ITS Intelligent Transportation Systems
U.S. Department of Transportation

NG9-1-1

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

Architecture Analysis Report

Washington D.C.

November 2007 | Version 1.0

Introduction
Arch. Analysis Approach
Architecture Definition
Key Arch. Considerations
NG9-1-1 DB Services
NG9-1-1 Network
NG9-1-1 PSAP
IP Call Origination
Architecture Summary
Source References
Appendices

Document Change History

Version	Publication Date	Description of Change
v0.1	September 2007	Draft
v0.2	October 2007	Revised draft
v1.0	November 2007	First release

Table of Contents

List of Figures

List of Tables

Introduction
Arch. Analysis Approach
Architecture Definition
Key Arch. Considerations
NG9-1-1 DB Services
NG9-1-1 Network
NG9-1-1 PSAP
IP Call Origination
Architecture Summary
Source References
Appendices

Section 1: Introduction

The purpose of this document is to provide an Architecture Analysis for the Next Generation 9-1-1 (NG9-1-1) System (or "system of systems"). The U.S. Department of Transportation (USDOT) understands that access to emergency services provided by 9-1-1 in today's world of evolving technology will ultimately occur within a broader array of interconnected networks comprehensively supporting emergency services—from public access to those services, to the facilitation of the services, to the delivery of the emergency information to dispatchers and first responders.

More specifically, USDOT views the NG9-1-1 System as a transition to enable the general public to make a 9-1-1 "call"[1] from any wired, wireless, or Internet Protocol (IP)-based device, and allow the emergency services community to take advantage of enhanced call delivery and advanced functional and operational capabilities through new internetworking[2] technologies based on open standards. By enabling the general public to access

[1] *The term "call" is used in this document to indicate any real-time communication—voice, text, or video—between a person needing assistance and a PSAP call taker.*

[2] *"Internetwork"—to go between one network and another; a large network made up of a number of smaller networks.*

9-1-1 services through virtually any communications device, the NG9-1-1 System provides a more direct ability to request help or share critical data with emergency services provider from any location. In addition, call takers at the Public Safety Answering Points (PSAP) will be able to transfer emergency calls to another PSAP and forward the location and other critical data, such as text messages, images, and video, with the call.

This 9-1-1 Architecture Analysis Report presents an evolved 9-1-1 architecture able to support next generation technologies, access methods, and operational capabilities. The legacy 9-1-1 architecture is described as a starting point and is then expanded to address the needed functions within the next generation environment. Key architectural considerations are discussed to draw attention to the characteristics and issues most key to the successful operation of the NG9-1-1 System.

1.1 Vision of NG9-1-1

The intent of USDOT is to promote the vision for the NG9-1-1 System and provide leadership, guidance, and resources to work with the public and private 9-1-1 stakeholders to lay out a path to achieve a phased migration of a nationally interoperable[3] emergency services internetwork.

USDOT's core vision for NG9-1-1 is that this new system of systems will provide the foundation for public emergency services in an increasingly mobile and technologically diverse society and ultimately enable Enhanced 9-1-1 (E9-1-1) calls from most types of communication devices. Once implemented, the NG9-1-1 System will enable—

- Quicker and more robust information delivered to both responders and the general public as the result of making a 9-1-1 call
- Better and more useful forms of information (text, images, and video) from any networked communications device
- Transfer of 9-1-1 calls between geographically dispersed PSAPs (and from PSAPs to remote public safety dispatch centers) if necessary
- Increased aggregation and sharing of data, resources, procedures, and standards to improve emergency response
- Maximized use of available public capital and operating cost savings for emergency communications services
- Promotion of increased coordination and partnerships within the emergency response community.

1.2 Scope

It is intended that this document serve as a reference for organizations, operators, entities, and individuals who currently support the 9-1-1 community and play a part in definition and development, management, and operations of the next generation system. The NG9-1-1 Architecture Analysis Report has benefited from the current efforts of several 9-1-1 community organizations, numerous standards development efforts, and key community stakeholders. Figure 1-1 below illustrates how these inputs and those from across the USDOT NG9-1-1 Initiative support this analysis effort.

Although the NG9-1-1 Architecture Analysis Report proposes an architecture that can support next generation needs, it does not seek to identify a standard implementation across any local or state jurisdiction. The key architecture considerations discussed in the analysis are not the full set of possible network and system characteristics and issues that must be evaluated in any single implementation. Rather, the key considerations discussed are intended to build an understanding of some of the important architectural issues that must be addressed during the design, development, deployment, and/or operations stages of the system. Follow-on analysis from

[3] *The emergency services internetwork will be "interoperable" in that the networks and systems that comprise the NG9-1-1 architecture system of systems will have the ability to work together using standard formats and protocols.*

Inputs to the NG9-1-1 Architecture

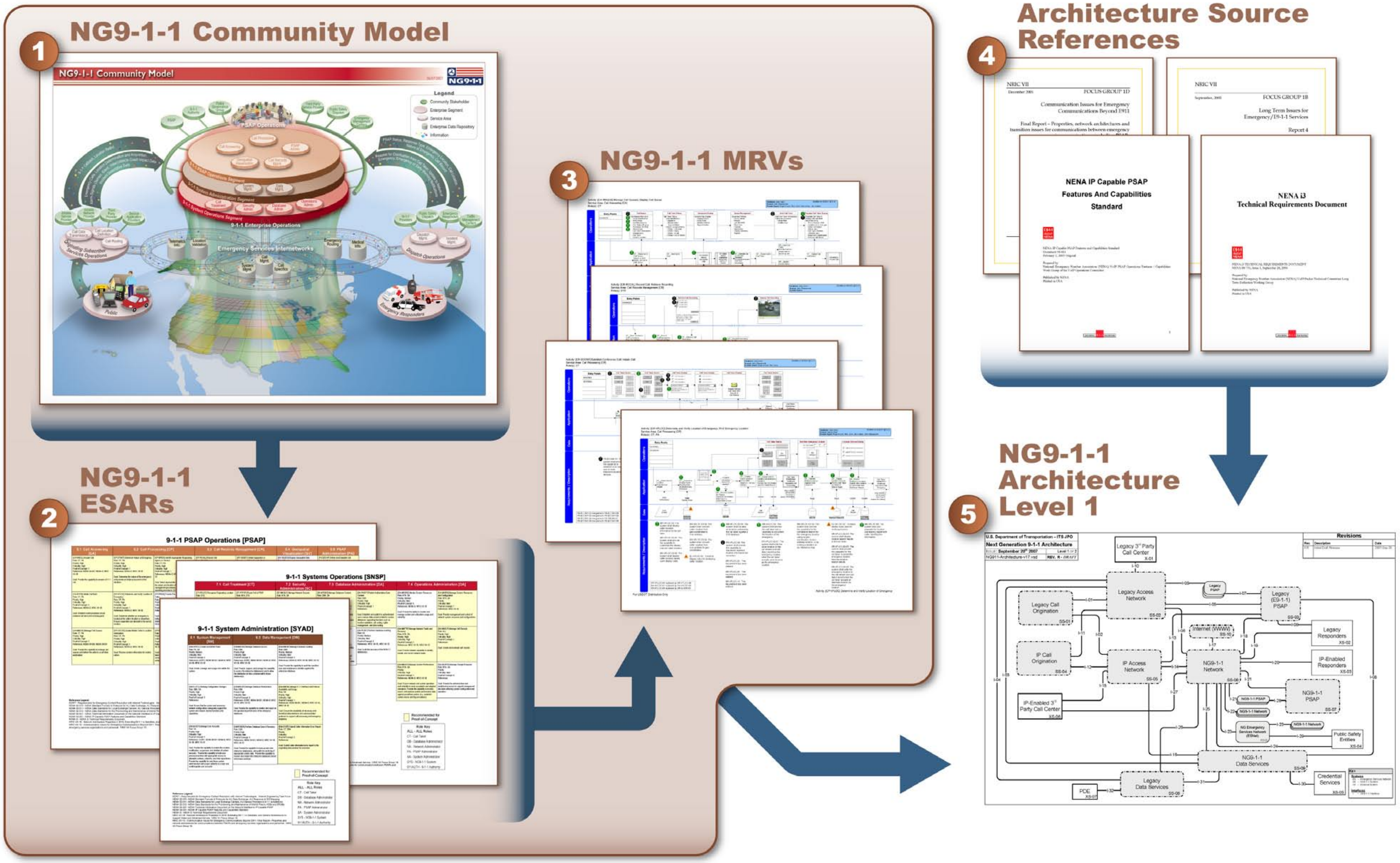

1
NG9-1-1 Community Model
NG9-1-1 Community Model
PSAP Operations
9-1-1 Enterprise Operations
Emergency Services Internetworks
Public
Emergency Responders
2
NG9-1-1 ESARs
9-1-1 PSAP Operations [PSAP]
9-1-1 Systems Operations [SNSP]
9-1-1 System Administration [SYAD]
3
NG9-1-1 MRVs
4
Architecture Source References
NRIC VII
FOCUS GROUP 1D
Communication Issues for Emergency Communications Beyond E911
FOCUS GROUP 1B
Long Term Issues for Emergency/E9-1-1 Services
NENA IP Capable PSAP Features And Capabilities Standard
NENA i3 Technical Requirements Document
5
NG9-1-1 Architecture Level 1
Legacy 3rd Party Call Center
Legacy Access Network
Legacy Call Origination
Legacy (E9-1-1) PSAP
Internet (WWW)
Legacy Responders
IP Call Origination
IP Access Network
NG9-1-1 Network
IP-Enabled Responders
IP-Enabled 3rd Party Call Center
NG9-1-1 PSAP
Public Safety Entities
NG9-1-1 Data Services
Legacy Data Services
Credential Services
PDE
Revisions

Figure 1–1: Inputs to the NG9-1-1 Architecture

this document could seek to address operational considerations or evaluate additional architectural considerations to produce additional references for NG9-1-1 developments.

1.3 Architecture Goals

Technology and standards identified and considered within this document are expected to support a number of system engineering qualities, including scalability, extensibility, reliability, configurability, and most important, interoperability.

The system must support scalability so that it can be sized to fit the needs of PSAPs and 9-1-1 authorities of differing sizes. PSAPs that protect the nation's largest cities (or states or regions) as well as those that protect individual communities will be able to implement an NG9-1-1 system or connect to an NG9-1-1 network to access the features and services of NG9-1-1. The scalability of the system should also permit horizontal and vertical scaling to allow individual NG9-1-1 systems to expand or change to manage such factors as additional call volume and increased network traffic, the addition of PSAPs, consolidation of PSAPs, addition of roadways, and changes in jurisdictional boundaries. System scalability should also make the system more affordable to 9-1-1 authorities because they can implement a system that is appropriately sized for their operations rather than having to adhere to a "one size fits all" rationale. Scalability limits are expected to depend on conditions such as political boundaries at state or sub-state levels, realistic bandwidth limitations in the networks, and database size and security management issues. System components and subsystems would be selected that support scalability needs.

The system must be extensible in that it must permit future technologies to be woven into the system without requiring wholesale replacement. Although future advances in technology cannot be predicted with certainty, the design principles of the system support quick adaptation of emerging technologies. The system would support "plug and play" functionality by natively supporting new devices or applications that meet the design standards of NG9-1-1, either through existing IP access networks or directly to the Emergency Services IP network. As new communications networks and devices are developed, the availability of open IP interface standards for 9-1-1 and emergency communications would allow initial designs to cope with 9-1-1 requirements at, optimally, the time of market introduction. System components would be selected that support extensibility needs.

There is no question that today's 9-1-1 communications systems are mission-critical systems and are major access points to the nation's critical infrastructure. As a result, NG9-1-1 demands that same mission-critical status and must be highly-reliable. Reliability is a key component of NG9-1-1 and requires redundant hardware, multipath connectivity, and no single point of failure. These requirements are particularly important because of the distributed nature of the overall system. System components would be selected that support reliability needs.

The NG9-1-1 System must support the ability to be highly configurable and support the diverse nature of PSAPs and 9-1-1 authorities. Public safety services throughout the nation have evolved through the years with different leadership, direction, and priority structures. As a result, no two PSAPs operate in the same manner. PSAPs serve very different geographies, citizens and responder groups, and types of calls, and must support the business rules and methods of call processing from one jurisdiction to another. System components would be selected that support configurability needs.

One of the greatest concerns is for the system to support interoperability with other NG9-1-1 systems, networks, and public safety entities. Interoperability can be provided by using gateways and border control devices to bridge the gap between diverse technologies. Standards will be employed to ensure the technology can interface and communicate across various systems and networks. In particular, well-established IP packet-switching methodologies will be employed as the protocol basis for the entire network system. System components would be selected that support interoperability needs.

It should be noted that as additional NG9-1-1 networks are interconnected, the system as a whole increases its interoperability, reliability, and connectivity.

1.4 Document Overview

This document contains the NG9-1-1 Architecture Analysis Report. It builds from the NG9-1-1 System Description and Requirements document to map NG9-1-1 required activities into the functional system elements that will support them. Further, this document then decomposes the system high-level functional architecture to identify detailed system and interface components necessary for the operation of the system. In addition to this Introduction, the NG9-1-1 Architecture Analysis Report is organized into the following numbered sections:

2. Architecture Analysis Approach
3. Architecture Definition
4. Key Architecture Considerations
5. NG9-1-1 Database Services
6. NG9-1-1 Network
7. NG9-1-1 PSAP
8. IP Call Origination/IP Access Network
9. Architecture Summary
10. Source References.

The ***Architecture Analysis Approach*** section describes the methodology used to develop the Architecture Analysis Report and describes the role of this analysis in support other key NG9-1-1 Initiative and industry efforts.

The ***Architecture Definition*** section introduces high-level and detailed architectures to support the NG9-1-1 System. It defines systems and interfaces within legacy and NG9-1-1 architectures and presents the requirements mapping analysis that maps NG9-1-1 functional needs to the component architecture elements.

The ***Key Architecture Considerations*** section defines the architecture characteristics to be discussed in the analysis and presents why the topics are important to the NG9-1-1 System.

The next four sections discuss NG9-1-1 architectural considerations based on the high-level NG9-1-1 composite architecture diagram presented in Section 3, Architecture Definition. Each section—***NG9-1-1 Database Services, NG9-1-1 Network, NG9-1-1 PSAP,*** and ***IP Call Origination/IP Access Network***—identifies key architecture considerations and discusses the benefits and considerations related to a specified aspect of the NG9-1-1 System.

The ***Architecture Summary*** section summarizes the NG9-1-1 required architectural elements and necessary characteristics of the architecture. It also summarizes key benefits and considerations to be taken into account in building the system functions.

The ***Source References*** section identifies sources of information used in development of the Architecture Analysis and lists key standards applicable to the work.

1.5 Intended Audience

The intended audience for this document includes the entities involved in current 9-1-1 system planning, operations, and technology; the organizations that will be involved in the development of NG9-1-1; and the organizations that will operate or produce NG9-1-1 elements. The general public is an implicit part of the intended audience because the NG9-1-1 System must ultimately serve its needs. Given the nature of the topics covered in this document, to most easily understand the discussions presented, knowledge of voice and data architecture and technologies and/or 9-1-1 networks and supporting technology is recommended for the reader.

Notes

Section 2: Architecture Analysis Approach

The NG9-1-1 architecture analysis approach allows a high-level analysis and identification of the technological deficiencies and gaps that must be addressed in order to achieve the required national NG9-1-1 System. The baseline architecture is the result of an evaluation of the functional requirements that were defined in the NG9-1-1 System Description and Requirements Document and other source materials. These requirements are analyzed and compared against system architecture needs to identify deficiencies and gaps between the functional requirements and the desired NG9-1-1 System. These gaps and deficiencies were used to determine the additional architectural components necessary to support next generation advanced functional and operational capabilities. The proposed NG9-1-1 baseline architecture is expected to undergo revision and upgrades to include future emerging technology features for NG9-1-1 to allow NG9-1-1 to be a flexible and adaptable system. Figure 2-1 on the following page depicts the architecture analysis process.

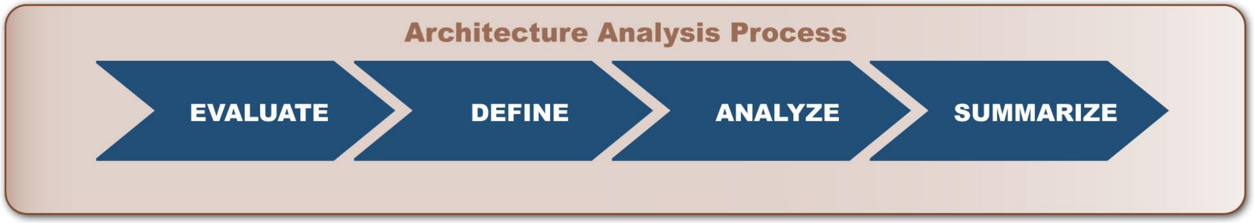


Figure 2–1: Architecture Analysis Process

Evaluate

The process begins with an evaluation of the legacy 9-1-1/E9-1-1 architectures and definition of the current baseline functional architecture. The existing NG9-1-1 functional requirements are then evaluated against the baseline architecture. Next, functional gaps are evaluated in order to identify the NG9-1-1 system components and technology necessary to support next generation capabilities.

Define

Next, the process defines the functional architecture based on the aforementioned functional gap evaluation. This includes defining an NG9-1-1 framework, which incorporates the key technical and architecture characteristics and the key current and emerging technical standards. Stakeholders within the 9-1-1 community have been approached to identify technological deficiencies and gaps and provide insight into the required national NG9-1-1 System characteristics needed to support next generation functional and operational capabilities. Results of the stakeholder outreach are included in the proposed analysis.

Analyze

The next step in the process is to define the impact of the key technical and architecture characteristics as they apply to the NG9-1-1 functionality. The leading benefits and considerations associated with these key characteristics were then discussed. Current and emerging technical standards and industry best practices are also considered as they apply to NG9-1-1 functionality. Specification documents and subject matter experts were consulted to ensure that NG9-1-1 architecture supports legacy 9-1-1 functionality.

Summarize

The final step in the analysis process is to summarize the use of this architecture analysis by today's 9-1-1 authorities and bring attention to those key considerations that designers, operators, and implementers must consider when planning their own local NG9-1-1 system.

As existing 9-1-1 systems transition to IP-based systems, various additional factors merit consideration, such as costs, responsibilities, and benefits for deploying IP-based technology. Thoroughly understanding these factors is facilitated by a defined architecture. A defined NG9-1-1 System architecture benefits the entire 9-1-1 community by establishing a standardized framework that will serve as the foundation for future system evolution.

Section 3: Architecture Definition

The NG9-1-1 Architecture consists of both high-level and detailed architectures. Within each of these levels, the architecture diagram is displayed in three distinct states: composite, legacy, and NG9-1-1. The composite architecture displays the entire system during its transition from a legacy 9-1-1 system to NG9-1-1. This composite architecture is then decomposed to present legacy 9-1-1 and NG9-1-1 system components. The legacy architecture indicates the technology as it exists today. Legacy technology includes wireline, wireless, and Voice over Internet Protocol (VoIP) devices connected through existing telephony switching and routing technologies to non-IP-enabled PSAPs. The NG9-1-1 architecture baseline includes all the proposed technology to support the NG9-1-1 System, including IP-enabled call origination, IP access networks, and NG9-1-1 routing to an IP-enabled PSAP.

It should be noted that for the architecture diagrams, descriptions, and tables in this document, the order of interfaces is purely for readability purposes and is not intended to specify a directional flow of data.

3.1 High-Level Architecture

The High-Level Architecture (also known as the Level 1 Architecture) describes the structure of NG9-1-1 at a system level, as shown in Figure 3-1 below. NG9-1-1 components and subsystems are described in the Detailed Architecture (Section 3.2 of this document). The Level 1 Architecture can be used as a basis for discussion by individuals and stakeholders when a non-technical view of the system is needed. The Level 1 diagram allows for a global view of the system and an understanding of how the major systems interact and interface with one another. Selected interfaces with external systems are included as well. This level of detail provides an indication of how a 9-1-1 call is initiated via call origination and transmitted through a network and ultimately to a PSAP. The NG9-1-1 network and supporting services are shown as the core of the NG9-1-1 Architecture and illustrate how all future network traffic will travel through the NG9-1-1 System. For additional information about any particular system, component, or interface, the Level 2 diagram (Section 3.2 of this document) provides a more detailed, technical view of the system.

Composite High-Level Architecture

The Composite High-Level Architecture describes the entire system during its transition phase from a legacy 9-1-1 system to NG9-1-1. All systems that exist in the baseline, as well as the NG9-1-1, are displayed, along with the interfaces between these high-level systems. The composite can be used to interpret today's system and which systems must be added to achieve an NG9-1-1 environment, but it does not show the end result of the full NG9-1-1 implementation. Each of the systems is described in detail in Section 3.1.1, and the interfaces between the systems are described in Section 3.1.2.

