Intelligent Transportation Systems
U.S. Department of Transportation

Next Generation 9-1-1 (NG9-1-1) System Initiative

Final System Design Document

Washington, D.C.
February 2009

Version 2.0

DOCUMENT CHANGE HISTORY

Version Number	Date	Description
V1.0	February 2008	Interim Release
V2.0	February 2009	Final Version

Table of Contents

EXECUTIVE SUMMARY

The Next Generation 9-1-1 (NG9-1-1) Initiative is a research and development project funded by the US Department of Transportation (USDOT) to define the framework and plan to deploy Internet Protocol (IP)-based emergency communications across the nation. The project has helped to define the concept of operations, functional requirements, and system architecture, and to develop a transition plan that considers implementation costs, values, and risks.

From a technical perspective, the project has been guided by its long-term goal: "To enable the general public to make a 9-1-1 'call' (any real-time communication—voice, text, or video) from any wired, wireless, or IP-based device…" Additional important considerations included advancing call delivery, locating callers, and improving system functionality "through new internetworking technologies based on open standards." The NG9-1-1 Initiative has helped demonstrate these principles throughout the project's duration.

The NG9-1-1 *Final System Design* document is the culmination of the technical work of the NG9-1-1 Initiative. Starting with the NG9-1-1 Concept of Operations (CONOPS), the project team leveraged past work done in the public safety and standards communities. After the CONOPS, the project developed both high-level and detailed requirements, an architecture analysis report, and the initial system design. These project artifacts served as the basis for the *Proof of Concept (POC) Deployment Plan*.

Using the *NG9-1-1 Architecture Analysis Report* as a basis, the NG9-1-1 POC system design relies on commercial off-the-shelf (COTS), open source, and common telecommunications and networking products used throughout the industry. Because of the limited project scope, the POC system design does not include all the components listed in the architecture (e.g., legacy systems); however, it does represent virtually all the "next generation" system design elements. During the POC demonstration, very little of the legacy technology was demonstrated because those systems are in place today. However, it is important to recognize that when NG9-1-1 is fully implemented, both legacy and next generation systems will likely need to run concurrently until the legacy systems can be replaced or retired.

While the NG9-1-1 POC demonstration was not envisioned as an operational demonstration, the facilities and staff of five public service answering points (PSAP) were used during the testing of the POC. At no time during the tests were real calls used nor did the test system interrupt the operations of the 9-1-1 system. This configuration allowed demonstration of the NG9-1-1 architecture in a controlled environment by professional call takers.

A number of system-wide decisions were made during the design of the POC. For example, the POC used Session Initiated Protocol (SIP) as the signaling protocol for call establishment, routing, and termination. Although other signaling protocols exist, SIP was chosen because of its wide industry acceptance and support and open source status. Another example of a design decision was the use of SIP gateways as interfaces to the NG9-1-1 POC network to demonstrate a modular architecture corresponding to a more realistic deployment scenario. These decisions helped control the scope of POC to maintain a tight implementation schedule.

The NG9-1-1 POC demonstrated selected features of the NG9-1-1 requirements and system design, focusing on the three main components of emergency calling: call origination, call support/processing, and call termination at a PSAP (more commonly known as a 9-1-1 Center). Because IP-based calling is a key factor for NG9-1-1, the POC used IP devices and systems, in addition to more traditional methods (e.g., wireline and wireless telephones, and legacy devices sending Short Message Service [SMS] text messages).

To demonstrate the networking features of NG9-1-1, a standalone and secure POC network was designed and implemented. The network connected three laboratory facilities (Booz Allen Hamilton and Texas A&M and Columbia Universities), four PSAPs (Rochester, New York; King County, Washington; St. Paul, Minnesota; and Helena, Montana) and one statewide PSAP network (the State of Indiana). Each of these entities was connected via secure Generic Route Encapsulation (GRE) tunnels over Internet2 and a mix of AT&T's Commodity Internet and Multi-Protocol Label Switching (MPLS) network.

Call Origination

During the POC, a variety of call origination scenarios were tested, including legacy Public-Switched Telephone Network (PSTN) telephones, cellular telephones (voice and SMS texting), third-party call centers (telematics systems), and IP User Agents (UA), including laptops with SIP clients, IP telephones, and IP wireless devices). These devices successfully demonstrated call initiation as the first step in the overall call delivery process. A mix of simulated and actual access service providers were used to show the various routes a call could take to reach the NG9-1-1 system.

Demonstration of call origination devices helped identify areas for future research, including conference server and video compression technology for multiparty conferencing to support the needs of video interpreting services for the deaf and hearing-impaired. In addition, the demonstration showed that SMS texting was an inferior technology to support emergency calling because of its inability to support identification of callers' location information and its inability to guaranteed delivery or receipt. Although citizens who call 9-1-1 today believe that being able to send SMS messages to 9-1-1 is a critical need, the technology was not designed or possibly ever intended for this type of important use. On a positive note, the design of the telematics use case and the maturity of that commercial technology provided positive results that may be seen in actual use before a full rollout of NG9-1-1.

IP Access Network

The POC's IP access network provided location acquisition and validation, network routing, and SIP signaling functions. To simulate an IP access network, the test laboratory implemented devices to dynamically assign IP addresses, translate host names to IP addresses, acquire locations for test calls, and provide network security for the POC network and devices.

POC test calls entered the IP access network through telephony gateways (and were converted to SIP) or were natively based on IP. Once within the IP access network, the calls accessed location acquisition and call routing services. The call's location was used to route the call, and it was forwarded out of an edge/ border gateway and onto the NG9-1-1 network.

NG9-1-1 Network

The primary function of the NG9-1-1 network was to identify the appropriate PSAPs based on the call origination information and to efficiently and accurately route the call while maintaining data integrity. Simulated databases of NG9-1-1 data were used to ensure that appropriate business rules were applied prior to routing the calls to the POC PSAPs. In the live NG9-1-1 network, the data will be decentralized and geographically distributed to maximize the stakeholders' needs for reliability, availability, scalability, and serviceability.

One of the main components of the NG9-1-1 network will be the Location to Service Translation (LoST) discovery protocol. LoST maps civic and geospatial regions to services (in this case, emergency services providers.) During the NG9-1-1 POC, LoST was used to resolve which PSAP a UA should contact for emergency services. The LoST server used its database to perform a lookup based on the caller's location and return the identification and contact information for the requested service.

NG9-1-1 PSAP

The primary role of the NG9-1-1 PSAP in the POC was to receive simulated 9-1-1 calls generated from a variety of call origination devices. As part of the POC, PSAP equipment and infrastructure were deployed at several live PSAPs that provide 9-1-1 emergency services within their city, county, or state. The project team ensured that the daily operations of the PSAPs were not disrupted while conducting the POC tests. POC equipment deployed at the PSAPs was isolated from their live environments, and while call takers participated in the testing, no real 9-1-1 calls were taken using POC equipment.

As part of the POC, the call taker's graphical user interface software was developed to terminate the calls and perform typical call taker support functions. In the NG9-1-1 environment, the amount and types of data displayed were dramatically increased; however, the call taker participants were able to quickly adapt to the new software with only minimal orientation.

The *NG9-1-1 Final System Design* document describes the technical design of NG9-1-1 and the POC implementation specifically, and discusses the key considerations and constraints of NG9-1-1 system components. It also provides insight on items for consideration for further research into NG9-1-1 technology.

1 POC SYSTEM DESIGN DOCUMENT OVERVIEW

This document describes the system design for the Next Generation 9-1-1 (NG9-1-1) Proof-of-Concept (POC) demonstration task. The NG9-1-1 Concept of Operations (CONOPS), High-Level Requirements document, and Architecture Analysis report, serve as the basis for this document. These documents are available for download at the U.S. Department of Transportation's (USDOT) NG9-1-1 website: http://www.its.dot.gov/ng911.

The NG9-1-1 POC demonstration was envisioned to demonstrate potential next generation features of the 9-1-1 system. This included—

- Call origination using—
  - Internet Protocol (IP) User Agents (UA) such as laptops with Session Initiation Protocol (SIP) clients, IP phones, and IP wireless devices (Audio, Text, Data, and Video)
  - Cellular devices with Short Message Service (SMS) (Audio, Text and Data)
  - Third-party call centers such as Telematics service providers (Audio and Data)
  - IP Video Relay Systems (VRS) for the deaf and hard-of-hearing community (Text, Data, and Video)
- Call support and processing using—
  - Standard IP access networks
  - NG9-1-1 Network components such as Emergency Services Routing Proxy (ESRP) and data gateways
  - NG9-1-1 databases such as Business Rules, and Location-to-Service Translation Protocol (LoST)
- Call termination at the Public Safety Answering Points (PSAP) using—
  - IP Automatic Call Distribution (ACD) systems
  - IP phones and workstations
  - Human machine interfaces

This POC System Design Document (SDD) focuses on the design of key functional components required to successfully demonstrate NG9-1-1 features and functionalities. It is envisioned that industry, research institutions, and other government agencies will continue to conduct research and development (R&D) activities to further develop and test NG9-1-1 components, both included and not included in the POC demonstration.

1.1 Document Objective

The objective of the POC SDD is to document the design of key NG9-1-1 components that were included in the POC demonstration.

1.2 Scope

The scope of the POC SDD includes developing a system design for the following NG9-1-1 POC demonstration functional components:

- Call origination, including legacy telephony, cellular devices with SMS capabilities, telematic systems, IP UAs and VRSs
- IP access network, including location acquisition and validation, and call routing
- NG9-1-1 Network, including LoST mapping and call routing
- NG9-1-1 databases, including Automatic Location Identification (ALI), LoST, Business Rules, and Call record database
- NG9-1-1 PSAPs, including call termination and call management.

1.3 Document Overview

The remaining sections of this document are organized as follows:

- **Section 2—POC System Design Overview:** Provides an overview of the NG9-1-1 POC system design components and describes the approach used to develop the POC SDD
- **Section 3—Call Origination POC System Design:** Describes the system design for originating NG9-1-1 calls using devices such as IP UAs (laptop, IP wireless devices, IP phones), cellular phones (handset with SMS), third-party call centers (telematics), and IP VRSs for the deaf and hard of hearing community
- **Section 4—IP Access Network POC System Design:** Describes the system design of the IP access network that was implemented in the Booz Allen Center for Network & Systems Innovation (CNSI) at One Dulles
- **Section 5—NG9-1-1 Network POC System Design:** Describes the system design of the POC NG9-1-1 network that was implemented in the Texas A&M University (TAMU)/Columbia University test laboratories
- **Section 6—NG9-1-1 PSAP POC System Design:** Describes the system design of equipment that was deployed at the PSAPs for emergency call termination
- **Section 7—Network Management System POC System Design:** Describes the design of the network management system that was used in the POC for monitoring the POC test-bed infrastructure and collecting system performance metrics
- **Appendix A—Acronyms:** Lists acronyms used in this document
- **Appendix B—Glossary:** Defines key terminology used in this document
- **Appendix C—Source References:** Provides a list of published documents that were referenced while developing this document

2 POC SYSTEM DESIGN OVERVIEW

The NG9-1-1 POC system design was developed from the NG9-1-1 architecture defined during Task 1f. The design uses commercial off-the-shelf (COTS), open source, and commonly used telecommunications vendor products. However, the design does not include all components in the architecture. Figure 2.1 depicts the overall NG9-1-1 architecture, with highlighting to indicate components that were built and deployed for the POC demonstration. The NG9-1-1 Architecture Analysis Report provides detailed descriptions of all NG9-1-1 components and their respective interfaces.

This page left blank intentionally.

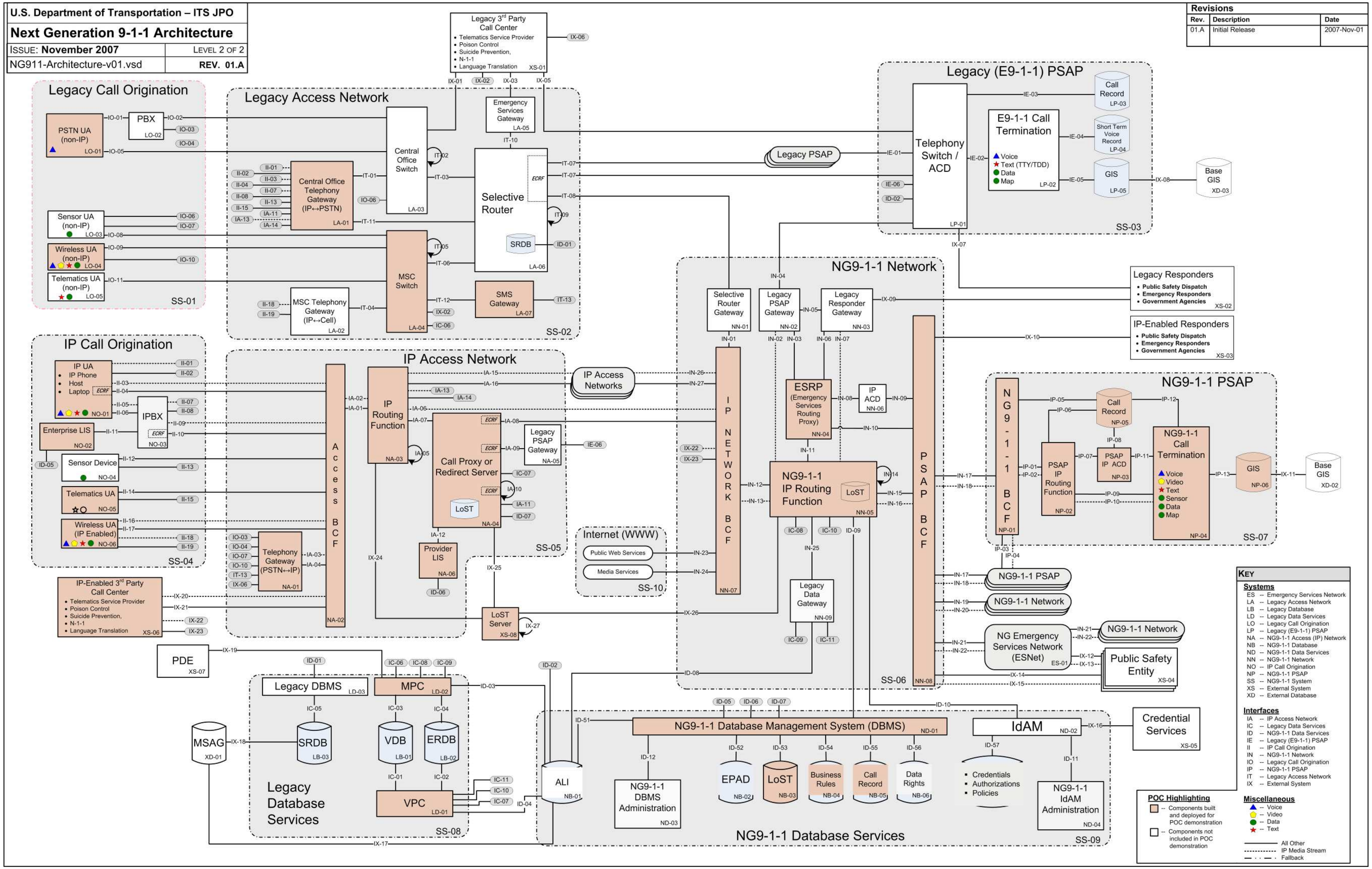

Figure 2.1: Reference Architecture

This page left blank intentionally.

The NG9-1-1 POC demonstration was not envisioned as an operational demonstration. At no time during the tests were real calls used; nor did the test system interrupt the operations of the 9-1-1 system. Rather, key components of the NG9-1-1 architecture were simulated and demonstrated in a controlled environment. End-to-end use cases, including call origination using legacy wireline telephony, cellular phones, third-party call centers (telematics), IP UAs and VRS for the deaf and hard-of-hearing community were developed and tested. Testing of these scenarios involved acquiring and validating location information from location information systems, routing the calls to the simulated NG9-1-1 Network, performing location-to-service mapping (LoST), querying various NG9-1-1 databases, and finally routing the calls to the appropriate PSAP participating in the NG9-1-1 POC demonstration. Pre-selected call takers at the PSAPs received and responded to the simulated NG9-1-1 calls. Testing included functional validation as well as the capture and analysis of various system performance metrics.

2.1 System-wide Design Decisions

Table 2.1 lists the system-wide design decisions that were made over the course of the NG9-1-1 POC.

Table 2.1: System-wide Design Decisions

#	POC Design Decisions	Remarks
1	• The POC used SIP as the signaling protocol for call establishment, routing and termination	• Signaling protocols such as IP Multimedia Subsystem (IMS), Signaling System 7 (SS7), H.323 are available, but SIP was chosen due to its wide industry acceptance and support. SIP also allowed for the use of Voice, video, text and additional data elements. SIP allowed the use of location by reference, information larger than the allowable fields in SIP can be added by using a URI to another service or database
2	• A laptop running the SIPc client was used to demonstrate IP-based call origination for the POC	• The SIPc software developed by TAMU/ Columbia team was enhanced to meet the NG9-1-1 IP user agent requirements
3	• A handheld device (Dual 802.11/Cellular) running a SIPc client was be used to demonstrate wireless IP-based call origination for the POC	• The SIPc software developed by TAMU/ Columbia team was enhanced to meet the NG9-1-1 IP user agent requirements
4	• A voice over IP (VoIP) phone was used to demonstrate IP-based call origination (Enterprise)	• A Cisco IP phone was used to test this use case
5	• An IP laptop with streaming video capabilities was used to demonstrate IP call origination for the deaf/hard-of-hearing using VRS	• This test served as a simulation of a VRS

#	POC Design Decisions	Remarks
6	• A legacy wireline emergency phone call was demonstrated by interfacing an analog phone with an IP telephony gateway	• A Standard IP telephony gateway, such as Cisco's Integrated Service Router, was used to perform the public switched telephone network (PSTN)-to-IP translation
7	• A Selective Router Database (SRDB) was not used for the POC	• Due to design decision #6, a legacy access network was not required, therefore, no selective router or SRDB was required
8	• Data Services using IP Sensor Systems were not demonstrated in the POC	• An IP Sensor System can be considered another IP source. Demonstrating integration with a IP-based telematics system was deemed adequate to showcase this NG9-1-1 capability
9	• IP call routing to legacy PSAPs was not demonstrated in the POC	• The POC environment did not include any legacy PSAP equipment. Therefore, call routing to legacy PSAPs was not demonstrated
10	• Identity and Access Management was not demonstrated during the POC	• Maintaining identities for administration of the NG9-1-1 IP network is important. Mechanisms for providing identity and access to the NG9-1-1 Network for Service Providers, PSAP Operators, Network Administrators, DB Administrators, and Data Access Rights for Users and Applications was not demonstrated but should be investigated in future NG9-1-1 efforts
11	• An MSAG database was not used for the POC	• Given the current support for legacy call origination, there is no technical need for an MSAG database for POC. • MSAG valid data was developed from participating PSAPs and then incorporated in the appropriate DB's (LoST, Location Information Server [LIS], ALI/ Mobile Positioning Center [MPC]/ VoIP Position Center [VPC]) for the POC
12	• A Network Management System was deployed for POC but in a limited context	• A basic out-of-box Network Management product was deployed for the POC • Integration occurred with all network devices (routers, switches, etc.) and servers (SIPd, LoST, etc.) residing on the NG9-1-1 Network • Only limited monitoring and reporting was supported for the POC since, management of an IP-based network was not the main focus of the POC
13	• A LoST DB server resided in the Booz Allen CNSI and TAMU / Columbia test facilities. The Booz Allen CNSI LoST DB contained national level routing data and the TAMU LoST DB contained state/county/local level routing data	• It was imperative that the hierarchical nature of LoST was tested during the POC because this mimics a practical implementation of the service in nationwide deployment

#	POC Design Decisions	Remarks
14	• The LIS/LoST data was considered pre-validated	• Because validating against a MSAG database was not possible because of integration challenges, pre-validated data was used for the POC demonstration
15	• An IP capable PSAP was demonstrated in the POC	• The IP PSAP comprised of a router, switch, and firewall to support the POC use cases, and PSAP ACD and workstation to direct calls to the proper call taker within the PSAP and the workstation to answer and process the calls • Standard IP routing protocols and T1 circuits provided the connectivity between the IP PSAP locations
16	• The Call Record Database was centrally managed within the NG9-1-1 Network	• To ease maintenance and acquisition of the data, the Call Record Database was hosted centrally • In a real deployment, each PSAP would be responsible for maintaining its own call record Database. Additionally, the data would be aggregated and managed centrally within the NG9-1-1 network for redundancy purposes
17	• A series of SIP Border Gateways were deployed within the Booz Allen CNSI laboratory. Four gateways were used to support the POC use cases (Legacy, IP, Telematics, Cellular)	• The SIP gateways served as interfaces onto the NG9-1-1 Network for the various call sources/media streams • This demonstrates a modular architecture corresponding to a more realistic deployment scenario. It also eased integration of call sources. Call sources can be added as an add-on component without affecting overall system reliability or up-time
18	• Dedicated T1 circuits were provisioned between the PSAPs and the TAMU/Columbia test laboratories via Generic Route Encapsulation (GRE) tunnels	• Dedicated T1 circuits were used to support the POC demonstration traffic in order to avoid integration issues with the PSAPs' production network • Protecting the integrity of the system is of paramount importance for all involved • Security must be multifaceted and implemented at multiple levels. Using basic elements of IT-based security principles, GRE tunnels were employed to protect the POC environment and its participants
19	• Use of COTS equipment	• With the exception of limited software developed specifically for the POC, all equipment used in the POC was COTS
20	• SMS converted to a SIP message	• To deliver SMS messages the text was converted to a SIP session. This allowed the user and the call taker to exchange messages. Since SMS is not a real time communication service, it is of limited value for requesting help in an emergency

The POC system leveraged components from the TAMU/Columbia NG9-1-1 prototype test-bed and expanded the system's capabilities by including additional products and solutions to address the NG9-1-1 Tier 1 requirements identified under Task 1. The system design incorporated new technologies and applications to enhance the scope of the prototype thus demonstrating a broad set of features and functionalities of the NG9-1-1 System. Within the architectural framework, the POC system design uses existing call origination devices, IP access networks, third-party call centers, and legacy 9-1-1 systems and databases. Later sections of this document describe the details of the above mentioned design decisions.

2.2 NG9-1-1 POC Demonstration Key Components

The NG9-1-1 POC demonstration includes the following key components:

- Call Origination
- IP Access Network
- NG9-1-1 Network
- NG9-1-1 Databases
- NG9-1-1 PSAPs.

