proposed requiring all wireless carriers and providers of text messaging applications to allowing customers to send text messages to 9-1-1 emergency services. The Federal Communications Commission has also resently employed a Technology Transition Policy task force whith the purpose of identifying issues with the transition from traditional switchboard networks to a fully IP-enabled Network. Other federal agencies have started supporting and adressing issues at state and local government levels to also easy the transition to NG911.

While there is still much indecision and suggestions in how Federal Entities should assist in the transition, the National Emergency Network Association (NENA) suggests that the Federal Communications Commission start adopting default NG911 regulations that would apply to states that have not yet made progress in accomidating a NG911 system in their Regulations. A summerisation of current recommondations for the role of the Federal Government in the transition to NG911 put forth by the NG911 Advancement Act are as following: [9]

1) Congress should facilitate the exercise of existing authority over NG911 by such federal agencies as the FCC, ICO, NHTSA, NTIA, and DHS, so that they are better able to support the NG911 transition and to coordinate with one another more effectively in these efforts.
2) To Address instances where states lack authority under state law to regulate certain elements of NG911 service or otherwise choose not to exercise such authority, Congress should consider enacting legislation creating a federal regulatory "backstop" to ensure that there is no gap between federal and state authority (or the exercise thereof) over NG911.

The federal government's role in the transition to NG911 is one that focuses on the support and organization of transition efforts by state and local governments and the development of NG911 architecture at a national level. The NG911 Improvement act recommends that state and local public safety authorities should proceed over the actual deployment of NG911 services in their respected jurisdiction, as there may be state laws regulation elements of NG911 services. Through this may result in voids in regulation of VoIP-based 911 services, the Federal Communications Commission will ensure steps to prevent these holes.

Another summarization of recommendations outlined in the NG911 Improvement act is that of the deployment of NG911 services: [9]

1) Congress should encourage and set a goal for early deployment of sate or regional ESInets
2) Congress should encourage or require the use of a common set of standards for seamless transmission of NG911 information between ESInets and with other public saftey networks, including the Nationwide Public Safety Broadband Network.
3) Congress should encourage the development of consolidated regional NG911 call centers where possible, for example, by offering preference for grant and eligilbity to states and regions that make progress towards this goal.

Emergency Systems IP Networks (ESInets) handle traffic of commercial networks to PSAPs and public safety authority data communications. ESInets will also act as bridges between PSAPs on the state and national basis ensuring flexible routing of emergency traffic and response. Though the Federal government is not supporting a national ESInet infrastructure, some action will be taken at the federal level to help state and regional

coordination. Also due to the fact the actual deployment of the ESInet another NG911 infrastructure falls to individual states, incentive by Congress help accomplish a swift and easy transition to NG911 services around the nation.

However NG911 may not be sustainable on fees paid by users of voice-centric wireline and wireless services as it traditional 911 has thus also in the NG911 Act the following recommendations were made: [9]

1) Congress should develop incentives for states to broaden the base of contributors to NG911 funding to more accurately reflect the benefits derived from NG911 service.
2) Congress should encourage states to provide funding for NG911 as well as legacy 911 purposes as part of any existing or future funding mechanism.
3) Congress should condition grants or other appropriate federal benefits on a requirement that funds collected for 911/NG911 funding be used only for 911 or NG911 purposes, and should provide for appropriate enforcement of such requirements.

Thus monetary support by the federal government would help minimize disparities among states that could potential lead to compatibility issues. Also expanding funding beyond that of fees paid by those who use wired and wireless services would thwart this issue. However the states have most of the responsibility including assigning and regulating liability protection of NG911 among providers of this service and the state itself. More recommendations to congress for new implementations of state liability are: [9]

1) Congress should consider incentives for states to service their liability regimes to provide appropriate protection for entities providing or supporting NG911 services, in conformance with standardized guidelines or model state legislation.

2) Congress should include appropriate liability protection as part of any federal law that imposes NG911 requirements or solicits voluntary NG911 activity.

911 liability protection gives a type of insurance that covers those that provide 911 emergency services. It would be unwise for congress to set federal liability protection standards for NG911 because of the variations in how emergency 911 services function in each state, though some individual carries argue otherwise. Still much of the duty for NG911 deployment, funding, upkeep, and improvement falls to the state and its own legislation.

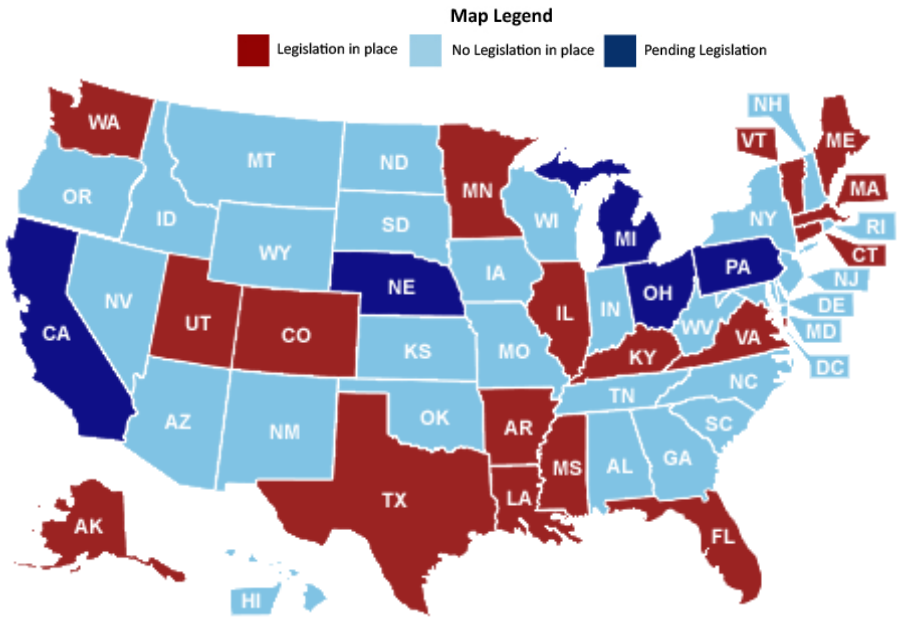


Figure 9: United States 9-1-1 Legislation, Pending Legislation, and No Legislation

Among the states who already have 911 legislation in place, Massachusetts is counted among them. Massachusetts has many laws regulating 911 and E911 services but has also taken initiative and has already started making accommodations for NG911 services by referencing

next generation 911 technology platforms, keeping consistent with regulations by the Federal Communications Commission. As Congress pushes transition to NG911 services changes to emergency telecommunications, states will create and continue to make adaptions to their laws and development towards a next generation emergency system.

2.7 NENA Standard Proposal

NENA's i3 specification [10] represents NENA's first attempt at designing the NG9-1-1 system. NENA specifies in the i3 document that a means to receive SMS, IM, video, and other means of communication is needed in modern emergency systems, as they are all reasonable forms of communication. The NG9-1-1 system NENA promotes is an IP based network that would incorporate all emergency services such as Fire, Paramedic, and Police. This network is termed an ESInet, Emergency Services Network. Using a PSAP or Public Safety Answering Point, the ESInet would be able to locate the caller by means of either latitude and longitude or street address. The i3 document specifies and outlines an IP based emergency calling system and redefining the means of NG9-1-1.

NENA's vision of an NG9-1-1 IP based infrastructure includes an ESInet based on either a SIP or IMS architecture that would allow a PSAP to locate the origination of the caller. The PSAP would accept multiple types of multimedia communications such as SMS messages, pictures, and video. The Architecture would look as such in Figure 10.

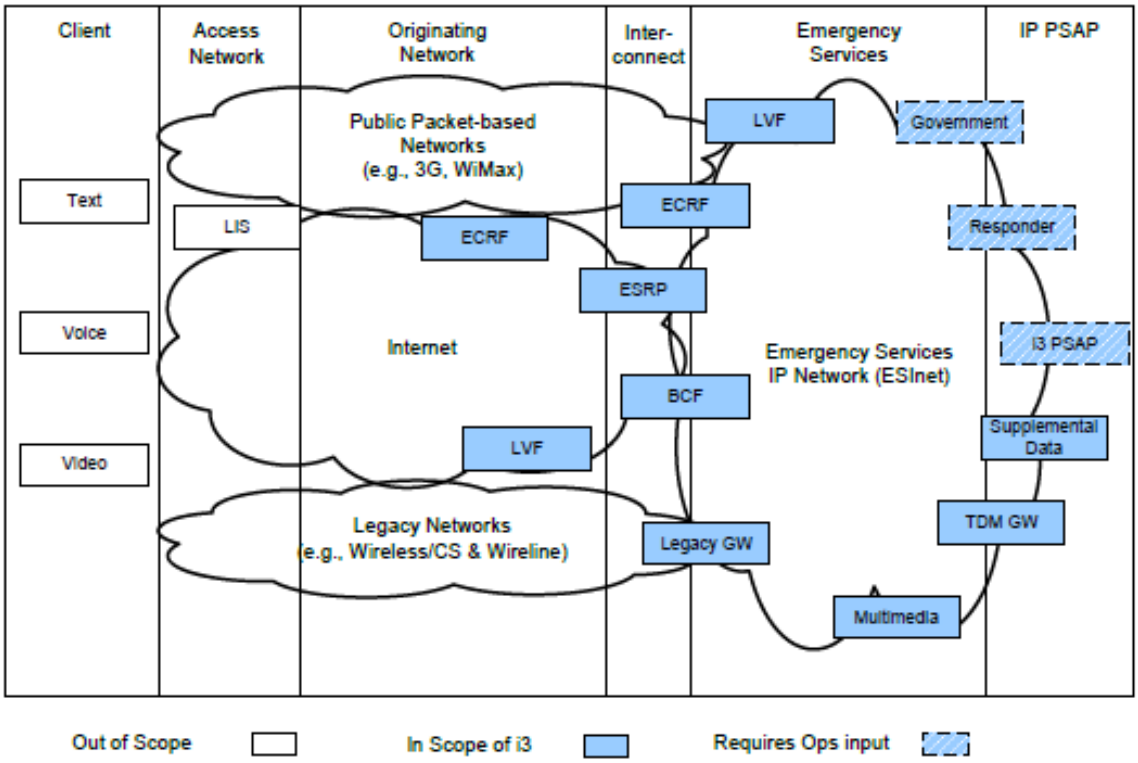


Figure 10: Envisioned NG-911 IP Based Infrastructure

Figure 10 describes the functional system in which NENA's NG9-1-1 system would function. This demonstrates how the client would enter the network, connect to emergency services, and be redirected to an IP PSAP capable of receiving IP signals within emergency calls. A better way to exemplify this type of architecture is by using a series of drawings to help better understand exactly how a piece of information enters the network and is routed to the ESInet.

The IP client sends a call, such as a voice, text message, or other means of communication to an access network such as an LIS (Location Information Server). The LIS is a part of the architecture that provides the locations, in Location-by-Reference and Location-by-Value, of endpoints such as the client. From here the signal is then sent to the originating network such as the global Internet, where it meets a Location Validation Function and an Emergency Call Routing Function. The Location Validation Function confirms the location of

the call and validates it to be sent to the correct PSAP. The Emergency Routing Function is also a function that receives location information and sends it to the PSAP. The signal then routes to the Emergency Services Routing Proxy, which determines which route to take within the ESInet. In which the corresponding responder is connected with the PSAP and told the location of the incident.

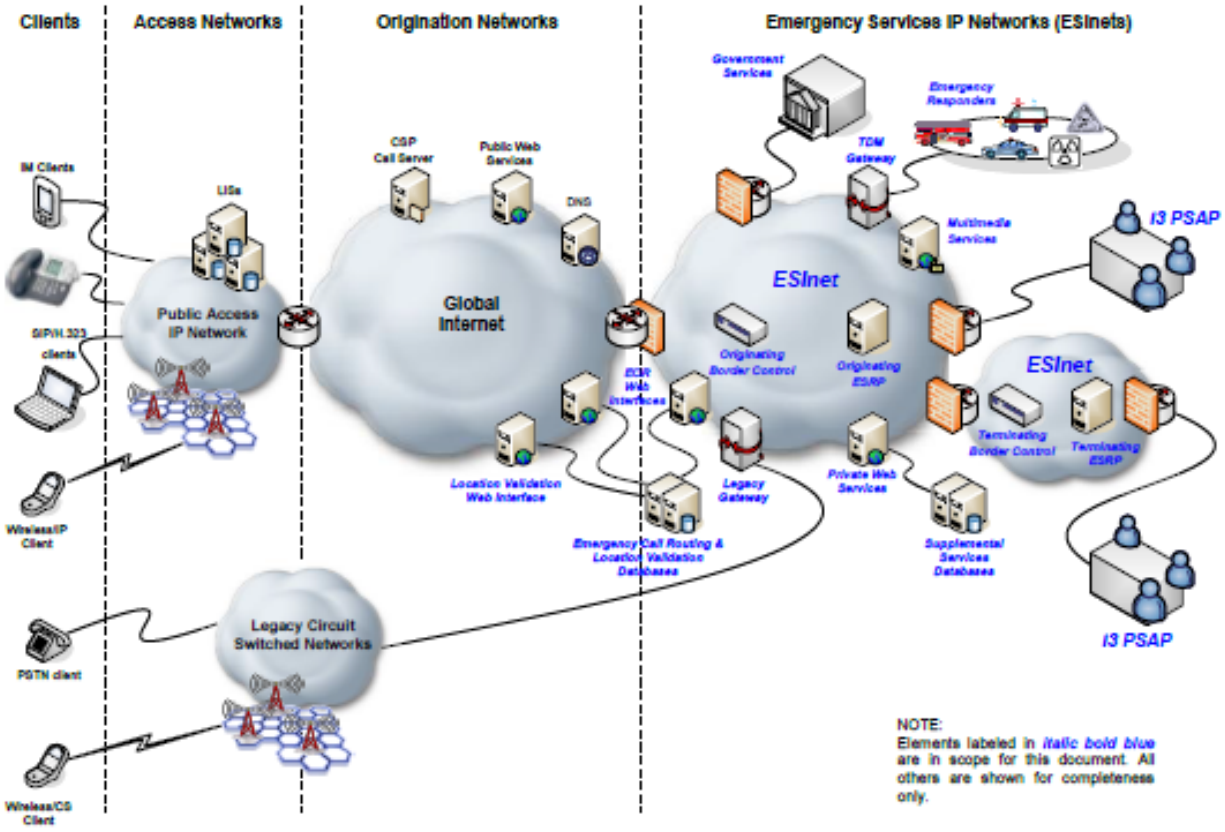


Figure 11: Client Connection to ESInet Via IP Network

A client connects to an access network and then how that signal is forwarded to the ESInet. The physical architecture demonstrates how a cellphone can connect to an access network. The steps demonstrated are the cellphone connects to a Public Access IP Network, then sent to an Origination network such as the Global internet, and are then forward to the ESInet to emergency responders and the PSAP. NENA shows here that the physical architecture is capable

of location determination that can be provided by a VoIP provider. A routing request will then be generated and rout the information to the correct location.

2.7.1 Architecture

Call Architecture is also an important aspect of NENA's plans of an IP centric NG9-1-1 calling system. A Local Acquisition Function is the basis behind accessing the location of the caller. This function is then retrieved by an LIS. The call is then generally presented to the ESInet and then further routed to the PSAP. This PSAP will accept multiple kinds of multimedia. A problem NENA identifies in this regard is receiving multiple calls on the incident via different types of multimedia. In the case that this occurs, a primary call and then secondary calls will be designated an identifier. NENA believes that this would solve the issue of multiple incidences in the same location being reported repetitively. A call is identified as a communication that is accepted by the PSAP whether it is an actual telephone call or an SMS Text Message.

2.7.2 NENA and IETF

NENA also recognizes the importance of comparing its i3 system to IETF Standards. IETF standards define, call signaling, media flows, location acquisition, conveyance to ESInet, distinguishing calls, and emergency call routing protocols to the correct PSAP [10].

In terms of location, the IETF body has proposed that information should be delivered to the endpoint or has a reference available to the location. The endpoint is then told where it is by an access infrastructure provider and then the communication service provider routes the call to the right location. Two major terms defined by the IETF standards are "Location-by-Value" and "Location-by-Reference." "Location-by-Value is defined as a location readily consumable by the recipient without transformation." [10] "Location-by-Reference is defined as a URI that, when de-referenced in the correct manner by an authenticated authorized entity, will yield the

location value of the endpoint." [10] These terms are important because it is what defines where the call is coming from in terms of latitude and longitude or a street address.

In signaling a call the IETF standards are based on SIP. SIP, Session Initiation Protocol, creates multimedia sessions such as voice, video, and even text. This would essentially be the foundation for the ESInet. The most important aspect of SIP is that it needs to go through many Proxy Servers thus allowing it to be easy to identify the caller. SIP also makes it very convenient to identify an emergency call. Where an emergency number is not universal throughout the world, SIP makes a universal URN (Universal Resource Name) and then can route any emergency number to the specific URN. From here a URN is specified by the IETF to determine the specific emergency, such as a fire emergency will be routed to that specific URN. Figure 12 demonstrates how calls are routed in an IETF SIP Network, as well as demonstrating which routes the emergency call would take to arrive at the appropriate PSAP. Not going directly to a PSAP is very beneficial in this situation because a middleman, the ESRP, determines exactly which PSAP will receive the call. This also results in increased security of the system.