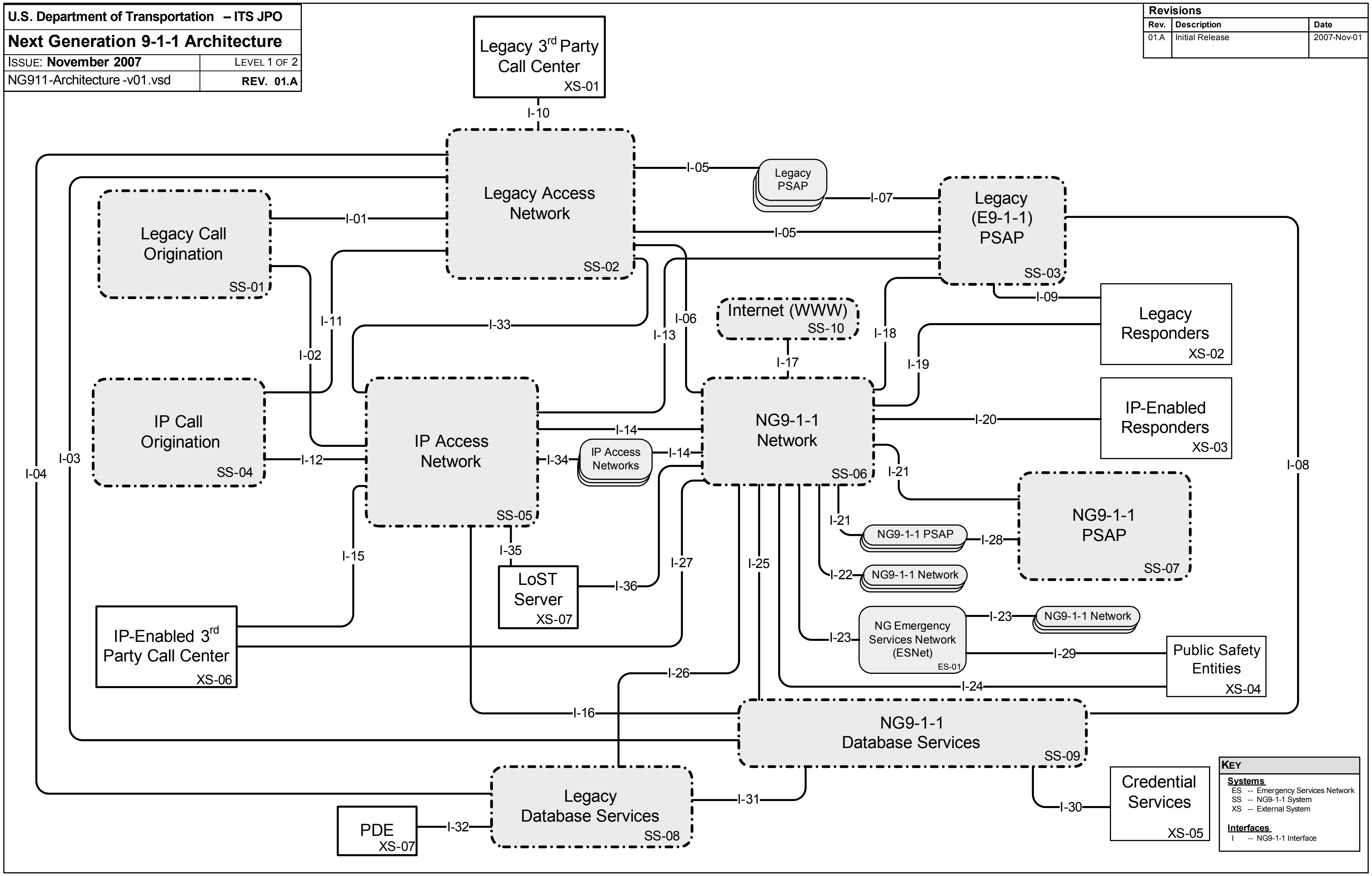
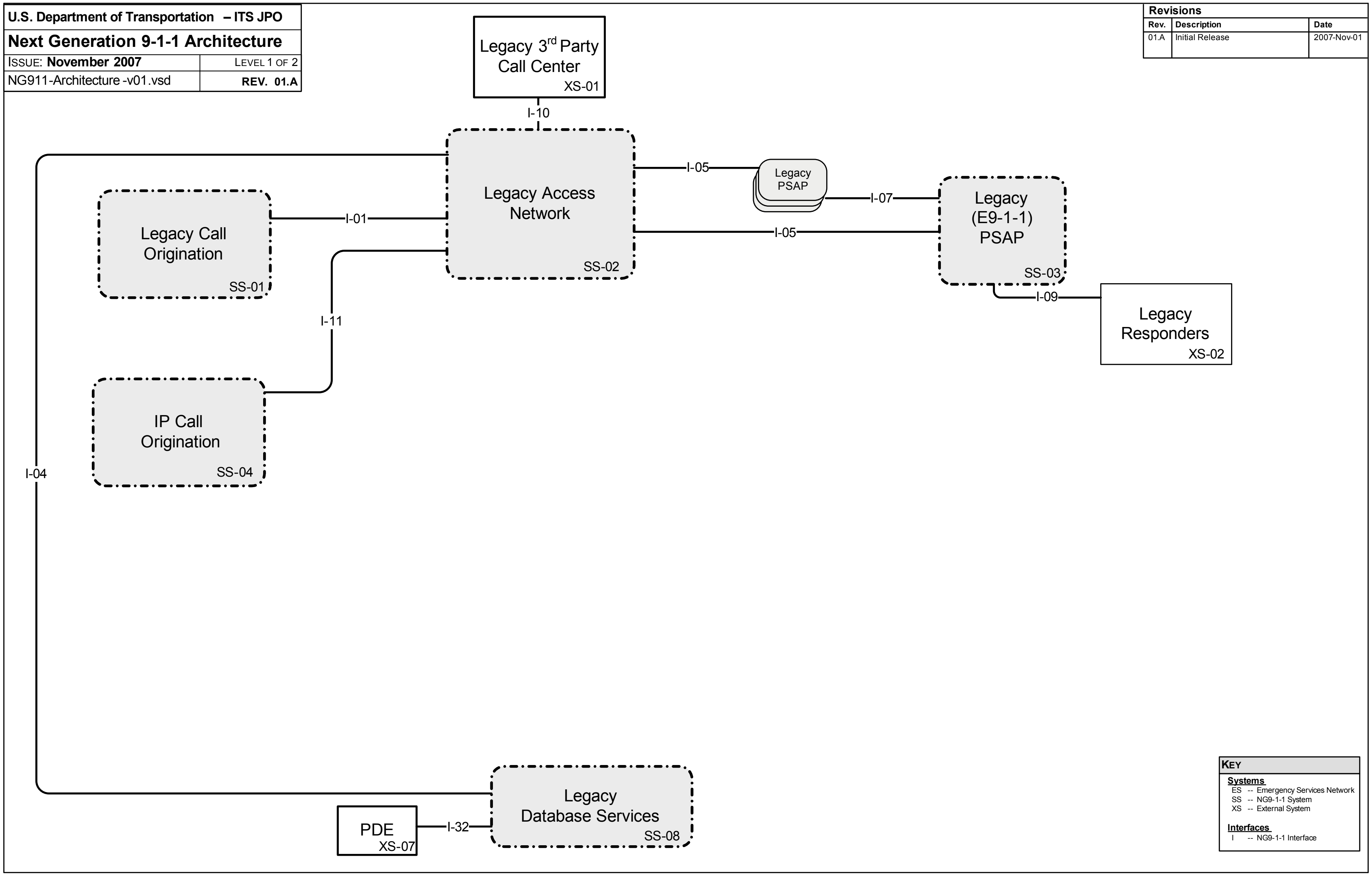


Figure 3–1: Composite High-Level Architecture

Legacy High-Level Architecture Baseline

The Legacy High-Level Architecture Baseline describes the 9-1-1 architecture in today's environment, as shown in Figure 3-2. This legacy representation includes legacy call origination, access network, PSAPs, and associated database services. Although some IP-enabled systems may exist in the legacy baseline, virtually all 9-1-1 calls originate from landlines, wireless (Commercial Mobile Radio Service [CMRS]) telephones, and some number of VoIP devices. Calls are routed through the legacy access network and forwarded through its Selective Router (based on predefined routing) to the legacy PSAP, typically through analog or digital trunks. The legacy systems are described in detail in Section 3.1.1, and the interfaces between the systems are described in Section 3.1.2.



U.S. Department of Transportation – ITS JPO	
Next Generation 9-1-1 Architecture	
ISSUE: November 2007	LEVEL 1 OF 2
NG911-Architecture -v01.vsd	REV. 01.A

Revisions		
Rev.	Description	Date
01.A	Initial Release	2007-Nov-01

Figure 3–2: Legacy High-Level Architecture Baseline

NG9-1-1 High-Level Architecture Baseline

The NG9-1-1 High-Level Architecture Baseline, as shown in Figure 3-3 describes what the NG9-1-1 System will consist of once the legacy services have been completely transitioned to NG9-1-1 or become statistically insignificant. IP-based call origination will route a call through an IP access network, determine its emergency calling status, and relay the call to the NG9-1-1 network. The NG9-1-1 network will use advanced routing capabilities to determine the most appropriate and available NG9-1-1 PSAP to which to forward the call and all associated data. Additional sources of data are also connected to the NG9-1-1 network and PSAPs to provide essential, supplemental, and supportive sets of data. Advanced security and authentication services are relied on to provide protection from intrusions or unauthorized access attempts. The NG9-1-1 systems are described in detail in Section 3.1.1, and the interfaces between the systems are described in Section 3.1.2.

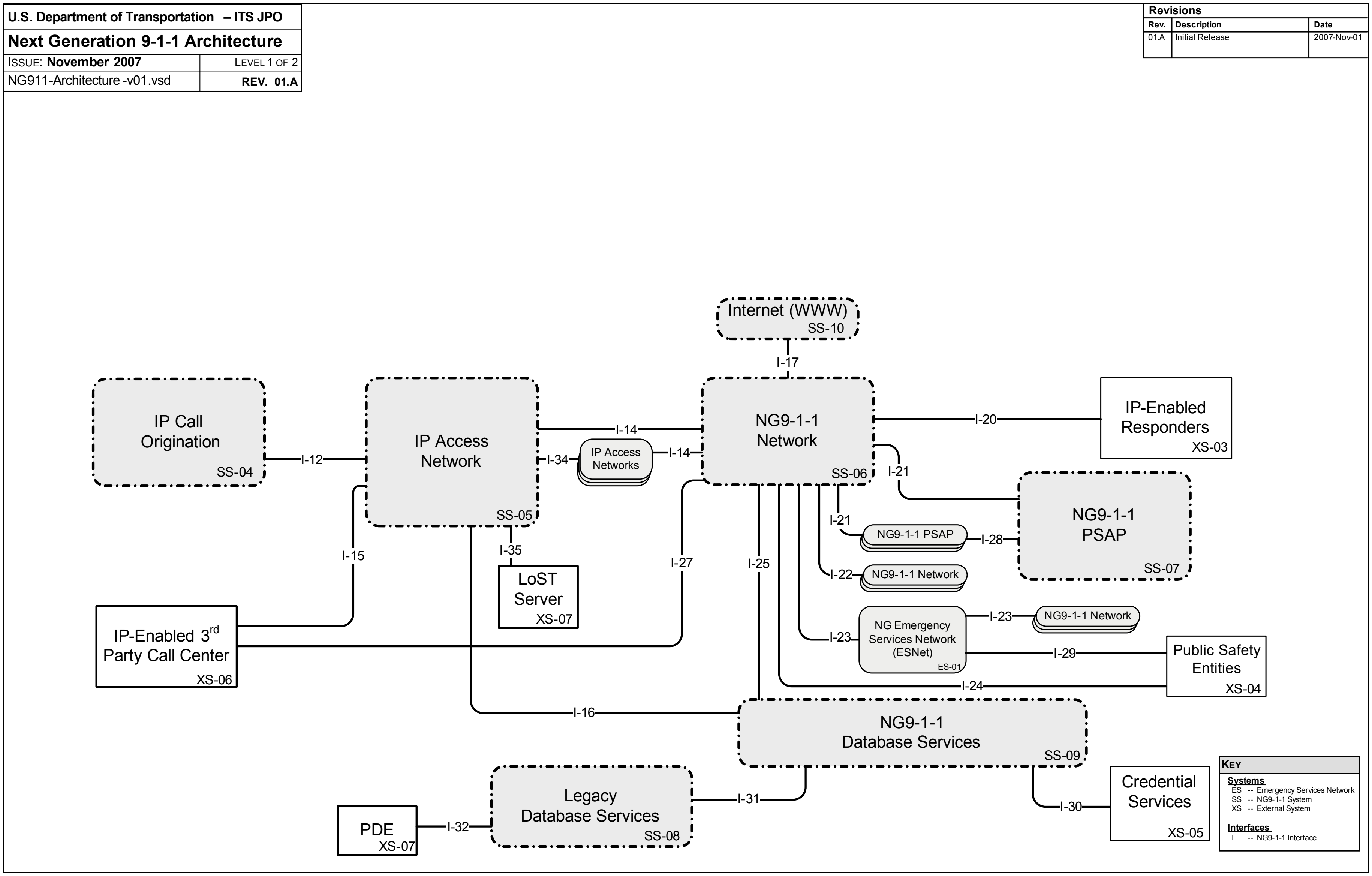


Figure 3–3: NG9-1-1 High-Level Architecture Baseline

3.1.1 Systems

Table 3-1 below contains a summary of all the systems in the Level 1 Architecture, organized by system ID. The table includes the system name, a description of what is accomplished by the system, and how it connects to other systems in the overall architecture. The system descriptions supplement the Level 1 Architecture diagrams included in Section 3.1 above.

Table 3–1: Summary of NG9-1-1 High-Level Systems

ID #	System Name	Description
SS-01	Legacy Call Origination	Legacy Call Origination describes the various non-IP devices that can access the Legacy Access Networks (SS-02) and the IP Access Networks (SS-05). These devices include: Public Switched Telephone Network (PSTN) User Agents (UA), non-IP Private Branch eXchange (PBX), non-IP sensors, non-IP wireless UAs, and non-IP telematics devices. When connecting to the IP Access Networks, the devices must connect to a Telephony Gateway (NA-01) to allow conversion of the non-IP-based call to an IP-based call.
SS-02	Legacy Access Network	Legacy Access Network describes the non-IP devices used to connect Legacy Call Origination (SS-01) devices to Legacy (E9-1-1) PSAPs (SS-03), typically using a Central Office (LA-03) or Mobile Switching Center (MSC) (LA-04) Switch. In addition, the Selective Router (LA-06) is used to determine the route to a pre-defined PSAP, and gateways typically exist to provide connectivity from newer technologies to the Legacy Access Network.
SS-03	Legacy (E9-1-1) PSAP	Legacy (E9-1-1) PSAP is the non-IP PSAP facility that receives inbound 9-1-1 calls from the Legacy Access Network (SS-02) through the use of a Telephony Switch/Automatic Call Distribution (ACD) (LP-01) device. The calls are distributed via the ACD device to the E9-1-1 Call Termination (LP-02) devices.
SS-04	IP Call Origination	IP Call Origination describes the various IP-based devices that can access the IP Access Network (SS-05) and the Legacy Access Networks (SS-02). These devices include: IP-based UAs, IP-based Private Branch eXchanges (IPBX), sensors, telematic devices, wireless UAs, and Short Message Service (SMS)/Text Message-capable devices. When connecting to Legacy Access Networks (SS-02), these IP-enabled devices must connect to either a Central Office (LA-01) or an MSC (LA-02) Telephony Gateway to allow conversion of the IP-based call to PSTN-based call.
SS-05	IP Access Network	IP Access Network describes the IP-based devices used to connect IP Call Origination (SS-04) devices to NG9-1-1 PSAPs (SS-07), through the use of a Call Proxy or Redirect Server (NA-04). An IP Access Network, as described in this architecture, is not necessarily the Internet and is used to describe any IP-based computer network used to deliver voice, video, text, and data via IP. Other components include a Provider Location Information Server (LIS) (NA-06) that delivers location information to provide the Call Proxy (NA-04) with a caller's location to make routing decisions. In addition, the Emergency Call Routing Function (ECRF) and a Location-to-Service Translation (LoST) database are used to take the caller's location and determine the routing path to the appropriate NG9-1-1 Network (SS-06). Routing of a call to a particular NG9-1-1 PSAP (SS-06) is performed within the routing functions of the NG9-1-1 Network (SS-06).

ID #	System Name	Description
SS-06	NG9-1-1 Network	NG9-1-1 Network provides the primary and central routing functions of the NG9-1-1 System. The NG9-1-1 Network receives inbound calls and requests from the IP Access Network (SS-05), Legacy (E9-1-1) PSAPs (SS-03), and NG9-1-1 PSAPs (SS-07), and determines the appropriate destination. In addition, the NG9-1-1 acts as the primary conduit for access to all Legacy (SS-08) and NG9-1-1 (SS-09) Database Services. The NG9-1-1 IP Routing Function (NN-05) uses a Location-to-Service Translation (LoST) database to take the caller's location and determine the routing path to the appropriate NG9-1-1 PSAP (SS-07).
SS-07	NG9-1-1 PSAP	NG9-1-1 PSAP describes all IP-enabled PSAPs that will share data with other NG9-1-1 PSAPs through the NG9-1-1 Network (SS-06). The NG9-1-1 PSAP will receive inbound 9-1-1 calls and events from the Legacy (SS-01) and IP (SS-04) Call Origination devices, and distribute the call and associated data to call takers via the PSAP IP Routing Function (NP-02) and PSAP IP ACD (NP-03) devices.
SS-08	Legacy Database Services	Legacy Database Services are those data sources and databases required for legacy operations and include the VoIP Positioning Center (VPC), the Mobile Positioning Center (MPC), and the Selective Router Database (SRDB).
SS-09	NG9-1-1 Database Services	NG9-1-1 Database Services include those data sources and databases required for NG9-1-1 operations and include Automatic Location Information (ALI) database, Master Street Address Guide (MSAG), Emergency Provider Access Directory (EPAD), and LoST database. Also, included in the NG9-1-1 Database Services are the Identity and Access Management (IdAM) data service to protect the integrity of the overall NG9-1-1 System.
SS-10	Internet (WWW)	The Internet (WWW) provides access to public web and media services. The Internet is used here to describe the ability for a call taker or NG9-1-1 system to query Internet-based services, like Public Web Services and Media Services. General Internet call origination is not expected nor would it be permitted to occur via this connectivity.
XS-01	Legacy 3rd Party Call Center	The Legacy 3rd Party Call Center is a generic name used to indicate those services that are important to the receipt, delivery, and response to 9-1-1 calls, but that are outside the boundaries of NG9-1-1. Examples of 3rd Party Call Centers include telematics service providers, poison control, suicide prevention, N-1-1, and language translation services. Legacy 3rd Party Call Centers are those that have not transitioned to IP connectivity to NG9-1-1 and will typically use voice communications to contact PSAPs and pass along data about their callers.
XS-02	Legacy Responders	Legacy Responders include public safety dispatchers and dispatch systems, emergency and supporting responders, and governmental and non-governmental agencies. Legacy Responders are those that use systems that have not transitioned to IP connectivity and typically are contacted via voice (telephone or radio) to receive information from NG9-1-1.
XS-03	IP-Enabled Responders	IP-Enabled Responders include public safety dispatchers and dispatch systems, emergency and supporting responders, and governmental and non-governmental agencies. IP-Enabled Responders are those that use systems that have transitioned to IP connectivity and can receive NG9-1-1 data automatically and electronically, with or without voice communications.

ID #	System Name	Description
XS-04	Public Safety Entities	Public Safety Entities include agencies or services that are connected directly to the Next Generation Emergency Services Network (ESNet) (ES-01). These agencies or services may provide supportive or supplemental data related to a call.
XS-05	Credential Services	Credential Services is the authoritative source of digital certificates and is used by the IdAM data service (ND-02) to support the credentialing and authority verification process within NG9-1-1.
XS-06	IP-Enabled 3rd Party Call Center	The IP-Enabled 3rd Party Call Center is the generic name used to indicate those services that are important to the receipt, delivery, and response to 9-1-1 calls, but that are outside the boundaries of NG9-1-1. Examples of 3rd Party Call Centers include telematics service providers, poison control, suicide prevention, N-1-1, and video relay/language translation services. IP-Enabled 3rd Party Call Centers are those that have transitioned to IP connectivity to NG9-1-1 and will typically use voice and data communications to contact PSAPs. IP-enabled centers surpass the capabilities of Legacy 3rd Party Call Centers because they will use the routing features of NG9-1-1 to determine the most appropriate PSAP for their caller's location and can transmit supplemental and supportive caller data to the PSAP automatically and electronically.
XS-07/	Position Determining Entity (PDE)	The PDE determines the geographic location of a wireless (CMRS) caller using one or more position-determining technologies. Note: PDE is also known as Location Determination Technology (LDT).
XS-08	Location-to-Service Translation (LoST) Server	The Location-to-Service Translation Protocol (LoST) Server describes a concept by which the LoST protocol is leveraged to map service identifiers and geospatial or civic location information to service contact Uniform Resource Locators (URL). Many LoST servers would likely exist, and IP Access Networks (SS-05) and NG9-1-1 Networks (SS-06) would use the LoST data as a method to identify appropriate routing of calls based on the caller's location.
ES-01	NG Emergency Services Network (ESNet)	NG ESNet is used to describe an infrastructure configuration in which multiple NG9-1-1 systems are connected together via a single but redundant and highly available nationwide network to support intersystem communications.

3.1.2 Interfaces

Table 3-2 summarizes all the interfaces in the Level 1 Architecture, organized by interface ID. The table includes the from and to system names, the interface name, and a description of the interface. The interface description identifies which two systems are being connected and what is accomplished by the interface. The system descriptions supplement the Level 1 Architecture diagrams included in Section 3.1 above.

Table 3–2: Summary of NG9-1-1 High-Level Interfaces

ID #	From	To	Interface/System Name	Description
I-01	SS-01	SS-02	Legacy Call Origination—Legacy Access Network	Legacy Call Origination interfaces with the Legacy Access Network to provide connectivity for devices able to make a call through their access providers.
I-02	SS-01	SS-05	Legacy Call Origination—IP Access Network	Legacy Call Origination interfaces with the IP Access Network through a gateway. This interface supports those legacy calls that are converted for an IP network.
I-03	SS-02	SS-09	Legacy Access Network—NG9-1-1 Database Services	The Legacy Access Network interfaces with the NG9-1-1 Database Services to access the NG9-1-1 databases.
I-04	SS-02	SS-08	Legacy Access Network—Legacy Database Services	The Legacy Access Network interfaces with the Legacy Database Services to access the legacy routing and positioning systems for mobile and voice over IP (VoIP) callers.
I-05	SS-02	SS-03	Legacy Access Network—Legacy (E9-1-1) PSAP	The Legacy Access Network interfaces with the Legacy (E9-1-1) PSAP for delivery of 9-1-1 calls (typically through a Selective Router [LA-05]).
I-06	SS-02	SS-06	Legacy Access Network—NG9-1-1 Network	The Legacy Access Network interfaces with the NG9-1-1 Network via a gateway to support delivery of calls from the Legacy Access Network to NG9-1-1.
I-07	SS-03		Legacy (E9-1-1) PSAP—Legacy (E9-1-1) PSAP	The Legacy (E9-1-1) PSAP interfaces with additional multiple legacy PSAPs to provide access from one legacy PSAP to another for transfer of calls (when one PSAP is connected to another PSAP's Automatic Call Distribution [ACD] device).
I-08	SS-03	SS-09	Legacy (E9-1-1) PSAP—NG9-1-1 Database Services	The Legacy (E9-1-1) PSAP interfaces with NG9-1-1 Database Services for access to the Automatic Location Information (ALI) database.
I-09	SS-03	XS-02	Legacy (E9-1-1) PSAP—Legacy Responders	The Legacy (E9-1-1) PSAP interfaces with the Legacy Responders to support delivery of call information. This is typically a voice interface via landline or radio, but could include limited electronic transfer of data.
I-10	SS-02	XS-01	Legacy Access Network—Legacy 3rd Party Call Center	The Legacy Access Network interfaces with Legacy 3rd Party Call Centers to receive calls from subscribers and to deliver requests to PSAPs via the Selective Router (LA-05). Typically, this interface provides voice-only connectivity between callers, the Legacy Access Network, and a Legacy (E9-1-1) PSAP (SS-03).

Introduction
Arch. Analysis Approach
Architecture Definition
Key Arch. Considerations
NG9-1-1 DB Services
NG9-1-1 Network
NG9-1-1 PSAP
IP Call Origination
Architecture Summary
Source References
Appendices

ID #	From	To	Interface/System Name	Description
I-11	SS-04	SS-02	IP Call Origination—Legacy Access Network	IP Call Origination interfaces with the Legacy Access Network through a gateway. This interface supports those IP call origination devices that require calls to be converted back to the Legacy Access Network.
I-12	SS-04	SS-05	IP Call Origination—IP Access Network	IP Call Origination interfaces with the IP Access Network to provide connectivity for devices able to make a call through their access providers.
I-13	SS-05	SS-03	IP Access Network—Legacy (E9-1-1) PSAP	The IP Access Network interfaces with a Legacy (E9-1-1) PSAP through a gateway to support IP network connectivity to Legacy (E9-1-1) PSAPs. This connectivity can provide direct input from the IP Access Network to a particular PSAP and could include delivery of IP-based calls, such as VoIP or sensor data. A Legacy PSAP Gateway (NA-05) would only exist during the transition to NG9-1-1 and would be eliminated by the routing capabilities and connectivity of the NG9-1-1 Network (SS-06)
I-14	SS-05	SS-06	IP Access Network—NG9-1-1 Network	The IP Access Network interfaces with the NG9-1-1 Network to provide routing services and deliver calls.
I-15	SS-05	XS-06	IP Access Network—IP-Enabled 3rd Party Call Center	The IP Access Network interfaces with an IP-Enabled 3rd Party Call Center to receive calls from subscribers and to deliver requests to PSAPs via the NG9-1-1 Network. This interface would be capable of transferring voice, video, text, and data across the IP Access Network and NG9-1-1 Network (SS-06) for use by the NG9-1-1 PSAP (SS-07).
I-16	SS-05	SS-09	IP Access Network—NG9-1-1 Database Services	The IP Access Network interfaces with the NG9-1-1 Database Services to provide access to databases that support the NG9-1-1 operations.
I-17	SS-06	SS-10	NG9-1-1 Network—Internet (WWW)	The NG9-1-1 Network interfaces with the Internet (WWW) to provide the NG9-1-1 Network and PSAP with access to public web and media services. General Internet call origination is not expected nor would it be permitted to occur via this interface.
I-18	SS-06	SS-03	NG9-1-1 Network—Legacy (E9-1-1) PSAP	The NG9-1-1 Network interfaces with a Legacy (E9-1-1) PSAP through a gateway to provide access for Legacy PSAPs to NG9-1-1.
I-19	SS-06	XS-02	NG9-1-1 Network—Legacy Responders	The NG9-1-1 Network interfaces with Legacy Responders through a gateway to transmit data related to NG9-1-1 calls.
I-20	SS-06	XS-03	NG9-1-1 Network—IP-Enabled Responders	The NG9-1-1 Network interfaces with IP-Enabled Responders to send and receive data related to NG9-1-1 calls.
I-21	SS-06	SS-07	NG9-1-1 Network—NG9-1-1 PSAP	The NG9-1-1 Network interfaces with NG9-1-1 PSAPs for the delivery of NG9-1-1 calls and associated data.
I-22	SS-06		NG9-1-1 Network—NG9-1-1 Network	The NG9-1-1 Network interfaces with other NG9-1-1 Networks to support communication among multiple NG9-1-1 Networks. This interface will allow an NG9-1-1 Network in one area/region to communicate with other NG9-1-1 Networks for primary and backup communications.