Figure 2.2, depicts a high-level design for the POC demonstration.

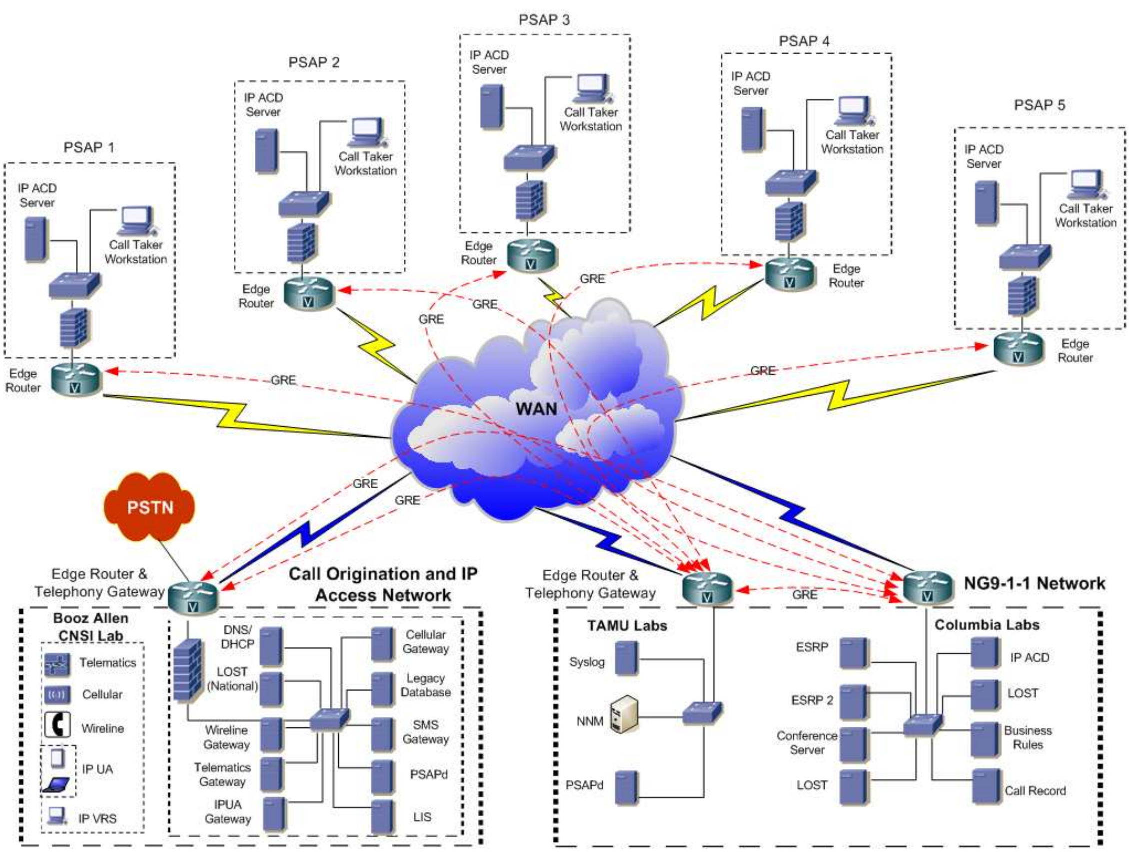

Figure 2.2: POC Demonstration High-Level Design

As shown, the Call Origination and the IP Access Network were hosted in the Booz Allen CNSI test laboratory (Herndon, VA), the NG9-1-1 Network was hosted logically between the TAMU (College Station, TX) and Columbia (New York, NY) test laboratories and the five PSAPs housed the call termination equipment. T1 circuits were provisioned between the Booz Allen, TAMU, and Columbia test laboratories and the five PSAPs to provide interconnectivity between all functional components.

Test calls originated from the call origination endpoints and were routed through the IP Access Network to the NG9-1-1 Network. Components within the NG9-1-1 Network analyzed the call and identified the appropriate PSAP to route the call to based on the call stream parameters.

Figure 2.3 depicts the general flow of calls demonstrated in the POC.

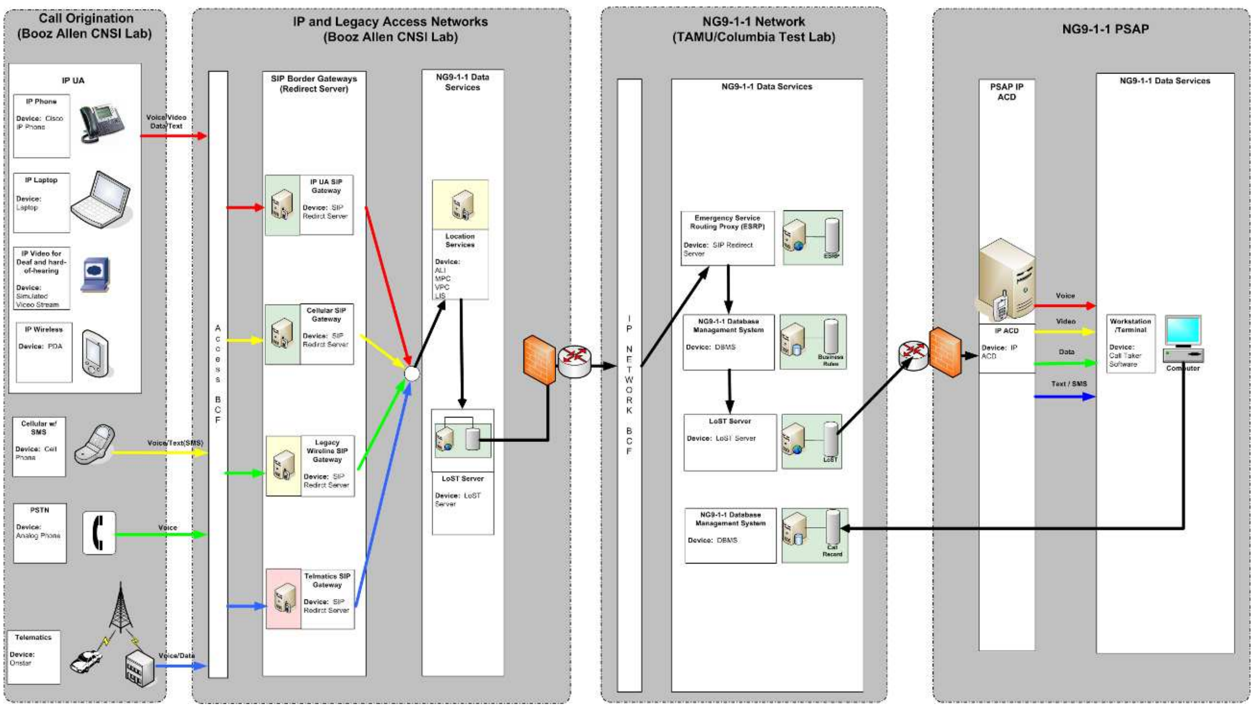

Figure 2.3: Flow Diagram for Call Testing

Subsequent sections of this document outline, in detail, the design of each component and specify products that will be used for the POC demonstration.

2.3 POC System Design Approach

Figure 2.4 depicts the four-step approach that the Booz Allen Team adopted to develop NG9-1-1 POC SDD.

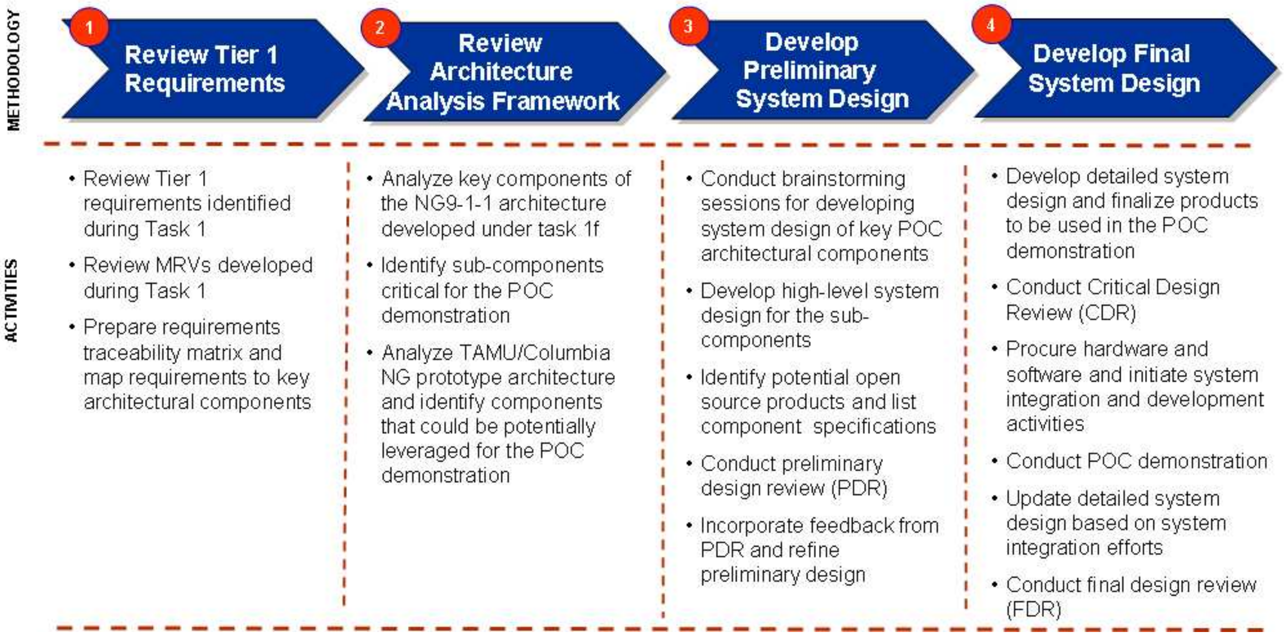

Figure 2.4: POC System Design Approach

As a first step, the Booz Allen Team reviewed the Tier 1 functional requirements developed during Task 1 and analyzed the Multidimensional Requirements Views (MRV) for various NG9-1-1 use cases. The MRVs are a layered representation of the functional requirements of the system. The team then analyzed the NG9-1-1 architecture developed during Task 1f to identify key components to be included in the POC demonstration. The team also conducted a gap analysis of the TAMU/Columbia prototype to identify components that could be leveraged from the prototype for the POC demonstration.

Subsequently, several brainstorming sessions were held to develop the preliminary system design of key components. A Preliminary Design Review (PDR) discussion was conducted to capture input on the initial system design. Input from the PDR was incorporated to develop the detailed system design for the CDR. Subsequent sections of this document outline the detailed system design of each architectural component to be included in the POC demonstration.

3 CALL ORIGINATION POC SYSTEM DESIGN

During the POC, a number of next generation call origination scenarios were tested. These include call origination using—

- Legacy PSTN Phones
- Cellular phones (Voice and SMS Texting)
- Third-Party Call Centers (Telematics Systems)
- IP UAs (including laptops with SIP clients, IP phones, and IP wireless devices)

The demonstration focused on the delivery of the call information from these call origination devices to the NG9-1-1 PSAP using IP access and NG9-1-1 networks.

3.1 Design Definition and Perspective

The architecture defined for the POC for originating calls was configured at the Booz Allen CNSI test laboratory. Figure 3.1 depicts the high-level design of the call origination devices and illustrates how they were interfaced with other NG9-1-1 System components.

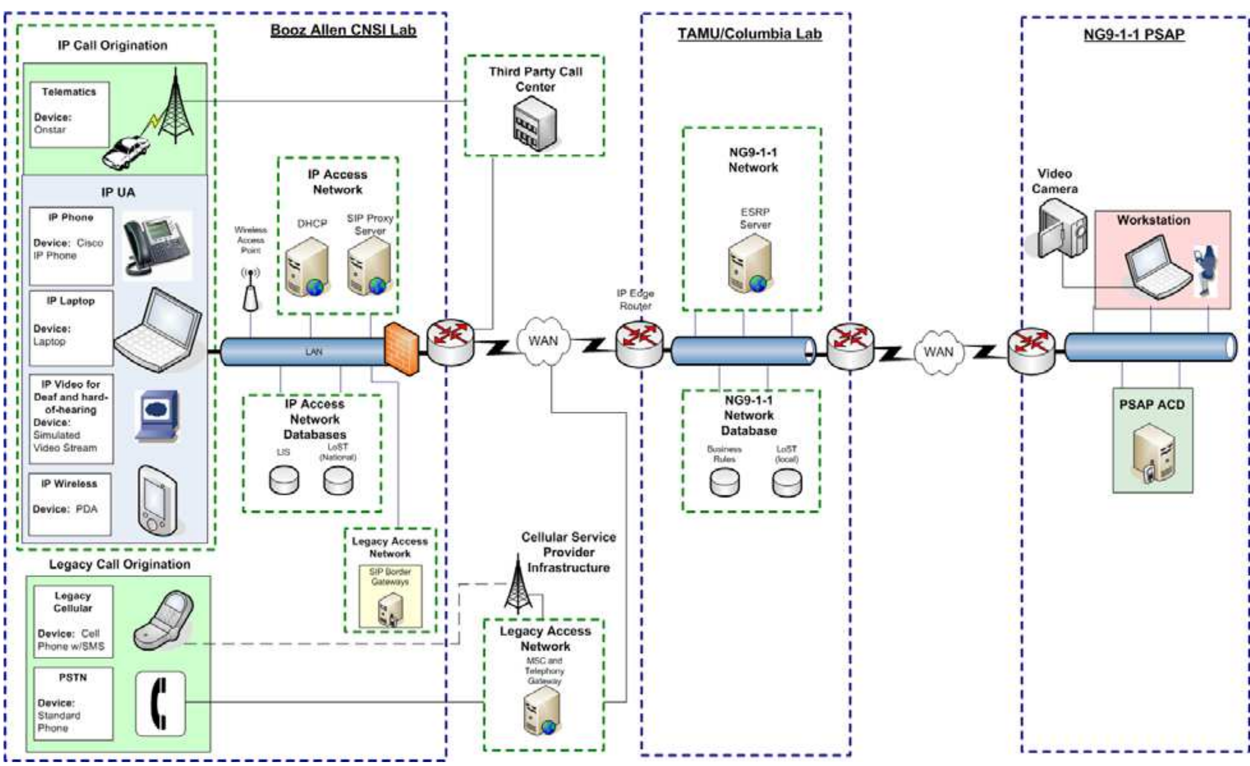

Figure 3.1: Call Origination Overview

The call origination devices were located in the Booz Allen CNSI test laboratory. The calls were routed through an IP access network to the NG9-1-1 Network. Subsequent subsections provide detailed design and system specifications for each call origination device type. Each device type is explained in later sections.

3.2 Design Constraints and Considerations

The call origination system design for the POC met all requirements for delivering IP and legacy calls to the NG9-1-1 Network. However, constraints limited successful demonstration of some features and functionalities. These constraints include—

- **Integration Constraint:** The NG9-1-1 routing paradigm requires a location for an emergency call to be presented with the call. Acquiring location information for the various call types (wireline, cellular, telematics, IP UA, and SMS) requires integration with a variety of external systems including ALI's, MPC's, VPC's, and LIS's. In some instances, such as SMS texting, the technology does not support location association or acquisition. Additionally, most commercial service providers would not allow access to their production locationing systems. This proved to be a significant integration and implementation challenge for the various call origination devices.
- **Development Constraint:** In order to overcome these location acquisition challenges many of the external location systems were simulated and developed specifically for the POC environment. For the POC an ALI, MPC, and SMS positioning system were developed this provide a much more controlled environment and limited the POC environment's dependence on external systems.

3.3 Call Origination Using IP UA (Laptop with SIP Clients, IP Wireless, IP Phones)—Design and Specifications

IP UAs were used to demonstrate IP voice, video, data and text to an NG9-1-1 PSAP. Figure 3.2 depicts the detailed system design of the IP UA call origination sub-component.

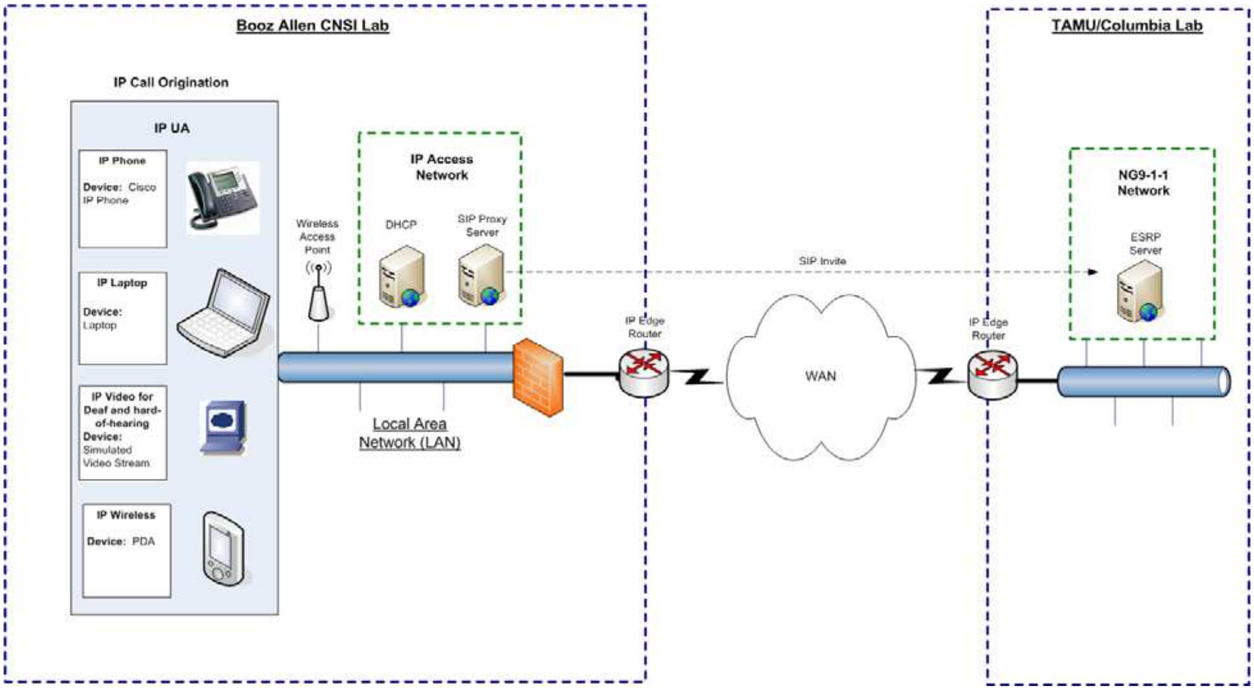

Figure 3.2: IP UA Call Origination Design Overview

The following IP-based communications devices were integrated into the POC environment to demonstrate the capabilities of an IP-UA:

- Laptop with a SIP client
- IP wireless devices (PDA with SIP client)
- IP phones
- IP VRS with streaming video client

The laptop, IP phone, wireless access point, and IP VRS were connected to a standard Cisco 3500 series switch. A SIP client was loaded on the laptop, and calls were initiated from it. An IP camera was also connected to the laptop to demonstrate streaming video capabilities. The video streams generated using the camera demonstrated the ability of the NG9-1-1 system to support the deaf and hard-of-hearing community. Unfortunately, due to constraints in the hardware the conference server used in the POC did not support three way video, although there are industry products available that support this capability. Additionally, the SIP client also provided the ability to support real-time texting. Users of the SIP client could establish an emergency instant message session with a PSAP call taker. The ability to simultaneously support voice, video and text demonstrated the diversity of communication mediums that the NG9-1-1 system could support. IP addresses were provided to the IP UAs using a Dynamic Host Configuration Protocol (DCHP) server located within the IP access network.

3.4 Call Origination Using Cellular Phone—Design and Specifications

Emergency Cellular and SMS calls were demonstrated in the POC. A simulated MPC database was used to obtain the location information for cellular voice calls. The MPC today is located in the providing carrier's network. Additionally, a SMS Positioning System was created to support location acquisition for SMS text messages. It should be noted that currently, there are no commercial systems available that locate senders of SMS. Given the mobile nature of cellular handheld devices the PSAP Call Taker was able to "Rebid" for an emergency caller's location. During a "Rebid" the NG9-1-1 System would re-query the cellular handheld to acquire its updated position information. Figure 3.3 shows the various sub-components that were used to demonstrate the Cellular Voice and SMS use case for the POC demonstration.

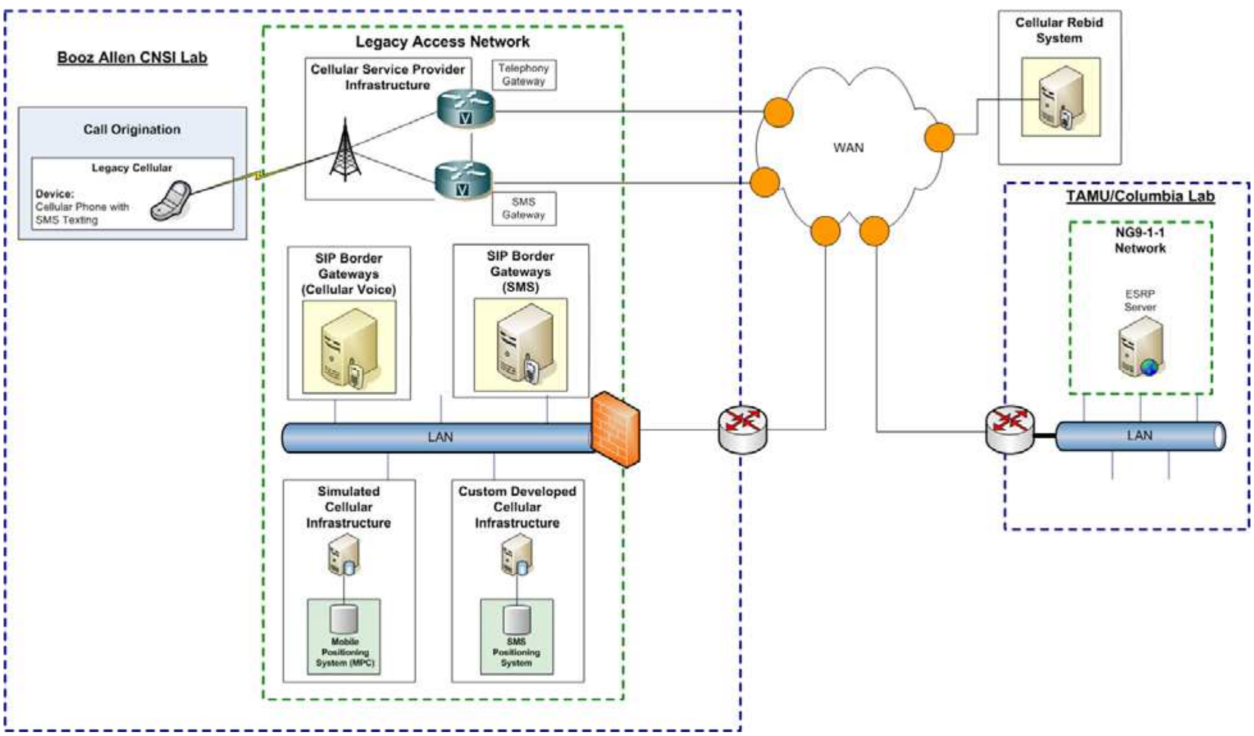

Figure 3.3: Cellular Call Origination Design Overview

The POC used a standard cellular phone and cellular network to communicate to the NG9-1-1 POC test-bed network and deliver standard voice calls and SMS to the NG9-1-1 System. A cellular phone generated emergency voice calls or SMS text messages which were sent to a cellular service provider. The cellular service provider forwarded the cellular voice call or SMS data to the respective Cellular or SMS Border gateway. For Cellular voice, the border gateway acquired location for the cellular call from a simulated MPC. It then embedded this information in the call stream and forwarded the call onto the NG9-1-1 network to an ESRP. Similarly, for the SMS Use Case, the SMS border gateway received an SMS text message, converted the SMS message to a SIP based message, acquired location from the SMS positioning system and then forwarded the message to an ESRP. IP was used to transport the voice and text information, and SIP will be used to establish and tear down the sessions. Once the call or text terminated at the PSAP the PSAP Call Taker had the ability to "Rebid" for the caller's location. In order to provide this capability the Call Taker Software would query a Cellular Rebid System. The Rebid System would check its internal DB and determine if it knew the location of the requested cellular phone. If the Rebid System did not have current information on the location of the caller it would send a query to the cellular device asking for updated location information. Once the Rebid System obtained location information on the caller it would send this information back to the Call Taker.