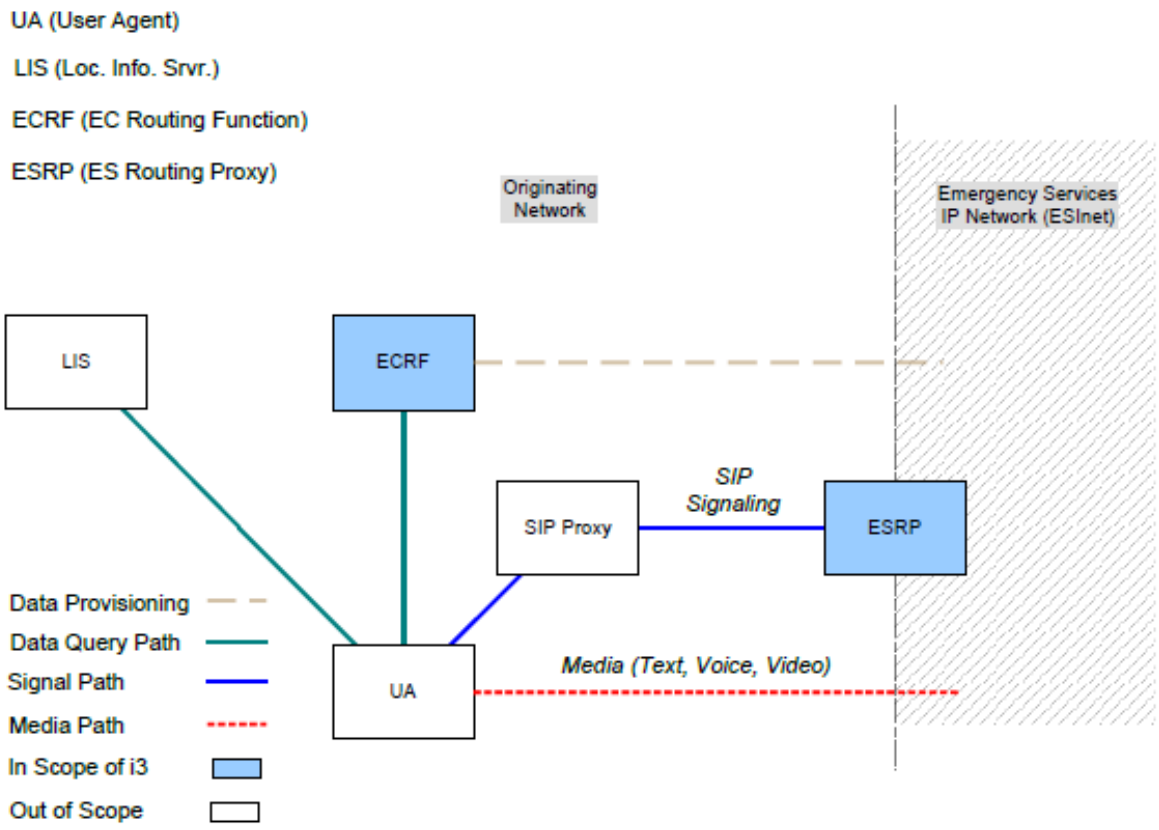


Figure 12: SIP Network Call Routing

If an ESInet were to be created it would need to be developed and run by a regional agency. The IP routers within the ESInet system can be hard wired or wireless and connect to all emergency services at the IP level. NENA basically describes the system as a "Network of Networks." This term means that there will be multiple networks at a state level that combine to a regional level, and then develop a national network. The networks build off of one another to make a super network of IP based infrastructure. This topology mirrors the existing IP network structure.

Another important relationship NENA considers with their i3 document is IMS standards within 3GPP. IMS, IP Multimedia Subsystems, are systems, which control calls. NENA recognizes two main uses for IMS in their i3 NG9-1-1: calling source and producing an ESInet. These IMS roles are important because many providers are beginning to include more services in

their devices, such as VoIP. Figure 13 fits 3gPP standards and is how an IMS origination function would flow to a PSAP in the ESInet. In order to support its i3 NG9-1-1 system NENA has presented a different call flow chart to satisfy the needs of their ESInet. This includes CSCF's, Call Session Control Functions; in which each have different functions. The P-CSCF, Proxy Call Session Control Function, detects the request and then selects an E-CSCF, Emergency Call Session Control Function, which determines location information.

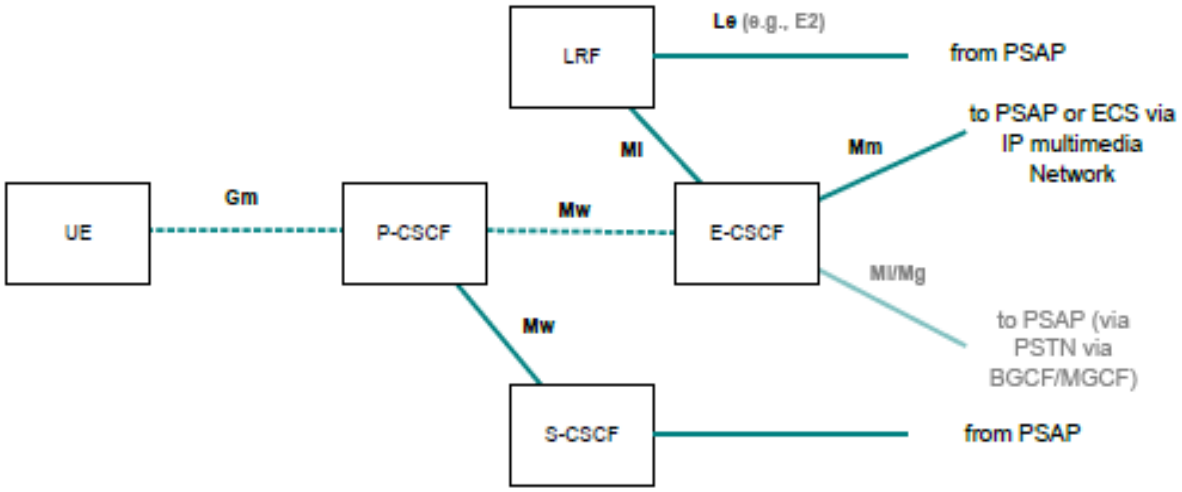


Figure 13: NENA IMS Infrastructure

The P-CSCF also arranges calls in the system as well. This system is demonstrated with the following flow chart representing the flow from the call to the PSAP.

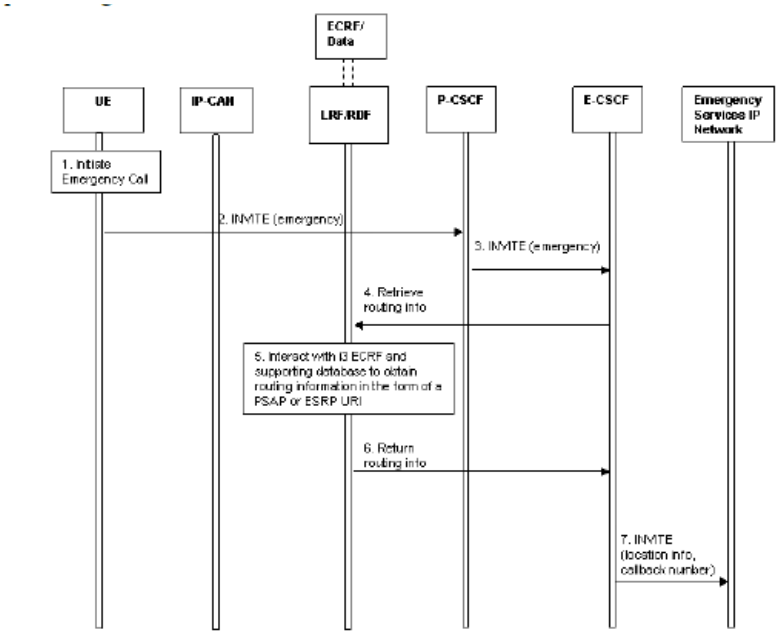


Figure 14: Alternative ESInet Flowchart

The flow of this call originates at the UE or User Element, which sends a signal (a SIP INVITE) to the P-CSCF. The P-CSCF then recognizes the request of an emergency and chooses the appropriate E-CSCF, which obtains information on routing location. After collecting routing information, the E-CSCF sends the signal to the correct ESInet determined by the PSAP.

NENA states that IMS can also be used as an Emergency IP Network. The way in which this architecture would function in which the INVITE signal, ESRP, and ECRF are all vital to determine location and route the call to the correct area. Figure 15 demonstrates the flow from the originating network to the CSCF's and ESRP within the ESInet. SIP signaling is used between each ESRP and then sent to the i3 PSAP network to ensure appropriate flow of the call to the correct part of the ESInet and location determination. Backups for routing in the IMS IP emergency system would also be present to allow for failsafe routing of the call to the correct endpoint.

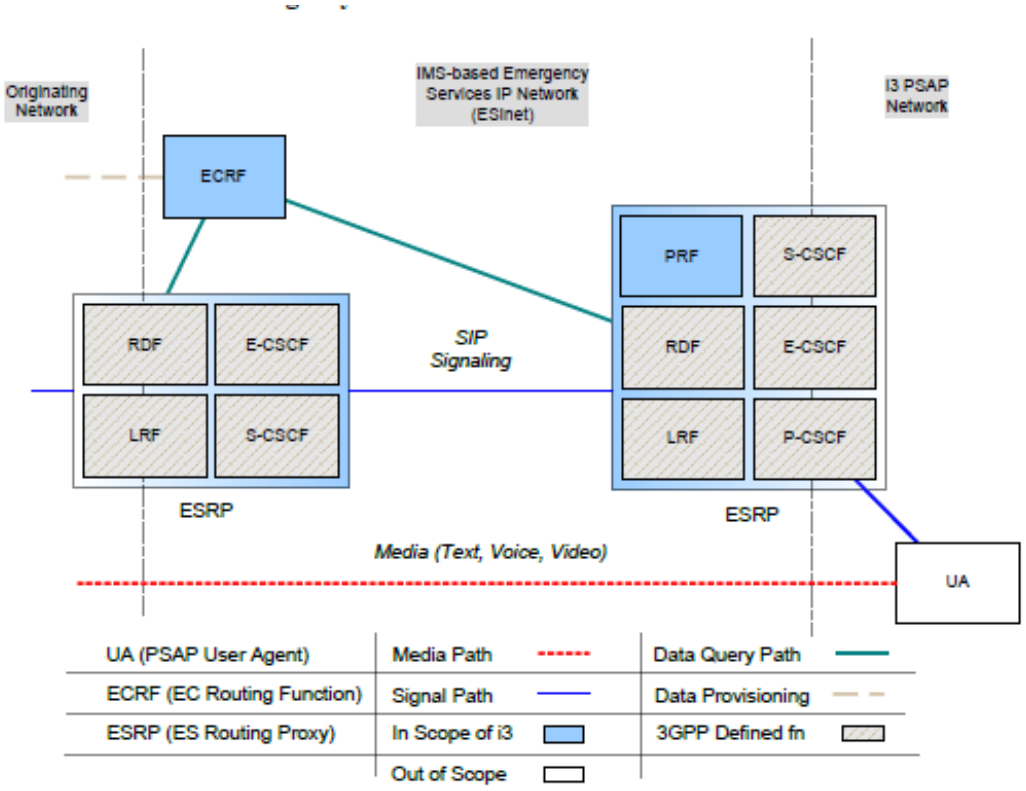


Figure 15: EMS Emergency IP Network

2.7.3 NENA and ATIS

Multiple standards boards have been formed out of the joint work of NENA and ATIS to standardize NG9-1-1. The Emergency Services Interconnection Forum created jointly by NENA and ATIS Works to promotes standards in the NG9-1-1 field. The Technology and Operations Council was created by ATIS to coordinate standards, and identify standards within the industry of NG9-1-1. Another standards Committee, the Packet Technologies and Systems Committee create standards on the architecture, routing, and signaling of communications in IP 911 systems. A final important committee is the Wireless Technologies and Systems Committee in which creates standards regarding wireless and mobile technologies.

2.7.4 Other Architecture

NENA identifies that there will always be wired and wireless connections creating calls to the emergency networks, and these legacy architectures will always need to be accounted for in the network. For hardwired telephones, the connection would be made and then arrive (routed) as an IP in the network for the ESInet to be able to use it in the network. The difference between hardwired phone calls and IP calls is that location information is generally not supported. For this case the gateway will need to get information based upon the caller's phone number and then locate the signal by LIS.

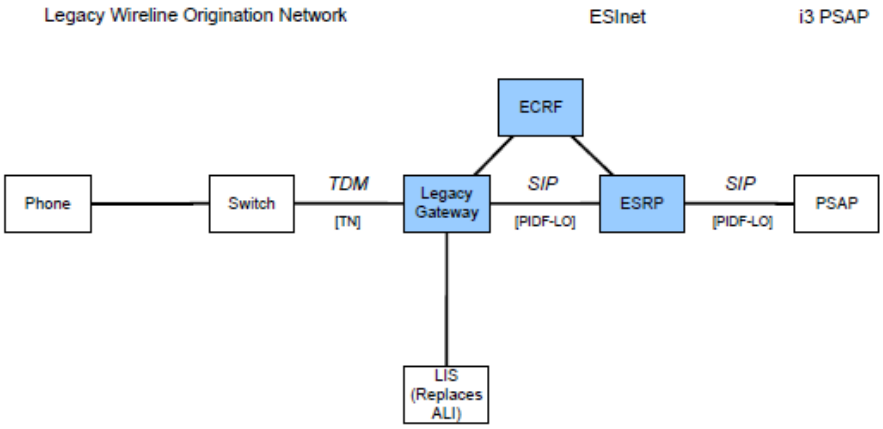


Figure 16: Legacy Wireline Original Network

Much like the hardwired network, wireless networks also need to be dealt with in NENA's i3 system. Calls will arrive and using the ECRF will be routed as an IP. Again a legacy gateway will need to be used to within the ESInet. For wireless use, the LIS will be able to determine the location of the caller via the gateway. The call is then routed further along using the ECRF to determine its correct place in the ESInet. The following figure demonstrates the connection of a wireless device to the ESInet. [10]

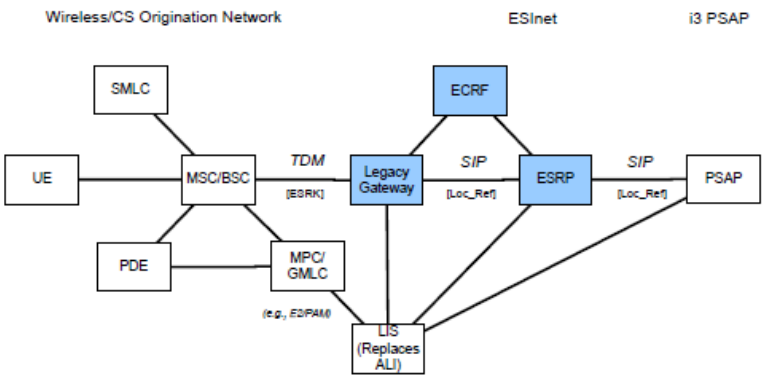


Figure 17: Wireless/CS Origination Network

2.7.5 Security

The need for a security architecture is also present when using IP based networking. The main importance of this aspect is to keep the network free of any potential viruses and/or hackers. This is one main critique of the IP based NG9-1-1 system. Network security means keeping the network free of viruses so that the system is still supported when a call trying to come through can be reported as an important emergency. If a virus enters the system and the system crashes at any crucial moment, an entire country could be without a means to report an emergency. As over 1000 call can be called into any 911 system per day, keeping the network operable is a must. Also if a hacker enters the system, key information on location of the caller and the emergency can be divulged, hence security is warranted. Though NENA does not thoroughly describe the way in which it would have a security infrastructure, it does demonstrate a chart on how to keep the system secure. The security involves three separate security domains, ensuring maximum safety of the infrastructure. The first Domain is within the Originating Network, the second is described as an "optional" domain and is within the ESInet, and the final security domain is in the PSAP network.

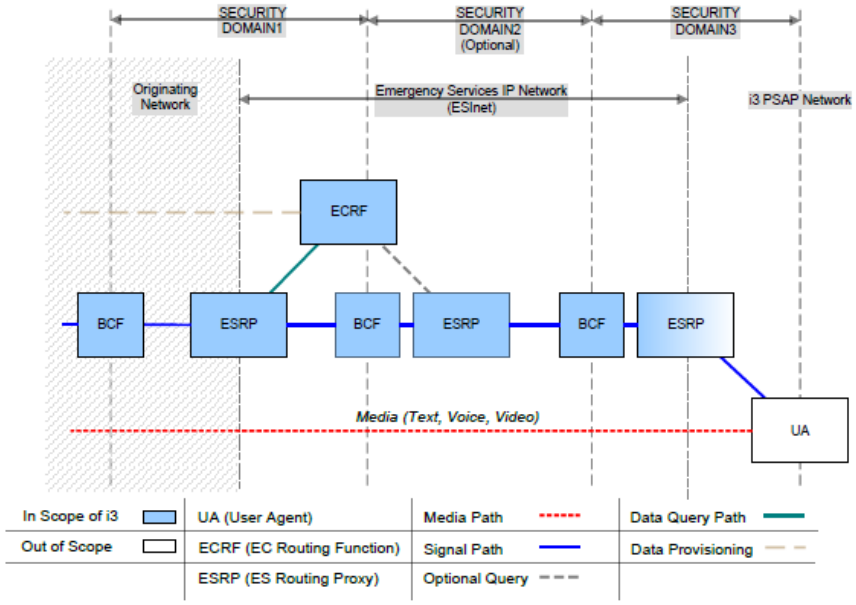


Figure 18: NENA Security Diagram

Security is a key aspect within any network, and the use of firewalls, and virus-detecting software will be needed to operate the ESInet. NENA states that TLS, Transport Layer Security, must be used within the ESInet for communications. There are occasions in which the TLS may not be needed such as if the path from sender to receiver is completely protected, even in this case the TLS should still be used to ensure protection. Certain measures that should not be used as a means of security are perimeter securities and segregating traffic.