ID #	From	To	Interface/System Name	Description
I-23	SS-06	ES-01	NG9-1-1 Network—NG Emergency Services Network (ESNet)	The NG9-1-1 Network interfaces with the NG Emergency Services Network (ESNet) to connect multiple NG9-1-1 systems via a single but redundant and highly available nationwide network to support intersystem communications.
I-24	SS-06	XS-04	NG9-1-1 Network—Public Safety Entities	The NG9-1-1 Network interfaces with Public Safety Entities to connect agencies or services that may provide supportive or supplemental data related to a call.
I-25	SS-06	SS-09	NG9-1-1 Network—NG9-1-1 Database Services	The NG9-1-1 Network interfaces with NG9-1-1 Database Services to provide access to databases that support the NG9-1-1 operations.
I-26	SS-06	SS-08	NG9-1-1 Network—Legacy Database Services	The NG9-1-1 Network interfaces with Legacy Database Services to provide access to the legacy routing and positioning systems for mobile and VoIP callers.
I-27	SS-06	XS-06	NG9-1-1 Network—IP-Enabled 3rd Party Call Center	The NG9-1-1 Network interfaces with IP-Enabled 3rd Party Call Centers to receive calls from subscribers and to deliver requests to PSAPs. This interface would be capable of transferring voice, video, text, and data directly to the NG9-1-1 Network for use by the NG9-1-1 PSAP (SS-07).
I-28	SS-07		NG9-1-1 PSAP—NG9-1-1 PSAP	The NG9-1-1 PSAP can interface directly with other NG9-1-1 PSAPs and share calls and related data.
I-29	ES-01	XS-04	NG Emergency Services Network (ESNet)—Public Safety Entities	The NG ESNet interfaces with Public Safety Entities to connect agencies or services that may provide supportive or supplemental data related to a call.
I-30	SS-09	XS-05	NG9-1-1 Database Services—Credential Services	The NG9-1-1 Database Services provides access to Credential Services to support the credentialing and authority verification process within NG9-1-1.
I-31	SS-09	SS-08	NG9-1-1 Database Services—Legacy Database Services	The NG9-1-1 Database Services interfaces with the Legacy Database Services to provide access to positioning systems for mobile and VoIP callers.
I-32	SS-08	XS-06	Legacy Database Services—PDE	The Legacy Database Services interfaces to the Position Determining Entity (PDE) to provide the geographic location of a wireless (CMRS) caller using one or more position determining technologies.
I-33	SS-02	SS-05	Legacy Access Network—IP Access Network	The Legacy Access Network interfaces with the IP Access Network through a gateway, typically to share non-IP-based data, like SMS and text messages.
I-34	SS-05		IP Access Network—IP Access Networks	The IP Access Network can interface directly with other IP Access Networks to transfer calls and data across multiple IP networks using standard network routing abilities.
I-35	SS-05	XS-07	IP Access Network—LoST Server	The IP Access Network interfaces with one or more LoST Servers to query a caller’s location to determine routing information.
I-36	SS-06	XS-07	NG9-1-1 Network—LoST Server	The NG9-1-1 Network interfaces with one or more LoST Servers to query a caller’s location to determine routing information.

3.2 Detailed Architecture

The High-Level Architecture (also known as the Level 2 Architecture) describes the structure of NG9-1-1 at a component or subsystem level. The NG9-1-1 systems are described in the High-Level Architecture (Section 3.1 of this document). The Level 2 Architecture can be used as a basis for discussion at a more detailed, technical level of the system. The Level 2 diagram allows for a global view of the system, coupled with a detailed look at which components are required for each system area. In addition, the interfaces between the components within each system provide for a lower level of detail with regard to how each system is connected with the others. This level of detail provides an indication of how, specifically, a 9-1-1 call is initiated via call origination and transmitted through an access network (and their components) and ultimately to a PSAP. The NG9-1-1 network, in particular the NG9-1-1 IP Routing Function and its supporting services, are shown as the core of the NG9-1-1 architecture and illustrate how all future network traffic will travel through the NG9-1-1 System.

Composite Detailed Architecture

The Composite Detailed Architecture describes the system and its components during its transition phase from a legacy 9-1-1 system to NG9-1-1, as shown in Figure 3-4. All systems and their components that exist in the baseline as well as the components of NG9-1-1 are displayed, along with their individual interfaces between the systems. The composite can be used to interpret today’s existing configuration and which systems must be added to achieve an NG9-1-1 environment, but it does not show the end result of the full NG9-1-1 implementation. Each of the components is described in detail in Section 3.2.1, and the interfaces between the components are described in Section 3.2.2.

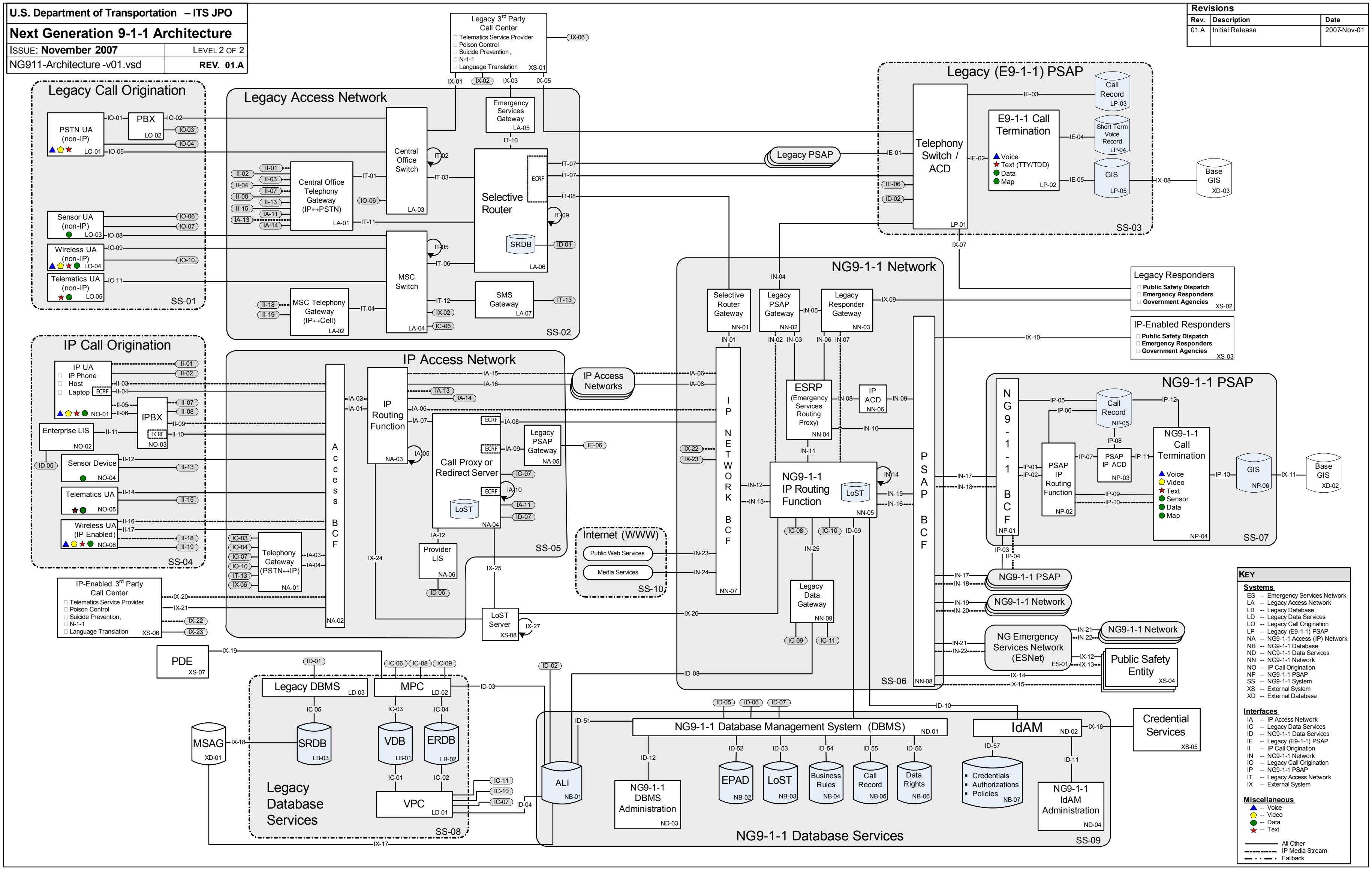


Figure 3–4: Composite Detailed Architecture

Legacy Detailed Architecture Baseline

The Legacy Detailed Architecture Baseline describes the 9-1-1 architecture in today's environment, as shown in Figure 3-5. This legacy representation includes the UAs that support legacy call origination, the central office, MSC, and selective router that comprise the access network, and the telephony switch and legacy call termination that exist at the PSAPs, along with their associated database services.

Legacy call origination includes traditional user agents like landline telephones, and non-IP-enabled wireless (CMRS) devices. These devices connect through either a central office switch or an MSC. In the legacy environment, the selective router makes the determination of how to forward the call to the correct PSAP, typically through analog or digital trunk circuits. The legacy PSAP receives the call through its telephony switch and typically employs an ACD device to distribute the call to a call taker workstation. In addition, in the legacy environment, IP-based calls are converted to non-IP calls through a gateway, before being routed to a PSAP.

The legacy components are described in detail in Section 3.2.1, and the interfaces between the systems are described in Section 3.2.2.

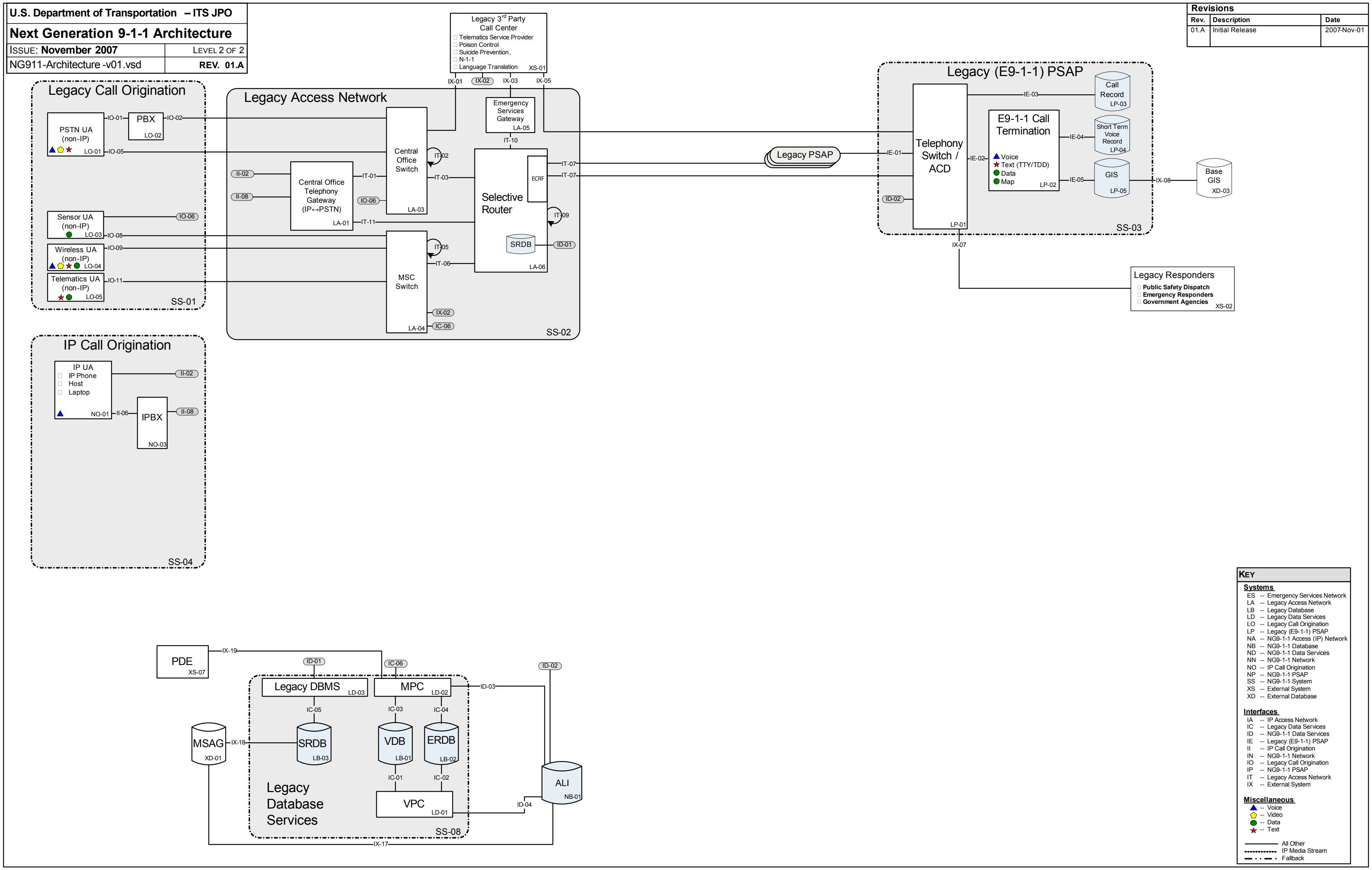


Figure 3–5: Legacy Detailed Architecture Baseline

NG9-1-1 Detailed Architecture Baseline

The NG9-1-1 Detailed Architecture Baseline describes what the NG9-1-1 System will consist of, once the legacy (non-IP-enabled) services have been completely transitioned to NG9-1-1 or become statistically insignificant, and is shown in Figure 3-6. IP-based call origination will route calls through an IP access network, determine its emergency calling status, and relay the call to the NG9-1-1 network. The NG9-1-1 network will use advanced routing capabilities to determine the most appropriate and available NG9-1-1 PSAP to which to forward the call and all associated data.

IP call origination includes IP-based UAs (such as VoIP phones or software), and IP-enabled wireless sensors, and telematics devices. These IP-based devices connect through an IP-enabled access network to handle IP routing and forwarding of network traffic. Once this IP traffic is recognized as an emergency call, a call proxy or redirect server is used to determine which NG9-1-1 network to which to send the call and its associated data.

The NG9-1-1 network, the core of the overall NG9-1-1 System, is used to receive all inbound emergency calls and route them to an appropriate PSAP through a Border Control Function (BCF) device. The BCF device acts as the boundary and access point to the NG9-1-1 network and will secure and protect the system from outside attack. By acting as a policy-based firewall and packet-scanning device, the BCF ensures that only authorized and authenticated traffic is allowed to pass through the NG9-1-1 network. In addition, invalid messages would be rejected, and the BCF could offer some security against intrusion by denying potentially malicious inbound activity.

Also within the NG9-1-1 network, the NG9-1-1 IP Routing Function provides the destination determination for the majority of all NG9-1-1 network traffic. Using a variety of data sources, the NG9-1-1 network forwards the call through the network to the most appropriate and available PSAP. The NG9-1-1 is responsible for providing connectivity among multiple PSAPs and among multiple NG9-1-1 networks. As previously stated, as NG9-1-1 networks are interconnected, the NG9-1-1 System as a whole increases its interoperability, reliability, and connectivity.

The NG9-1-1 (IP-enabled) PSAP receives calls and associated data from the NG9-1-1 network and is able to more efficiently route them within the PSAP to maximize call processing efforts (e.g., forwarding a call to the most appropriate call taker, based on a variety of parameters, such as language or special training), while minimizing call handling time and leveraging the available supporting data.

The NG9-1-1 components are described in detail in Section 3.2.1, and the interfaces between the components are described in Section 3.2.2.

U.S. Department of Transportation – ITS JPO	
Next Generation 9-1-1 Architecture	
ISSUE: **November 2007**	LEVEL 2 OF 2
NG911-Architecture -v01.vsd	**REV. 01.A**

Revisions

Rev.	Description	Date
01.A	Initial Release	2007-Nov-01

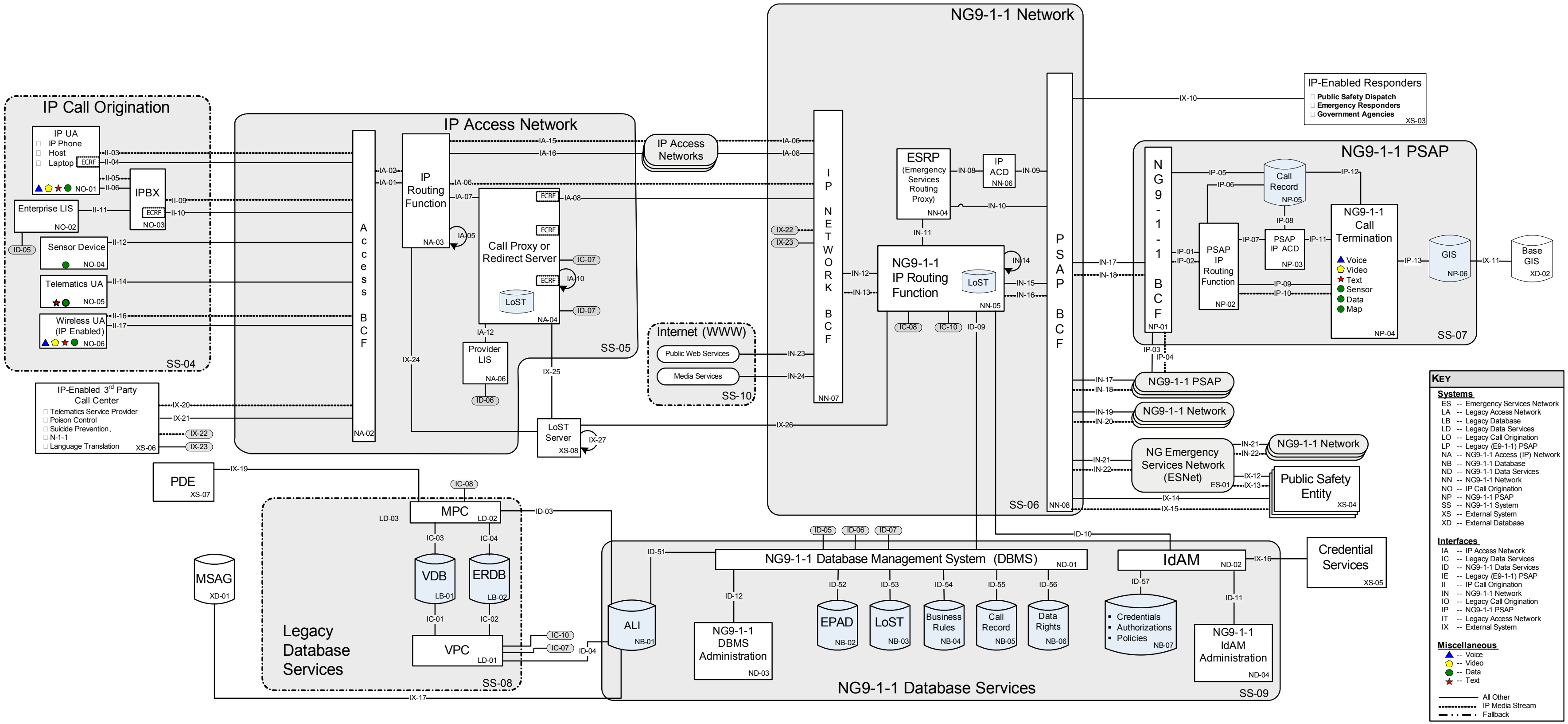


Figure 3–6: NG9-1-1 Detailed Architecture Baseline

3.2.1 Components

Table 3-3 below contains a summary of all the components in the Level 2 Architecture, organized by component ID. The table includes the component name and a description of what is accomplished by the device or system and how it connects to other components in the overall architecture. The component descriptions supplement the Level 2 Architecture diagrams included in Section 3.2 above.

Table 3–3: Summary of NG9-1-1 Components

ID #	Component Name	Description
LA-01	Central Office Telephony Gateway (IP <-> PSTN)	As part of the Legacy Access Network, the Central Office Telephony Gateway is used to transition IP-based calls to the Public Switched Telephone Network (PSTN). This component is located at a central office and is typically operated by a Local Exchange Carrier (LEC).
LA-02	Mobile Switching Center (MSC) Telephony Gateway (IP <-> Cell)	As part of the Legacy Access Network, the MSC Telephony Gateway (IP <-> Cell) switches IP-based call origination devices to traditional cellular service for routing through the MSC Switch (LA-04).
LA-03	Central Office Switch	As part of the Legacy Access Network, the Central Office Switch is the LEC facility where access lines are connected to switching equipment for dial tone and connectivity to the PSTN. For 9-1-1 calls, it serves as the connection point between call origination devices and a Selective Router (LA-05).
LA-04	MSC Switch	As part of the Legacy Access Network, the MSC is the wireless equivalent of a Central Office (LA-03), which provides switching functions for wireless (CMRS) calls.
LA-05	Emergency Services Gateway (ESGW)	As part of the Legacy Access Network, the ESGW provides connectivity from the Legacy 3rd Party Call Center (XS-01) directly to the Selective Router (LA-06). This gateway provides routing services for call centers to reach Legacy PSAPs (SS-03).
LA-06	Selective Router	As part of the Legacy Access Network, the Selective Router is used to distribute 9-1-1 calls to the appropriate PSAP
LA-07	Short Message Service (SMS) Gateway	As part of the Legacy Access Network, the SMS Gateway provides connectivity from the MSC Switch (LA-04) to a Telephony Gateway (NA-01) in the IP Access Network (SS-05). This gateway would forward SMS message traffic through the IP Access Network for routing to an NG9-1-1 PSAP (SS-07)
LB-01	Validation Database (VDB)	As a Legacy Database, the VDB contains geographic-based information that describes the current, valid civic address space defined by the Emergency Services Network Provider's Master Street Address Guide (MSAG). Both the Voice over IP (VoIP) Positioning Center (VPC) (LD-01) and the Mobile Positioning Center (MPC) (LD-02) use the VDB to ensure that the address exists.