3.5 Call Origination using Telematics UA—Design and Specifications

The Telematics use case was demonstrated using a third-party call center service from OnStar. Figure 3.4, depicts the design used to demonstrate this use case.

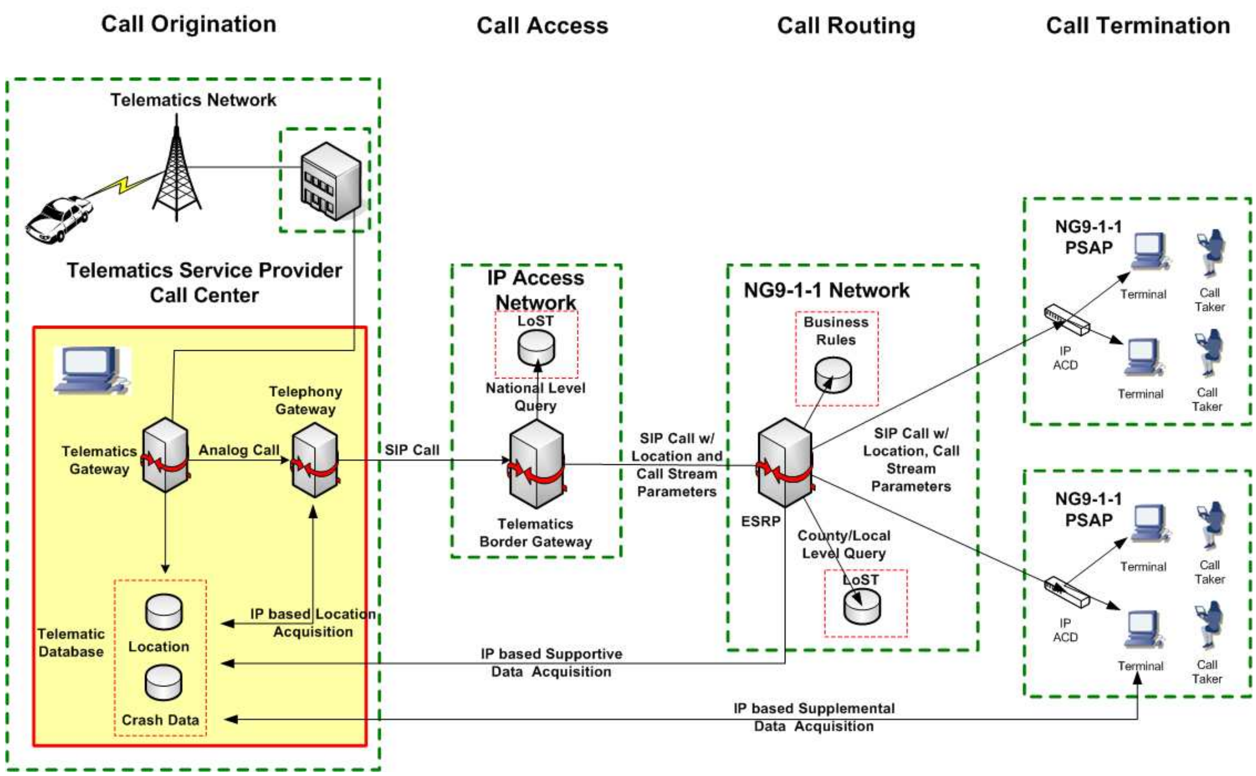

Figure 3.4: Telematics Device Call Originations Design Overview

As shown, the emergency crash notification data is sent to the telematics service provider's call center using a cellular link. Within the telematics service providers call center the emergency call is converted to a SIP based call. The telematics service provider also embeds the location of the incident within the call stream and forwards the call to the Telematics border gateway. The Telematics border gateway determines where to route the call by querying the LoST DB and then forwards it to an ESRP. The ESRP can query its business rules DB or obtain additional supportive data that may effect where the call is routed. As an example, an ESRP could determine the severity of the crash by obtaining additional Automatic Crash Notification (ACN) data. Based on the severity of the crash the ESRP may route the call to a different PSAP or automatically conference in a third party such as an EMS or trauma center. The ESRP then forwards the call onto a PSAP where a call taker can handle the call. The Call Taker also has access to all ACN data and is presented this information on the Call Taker software.

3.6 Call Origination Using Legacy Wireline Device—Design and Specifications

The POC demonstrated the ability to deliver a standard wireline emergency call through an IP transport. Calls originating from the legacy PSTN phones were routed to the NG9-1-1 Network using a telephony gateway. The telephony gateway converted the call to SIP, acquired location from a simulated ALI DB and forwarded the call to a SIP border gateway server, which initiated a SIP session to the NG9-1-1 Network. Figure 3.5 depicts the design for this scenario.

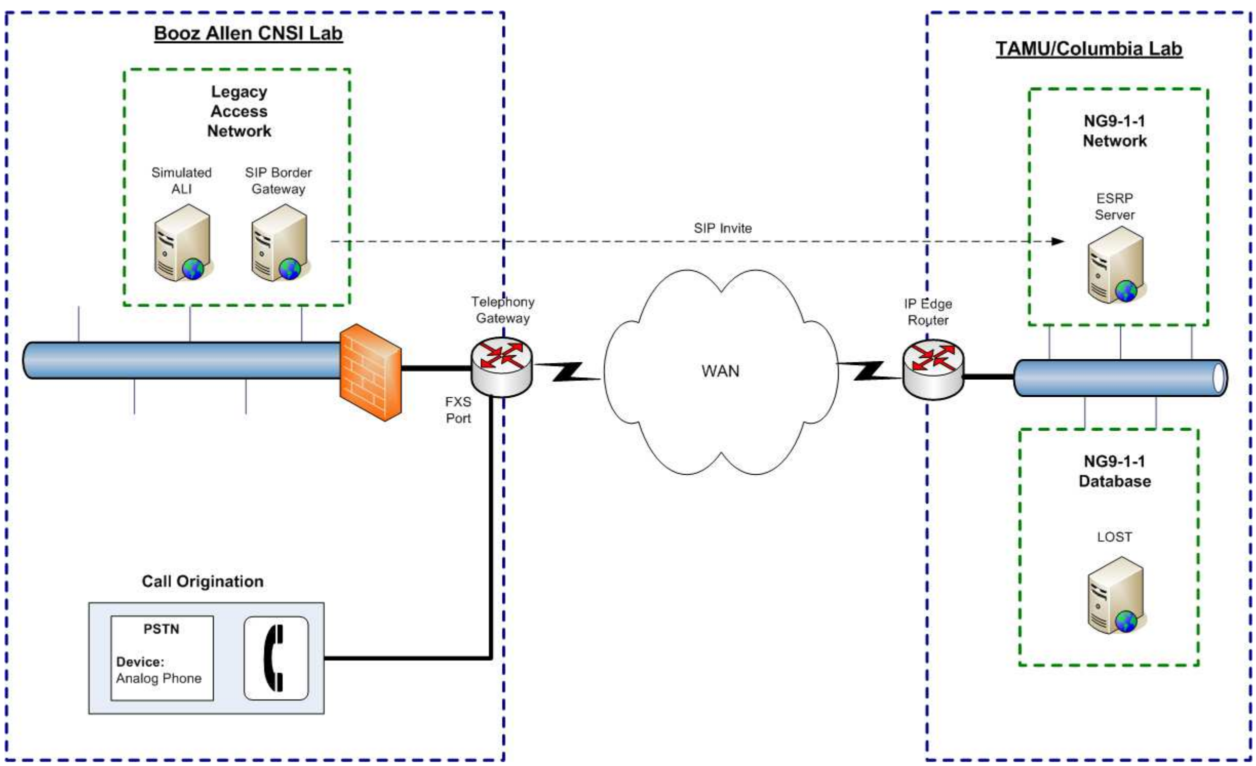

Figure 3.5: Wireline Call Origination Design Overview

4 IP ACCESS NETWORK POC SYSTEM DESIGN

The purpose of the IP access network in the POC is to provide location acquisition and validation, IP routing, and SIP signaling functions. The IP access network was simulated at the Booz Allen CNSI test laboratory and hosted the following equipment: Dynamic Host Configuration Protocol (DHCP) Server to allocate IP addresses dynamically to network devices, Domain Name System (DNS) Server to translate host names to IP addresses, Acquisition Servers (ALI, MPC, VPC, LIS), LoST, SIP Border Gateway Servers, Telephony Gateway, and routers. In addition, the IP access network routed the 9-1-1 calls to the NG9-1-1 Network.

4.1 Design Definition and Perspective

The Booz Allen CNSI test laboratory was used to simulate and host the test-bed for the IP access network for the POC. In the POC, the IP access network provided the function of a service provider's network and provided services such as DHCP, DNS, location acquisition, signaling, and IP routing. The IP access network served as the bridge between the IP call origination function and the NG9-1-1 Network and routed IP packets using traditional WAN routing protocols such as Multiprotocol Label Switching (MPLS).

The DHCP service provided the IP address to the IP endpoints, and location acquisition and validation was performed using multiple mechanisms/databases such as ALIs, MPCs, VPCs, LISs, Global Positioning System (GPS) devices, Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) and DHCP. A telephony gateway provided an interface for legacy wireline and cellular systems to connect to the IP access network. The telephony gateway converted incoming legacy technologies into SIP based calls. SIP signaling was used to transport the call and its associated call stream information (location, call type, supplemental data links, etc.) to the NG9-1-1 Network.

4.2 Design Constraints and Considerations

In a real-world implementation of the NG9-1-1 architecture multiple networks would serve as the IP access network. For the POC, the IP access network was simulated solely within the Booz Allen CNSI test laboratory. In addition, implementation of location acquisition services would vary by service provider and would depend on the technologies that service provider supported (legacy wireline, cellular, VoIP, SMS, telematics, sensor data, etc.) Although the POC tested and demonstrated several different types of location acquisition mechanisms, some of these systems (ALI, MPC, SMS) were simulated in order to ease integration and scheduling constraints.

4.3 IP Routing Design and Specifications

The NG9-1-1 System relied on standard protocols and best practices for IP routing of converged service networks. All voice, video, and data traffic was embedded in IP packets and transported across the IP access and NG9-1-1 networks. Since there was limited traffic on the POC network, no priority or QOS mechanisms were utilized.

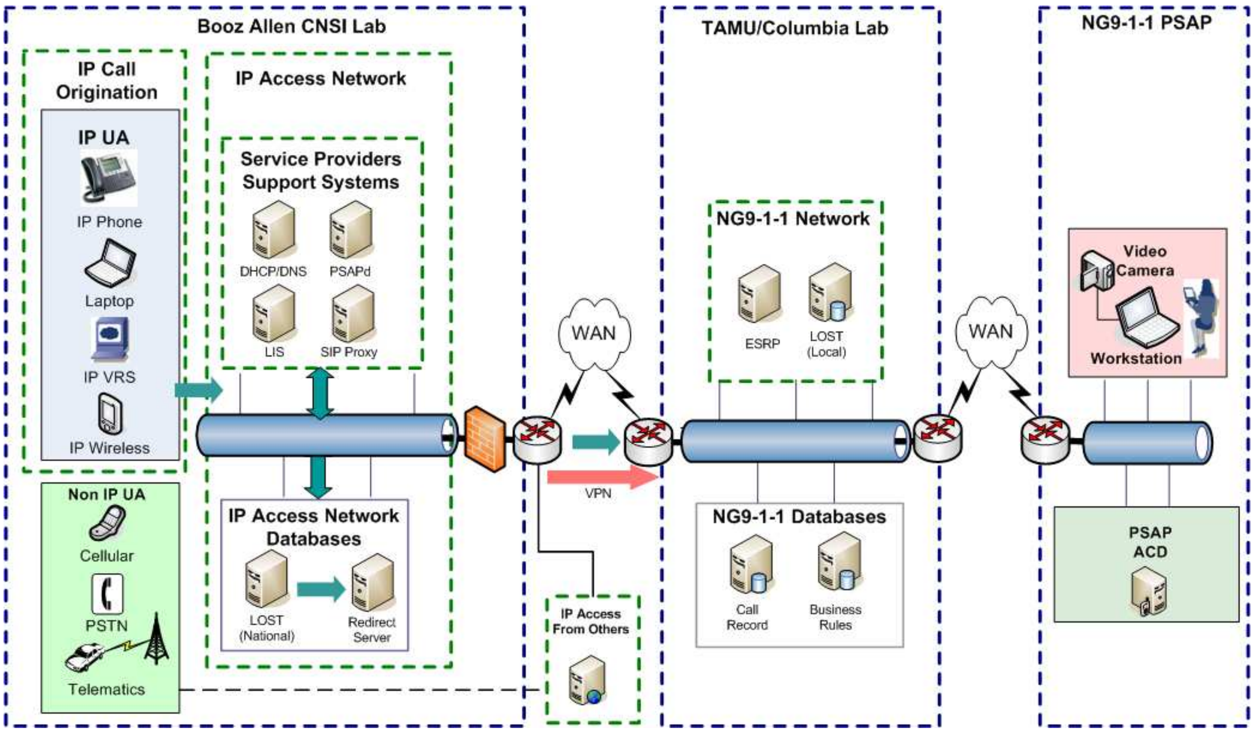

Figure 4.1: IP Routing Within IP Access Network Overview

Figure 4.1 depicts a high-level design of IP routing within the IP access network for the POC. Later sections depict the routing of specific types of user devices. All incoming emergency calls regardless of technology (wireline, cellular, telematics, IP UA, SIP) were converted to IP at a gateway. Once the call was converted to IP it could be routed just as any other standard IP packet across the POC network. Calls entered the IP access network through telephony gateways or were natively based on IP. Once within the IP access network the IP calls accessed location and call routing services. Once it was determined where to route the call, the call was forwarded out of an edge/border gateway across the WAN via Virtual Private Network (VPN) and onto the NG9-1-1 network. Traditional WAN routing protocols such as MPLS and ATM were used to route the IP packets across the IP Access and NG9-1-1 Networks. The IP access network, NG9-1-1 network, and PSAPS were connected using GRE Tunneling to create a VPN environment. Within the LAN environments standard switching mechanism were utilized to route the IP calls.

IP routing within the POC environment was performed using industry standard Cisco routers. Cisco 2821 routers were used to route IP packets from the IP Call Origination sources to the NG9-1-1 PSAP. The Cisco 2821 router was chosen because it is capable of supporting T1 WAN interfaces and SIP and can support various security features such as VPNs.

The security function of the IP access network includes a firewall feature-set. For the POC, Cisco ASA5505-K8 was used to provide this function. Appropriate ports were opened on the firewall to enable end-to-end secure connectivity. Logs from the firewall and other network devices were sent to the Syslog server to log alarms and alerts. The Cisco ASA5505-K8 also terminated VPN connections to the NG9-1-1 Network's edge router.

For the POC, SIP signaling was used for session establishment and tear down. All call origination sources were converted to SIP and therefore could be handled similarly through the system. Figure 4.2 below depicts how a SIP session was established and terminated within the POC environment.

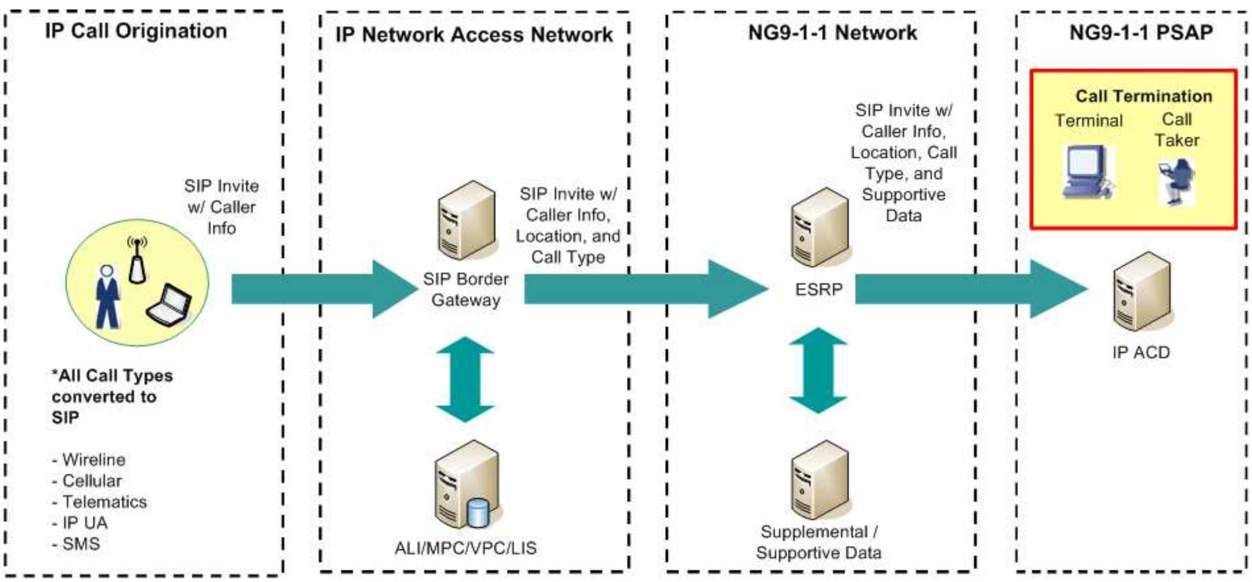

Figure 4.2: End-to-End SIP Session

For the POC all call origination sources (wireline, cellular, telematics, and SMS) were converted to a SIP based call. It should be noted that the IP UA's (IP phones, IP wireless devices, and SIP clients) natively supported SIP. Upon instantiation, the SIP call was initially registered by the SIP Border Gateway Server located within the IP access network. If it was not already contained within the SIP Invite, the SIP Border Gateway used the Caller's Information to obtain location information for the caller. Various Location Acquisition Systems were used depending on the type of call. From the location information the SIP Border Gateway queried a LoST Server to determine which PSAP location the call should be routed to. The SIP Border Gateway embedded this information within the SIP invite and forwarded it to the appropriate ESRP located within the NG9-1-1 Network. The ESRP then queried another LoST Database to determine the appropriate PSAP to forward the SIP invite to. The PSAP IP ACD received the incoming SIP Invite, terminated the invite, and forwarded the call to the first available and most capable Call Taker. The Call Taker's Workstation and the Call Origination Device then establishes a two-way media session that can contain voice, video and/or data depending on the capabilities of the caller and call taker. Once the Call completed and the needs of the Caller were addressed the call was torn down using a similar process of SIP BYE messages.

4.4 Location Acquisition and Validation—Design and Specifications

For the POC, location information was acquired in numerous ways. The most simplistic use case required that the Call Origination device itself acquire location. This was demonstrated using the SIP client software. The SIP client software was able to interface with GPS, DHCP Servers and LLDP-MED compatible switches.

For most technologies location could not obtain by the device itself as was the case for legacy wireline, cellular, telematics, and IP Phones. For the legacy wireline, cellular and SMS devices the call was converted to SIP and forwarded into the network with no location information. When the call arrived at a SIP Border Gateway, the Border Gateway would determine what type of call it was and query its respective network location information system. For example, for a wireline call the SIP Border Gateway would query a simulated ALI DB. For cellular and SMS calls the SIP Border Gateway would query an MPC or SMS Positioning System respectively.

For telematics calls and IP Phones a network LIS proxy was used to acquire location. As these calls traversed the IP Access network they passed through an LIS proxy device which automatically embedded location information into the call stream. Figure 4.3 shows how location acquisition was executed for the various call types in the POC demonstration.