Another important means of security is authentication, and NENA identifies this in their i3 document very precisely. The authentication guidelines are very strict and impose that two or three means of authentication be used to access PSAPs. Examples of this type of authentication include passwords and smartcards. NENA also states that every response mechanisms need to be encrypted. Authorization is also touched upon by NENA as well, the ESInet must be able to authorize the roles to access certain parts of the network. These roles include, the call taker, Supervisor, PSAP Manager, Database and etcetera. [10]

2.7.6 Call Flow

When a call is initiated to the 9-1-1 systems, it flows through many aspects before ending at the end point. The call first flows through an ECRF, which is used by the ESRP to route the call to its specified area in the network. The calls go through a Border control function, which secures the IP network against any type of attack such as a virus. Another Border Control Function would also be present between the ESInet and the PSAP further securing the network. When the PSAP finally obtains the call, it routes the call to a body receiving the call. If a call comes in with the wrong IP address the ECRF will be able to use that existing address but depending upon the situation the ECRF can add a portion to the address delegating which emergency service is needed.

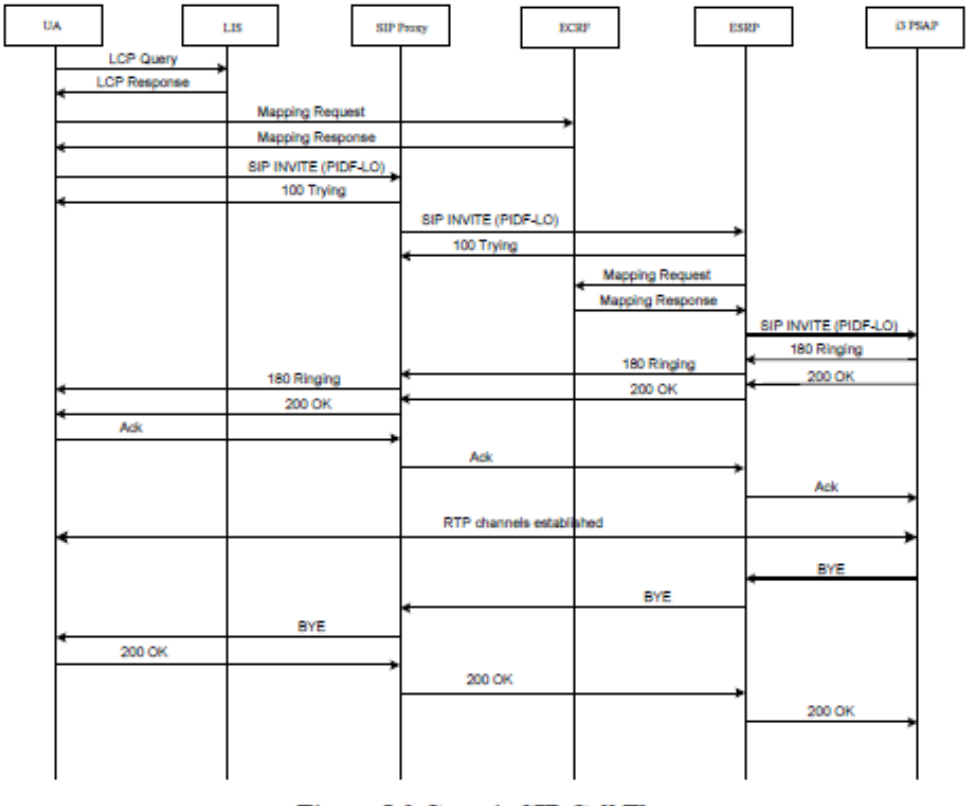


Figure 19: SIP Call Natural Flow

If a legacy call is received, two important functions need to be used in order for the call to enter the system a "location retrieval function and a routing determination function." The location retrieval function changes the legacy information into readable location information that the network can use for routing purposes and send to the routing determination function. The same ECRF will be used for all legacy calls and then determine which PSAP will receive the call. When a call is routed, a routing function is generally applied at all ECRF. The Policy routing Functions determine multiple facets of the call, including location, time, PSAP state, and caller classification.

There are also some abnormal conditions that NENA identifies at multiple levels. At the ESRP level many things could happen such as not identifying the ECRF, no routing information, or not response from the ECRF. Abnormalities here result in no information to route. If these errors occur the ESRP defaults and routes the call to the default area. NENA also states that if information was unable to be found from the ECRF because of an error message then the ESRP will find which URI to send the request. In each case a default URI or alternate URI's are provided to get the call to the ESInet to connect with the PSAP. Abnormalities also occur at the ECRF level including, a poor routing query, not identifying a PSAP URI, or a lack in authorization. In each of these cases NENA points out that the ECRF will send and error message to the ESRP.

IMS call flow has multiple steps as well that is very similar to basic call flow. Most of the functionality is location identification be the ESRP and LRF/RDF. Once the location information is determined the information is sent to the en point PSAP [10].

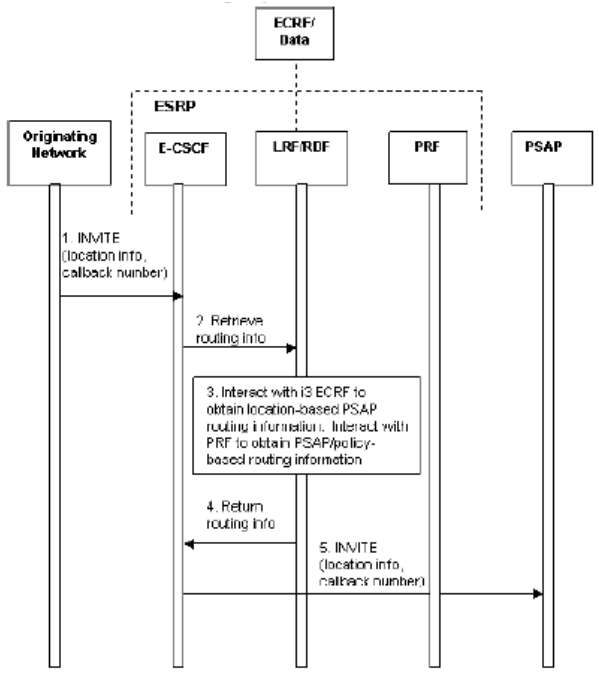


Figure 20: IMS Call Flow

2.7.7 Information Flows

The PSAP must acquire authorization via registering and deregistering so emergency calls can be delivered. To register the PSAP a request is sent to the Authorization, Admission and Accounting server and the PSAP also sends its credentials to the server. The ESRP then informs the PSAP and routes.

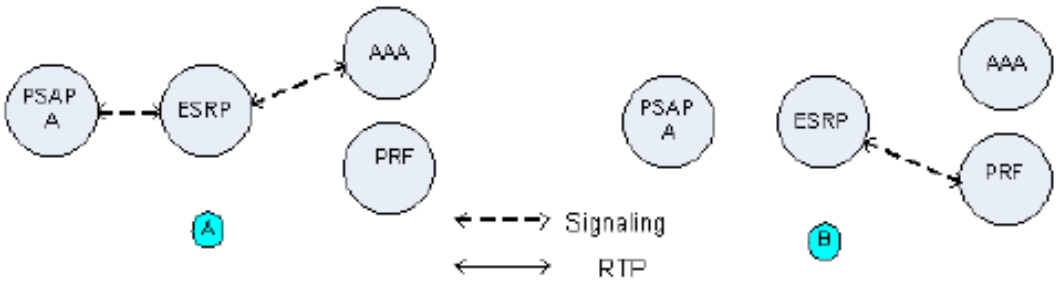


Figure 21: Information Flows

The PSAP can also send a deregister signal to the server as well. Also if the PSAP needs to complete an action it can subscribe to a state subscription.

In an IMS based network, the call first starts an emergency request that is sent to the P-CSCF, which chooses the corresponding E-CSCF and begins an emergency session. The system then determines how the call should be routed and then interacts with the ECRF locating the information of the location. The information is then sent to the PSAP within the ESInet.

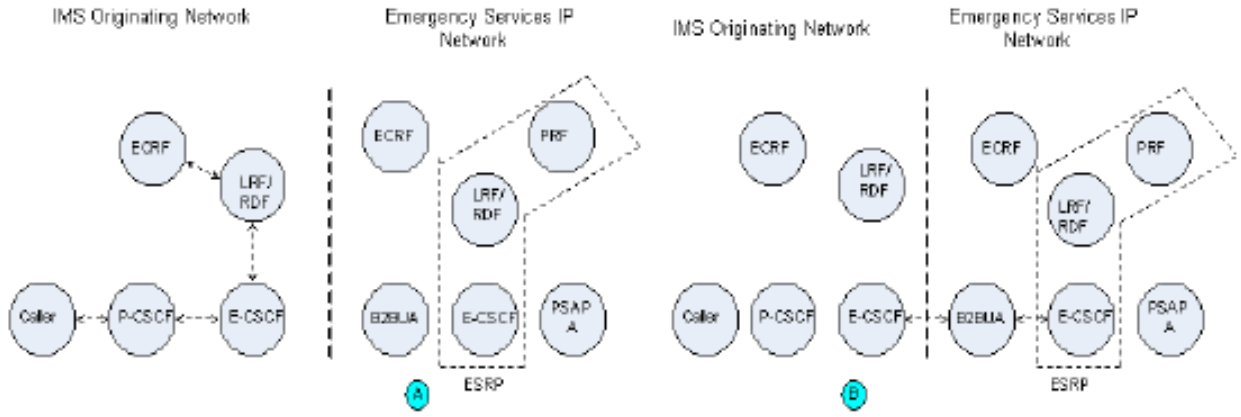


Figure 22: Signaling in IMS Calling

The PSAP can also become busy in an IMS system. If this occurs NENA recognizes that the call must be routed to an alternative PSAP. First a request is sent to the ESRP, routing instructions are then given. Once the ECRF is reached, a PSAP address is given and location information is reported in the form of a street address or geological information. Also, when routing through the LRF, multiple alternate PSAP addresses are given. If one of the PSAP's is busy an alternate route will be chosen and the signal will reach the endpoint. If the PSAP is unreachable an alternative PSAP will be called. If the alternative PSAPs cannot be reached, then the ESRP function defaults.

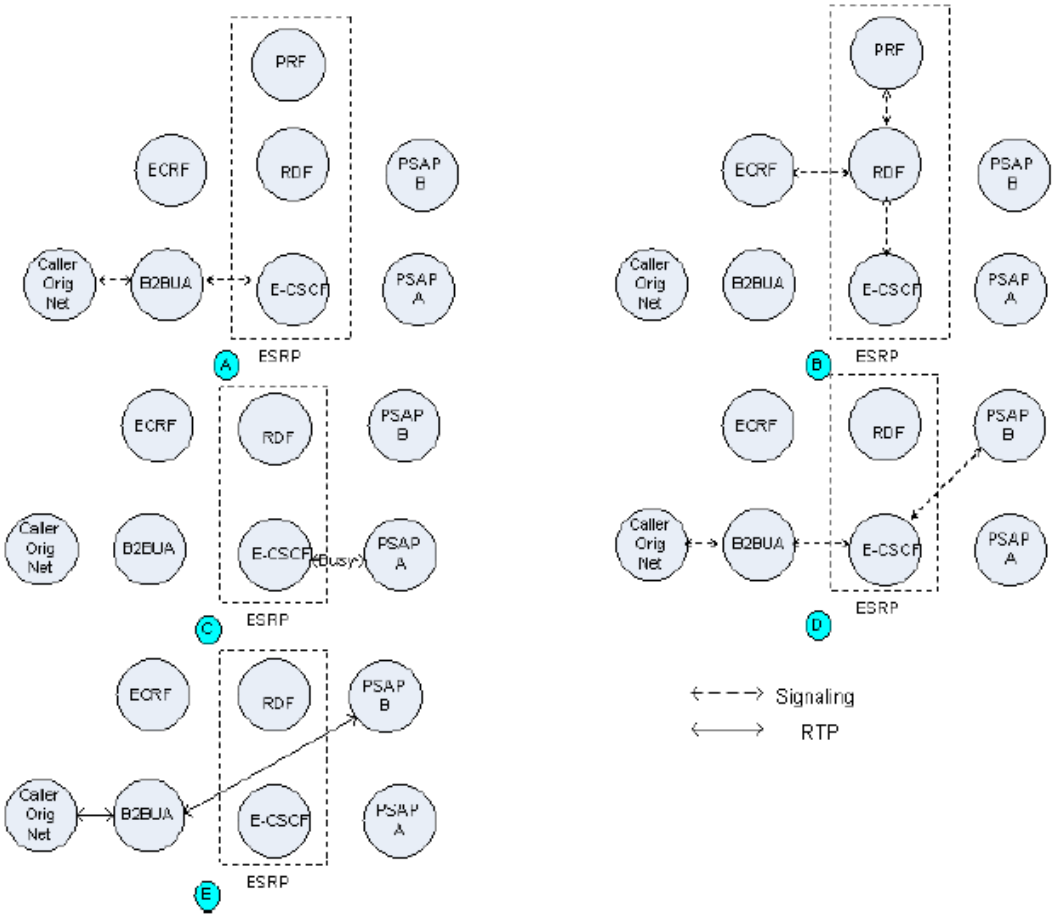


Figure 23: Accessing an Alternate PSAP

Another important situation NENA defines is what route the Call will take if the PSAP is unavailable to take calls. In the case that the PSAP is unavailable it is required to deregister and then the ECRF chooses the most important PSAP. However, if it is not in service, an alternative PSAP will be sent to the E-CSCF. The flow of the call when the primary PSAP is unavailable is demonstrated in further depth with the following flow chart, showing the call path from initiation to the ESInet.

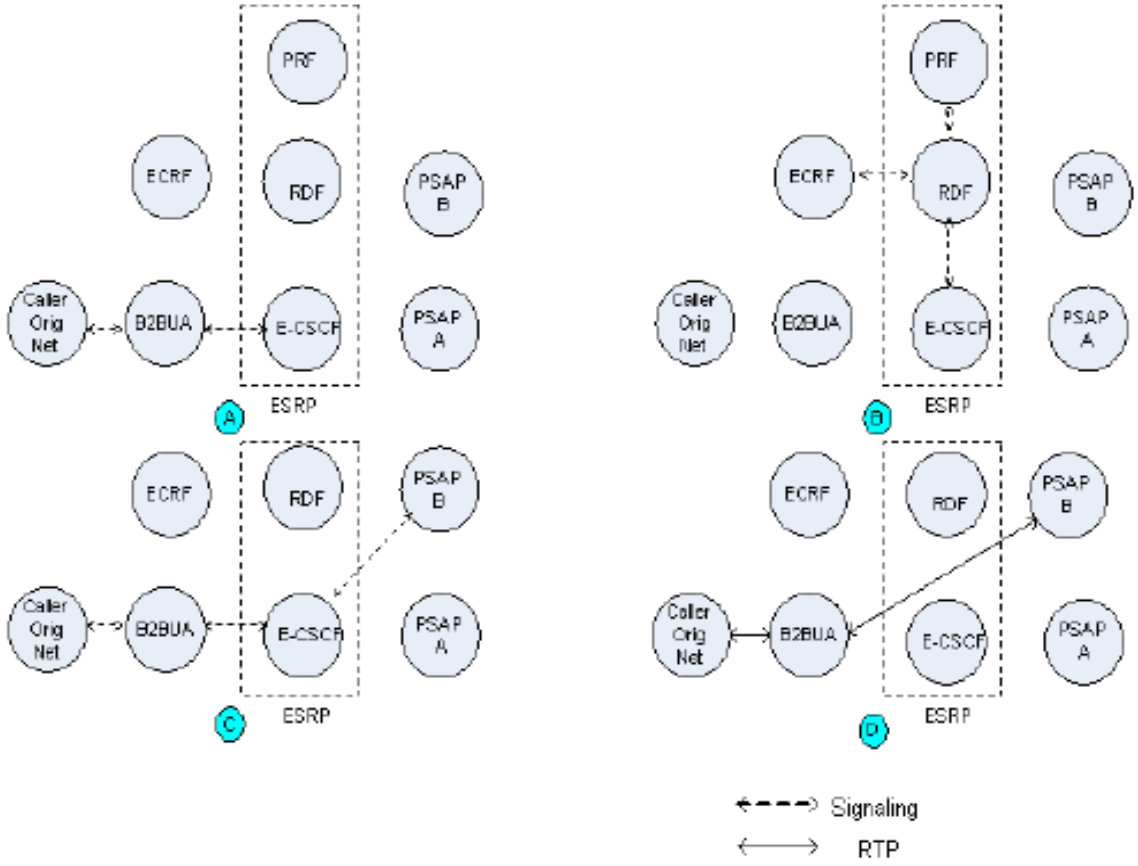


Figure 24: Call Path, Initiation to ESInet

Overloads can also occur in the system with the copious amounts of calls that are routed through the ESInet. The i3 system contains the problem that the number of calls going through the system will most likely exceed the number of call takers. The two main types of over load that could occur are PSAP Overload and Elemental Overload. A PSAP overload is when the PSAP is unable to answer calls being routed to it, this occurs when there is an immediate increase in the number of calls. An Elemental Over load is when an element in the system cannot take the number of signals being sent to it, this also occurs when more calls are coming in than the system can handle.