ID #	Component Name	Description
LB-02	Emergency Routing Database (ERDB)	As a Legacy Database, the ERDB contains routing information associated with Emergency Service Zones (ESZ). It supports the boundary definitions for ESZs and the mapping of civic address or geospatial coordinate location information to a particular ESZ.
LB-03	Selective Router Database (SRDB)	As a Legacy Database, the SRDB is the routing table that contains telephone number-to-Emergency Service Number (ESN) relationships that determine the routing of 9-1-1 calls.
LD-01	VoIP Positioning Center (VPC)	As a Legacy Database Service, the VPC supports the routing of VoIP emergency calls. Using the Automatic Location Information (ALI) Database (NB-01), the VPC delivers location information as an ALI record. In addition, the VPC provides access to validation (VDB [LB-01]) and routing data (ERDB [LB-02]).
LD-02	Mobile Positioning Center (MPC)	As a Legacy Database Service, the MPC delivers mobile positioning data from the Position Determining Entity (PDE) to determine the geographic location of a wireless caller through the use of one or more position determining technologies. Using the ALI Database (NB-01), the MPC delivers location information as an ALI record. In addition, the MPC provides access to validation (VDB [LB-01]) and routing data (ERDB [LB-02]).
LD-03	Legacy Database Management System (DBMS)	As a Legacy Data Service, the Legacy DBMS is used to support requests from the Selective Router (LA-05) to the Selective Router DB (LB-03).
LO-01	Public Switched Telephone Network (PSTN) User Agent (UA) (non-IP)	As one of the Legacy Call Origination methods, the non-IP PSTN UA is most typically a telephone. This device is the beginning point for a “traditional” non-IP caller and the legacy call origination method for the vast majority of “traditional analog landline 9-1-1 calls.”
LO-02	Private Branch eXchange (PBX)	As one of the Legacy Call Origination methods, the PBX is frequently used in an office or building setting and supports telephone exchange features. This UA is the beginning point for a “traditional” non-IP caller who is calling through a non-IP PBX.
LO-03	Sensor User Agent (UA) (non-IP)	As one of the Legacy Call Origination methods, a non-IP Sensor UA forwards messages from sensor activations to PSAPs. When activated, sensors typically contact a PSAP and transmit an alarm number or code, which must be referenced to determine the alarm’s nature, location, and other important data. Alarms include police, fire, or emergency medical services, and could be monitored by a 3rd Party Call Center (XS-01). In legacy call origination, sensor data (when available) is transferred verbally to the PSAP.
LO-04	Wireless User Agent (UA) (non-IP)	As one of the Legacy Call Origination methods, the non-IP Wireless UA describes analog wireless phones that connect through an MSC (LA-04) or whose calls are converted to IP via a Telephony Gateway (NA-01). In legacy call origination, this was the primary method for wireless phones connecting to PSAPs in the pre-digital (pre-IP) age of wireless telephony. In addition, SMS message traffic that originates from a non-IP Wireless UA would be routed through an SMS Gateway (LA-07).

ID #	Component Name	Description
LO-05	Telematics User Agent (UA) (non-IP)	As one of the Legacy Call Origination methods, the non-IP Telematics UA, typically a motor vehicle, is equipped with a telecommunications device that can manually or automatically contact a 3rd Party Call Center (XS-01). When a vehicle contacts the call center, it can potentially open a voice and/or data communications channel. The vehicle can typically transmit data from an onboard Automatic Collision Notification (ACN) device, which can include the Global Positioning System (GPS) location of the vehicle and crash-related data, including speed, delta velocity, number of occupants, and rollover data. The 3rd Party Call Center must determine the location of the vehicle and which PSAP is geographically responsible for that location before contacting a PSAP. The data gathered from the ACN device must be transmitted verbally from the call center to the PSAP.
LP-01	Telephony Switch/Automatic Call Distribution (ACD)	As a feature within the Legacy (E9-1-1) PSAP, the Telephony Switch/ACD device is connected to the Selective Router (LA-05) and accepts inbound 9-1-1 calls for the Legacy (E9-1-1) PSAP. In addition, the ACD device is responsible for the distribution of calls to call takers within a PSAP. The ACD device within a Legacy PSAP typically uses the longest time idle to determine to which call taker a call should be routed.
LP-02	E9-1-1 Call Termination	As a feature within the Legacy (E9-1-1) PSAP, the E9-1-1 Call Termination is a phone-based system used to connect the caller to the call taker. In a Legacy PSAP, the call taker can process voice calls using a phone, and deaf/hearing-impaired ,callers use a Teletype/Telecommunications Device for the Deaf (TTY/TDD). Automatic Number Identification (ANI)/ALI is displayed to the call taker, and a tactical map display can be used to graphically display the caller's location. In addition, the E9-1-1 Call Termination device provides standard telephony features, including hold, conference, transfer, redial, etc.
LP-03	Call Record	As a feature within the Legacy (E9-1-1) PSAP, the Call Record is a text-based log of incoming call information for the PSAP (SS-03). The Call Record is used to support subsequent queries for data to determine how a particular call was handled and is considered a legal record.
LP-04	Short-Term Voice Record	As a feature within the Legacy (E9-1-1) PSAP, the Short-Term Voice Record provides an audio recording of the telephone call received by the PSAP, and the call taker can retrieve the recording for a call within the very recent past.
LP-05	Geographic Information System (GIS)	As a feature within the Legacy (E9-1-1) PSAP, the GIS supports the creation, storage, management, and retrieval of geographic-based data. The primary source of GIS data is a base GIS, which is outside the boundary of the Legacy (E9-1-1) PSAP.
NA-01	Telephony Gateway (PSTN <-> IP)	As part of the NG9-1-1 Access (IP) Network, the Telephony Gateway (PSTN <-> IP) is used to convert non-IP PSTN calls to IP-based calls and to access IP-based networks. This device is typically operated by the LEC and is generally used in the daily delivery of telephony services on an IP-based network.

ID #	Component Name	Description
NA-02	Access Border Control Function (BCF)	As part of the NG9-1-1 Access (IP) Network, the Access BCF is used as the gateway from IP Call Origination Devices (SS-04) to the IP Access Network (SS-05) and acts as a policy-based firewall and packet-scanning device.
NA-03	IP Routing Function	As part of the NG9-1-1 Access (IP) Network, the IP Routing Function device is the conduit between the Access BCF (NA-02) and the Call Proxy/Redirect Server (NA-04). Using IP-based routing rules and technology, calls are transmitted to an appropriate server for routing purposes.
NA-04	Call Proxy or Redirect Server	As part of the NG9-1-1 Access (IP) Network, the Call Proxy or Redirect Server uses an Emergency Call Routing Function (ECRF) and a Location to Service Translation (LoST) database to take the caller's location and determine the routing path to the NG9-1-1 Network (SS-06).
NA-05	Legacy PSAP Gateway	As part of the NG9-1-1 Access (IP) Network, the E9-1-1 Gateway is used to take calls from the IP Access Network (SS-05) and forward them to a Legacy (E9-1-1) PSAP (SS-03).
NA-06	Provider Location Information Server (LIS)	As part of the NG9-1-1 Access (IP) Network, the Provider LIS delivers location information that is passed along with the 9-1-1 call to provide the Call Proxy with a caller's location to make routing decisions.
NB-01	Automatic Location Information (ALI)	As an NG9-1-1 database, the ALI database contains the address/location of the telephone and supplementary emergency service information related to the caller's telephone number. The database uses the ANI as the key to each ALI record.
NB-02	Emergency Provider Access Directory (EPAD)	As an NG9-1-1 Database, the EPAD is a GIS-enabled database registry of local, state, and federal emergency authorities and public service providers. The database will be used to provide connection methods and details to NG9-1-1 to establish direct communications with emergency providers and responders.
NB-03	Location to Service Translation (LoST)	As an NG9-1-1 data source, the LoST protocol is used to map location and service names to service location and obtain associated information. LoST mapping queries can contain either civic or geodetic location information. The LoST protocol has been defined by the Internet Engineering Task Force (IETF), Emergency Context Resolution with Internet Technologies (ECRIT) working group.
NB-04	Business Rules	As an NG9-1-1 database, the Business Rules provide the NG9-1-1 System with a series of rule sets that determine how data should be displayed within the system, how the system determines routing, and how the system should respond when particular situations arise. The Business Rules are activated by various activities within the NG9-1-1.
NB-05	Call Record	As an NG9-1-1 database, the Call Record stores all call recordings and call detail records. The Call Record is used to support subsequent queries for data to determine how a particular call was handled and is considered a legal record.

ID #	Component Name	Description
NB-06	Data Rights	As an NG9-1-1 database, the Data Rights database provides the rules and methods of handing inbound requests for data.
NB-07	Credentials/Authorizations/ Policies	As an NG9-1-1 database, the Credentials/Authorizations/ Policies provide the system Identity and Access Management (IdAM) information that will be the authoritative data set used to manage authentication and authorization for the NG9-1-1 System.
ND-01	NG9-1-1 Database Management System (DBMS)	As an NG9-1-1 Data Service, the NG9-1-1 DBMS acts as the overall umbrella for each of the NG9-1-1 databases within the system, and it controls the creation, storage, management, and retrieval of data. The DBMS is the connection point between NG9-1-1 and the various sources of data used in the daily operation of the system.
ND-02	Identity and Access Management (IdAM)	As an NG9-1-1 Data Service, the IdAM service defines how identities and the management of those identities provide the authority for the NG-9-1-1 community to share information in a manner that maximizes desired information confidentiality, integrity, authenticity, and non-repudiation.
ND-03	NG9-1-1 Database Management System (DBMS) Administration	As an NG9-1-1 Data Service, the NG9-1-1 DBMS Administration service determines how the DBMS will be managed within the NG9-1-1 System.
ND-04	NG9-1-1 Identity and Access Management (IdAM) Administration	As an NG9-1-1 Data Service, the NG9-1-1 IdAM Administration service determines how IdAM will be managed within the NG9-1-1 System.
NN-01	Selective Router Gateway	As a feature within the NG9-1-1 Network, the Selective Router Gateway is used to connect the legacy Selective Router (LA-05) to the NG9-1-1 network. This gateway will be required to support translation and communications between the Legacy Access Network (SS-02) and the NG9-1-1 Network (SS-06) during the transition to NG9-1-1.
NN-02	Legacy PSAP Gateway	As a feature within the NG9-1-1 Network, the Legacy PSAP Gateway is used to connect the Legacy (E9-1-1) PSAP (SS-03) to the NG9-1-1 Network (SS-06). This gateway will be required to support translation and communications between the Legacy PSAPs and NG9-1-1 during the transition to NG9-1-1.
NN-03	Legacy Responder Gateway	As a feature within the NG9-1-1 Network, the Legacy Responder Gateway is used to connect the Legacy Responders (XS-02) to the NG9-1-1 Network (SS-06). This gateway will be required to support translation and communications between these entities during the transition to NG9-1-1.
NN-04	Emergency Services Routing Proxy (ESRP)	As a feature within the NG9-1-1 Network, the ESRP is used to provide a communications link between Legacy PSAPs (NN-02) and Responders (NN-03) to the NG9-1-1 IP Routing (NN-05) and the NG9-1-1 network IP ACD (NN-06) device. The ESRP will route traffic primarily from legacy services to the NG9-1-1 PSAP (SS-07).

ID #	Component Name	Description
NN-05	NG9-1-1 IP Routing Function	As a feature within the NG9-1-1 Network, the NG9-1-1 IP Routing Function is the main routing function within the NG9-1-1 network. The device supports inbound calls and requests that originate via the IP Network BCF (NN-07), the PSAP BCF (NN-08), or the ESRP (NN-04), and determines the appropriate destination. In addition, the NG9-1-1 IP Routing Function device acts as the conduit for Legacy Database Services (SS-08) and NG9-1-1 Database Services (SS-09).
NN-06	IP Automatic Call Distribution (ACD)	As a feature within the NG9-1-1 Network, the IP ACD device is responsible for the distribution of calls within the network. The ACD device uses various rules to determine how the call should be routed to a PSAP. The NG9-1-1 network's IP ACD device provides the conduit between the ESRP (NN-04) to the PSAP BCF (NN-08).
NN-07	IP Network Border Control Function (BCF)	As a feature within the NG9-1-1 Network, the IP Network BCF is the primary gateway for the IP Access Network (SS-05) and provides security and firewall functions to protect the integrity of the NG9-1-1 Network (SS-06). In addition, the IP Network BCF is the only connection from NG9-1-1 to the Internet (WWW) and provides access to public web and media services.
NN-08	PSAP Border Control Function (BCF)	As a feature within the NG9-1-1 Network, the PSAP BCF is the gateway between the NG9-1-1 Network (SS-06) and the NG9-1-1 PSAPs (SS-07). In addition, The PSAP BCF provides security and firewall functions to protect the integrity of the NG9-1-1 Network (SS-06) and is the connectivity to the NG Emergency Services Network (ESNet) (ES-01).
NN-09	Legacy Data Gateway	As a feature within the NG9-1-1 Network, the Legacy Data Gateway provides the NG9-1-1 System with access to Legacy Database Services (SS-08), in particular the VPC (LD-01), the MPC (LD-02) and the ALI (NB-01).
NO-01	IP User Agent (UA)	As one of the IP Call Origination methods, the IP UA is a device capable of initiating a 9-1-1 call via an IP-based device (IP phone) typically using a software application. A Vo IP provider is an example of an IP UA.
NO-02	Enterprise Location Information Server (LIS)	As part of the IP Call Origination methods, the Enterprise LIS supports location determination for an IP-based Private Branch eXchange (IPBX) (NO-03). When a 9-1-1 call is made through an IPBX, the Enterprise LIS provides location information that is passed along with the 9-1-1 call to provide the PSAP with a caller's location.
NO-03	IP-based Private Branch eXchange (IPBX)	As one of the IP Call Origination methods, the IPBX is frequently used in an office or building setting and supports telephone exchange features. As an IPBX, the system can transmit additional data to the NG9-1-1 (such as caller's location) that can be used by the system to enhance the delivery (routing) or processing of the call.

ID #	Component Name	Description
NO-04	Sensor Device	As one of the IP Call Origination methods, an IP-based sensor device forwards messages from sensor activations to PSAPs either directly or through an IP-based 3rd Party Call Center (XS-05). When activated, IP-based sensors will use the routing features of the NG9-1-1 to determine the most appropriate PSAP for the sensor location and can transmit supplemental and supportive caller data to the PSAP automatically and electronically. This additional data can be used by the system to enhance the delivery (routing) or processing of the sensor activation.
NO-05	Telematics User Agent (UA)	As one of the IP Call Origination methods, the Telematics UA is an IP-based device, typically a motor vehicle, equipped with a telecommunications device that can manually or automatically contact a PSAP either directly or via a 3rd Party Call Center (XS-01). When a vehicle contacts a PSAP, it can potentially open a voice and/or data communications channel. The vehicle will transmit data from an onboard ACN device, which can include the GPS location of the vehicle and crash-related data, including: speed, delta velocity, number of occupants, and rollover data.
NO-06	Wireless User Agent (UA) (IP-Enabled)	As one of the IP Call Origination methods, an IP-Enabled Wireless UA describes digital (IP-based) wireless phones that connect to an IP Access Network (SS-05) for telephony services. The vast majority of today's wireless (CMRS) call origination is performed via an IP-based wireless UA. To access a Legacy (E9-1-1) PSAP (SS-03), the call is connected via an MSC Telephony Gateway (LA-02) and through the Legacy Access Network (SS-02).
NP-01	NG9-1-1 Border Control Function (BCF)	As a feature within the NG9-1-1 PSAP, the NG9-1-1 BCF is the gateway from the PSAP BCF (NN-08) to the NG9-1-1 PSAP. The NG9-1-1 BCF is the gateway from the PSAP to the network and provides security and firewall functions.
NP-02	PSAP IP Routing Function	As a feature within the NG9-1-1 PSAP, the PSAP IP Routing Function device supports distribution of calls from the NG9-1-1 BCF (NP-01) to both the PSAP IP ACD (NP-03) device and the NG9-1-1 Call Termination (NP-04). The PSAP IP Routing Function can bypass the PSAP IP ACD device, in particular for the distribution of IP-based media streams.
NP-03	PSAP IP Automatic Call Distribution (ACD)	As a feature within the NG9-1-1 PSAP, the PSAP IP ACD device is responsible for the distribution of calls to call takers within a PSAP. The ACD device uses various rules to determine to which call taker a call should be routed, including longest time idle, language ability, or special training. Many ACD devices will include a reporting system to provide detailed information about call metrics within the PSAP, including call volume, wait time, and system/call taker performance.

ID #	Component Name	Description
NP-04	NG9-1-1 Call Termination	As a feature within the NG9-1-1 PSAP, the NG9-1-1 Call Termination is a multimedia, IP-based system used to connect the caller to the call taker. In NG9-1-1, the call taker can process voice callers, deaf/hearing-impaired callers, and input from sensors, telematics, and text devices. Essential, supportive, and supplemental data is displayed to the call taker and is used to enhance call processing and decision making by the call taker. In addition, a tactical map display can be used to graphically display the caller's location automatically, using the location data as provided in the call stream. The NG9-1-1 Call Termination device provides standard telephony features, including hold, conference, transfer, redial, etc.
NP-05	Call Record	As a feature within the NG9-1-1 PSAP, the Call Record is used to record both the Call Recording (real-time communications) and the Call Detail Record (call stream and other data).
NP-06	Geographic Information System (GIS)	As a feature within the NG9-1-1 PSAP, the GIS supports the creation, storage, management, and retrieval of geographic-based data. The primary source of GIS data is a base GIS, which is outside the boundary of the NG9-1-1 System.
XD-01	Master Street Address Guide (MSAG)	As an external database, the MSAG is a geographically based database of street names and address ranges to associate addresses with ESNets to enable proper routing of 9-1-1 calls.
XD-02	Base Geographic Information System (GIS)	As an external database, the Base GIS is the primary source of geographic-based data for the NG9-1-1 PSAP (SS-07).
XD-03	Base Geographic Information System (GIS)	As an external database, the Base GIS is the primary source of geographic-based data for the Legacy (E9-1-1) PSAP (SS-03).
XS-01	Legacy 3rd Party Call Center	As an external system, a 3rd Party Call Center is used generically to indicate those services that are important to the receipt, delivery, and response to 9-1-1 calls, but are outside the boundaries of NG9-1-1. Examples of 3rd Party Call Centers include telematics service providers, poison control, suicide prevention, N-1-1, and video relay/language translation services. Legacy 3rd Party Call Centers are those that have not transitioned to IP connectivity to NG9-1-1 and will typically use voice communications to contact PSAPs and pass along data about their callers.
XS-02	Legacy Responders	As an external system, Legacy Responders include public safety dispatchers and dispatch systems, emergency and supporting responders, and governmental and non-governmental agencies. Legacy Responders are those that use systems that have not transitioned to IP connectivity and typically are contacted via voice (telephone or radio) to receive information from NG9-1-1.

ID #	Component Name	Description
XS-03	IP-Enabled Responders	As an external system, IP-Enabled Responders include public safety dispatchers and dispatch systems, emergency and supporting responders, and governmental and non-governmental agencies. IP-Enabled Responders are those that use systems that have transitioned to IP connectivity and can receive NG9-1-1 data automatically and electronically, with or without voice communications.
XS-04	Public Safety Entity	Public Safety Entities include agencies or services that are connected directly to the NG ESNet (ES-01). These agencies or services may provide supportive or supplemental data related to a call.
XS-05	Credential Services	As an external system, the Credential Services is the authoritative source of digital certificates and is used by the IdAM data service (ND-02) to support the credentialing and authority verification process within NG9-1-1.
XS-06	IP-Enabled 3rd Party Call Center	As an external system, an IP-Enabled 3rd Party Call Center is generically used to indicate those services that are important to the receipt, delivery, and response to 9-1-1 calls, but that are outside the boundaries of NG9-1-1. Examples of 3rd Party Call Centers include telematics service providers, poison control, suicide prevention, N-1-1, and video relay/language translation services. IP-Enabled 3rd Party Call Centers are those that have transitioned to IP connectivity to NG9-1-1 and will typically use voice and data communications to contact PSAPs. IP-enabled centers surpass the capabilities of Legacy 3rd Party Call Centers because they use the routing features of NG9-1-1 to determine the most appropriate PSAP for their caller's location and can transmit supplemental and supportive caller data to the PSAP automatically and electronically.
XS-07	Position Determining Entity (PDE)	As an external system, the PDE determines the geographic location of a wireless (CMRS) caller through the use of one or more position determining technologies. Note: PDE is also known as Location Determination Technology (LDT).
XS-08	Location-to-Service Translation (LoST) Server	The Location-to-Service Translation Protocol (LoST) Server describes a concept by which the LoST protocol is leveraged to map service identifiers and geospatial or civic location information to service contact Uniform Resource Locators (URLs). Many LoST servers would likely exist, and IP Access Networks (SS-05) and NG9-1-1 Networks (SS-06) would use the LoST data as a method to identify appropriate routing of calls based on the caller's location.

3.2.2 Interfaces

Table 3-4 below contains a summary of all the interfaces in the Level 2 Architecture, organized by interface ID. The table includes the from and to component names, the interface name, and a description of the interface. The interface description identifies which two systems are being connected and what is accomplished by the interface. The system descriptions supplement the Level 2 Architecture diagrams included in Section 3.2 above.

Table 3–4: Summary of NG9-1-1 Detailed Interfaces

ID #	From	To	Interface/System Name	Description
IA-01	NA-02	NA-03	Access BCF—IP Routing Function	The Access Border Control Function (BCF) interfaces with the IP Routing Function device to deliver all calls received from IP Call Origination (SS-04) for routing purposes.
IA-02	NA-02	NA-03	Access BCF—IP Routing Function	The BCF interfaces with the IP Routing Function device to deliver all IP media streams received from IP Call Origination (SS-04) for routing purposes.
IA-03	NA-01	NA-02	Telephony Gateway (PSTN <-> IP)—Access BCF	The Telephony Gateway (PSTN <-> IP) interface with the BCF provides the communications link from those IP media streams converted from the Public Switched Telephone Network (PSTN) to IP to the Access BCF for routing purposes.
IA-04	NA-01	NA-02	Telephony Gateway (PSTN <-> IP)—Access BCF	The Telephony Gateway (PSTN <-> IP) interface with the BCF provides the communications link from those calls converted from PSTN to IP to the Access BCF for routing purposes.
IA-05	NA-03	NA-03	IP Routing Function—IP Routing Function	The IP Routing Function device is connected to other IP Routing Function devices to transport data across multiple IP Access Networks.
IA-06	NA-03	NN-07	IP Routing Function—IP Network BCF	The interface between the IP Routing Function device and the IP Network BCF serves as the conduit for IP media streams to access the NG9-1-1 Network (SS-06) directly.
IA-07	NA-03	NA-04	IP Routing Function—Call Proxy or Redirect Server	The IP Routing Function device interfaces with the Call Proxy or Redirect Server to support routing of calls based on the Emergency Call Routing Function (ECRF) and Location to Service Translation (LoST) database functions of the redirect server. This acts as the conduit from the IP Access Network (SS-05) to the NG9-1-1 Network (SS-06).
IA-08	NA-04	NN-07	Call Proxy or Redirect Server—IP Network BCF	The interface between the Call Proxy or Redirect Server and the IP Network BCF is the main connection between the IP Access Network (SS-05) and the NG9-1-1 Network (SS-06) and is used to transport IP-based emergency calls to the NG9-1-1 System.

ID #	From	To	Interface/System Name	Description
IA-09	NA-04	NA-05	Call Proxy or Redirect Server—Legacy PSAP Gateway	The Call Proxy or Redirect Server interfaces with a legacy E9-1-1 Gateway to support connectivity between the IP Access Network (SS-05) and the Legacy (E9-1-1) PSAP (SS-03).
IA-10	NA-04	NA-04	Call Proxy or Redirect Server—Call Proxy or Redirect Server	The Call Proxy or Redirect Server interfaces with other Call Proxy or Redirect Servers to transport data across multiple IP Access Networks.
IA-11	NA-04	LA-01	Call Proxy or Redirect Server—Central Office Telephony Gateway (IP <-> PSTN)	The Call Proxy or Redirect Server interfaces with the Central Office Telephony Gateway (IP <-> PSTN) to support routing of calls from the IP Access Network (SS-05) to the Legacy Access Network (SS-02). This connection typically supports Voice over IP (VoIP) calls being directed to Legacy (E9-1-1) PSAPs (SS-03) via a Selective Router (LA-06).
IA-12	NA-04	NA-06	Call Proxy or Redirect Server—Provider LIS	The Call Proxy or Redirect Server interfaces with a Provider Location Information Server (LIS) to provide location information to make routing decisions.
IA-13	NA-03	LA-01	IP Routing Function— Central Office Telephony Gateway (IP <-> PSTN)	The IP Routing Function interfaces with the Central Office Telephony Gateway (IP <-> PSTN) to support routing of IP media streams from the IP Access Network (SS-05) to the Legacy Access Network (SS-02). This connection typically supports VoIP calls being directed to Legacy (E9-1-1) PSAPs (SS-03) via a Selective Router (LA-06).
IA-14	NA-03	LA-01	IP Routing Function— Central Office Telephony Gateway (IP <-> PSTN)	The IP Routing Function interfaces with the Central Office Telephony Gateway (IP <-> PSTN) to support routing of calls from the IP Access Network (SS-05) to the Legacy Access Network (SS-02). This connection typically supports VoIP calls being directed to Legacy (E9-1-1) PSAPs (SS-03) via a Selective Router (LA-06). This differs from interface IA-11 for those calls that are not routed through a Call Proxy or Redirect Server (NA-04).
IC-01	LD-01	LB-01	VPC—VDB	The VoIP Positioning Center (VPC) interfaces with the Validation Database (VDB) to confirm that a VoIP location has a valid format.
IC-02	LD-01	LB-02	VPC—ERDB	The VPC interfaces with the Emergency Routing DB (ERDB) to determine the appropriate routing for an emergency VoIP call.
IC-03	LD-02	LB-01	MPC—VDB	The Mobile Positioning Center (MPC) interfaces with the VDB to confirm that a mobile location has a valid format.
IC-04	LD-02	LB-02	MPC—ERDB	The MPC interfaces with the ERDB to determine the appropriate routing for an emergency MPC call.
IC-05	LD-03	LB-03	Legacy DBMS—SRDB	The interface provides access from the Legacy Database Management System (DBMS) to the Selective Router DB (SRDB) data.