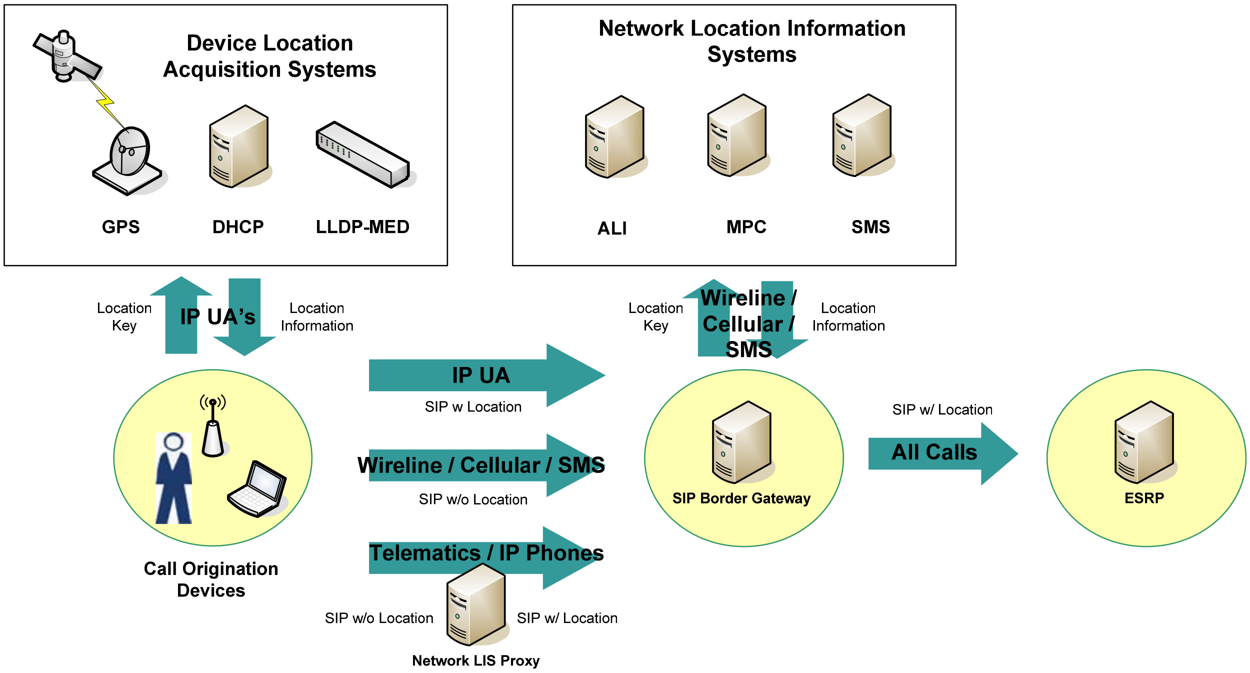

Figure 4.3: Location Acquisition and Validation Overview

For the POC, all caller location information was assumed to be pre-validated. Therefore, the location information was not validated for proper street number ranges or street names. A typical location validation process involves sending a query to an official MSAG DB. MSAGs are hosted and administered either directly by a 9-1-1 service provider or outsourced to a third-party vendor, this was not possible for the POC due to scheduling constraints.

4.5 Telephony Gateway Design and Specifications

The function of the telephony gateway in the POC was to connect legacy PSTN and Cellular devices to the IP access network. Figure 4.4 depicts the high-level interconnectivity design of the telephony gateway.

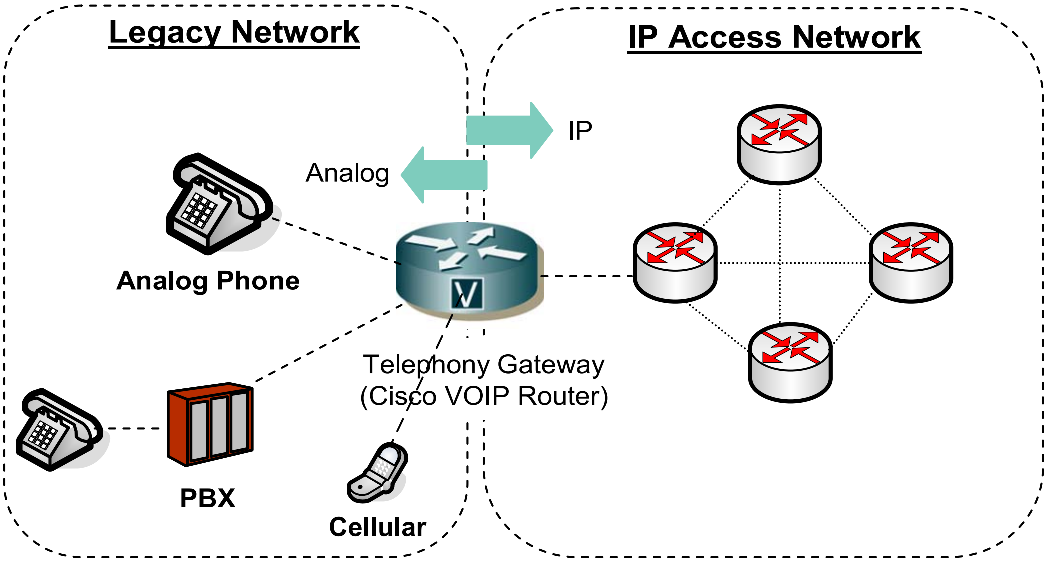

Figure 4.4: Telephony Gateway Design

Analog wireline and cellular phones were connected through their respective service providers to the telephony gateway, which performed the analog-to-IP conversion, encapsulated voice traffic into IP packets, and forward them to the IP access network.

5 NG9-1-1 NETWORK POC SYSTEM DESIGN

The primary function of the NG9-1-1 Network is to identify appropriate PSAPs based on the call origination information and to efficiently route the call to them while maintaining data integrity. Several simulated next generation databases included in the design were used to streamline this process and ensure that appropriate business rules were applied prior to routing the calls to the PSAP.

The NG9-1-1 Network test-bed for the POC was hosted at the TAMU/Columbia laboratories. The sub-components included in the design were—

- ESRP
- LoST server
- Identity Management Database (including Data Rights)
- Business Rules Database
- Call Record Database.

5.1 Design Definition and Perspective

The NG9-1-1 Network for the POC is designed using standard Open System Interconnect (OSI) architecture. At the network layer, T1 circuits were used to provide the WAN connectivity to the PSAPs. IP WAN routers connecting to the dedicated T-1s within the TAMU and Columbia laboratories routed the calls to the appropriate PSAPs.

A network designed as an IP overlay is a cost effective method of building a WAN to support the POC Layer 3 functions of the POC. The entire NG9-1-1 POC network was designed to be scalable and employed a WAN architecture to focus on IP delivery across the network. This design created a hierarchical framework to allow multiple services to access the network. The T-1 network using IP creates a common interface to the various devices and technologies associated with the POC.

The NG9-1-1 Network also used an ESRP. The ESRP made all the call routing decisions within the POC network. The ESRP received location information from the NG9-1-1 databases and forwarded the call and data to the IP WAN for routing the call to the correct PSAP.

The NG9-1-1 Network used SIP signaling to terminate calls. In the POC, the network provided bandwidth and transport facilities that allowed the delivery of the calls across the WAN to one of the PSAPs. All database functions were centrally located at the TAMU/Columbia test facilities.

5.2 Design Constraints and Considerations

The NG9-1-1 Network design was based on a hub spoke architecture in which the Booz Allen and Columbia labs and PSAP all connected to the TAMU test laboratory. To maintain integrity of the data over the WAN, VPNs were configured using GRE tunnels. However, the GRE tunnels limited the use of dynamic routing protocols over the WAN.

Standards for several NG9-1-1 databases such as Data Rights and Business Rules do not exist today and had to be custom developed.

5.3 NG9-1-1 IP Routing Design and Specifications

The IP routing within the POC NG9-1-1 Network was performed by the WAN edge routers located at the TAMU/Columbia test laboratories. Based on the call stream parameters, the ESRP routed the call data to the appropriate PSAP. Figure 5.1 depicts, at a high-level, how routing was executed within the NG9-1-1 Network.

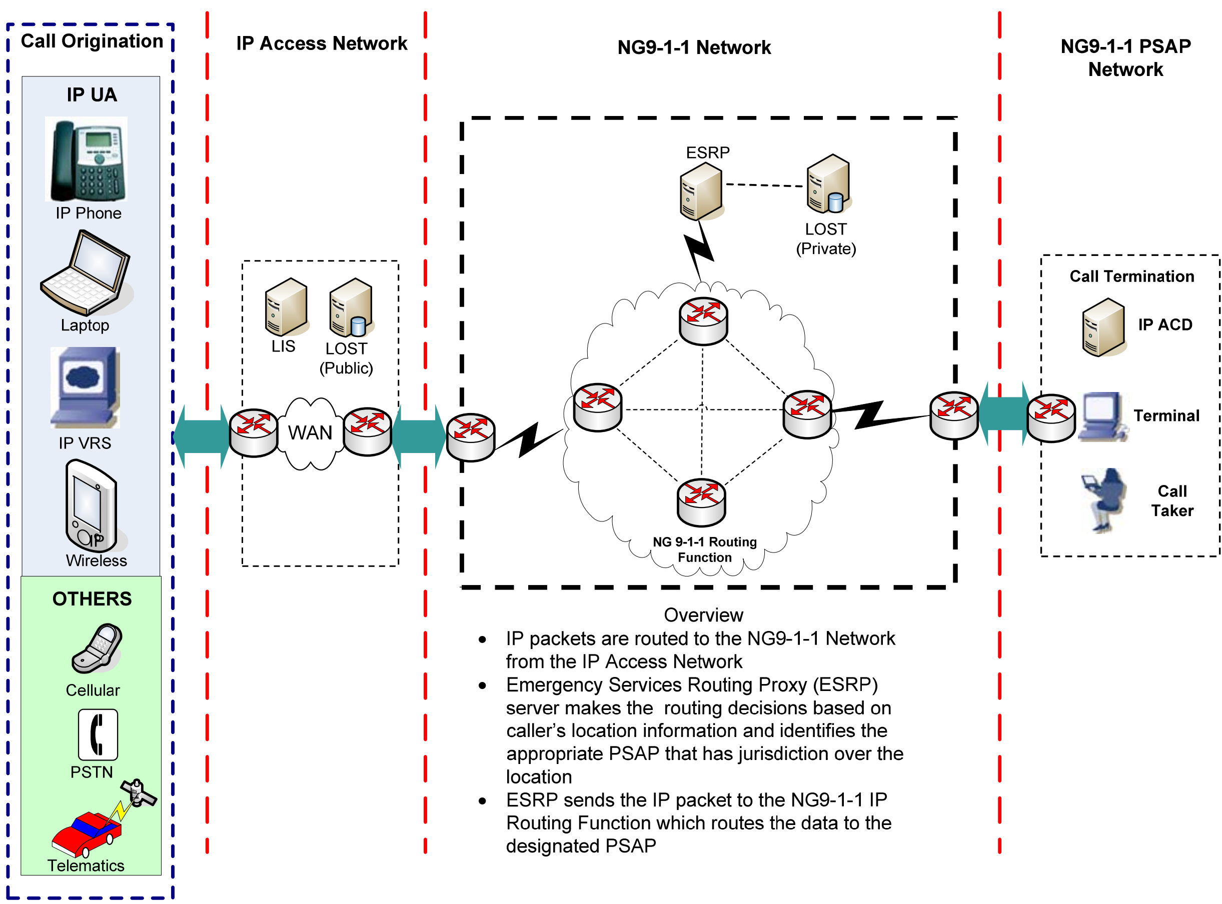

Figure 5.1: NG9-1-1 Network IP Routing Overview

VPN tunnels configured on the WAN edge routers at the TAMU/Columbia test labs encrypt and route the IP packets to the appropriate PSAP. If the target PSAP is unavailable, then the call was dynamically routed to the backup PSAP. SIP signaling was used to establish SIP calls between the ESRP and the IP ACD server located at the PSAPs.

5.4 NG9-1-1 Database Design

Databases are a key component of the NG9-1-1 POC System Architecture. Databases store a variety of data and enable numerous system functions on the NG9-1-1 Network. Given the functional diversity of the data, geographically distributed nature of the network, decentralized operation of the stakeholders, and stringent emergency service requirements for reliability, availability, scalability, and serviceability, each database is designed uniquely to serve its specific function.

There is also a need for the NG9-1-1 Network to integrate with a variety of legacy databases to support emergency services for older communications systems. These legacy databases may eventually be phased out as communication systems shift from analog to digital mode, as control methods change, or as federal policy mandates. In addition, these databases were appropriately scaled with hardware, software, and network connectivity based on expected transactional loads and desired use cases for the POC. Figure 5.2 depicts the high-level overview of the NG9-1-1 and legacy databases.

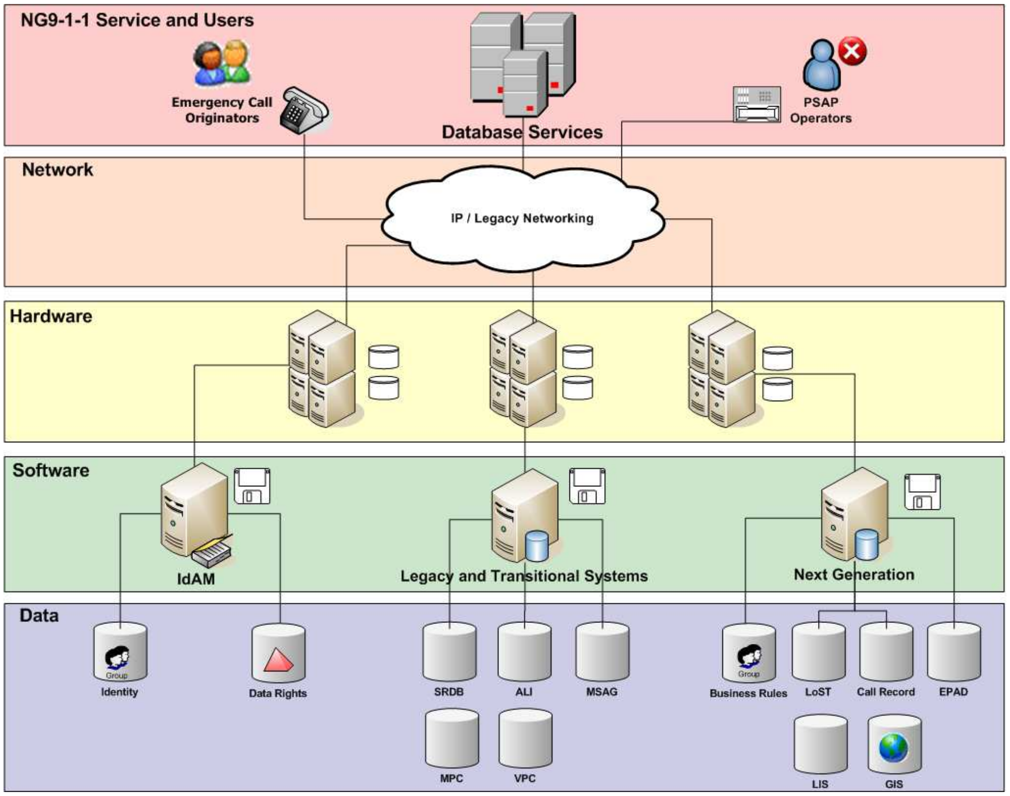

Figure 5.2: NG9-1-1 Databases Overview

For conciseness, only those databases implemented and/or simulated for the POC were documented in the subsequent sections.

5.4.1 Automatic Location Identification (ALI)

For the POC the ALI DB was simulated using an IP addressable relational database. An ALI Database provides caller location, subscriber name, Call Type related data, and other ALI data items to the call stream when a legacy 9-1-1 call enters the NG9-1-1 Network. This data was then used to support routing of the call to the appropriate PSAP and to display caller information to the call taker.

Because of technical complications and time and budget constraints, an IP-accessible LIS approach was used for the POC, with simulated ALI data populated into the LIS. The National Emergency Number Association (NENA) Data Exchange Standard 02-010 provides the content and format of the data required to be used to populate the ALI data records. This document can be downloaded from the following site: http://www.nena.org/media/files/02-010_20070717.pdf

5.4.2 Mobile Positioning Center (MPC)

MPCs are typically operated for cellular carriers by vendors and are based on near-real-time location acquisition from other servers. They also provide routing code assignment services for cellular 9-1-1 calls to E9-1-1 systems. Dynamic ALI update data, including the caller's location, are provided to ALI servers so that full ALI can be provided to PSAPs during a cellular 9-1-1 call. The interface between ALI servers and MPCs is typically, but not exclusively, known as an E2+ interface and is a specialized protocol for this application.

The E2+ interface supplies the mobile cellular caller telephone number, the current estimated location of the handset, and other ALI equivalent data for the cellular service type. The E2 interface must be able to handle queries and responses for these various network configurations. That is, both ALI servers (typically configured as a redundant pair) must be capable of querying both MPCs in a network configuration where both operate as redundant nodes. Transmission Control Protocol (TCP)/IP and Transaction Capabilities Applications Part (TCAP) are recommended, and more specifics are available in NENA Technical Standard 05-001 at:
http://www.nena.org/media/files/05-001_20031202.pdf

For the POC, the cellular data normally provided from an MPC was acquired from a simulation of the MPC functions using a static relational database. A second method of dynamic location acquisition was tested using a third party software loaded on the cellular handset.

5.4.3 VoIP Positioning Center (VPC)

VPCs are typically operated for VoIP by Internet service providers and, based on previously stored subscriber data, provide routing code assignment services for VoIP 9-1-1 calls to E9-1-1 systems, and dynamic ALI update data, including the caller's location, to ALI servers so that full ALI can be provided to PSAPs during an Internet-based VoIP 9-1-1 call. The interface between ALI servers and VPCs is typically, but not exclusively, known as an E2+ interface, and is a specialized protocol for the similar cellular application. The E2+ interface supplies the fixed or nomadic VoIP caller telephone number, the stored current `registered address' of the handset, and other ALI equivalent data for the VoIP service type. More specifics are available in NENA Technical Standard 05-001 at: http://www.nena.org/media/files/05-001_20031202.pdf

For the POC interfacing with a VPC was not possible, the VoIP subscriber data normally provided by a VPC was simulated.

5.4.4 LoST

LoST is a discovery protocol centered on mapping civic and geospatial regions to services. For the NG9-1-1 POC, LoST was used to resolve which PSAP a UA should contact for emergency services. LoST queries contain either civic or geodetic location information and traverse from a LoST client to a LoST server. The LoST server uses its database to map the input values to one or more Uniform Resource Identifiers (URI) and returns those URIs to the LoST client. If the server cannot resolve the query itself, it may, in turn, query another server or return the address of another LoST server, identified by a LoST server name. For the POC, LoST servers resided at the Booz Allen CNSI test laboratory and the TAMU lab to simulate location acquisition. Therefore, LoST queries were resolved either recursively or iteratively. Figure 5.3 depicts the LoST function.

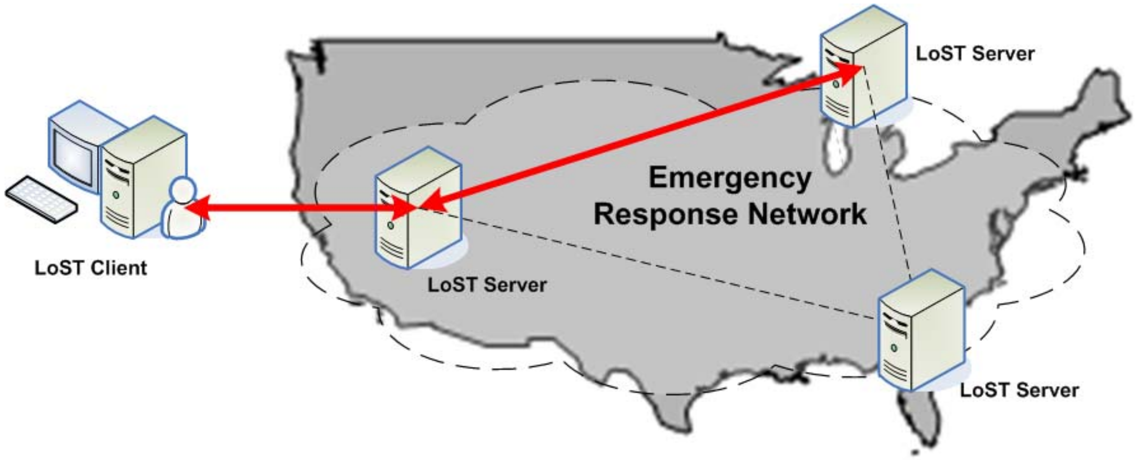

Figure 5.3: LoST Function

For the POC, the following design assumptions were made:

1. LoST clients must discover LoST Servers by using either DHCP or manual configuration.
2. The LoST database is populated with datasets (civic and geodetic) and is managed by an external authority.
3. It is the responsibility of the LoST client to query, cache, and maintain service mappings. A LoST client will not be notified if service mappings defined within the LoST databases change.
4. The datasets within the geographically distributed LoST databases will not be automatically synchronized.

As depicted in Figure 5.4, the LoST Database contained two tables that support civic and geospatial service resolution. The "civic_us" table stored civic information as defined in the Internet Engineering Task Force (IETF) Presence Information Data Format–Location (PIDF-LO) standard and associates it with a given service URI. The "geo_us" table stored geospatial information defined by a geometry object. The database was enabled with geographic information system (GIS) extensions that support geospatial queries.

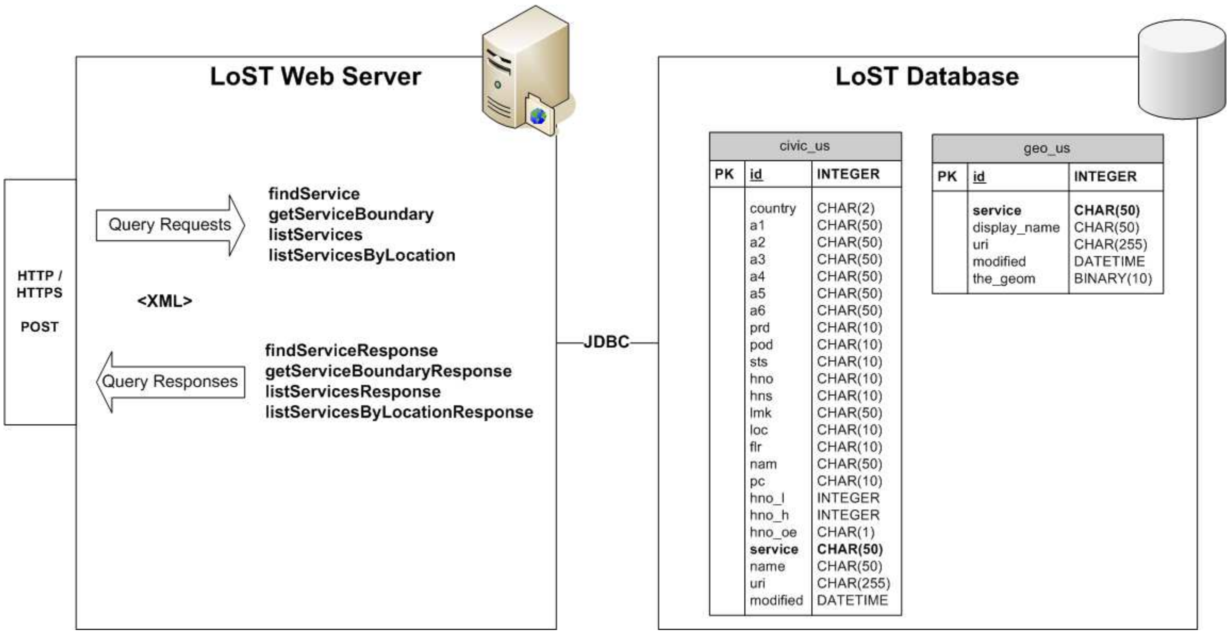

Figure 5.4: LoST Database Structure

Tables 5.1 and 5.2 list the structure of the civic and geospatial tables within the LoST Database.