In the case of a PSAP overload, calls are diverted to alternate PSAPs if there are an overload of calls and not enough call takers. That PSAP will have to provide all the information

that the original appropriate PSAP would have given. In this diversion process, the PSAP must be able to accept the diverted call and a difference needs to be recognized between a diverted call and an originally routed call. This PSAP is able to access the appropriate ECRF that the original PSAP would have signaled to ensure correct responders are notified of the situation.

In the case of an elemental overload, the ESInet would be experiencing traffic that exceeds its capacities. In most cases a service error will be sent to the by the overloaded element, but the error needs to be completely correct. If this is not the case a busy signal will be sent by the element reporting that it is busy and cannot receive a signal due to the shear load that the element is experiencing. [10]

2.7.8 Bridging

NENA Also touches upon the very important aspect of bridging PSAPs. The bridges present are SIP based and use bridging in a multimedia manner for bridging calls. This function is used to transfer calls to PSAPs and redirects a wrongly routed call to the corresponding PSAP. In bridging the first step is to connect into the conversation. The PSAP then recognizes the need to bridge the call to another PSAP. An ID is then given to identify the bridged parties in the call. A signal is then sent by the PSAP to join the conference and the caller then joins the conference.

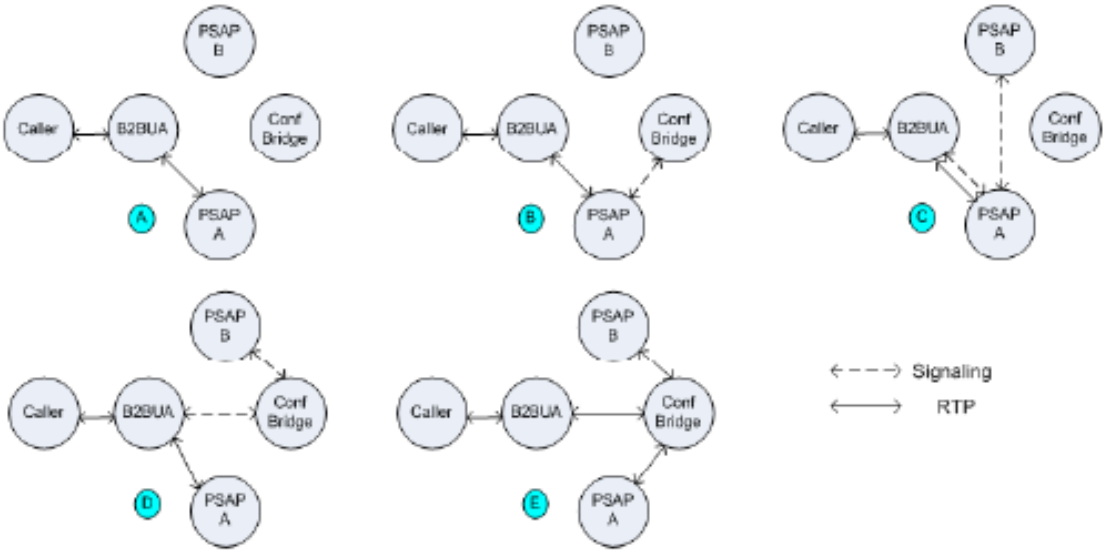


Figure 25: PSAP Bridging

Services are also an important part of the ESInet. A service needs to be recognized by a service provider. A Service is defined as "an abstract resource that represents the capability of performing tasks. The two most important aspects of a service are the service provider and the service consumer. The service provider is the portion that "exposes and implements the service and its interface, making it available." [10] The service consumer is "the part of the entity's behavior that makes use of the service via the service interface." [10]

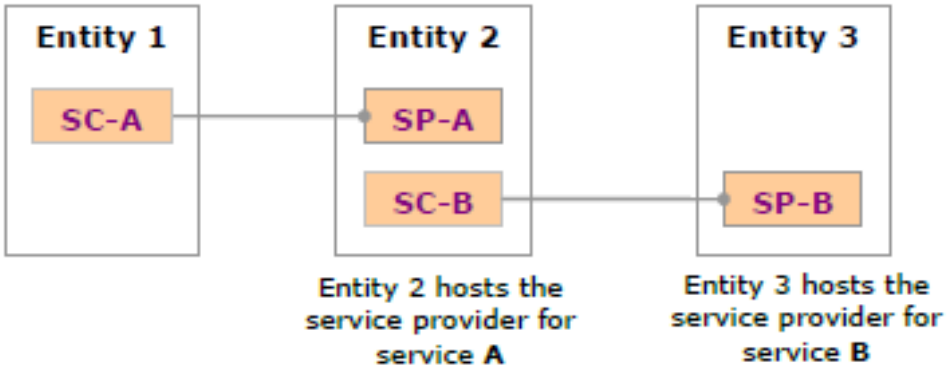


Figure 26: ESI Services

The ESInet architecture and the IP PSAP host both roles of service provider and service consumer to ensure the interface is satisfied. The architecture in which a service is created consists of the following: a correlation, sequence, aggregation, cache proxy and mediation. According to NENA, the correlation simply correlates information, sequencing allows providers to receive and complete the action signaled. The aggregation compiles information and makes it available to consumers. Mediation gives an overall singular appearance of the service interfaces within the ESInet.

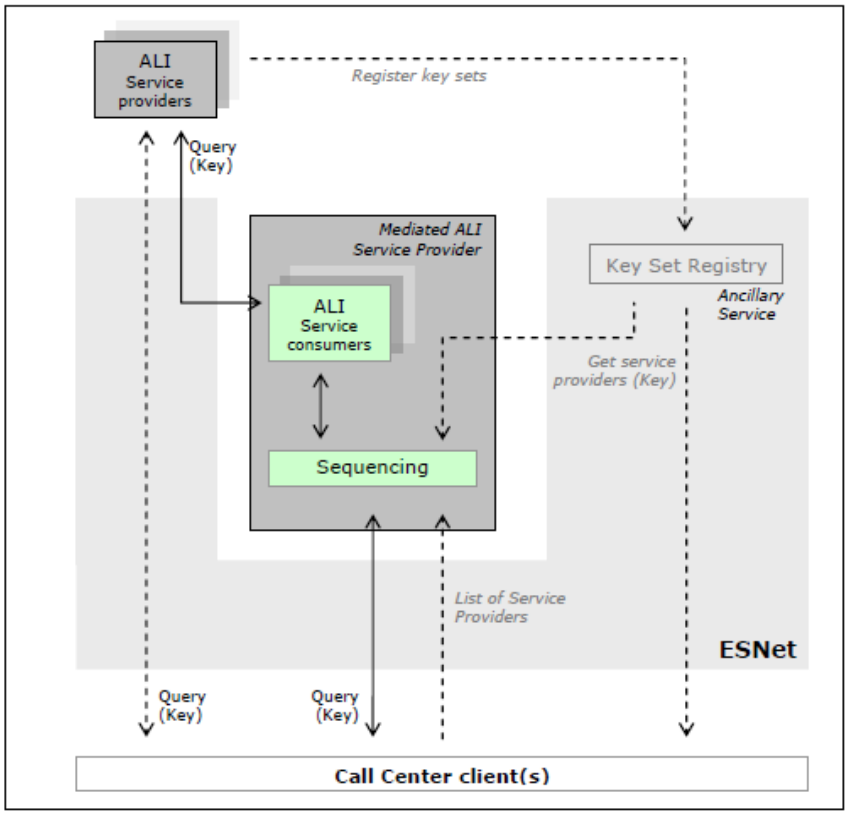


Figure 27: Singular Appearance of ESI Services

The way in which a service is specified is demonstrated in Figure 28.

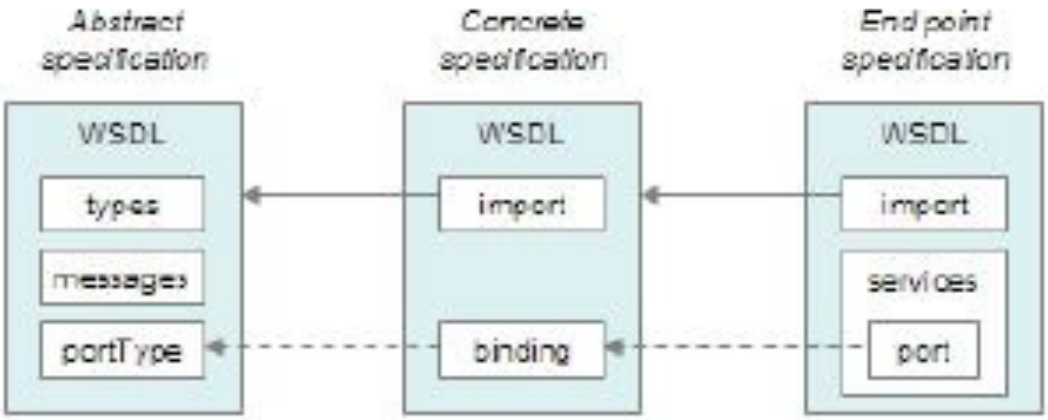


Figure 28: ESInet Specified Service

Services also need to register within the ESInet, and the service provider usually does this. Exposing the interface through multiple bindings allows the discovery of a service. Services also come in different types as well. Data is associated with every aspect of the call, the caller, and location.

Logging is also an important aspect. The ESInet provides a logging service, and logs every important event that happens in the network. The PSAPs can also have their own logging action. All forms of multimedia processed through the ESInet are logged and recorded using the ESInet logging service. Types of multimedia that can be logged and time stamped are audio, video, text and many other forms of multimedia.

The i3 document raises a standard to NG9-1-1 IP based system that can be used to compare other NG9-1-1 IP based systems. NENA's i3 allows for a basis for NG9-1-1 systems to come and how to approach an IP base NG9-1-1 system. [10]

Chapter 3: Project Outcomes

3. Introduction

Chapter 3 focuses specifically on our feasibility study, describing our findings and solution to challenges within IPW-911. In the previous chapter, several technologies and laws were examined in order to determine major challenges, which must be addressed in order to meet the string requirements of an E9-1-1 network. These requirements are necessary primarily due to the cost if the network were to fail in emergencies. Therefore any drawbacks of the solutions themselves are discussed as well.

3.1 IPW-911 Analysis

When it comes to addressing the technological barriers to planning and implementing a fully IP-enabled emergency communication infrastructure, there are a variety of issues to resolve. This section will examine architectural technology schemes, which control the flow of information across the various subsystems of this infrastructure. While there is need for a wholly new services or technologies to fill holes that present technologies lack, for the most part, society is completely capable of implementing a diversely functional, redundant, secure, quality IP-enabled 9-1-1 today with present capabilities. The matter that is still in need of definition is the standardization of the various communication and infrastructural technologies, which make up the backbone of what would be the new 9-1-1, so that a measure of control and quality of service can be guaranteed.

The first matter of standardization addressed here engages the work of O'Reilly, Richman, and Kelic in their paper titled "Power, Telecommunications, and Emergency Services in a Converged Network World [15]." As they present, "[c]ritical national infrastructures for

power, emergency services…, and other basic industries rely heavily on information and telecommunications networks (voice, data, Internet) to provide services and conduct business." It is possible to see their point graphically in the figures below.

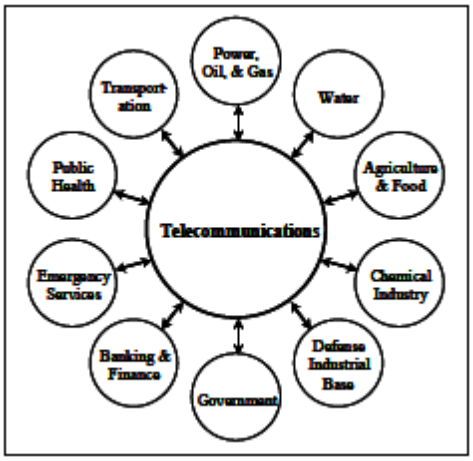


Figure 29: Pairwise Inter-Infrastructure

The problem that is presented by this is evident in the cascading nature of impacts across infrastructures in the case that the Power infrastructure is disabled or disrupted. Since the Telecom infrastructure relies and the Power Infrastructure, and consequently the Emergency Services Infrastructure is reliant on the Telecom infrastructure, we see a vulnerability, which is based on the continuous and undisrupted supply of power.

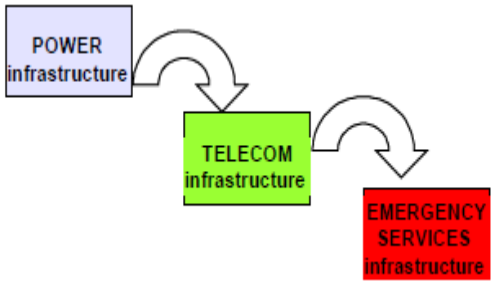


Figure 30: Cascading of Impacts across Infrastructures

The case being described by O'Reilly, Richman, and Kelic is true today, however, the point that they are primarily making is that as network services are converging in the world. As they are now, services today, which are highly reliable, might become less reliable as time moves on. The conclusion these authors draw is the need for battery reserves on the cascading infrastructure elements in future converged networks to handle the stress of power instability caused by blackouts and other such events. While this is done today to some extent, battery backup systems are expensive and require maintenance. Batteries themselves are also very expensive, and must be replaced at intervals. For this reason, many network elements go without power reserves. This means that in the event of an emergency situation, which causes, or is caused, by a blackout or other disruption of power that the remaining operating elements are stressed much higher than expected. This can lead to them failing due to load, or shorten their expected battery backup operation due to increased power consumption.

It is with this in mind that the authors of this paper suggest the need for continued research efforts into power backup methods, paired with continued efforts to back up the present infrastructure. There is a need to determine a minimally efficient mapping of the various communication infrastructure elements throughout the country, taking into account redundant and emergency routing schemas, so that there is minimally a dual-redundant, and preferably triple-redundant, backbone to all regions. This would identify the minimum number and location of elements, which require proper backup systems. This would require coordination outside of the regional/statewide operators of the system elements concerned, as the distributed nature of power and the consumption of that power does not fall easily within regional/statewide lines.
Other concerns, which address the shift of Emergency Services towards IP-enabled technologies, include security and regulatory matters.

IP-enabled services would serve as the background of a future EMS and 9-1-1 lifelines. Much of the initial concern is surrounding the difficulty of localizing IP network communications as they traverse the World Wide Web's IP infrastructure. Inherently diversified architecture of the web creates the unavailability of mechanism inherent to IP technologies. Reliable location information from a caller would be generated, as well as location information, which is required for first responders to appropriately act to help in the event of an emergency. Two prominent applications of IP networks for communication are VoIP, Voice over IP, and SIP, Session Initiation Protocol. In the paper "A VoIP Emergency Services Architecture and Prototype," authors Mintz-Habib, Rawat, Schulzrinne, and Wu discuss possible solutions to the matter of embedded location information in the packetized data, which constitutes the VoIP call [12]. The problem with the present VoIP implementations is that, if they provide any location information at all beyond the services provider, it has a tendency to be inaccurate or out-of-date. The operator of the service has the responsibility to create a server which identifies the location of a particular end unit. This results in a cost and operating expense that is secondary in many cases to other operation efforts. The responsibility of the end-user is to update that information should it change. Since VoIP is very popular in large and distributed businesses as well as in multi-dwelling homes (where the services are often cheaper), it is fact of the present implementations that the information in the system is often inaccurate or simply incorrect. The authors suggest that the development and use of specialized IP gateways, which initiate an extra layer of localization as communication is taking place, would alleviate much of the problems associated with the present VoIP implementations.

This point is reiterated and expanded on by "Improved IP Network for Emergency Service," by Khan, Saeed, Nazir, Bilal, and Ayub [20]. Where the authors of this paper

expanded was in the area of choosing an element of the callers IP system which to bind to a fixed service relay in DHCP servers. They suggest that the MAC, or Media Access Control, address, which is unique to each IP-enabled device, be used to bind an IP-enabled device to its location, determined through a DHCP relay at the point when access is given to the Internet for a device. You can see a figure, which details the architecture they propose below. The advantages of this architecture, in the words of the authors, lie in the creation of deterministic architecture from a probabilistic one, while also simplifying the architecture and reducing the installation cost of Location Information Servers (LIS).