ID #	From	To	Interface/System Name	Description
IC-06	LA-04	LD-02	MSC Switch—MPC	The MSC Switch interfaces with an MPC to make requests for caller's location and to receive updated location information that will determine call routing.
IC-07	NA-04	LD-01	Call Proxy or Redirect Server—VPC	The Call Proxy or Redirect Server interfaces with a VPC to receive location information for VoIP callers.
IC-08	LD-02	NN-05	MPC—NG9-1-1 IP Routing Function	The MPC interfaces with an NG9-1-1 IP Routing Function device to transmit mobile caller's location to the NG9-1-1 System to assist in call routing. When a direct interface is made (rather than through a Legacy Data Gateway [NN-09]), the MPC has been enhanced to support communications directly with the NG9-1-1 network and does not require translation.
IC-09	LD-02	NN-09	MPC—Legacy Data Gateway	The MPC interfaces with the Legacy Data Gateway to transmit the mobile caller's location to the NG9-1-1 System to assist in call routing. When interfacing through a Legacy Data Gateway, the MPC has not been enhanced to support communications directly with the NG9-1-1 Network (SS-06) and requires translation.
IC-10	LD-01	NN-05	VPC—NG9-1-1 IP Routing Function	The VPC interfaces with an NG9-1-1 IP Routing Function device to transmit a VoIP caller's location to the NG9-1-1 System to assist in call routing. When a direct interface is made (rather than through a Legacy Data Gateway [NN-09]), the VPC has been enhanced to support communications directly with the NG9-1-1 network and does not require translation.
IC-11	LD-01	NN-09	VPC—Legacy Data Gateway	The VPC interfaces with the Legacy Data Gateway to transmit a VoIP caller's location to the NG9-1-1 System to assist in call routing. When interfacing through a Legacy Data Gateway, the VPC has not been enhanced to support communications directly with the NG9-1-1 Network (SS-06) and requires translation.
ID-01	LA-05	ND-01	Selective Router—NG9-1-1 Database Management System (DBMS)	The Selective Router interfaces with a DBMS to access the SRDB.
ID-02	LP-01	NB-01	Telephony Switch/ ACD—ALI	The Legacy (E9-1-1) PSAP Telephony Switch/ Automatic Call Distribution (ACD) device interfaces with the Automatic Location Information (ALI) database to query location information based on the provided Automatic Number Identification (ANI).
ID-03	LD-02	NB-01	MPC—ALI	The MPC interfaces with the ALI database to provide location data for mobile callers.
ID-04	LD-01	NB-01	VPC—ALI	The VPC interfaces with the ALI database to provide location data for VoIP callers.

ID #	From	To	Interface/System Name	Description
ID-05	NO-02	ND-01	Enterprise LIS—NG9-1-1 Database Management System (DBMS)	The Enterprise LIS connects to the NG9-1-1 DBMS to provide access to the ALI database for location determination when using an IP-based Private Branch eXchange (IPBX) (NO-03). Typically, the Enterprise LIS is managed by a company running an IP-based PBX or its vendor to contain and support location identification provision for Enterprise devices.
ID-06	NA-06	ND-01	Provider LIS—NG9-1-1 Database Management System (DBMS)	The Provider LIS connects to the NG9-1-1 DBMS to provide access to the ALI database for location determination.
ID-07	NA-04	ND-01	Call Proxy or Redirect Server—NG9-1-1 Database Management System (DBMS)	The Call Proxy or Redirect Server interfaces with the NG9-1-1 DBMS to provide access to the LoST DB.
ID-08	NN-09	NB-01	Legacy Data Gateway—ALI	The interface between the Legacy Data Gateway and the ALI database provides access for the NG9-1-1 Network (SS-06) to caller location information.
ID-09	NN-05	ND-01	NG9-1-1 IP Routing Function—NG9-1-1 Database Management System (DBMS)	The NG9-1-1 IP Routing Function device interfaces with the NG9-1-1 DBMS to provide access for the NG9-1-1 Databases and Database Services.
ID-10	NN-05	ND-02	NG9-1-1 IP Routing Function—IdAM	The NG9-1-1 IP Routing Function device interfaces with the Identity and Access Management (IdAM) data service to support the credentialing and authority verification process within the NG9-1-1 Network (SS-06).
ID-11	ND-02	ND-04	IdAM—NG9-1-1 IdAM Administration	The IdAM data service interfaces with the NG9-1-1 IdAM Administration data service for management of the IdAM data service.
ID-12	ND-01	ND-03	NG9-1-1 Database Management System (DBMS)—NG9-1-1 DBMS Administration	The NG9-1-1 DBMS data service interfaces with the NG9-1-1 DBMS Administration data service for management of the DBMS.
ID-51	ND-01	NB-01	NG9-1-1 Database Management System (DBMS)—ALI	The NG9-1-1 DBMS interfaces with the ALI DB to provide the NG9-1-1 DBMS with access to ALI data.
ID-52	ND-01	NB-02	NG9-1-1 Database Management System (DBMS)—EPAD	The NG9-1-1 DBMS interfaces with the Emergency Provider Access Directory (EPAD) to provide the NG9-1-1 DBMS with access to EPAD data.
ID-53	ND-01	NB-03	NG9-1-1 Database Management System (DBMS)—LoST	The NG9-1-1 DBMS interfaces with the LoST DB to provide the NG9-1-1 DBMS with access to LoST data.
ID-54	ND-01	NB-04	NG9-1-1 Database Management System (DBMS)—Business Rules	The NG9-1-1 DBMS interfaces with the Business Rules DB to provide the NG9-1-1 DBMS with access to the Business Rules.
ID-55	ND-01	NB-05	NG9-1-1 Database Management System (DBMS)—Call Record	The NG9-1-1 DBMS interfaces with the Call Record DB to provide the NG9-1-1 DBMS with access to the Call Records.

ID #	From	To	Interface/System Name	Description
ID-56	ND-01	NB-06	NG9-1-1 Database Management System (DBMS)—Data Rights	The NG9-1-1 DBMS interfaces with the Data Rights Database to provide the NG9-1-1 DBMS with access to Data Rights.
ID-57	ND-02	NB-07	IdAM—Credentials/ Authorizations/ Policies	The IdAM NG9-1-1 Data Service interfaces with Credentials/Authorizations/ Policies database to provide the system information that will be the authoritative data set used to manage the authentication and authorization for the NG9-1-1 System.
IE-01	LP-01		Telephony Switch/ ACD—Legacy PSAP	The Telephony Switch/ACD device interfaces with additional multiple legacy PSAPs to provide access from one legacy PSAP to another for transfer of calls (when one PSAP is connected to another PSAP's ACD device).
IE-02	LP-01	LP-02	Telephony Switch/ ACD—E9-1-1 Call Termination	The Telephony Switch/ACD device interfaces with the E9-1-1 Call Termination to support distribution and delivery of calls to call takers.
IE-03	LP-01	LP-03	Telephony Switch / ACD—Call Record	The E9-1-1 Call Termination interfaces with the Call Record to store details about the caller, in particular ALI, call taker workstation, etc.
IE-04	LP-02	LP-04	E9-1-1 Call Termination—Short Term Voice Record	The E9-1-1 Call Termination interfaces with the Call Record to record the audio portion of a Legacy 9-1-1 call.
IE-05	LP-02	LP-05	E9-1-1 Call Termination—GIS	The E9-1-1 Call Termination interfaces with the Geographic Information System (GIS) to obtain geographic information for use in location determination and to update local files, mapping software, etc.
IE-06	NA-05	LP-01	Legacy PSAP Gateway—Telephony Switch / ACD	The E9-1-1 Gateway interfaces with the Legacy (E9-1-1) PSAP Telephony Switch/ACD device to provide access for the Legacy PSAP (SS-03) to the IP Access Network (SS-05).
II-01	NO-01	LA-01	IP UA—Central Office Telephony Gateway (IP <-> PSTN)	The IP User Agent (UA), an IP-based telephone (like VoIP), interfaces with a Central Office Telephony Gateway and converts the IP-based media stream to the a PSTN media stream for purposes of accessing the Legacy Access Network (SS-02).
II-02	NO-01	LA-01	IP UA—Central Office Telephony Gateway (IP <-> PSTN)	The IP UA, an IP-based telephone (like VoIP), interfaces with a Central Office Telephony Gateway and converts the IP-based call to a PSTN media stream for purposes of accessing the Legacy Access Network (SS-02). Note: access for the IP UA would be provided through an IP access network, but is not shown in this architecture diagram because it is not relevant to the overall architecture analysis.
II-03	NO-01	NA-02	IP UA—Access BCF	The IP UA, an IP-based telephone (like VoIP), interfaces with the IP Access Network (SS-05) to deliver an IP media stream through the Access BCF.
II-04	NO-01	NA-02	IP UA—Access BCF	The IP UA, an IP-based telephone (like VoIP), interfaces with the IP Access Network (SS-05) to deliver a call through the Access BCF. This is one method for a VoIP call to access an IP-based telephony network.

ID #	From	To	Interface/System Name	Description
II-05	NO-01	NO-03	IP UA—IPBX	The IP UA, an IP-based telephone (like VoIP), interfaces with an IPBX to access telephony exchange functions and deliver a call to the IPBX.
II-06	NO-01	NO-03	IP UA—IPBX	The IP UA, an IP-based telephone (like VoIP), interfaces with an IPBX to access telephony exchange functions and deliver an IP media stream to the IPBX.
II-07	NO-03	LA-01	IPBX—Central Office Telephony Gateway (IP <-> PSTN)	The IPBX interfaces with a Central Office Telephony Gateway to convert IP media streams to PSTN media streams and to access traditional PSTNs. The interface supports IP-based media streams that are converted for a non-IP (PSTN) network via a telephone gateway.
II-08	NO-03	LA-01	IPBX—Central Office Telephony Gateway (IP <-> PSTN)	The IPBX interfaces with a Central Office Telephony Gateway to convert IP-based calls to PSTN calls and to access traditional PSTN networks. The interface supports IP-based calls that are converted to non-IP (PSTN) calls via a telephone gateway.
II-09	NO-03	NA-02	IPBX—Access BCF	The IPBX interfaces with the Access BCF to deliver IP media streams to the IP Access Network (SS-05).
II-10	NO-03	NA-02	IPBX—Access BCF	The IP-based IPBX interfaces with the Access BCF to deliver calls to the IP Access Network (SS-05). The IPBX can transmit additional data to the NG9-1-1 (such as caller's location) that can be used by the system to enhance the delivery (routing) or processing of the call.
II-11	NO-02	NO-03	Enterprise LIS—IPBX	The Enterprise LIS interfaces to an IPBX to provide location determination data that is passed, along with the 9-1-1 call, to provide the PSAP with a caller's location.
II-12	NO-04	NA-02	Sensor Device—Access BCF	The Sensor Device interfaces with the Access BCF to deliver sensor activations to the IP Access Network (SS-05). This interface is the beginning point for an IP-based sensor to access a system to deliver its sensor data or message over IP.
II-13	NO-04	LA-01	Sensor Device—Central Office Telephony Gateway (IP <-> PSTN)	The Sensor Device interfaces with the Central Office Telephony Gateway (IP <-> PSTN) to convert IP-based sensor data or messages to PSTN data or messages via the Legacy Access Network (SS-02). This interface is the beginning point for an IP-based sensor when accessing the legacy systems to deliver its sensor data or message. This is one method for IP-based sensors to access a Legacy (E9-1-1) PSAP (SS-03), by connecting through a telephone gateway.
II-14	NO-05	NA-02	Telematics UA—Access BCF	The IP-based Telematics UA interfaces with the IP Access Network (SS-05) via the Access BCF to directly connect the IP Access Network to ultimately deliver data to a PSAP.

ID #	From	To	Interface/System Name	Description
II-15	NO-05	LA-01	Telematics UA—Central Office Telephony Gateway (IP <-> PSTN)	The Telematics UA interfaces with the Central Office Telephony Gateway (IP <-> PSTN) to convert the output of an IP-based telematics device to PSTN output.
II-16	NO-06	NA-02	Wireless UA (IP-Enabled)—Access BCF	The IP-based Wireless UA interfaces with the Access BCF to deliver IP-based media streams to the IP Access Network (SS-05). This interface is the method by which the majority of digital wireless (CMRS) callers access their provider network.
II-17	NO-06	NA-02	Wireless UA (IP-Enabled)—Access BCF	The IP-based Wireless UA interfaces with the Access BCF to deliver IP-based calls to the IP Access Network (SS-05). This interface is the method by which the majority of digital wireless (CMRS) callers access their provider network.
II-18	NO-06	LA-02	Wireless UA (IP-Enabled)—MSC Telephony Gateway (IP <-> Cell)	The Wireless UA interfaces with the Mobile Switching Center (MSC) Telephony Gateway (IP <-> Cell) to convert the IP-based media streams for the Legacy Access Network (SS-02).
II-19	NO-06	LA-02	Wireless UA (IP-Enabled)—MSC Telephony Gateway (IP <-> Cell)	The Wireless UA interfaces with the MSC Telephony Gateway (IP <-> Cell) to convert the IP-based call for the Legacy Access Network (SS-02).
IN-01	NN-01	NN-07	Selective Router Gateway—IP Network BCF	The Selective Router Gateway interfaces with the IP Network BCF to translate calls from the Legacy Access Network (SS-02) to the NG9-1-1 Network (SS-06) via a gateway.
IN-02	NN-02	NN-05	Legacy PSAP Gateway—NG9-1-1 IP Routing Function	The Legacy PSAP Gateway interfaces with the NG9-1-1 IP Routing Function device to translate and deliver connectivity between the Legacy (E9-1-1) PSAPs (SS-03) and the NG9-1-1 Network (SS-06).
IN-03	NN-02	NN-04	Legacy PSAP Gateway—ESRP (Emergency Service Routing Proxy)	The Legacy PSAP Gateway interfaces with the Emergency Service Routing Proxy (ESRP) to support connectivity between the Legacy (E9-1-1) PSAPs (SS-03) and the NG9-1-1 Network (SS-06) for routing purposes.
IN-04	LP-01	NN-02	Telephony Switch/ ACD—Legacy PSAP Gateway	The Telephony Switch/ACD device interfaces with the Legacy PSAP Gateway to support translation and connectivity between the Legacy (E9-1-1) PSAPs (SS-03) and the NG9-1-1 Network (SS-06).
IN-05	NN-02	NN-03	Legacy PSAP Gateway—Legacy Responder Gateway	The Legacy PSAP Gateway interfaces to the Legacy Responder Gateway to provide connectivity from Legacy Responders (XS-02) to the Legacy (E9-1-1) PSAP (SS-03) via the NG9-1-1 Network (SS-06). Not all Legacy Responders will have direct access to their Legacy PSAPs and can use the NG9-1-1 Network as a conduit.
IN-06	NN-03	NN-04	Legacy Responder Gateway—ESRP (Emergency Service Routing Proxy)	The Legacy Responder Gateway interfaces to the ESRP for routing purposes. The ESRP will take data bound for the Legacy Responders, determine the routing, and deliver the information.

ID #	From	To	Interface/System Name	Description
IN-07	NN-03	NN-05	Legacy Responder Gateway—NG9-1-1 IP Routing Function	The Legacy Responder Gateway interfaces with the NG9-1-1 IP Routing Function device to send and receive data for routing purposes. The IP Routing Function device will take data bound for the Legacy Responders, determine the routing, and deliver the information.
IN-08	NN-04	NN-06	ESRP (Emergency Service Routing Proxy)—IP ACD	The ESRP interfaces with the IP ACD device to perform call distribution within the NG9-1-1 Network (SS-06).
IN-09	NN-06	NN-08	IP ACD—PSAP BCF	The IP ACD device interfaces to the PSAP BCF to deliver calls and data to an NG9-1-1 PSAP (SS-07) when the call is being distributed within the NG9-1-1 Network (SS-06).
IN-10	NN-04	NN-08	ESRP (Emergency Service Routing Proxy)—PSAP BCF	The ESRP interfaces with the PSAP BCF for routing purposes to deliver calls to the NG9-1-1 PSAP (SS-07).
IN-11	NN-04	NN-05	ESRP (Emergency Service Routing Proxy)—NG9-1-1 IP Routing Function	The ESRP interfaces with the NG9-1-1 IP Routing Function device to support connectivity between the legacy gateways and the IP Routing Function device for routing purposes.
IN-12	NN-07	NN-05	IP Network BCF—NG9-1-1 IP Routing Function	The IP Network BCF interfaces with the NG9-1-1 IP Routing Function device to forward calls from the IP Access Network (SS-05) to the NG9-1-1 IP Routing Function device for routing purposes.
IN-13	NN-07	NN-05	IP Network BCF—NG9-1-1 IP Routing Function	The IP Network BCF interfaces with the NG9-1-1 IP Routing Function device to forward IP media streams from the IP Access Network (SS-05) to the NG9-1-1 IP Routing Function device for routing purposes.
IN-14	NN-05	NN-05	NG9-1-1 IP Routing Function—NG9-1-1 IP Routing Function	The NG9-1-1 IP Routing Function device can be interfaced with other NG9-1-1 IP Routing Function devices to support intersystem communications and transport of calls from one NG9-1-1 Network (SS-06) to another.
IN-15	NN-05	NN-08	NG9-1-1 IP Routing Function—PSAP BCF	The NG9-1-1 IP Routing Function device interfaces with the PSAP BCF and is the primary delivery method for routing calls within the NG9-1-1 Network (SS-06).
IN-16	NN-05	NN-08	NG9-1-1 IP Routing Function—PSAP BCF	The NG9-1-1 IP Routing Function device interfaces with the PSAP BCF and is the primary delivery method for routing IP media streams within the NG9-1-1 Network (SS-06).
IN-17	NN-08	NP-01	PSAP BCF—NG9-1-1 BCF	The PSAP BCF interfaces with the NG9-1-1 BCF and is the primary delivery method for routing calls from the NG9-1-1 Network (SS-06) to NG9-1-1 PSAP (SS-07).
IN-18	NN-08	NP-01	PSAP BCF—NG9-1-1 BCF	The PSAP BCF interfaces with the NG9-1-1 BCF and is the primary delivery method for routing IP media streams from the NG9-1-1 Network (SS-06) to NG9-1-1 PSAP (SS-07).

ID #	From	To	Interface/System Name	Description
IN-19	NN-08		PSAP BCF—NG9-1-1 Network	The PSAP BCF interfaces with the NG9-1-1 Network to support connectivity among multiple NG9-1-1 Networks. This interface allows an NG9-1-1 Network in one area/region to communicate with other NG9-1-1 Networks for primary and backup communications.
IN-20	NN-08		PSAP BCF—NG9-1-1 Network	The PSAP BCF interfaces with the NG9-1-1 Network to support connectivity among multiple NG9-1-1 Networks. This interface allows an NG9-1-1 Network in one area/region to transmit IP media streams to other NG9-1-1 Networks for primary and backup communications.
IN-21	NN-08	ES-01	PSAP BCF—NG Emergency Services Network (ESNet)	The PSAP BCF will interface with the NG Emergency Services Network (ESNet) to connect multiple NG9-1-1 systems via a single, but redundant and highly available nationwide network to support intersystem communications.
IN-22	NN-08	ES-01	PSAP BCF—NG Emergency Services Network (ESNet)	The PSAP BCF will interface with the NG ESNet to connect multiple NG9-1-1 systems via a single, but redundant and highly available nationwide network to support intersystem transfer of IP media streams.
IN-23	NN-07		IP Network BCF—Public Web Services (Internet)	The IP Network BCF interfaces to Internet Public Web Services to access supplemental or supportive call data.
IN-24	NN-07		IP Network BCF—Media Services (Internet)	The IP Network BCF interfaces to Internet Media Services to access supplemental or supportive call data.
IN-25	NN-05	NN-09	NG9-1-1 IP Routing Function—Legacy Data Gateway	The NG9-1-1 IP Routing Function interfaces to a Legacy Data Gateway to provide access to the Voice over IP (VoIP) Positioning Center (VPC), Mobile Positioning Center (LD-02) and Automatic Location Information (ALI) (NB-01) data sources for use when making routing decisions within the NG9-1-1 Network (SS-06).
IO-01	LO-01	LO-02	PSTN UA (non-IP)—PBX	The PSTN UA (typically a telephone) interfaces with a PBX to support telephone exchange features and frequently used in an office or building setting. This interface is the beginning point for a “traditional” non-IP caller calling through a non-IP PBX.
IO-02	LO-02	LA-03	PBX—Central Office Switch	The PBX interfaces with the Central Office Switch to provide dial tone and connectivity to other telephones and systems. This interface is the connection between the PBX and the telephone company.
IO-03	LO-02	NA-01	PBX—Telephony Gateway (PSTN <-> IP)	The PBX interfaces with the Telephone Gateway to convert PSTN calls to IP-based calls and to access IP-based networks. The interface supports “traditional” non-IP calls that are converted for an IP network via a telephone gateway.

ID #	From	To	Interface/System Name	Description
IO-04	LO-01	NA-01	PSTN UA (non-IP)—Telephony Gateway (PSTN <-> IP)	The PSTN UA (typically a telephone) interfaces with the Telephone Gateway to convert non-IP PSTN calls to IP-based calls and to access IP-based networks. This interface is the beginning point for a “traditional” non-IP call that is converted into an IP-based network.
IO-05	LO-01	LA-03	PSTN UA (non-IP)—Central Office Switch	The PSTN UA (typically a telephone) interfaces with the Central Office Switch to provide dial tone and connectivity to other telephones and systems. This interface is the beginning point for a “traditional” non-IP caller. In addition, this particular interface is the legacy call origination method for the vast majority of “traditional analog landline 9-1-1 calls”.
IO-06	LO-03	LA-03	Sensor UA (non-IP)—Central Office Switch	The Sensor UA interfaces with the Central Office Switch to provide connectivity to other systems. This interface is the beginning point for a legacy non-IP sensor accessing a system to deliver its sensor data or message. This interface could include an alarm activation that dials a 7-or 10-digit number to play a recorded message.
IO-07	LO-03	NA-01	Sensor UA (non-IP)—Telephony Gateway (PSTN <-> IP)	The Sensor UA interfaces with the Telephone Gateway to convert non-IP sensor data or messages to IP-based data or messages and to access IP-based networks. This interface is the beginning point for a legacy non-IP sensor to access a system to deliver its sensor data or message over IP by connecting through a telephone gateway.
IO-08	LO-03	LA-04	Sensor UA (non-IP)—MSC Switch	The Sensor UA interfaces with the MSC to provide connectivity from a wireless-based sensor to the MSC. The MSC supports switching functions and manages the communications between the wireless-based sensor and the wireless service provider.
IO-09	LO-04	LA-04	Wireless UA (non-IP)—MSC Switch	The Wireless UA interfaces with the MSC to support switching functions and to manage the communications between wireless (CMRS) callers and the PSTN. In addition, this particular interface is the legacy call origination method for the vast majority of “traditional analog wireless 9-1-1 calls”.
IO-10	LO-04	NA-01	Wireless UA (non-IP)—Telephony Gateway (PSTN <-> IP)	The Wireless UA interfaces with the Telephone Gateway to convert non-IP wireless (CMRS) calls to IP-based calls and to access IP-based networks. This interface is the beginning point for a legacy non-IP wireless caller to access the system by connecting through a telephone gateway.
IO-11	LO-05	LA-04	Telematics UA (non-IP)—MSC Switch	The Telematics UA is connected to the MSC to support switching functions and to manage the communications between telematics services and the PSTN. This interface is the legacy call origination method for the non-IP telematics UA.
IP-01	NP-01	NP-02	NG9-1-1 BCF—PSAP IP Routing Function	The NG9-1-1 BCF interfaces with the PSAP IP Routing Function device to support distribution of calls within the NG9-1-1 PSAP (SS-07).