LoST Civic Table

Table 5.1: LoST Civic Table Structure

Table Description		
Name	civic_us	
Description	This table maps a civic boundary defined by a PIDF-LO Profile to a service URI.	
Parameter	**Type**	**Values/Restrictions**
Id	Integer	Primary Key—must be unique
Description	unique identifier	
Country	Character	Length—2 characters
Description	two-letter ISO 3166 country code	
a1	Character	Length—50 characters
Description	national subdivisions (state, region, province, prefecture)	
a2	Character	Length—50 characters
Description	county, parish, district (IN)	
a3	Character	Length—50 characters
Description	city, township	
a4	Character	Length—50 characters

Description	city division, borough, city district, ward, etc.	
a5	Character	Length—50 characters
Description	neighborhood, block	
a6	Character	Length—50 characters
Description	Street	
Prd	Character	Length—10 characters
Description	leading street direction	
Pod	Character	Length—10 characters
Description	trailing street suffix	
Sts	Character	Length—10 characters
Description	street suffix	
Hno	Character	Length—10 characters
Description	house number (numeric part only)	
Hns	Character	Length—10 characters
Description	house number suffix	
Lmk	Character	Length—50 characters
Description	landmark or vanity address	
Loc	Character	Length—10 characters
Description	additional location information	
Flr	Character	Length—10 characters
Description	Floor	
Nam	Character	Length—50 characters
Description	name (residence, business, or office occupant)	
Pc	Character	Length—10 characters
Description	postal code	
hno_l	Integer	
Description	low in house number range	
hno_h	Integer	
Description	high in house number range	
hno_oe	Character	Length—1 character
Description	odd/even indicator	
Service	Character	Length—50 characters
Description	service Uniform Resource Name (URN)	
Name	Character	Length—50 characters
Description	service entity description for display	

Uri	Character	Length—256 characters
Description	SIP Uniform Resource Locator (URL) of a service	
modified	Timestamp	
Description	timestamp when the record is modified	
is_default	Boolean	
Description	indicator whether the record is for a default route	

LoST Geospatial Table

Table 5.2: LoST Geospatial Table Structure

Table Description		
Name	geo_us	
Description	This table maps a geospatial boundary defined by Geography Markup Language (GML) to a service URI.	
Parameter	**Type**	**Values/Restrictions**
Id	Integer	Primary Key—must be unique
Description	unique identifier	
Service	Character	Length—50 characters
Description	service URN	
display_name	Character	Length—50 characters
Description	service description for display	
Uri	Character	Length—256 characters
Description	SIP URL of a service	
Modified	Timestamp	
Description	timestamp when the record is modified	
the_geom	Geometry	Multipolygon
Description	the polygon that represents the service boundary	

LoST Database Interface

To accommodate the diverse set of LoST clients and support higher level functionality defined by the LoST protocol, the LoST Database is abstracted from LoST clients with a web interface. This interface is implemented by the LoST Web Server using HTTP and HTTPs protocol exchanges. For the POC, the queries listed in Table 5.3 will be supported. For more detail on the format and structure of the queries request/responses refer to the "IETF LoST Standard."

Table 5.3: LoST Database Interface

LoST Interface	
Interface Name	LoST Interface ID-53
Interface Design Doc	IETF LoST draft Standard
Description	This interface allows a client to query the LoST database for Service Names, Service URIs, and Service Boundaries using a variety of XML-based queries defined below.
Applications Protocol	LoST Protocol (XML) over HTTP(S)
Transport/Network Protocol	TCP / IP
Supported LoST Queries	**Description**
<findService> and <findServiceResponse>	A LoST client can retrieve service contact URIs based on location information and a service identifier.
<getServiceBoundary> and <getServiceBoundaryResponse>	A LoST client can obtain a service boundary.
<listServices> and <listServicesResponse>	A LoST client can find out which services a LoST server supports.
<listServicesByLocation> and <listServicesByLocationResponse>	A LoST client can determine which services are available for a specific location region.

5.4.5 Emergency Provider Access Directory

EPAD planned capabilities, including data or digital rights management, were not expected to be ready in alpha design form until mid-2008. Data rights management functions was not part of the current EPAD prototype. EPAD functionality was featured in the LoST database for the POC demonstration. The proposed data structure of EPAD can be downloaded from the following link: http://www.comcare.org/uploads/EPAD%20Technical%20Implementation%20Guide%20v1%202%2010242005.pdf

5.4.6 Master Street Address Guide

Current MSAG functions, including definition of valid address ranges, streets and communities, address validation data provision to other functions based on the above definitions, and the relationship of street segments and communities to public safety jurisdictions and their assigned routing codes (Emergency Service Number [ESN]) will be structured and managed differently in NG9-1-1. These types of data will appear as GIS data layers, associated with the LoST databases. As a result, the MSAG data and related physical databases were not accessed directly by NG9-1-1 functions or POC equipment.

MSAG data, however, was needed to set up the address validation and routing relationships in the POC databases, as structured under NG9-1-1 definitions. The appropriate MSAG data content was acquired for the 9-1-1 Authorities involved in the POC. The contents of a typical MSAG data record are as shown in the NENA 02-010

Data Exchange document, which is available at:
http://www.nena.org/media/files/02-010_20070717.pdf

5.4.7 Identity and Access Management (IdAM)

The IdAM databases provide identity, authentication, and authorization for users and administrators of the NG9-1-1 System. Given that the NG9-1-1 Network emphasizes an IP-based paradigm, the network, as well as its users and resources, must be protected with safeguards similar to those currently implemented in most enterprise IP-based networks today. Figure 5.5, depicts an overview of the IdAM databases.

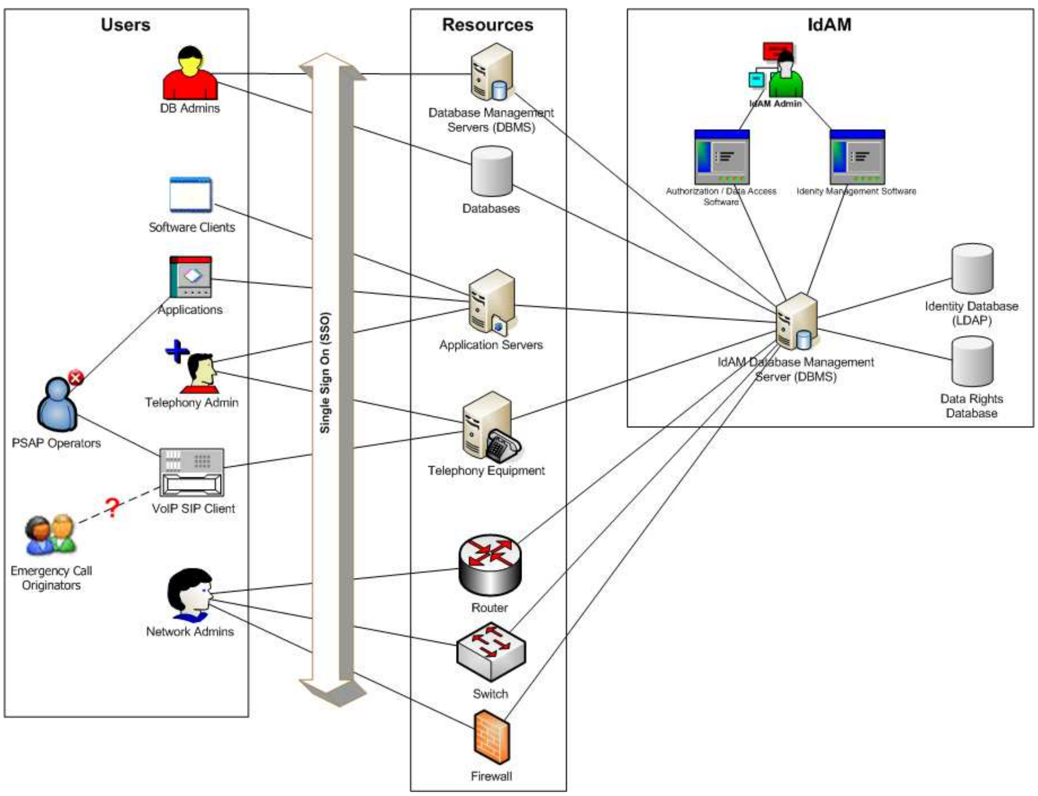

Figure 5.5: Identity and Access Management Databases

In the context of IdAM, the term *user* defines any entity that uses the NG9-1-1 Network. User is a generic term and captures a variety of entities, including system administrators, software clients, Internet service providers, and PSAP operators. It should be noted that these entities can be both animate (people) and inanimate objects (applications, devices, connections, etc). The purpose of the Identity database is to maintain and manage these identities. Due to the significant level of effort required to implement IdAM, it was not included in the scope for the POC.

Complementary to users, the term *resource* defines objects within the NG9-1-1 Network that perform a specific function (routing, switching, etc.) or provide a piece of information (database records) to users. Users use resources to execute a defined activity or use case. Examples of resources include communication infrastructure such as routers, switches, and firewalls; servers that support IP telephony or applications; or database management systems with their associated databases. The Identity database is also responsible for tracking and maintaining the identity of NG9-1-1 resources.

The Data Rights database provides authorization capabilities for the NG9-1-1 System. The Data Rights database is responsible for maintaining a mapping between users and resources. When a user attempts to access a resource, the resource queries the Data Rights database to ensure the user has appropriate privileges. It is usually the responsibility of an IdAM Administrator to maintain a user's roles and privileges within the system.

It is envisioned that in order to move to an IP-based NG9-1-1 Network, an Enterprise Network Operations Center (ENOC) will have to be created to manage IdAM functionality. Given the geographically distributed and loosely coupled nature of the NG9-1-1 Network, IdAM functionality will likely be implemented in a federated manner. Given that the NG9-1-1 POC's main focus is emergency operations and use cases, a simplistic IdAM approach was demonstrated for the POC. However, this topic should be reevaluated in a nationwide operational deployment of the NG9-1-1 Network.

Figure 5.6, depicts the overview of the IdAM database structure.

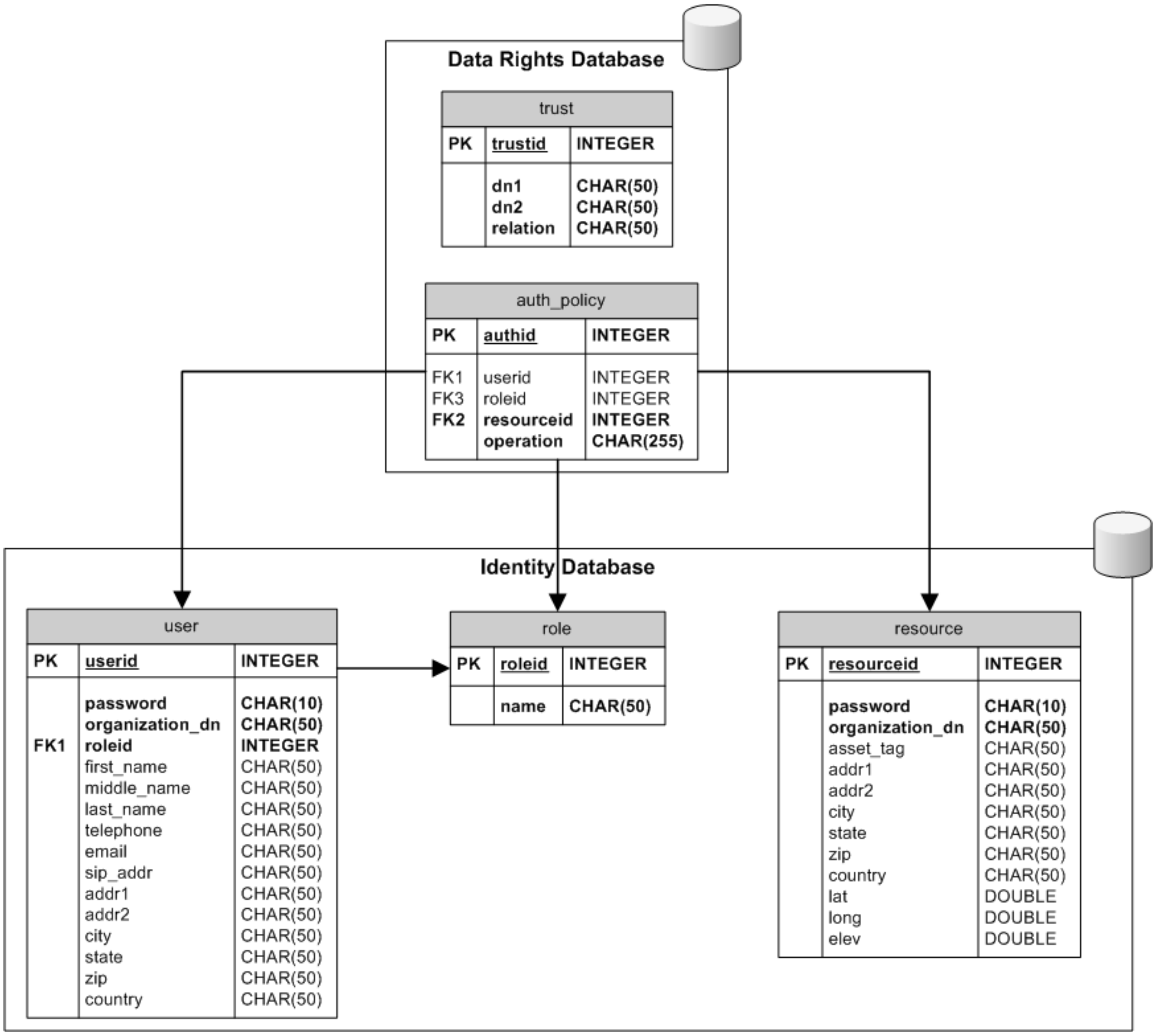

Figure 5.6: IdAM Database Structure Overview

It should be noted the defined IdAM schema is strictly conceptual in nature. There are a variety of standards-based vendor products that implement IdAM functionality. This schema captures the basic functionality of an IdAM system. Structure for the user, role, resource, authorization, and trust tables are shown below.

User Table

Table 5.4: User Table Structure

Table Description		
Name	User	
Description	This table stores the properties and credentials of an NG9-1-1 Network User.	
Parameter	**Type**	**Values/Restrictions**
Userid	Integer	Primary Key—must be unique

Description	unique identifier for an NG9-1-1 Network User	
Password	Character	Length—50 Characters
Description	password for the User (Provides Single Sign On (SSO) capability)	
organization_dn	Character	Length—50 Characters
Description	domain to which the User belongs	
Roleid	Integer	Length—50 Characters
Description	role of the User (e.g., DB Admin, Sys Admin, PSAP Call Taker etc.)	
first_name	Character	Length—50 Characters
Description	first name of the User	
middle_name	Character	Length—50 Characters
Description	middle name of the User	
last_name	Character	Length—50 Characters
Description	last name of the User	
Telephone	Character	Length—50 Characters
Description	POTS telephone number of the User	
Email	Character	Length—50 Characters
Description	e-mail address of the User	
sip_addr	Character	Length—50 Characters
Description	SIP address of the User	
addr1	Character	Length—50 Characters
Description	address of the User	
addr2	Character	Length—50 Characters
Description	supplemental address information for the User	
City	Character	Length—50 Characters
Description	city in which the User resides	
State	Character	Length—50 Characters
Description	state in which the User resides	
Zip	Character	Length—50 Characters
Description	zip code in which the User resides	
Country	Character	Length—50 Characters
Description	country in which the User resides	

Role Table

Table 5.5: Roles Table Structure

Table Description		
Name	Role	
Description	This table stores the defined NG9-1-1 System Roles.	
Parameter	**Type**	**Values/Restrictions**
roleid	Integer	Primary Key—must be unique
Description	unique identifier for an NG9-1-1 System role	
name	Character	Length—50 Characters
Description	Text Tag identifying the role (e.g., Sys_Admin, DB_Admin, etc.)	

Resource Table

Table 5.6: Resource Table Structure

Table Description		
Name	Resource	
Description	This table stores the properties and credentials of a NG9-1-1 Resource.	
Parameter	**Type**	**Values/Restrictions**
Resourceid	Integer	Primary Key—must be unique
Description	unique identifier for an NG9-1-1 Resource	
Password	Character	Length—50 Characters
Description	password for the Resource	
organization_dn	Character	Length—50 Characters
Description	domain the Resource belongs to	
asset_tag	Character	Length—50 Characters
Description	Asset Tag of the Resource for tracking purposes	
addr1	Character	Length—50 Characters
Description	address of the Resource	
addr2	Character	Length—50 Characters
Description	supplemental address information for the Resource	
City	Character	Length—50 Characters
Description	city the Resource resides in	
State	Character	Length—50 Characters
Description	state the Resource resides in	
Zip	Character	Length—50 Characters
Description	zip code the Resource resides in	
Country	Character	Length—50 Characters
Description	country the Resource resides in	

Lat	Double	
Description	latitude of the Resource	
Long	Double	
Description	longitude of the Resource	
Elev	Double	
Description	elevation above/below sea level of the Resource	

Authorization Policy Table

Table 5.7: Authorization Table Structure

Table Description		
Name	auth_policy	
Description	This table creates an association between a User and a Resource. When a User attempts to access a Resource, it is the responsibility of the Resource to query the IdAM System/databases and validate that the User has appropriate privileges to perform the requested action. The IdAM System should ensure— 1) The User and the Resource are associated with one another in the "auth_policy" Table. This association can occur explicitly by having a UserID directly linked to a ResourceID. Alternatively, the association can occur implicitly by validating that a User's Role is associated with a specific Resource. 2) The User belongs to the same domain as the Resource, or the domains are trusted by one another as defined by the "trust Table" 3) The User can perform the requested operation.	
Parameter	**Type**	**Values/Restrictions**
authid	Integer	Primary Key—must be unique
Description	unique identifier for an authorization policy	
userid	Integer	Can be blank if the roleid is populated
Description	User specific to the authorization policy	
roleid	Integer	Can be blank if the userid is populated
Description	Role specific to the authorization policy	
resourceid	Integer	
Description	The Resource with which the User/Role is associated	
operation	Character	Length—255 Character
Description	The privileges the User/Role can perform on the Resource. (e.g., Create, Query, Update, Delete, etc)	

Trust Table

Table 5.8: Trust Table Structure

Table Description		
Name	Trust	
Description	This table creates an association and trust between two domains.	
Parameter	**Type**	**Values/Restrictions**
trustid	Integer	Primary Key—must be unique
Description	unique identifier for the trust	
dn1	Character	Length—50 Characters
Description	First Domain within the Trust	
dn2	Character	Length—50 Characters
Description	Second Domain within the Trust	
relation	Character	Length—50 Characters Values: DN1-trusts-DN2, DN2-trusts-DN1, or SYM-trust
Description	The type of trust between the two domains. It can be a symmetric or an asymmetric relationship. Only the three defined relationships above are possible.	

5.4.8 Business Rules

The NG9-1-1 Business Rules Database contains the policy of the NG9-1-1 System. The Business Rules Database provides the NG9-1-1 System with a series of rule sets that determine how the system routes calls to the appropriate PSAP, and where and if the system can get Supportive or Supplemental data. Figure 5.7 depicts how the Business Rules Database was accessed for the POC.

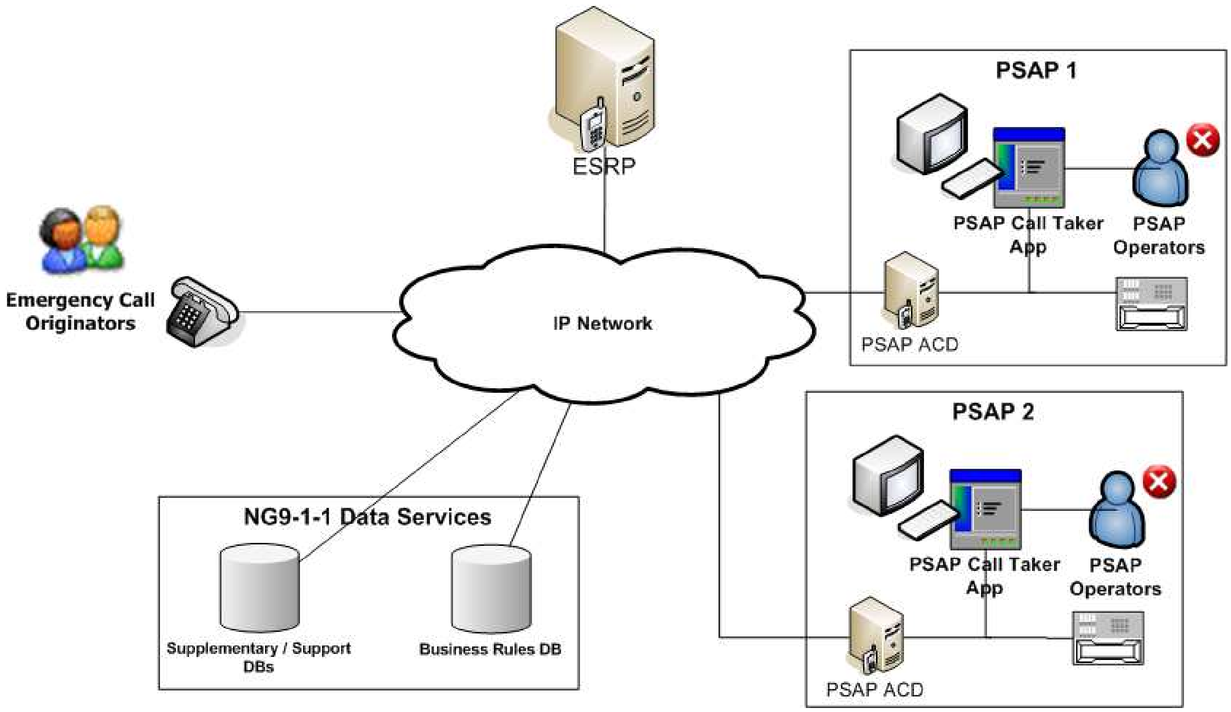

Figure 5.7: Business Rules Database Overview

Various SIP-based Server Devices (SIP Border Gateways, ESRPs, PSAP IP ACDs) access the Business Rule database to make appropriate routing and call handling decisions as well as acquire information on external data sources (supportive and supplemental). When a SIP-based call is routed to a SIP server, the SIP Server extracts various parameters from the call stream, either directly or by reference. These parameters include information such as Call Location, Call Type, Call Source, Call Originator, etc. Based on the extracted parameters the SIP server queries the Business Rules Database to determine whether there are any special routing rules for that specific type of call. In addition, a SIP server can determine whether there are any additional external data sources that should be queried for supportive or supplemental data relating to that call type.