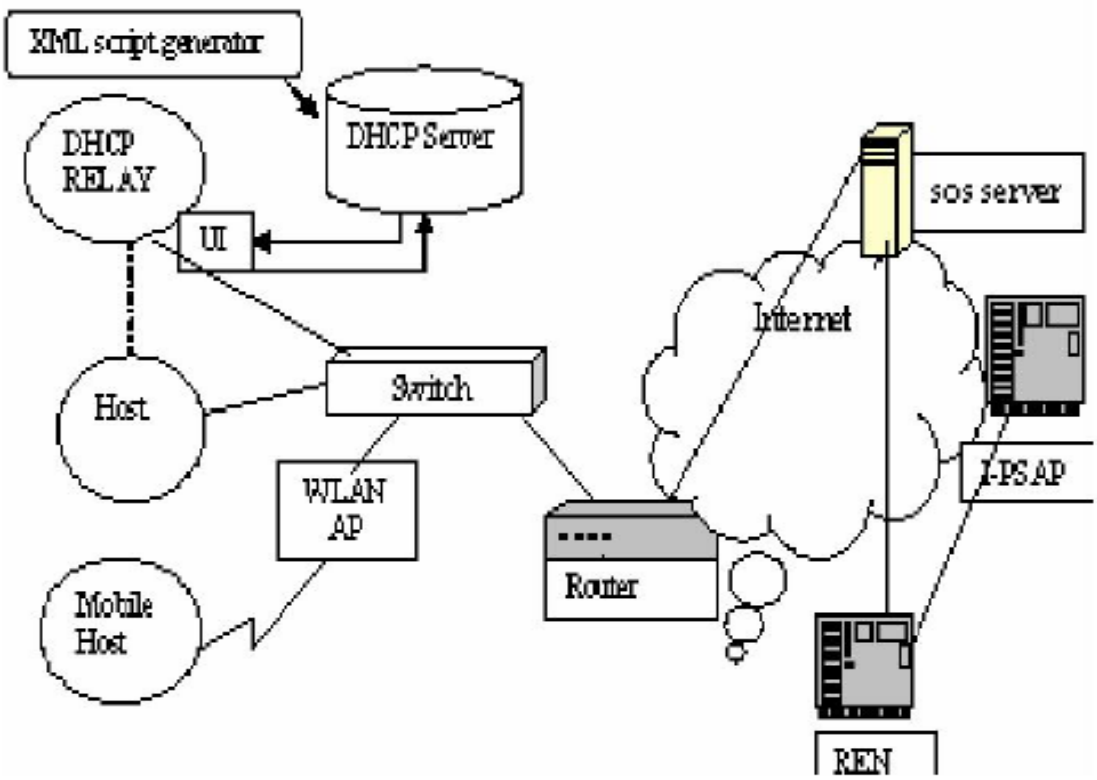


Figure 31: Proposed Architecture with DHCP Relays for Location Acquisition [20]

The presence of distributed and divergent networks, which are growing to characterize the primary means of intercommunication for private and public entities, are necessary to adapt our understanding of how to provide these infrastructural services in order to mediate the challenges of the new network schemes. This is accomplished while expanding present functionality to increase user and operator abilities where possible. Authors Feng and Lee of the paper "Exploring Development of Service-Orientated Architecture for Next Generation Emergency Management Systems," make great strides to develop a language with which to construct new architectures, which embrace the new methodologies that are needed in emergency communications [13]. They define a generic SOA (Services Orientated Architecture), as a design of a distributed system which aims to maximize the reuse of multiple services so as to simply the overall architecture without sacrificing the ability to meet the needs of an increasing complex world. The SOA platform services generally have the following characteristics:

- Service are autonomous;
- Services are loosely coupled, "[implying] that services discover the needed information at the time that they need it." An ability which affords services "flexibility, scalability, ability to be easily replaced, and fault tolerance;"
- Service can work in a choreographed nature to execute operations which depend on the messages that are sent or received;
- Services can easily discover one another, hopefully automatically. These characteristics would require meta-data of the services, such as their capabilities, interfaces, polices and supported protocols, to be exposed by the services to each other so that they may interwork seamlessly.

This sort of SOA platform design is heuristic in nature and must essentially be customized for any end application, due to the fact that services in heterogeneous systems are characteristically unique, and do not lend themselves to an open-source, generically repeatable, form factor. An example of what is meant by such a SOA platform is depicted in the figure below. It is possible to see that the workflow across the diagram is performed by the interaction of a subset of repeatable elements which communication with each other in defined manners.

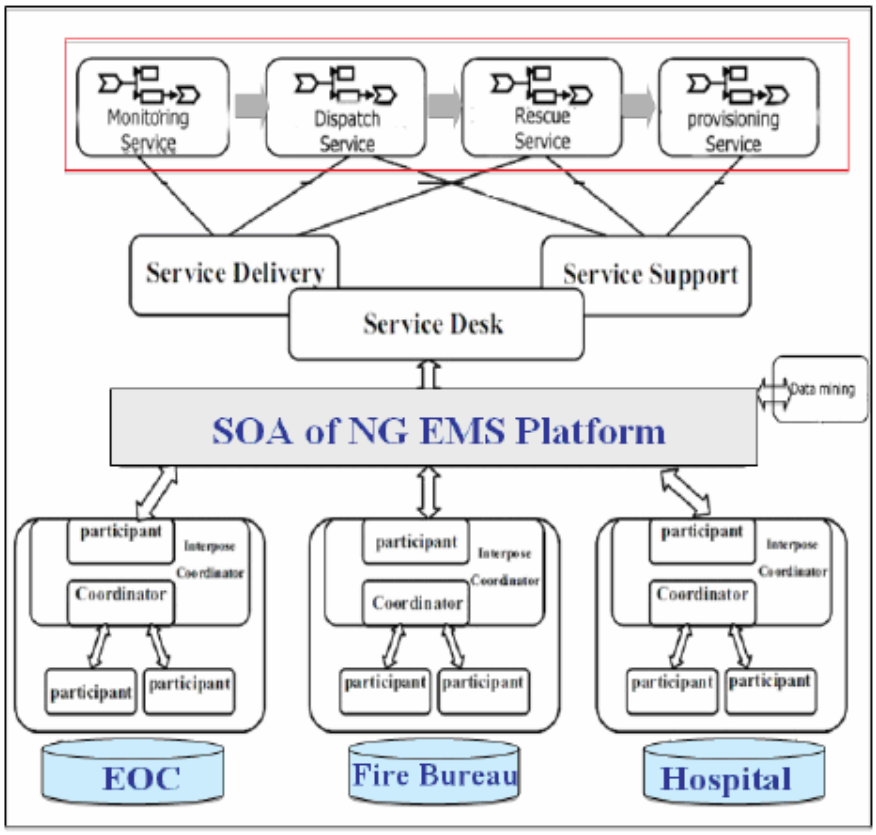


Figure 32: SOA of NG EMS Platform Structure

Much of the advantage of this SOA structure is also attributed to 3-layers architecture pictured below. At the bottom level you see the Service Layer. This is the “front line” of the EMS architecture. It provides congenital emergency services and it represents a configurable array of

service elements, which can be used to implement the present EMS capabilities, while expanding them as well. Above that we have the Process Layer. The Process Layer serves to communicate meta-data between the services by publish service specifications within the platform to all connected services. It also serves to link the higher-level management of the manner in which services are orientated. The uppermost layer is the Domain Layer, which provides the highest level of management oversight, which can be supplied by emergency agencies or government organizations.

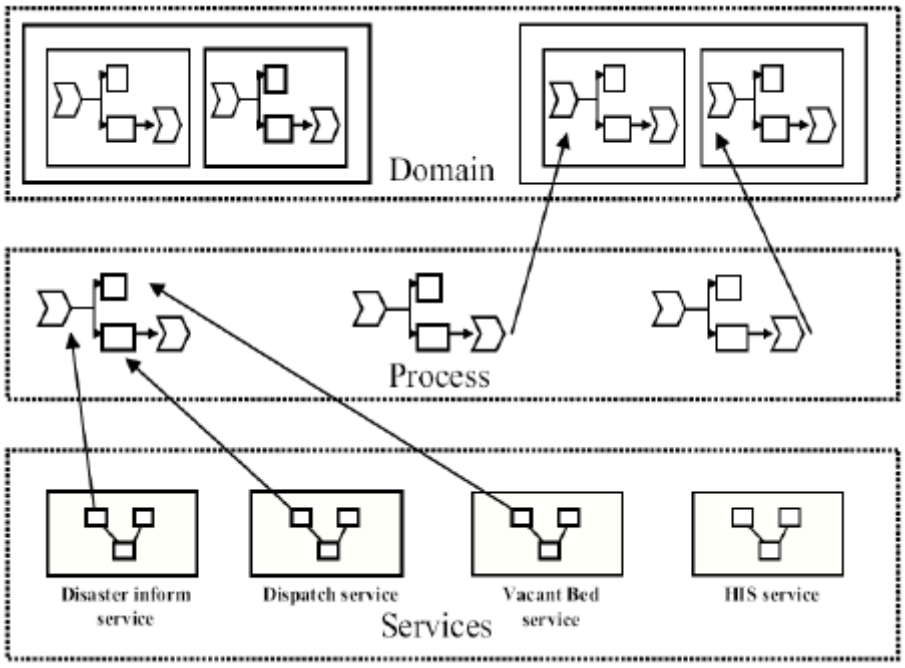


Figure 33: EMS Domain Service Processes

In the end, the benefit of such a services orientated architecture is a highly efficient and sensitive system, which can address each of the requirements of an Emergency Services operator with proper granularity. It also serves to alleviate response latency by providing an efficiently and well-defined system by which the communication process is implemented.

In order to facilitate the construction and configuration of such a services-orientated platform, it is going to require some specialized hardware on the part of the IP providers. Gateways, as mentioned earlier, bridge 2 or more different communication protocols, adapting the data so that there is a seamless exchange between the two systems. These gateways, however, are expensive and often proprietary. In "Open Multi-Purpose Gateway for Emergency Services Internetworking," authors Varakliotis, Stephan, and Kirstein address the matter of open platforms, which can address incompatibilities introduced as a result of widely disparate uses and varying capabilities of the various devices needed in the communication architecture of Emergency Services [14]. The emphasis on the use of open-standards for the implementation of these multi-purpose gateways would serve to provide a combination of benefits: open-standards mean that more manufacturers can introduce products and lower prices and better products will emerge in the industry. These gateways will be able to dynamically handle highly heterogeneous systems more capably than traditional 2-way proprietary gateways, which are most common in industry. Heterogeneous capability also leaves room for later integration of new platforms and technologies with less expense and time. Such gateways will also serve to simplify the overall architecture of emergency communication by reducing the overall number of components necessary to basically implement the system.

One such system concept, which could be more easily adopted along with the implementation of open multi-purpose gateways, is that of SALICE (Satellite-Assisted Localization and Communication System for Emergency Services) [16]. A research project with a plethora of goals, SALICE can be generalized as a system, which enables reconfigurable NAV/COM devices, and systems that are satellite based to be integrated into the emergency communication infrastructure. However, it is not so simple as just adding in extra data packets

with GPS data, though this would be a simplified version of the type of process the authors are calling for in SALICE. Re, Morosi, Jayousi, and Sacchi are hoping to define a methodology for responding to incident areas which utilizing situational data provided by NAV/COM satellites and there various terrestrial counterpart devices (e.g GPS receivers, navigation aids, etc.). While the baseline SALICE scenario is somewhat specific in nature, it requires the creation of new roles in the emergency responder services. The generic ideas of integrating situational awareness in a higher level communication infrastructure which supplements data collected on by other means to provide actionable intelligence holds great potential for emergency responders. Military forces have long implemented similar concepts. The benefits of which are highly documented and virtually universally favorable.

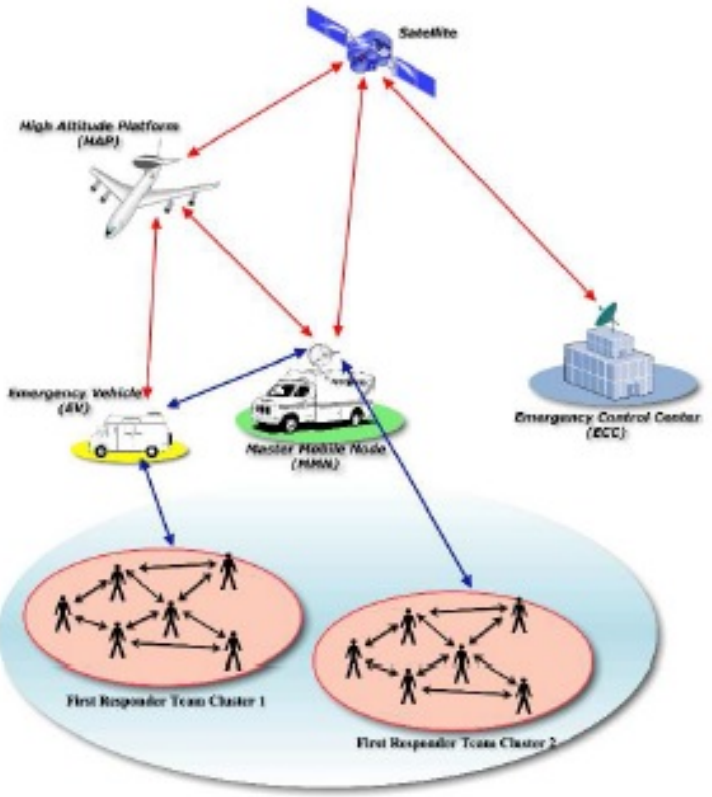


Figure 34: SALICE Baseline Scenario

3GPP IMS (IP Multimedia Subsystem), a new case of EMS architecture still being researched, has a major impact. 3G services are arguably the closest practical implementation of a ubiquitous wireless interconnection infrastructure. It is of great interest to many parties whom are seeking to expand the present capabilities of EMS and EMS responders. While most emergency communication networks around the world today do not actively accept IMS content as an input for emergency messages to be delivered, their eventual integration could mark a great expansion in present capabilities characteristics with more multi-modal communication methods (the use of images, data, and videos in addition to simply voice). 3G networks consist of "a control layer that enables the seamless provision of IP multimedia services to end users. While the 3GPP organization has a standing IMS emergency services architecture, however, there are a great deal of area for improvement in its formulation, as is addressed in "Enhancing the QoS and Resource Management Aspects of the 3GPP IMS Emergency Services Architecture [17]." As authors Barachi, Glitho, and Dssouli address in their work, the solution provided by 3GPP only provides preferential treatment for public-initiated emergency communications. It fails to offer any special treatment for "mission-critical calls, PSAP callbacks, and urgent communications among citizens." This preferential treatment is also handled at the application layer, and not at the transport layer. In other words, once you complete your message and send it, the service identifies it as a priority message. This is in opposition to the manner in which the 911 system is set up on the PTSN, in which as soon as 911 is entered in that sequence, a series of events occur to immediately initiate an emergency priority call. The difference between application and transport layer implementation of prioritization may lead to unacceptable emergency session setup delays and even emergency session failures when there is a strong contention for available

transport resources. With the introduction of a new QoS profile for emergency sessions, along with a transport layer implementation of prioritization, could create viability in IMS emergency services, which would enable their reliable use in EMS systems.

The same authors, along with the addition of Khendek, also have investigated the potential to enrich IMS emergency service with a richer set of contextual information, which could be exploited to enhance emergency services and create a more efficient operating system. In "An Architecture for the Provision of Context-Aware Emergency Services in the IP Multimedia Subsystem," the authors delve in to this mater precisely [18].

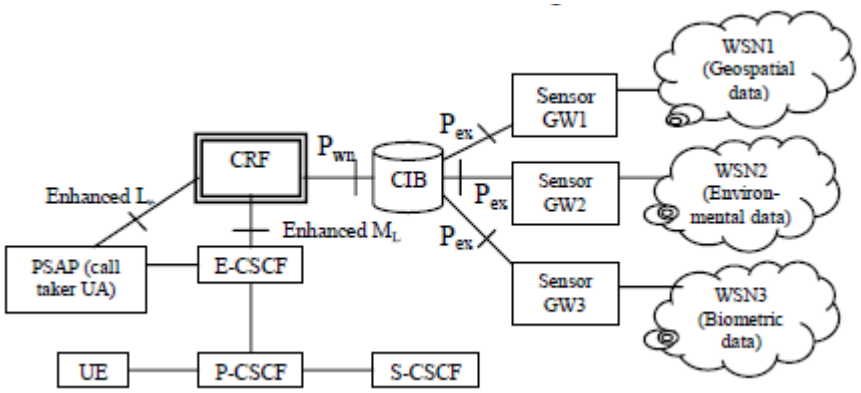


Figure 35: Extended IMS Emergency Service Architecture

Where WSNs are wireless sensor networks, GWs are sensor gateways, CIB is context information base, and the CRF is the context retrieval function. As can be seen in the figure, geospatial, environmental and biometric (in this example) data are being retrieved and given to the PSAP operator at their initiation. This wealth of context specific information allows the PSAP operator to respond more intelligently and efficiently to a given emergency situation.

When it comes to the character of networks such as mobile networks, new terminology was needed in order to efficiently advance technology in the field. A generic term that is often heard when speaking of mobile networks is Ad-Hoc. This has the meaning of being formulated or coordinated at the time of origination with the resources and paths are best available to meet the needs at that time. This is contrasted with such systems as the PTSN network, which is deterministic at its outset. One can determine, in advance, the path, or possible paths, which a call will take from one location to another in advance of ever making the call. With Ad-Hoc networks, such as 802.11 Wi-Fi, or cellular networks it is practically impossible to determine in advance the path a message is going to traverse prior to its origination, or for that matter to replicate a single path. This is due to the fact that TCP/IP and other IP networking protocols take advantage of the resources available at an instance in time and utilize methods such as broadband communication, multi-casting, message forwarding, time-to-live functionality, and methods of recasting messages in order to ensure a proper traversal of the OSI network model for IP infrastructures. The OSI model characterizes any interconnection of systems and enables a language for referring to networks. You can see the Transport and Application Layers we were referring to previously. Starting with the Application Layer, the, generally referred to as Layer 7, the top 4 layers are defined within the host. The lower 3 layers fall within the domain of the media.