ID #	From	To	Interface/System Name	Description
IP-02	NP-01	NP-02	NG9-1-1 BCF—PSAP IP Routing Function	The NG9-1-1 BCF interfaces with the PSAP IP Routing Function device to support distribution of IP media streams within the NG9-1-1 PSAP (SS-07).
IP-03	NP-01		NG9-1-1 BCF—NG9-1-1 PSAP	The NG9-1-1 BCF interfaces with an NG9-1-1 PSAP to share calls directly among PSAPs.
IP-04	NP-01		NG9-1-1 BCF—NG9-1-1 PSAP	The NG9-1-1 BCF interfaces with an NG9-1-1 PSAP to share IP media streams directly among PSAPs.
IP-05	NP-01	NP-05	NG9-1-1 BCF—Call Record	The NG9-1-1 BCF interfaces with the Call Record to record both the Call Recording (real-time communications) and the Call Detail Record (call stream and other data). Retrieval of call record data is supported via this interface.
IP-06	NP-02	NP-05	PSAP IP Routing Function—Call Record	The PSAP IP Routing Function interfaces with the Call Record to record both the Call Recording (real-time communications) and the Call Detail Record (call stream and other data). Retrieval of call record data is supported via this interface.
IP-07	NP-02	NP-03	PSAP IP Routing Function—PSAP IP ACD	The PSAP IP Routing Function device interfaces with the PSAP IP ACD device to distribute calls to call takers using pre-defined ACD rules.
IP-08	NP-03	NP-05	PSAP IP ACD—Call Record	The PSAP IP ACD device interfaces with the Call Record to record both the Call Recording (real-time communications) and the Call Detail Record (call stream and other data). Retrieval of call record data is supported via this interface.
IP-09	NP-02	NP-04	PSAP IP Routing Function—NG9-1-1 Call Termination	The PSAP IP Routing Function interfaces with the NG9-1-1 Call Termination to allow the system to route calls directly to a particular call taker workstation, bypassing the IP ACD (NP-03) device.
IP-10	NP-02	NP-04	PSAP IP Routing Function—NG9-1-1 Call Termination	The PSAP IP Routing Function interfaces with the NG9-1-1 Call Termination to allow the system to route IP media streams directly to a particular call taker workstation, bypassing the IP ACD (NP-03) device.
IP-11	NP-03	NP-04	PSAP IP ACD—NG9-1-1 Call Termination	The PSAP IP ACD device interfaces with NG9-1-1 Call Termination to allow the system to route calls based on a set of rules. The system can determine characteristics associated with the call stream data and better match them to a more appropriate and available call taker that could leverage a language ability or special training capabilities.
IP-12	NP-04	NP-05	NG9-1-1 Call Termination—Call Record	The NG9-1-1 Call Termination device interfaces with the Call Record to record both the Call Recording (real-time communications) and the Call Detail Record (call stream and other data). Retrieval of call record data is supported via this interface.

ID #	From	To	Interface/System Name	Description
IP-13	NP-04	NP-06	NG9-1-1 Call Termination—GIS	The NG9-1-1 Call Termination device interfaces with the GIS primarily to support the geographic needs of the call taker. Display of a tactical map display or a geographic-based query will use this interface.
IT-01	LA-01	LA-03	Central Office Telephony Gateway (IP <-> PSTN)—Central Office Switch	The Central Office Telephone Gateway interfaces with the Central Office to deliver calls converted from IP-based calls to PSTN calls to the Central Office. This interface is an interim step to provide dial tone and connectivity to other telephones and systems.
IT-02	LA-03	LA-03	Central Office Switch—Central Office Switch	The Central Office Switch interfaces with other Central Office Switches to transport landline calls across multiple Legacy Access Networks (SS-02).
IT-03	LA-03	LA-06	Central Office Switch—Selective Router	The Central Office is connected to the legacy Selective Router for routing purposes. This interface is the method by which the majority of landline calls are delivered to Legacy (E9-1-1) PSAPs (SS-03).
IT-04	LA-02	LA-04	MSC Telephony Gateway (IP <-> Cell)—MSC Switch	The MSC Telephony Gateway (IP <-> Cell) interfaces with the MSC Switch to deliver IP-based calls to the Legacy Access Network (SS-02).
IT-05	LA-04	LA-04	MSC Switch—MSC Switch	The MSC Switch interfaces with other MSC Switch devices to transport mobile calls and their associated data across multiple Legacy Access Networks (SS-02).
IT-06	LA-04	LA-06	MSC Switch—Selective Router	The MSC Switch interfaces with the Selective Router to deliver mobile calls to PSAPs using the routing capabilities of the Selective Router.
IT-07	LA-05	LP-01	Selective Router—Telephony Switch/ACD	The Selective Router interfaces with a Telephony Switch/ACD device to allow proper routing and delivery of calls.
IT-08	LA-05	NN-01	Selective Router—Selective Router Gateway	The Selective Router interfaces with the NG9-1-1 Network (SS-06) to provide access for Legacy Access Networks (SS-02) to connect to NG9-1-1 and ultimately an NG9-1-1 PSAP (SS-07).
IT-09	LA-06	LA-06	Selective Router—Selective Router	The Selective Router interfaces with other Selective Routers for legacy call transfer among multiple legacy PSAPs (LP-01). When a transfer is made among these PSAPs, ANI data is passed along with the call.
IT-10	LA-05	LA-06	Emergency Services Gateway—Selective Router	The Emergency Services Gateway interfaces directly with a Selective Router to transfer calls to a Legacy (E9-1-1) PSAP (SS-03).
IT-11	LA-01	LA-06	Central Office Telephony Gateway (IP <-> PSTN)—Selective Router	The Central Office Telephony Gateway (IP <-> PSTN) interfaces directly with a Selective Router to transfer calls to a Legacy (E9-1-1) PSAP (SS-03) for those IP-based calls that bypass the Central Office Switch (LA-03). This type of call can include Voice over IP (VoIP) callers, originating from the IP Access Network (SS-05).

ID #	From	To	Interface/System Name	Description
IT-12	LA-04	LA-07	MSC Switch—SMS Gateway	The MSC Switch interfaces with an SMS Gateway to deliver SMS messages to the IP Access Network (SS-05) for delivery to an NG9-1-1 PSAP (SS-07).
IT-13	LA-07	NA-01	SMS Gateway—Telephony Gateway (PSTN <-> IP)	The SMS Gateway interfaces with a Telephony Gateway to deliver SMS messages through the IP Access Network (SS-05) for delivery to an NG9-1-1 PSAP (SS-07).
IX-01	LA-03	XS-01	Central Office Switch—Legacy 3rd Party Call Center	The Central Office Switch interfaces to a Legacy 3rd Party Call Center to deliver voice calls over landlines.
IX-02	LA-04	XS-01	MSC Switch—Legacy 3rd Party Call Center	The MSC Switch interfaces to a Legacy 3rd Party Call Center to connect mobile callers with a Legacy 3rd Party Call Center. This interface is the path used to provide access for telematics devices to connect to Legacy (E9-1-1) PSAPs (SS-03).
IX-03	XS-01	LA-06	Legacy 3rd Party Call Center—Emergency Services Gateway	The Legacy 3rd Party Call Center interfaces with an Emergency Services Gateway to provide routing services to access Legacy (E9-1-1) PSAPs (SS-03).
IX-04	XS-01	LP-01	Legacy 3rd Party Call Center—Telephony Switch/ACD	As a fallback solution, a Legacy 3rd Party Call Center interfaces directly with a Telephony Switch/ACD device to support accessing a Legacy (E9-1-1) PSAP when the selective routing functions are not available or have not been defined. This interface is defined as a fallback solution because of mandates requiring 3rd Party Call Centers to use Selective Routers (LA-05) for call delivery.
IX-05	XS-01	LP-01	Legacy 3rd Party Call Center—Telephony Switch/ACD	As a transitional solution, a Legacy 3rd Party Call Center interfaces directly with a Telephony Switch/ ACD device to support accessing a Legacy (E9-1-1) PSAP.
IX-06	XS-01	NA-01	Legacy 3rd Party Call Center—Telephony Gateway (PSTN <-> IP)	A Legacy 3rd Party Call Center interfaces with an Access BCF device to provide connectivity for Legacy 3rd Party Call Centers to the IP Access Network (SS-05).
IX-07	LP-01	XS-02	Telephony Switch/ ACD—Legacy Responders	The Telephony Switch/ACD device interfaces with the Legacy Responders to support delivery of call information by Legacy (E9-1-1) PSAPs (SS-03). This interface is typically voice via landline or radio, but can include limited data transfer.
IX-08	LP-04	XD-03	GIS—Base GIS	The Legacy (E9-1-1) PSAP (SS-03) interfaces with a local geographic database system (GIS) that uses a base GIS as a primary data source. This interface provides the connectivity to support the initial population and ongoing maintenance of the GIS as the base GIS data continues to be improved.

ID #	From	To	Interface/System Name	Description
IX-09	NN-03	XS-02	Legacy Responder Gateway—Legacy Responders	The Legacy Responder Gateway interfaces with Legacy Responders to allow them to connect to the NG9-1-1 Network (SS-06) to send and receive data related to NG9-1-1 calls. The gateway translates IP-based data to non-IP responder systems.
IX-10	NN-08	XS-03	PSAP BCF—IP-Enabled Responders	The PSAP BCF interfaces with IP-Enabled Responders to send and receive IP-based data related to NG9-1-1.
IX-11	NP-06	XD-02	GIS—Base GIS	The NG9-1-1 PSAP (SS-07) interfaces with a local GIS that uses a base GIS as a primary data source. This interface provides the connectivity to support the initial population and ongoing maintenance of the GIS as the base GIS data continues to be improved.
IX-12	ES-01	XS-04	NG Emergency Services Network (ESNet)—Public Safety Entity	NG ESNet interfaces with a Public Safety Entity to provide access for supportive or supplemental call data from agencies or services connected directly to the ESNet.
IX-13	ES-01	XS-04	NG Emergency Services Network (ESNet)—Public Safety Entity	NG ESNet interfaces with a Public Safety Entity to provide access for supportive or supplemental IP-based media streams from agencies or services connected directly to the ESNet.
IX-14	NN-08	XS-04	PSAP BCF—Public Safety Entity	The PSAP BCF interfaces with a Public Safety Entity to provide direct access for supportive or supplemental call data from agencies or services connected directly to the NG9-1-1 Network.
IX-15	NN-08	XS-04	PSAP BCF—Public Safety Entity	The PSAP BCF interfaces with a Public Safety Entity to provide direct access for supportive or supplemental IP-based media streams from agencies or services connected directly to the NG9-1-1 Network.
IX-16	ND-02	XS-04	IdAM—Credential Services	The IdAM data service interfaces with Credential Services to support the credentialing and authority verification process within NG9-1-1. Information about certificate validity is provided to the IdAM data service via this interface.
IX-17	NB-01	XD-01	ALI—MSAG	The ALI database interfaces with the Master Street Address Guide (MSAG) to access data source for maintenance and update purposes.
IX-18	LB-03	XD-01	SRDB—MSAG	The SRDB interfaces with the MSAG to access data for maintenance and update purposes.
IX-19	LD-02	XS-06	MPC—PDE	The Position Determining Entity (PDE) interfaces with the MPC to provide the geographic location of a wireless (CMRS) caller using one or more position determining technologies.
IX-20	XS-06	NA-02	IP-Enabled 3rd Party Call Center—Access BCF	The IP-Enabled 3rd Party Call Center interfaces with the Access BCF to receive IP media streams from its customers via the IP Access Network (SS-06).

ID #	From	To	Interface/System Name	Description
IX-21	XS-06	NA-02	IP-Enabled 3rd Party Call Center—Access BCF	The IP-Enabled 3rd Party Call Center interfaces with the Access BCF to receive calls and data from its customers via the IP Access Network (SS-06).
IX-22	XS-06	NN-07	IP-Enabled 3rd Party Call Center—IP Network BCF	The IP-Enabled 3rd Party Call Center interfaces with the NG9-1-1 Network (SS-06) via the IP Network BCF to forward IP media streams to the appropriate PSAP using the routing functions of NG9-1-1.
IX-23	XS-06	NN-07	IP-Enabled 3rd Party Call Center—IP Network BCF	The IP-Enabled 3rd Party Call Center interfaces with the NG9-1-1 Network (SS-06) via the IP Network BCF to forward emergency calls to the appropriate PSAP using the routing functions of NG9-1-1.
IX-24	NA-03	XS-08	IP Routing Function—LoST Server	The IP Routing Function uses a LoST database to capture the caller's location and determine the routing path to the appropriate NG9-1-1 Network (SS-06).
IX-25	NA-04	XS-08	Call Proxy or Redirect Server—LoST Server	The Call Proxy or Redirect Server uses a LoST database to capture the caller's location and determine the routing path to the appropriate entity (including other IP Access Networks, Call Proxy or Routing Servers, or other IP Routing Functions).
IX-26	NN-05	XS-08	NG9-1-1 IP Routing Function—LoST Server	The NG9-1-1 IP Routing Function uses a LoST database to capture the caller's location and determine the routing path to the appropriate NG9-1-1 PSAP (SS-07).
IX-27	XS-08	XS-08	LoST Server—LoST Server	The LoST Server interfaces with other LoST Servers in order to share and replicate data across multiple LoST servers and can be used to search for mapping information that exists outside the local server.

3.2.3 Location Determination Components

Determining the location of the caller is critical to the success of NG9-1-1. However, the architecture is dramatically different from that of legacy E9-1-1.

Legacy E9-1-1 Location Determination

The components of location determination for Legacy E9-1-1 include the Call Origination Devices (SS-01), the Legacy Access Network (SS-02), and limited components within the Legacy (E9-1-1) PSAP (SS-03). To illustrate: in the legacy system, when a landline PSTN call (LO-01) originates, it does so with ANI embedded in the call. ANI is used by the Central Office Switch (LA-03) to determine the correct Selective Router (LA-06) which will determine from the SRDB (LB-03) how to distribute the call to the appropriate Legacy (E9-1-1) PSAP (SS-03). The Legacy PSAP will use the ANI to send a query (via ID-02) to lookup ALI (NB-01) to identify the caller's location. ALI is displayed on the call taker's screen (LP-02) and verified during the interrogation process.

For calls originating via wireless (CMRS) devices (LO-04), the process is a bit different, and both network and handset location determination processes are used to identify the location of the caller. Calls from wireless devices are routed through an MSC Switch (LA-04) which accesses an MPC (LD-02) to determine location. In a manner similar to the PSTN origination call, the MPC will specify the Selective Router (LA-06), which distributes the call to the appropriate Legacy (E9-1-1) PSAP (SS-03). A query to the ALI database results in dynamically updated location data for the call, obtained from an MPC provider, to be sent back to the PSAP call taker's screen.

NG9-1-1 Location Determination

Multiple components exist for location determination in NG9-1-1 and location-specific information becomes part of the IP media stream (a.k.a. call stream) that is used for call identification and distribution purposes. The location of the call is queried from the call stream and additional queries of the LoST data sources are made to provide correct routing of the call. The initial query can be performed in the IP Access Network (NA-04) in order to route the call to the appropriate NG9-1-1 Network (SS-06), and a subsequent query can be performed in the NG9-1-1 Network as part of the NG9-1-1 IP Routing Function (NN-05) to identify the appropriate NG9-1-1 PSAP (SS-07) destination. See Section 8.3 of this document for additional information on LoST.

Requirements Analysis

As part of the overall requirements analysis effort, the system functionality was mapped to the proposed architecture. The mapping is provided to describe which component of the NG9-1-1 architecture is primarily responsible for supporting the functional activity and the requirements for each activity. The NG9-1-1 System Description and Requirements Document includes an Enterprise Segment Activity Roadmap (ESAR). The ESAR consists of a table of functions, or activities, for each of the system's enterprise segments. It provides an index that defines the scope of activities that need to be supported by the NG9-1-1 System. The activities are the component work functions that will be performed within the NG9-1-1 System.

Each activity within the ESAR represents a unique function the NG9-1-1 System should perform. These activities are defined by the set of attributes listed below:

- **Activity Code**—A unique code used to identify the Activity name and its associated service area name
- **Activity Name**—The name of the Activity being described
- **Role**—A name of the job role of the person or the functional role of a technology that performs the Activity
- **Proof-of-Concept: Yes/No**—A recommendation on whether the Activity should be demonstrated in a Proof-of-Concept
- **References**—Abbreviations of the documents used as references when defining the Activity
- **Architecture Elements**—The system or component name within the architecture diagram that is primarily responsible for supporting the functionality
- **Goal**—A brief description of the end result of the Activity.

Each functional activity in the following three ESARs (Figure 3-7, Figure 3-8, and Figure 3-9) are mapped to the architectural components as described in Section 3.2.1, as indicated by the "Architecture Elements" field. It should be understood that virtually every functional activity will interact with multiple architectural elements within the NG9-1-1 architecture in this section. The selected mapping of elements in the following ESARs will only indicate the primary architectural element associated with the functionality or system feature.

9-1-1 PSAP Operations [PSAP]

5.1 Call Answering [CA]	5.2 Call Processing [CP]		5.3 Call Records Management [CR]	5.4 Geospatial Visualization [GV]	5.5 PSAP Administration [PA]
[CA-MNQUE] Manage Call Queues Role: CT, PA Proof-of-Concept: Yes References: NENA 56-005, NENA 58-001 **Architecture Elements : NP-03: PSAP IP Automatic Call Distribution** Goal: Provide the capability to manage call queues and deliver the caller to a call taker workstation .	[CP-DTNAT] Determine Nature of Emergency Role: CT, PA Proof-of-Concept: Yes References: NENA-i3, NRIC VII -1B **Architecture Elements : NP-04: NG9-1-1 Call Termination** Goal: Determine the nature of the emergency and provide an initial assessment of the situation .	[CP-IDRES] Identify Appropriate Responding Agency or Service Role: CT, PA Proof-of-Concept: Yes References: NENA-i3, NRIC VII -1B, NRIC VII -1D **Architecture Elements : NP-04: NG9-1-1 Call Termination** Goal: Select appropriate responders based on the nature and location of emergency , incident management procedures, and standard operating procedures (SOP).	[CR-RCCAL] Record Call Role: CT, SYS Proof-of-Concept: Yes References: NENA 08-501, NENA 58-001 **Architecture Elements : NP-05: Call Record** Goal: Preserve a detailed record of the interactive communications occurring during a call .	[GV-DSGEO] Display Geospatial Data Role: CT Proof-of-Concept: Yes References: **Architecture Elements : NP-04: NG9-1-1 Call Termination** Goal: Display location and geospatial information on a map .	[PA-DECHP] Define and Establish Call Handling Protocols Role: PA, SA Proof-of-Concept: Yes References: NENA 08-501, NRIC VII -1B **Architecture Elements : SS-07: NG9-1-1 PSAP** Goal: Ensure proper and efficient call handling and compliance with PSAP processes and best practices through the creation and automation of protocols and procedures.
[CA-ANSCL] Answer Call Role: CT, PA Proof-of-Concept: Yes References: NENA 58-001, NENA-i3, NRIC VII -1B **Architecture Elements : NP-04: NG9-1-1 Call Termination** Goal: Provide the capability to answer a 9-1-1 call.	[CP-VFLOC] Determine and Verify Location of Emergency Role: CT, PA Proof-of-Concept: Yes References: NENA-i3, NRIC VII -1B **Architecture Elements : NP-04: NG9-1-1 Call Termination** Goal: Determine whether an emergency is located at the caller's location or elsewhere . Ensure responders are directed to the correct location .	[CP-PRINS] Provide Pre-Arrival Instructions to Caller Role: CT Proof-of-Concept: No References: NENA-i3, NRIC VII -1B **Architecture Elements : NP-04: NG9-1-1 Call Termination** Goal: Provide appropriate pre-arrival instructions to call taker . A call taker may distribute pre -arrival instructions to a caller as necessary .	[CR-OSSDT] Obtain Supportive or Supplemental Data Post Call Delivery Role: CT, PA Proof-of-Concept: Yes References: NENA 02-011, NENA 58-001 **Architecture Elements : NP-04: NG9-1-1 Call Termination** Goal: Obtain supportive or supplemental data after call delivery to facilitate call processing .	[GV-MPGEO] Manipulate Geospatial Data Role: CT, PA Proof-of-Concept: No References: **Architecture Elements : NP-06: GIS** Goal: Manipulate location and geospatial information .	[PA-SCHST] Schedule Staff Role: PA Proof-of-Concept: No References: NENA 08-501, NRIC VII -1B **Architecture Elements : NP-03: PSAP IP Automatic Call Distribution** Goal: Ensure the staffing level is set to handle the call volume .
[CA-INTCB] Initiate Call Back Role: CT, PA Proof-of-Concept: Yes References: NENA-i3, NRIC VII -1B **Architecture Elements : NP-04: NG9-1-1 Call Termination** Goal: Establish communications circuit between call taker and receiving party .	[CP-UCLOC] Update Mobile Caller's Location Information Role: CT, PA Proof-of-Concept: Yes References: NENA-i3, NRIC VII -1B **Architecture Elements : NP-04: NG9-1-1 Call Termination** Goal: Receive location information for mobile callers .	[CP-ECONF] Establish Conference Call Role: CT, PA Proof-of-Concept: Yes References: NENA 58-001, NENA-i3, NRIC VII -1B, NRIC VII -1D **Architecture Elements : NP-04: NG9-1-1 Call Termination** Goal: Establish communication among the call taker , caller, third-party (e.g., telematics) service provider , and appropriate public safety entities .	[CR-ENDCL] End Call Role: CT, PA Proof-of-Concept: Yes References: NENA 08-501, NRIC VII -1B **Architecture Elements : NP-04: NG9-1-1 Call Termination** Goal: Terminate existing call and return to ready to accept next call .		[PA-CSCTG] Create Specialized Call Taker Groups Role: PA Proof-of-Concept: No References: NENA 08-501, NENA 58-001, NRIC VII -1B **Architecture Elements : NP-03: PSAP IP Automatic Call Distribution** Goal: Create specialized call taker groups to be used in conjunction with call distribution rules .
			[CR-TRCIN] Transfer Call Records Role: CT, PA Proof-of-Concept: Yes References: **Architecture Elements : NP-03: PSAP IP Automatic Call Distribution** Goal: Transfer all Essential , Supportive, Supplemental, and/or manually-entered data concerning the call to the appropriate responding agency dispatch or other authorized entity .		[PA-MACDR] Manage Automatic Call Distributor Rules Role: PA, SA Proof-of-Concept: No References: NENA 08-501, NENA 58-001, NRIC VII -1B **Architecture Elements : NP-03: PSAP IP Automatic Call Distribution** Goal: Create, manage, and distribute rules and policies governing the distribution of incoming 9-1-1 calls and automatic event alerts , along with the associated data to call takers .