For example, one could imagine a call that was tagged as a telematics call. By querying the Business Rules Database, a SIP server could learn of a separate Crash Database that would allow the SIP server to obtain additional crash information it could use in processing the call.

As another use case, an IP-based call originator might tag his call as a Spanish Call. When the call was received by the PSAP IP ACD, it would query the Business Rules Database to determine which call taker is best suited to receive the Spanish-based voice call.

When examining the Business Rules Database, it becomes apparent that the number of possible business rule permutations is exponentially large. The exact Business Rules (Routing Use cases) for the POC was limited. However, the Business Rules Database is designed in a flexible and modular manner allowing Business Rules to be efficiently and dynamically created and modified. Figure 5.8, depicts the high-level structure of the Business Rules Database.

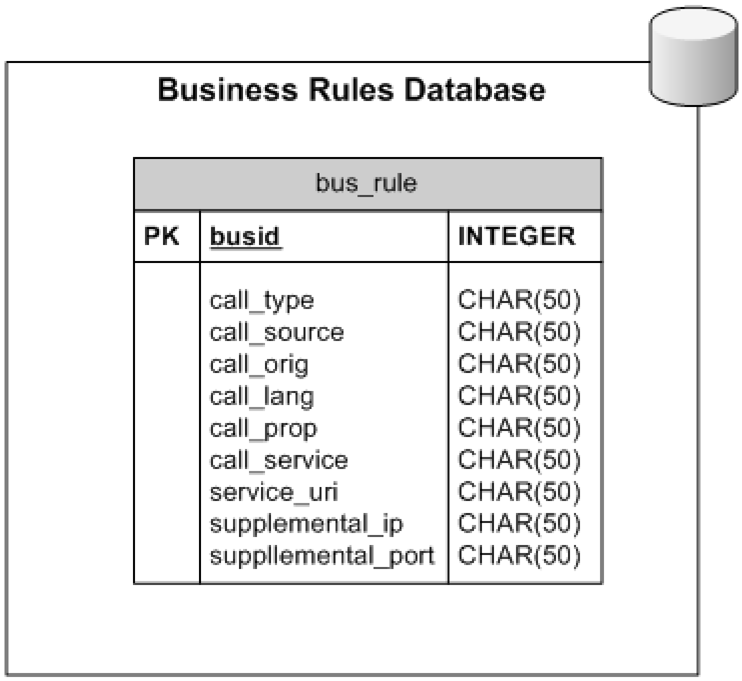

Figure 5.8: Business Rules Database Structure

Table 5-9 depicts the Business Rules Database structure.

Table 5-9: Business Rules Table

Table Description		
Name	bus_rule	
Description	This table stores the Business Rules of the NG9-1-1 Network.	
Parameter	**Type**	**Values/Restrictions**
Busid	Integer	Primary Key—must be unique
Description	unique identifier for an NG9-1-1 Business Rule	
call_type	Character	Length—50 Characters
Description	The type of call entering the NG9-1-1 Network (e.g., IP_Voice, IP_Video, Telematics, POTS, etc.)	
call_source	Character	Length—50 Characters
Description	The vendor or service provider from which the call is originating (e.g., Verizon, OnStar, AT&T)	

call_orig	Integer	Length—50 Characters
Description	The caller's name or identify credentials (e.g., Full Name, SSN, etc). Useful for obtain External Data.	
call_lang	Character	Length—50 Characters
Description	Preferable Language of the Call Originator (e.g., English, Spanish, etc.)	
call_prop	Character	Length—50 Characters
Description	Unique characteristics of the Call Originator (e.g., Deaf, Hard of Hearing, Medical Condition, etc.)	
call_service	Character	Length—50 Characters
Description	Required Service of the Call Originator (e.g., Police, Fire, EMS, etc)	
Service_uri	Character	
Description	SIP URL of the appropriate PSAP or PSAP Call Taker	
External_source_ip	Character	
Description	IP Address of the External Data Repository (e.g., OnStar Crash Test Data, Medical Records, SOPs)	
External_source_ip	Character	
Description	Port of the External Data Repository	

5.4.9 Call Record Database

The Call Record Database stores information and properties associated with an incoming emergency call that enters the NG9-1-1 Network. As a call comes into a NG9-1-1 Network, various software components (Border Controller, ESRP, PSAP ACD, etc.) create and update the associated call record. The call record is included in the Call Record Database for auditing purposes. As the call taker interacts with the call originator and acquires additional information about the emergency, this too is stored to the Call Record Database. Any media (voice, video, data) that are contained within the call stream are also associated with the call record and included in the database. Figure 5.9 depicts the Call Record Database structure.

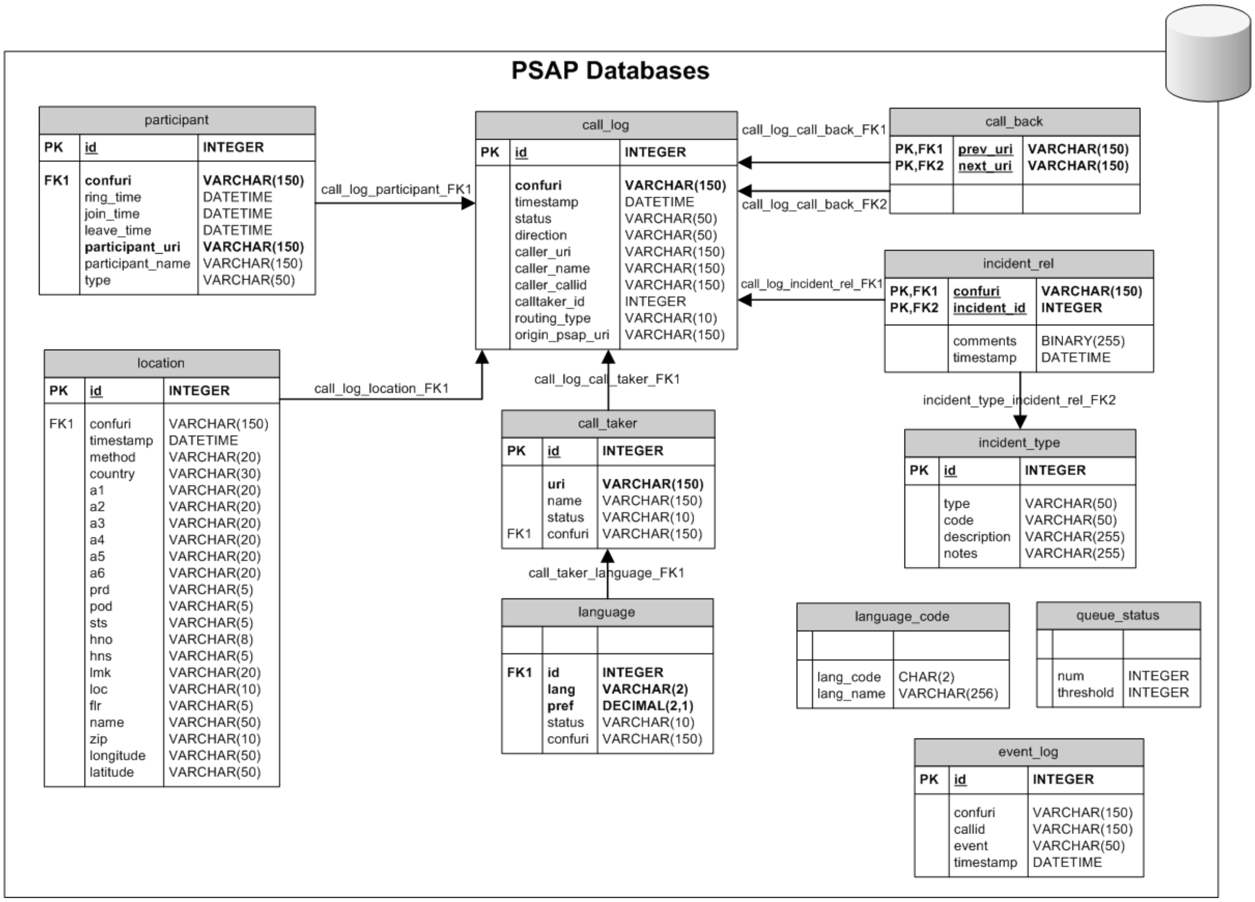

Figure 5.9: Call Record Database

The Call Record Database is one of the primary databases with which an emergency call taker interacts. Given the nature of the work, performance and reliability of this database are essential. For the POC, the Call Record Database was centralized in the NG9-1-1 Network in order to ease data management and acquisition. However, in an operational setting each system owner (Call Origination, 9-1-1 Network, PSAP, etc.) would likely manage and maintain its own Call Record Database. The following tables outline the structure of the call log, language code, participants, location, incident type, incident reference, queue status, and event log tables.

Call Log Table

Table 5.10: Call Log Table Structure

Table Description		
Name	call_log	
Description	This table stores the call record of emergency calls.	
Parameter	**Type**	**Values/Restrictions**
Id	Integer	Primary Key—must be unique

Description	unique identifier	
confuri	Character	Length—256 characters
Description	conference URI of an emergency call. This acts as a unique identifier of emergency calls.	
timestamp	Timestamp	
Description	initial timestamp when a call comes in	
status	Enum	init, active, closed, failed, canceled, queued
Description	current status of an emergency call	
direction	Enum	in, out
Description	indicator whether a call is inbound or outbound (call back)	
caller_uri	Character	Length—256 characters
Description	caller's SIP URL	
caller_name	Character	Length—256 characters
Description	caller's name	
caller_callid	Character	Length—256 characters
Description	Call-ID of a call from a caller	
calltaker_id	Integer	Foreign key referring 'id' in call taker
Description	ID of the call taker who picks up	
routing_type	Enum	normal, overflow, failover
Description	reason of routing	
origin_psap_uri	Character	Length—256 characters
Description	the URL of the original PSAP from which this call is transferred	

Call Taker Table

Table 5.11: Call Taker Table Structure

Table Description		
Name	call_taker	
Description	This table stores the information of each call taker in a PSAP.	
Parameter	**Type**	**Values/Restrictions**
Id	Integer	Primary Key—must be unique
Description	unique identifier	
Uri	Character	Length—256 characters
Description	call taker's SIP URL	

name	Character	Length—256 characters
Description	call taker's name	
status	Enum	available, busy, offline
Description	call taker's status	
confuri	Character	Length—256 characters
Description	conference URL of the emergency call in which the call taker currently participates	

Language Table

Table 5.12: Language Table Structure

Table Description		
Name	Language	
Description	This table maps a call taker and language preference.	
Parameter	**Type**	**Values/Restrictions**
Id	Integer	Foreign key referring 'id' in call taker
Description	call taker's ID	
lang	Character	Length—2 characters
Description	ISO 639 2-letter language code	
pref	Decimal	0.0—1.0
Description	call taker's preference value of a certain language	

Language Code Table

Table 5.13: Language Code Table Structure

Table Description		
Name	language_code	
Description	This table maps a 2-letter language code and a display name.	
Parameter	**Type**	**Values/Restrictions**
lang_code	Integer	Foreign key referring 'id' in call taker
Description	ISO 639 2-letter language code	
lang_name	Character	Length—256 characters
Description	display name of a language	

Participant Table

Table 5.14: Participant Table Structure

Table Description	
Name	Participant

Description	This table logs participants in an emergency call.	
Parameter	**Type**	**Values/Restrictions**
Id	Integer	Primary Key—must be unique
Description	unique identifier	
confuri	Character	Foreign key referring confuri in call_log
Description	identifier of the emergency call in which this participant is participating	
Ring_time	Timestamp	
Description	timestamp when a participant receives a ring signal	
Join_time	Timestamp	
Description	timestamp when a participant joins an emergency call	
leave_time	Timestamp	
Description	timestamp when a participant hangs up	
participant_uri	Character	Length—25 characters
Description	participant's SIP URL	
participant_name	Character	Length—25 characters
Description	participant's name	
Type	Enum	caller, calltaker, 3rd_party
Description	participant's type	

Location Table

Table 5.15: Location Table Structure

Table Description		
Name	Location	
Description	This table stores location information of a caller.	
Parameter	**Type**	**Values/Restrictions**
Id	Integer	Primary Key—must be unique
Description	unique identifier	
Confuri	Character	Foreign Key referring confuri in call_log
Description	identifier of the emergency call to which location information pertains	
timestamp	Timestamp	
Description	timestamp when location information is received	
method	Character	Length—50 characters
Description	the way that the location information was derived or discovered	

country	Character	Length—2 characters
Description	two-letter ISO 3166 country code	
a1	Character	Length—50 characters
Description	national subdivisions (state, region, province, prefecture)	
a2	Character	Length—50 characters
Description	county, parish, district (IN)	
a3	Character	Length—50 characters
Description	city, township	
a4	Character	Length—50 characters
Description	city division, borough, city district, ward, etc.	
a5	Character	Length—50 characters
Description	neighborhood, block	
a6	Character	Length—50 characters
Description	Street	
prd	Character	Length—10 characters
Description	leading street direction	
pod	Character	Length—10 characters
Description	trailing street suffix	
Sts	Character	Length—10 characters
Description	street suffix	
hno	Character	Length—10 characters
Description	house number (numeric part only)	
hns	Character	Length—10 characters
Description	house number suffix	
lmk	Character	Length—50 characters
Description	landmark or vanity address	
Loc	Character	Length—10 characters
Description	additional location information	
Flr	Character	Length—10 characters
Description	Floor	
nam	Character	Length—50 characters
Description	name (residence, business or office occupant)	
zip	Character	Length—10 characters
Description	postal code	

longitude	Character	Length—50 characters
Description	Longitude	
latitude	Character	Length—50 characters
Description	Latitude	

Call-Back Table

Table 5.16: Call-Back Table Structure

Table Description		
Name	call_back	
Description	This table maps an original emergency call and a callback call.	
Parameter	Type	Values/Restrictions
prev_uri	Character	Foreign key referring confuri in call_log
Description	identifier of an original emergency call	
next_uri	Character	Foreign key referring confuri in call_log
Description	identifier of a call back call	

Incident Type Table

Table 5.17: Incident Type Table Structure

Table Description		
Name	incident_type	
Description	This table stores the predefined incident information.	
Parameter	**Type**	**Values/Restrictions**
Id	Integer	Primary Key—must be unique
Description	unique identifier	
Type	Character	Length—50 characters
Description	incident type	
Code	Character	Length—50 characters
Description	incident code	
description	Character	Length—256 characters
Description	incident description	
Note	Character	Length—256 characters
Description	additional information	

Incident Reference Table

Table 5-18: Incident Reference Table Structure

Table Description		
Name	incident_reference	
Description	This table maps an emergency call and incident information.	
Parameter	**Type**	**Values/Restrictions**
Confuri	Character	Foreign key referring confuri in call_log
Description	identifier of an emergency call to which an incident reference belongs	
incident_id	Integer	Foreign key referring id in incident
Description	incident type	
Comments	Blob	
Description	additional information	
Timestamp	Timestamp	
Description	timestamp when an incident reference is created	

Queue Status Table

Table 5.19: Queue Status Table Structure

Table Description		
Name	queue_status	
Description	This table stores the call queue information.	
Parameter	**Type**	**Values/Restrictions**
Num	Integer	
Description	the number of calls in the call queue	
Threshold	Integer	
Description	the maximum number of calls that can reside in the call queue	

Event Log Table

Table 5.20: Event Log Table Structure

Table Description		
Name	event_log	
Description	This table logs major events in psapd for debugging purposes.	
Parameter	**Type**	**Values/Restrictions**
Id	Integer	Foreign key referring confuri in call_log
Description	unique identifier	

confuri	Character	Foreign key referring confuri in call_log
Description	identifier of an emergency call to which the event belongs	
callid	Character	Length—256 characters
Description	Call-ID of the call leg that initiates the event	
event	Character	Length—50 characters
Description	event code	
timestamp	Timestamp	
Description	timestamp when the event occurred	

6 NG9-1-1 PSAP POC SYSTEM DESIGN

The primary role of the NG9-1-1 PSAP in the POC was to receive simulated 9-1-1 calls generated from a variety of call origination devices.

6.1 Design Definition and Perspective

The NG9-1-1 PSAP housed infrastructure to terminate the simulated emergency calls. PSAP call takers were trained to receive calls with PSAP Call Taker Software loaded on an IP-enabled laptop. The NG9-1-1 Network delivered the call through the system to the appropriate PSAP Call Taker Workstation. For the POC, the IP ACD function was provided by software (psapd) developed by Columbia University. From the NG9-1-1 PSAP, there was reachback connectivity to the NG9-1-1 Network, other PSAPs, and supportive data sources such as GISs.

For the POC, the NG9-1-1 PSAP POC design focused on the following areas:

- The ability to capture IP-based call record information to record IP call statistics.
- The enablement of IP voice, video and data at a call taker's workstation.
- The ability to deliver GIS map data to the call taker screen.

6.2 Design Constraints and Considerations

The NG9-1-1 PSAP test equipment was deployed at several live PSAPs which provide 9-1-1 emergency services within their state or county. A key constraint was to ensure that the PSAPs' existing services were not disrupted while conducting the POC tests. Therefore, POC equipment deployed at the PSAPs was isolated from the production environment. Some call takers at the PSAPs participating in the POC demonstration were trained to receive simulated 9-1-1 calls using the POC test equipment. A dedicated T1 circuit was deployed to support the POC test traffic.

6.3 POC NG9-1-1 PSAP Design and Specifications

The NG9-1-1 PSAP included the following infrastructure:

- T1 circuit
- Edge router
- Firewall
- Switch
- IP ACD
- IP Call Taker Workstation

Figure 6.1 depicts the design of the POC NG9-1-1 PSAP.

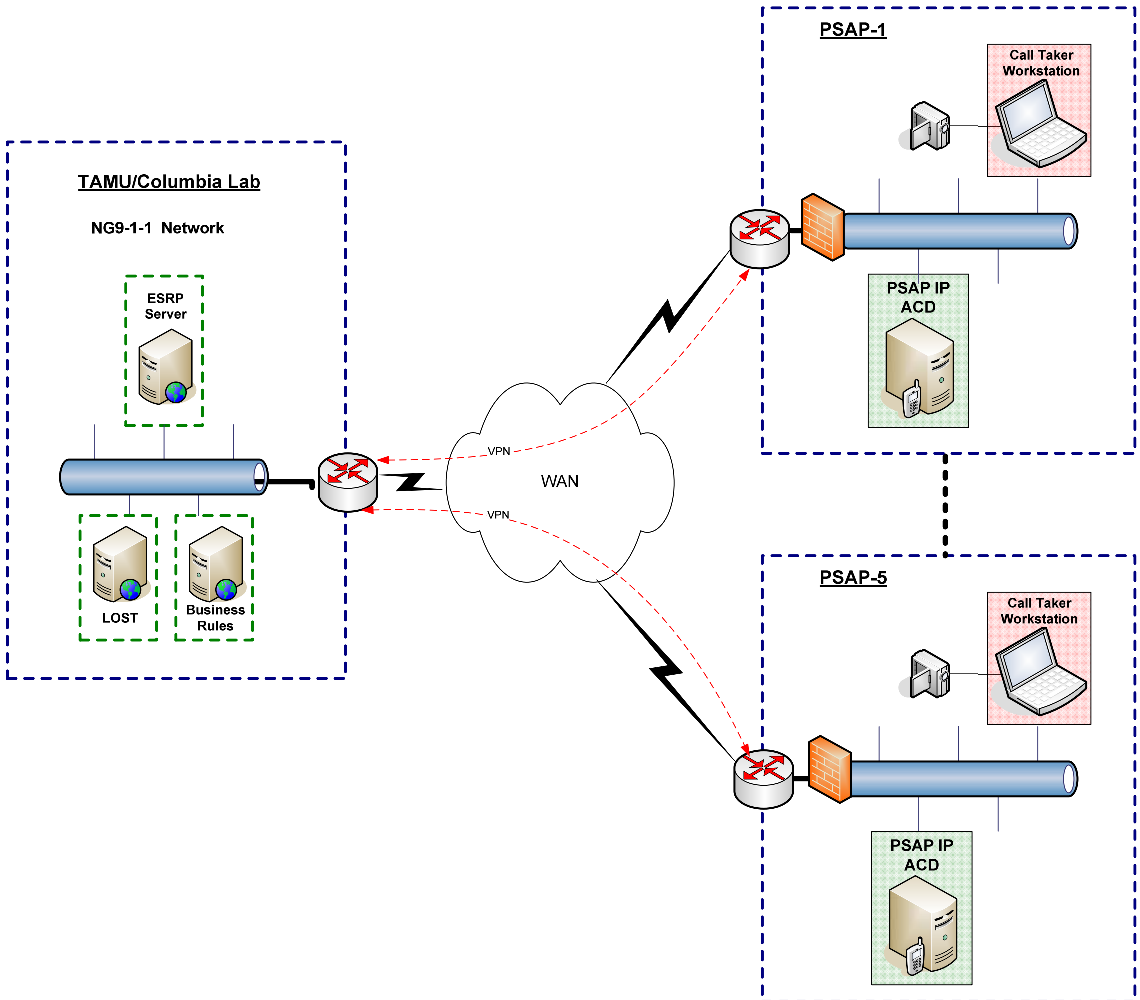

Figure 6.1: PSAP Design

As shown, each PSAP had a dedicated WAN edge router and a leased T1 circuit. The T1 circuit was connected to a network service provider's IP WAN to simulate the NG9-1-1 network. The equipment within the PSAP was connected to a standard LAN switch. Each PSAP had its own IP address block. Calls terminated on the call taker workstation.

IP call acceptance and distribution to a call taker workstation was an important functional requirement for the POC demonstration. The IP ACD function enabled call routes to be dynamically assigned based on a variety of factors. The IP ACD was able to intelligently route an incoming call to a Call Taker Workstation based the availability of the call taker, the capabilities of the call taker, and the capabilities of the workstation. The IP ACD function for the POC was demonstrated using the "psapd" software tool developed by Columbia University.