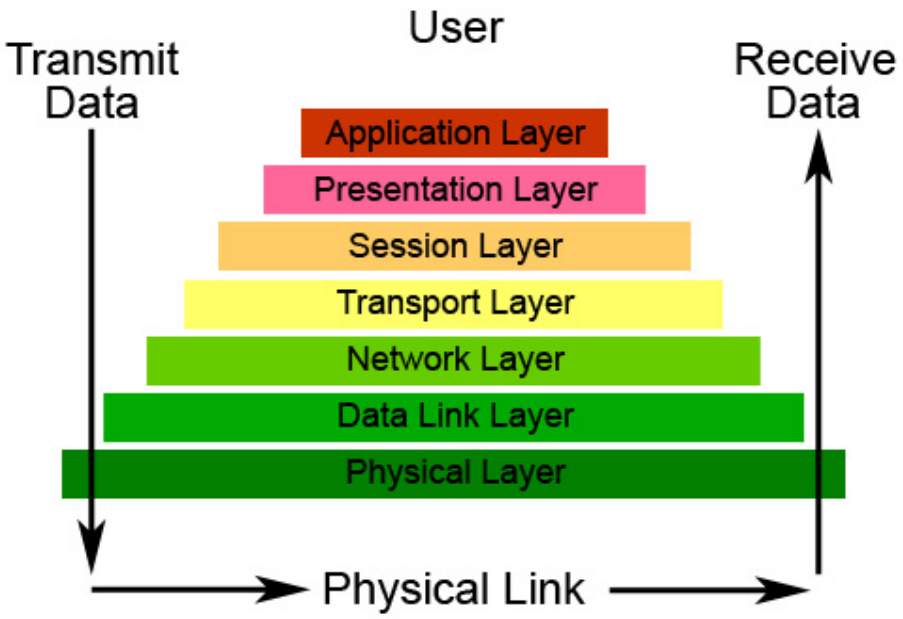


Figure 36: 7 Layer OSI Model

The boundary between the host and the media is an important place to examine in detail when we are discussing divergent and mobile networks as we are here. The Transport Layer is responsible for end-to-end communications, reliability and flow control. Generally speaking, the transports layer is to provide transparent data transfer between the host and media layers. It does this through a wide variety of methods such as error control and correction, message segmentation or concatenation, error recovery, connection reinitiating, multiplexing, and retransmission. The network layer provides the methods, which functionally transfer data from the host on a network, to a host on another network via the other media layers. This layer of the OSI model handles path determination and logical addressing of data. When the application is using TCP/IP, a common Internet enabled protocol; it follows a specific methodology along each of these layers. TCP/IP is a very reliable system in the context of general Internet applications. However, TCP (in addition to other IP protocols) do not have effective solutions for the handling

of fragile networks, where the quality or quantity of available participating nodes is indeterminate. Generically we can refer to networks such as these as challenged networks. They can be challenged in the sense of the following example. Assume a system, which has 3 nodes, for simplicity, in it at its origination, labeled A through C. A message is originating at node A and traveling to node C via a hop at node B. At origination of the message, the transport layer has routed the message and the proper links have been made, so the message is sent. After some unit of time, the message arrives at node B, however, the connection between node B and node C is no longer linked (say, for instance, node B is now out of range of node C), and there are no other paths from nodes B to C. At this point, the link between A and C must be reestablished. But this is sometime not easily done, or even possible with the present network configuration. Establishing a link and routing table in a traditional IP protocol is also one of the most time intensive elements in the process, which means the overall communication is going to have greatly increased latency should a reestablished connection be made possible.

It was for the reasons addressed above that the idea of Delay-Tolerant networks was conceived. These networks address the often unspoken assumptions of traditional IP networking protocols: that a path exists between the data source and its peers which is end-to-end in nature, that the maximum round-trip time between any source and peer node in a network does not grow excessively large, and finally that the probability for packets to reach their desired destination peer is large. Challenged networks often violate these assumptions and, thereby, prove difficult to implement using traditional IP protocols. Kevin Fall presents a conceptual discussion of challenged networks and alleviating the challenge of dealing with them via Delay-Tolerant networks in his paper "A Delay-Tolerant Network Architecture for Challenged Internets [19]." In his work he addresses the challenged internets qualitatively as "challenged internetworks…

characterized by latency, bandwidth limitations, error probability, node longevity, or path instability that are substantially worse than is typically present in today's Internet."

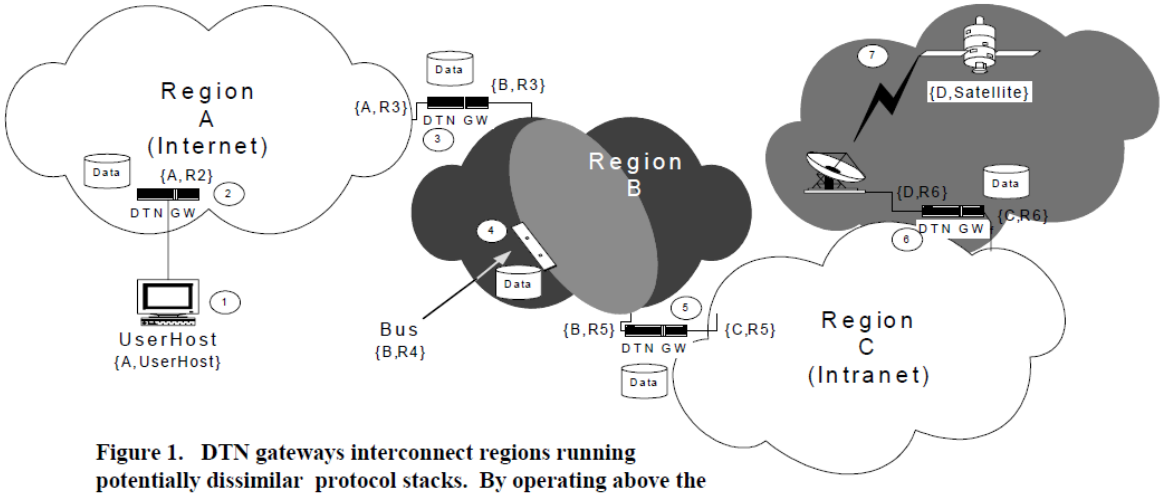


Figure 1. DTN gateways interconnect regions running potentially dissimilar protocol stacks. By operating above the transport protocols in use on the incident networks, they provide virtual message switching, in-network retransmission, and name mapping, allowing globally-interoperable names to be mapped

Figure 37: Challenged Network Illustration

A common solution, which is presented for the problem of implementing Delay-Tolerant networks, is the addition of another OSI layer above the transport layer called the bundle layer. This layer handles the temporary storage of and confirmation of receipt of data in the event that a physical link cannot be continuously maintained between the disparate Internets. The general layout of the functionality is depicted below. It is possible to see that each node temporary stores the information prior to forwarding it to the next node. The deletion of the stored info occurs either when the next node confirms complete receipt of message, or when the terminal destination node confirms receipt of message (the latter being a much more costly process in implementation).

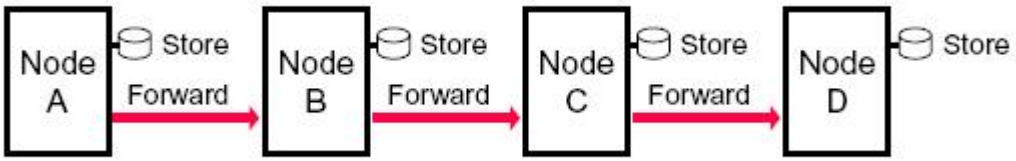


Figure 38: DTN Functionality Example

The bundle layer itself exists in the OSI model between networks in a challenged environment.

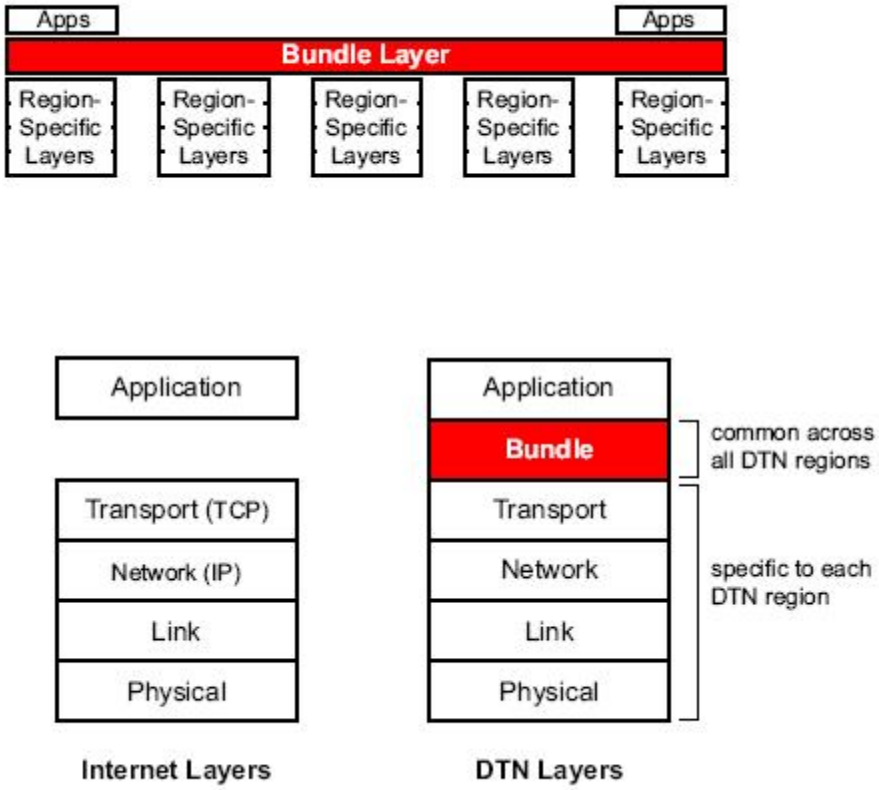


Figure 39: Bundle Layer as it Appears in the OSI Model

The concept of delay tolerant networking, DTN, was initially crafted in response to inquiries regarding interplanetary Internets. However, the principles apply directly to mobile, ad-hoc networks in modern cellular and wireless devices.

Chapter 4: Conclusion

Considerable work has been done towards upgrading traditional wire line 9-1-1 infrastructures to accommodate emerging VoIP technologies. VoIP has a distinct disadvantage in that it is much more difficult to locate the subscriber in order to direct emergency resources appropriately. Traditionally, the physical and stationary nature of the Public Switched Telephone Network allowed it to keep fixed databases in order to determine caller location. This location was used to route the call to the nearest PSAP and therefore minimize response time, essentially saving lives. With the introduction of VoIP services, this dynamic changed. New architecture is necessary to determine the spatial location of a subscriber, due to the fact that they can change their network location, and network location is not a reliable way to determine the physical location of a caller. New technologies have to be leveraged, and adaptations made within the existing infrastructure in order to implement next generation E9-1-1 services.

There are risks posed by a lack of reliable data. In addition there are limitations in VoIP networks, which need to be taken into account when liability is determined. The Wireless Communications and Public Safety Act of 1999, and additional legislation that sought to improve E9-1-1. This act gave those who provided any form of unconventional phone services the same liability to protect and ensure their customers were given equal access and treatment in relation to E9-1-1 use, unless special circumstances existed.

The proposal took these factors into account to accommodate for the various limitations and constraints which a wireless, ubiquitous, next-generation 911 Wide-Area-Network must account for. These constraints are largely tied to the underlying technologies, which form the base of the proposal. Properly leveraged, and with the correct protocols, we show that a

workable and reliable system can be formulated and that it is practical to scale this system to serve a large area.

Though there are concerns in security, funding, and implementation; it is feasible to apply an IP NG9-1-1 system to a large area. Taking these concerns into account, NENA has set standards in its i3 document describing how these concerns can be resolved. Through significant research, overcoming these concerns has been proven to be possible. The background research conducted for this project was of the utmost importance to proving the feasibility of an IP based NG9-1-1 network. Examining documents such as FCC legislature and NENA standards, an understanding of an IP NG9-1-1 system was met. Recognizing the weaknesses and strengths of existing NG9-1-1 technologies and legislature, it is proved that a reliable IP based NG9-1-1 system can be formulated.

References

[1] Medhi, D., Ramasamy, K., 2007, "Network Routing: Algorithms, Protocols, and Architectures (The Morgan Kaufmann Series in Networking)," Morgan Kaufmann: pp. 21-22, 439-486.

[2] Kurose, J. F., Ross, K. W., 2010, "Computer Networking A Top-Down Approach," Addison-Wesley: New York, Boston, San Francisco, London, Toronto, Sydney, Tokyo, Singapore, Madrid, Mexico City, Munich, Paris, Cape Town, Hong Kong, Montreal, pp. 48-54.

[3] 2013, "E911 Call Processing," Bell Services West, http://www.bellserviceswest.com/downloads/E911_Call_Processing.pdf, (accessed April 1, 2013)

[4] Consumer and Governmental Affairs Bureau, 2013, "FCC Consumer Advisory 911 Wireless Services," Federal Communications Commission, http://www.fcc.gov/guides/wireless-911-services, (accessed April 1, 2013)

[5] Consumer and Governmental Affairs Bureau, 2013, "FCC Consumer Advisory VoIP and 911 Service," Federal Communications Commission, http://www.fcc.gov/guides/voip-and-911-service, (accessed April 1, 2013)

[6] Prusansky, C., May 2008, "VoIP and 911: Is Your Agency Prepared?," Fire Engineering, Volume 161, Issue 5, pp. 109.

[7] Wireless Communications and Public Safety Act of 1999, PUBLIC LAW 106–81, 113 STAT. 1286 (1999).

[8] Costa-Requena, J., Tang, H., 2001, "Enhancing SIP with Spatial Location for Emergency Call Services", Computer Communications and Networks, 2001. Proceedings., IEEE, pp. 326-333.

[9] United States. Cong. Federal Communications Comission. *Www.fcc.gov*. 112 Cong. Cong. Rept. 112 - 96 (2012). N.p., n.d. Web.

[10] 2007, "NENA Functional and Interface Standards for Next Generation 9-1-1 Version 1.0 (i3)," National Emergency Number Association 08-002: USA, Version 1.0, December 18, 2007

[11] 2013, "Best Practices and Guidelines for Location Based Services," Cellular Telecommunication Industry Association, http://www.ctia.org/business_resources/wic/index.cfm/AID/11300 (Accessed April 10th, 2013)

[12] A VoIP Emergency Service Architecture and Prototype, IEEE 0-7803-9428-3, May 2005, authors: Matthew Mintz-Habib, Anshuman Rawat, Henning Schulzrinne, and Xiaotao Wu, all of Dept of CS at Columbia U

[13] Exploring Development of Service-Orientated Architecture for Next Generation Emergency Management Systems, 2010 IEEE 24th International Conference on Advanced Information Networking and Applications Workshops, authors: Yi-Heng Feng, and C. Joesph Lee

[14] Open Multi-Purpose Gateway for Emergency Services Internetworking, IEEE 978-1-4244-3437-4, Sept 2009, authors: Socrates Varakliotis, Nikolas Stephan, Peter T. Kirstein

[15] Power, Telecommunication, and Emergency Services in a Converged Network World, authors: Gerard P. P'Reilly, Steven H. Richman, Andjelka Kelic

[16] SALICE - Satellite-Assisted Localication and Communication systems for Emergency Services, IEEE 978-1-4244-4067-2, Sept. 2009, authors: Enrico Del Re, Simone Morosi, Sara Jayousi, Claudio Sacchi