🟨 Recommended for Proof-of-Concept

Reference Legend
ECRIT - Requirements for Emergency Context Resolution with Internet Technologies Internet Engineering Task Force
NENA 02-010 - NENA Standard Formats & Protocols for ALI Data Exchange, ALI Response & GIS Mapping
NENA 02-011 - NENA Data Standards for Local Exchange Carriers, ALI Service Providers & 9-1-1 Jurisdictions
NENA 02-013 - NENA Data Standards for the Provisioning and Maintenance of MSAG Files to VDBs and ERDBs
NENA 08-501 - NENA Technical Information Document on the Network Interface to IP Capable PSAP
NENA 58-001 - NENA IP Capable PSAP Features and Capabilties Standard
NENA-i3 - NENA i3 Technical Requirements Document
NRIC VII-1B - 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
NRIC VII-1D - 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

Role Key
ALL - ALL Roles
CT - Call Taker
DB - Database Administrator
NA - Network Adminstrator
PA - PSAP Adminstrator
SA - System Adminstrator
SYS - NG9-1-1 System
911AUTH - 9-1-1 Authority

Figure 3–7: 9-1-1 PSAP Operations Service Area ESAR

9-1-1 System Administration [SYAD]

6.1 System Management [SM]	6.2 Data Management [DM]	
[SM-CRROL] Create and Define Roles Role: PA, SA Proof-of-Concept: No References: ECRIT, NENA 08-501, NENA-i3, NRIC VII-1B, NRIC VII-1D **Architecture Elements: SS-06: NG9-1-1 Network** Goal: Create, manage, and assign roles within the system.	[DM-MNDBA] Manage Database Access Role: DBA Proof-of-Concept: No References: ECRIT, NENA 08-501, NENA-i3, NRIC VII-1B, NRIC VII-1D **Architecture Elements: ND-01: NG9-1-1 Database Management System (DBMS)** Goal: Provide, support, and manage the capability to access the enterprise database (s) and to allow the distribution of data contained within those database(s).	[DM-MNDBT] Manage Database Auditing Role: DBA Proof-of-Concept: No References: NENA-i3, NRIC VII-1B, NRIC VII-1D **Architecture Elements: ND-01: NG9-1-1 Database Management System (DBMS)** Goal: Provide the capability to audit the specified user and maintenance activities against the enterprise database.
[SM-MUSER] Manage User Accounts Role: SA Proof-of-Concept: No References: ECRIT, NENA 08-501, NENA-i3, NRIC VII-1B, NRIC VII-1D **Architecture Elements: SS-06: NG9-1-1 Network** Goal: Provide the capability to enable the creation, modification, suspension, and deletion of system accounts Provide the capability to build user permissions/views with appropriate access to allowable systems, networks, and databases Provide the capability for only those system administrators with proper authority to create and modify/update user accounts	[DM-MNDBP] Manage Database Performance Role: DBA Proof-of-Concept: No References: ECRIT, NENA 08-501, NENA-i3, NRIC VII-1B, NRIC VII-1D **Architecture Elements: ND-01: NG9-1-1 Database Management System (DBMS)** Goal: Provide the capability to monitor and report on the operational performance of the enterprise databases.	[DM-MNDBI] Manage 9-1-1 Interface and Protocol Availability and Usage Role: SA Proof-of-Concept: Yes References: NENA 08-501, NENA-i3, NRIC VII-1B, NRIC VII-1D **Architecture Elements: ND-01: NG9-1-1 Database Management System (DBMS)** Goal: Ensure the availability of necessary and beneficial data interfaces and communication protocols to support call processing and emergency response.
[SM-PLCFC] Planning Configuration Changes Role: DBA, SA Proof-of-Concept: No References: **Architecture Elements: SS-06: NG9-1-1 Network** Goal: Ensure that the system and necessary network configurations adequately support the system and network desired functions and capabilities.	[DM-PDBSR] Perform Database Save & Recovery Role: DBA Proof-of-Concept: No References: NENA 08-501, NENA-i3, NRIC VII-1B, NRIC VII-1D **Architecture Elements: ND-01: NG9-1-1 Database Management System (DBMS)** Goal: Provide the capability to back up and save enterprise database(s), along with the archiving of appropriate system data. Provide the capability to recover and restore the enterprise databases based on previous backups.	[DM-SCIER] Submit Caller Information Error Report Role: CT, DBA Proof-of-Concept: No References: **Architecture Elements: NP-04: NG9-1-1 Call Termination** Goal: Submit caller information error report to the originating data provider for correction.

🟨 Recommended for Proof-of-Concept

Role Key

- ALL - ALL Roles
- CT - Call Taker
- DB - Database Administrator
- NA - Network Adminstrator
- PA - PSAP Adminstrator
- SA - System Administrator
- SYS - NG9-1-1 System
- 911AUTH - 9-1-1 Authority

Reference Legend
ECRIT - Requirements for Emergency Context Resolution with Internet Technologies Internet Engineering Task Force.
NENA 02-010 - NENA Standard Formats & Protocols for ALI Data Exchange, ALI Response & GIS Mapping
NENA 02-011 - NENA Data Standards for Local Exchange Carriers, ALI Service Providers & 9-1-1 Jurisdictions
NENA 02-013 - NENA Data Standards for the Provisioning and Maintenance of MSAG Files to VDBs and ERDBs
NENA 08-501 - NENA Technical Information Document on the Network Interface to IP Capable PSAP
NENA 58-001 - NENA IP Capable PSAP Features and Capabilties Standard
NENA-i3 - NENA i3 Technical Requirements Document
NRIC VII-1B - 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
NRIC VII-1D - 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

Figure 3–8: 9-1-1 System Administration Service Area ESAR

9-1-1 Systems Operations [SNSP]

7.1 Call Treatment [CT]		7.2 Security Administration [SC]	7.3 Database Administration [DA]	7.4 Operations Administration [OA]	
[CT-ROLOC] Recognize Originating Location Role: SYS Proof-of-Concept: Yes References: NENA 58-001, NENA-i3, NRICVII -1B, NRICVII -1D **Architecture Elements : NN-05: NG9-1-1 IP Routing Function** Goal: Receive and electronically validate location - originating caller location information (civic or geospatial).	[CT-LGCAL] Document Call Detail Information Role: SYS Proof-of-Concept: No References: NENA-i3 **Architecture Elements : NB-05: Call Record , NP-05: Call Record** Goal: Preserve a record of call information in a data file.	[SC-MNSEC] Manage Network Security Role: NTA, SA Proof-of-Concept: Yes References: NENA-i3, NRICVII -1B, NRICVII -1D **Architecture Elements : SS-06: NG9-1-1 Network** Goal: Ensure managed access to network resources, ensure data integrity, and provide usage auditability.	[DA-MTDBC] Manage Database Content Role: DBA, SA Proof-of-Concept: Yes References: NENA 02-010, NENA 02-011, NENA 02-013, NRICVII -1B, NRICVII -1D **Architecture Elements : ND-01: NG9-1-1 Database Management System (DBMS)** Goal: Provide the capability to manage and maintain the logical database structure supporting the NG 9-1-1 enterprise database environment.	[OA-MOSRE] Monitor System Resources Role: NTA, SA Proof-of-Concept: No References: NENA-i3, NRICVII -1B **Architecture Elements : SS-06: NG9-1-1 Network** Goal: Provide the ability to monitor and manage system and subsystem usage and reliability .	[OA-MNSRE] Manage System Resources and Configuration Role: NTA, SA Proof-of-Concept: Yes References: NRICVII -1B **Architecture Elements : SS-06: NG9-1-1 Network** Goal: Provide management and control of network system resources and configurations .
[CT-REGCT] Identify Call Type Role: SYS Proof-of-Concept: Yes References: NENA-i3, NRICVII -1B, NRICVII -1D **Architecture Elements : NN-05: NG9-1-1 IP Routing Function** Goal: Receive and validate call type information (e.g., telematics, silent alarm) from telecommunications devices and recalculate call type and default priority based on supporting data .	[CT-PNWBS] Provide Network Bridging Services Role: SYS Proof-of-Concept: Yes References: NENA 58-001, NENA-i3 **Architecture Elements : NP-02: PSAP IP Routing Function** Goal: Ensure that all system and network entities are able to conference and share data as appropriate and beneficial to call treatment and processing .	[SC-LOGIN] Login Role: ALL Proof-of-Concept: No References: **Architecture Elements : SS-06: NG9-1-1 Network** Goal: Authenticate and provide system access to users.	[DA-MTDBI] Populate and Maintain 9-1-1 Data Interfaces Role: DBA Proof-of-Concept: No References: NENA 02-010, NENA 02-011, NENA 02-013, NENA-i3, NRICVII -1B, NRICVII -1D **Architecture Elements : ND-01: NG9-1-1 Database Management System (DBMS)** Goal: Provide the capability to update and modify the metadata database based on changes in data standards or enterprise databases .	[OA-MNFTR] Manage Network Faults and Recovery Role: NTA, SA Proof-of-Concept: Yes References: NRICVII -1B, NRICVII -1D **Architecture Elements : SS-06: NG9-1-1 Network** Goal: Provide network capability to identify , isolate, and correct network faults .	[OA-MNCLR] Manage Call Records Role: ALL Proof-of-Concept: Yes References: **Architecture Elements : SS-06: NG9-1-1 Network** Goal: Create and maintain call records
[CT-RTPSP] Route Call to PSAP Role: NTA, SYS Proof-of-Concept: Yes References: NENA 58-001, NENA-i3, NRICVII -1B, NRICVII -1D **Architecture Elements : NN-05: NG9-1-1 IP Routing Function** Goal: Route call from the initiator and call -originating service to the appropriate destination based on identified call treatment including location information received (civic or geospatial).	[CT-CAUTH] Call Authentication Role: SYS Proof-of-Concept: Yes References: IETF RFC -3647, IETF RFC -4474, NENA 02-502, NENA 04-503, NENA 08-001, NENA 58-001 **Architecture Elements : NN-07: IP Network Border Control Function (BCF), NP-01: NG9-1-1 Border Control Function (BCF)** Goal: The call authentication process ensures that the appropriate entity , such as the originating provider or other responsible party , has been granted permission to access the system .		[DA-PADCT] Publish Authoritative Data Content Role: DBA Proof-of-Concept: Yes References: **Architecture Elements : ND-01: NG9-1-1 Database Management System (DBMS)** Goal: Establish and publish to authenticated users various data content related to system databases supporting functions such as location validation , call routing, rights management, and data routing.	[OA-MANSP] Manage System Performance Role: NTA, SA Proof-of-Concept: Yes References: NENA-i3, NRICVII -1B **Architecture Elements : SS-06: NG9-1-1 Network** Goal: Ensure network and system operation and reliability to meet acceptable and adopted standards . Provide the capability to monitor , record, and analyze system performance data against predefined metrics (i.e., establish system norms and flag exceptions).	[OA-MCHRQ] Manage Change Requests Role: NTA, SA Proof-of-Concept: No References: **Architecture Elements : SS-06: NG9-1-1 Network** Goal: Provide the administrative and analytical resources to support management decisions affecting system configuration and operation .
			[DA-PFDBT] Perform Database Auditing Role: SA Proof-of-Concept: No References: NRICVII -1B, NRICVII -1D **Architecture Elements : ND-01: NG9-1-1 Database Management System (DBMS)** Goal: Audit the accuracy of the NG 9-1-1 database(s).		

🟨 Recommended for Proof-of-Concept

Role Key
ALL - ALL Roles
CT - Call Taker
DB - Database Administrator
NA - Network Adminstrator
PA - PSAP Adminstrator
SA - System Administrator
SYS - NG9-1-1 System
911AUTH - 9-1-1 Authority

Reference Legend
ECRIT - Requirements for Emergency Context Resolution with Internet Technologies Internet Engineering Task Force
NENA 02-010 - NENA Standard Formats & Protocols for ALI Data Exchange, ALI Response & GIS Mapping
NENA 02-011 - NENA Data Standards for Local Exchange Carriers, ALI Service Providers & 9-1-1 Jurisdictions
NENA 02-013 - NENA Data Standards for the Provisioning and Maintenance of MSAG Files to VDBs and ERDBs
NENA 08-501 - NENA Technical Information Document on the Network Interface to IP Capable PSAP
NENA 58-001 - NENA IP Capable PSAP Features and Capabilties Standard
NENA-i3 - NENA i3 Technical Requirements Document
NRIC VII-1B - Network Architecture Properties in 2010, Extending E9 1 1 to Satellites, and Generic Architectures to Support Video and Advanced Service. NRIC VII Focus Group1B
NRIC VII-1D - 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

Figure 3–9: 9-1-1 Systems Operations Service Area ESAR

Section 4: Key Architecture Considerations

The proposed NG9-1-1 System is extremely robust and scalable. It is composed of various smaller subsystems, components, and voice, data, and network interfaces. The subsystems can be further decomposed to identify the technical characteristics that must be considered in the design and operation of the NG9-1-1 System. Twelve such topics have been identified as key elements in the architectural framework of the NG9-1-1 System.

It is important to note that the 12 topics that were identified do not constitute an exhaustive, comprehensive list that defines the detailed framework for the NG9-1-1 System. More accurately, these topics serve to identify key architectural characteristics that must be considered by architecture planners and their discussion seeks to build an understanding of their importance within the NG9-1-1 System.

Each of the topics selected for discussion plays a critical role within an NG9-1-1 System function and can be supported by a well understood and stable set of associated standards. An explanation of the importance of each topic within the NG9-1-1 System is provided in the following text:

Identity and Access Management

IdAM is the foundation for securing the NG9-1-1 infrastructure and operations. IdAM is a key consideration for the NG9-1-1 architecture because it provides authentication, credentialing, authorization, and entity management services for NG9-1-1 entities, including users, devices, and organizations. Given the cross-organizational nature of the NG9-1-1 community, a centralized and federated IdAM is required to establish a trusted identity and various access control mechanisms for NG9-1-1 operations.

Database Architecture

Database Architecture refers to the structure of NG9-1-1 databases that deliver meaningful information that enables public safety organizations to complete their duties. NG9-1-1 national and local systems must call on database systems to enable data storage and querying of critical information. The NG9-1-1 information architecture requires a proven database architecture that delivers functionality, scalability, high availability, and low latency.

Data Management

Database Management is the means by which the NG9-1-1 database architecture is managed and its functionality is supported. A DBMS enables the configuration of the database structure and configuration. Data management is critical to NG9-1-1 operation because it allows the acquisition of data from variable sources to match system needs and populate the various databases in the NG9-1-1 System.

Network Structure

Network structure defines the NG9-1-1 IP routing backbone and hence is the foundation of the NG9-1-1 System. The NG9-1-1 network structure addresses three primary elements: redundancy and failover, gateway architecture, and network border control functionality.

Border Control Function

BCFs manage the boundaries of the legacy PSTN, NG9-1-1, the IP networks, and the PSAPs to which the traffic must be delivered. BCF is a key topic because the NG9-1-1 IP network will deploy BCFs at various levels to ensure all of the network boundaries are accessible and functional. BCFs also serve the vital purpose of controlling access at the edge of the network while allowing access to the resources within any network connected to the backbone.

Media Gateways

Media gateways are the primary interface to the NG9-1-1 network. Gateways will provide the translation of legacy 9-1-1 traffic for IP transport and provide a collection point for traffic from attached networks to the NG9-1-1 backbone. The NG9-1-1 System will require several gateways supporting multiple translation functions.

Network Interconnections

The mesh/hub-spoke virtual private network (VPN) interconnection structure is a necessary component of an IP network because it offers greater redundancy, physical diversity, and survivability. This network interconnection schema allows for resource sharing across networks when interconnecting a wide area network (WAN). Mesh networks create a redundant environment by overlaying a physical circuit architecture, increasing reliability and failure resistance. Integrated and separate gateways allow networks to reconfigure IP traffic.

IP Call Distribution

With IP as the primary routing protocol, all calls will have the ability to be distributed to one or more PSAP destinations. The PSAPs or 9-1-1 authorities within the NG9-1-1 System can then define call distribution and routing according to each jurisdiction's policies and needs. Consequently, the NG9-1-1 System must define IP call distribution.

PSAP User Interface (Human Machine Interface)

Although the topics surrounding the network, protocols, and the arrangement of hardware to support NG9-1-1 operations are vitally important, the quality and capability of the system is only as powerful as the interface through which the operator delivers emergency services. The PSAP User Interface (Human Machine Interface) discussion addresses both application architecture and key design considerations that will enable the efficient use and integration of next generation functionality within the overall NG9-1-1 System. Key points of discussion include appropriate display of data, open-source and proprietary tools, and commercial off-the-shelf (COTS) and custom-developed tools.

IP-based Access to NG9-1-1

IP-based access is considered a key topic because of the benefits it provides in the areas of call origination and call routing. Providing IP-based access to the NG9-1-1 System will allow end users to connect to the Internet and other IP networks using their handheld devices. The caller will be able to send voice, video, and text messages to the appropriate PSAPs where the multimedia information will be processed using IP-enabled applications.

IP Call Origination

IP call origination using IP UAs such as laptops, IP phones, and personal digital assistants (PDA) is an important feature of the NG9-1-1 architecture. End users can originate emergency calls using their handheld devices from any location that has connectivity to the Internet. IP applications (such as VoIP via Internet, VoIP via non-Internet IP network, WiFi, and WiMAX) or other IP-enable devices that meet accepted system interface standards would also be capable of originating emergency calls. Additional flexibility of the NG9-1-1 architecture is provided through support for originating emergency calls from sensors and wireless devices. The architecture enables these devices to interface with IP networks, which can transport and route emergency calls to the appropriate PSAPs.

IP Call Routing/Signaling (LoST/SIP)

Prioritizing and routing emergency calls over IP networks while ensuring the privacy of the geospatial data is another critical feature of the NG9-1-1 architecture. Transport Layer Security (TLS) is recommended for end-to-end secure data transmission. Location to service mapping is provided by the Location-to-Service Translation (LoST) protocol, and the location information is sent to the PSAP using the industry-standard Session Initiation Protocol (SIP) for signaling. Using IP to route emergency calls enables the NG9-1-1 architecture to leverage several features and functionalities of the IP protocol such as path redundancy, and traffic prioritization. Path redundancy ensures that multiple routes are available from the source to the destination for routing 9-1-1 calls. Queuing technologies such as low-latency-queuing (LLQ) ensures prioritization of critical traffic such as emergency 9–1–1 calls over IP networks.

Notes

Introduction
Arch. Analysis Approach
Architecture Definition
Key Arch. Considerations
NG9-1-1 DB Services
NG9-1-1 Network
NG9-1-1 PSAP
IP Call Origination
Architecture Summary
Source References
Appendices

Section 5: NG9-1-1 Database Services

At the core of the NG9-1-1 System, database services enable the core functionality of the system by processing and converting data to meaningful information useful by system entities. Database services consist of multiple physical and logical functions, including—

- **IdAM**—The ability to define and authorize individuals or entities to gain secure access to appropriate NG9-1-1 resources
- **Database Architecture**—The logical structure and relationships between data repositories that enable the system to access information that supports decision making
- **Data Management**—The functional ability to structure, organize, and store data within database repositories using a DBMS to maintain and administer data.

The following sections define the functionality and operational parameters for each of the database services.

Introduction
Arch. Analysis Approach
Architecture Definition
Key Arch. Considerations
NG9-1-1 DB Services
NG9-1-1 Network
NG9-1-1 PSAP
IP Call Origination
Architecture Summary
Source References
Appendices

5.1 Identity and Access Management

5.1.1 Description

The IdAM service specifies how the NG9-1-1 system administers user identification and system access to ensure confidentiality, integrity, authentication, and non-repudiation of sensitive data. The service empowers the NG9-1-1 community and sets the manner in which information is shared and to what extent other PSAPs and entities can access the data. Figure 5-1 illustrates a basic NG9-1-1 IdAM scenario. The subsections that follow describe how IdAM services will support public, ESNet, and emergency responder access to the NG9-1-1 System. The remainder of this section discusses the NG9-1-1 IdAM Community of Interest (COI) and presents two architecture options for IdAM.

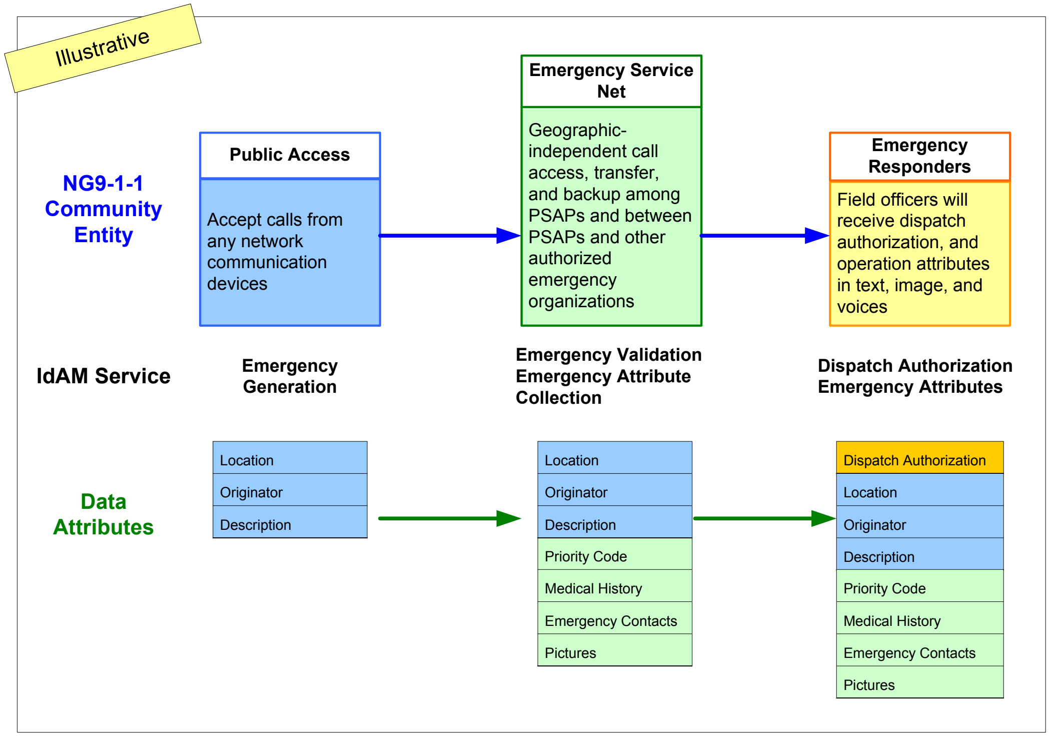

Illustrative
NG9-1-1 Community Entity
Public Access
Accept calls from any network communication devices
Emergency Service Net
Geographic-independent call access, transfer, and backup among PSAPs and between PSAPs and other authorized emergency organizations
Emergency Responders
Field officers will receive dispatch authorization, and operation attributes in text, image, and voices
IdAM Service
Emergency Generation
Emergency Validation Emergency Attribute Collection
Dispatch Authorization Emergency Attributes
Data Attributes
Location
Originator
Description
Location
Originator
Description
Priority Code
Medical History
Emergency Contacts
Pictures
Dispatch Authorization
Location
Originator
Description
Priority Code
Medical History
Emergency Contacts
Pictures

Figure 5–1: NG9-1-1 Illustrative Scenario

Public Access

NG9-1-1 will receive calls from IP-enabled network communication devices. IdAM services will—

- Provide the mechanism to associate data attributes in various formats with the correct call.
- Provide end-to-end message-level integrity for the call data. This end-to-end message-level integrity is required for traffic traversing an IP network to guard against unauthorized access and other possible routes of attack.

Emergency Service Net (ESNet)

The ESNet consists of a variety of public safety entities, including PSAPs, third-party call centers, telematics service providers, and medical centers. The ESNet will confirm the validity of emergency calls and collect required data elements in order to share information among public safety entities. IdAM will—

- Build appropriate trust levels, trust agreements, and trusted identities as a common ground for various NG9-1-1 parties to share information
- Facilitate data element (e.g., emergency contacts, images, and medical history) collection within the ESNet
- Protect the integrity and confidentiality of NG9-1-1 System and user data.