Call termination equipment is the most important piece of the system for a call taker. The call taker will use this equipment to perform the critical functions of receiving, processing, and dispatching an emergency call for service from the public. This equipment must be user friendly and require a limited number of actions on the part of the call taker.

The POC call termination equipment consisted of a computer workstation with the SIPcalltaker software developed by Columbia University. The Human Machine Interface (HMI) Design Document developed under Task 3b includes specifications for the HMI that was developed.

7 POC NETWORK MANAGEMENT SYSTEM DESIGN

As with any IP based network implementation, a Network Management System (NMS) was installed and configured to monitor, maintain, and troubleshoot system-wide issues. During the POC demonstration, a network management tool was use to monitor network and applications infrastructure deployed within the POC test-bed. The tool was also used to capture performance statistics from applications and the network segments. Another function of the NMS was to provide proactive monitoring and health check of all devices deployed within the POC environment. Furthermore, the NMS tool assisted in capturing test results while executing POC test scripts.

7.1 Design Definition and Perspective

During the POC, the NMS tool was used to provide proactive monitoring of all network and applications infrastructure deployed within the test-bed environment. This included the monitoring of firewalls, switches, routers, and servers. Statistics such as availability, uptime, and utilization was monitored during all POC demonstrations. Simple Network Management Protocol (SNMP) was used to set up traps and download statistics from all devices. SNMP is an application layer protocol that facilitates the exchange of management information between network devices. The NMS tool served three primary roles during the POC—Performance Management, Fault Management, and Security Management. Performance Management measured various aspects of network so that overall system performance could be maintained at an acceptable level. The function of Fault Management was to detect, log, and notify system administrators of any technical issues that might cause network or system failure. Finally, Security Management controlled access to the network and applications infrastructure in order to minimize unauthorized configuration changes.

7.2 Design Constraints and Considerations

A variety of NMS tools are currently available, however cost was a major constraint. For the POC demonstration, an inexpensive NMS tool was selected. The selected tool did not have the enhanced features of some of the production grade NMS tools; however, it was deemed sufficient for the POC. In addition, several open source based hardware and software products were deployed in the POC environment. Some of these products did not have adequate plug-ins to support SNMP, therefore SNMP performance statistics were not collected for those components.

7.3 Network Management System Design

The NMS tool selected for the POC was HP Network Node Manager (NNM) software. Figure 7.1 depicts a high-level diagram of how the tool was deployed and used to monitor network and applications infrastructure during the POC.

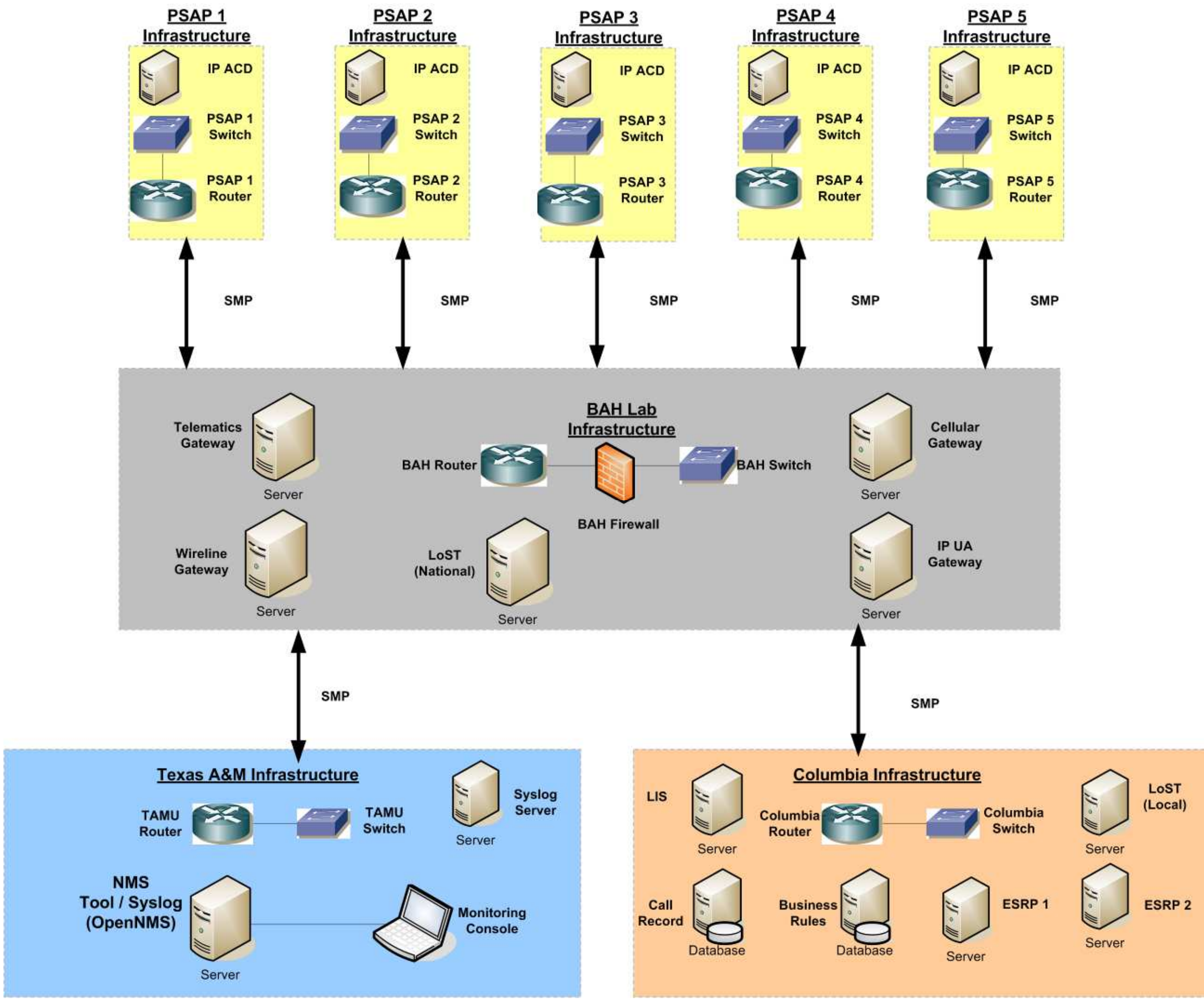

Figure 7.1: POC NMS Design

As shown in Figure 7.1, HP NNM software was deployed on a server, and SNMP traps were configured on network and applications devices. The NMS tool pulled SNMP MIB statistics from servers, routers, switches, and firewalls, and display them using a graphical user interface (GUI). Customized reports depicting availability, performance (latency, jitter, and packet loss), and utilization was generated and analyzed.

The HP NNM software had several features that were leveraged during the POC. These include—

- Ability to capture trace information and summarize it
- Intuitive drill-down reports for thread analysis
- "Thread Analysis" and "Conversation Bounce" to identify the timing and sequence of each packet traversing the network.

In addition, a Syslog server was used to store logs from network and applications infrastructure. During the POC demonstration, logs were stored and analyzed.

8 NG9-1-1 System Design Considerations

Throughout the NG9-1-1 Initiative, determinations and decisions about the functionality, features and architecture have been made based on input by the project team, SMEs and other interested parties. These decisions helped shaped the CONOPS, requirements and system architecture and led to the POC system design. Looking forward to actual implementations of NG9-1-1, the choices made in the system design and the reasons for those choices will assist individuals and entities as they implement these next generation solutions. The most pressing and influential issues are outlined in this section.

Standardization on SIP

As previously described, the POC used SIP as the "signaling protocol for call establishment, routing, and termination." Although signaling protocols such as IMS, SS7, and H.323 are available, SIP was chosen for a number of important reasons. SIP enjoys a wide industry acceptance, readily-available support and open source status. Additionally, the project team had direct access to one of the primary developers of SIP, as well as the participation of leading SIP developers through the project's academic partnerships.

The flexibility of the SIP standard to support a variety of multimedia communications sessions is consistent with the needs of NG9-1-1 to deliver multimedia-based calls over IP networks. The POC successfully demonstrated the use of SIP to deliver voice, video conferencing, instant messaging and real-time texting, as well as provide essential, supportive and supplemental data.

SIP was selected for its ability to invite participants to already existing sessions, such as multicast conferences. One of the NG9-1-1 requirements is to automatically enable conferencing for a variety of situations, including the need for language interpreting services. Similarly, SIP supports the ability to add (and remove) media from existing sessions. As demonstrated during the POC, although a voice channel was established, SIP provided the ability to add transport of text, video and other data, simultaneously with the audio channel. The resulting call was media-rich and offered multiple sources of data input for the calltaker.

Use of Reference Links

Generally with NG9-1-1, there is a desire to include a significant amount of data associated with the call, at all stages of the call session. However, there are real concerns about exceeding limits on message length, and the message header, in particular. Specifically, one benefit of limiting the message size would be to avoid fragmenting packets (which could lead to packet loss, as well as some denial-of-service attacks have been attributed to fragmented packets).

The use of location by reference[1] and other reference link methods have permitted the use of data much larger then the maximum field or header length allowed. In this manner, links or pointers can be included in the standard message fields, by using a Uniform Resource Identifier (URI) that points to (indicates) another service or database. Although the message does not contain the complete set of data, it does provide an indication that information exists and the definitive source for obtaining the data.

This method of providing a link to the necessary information helps solve potential technical issues and introduces the opportunity to enhance security protection of that data. Varying levels of access to subsets of the data are necessary throughout the lifespan of a NG9-1-1 call. For example, a call taker must have immediate access to the caller's location, but may not need access to next-of-kin information associated with a medical alarm activation. However, the dispatchers and emergency responders may need that contact information to gain access to the home of someone experiencing a medical emergency. In this manner, the call stream message would indicate the availability of this contact information and business rules would specify which users or entities are authorized to access the data in question. This would support preservation of proper data access, in accordance with the myriad of privacy and data protection laws and regulations (e.g., Privacy Act of 1974[2], HIPAA[3], et al.) currently in place.

Use of Hierarchical LoST Server Architecture

One of the key features of the LoST protocol[4] architecture is its ability to be implemented in a "distributed, scalable and highly resilient infrastructure." As the draft paper on the subject further describes that "authoritative knowledge" about mapping locations to services is "distributed among a large number of autonomous entities that may have no direct knowledge of each other."[5] As part of the POC effort,

---

[1] For more information about the Location by Reference Requirements, visit the IETF's GEOPRIV Working Group for their current draft: http://www.ietf.org/internet-drafts/draft-ietf-geopriv-lbyr-requirements-05.txt (last accessed January 19, 2008).
[2] The Privacy Act of 1974, 5 U.S.C. § 552a, available at: http://www.law.cornell.edu/uscode/5/552a.html (last accessed January 19, 2008).
[3] For more information on the security restrictions associated with Health Insurance Portability and Accountability Act (HIPAA), see: http://en.wikipedia.org/wiki/Hipaa#The_Security_Rule (last accessed January 19, 2008).
[4] IETF ECRIT Working Group, *LoST: A Location-to-Service Translation Protocol* [RFC5222], available at: http://tools.ietf.org/html/rfc5222 (last accessed January 19, 2008).
[5] IETF ECRIT Working Group, *Location-to-URL Mapping Architecture and Framework,* available at: http://tools.ietf.org/html/draft-ietf-ecrit-mapping-arch-03 (last accessed January 19, 2008).

the Emergency Services Routing Proxies (ESRP) that hosted the LoST servers were configured in a hierarchical and distributed manner. A similar configuration is very likely as part of NG9-1-1 implementation, as it provides the maximum operational flexibility and control for 9-1-1 Authorities.

The POC demonstrated the ability to have large regionalized LoST servers (e.g., Western U.S. and Eastern U.S.) that connected to statewide, regional or local LoST servers. Deploying LoST for NG9-1-1 can be accomplished in a similar manner, with several options. Some organizations may wish to deploy their own local or regional LoST servers (a bottoms-up approach), which eventually lead to nationwide coverage. Another option would be for some large, authoritative systems to implement LoST at a nationwide, multi-state or large regional area, allowing further coverage to grow over time. Most likely, there will be a hybrid of approaches, initially creating a patchwork of coverage.

Overall Security Concerns

Security of the NG9-1-1 system as a whole is of paramount importance and typically one of the leading concerns raised by stakeholders. With today's 9-1-1 system primarily consisting of legacy technology and closed networks, security risks are mostly known and manageable. However, in an IP-based system, more widely connected across multiple networks and systems, the opportunity for a compromise to occur is increased significantly. Although there are more chances, the situation remains manageable, through the use of best current practices within the IT and public safety community.

IT-based systems require a solid security foundation that is multifaceted and implemented at multiple levels. For mission-critical applications, such as NG9-1-1, the importance of restricting access to only authorized users becomes even more crucial. High levels of protection are not new to IP-based enterprise networks and systems, such as those used in national defense, intelligence, and banking communities. Lessons-learned and best practices within those environments should be leveraged for NG9-1-1 to develop a comprehensive security solution. As described in Section 5.4.7 of this document, through use of an IdAM methodology, NG9-1-1 can manage identity, authentication, and authorization for users and administrators of the NG9-1-1 system.

<u>POC Use of VPN/GRE Tunnels</u>

When implementing the POC network, it was necessary to create connectivity between multiple POC PSAPs and testing laboratories. This was accomplished using secure GRE tunnels over Internet2 and a mix of AT&T's Commodity Internet and MPLS network. This configuration allowed for creation of a virtual point-to-point link between multiple, geographically-dispersed entities. Although this was a viable option for the POC, it may or may not be appropriate for universal adoption for NG9-1-1. Some organizations may need to follow local customs with regard to IT networking configuration which may differ from this method. A NENA Technical Committee Working Group is focused on NG9-1-1 security concerns; their published findings should be a point of reference when implementing an NG9-1-1 network.

It has been noted that further research and testing are needed to identify the impact of various security measures on overall system and network performance. One of the findings of the POC testing was that some firewall settings had caused the network to have unanticipated delays and testing could not be completed with this configuration. Throughput, particularly when streaming multimedia, had decreased to an unusable point. While disabling those features improved response time so testing could be completed, it decreased the overall desired levels of protection.

COTS Hardware and Software

COTS typically refers to technology that is commonly and commercially available and does not require specialized support throughout its lifecycle. In the context of the NG9-1-1 POC, the use of COTS hardware and software was done to avoid any indication of preference for a single vendor. Additionally, it demonstrated that stakeholders are able to employ components developed by vendors for which they have a particular comfort level or experience with, without losing features or functionality. Legacy 9-1-1 components historically have been proprietary and not COTS, due to the relative small size of the 9-1-1 marketplace and the perceived need for specialized equipment to operate those systems.

Some benefits of using COTS include a cost savings and more widespread understanding of the technical limitations and issues associated with a commercially-available product. Operations and maintenance of COTS hardware is frequently easier and less expensive as replacement parts are usually more readily available.

The use of COTS, wherever possible and appropriate, is encouraged for NG9-1-1 to reduce cost and risk and increase usability and ease of maintenance.

Inclusion of SMS Technology

The POC included testing and demonstration of SMS text messages as a method of call origination, out of the belief that citizens desire the ability to send text messages to 9-1-1 and are surprised to learn that it is not a feature of today's 9-1-1 system. While some individuals in the emergency communications field believe that SMS has its merits and should be supported in NG9-1-1, many others feel that it is an "inferior technology" for emergency calling, primarily due to its fundamental inability to support identification of callers' location information. Although the POC created an "SMS Positioning Center" system to support SMS location acquisition, there are no commercial systems available that identify SMS sender's location. There would need to be significant changes made to the technology and devices to support location acquisition and delivery. Other problems with SMS exist as well, as it does not provide the call taker with an easy method of caller interrogation and because SMS technology was never designed to guarantee message delivery or receipt.

From an operational perspective, the POC environment only permitted a single text-based conversation at one time. For example, it is expected that in NG9-1-1, call takers will need to interact with multiple, simultaneous SMS messages (from different callers). For the call taker, this introduces risks associated with talking to multiple callers all at the same time, something that is not typically done in today's 9-1-1. Limiting the call taker to respond to a single SMS at a time may strain the limited resources of a typical PSAP. NENA has a working group addressing these operational issues, but more research must be performed to reduce risk and decrease the chance of introducing a potentially serious system design flaw.

While the technology was successfully demonstrated, there may be better technologic options for both emergency callers and call takers over that of SMS. For example, development or modification of a real-time texting (similar to instant message or chat) application could support delivery of caller's location, improve the ability for the call taker to quickly obtain additional critical information during their interrogation, and eliminate the 140 character limitation of SMS. Real-time texting was also successfully demonstrated in the POC.

Streaming Video for Emergency Calling

Demonstration of technologies to support the deaf and hard-of-hearing community was one of the primary project requirements. Included as one of three operational scenarios in the *NG9-1-1 Concept of Operations* document,[6] the ability to transmit and receive video streams as part of a call, was determined to be one way to use technology to assist the needs of this community. Included as part of the POC, benefits and challenges to integrating this technology in the emergency calling environment were identified.

Emerging technology (in the form of handheld wireless devices with a screen and camera) has started to make portable streaming video possible. Although the POC focused on fixed, PC-based web cameras to demonstrate this functionality, wireless concepts were successfully tested. For the POC, open source technology was selected

[6] USDOT ITS JPO, *Next Generation 9-1-1 (NG9-1-1) System Initiative: Concept of Operations*, April 2007, available at http://www.its.dot.gov/ng911/pdf/NG911ConOps_April07.pdf (last accessed January 19, 2009).

(in keeping with the project's design parameters) and due to various limitations of the technology, mixed results were found. The conferencing server used to support streaming video distribution did not support multiple parties (although there are commercial products available that support this capability, but not in a wireless environment). Multiple party conferencing is needed so that a deaf or hard-of-hearing caller, a sign language interpreter, and an emergency call taker can all communicate in concert to obtain the necessary information quickly and efficiently.

Due to the current limitations of cellular carriers' networks, transmitting compressed video, with the quality needed to deliver an intelligible sign language conversation, is not readily available in the United States. Research into new encoding techniques is currently underway,[7] and with improvements in the cellular networks, may provide the ability to transmit video to the PSAP.

Selection of Databases for POC Testing

A number of databases were included in the POC testing and demonstrations: MPC, LoST, LIS, business rules and call record detail. Others (MSAG, SRDB, EPAD, and IdAM / Data Rights Management) while important to today's 9-1-1 and NG9-1-1, were omitted from the plan for the POC. The MSAG and SRDB are critical to the daily operations of today's 9-1-1 systems and the legacy technology does not pose any current need for review or research. The POC did use valid MSAG data from the participating PSAPs in the development of other databases (LoST, LIS, and ALI / MPC). The ESRP will replace the functionality of the SRDB in future 9-1-1 systems and was not included.

Initial work was done as part of the project to identify requirements for a Business Rules database, however, much work remains. In particular, there are two types of business rules:

- Policy-based rules, used when handling or processing a call (can affect routing)
- Configuration of software and/or components within the NG9-1-1 system (affects how a call taker interacts with a call)

Due to the importance of this database, both NENA's Technical and Operational committees are already working to establish business rules for the transition to NG9-1-1. It will be necessary to identify a concept of operations and additional detailed requirements to have a better understanding of the types of data that will be managed by a Business Rules database.

The IdAM and Data Rights Management databases are key to overall system security, however implementing such a system was beyond the available means of the project,

[7] MobileASL is a research project at the University of Washington, seeking to enable sign language conversations on cell phones. More information is available at: http://mobileasl.cs.washington.edu/ (last accessed January 19, 2009).

within the time and resources provided. More study into the requirements of these security-related databases is needed by the stakeholder community. As the POC focused on the call origination, delivery and termination at a PSAP, hand-off to a dispatch organization was determined to be outside the scope of the project as well. Use of the EPAD database will be important in determining which emergency responder would be responsible for handing the incident in the NG9-1-1 system.

User Interface

The HMI was designed specifically for the POC and while usable in a test environment, it was never intended for live, operational use. The nature of the POC testing required multiple features in the HMI, including: CPE, ACD, and the ability to record caller detail information. In NG9-1-1, this functionality may be provided by a single system or multiple, tightly-integrated systems. Some data displayed to the call taker was done to aid the testing and demonstration process and would not normally be displayed to the end user. For example, in demonstration of the telematics scenario, all 130+ data elements associated with the crash notification were displayed. In NG9-1-1, it is expected that only the 5-6 most important criteria would be shown to assist the call taker in making a response decision, based on the likelihood and severity of injury. Further, some systems may not show any of the detailed telematics data to the user and only display an indication of the severity, based on processing of the data through an algorithm.[8]

Additional research into the content, format and layout of the HMI will be necessary by vendors seeking to market their products, to ensure usability for call takers. Previous work done for the NG9-1-1 Initiative[9] may assist in the development of future user interfaces.

Telematics Service Provider Integration

The project team worked closely with a major telematics service provider (TSP) throughout the project, as they were key stakeholders who provided technical and operational information and responded to requests for feedback and input. Integration of a telematics call was an important requirement for the POC and some work by the

[8] The **Urgency Algorithm** was developed to predict the probability of serious injuries, resulting from a vehicle crash. More information is available at: http://www.comcare.org/urgency.html (last accessed January 19, 2009).

[9] There are two project documents that specifically describe research into the call taker's HMI, including: *NG9-1-1 Call Taker Human Factors Issues Report,* November 2007. Available through the ITS JPO; and *NG9-1-1 Human Machine Interface Display Design Document,* January 2008. Available at: http://www.its.dot.gov/ng911/pdf/NG911_HMI_Display_Design_FINAL_v1.0.pdf (last accessed January 19, 2009).

TSP had already been underway prior to the POC. The TSP was leveraging previous work done to create the Vehicular Emergency Data Set (VEDS)[10] standard and the POC was able to successful integrate and demonstrate "calls" originating from the TSP's laboratory.

Although important to demonstrate on its own merits, the knowledge gained testing the telematics scenario is directly applicable to development, integration and testing of non-human-initiated automatic event alerts, such as alarms or sensors. For example, the Association of Public-Safety Communications Officials (APCO) International has helped to develop a standard data exchange method to transmit data between alarm monitoring companies and PSAPs.[11] The NG9-1-1 system will support this approved standard and the process should be integrated into the requirements for NG9-1-1.

[10] VEDS is an XML-based standard, used to transmit telematics data to PSAPs. More information is available at: http://www.comcare.org/veds.html (last accessed January 19, 2009).