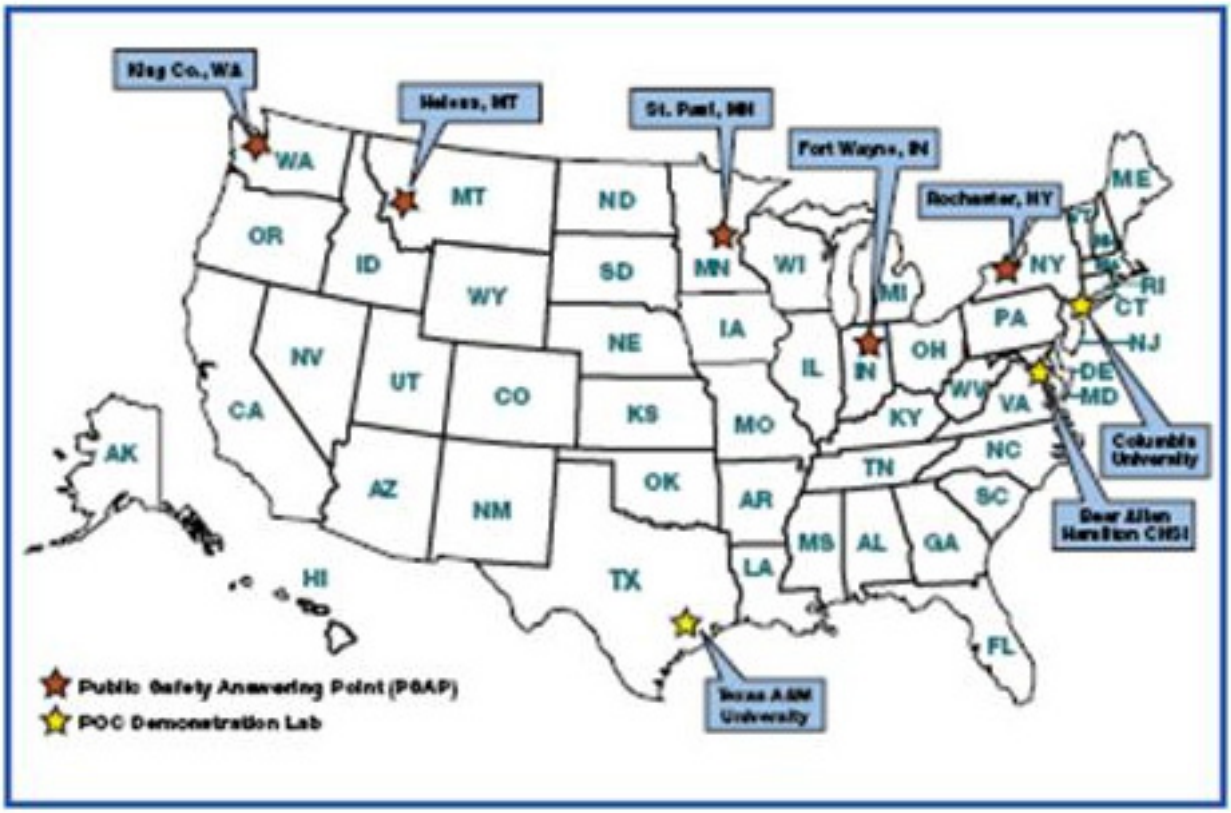
[17] Enhancing the QoS and Resource Management of Aspects of the 3GPP IMS Emergency Service Architecture, IEEE 1-4244-1457-1, Aug 2008, authors: May El Barachi, Roch Glitho, Rachida Dssouli

[18] An Architecture for the Provision of Context-Aware Emergency Service in the IP Multimedia Subsystem, IEEE 978-1-4244-1645-5, Aug 2008, authors: May El Barachi, Roch Glitho, Ferhat Khendek, Rachida Dssouli

[19] A Delay-Tolerant Network Architecture for Challenged Internets, SIGCOMM 1-58113-735-4, Aug 2003, author: Kevin Fall

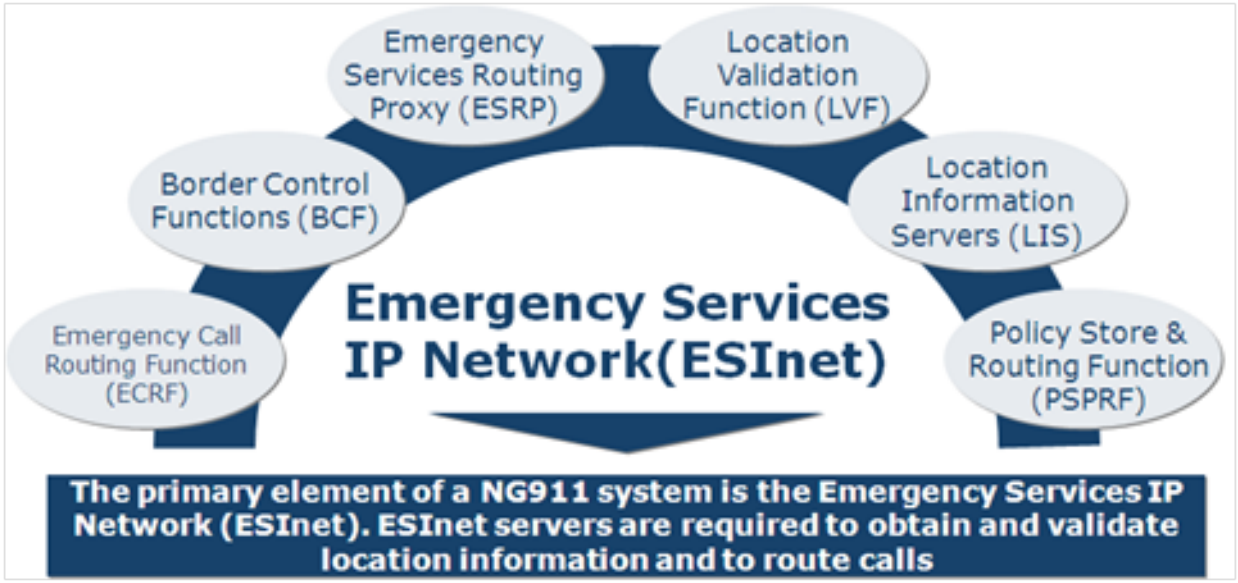
[20] Improved IP Network for Emergency Service, IEEE 978-1-4244-1494-9, Nov. 2007, authors: Fiaz Gul Khan, Aamir Saeed, Babar Nazir, Kashif Bilal, Nouhman Ayub

Appendix A: Additional Figures

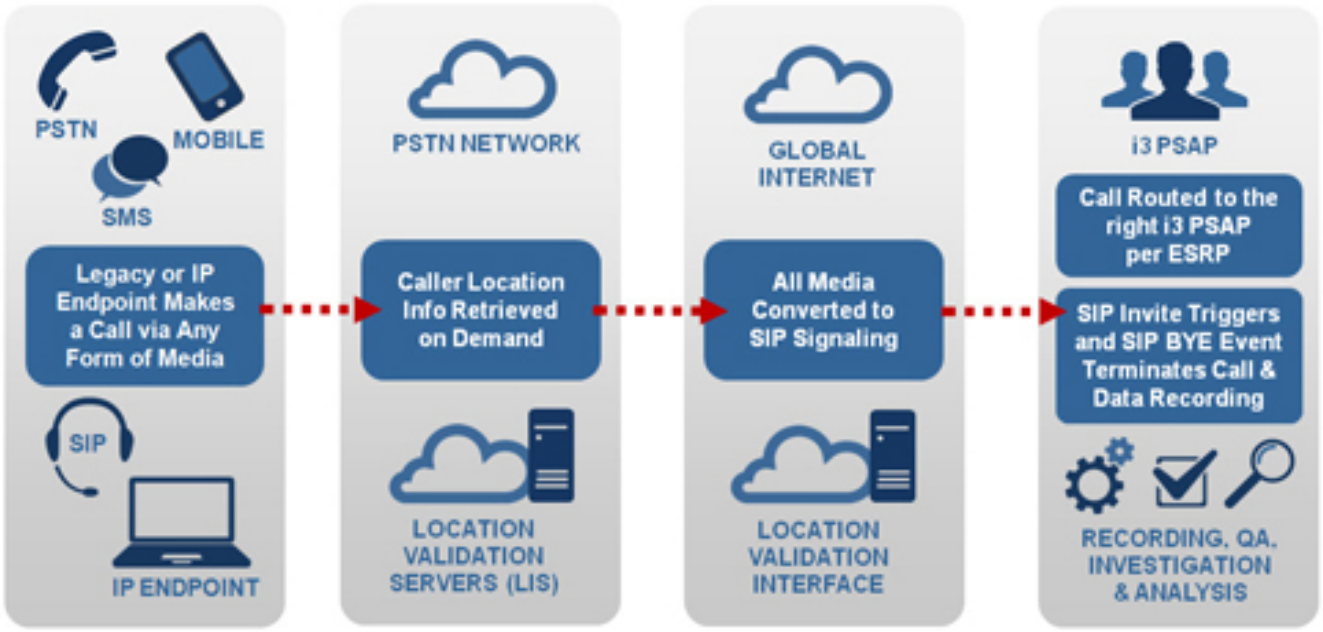


Possible Future PSAP locations
http://www.its.dot.gov/NG911/

Community Model of NG9-1-1
http://www.its.dot.gov/NG911/



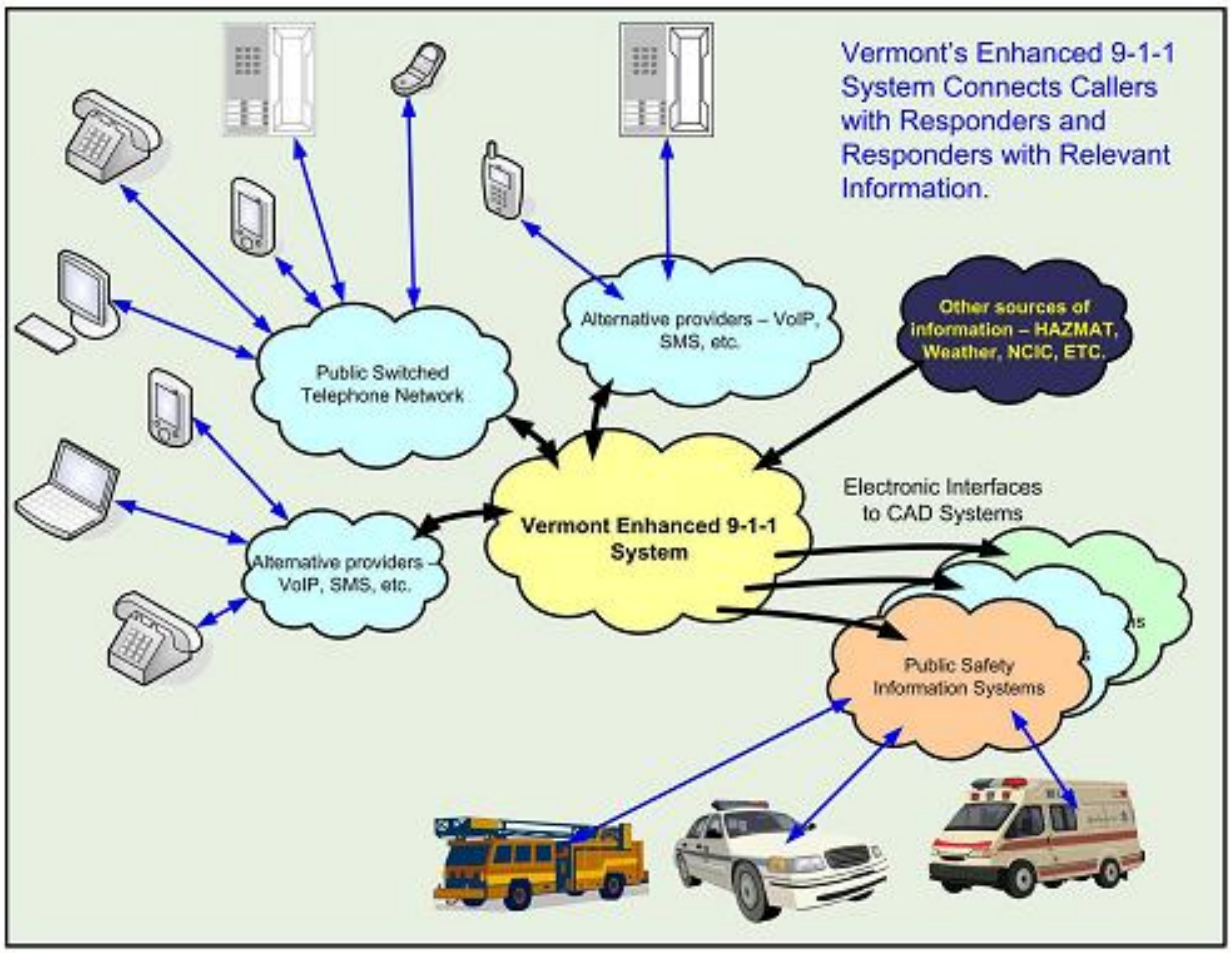
Core Elements of NENA ESInet
http://www.frost.com/reg/blog-personal-index.do?userId=10512



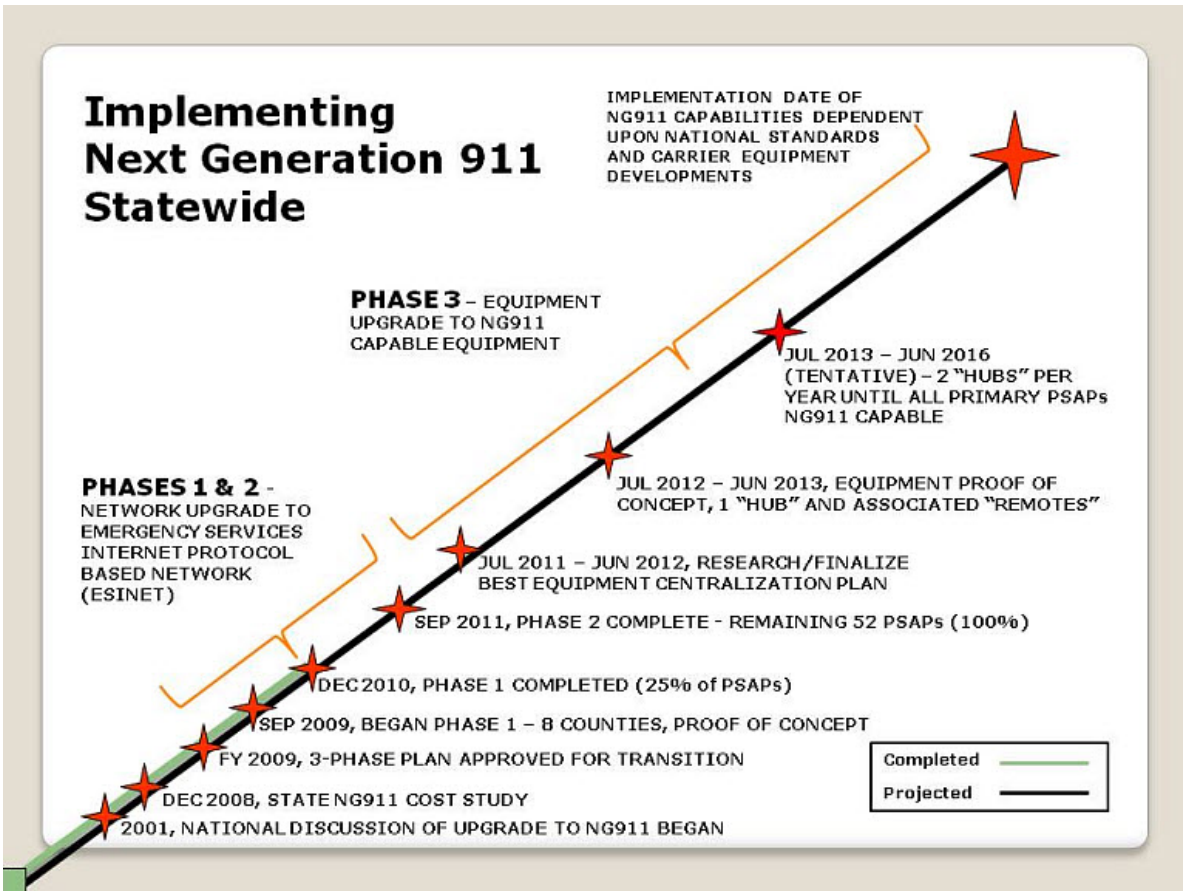
Basic Call Routing in i3
http://www.vpi-corp.com/NENA-Next-Generation-911-Recording-System.asp

Media Types Forwarded Through NG9-1-1

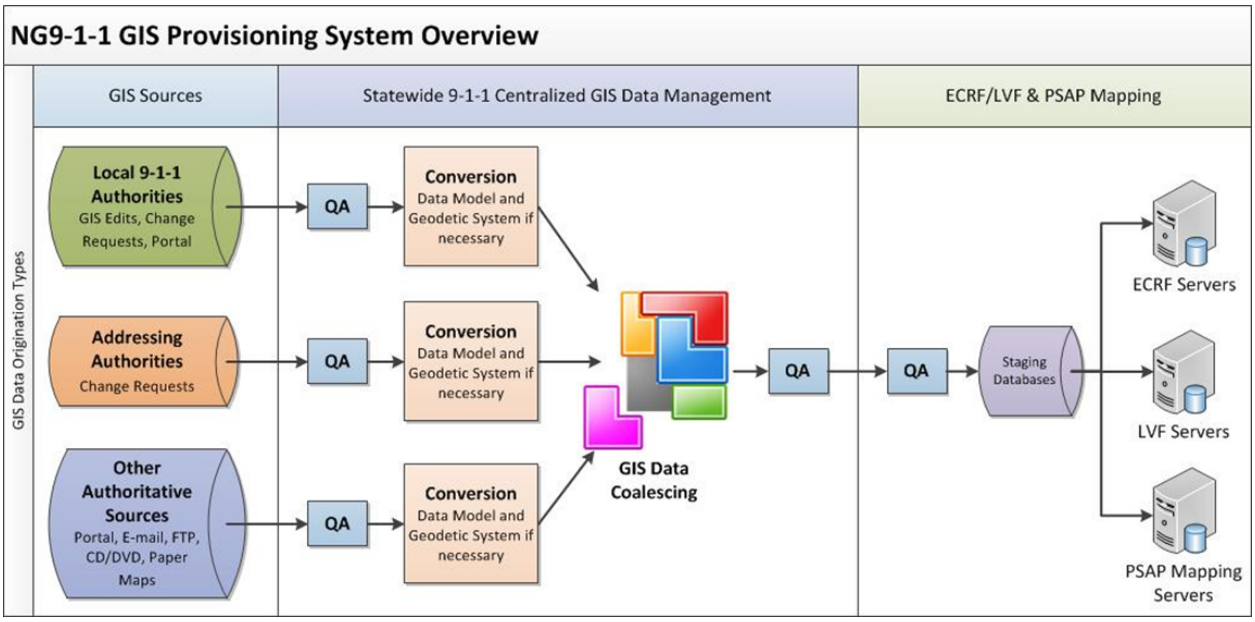
http://www.vpi-corp.com/NENA-Next-Generation-911-Recording-System.asp



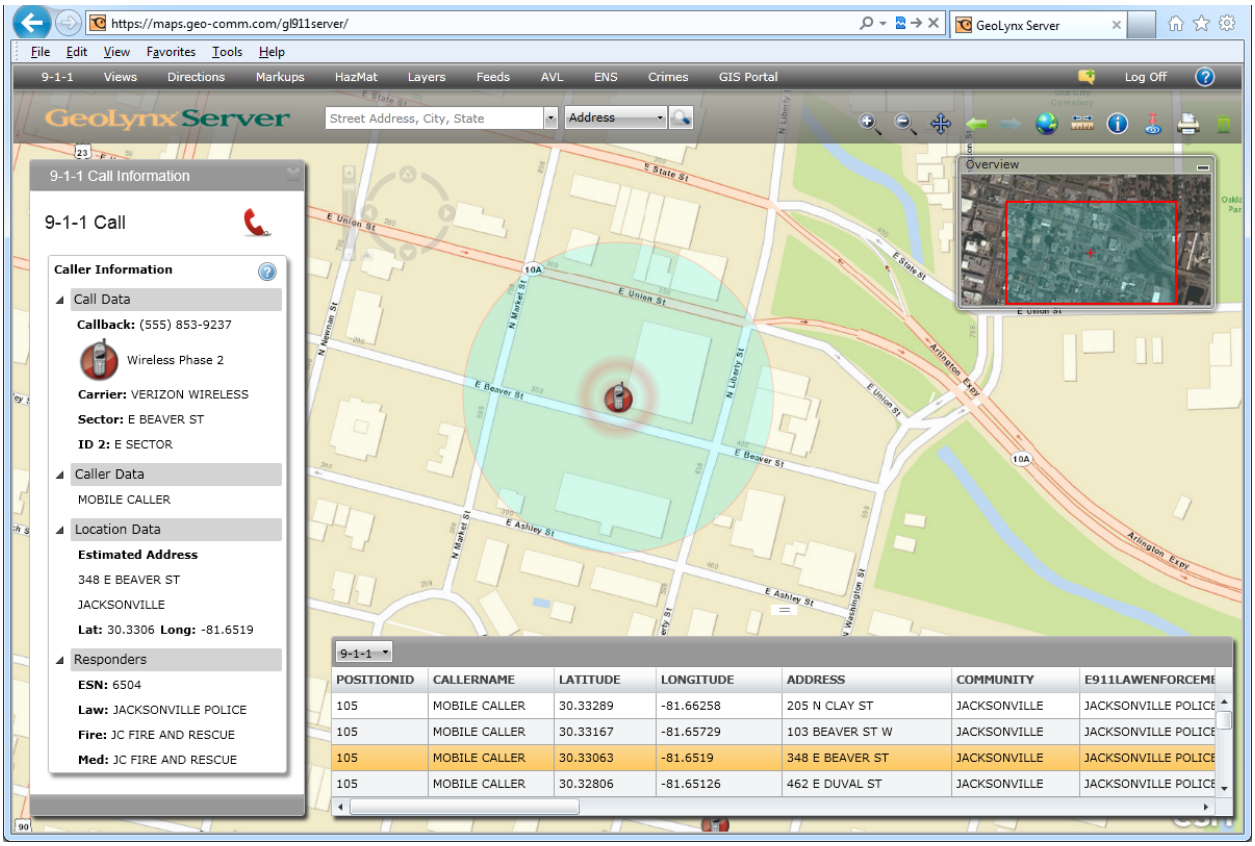
Sample State Wide System
http://e911.vermont.gov/vermont_911/system_information/network_overview



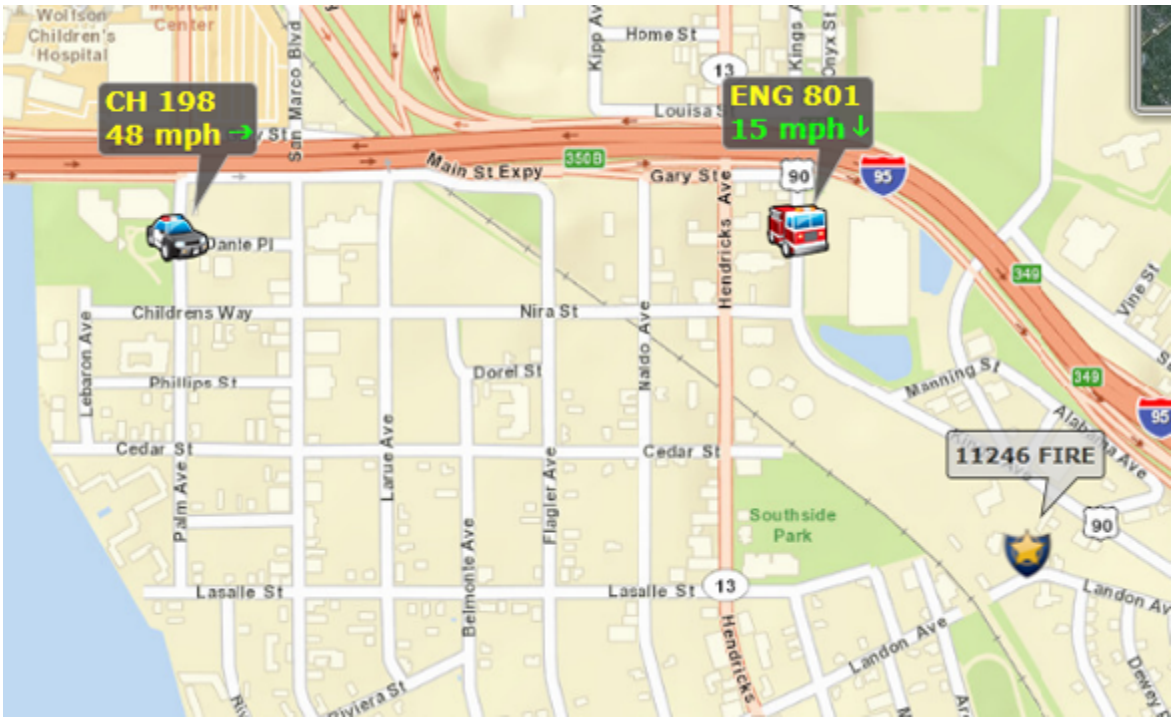
Washington State Steps to Implement an NG9-1-1
http://performance.wa.gov/FinalPublicSafety/PS031611/Readiness/NextGeneration911/Pages/Default.aspx



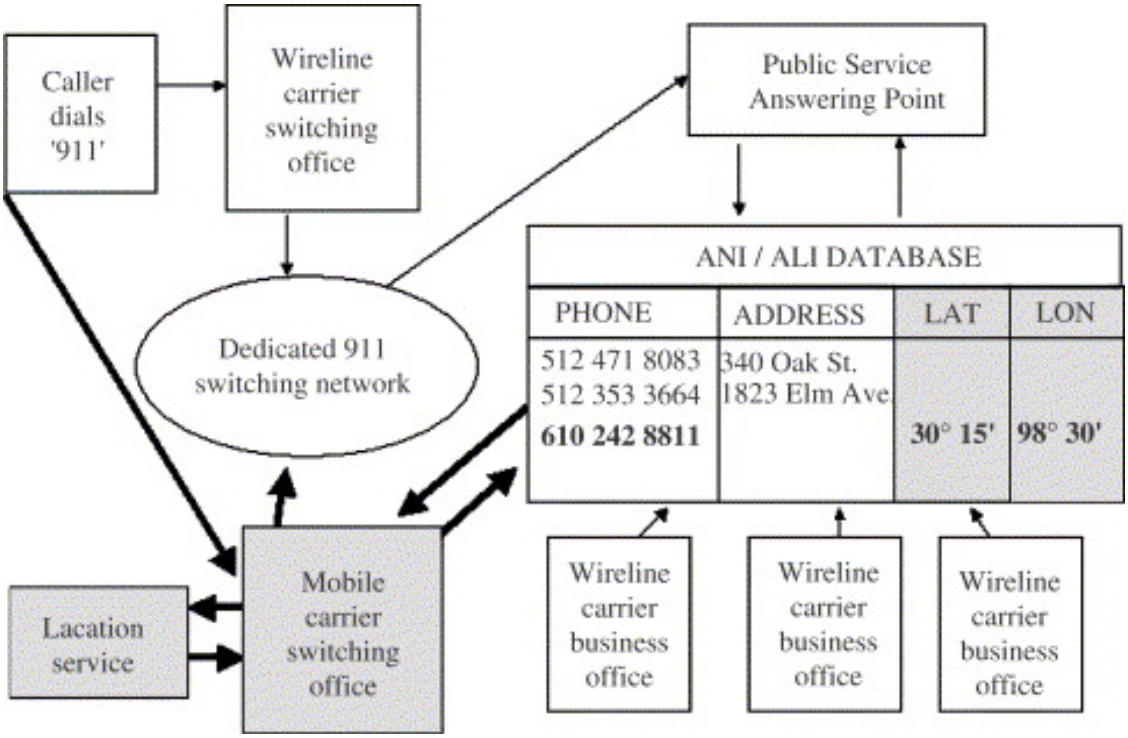
GIS Provisioning Overview
http://www.geo-comm.com/geolynx/spatial-router-ecrflvf/



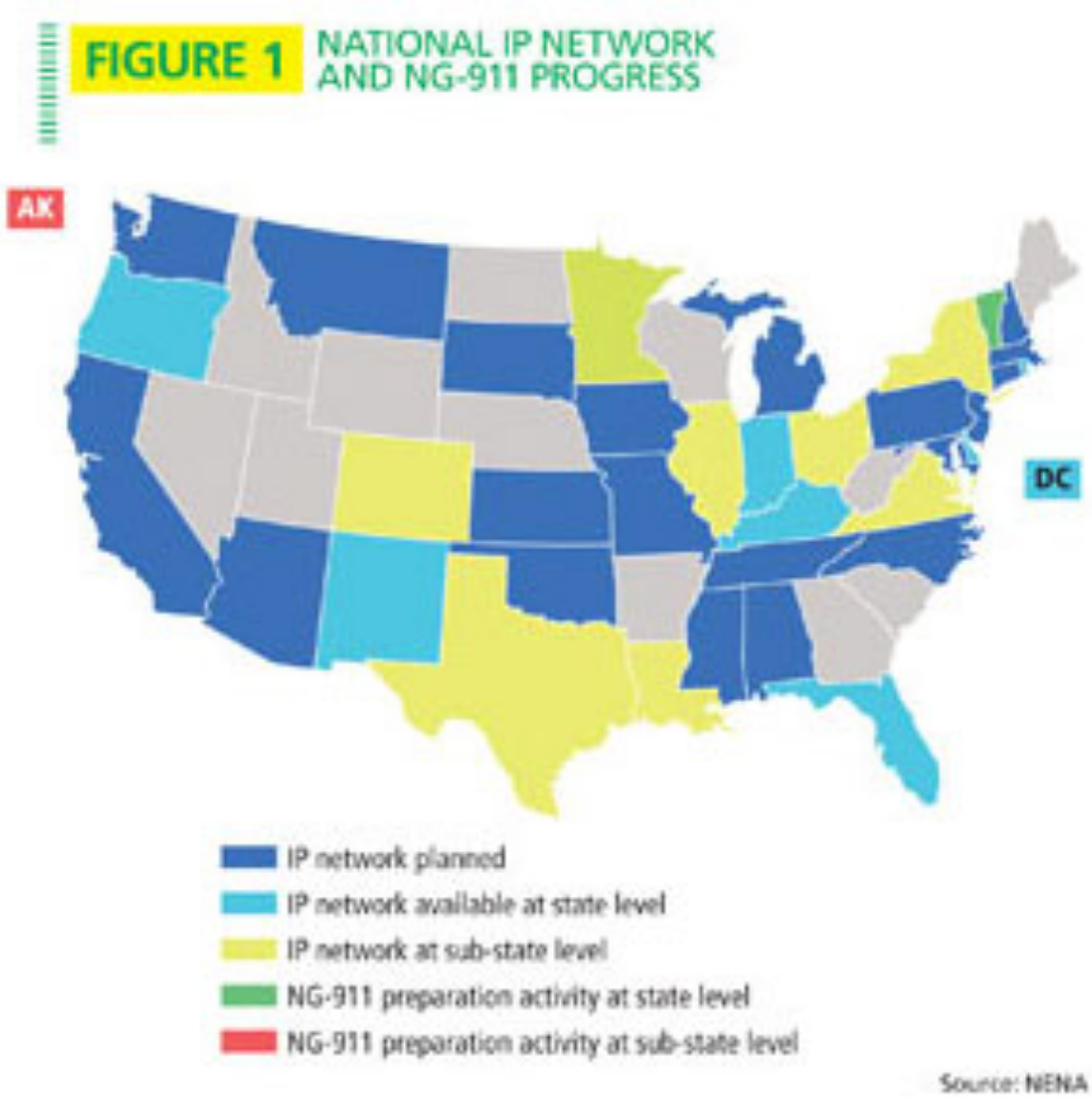
Sample NG9-1-1 System Using GIS To Locate Caller
http://www.geo-comm.com/ng9-1-1/esinet-tactical-mapping/



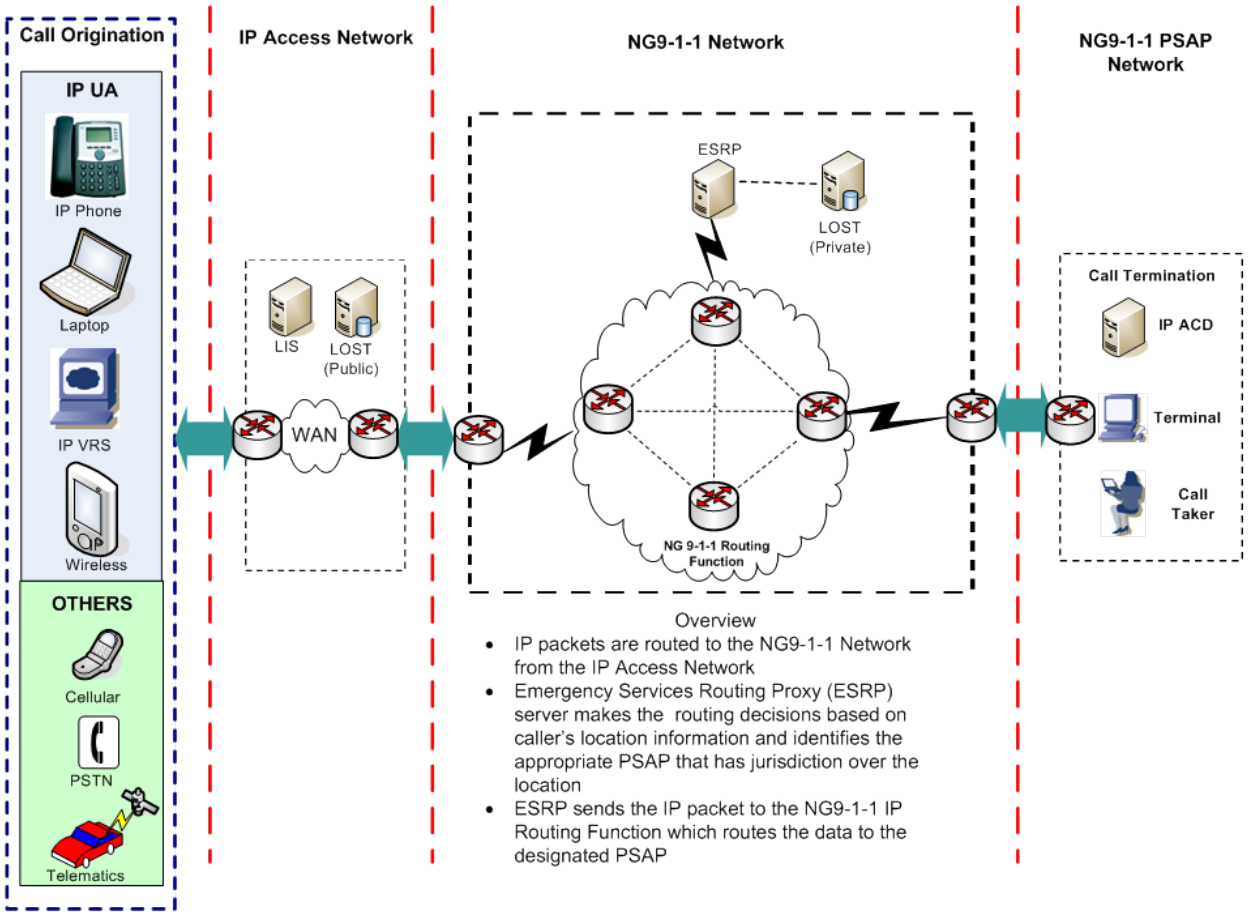
Sample Location Of Emergency Services Using NG9-1-1 System
http://www.geo-comm.com/ng9-1-1/esinet-tactical-mapping/



Current 9-1-1 System
http://www.sciencedirect.com/science/article/pii/S030859610500087X



IP Network Capability and progress
http://urgentcomm.com/policy-amp-law-mag/home-stretch



Detailed IP Call Flow

http://www.its.dot.gov/ng911/pubs/USDOT_NG911_FINAL_System_Design.htm