[11] *Alarm Monitoring Company to Public Safety Answering Point (PSAP) Computer-aided Dispatch (CAD) External Alarm Interface Exchange*. More information is available at: http://www.apcointl.org/new/commcenter911/documents/APCO-CSAA-ANS2-101-1web.pdf (last accessed January 19, 2009).

Appendix A—Acronyms

Acronym	Definition
ACD	Automatic Call Distribution
ACN	Automatic Crash Notification
ALI	Automatic Location Identification
ATM	Asynchronous Transfer Mode
BCF	Border Control Function
CDR	Critical Design Review
CONOPS	Concept of Operations
COTS	Commercial Off-the-Shelf
CNSI	Booz Allen Center for Network & Systems Innovation at One Dulles (Herndon, VA)
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ENOC	Enterprise Network Operations Center
EPAD	Emergency Provider Access Directory
ERDB	Emergency Service Zone (ESZ) Routing Database
ESN	Emergency Service Number
ESRP	Emergency Services Routing Proxy
ESZ	Emergency Service Zone
FXO	Foreign Exchange Office
FXS	Foreign Exchange Subscriber
GIS	Geographic Information System
GML	Geography Markup Language
GPS	Global Positioning System
GRE	Generic Route Encapsulation
GUI	Graphical User Interface
HMI	Human Machine Interface
HTTP(S)	Hypertext Transfer Protocol (Secure)
IdAM	Identity Management
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IOS	Internet Operating System
IP	Internet Protocol
IPSec	Internet Protocol Secure
LAN	Local Area Network
LIS	Location Information Server
LLDP-MED	Link Layer Discovery Protocol-Media Endpoint Discovery
LoST	Location-to-Service Translation Protocol

Acronym	Definition
MIB	Management Information Base
MPC	Mobile Positioning Center
MPLS	Multiprotocol Label Switching
MRV	Multi-Dimensional Requirements View
MSAG	Master Street Address Guide
MSC	Mobile Switching Center
NAT	Network Address Translation
NENA	National Emergency Number Association
NG9-1-1	Next Generation 9-1-1
NNM	HP's Network Node Manager software
NMS	Network Management System
OSI	Open System Interconnect
PBX	Private Branch Exchange
PDA	Personal Digital Assistant
PDR	Preliminary Design Review
PIDF-LO	Presence Information Data Format–Location
POC	Proof-of-Concept
POTS	Plain Old Telephone System
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
R&D	Research and Development
SBC	Session Border Controller
SDD	System Design Document
SIP	Session Initiation Protocol
SIPc	Session Initiation Protocol client
SIPd	Session Initiation Protocol daemon
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SRDB	Selective Router Database
SS7	Signaling System 7
SSO	Single Sign On
TAMU	Texas A&M University
TCAP	Technical Capabilities Application Part
TCP	Transmission Control Protocol
TIA	Telecommunications Industry Association
UA	User Agent
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
USDOT	U.S. Department of Transportation

Acronym	Definition
VoIP	Voice over IP
VPC	VoIP Position Center
VPN	Virtual Private Network
VRS	Video Relay System
WAN	Wide Area Network
XML	Extensible Markup Language

Appendix B—Glossary

System definitions are consistent with those published by NENA in its Master Glossary of 9-1-1 Terminology (NENA 00-001—Version 10, dated June 5, 2007), which was used as a source document.

9-1-1	A three-digit telephone number to facilitate the reporting of an emergency requiring response by a public safety agency.
9-1-1 System	The set of network, database, and customer premises equipment (CPE) components required to provide 9-1-1 service.
Analog	Continuous and variable electrical waves that represent an infinite number of values; as opposed digital.
Authentication	Determination or verification of a user's identity and/or the user's eligibility to access to a system, network, or data; measures to prevent unauthorized access to information and resources.
Automatic Call Distributor (ACD)	Equipment or application that automatically distributes incoming calls to available PSAP call takers in the order the calls are received, or queues calls until a call taker becomes available.
Automatic Crash Notification (ACN)	The process of identifying that a motor vehicle has been involved in a collision, collecting data from sensors in the vehicle, and communicating that data to a PSAP.
Automatic Event Alert	9-1-1 calls placed by sensors or similar initiating devise. Includes alarms, telematics, and sensor data, and may also include real-time communications.
Automatic Location Identification (ALI)	The automatic display at the PSAP of the caller's telephone number, the address or location of the telephone, and supplementary emergency services information.
Automatic Location Identification (ALI) Database	The set of ALI records residing on a computer system.
Automatic Number Identification (ANI)	Telephone number associated with the access line from which a call originates.
Availability	The operational ability of necessary and beneficial data interfaces to support call processing and emergency response; or the amount or percentage of time that the system provides service.
Backup Public Safety Access Point (Backup PSAP)	Typically, a disaster recovery answering point that serves as a backup to the primary PSAP and is not collocated with the primary PSAP.

Border Control Function (BCF)
BCF activities create a boundary between the internal network resources and the external network(s). Access to particular network resources behind a BCF-enabled gateway, can be restricted by a variety of methods. Most BCFs offer a level of Network Address Translation (NAT) and provide firewall-like functions. The deployment of BCFs at the edge of the network can secure and protect the system from outside resources by creating a Demilitarized Zone (DMZ) that protects the internal network resources from the outside network. The DMZ allows access only to the trusted parties that authenticate to the network. BCFs can also offer network-to-network interface functions for allowing traffic to be delivered across the network and Session Initiation Protocol (SIP) session border control functionality.

Call
For the purposes of this NG9-1-1 Architecture Analysis Report, any real-time communication—voice, text, or video—between a person needing assistance and a PSAP call taker. This term also includes non-human-initiated automatic event alerts, such as alarms, telematics, or sensor data, which may also include real-time communications.

Callback
The ability to re-contact the calling party.

Call Delivery
The capability to route a 9-1-1 call to the designated selective router for ultimate delivery to the designated PSAP for the caller's ANI/KEY.

Call Detail Record
All system (including network) data accessible with the delivery of the call, and all data automatically added as part of call processing. This includes Essential Data (including reference key to network component and call progress records) and Supportive Data. Part of the Call Record.

Caller Location Information
Data pertaining to the geospatial location of the caller, regardless of whether the caller is a person or an automatic event alert system.

Call Narrative
Supplemental Data (or caller-generated data) manually gathered and entered by the call taker for the purposes of documenting the call. Part of the Call Record.

Call Record
The collection of all information related to a call (including Essential, Supportive, and Supplemental data); composed of Call Detail Record, Call Recording, and Call Narrative.

Call Recording
The electronic documentation of the interactive communication (e.g., audio, video, text, image) between the caller, call taker, and any conferenced parties. Part of the Call Record.

Call Routing
The capability to selectively direct the 9-1-1 call to the appropriate PSAP.

Call Taker	As used in 9-1-1, a person (sometimes referred to as a telecommunicator) who receives emergency and non-emergency calls by telephone and other sources, determines situations, elicits necessary information, and relays essential information to dispatches, staff, and other agencies, as needed, using telephony and computer equipment.
Call Transfer	The capability to redirect a call to another party.
Call Type	Classification of a 9-1-1 call that indicates the call access method, which can affect call treatment, routing, and processing. Call types may include voice caller, short message service (SMS) text, Simple Mail Transfer Protocol (SMTP) text, multimedia, telematics data, ANI, silent alarms, etc.
Circuit-Switch	The establishment, by dialing, of a temporary physical path between points. The path is terminated when either end of the connection sends a disconnect signal by hanging up.
Civic Address Information	Street address data, inclusive of suite/office number, where appropriate.
Cross-System Authentication	Authentication across a number of systems or networks via a single authentication process, sometimes referred to as Single Sign-On (SSO), and potentially achieved via proxy authentication.
Customer Premises Equipment (CPE)	Communications or terminal equipment located in the customer's facilities; terminal equipment at a PSAP.
Database	An organized collection of information, typically stored in computer systems, composed of fields, records (data), and indexes. In 9-1-1, such databases include the master street address guide, telephone number, and telephone customer records.
Data Integrity	The property of not having been altered or destroyed in an unauthorized manner.
Digital	Relating to calculation, storage, or transmission by numerical methods or discrete units, as opposed to the continuously variable analog. Computerized.
Disaster	Any event that can cause a significant disruption to normal emergency calling capability.
Dispatcher	As used in public safety, a person responsible for receiving and transmitting information pertaining to requests for emergency service and other related activities, tracking vehicles and equipment, and recording other important information using a telephone, radio, and other communications resources.
Dispatch Operations	The distribution of emergency information to responder organizations responsible for delivery of emergency services to the public.

Emergency Call	A telephone request for public safety agency emergency services that requires immediate action to save a life, to report a fire, or to stop a crime. May include other situations as determined locally.
Emergency Location Information	Data pertaining to the location of the emergency, which may be different from the caller location.
Emergency Medical Service (EMS)	A system providing pre-hospital emergency care and transportation to victims of sudden illness or injury.
Emergency Response	An effort by public safety personnel and citizens to mitigate the impact of an incident on human life and property.
Enhanced 9-1-1 (E9-1-1)	An emergency telephone system that includes network switching, database, and CPE elements capable of providing selective routing, selective transfer, fixed transfer, caller routing and location information, and ALI.
Enterprise	The highest level of system functionality.
Essential Call Data	Data that support call delivery and adequate response capability. These data, or a reference to them, is automatically provided as a part of call or message initiation. Examples include location, callback data, and call type.
Extensibility	The property of a system to be adaptable for future growth. The ability to add extended functionality to a system.
Fixed Transfer	The capability of a PSAP call taker to direct a 9-1-1 call to a predetermined location by depressing a single button.
Firewall	The primary method for keeping a computer secure from intruders. It allows or blocks traffic into and out of a private network or the user's computer.
Functional Activity	Bounded piece of work to be performed that describes the people, processes, and technology used.
Gateway	The point at which a circuit-switched call is encoded and repackaged into IP packets; equipment that provides interconnection between two networks with different communications protocols; two examples are packet assembler/disassemblers and protocol converters.
Generic Route Encapsulation (GRE)	A tunneling protocol that can encapsulate a variety of network-layer protocol packet types inside IP tunnels. This protocol creates a virtual point-to-point link between geographically-dispersed routers over an IP-based internetwork.

Geographic Information System (GIS)	A computer software system that enables one to visualize geographic aspects of a body of data. It contains the ability to translate implicit geographic data (such as a street address) into an explicit map location. It has the ability to query and analyze data in order to receive the results in the form of a map. It also can be used to graphically display coordinates on a map (i.e., latitude/longitude) from a wireless 9-1-1 call.
Global Positioning System (GPS)	A satellite-based location determination technology.
Integrity	See "Data Integrity."
International Telecommunications Union (ITU)	The telecommunications agency of the United Nations established to provide worldwide standard communications practices and procedures. Formerly CCITT.
Internet Engineering Task Force (IETF)	The lead standards-setting authority for Internet protocols.
Internet Protocol (IP)	The set of rules by which data are sent from one computer to another on the Internet or other networks.
Internetwork	To go between one network and another; a large network made up of a number of smaller networks.
Interoperability	The capability for disparate systems to work together.
Landline	Colloquial term for the Public Switched Telephone Network access via an actual copper or fiber optic transmission line that located underground or on telephone poles. Used to differentiate the "wireless" connectivity of a cellular or personal communications services system. Also referred to as "wireline."
Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED)	The Link Layer Discovery Protocol-Media Endpoint Discovery is protocol that provides device location discovery to allow creation of location databases to support location identification for 9-1-1 calls. The protocol is approved and published as: "ANSI/TIA-1057" by the Telecommunications Industry Association (TIA).
Local Exchange Carrier (LEC)	A telecommunications carrier under the state/local Public Utilities Act that provides local exchange telecommunications services. Also known as Incumbent Local Exchange Carrier (ILEC), Alternate Local Exchange Carrier (ALEC), Competitive Local Exchange Carrier (CLEC), Competitive Access Provider (CAP), Certified Local Exchange Carrier (CLEC), and Local Service Provider (LSP).
Location	See "Caller Location Information" and "Emergency Location Information."

National Emergency Number Association (NENA)	A not-for-profit corporation established in 1982 to further the goal of "One Nation–One Number." NENA is a networking source and promotes research, planning, and training. It strives to educate, set standards, and provide certification programs, legislative representation, and technical assistance for implementing and managing 9-1-1 systems.
Nature of Emergency	Reason for a citizen's request for response from emergency services (e.g., heart attack, vehicle collision, burglary)
Network	An arrangement of devices that can communicate with each other.
Overflow	The telecommunications term for the condition when there are more calls than the primary network path is designated to handle. This condition invokes the need to perform some form of call treatment, such as busy signals or alternate routing.
Packet	Logical grouping of information that includes a header containing control information and (usually) user data. Packets are most often used to refer to network layer units of data. The terms *datagram*, *frame*, *message*, and *segment* are also used to describe logical information groupings at various layers of the Operating System Interface (OSI) reference model and in various technology circles.
Packet-Switch	A network technology that breaks up a message into small packets for transmission. Each packet contains a destination address. Thus, not all packets in a single message must travel the same path. As traffic conditions change, they can be dynamically routed via different paths in the network, and they can even arrive out of order. The destination computer reassembles the packets into their proper sequence.
Personal Digital Assistant (PDA)	Small, handheld device used to store address book information, telephone numbers, personal contacts, and other personal information.
Protocol	A set of rules or conventions that govern the format and relative timing of data in a communications network. There are three basic types of protocols: character-oriented, byte-oriented, and bit-oriented. The protocols for data communications cover such activities as framing, error handling, transparency, and line control.
Public Safety Answering Point (PSAP)	A facility equipped and staffed to receive 9-1-1 calls; a generic name for a municipal or county emergency communications center dispatch agency that directs 9-1-1 or other emergency calls to appropriate police, fire, and emergency medical services agencies and personnel.
Public Switched Telephone Network (PSTN)	The network of equipment, lines, and controls assembled to establish communication paths between calling and called parties in North America.
PSTN UA	Typically a traditional telephone, but can also be a TDD/TTY (Telecommunications Device for the Deaf or Teletype device).

Redundancy	Duplication of components, running in parallel, to increase reliability; a backup system (either a device or a connection) that serves in the event of primary system failure.
Reliability	The ability of a system or component to perform its required functions under stated conditions for a specified period of time.
Requirement	A statement of a characteristic that the system must possess in order to be acceptable; the desired system is defined as one that fulfills all of the requirements.
Router	An interface device between two networks that selects the best path to complete the call even if there are several networks between the originating network and the destination.
Scalability	The property of a system to be readily enlarged, e.g., by adding hardware to increase capacity or throughput.
Security	The ability to provide adequate data and service protection to mitigate unauthorized access, service exploitation, and leakage of confidential or sensitive information.
Selective Routing	Direction of a 9-1-1 call to the proper PSAP based on the location of the caller.
Selective Transfer	The capability to convey a 9-1-1 call to a response agency by operation of one of several buttons typically designated as police, fire, and emergency medical.
Service Provider	An entity providing one or more of the following 9-1-1 elements: network, CPE, or database service.
Short Message Service (SMS)	A text message service that enables messages generally no more than 140–160 characters in length to be sent and transmitted from a cellular telephone. Short messages are stored and forwarded at SMS centers, allowing their retrieval later if the user is not immediately available to receive them.
Session Initiation Protocol (SIP)	A signaling protocol used to exchange data (including voice, video, and text) among an association of participants (RFC 3261)
Spatial	Concept of describing a space or area of space.
Stakeholder	An individual or group with an interest in the successful delivery of intended results by a project.

Supplemental Call Data	Information that may complement, but is not necessary for, call handling and dispatch. This data typically would be automatically or manually queried after the call is delivered to the call taker. Examples include contact information for someone who should be notified of a medical emergency, building blueprints, other addresses in the immediate vicinity, etc.
Supportive Call Data	Information beyond essential data that may support call handling and dispatch. This data typically would be automatically or manually queried by the system before the call is delivered to the call taker. The addition of this data to the call stream is triggered by one or more of the data or reference items in essential data for a given call type. An example is ACN data such as "vehicle rollover."
System of Systems	Interconnected and decentralized system of interoperable networks and software services.
Telecommunications Industry Association (TIA)	A lobbying and trade association, which is the result of the merger of the USTA (United States Telephone Association) and the EIA (Electronic Industries Association).
TCP (Transmission Control Protocol)	The set of rules within the TCP/IP protocol suite that ensures that all data arrives accurately and 100-percent intact at the destination.
Telematics	The system of components that supports two-way communications with a motor vehicle for the collection or transmission of information and commands.
Telephony	The electronic transmission of the human voice.
Transfer	A feature that allows PSAP call takers to redirect a 9-1-1 call to another location.
Transmission Control Protocol/Internet Protocol (TCP/IP)	A layered set of protocols (sets of rules) used to connect dissimilar computers together. TCP provides the transport service required by the application layer. The TCP layers in the two host computers that are sending data will communicate with each other to ensure reliable data packet transport. IP provides the service user to deliver the datagram to its destination, providing the routing through the network and the error messages if the datagram is undeliverable.
User Authentication	See "Authentication."
Voice over Internet Protocol (VoIP)	A set of rules that provides distinct packetized voice information in digital format using the Internet Protocol. The IP address assigned to the user's telephone number may be static or dynamic.

Wireless In the telecommunications industry, typically refers to mobile telephony and communications through handheld devices that make a connection using radio frequency (in particular frequency bands often reserved for mobile communications) for personal telecommunications over long distances.

Wireline Standard telephone and data communications systems that use in-ground and telephone pole cables. Also known as landline or land-based.

Appendix C—Source References

The following published documents are primary sources of information used in this document.

- *Next Generation 9-1-1 (NG9-1-1) System Initiative: Concept of Operations.* USDOT ITS JPO. April 2007. http://www.its.dot.gov/ng911/pdf/NG911ConOps_April07.pdf—This formal document provides a user-oriented vision of NG9-1-1 in the context of an emergency services internetwork that can be understood by stakeholders with a broad range of operational and technical expertise. It is intended to communicate the vision of this system to stakeholders so that they can be actively engaged in its development and deployment.

- *Next Generation 9-1-1 (NG9-1-1) System Initiative: System Description and Requirements Document.* USDOT ITS JPO. July 2007. http://www.its.dot.gov/ng911/ng911_pubs.htm—This formal document identifies NG9-1-1 user and system needs. Operational, systems, and data behaviors to support NG9-1-1 required activities are also detailed in this document.

- *Network Architecture Properties in 2010, Extending E9-1-1 to Satellites, and Generic Architectures to Support Video and Advanced Service*. NRIC VII Focus Group 1B, FCC. June 2005. *Long Term Issues for Emergency/E9-1-1 Services* (Draft)—These documents are designed to provide a set of specific recommendations regarding future emergency communications network properties and their capabilities by 2010 to support the exchange of voice, data, text, photographs, and live video through the emergency services internetwork to the PSAP and beyond.

- *Communication Issues for Emergency Communications Beyond E911: Final Report—Properties and network architectures for communications between PSAPs and emergency services organizations and personnel.* NRIC VII Focus Group 1D, FCC. December 2005. http://www.nric.org/meetings/docs/meeting_20051216/FG1D_Dec%2005_Final%20Report.pdf—The purpose of these documents is to describe the properties that network architectures for communications between PSAPs and emergency services personnel must meet.

- *NENA i3 Technical Requirements Document* [NENA i3]. NENA VoIP/Packet Technical Committee Long-Term Definition Working Group. September 2006. http://www.nena.org/media/files/08-751_20060928.pdf—This document provides requirements for a NENA-recommended standard for the i3 architecture for end-to-end emergency calling over IP networks.

- *Requirements for Emergency Context Resolution with Internet Technologies* [ECRIT]. IETF. August 2006. http://www.ietf.org/internet-drafts/draft-ietf-ecrit-requirements-12.txt—This document enumerates requirements for emergency calls placed by the public using VoIP and general Internet multimedia systems, where Internet protocols are used end-to-end.

- *NENA Technical Information Document (TID) on the Network Interface to IP Capable PSAP* [NENA 08-501]. NENA Migration Working Group of the Network Technical Committee. June 2004. http://nena.org/9%1e1%1e1TechStandards/TechInfoDocs/NENATIDIPPSAPIF.pdf—This TID provides information to guide manufacturers of network equipment and PSAP customer premises equipment (CPE) in the development of IP-based interfaces between the network and PSAP CPE and to assist E9-1-1 network service providers and PSAPs in implementing such interfaces.

- *NENA IP-Capable PSAP Minimum Operational Requirements Standard* [58-001]. Issue 2, June 2007. http://www.nena.org/media/files/NENA58-001OpsIP-PSAPStd-final06092007.pdf—This standard contains a list of capabilities or features that are expected to be supported in a PSAP using IP-based 9-1-1 equipment, and software developed in an open architecture environment that will allow interoperability at all levels of the 9-1-1 network, regardless of vendors.

- *NENA Data Standards for Local Exchange Carriers, ALI Service Providers, & 9-1-1 Jurisdictions* [NENA 02-011]. NENA Technical Committee Chairs. November 2006. http://www.nena.org/media/files/02-011_20061121.pdf—This document establishes technical standards for all service providers involved in providing telephone services.

- *NENA Data Standards for the Provisioning and Maintenance of MSAG Files to VDBs and ERDBs* [NENA 02-013]. NENA Data Technical Committee, VDB/MSAG Working Group. January 2007. http://www.nena.org/media/files/02-013_20070109.pdf—This document contains system and process requirements for the Validation Database (VDB), Emergency Service Zone (ESZ) Routing Database (ERDB), and system administrator to maintain the Master Street Address Guide (MSAG) and ALI required in i2 system architecture.

- *NENA Technical Information Document on Future 9-1-1 Models* [NENA 07-501]. NENA Future Models Working Group. June 2004. http://www.nena.org/media/files/07-501_20040601_1.pdf—This TID lays out the framework for 9-1-1 systems that will provide the functionalities that public safety responder agencies need or will need to respond to emergency 9-1-1 calls.

- *A Framework for Inter-Domain Route Aggregation* [RFC 2519]. IETF Network Working Group. February 1999. http://www.ietf.org/rfc/rfc2519.txt—This document presents and analyzes a framework for inter-domain route aggregation, a flexible and scalable solution.

- *A Border Gateway Protocol (BGP-4)* [RFC 1771]. IETF Network Working Group. March 1995. http://www.ietf.org/rfc/rfc1771.txt—This document defines an Internet routing protocol.

This page left blank intentionally.