The ESNet requires distributed information sharing across different security boundaries. Later in this section, approaches (both centralized and federated) are presented that achieve this mission need.

Emergency Responders

Emergency responders receive dispatch authorization and caller data to facilitate response operations. IdAM services will ensure—

- Authenticity of dispatch authorization
- Non-repudiation of dispatch authorization
- Integrity and confidentiality of dispatch authorization and associated caller data.

NG9-1-1 can issue dispatch authorization to dispatch and responder agencies via different media paths to help ensure that critical missions can be carried out when the legacy voice system is not available. IdAM services need to ensure, under all circumstances, the authenticity, integrity, non-repudiation, and confidentiality (if applicable) of dispatch authorizations. Based on previously developed NG9-1-1 scenarios, personal identifiable information, such as medical history, could be transmitted to the field. IdAM services must protect the integrity and confidentiality of this information.

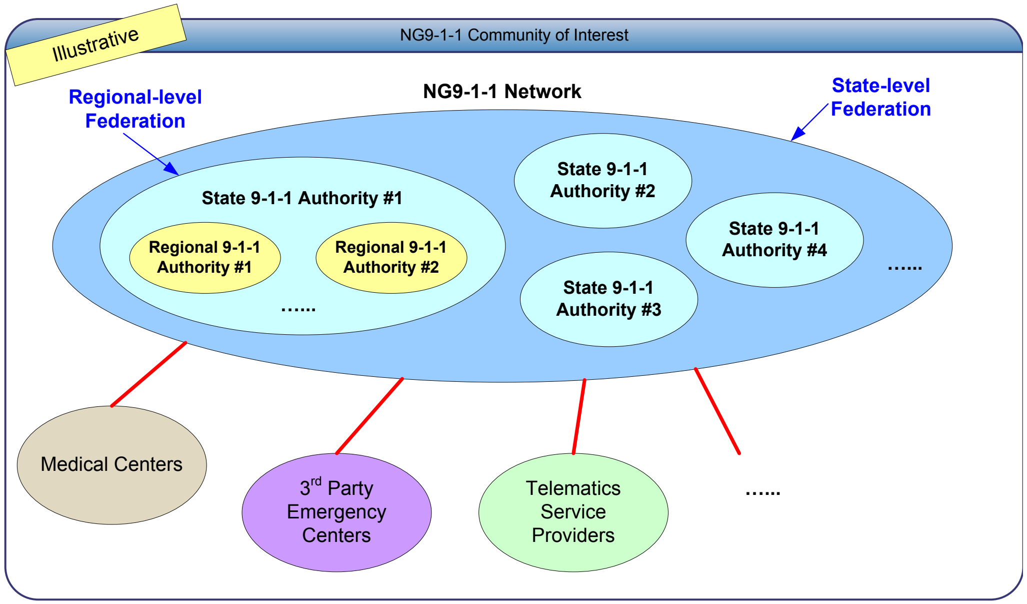


Figure 5–2: NG9-1-1 Community of Interest

NG9-1-1 IdAM Community of Interest (COI)

The NG9-1-1 COI defines groups of entities involved in sharing emergency operations-related information. This information can include emergency location, emergency contacts, NG9-1-1 identification credentials, and personal medical history, which are created and maintained by various COIs. Figure 5-2 shows the potential NG9-1-1 COIs.

The COI defines security boundaries among NG9-1-1 entities involved in emergency operations. At its core is the NG9-1-1 Network, with its own security boundary. Because of the potential large scale of the NG9-1-1 Network, it will have a state-level federation and a regional-level federation. At the state-level federation, each state's 9-1-1 Authority will define its IdAM policies. Examples of IdAM policies include:

- Procedures for issuing, maintaining, validating, and revoking NG9-1-1 credentials
- Roles and responsibilities of state 9-1-1 authorities
- Credential acceptance protocols among state 9-1-1 authorities
- Access permissions to information among state 9-1-1 authorities.

The state-level federation enables participating state 9-1-1 authorities to share information securely. Trust levels and trust agreements detailing IdAM policies must be negotiated so that a trusted credential across the state-level federation can be established. Based on the trusted credential, state 9-1-1 authorities will maintain the authority over authorization decisions.

State 9-1-1 authorities will also manage the regional-level federation. Regional 9-1-1 authorities may include counties or metropolitan areas, depending on local policies and needs. Trust levels and trust agreements detailing IdAM policies would be negotiated so that a trusted credential across regional 9-1-1 authorities within a state could be established. Similar to the state-level federation, regional-level federation will provide a trusted credential while regional 9-1-1 authorities will make authorization decisions.

Outside the NG9-1-1 COI, various COIs exist such as medical centers, telematics service providers, and third-party call centers. COIs outside the NG9-1-1 Network will create trust agreements with the NG9-1-1 Network to be part of the larger federation if they need to share information with the NG9-1-1 Network. The NG9-1-1 Network will develop a master trust agreement defining its IdAM policies for other COIs to join the federation.

Centralized IdAM Architecture

Figure 5-3 is an illustrative example of a centralized IdAM architecture used to implement IdAM services for a regional 9-1-1 Authority.

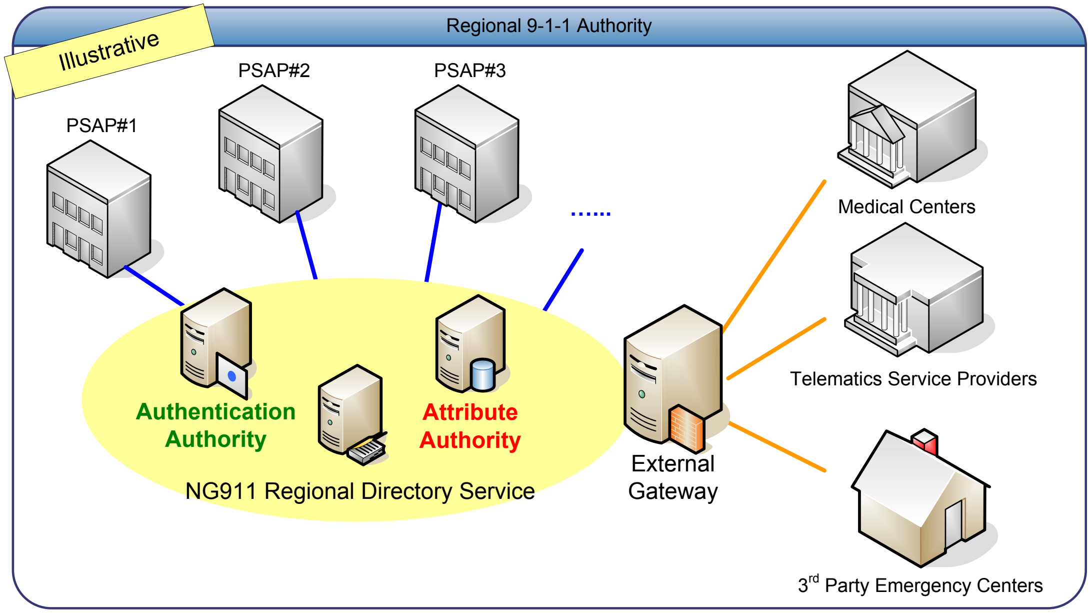


Figure 5–3: Centralized IdAM Architecture for Regional 9-1-1 Authority

Table 5–1: Authentication Credential Assurance Levels

Assurance Levels	Authentication Credential
High	X.509 Certificate
Medium	One-time password device
Low	Username/Password

The centralized IdAM architecture will build one centralized authentication authority, directory service and attribute authority:

- **Authentication Authority**—An authentication authority is the credential service provider of the regional-level 9-1-1 authority that issues and validates authentication credentials for its PSAPs. Authentication credentials can be categorized using assurance levels. Assurance levels define how strong the credentials are. For example, a X.509 certificate provides a higher assurance level than a username/password token. Depending on regional level 9-1-1 authority's trust policies (which could be derived from state-level or regional-level federation trust policies) and the sensitivity of transactions, the credential service providers can request different types of authentication credentials from users, devices, or organizations. Examples of authentication credentials with various assurance levels are listed in Table 5-1.

  Regional 9-1-1 authorities can build their own credential provider or leverage a third-party credential service provider (e.g., Verisign, Cybertrust).
- **Authorization Authority**—An authorization authority collects and stores caller data (e.g., caller's name, caller's address, location of the emergency, nature of the emergency) that support NG9-1-1 operations. In a centralized IdAM architecture, required data can be collected from participants before operations begin
- **Directory Service**—The directory service provides "where is" information to aid all participants in locating the authentication and authorization authority.

Federated IdAM Architecture

The design philosophy of the federated IdAM architecture is to leverage existing IdAM services from participants instead of building new ones as in the centralized IdAM architecture. The federated approach is usually recommended for a larger group. Figure 5-4 is an illustrative example of using the federated IdAM approach to implement regional-level federation.

The federated IdAM architecture comprises the following services.

- **Authentication Authority**—The federated IdAM architecture will leverage existing authentication authorities from regional 9-1-1 authorities. Multiple authentication authorities will co-exist in the federated approach. The regional-level federation will define trust levels and establish trust agreements so that each regional 9-1-1 Authority can trust credentials issued by any authentication authority inside the federation. All authentication authorities must be certified and accredited to ensure minimum requirements listed in the trust agreement have been satisfied.
- **Authorization Authority**—Regional 9-1-1 authorities will store entity (users and devices) attributes under their jurisdiction (instead of maintaining a centralized attribute authority.) Attributes will be collected from regional 9-1-1 authorities during operations if necessary. The attribute collection process will access multiple authorization authorities based on different field operation scenarios. Authorization authorities must be certified and accredited based on the regional-level federation trust agreement.
- **Directory Service**—The directory service provides "where is" information to aid all regional 9-1-1 authorities in locating authentication and authorization authorities. Certified and accredited authentication and authorization authorities will be registered in the directory service.

Access control decisions will be made locally under pre-defined guidance so that the community can trust and accept decisions from each other. Each participant will maintain authentication and authorization responsibility within its own jurisdiction. All participants will define assurance levels (e.g., public, sensitive, and confidential or low, medium, high) of exchanged information and negotiate a trust agreement describing required processes and procedures for handling exchanged information. Under the trust agreement, participants can accept authentication claims from each other and enable attribute collection across security boundaries when policies allow.

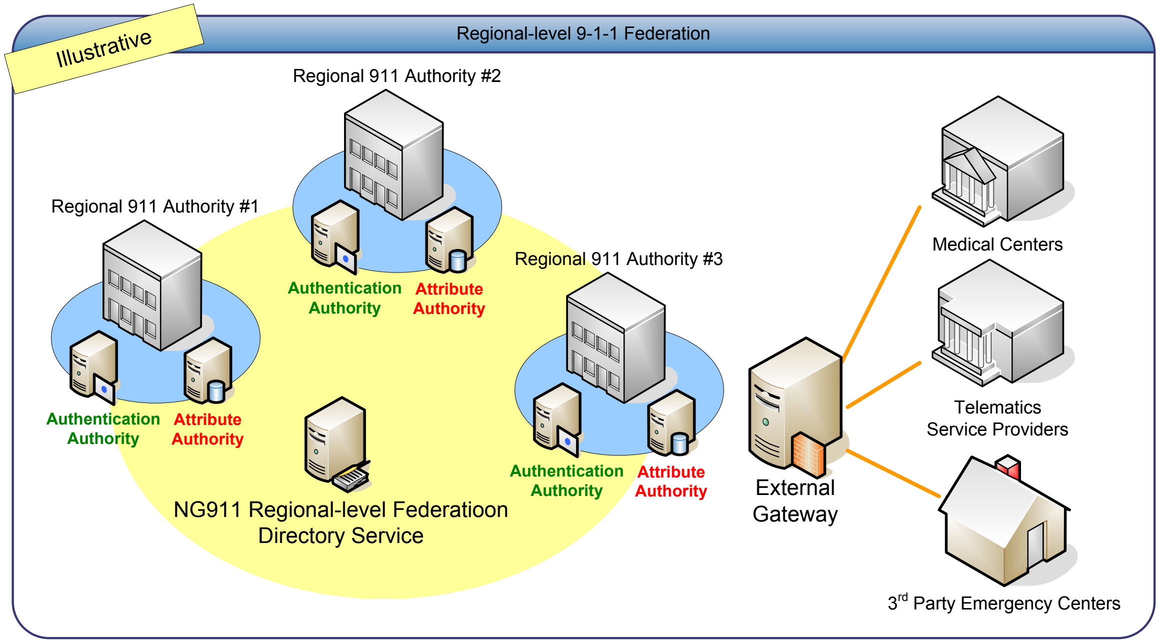

Illustrative
Regional-level 9-1-1 Federation
Regional 911 Authority #2
Authentication Authority
Attribute Authority
Regional 911 Authority #1
Authentication Authority
Attribute Authority
Regional 911 Authority #3
Authentication Authority
Attribute Authority
NG911 Regional-level Federatioon Directory Service
External Gateway
Medical Centers
Telematics Service Providers
3rd Party Emergency Centers

Figure 5–4: Federated IdAM Architecture at Regional-level Federation

5.1.2 Benefits

IdAM services are the foundation to secure distributed NG9-1-1 operations. The pros and cons of two proposed IdAM architecture are listed in the following table:

Table 5–2: IdAM Architecture Pros & Cons

	Centralized IdAM	Federated IdAM
Pros	Has an easy-to-enforce centralized access control policies Employs a simple architecture requiring fewer technologies Provides efficient attribute collection and makes it easier to trust the centralized services	Maintains local jurisdictions Is easy to scale, results in less duplicated information, and makes it easier to maintain data accuracy Leverages existing infrastructure and investments Offers a resilient architecture (no single point of failure)
Cons	Permits duplicate information (local and centralized copies), which leads to maintenance challenges Is difficult to scale, and the centralized services will become another stovepipe Represents a single point of failure Does not leverage existing infrastructure	Has increased complexity because of the larger number of technologies involved Might create challenges in establishing a trust agreement because of discrepancies of infrastructure maturity among participants Requires a neutral party to certify and accredit participants to enforce the trust agreement

5.1.3 Considerations

Building a scalable IdAM architecture is a critical foundational element for deploying various security services (integrity, authenticity, confidentiality, and non-repudiation) for the NG9-1-1 architecture. Based on characteristics of centralized and federated IdAM architecture, it is likely that the NG9-1-1 will need a hybrid of the two approaches. A regional 9-1-1 Authority might build a centralized IdAM architecture within its local jurisdiction and join a regional-level federation as a member. To successfully federate state and regional 9-1-1 authorities into the NG9-1-1 Network and create trust between other communities of interest (e.g., medical centers, third-party call centers, telematics service providers), the following steps are recommended:

- Define a security engineering process and a governance structure to engage NG9-1-1 participants
- Develop NG9-1-1 federated IdAM scenarios to align IdAM services with NG9-1-1 operations
- Define an infrastructure maturity assessment framework to assess the infrastructure gaps among potential federation participants
- Implement a Proof-of-Concept (PoC) to integrate and validate the various technologies.

Implementing IdAM services requires a layered operating model, including policies, operating standards, procedures, and guidelines. Recognizing the benefits and concerns of different IdAM approaches will ensure alignment of IdAM services with business needs, successful deployment, and operations.

5.2 Database Architecture

5.2.1 Description

One measure of success for the NG9-1-1 System is based on the ability of data repositories to deliver meaningful information that enable public safety organizations to better complete their duties. National and local NG9-1-1 systems must employ database systems to enable data storage and querying of critical information. The NG9-1-1 information architecture will require a database architecture that supports these database and query requirements while also supporting high availability and low latency and no single point of failure.

The NG9-1-1 system architecture should support a hierarchical database architecture and topology. At the top level, a hierarchical database architecture supports a network of nationwide databases that aggregate and consolidate data from regional, state, or local jurisdictions. The regional, state, and local jurisdictions all form the hierarchical database architecture reporting chain. For example, a region may be responsible for a database with data from each state database. The state database is responsible for the data from local jurisdiction databases. The number of databases increases as the system becomes increasingly distributed from the few nationwide aggregated databases to the multiple regional and local levels. Consequently, the database architecture at each level within the hierarchy must support data sharing and reporting to at least one hierarchical level above and below to facilitate the flow of data within the NG9-1-1 System, and to enable access and control under disaster management conditions where other PSAPs are required to take over call handling and dispatch functions. In addition, the architecture could be implemented in a manner where it is not strictly hierarchical, in that regional databases that cross state boundaries could coexist within the existing structure.

The database architecture can be further decomposed into the logical database structures or schemas that provide database and query capabilities, call and data routing control, geophysical validation functions, location information access, and business rules/policies that will control and enable new features and options in the NG9-1-1 System. For devices that do not self-discover their location, LISs provide validated location information for Enterprise, wireline, or cellular services at the call origination point or the entry point to the NG9-1-1 System. The identity and access management and security databases relate to all the above. The structure of a database is critical to enable data record storage and correlation and to enable system functions and applications to query the database. The responses provided by the database are information used for decision making or reporting. A common database structure builds on the concept of relational databases. Relational database architectures typically include one or more tables with a set of attributes that define relationships between the tables. Alternate database architectures can be employed as well.

To achieve the correct information outputs, the NG9-1-1 database architecture would be composed of multiple tables architected and structured based on the system's unique data inputs. System data flows would be defined by the data structure and relationships to deliver system application functionality. Furthermore, as a nationwide system, NG9-1-1 must scale the logical database architecture and interoperability to a national system. The data structure must maintain integrity to ensure that data entered in the database is accurate and valid. Additionally, the national, regional, state, and local databases must be interoperable.

5.2.2 Benefits

An NG9-1-1 database architecture is fundamental to the system's operation because it enables data storage and information sharing across jurisdictional boundaries. The database architecture will fundamentally transform current public safety system operations through an interoperable and scalable architecture. Interoperability will enable public safety agencies and organizations to collaborate and improve their delivery of services.

5.2.3 Considerations

The most critical part of the NG9-1-1 database architecture is its ability to scale and be interoperable at all jurisdictional levels. The scope of the database architecture spans national to local systems and therefore must be carefully designed. The design must be hierarchical or structured in a manner that enables secure data flow across boundaries. Given the criticality of the database architecture to NG9-1-1, its availability and disaster recovery options must maximize system uptime and provide for no single point of failure. The database architecture at each jurisdictional level must provide redundant processing capabilities through mirrored databases. In addition, the databases must be backed up to a remote site for complete disaster recovery. The physical database server architecture options include hardware server clusters, redundant databases, disaster site databases, replicated databases, and clustered databases. The National Emergency Number Association (NENA) i3 Technical Requirements Document architecture definitions assume that the system will minimally employ: distributed databases with redundancy, replication, and disaster site characteristics.

Interoperability across the end-to-end NG9-1-1 architecture must be required and enforced. The database architecture should be based on recommended and standardized physical server platforms. Although the server platforms can be diverse, functionality and performance in accordance with the requirements of the national system cannot be compromised. To further minimize interoperability issues, the NG9-1-1 System should use open source or open standards-based products and development policies. In summary, the database architecture should be an interoperable and scalable design that supports a diverse user base through the use of these open standards and technology standardization practices.

5.3 Data Management

5.3.1 Description

Database management is the means by which the NG9-1-1 database architecture is managed and supported. The traditional approach to database management is the use of software to perform the configuration, operation, and management of the database architecture. The management software, collectively known as the DBMS, consists of a products suite that enables all functions related to managing and operating databases. The DBMS provides the system operator with the human machine interface to define, structure, configure, and manage all database functions, queries, and processes.

Desirable characteristics for the NG9-1-1 DBMS include—

- Use of either relational or object-oriented database structures for NG9-1-1 databases, or a combination of both
- Query schemas or languages for ease of information requests to the database
- Replication/backup of database servers so that any corruption of the primary database does not disrupt system operations
- Maintenance of integrity of the database structure so that rules, attributes, identities, or keys are not corrupted by users or other changes
- Maintenance of security on the DBMS to prevent unauthorized changes to the database architecture, structure, or attributes
- Automated optimization for frequently occurring usage patterns or requests, allowing a DBMS to adjust itself to improve processing speed.

The DBMS for NG9-1-1 would be deployed at various levels of the public safety system hierarchy and provide interoperability with other jurisdictions. This requires that individual jurisdictions select interoperable and scalable DBMSs that can receive and share data with other jurisdictions up to the national level and down to the local level. The DBMS should share the database architecture's design in order to ensure that interoperability and standard configurations are implemented.

Within database management, NG9-1-1 must define the management of disaster recovery (DR) and Continuity of Operations (COOP) planning. Each jurisdiction should be responsible for planning and coordinating the backup of all its data to an alternate location. At a minimum, data should be redundant within any single site, but mirrored to an alternate site. Alternate sites would be maintained with the same availability as the primary databases/data center. Maintaining both a primary and alternate data site ensures high availability and decreases the potential of downtime.

5.3.2 Benefits

Database management is critical to the NG9-1-1 system to ensure that information is available to all stakeholders. Data is the basic element upon which public safety agencies rely to fulfill their duties. Ensuring that data is managed and stored in an accessible manner requires DBMSs. The presence of DR/COOP will deliver high availability of the databases within the NG9-1-1 System to prevent mission failure. Collectively, database management governs the principles for operating, sharing, and storing data.

5.3.3 Considerations

Technically, ease and efficiency of use by system and database managers are only indirectly related to database management internal to the NG9-1-1 System architecture. However, achieving these function characteristics requires that human interfaces to various databases and between related databases within NG9-1-1 be a conscious part of design work. Allowing human–system interface design to be less than effective leads to user frustration and potential operational difficulties that can affect NG9-1-1 service performance.

Data rights management (DRM) is applicable to all users that interact, use, transmit, and govern access to data. DRM is primarily implemented through IdAM to authorize users and grant access to data. Through interaction with NG9-1-1 business rules and data rights definitions, the NG9-1-1 system is expected to be able to automatically or manually (by call taker) acquire data from diverse sources and integrate it with call stream data to measurably increase the availability and usability of data in support of call handling and incident response. Data rights are also related to privacy issues, and to "need to know" rules and regulations.

Data aggregation enables data access from variable sources, including originating service provider, and subscriber-specific, governmental, and public safety sources, and transforms it to match system needs to populate the various databases in the NG9-1-1 system. Data acquisition processes can be complex, and significant operational problems can occur with improperly designed data aggregation systems. The range of data values or data quality in an operational system may be outside the expectations of designers at the time validation and transformation rules are specified.

Examples of this data are—

- Service Order extracted data by telephone number for wireline service
- "Shell record" data for legacy cellular routing codes and transitional VoIP service routing codes
- Uniform Resource Identifier (URI) addresses and related contact information for PSAPs and other public safety entities
- Base GIS data for routing data layers
- Address validation data sets
- Credential data
- Decision information supporting database content associated with business rule definition.

Scalability needs to be established, including understanding the data volumes involved. NG9-1-1 will likely require multiple daily processing that at least approaches near real time, in order to acquire, transform, and load various databases with updates. Designers should investigate the current and future need for real-time or near real-time updating. A service-oriented architecture (SOA) across multiple organizational boundaries may not be obtainable.

Geospatial data is used throughout NG9-1-1, and dependence on it will become even more widespread over time as the use of mobile devices increases. Under current standards, geospatial location representation applies to all devices using air linked mobility design. In addition, fixed and nomadic (movable, but at a fixed location when in use) devices can have their location represented by both required civic addressing and optional geospatial coordinates. Consequently, geospatial data must be stored and available to the NG9-1-1 System for location identification, location validation, routing control, and information display at the PSAP or other entity. Databases involved in NG9-1-1 location-related functions must be capable of storing, manipulating, and using geospatial data. The data layers applicable to 9-1-1 service are discussed in NENA GIS Data Collection and Maintenance Standards, NENA

02-014. Note that additional layers may be required as NG9-1-1 and general Next Generation Emergency Communications evolve, and impacts may affect database scalability considerations.

Use of different types of geospatial data or calculation methods at various points in the NG9-1-1 system can cause comparative inaccuracies in location databases and in displayed caller or emergency locations for response. Accuracy standards for NG9-1-1 should be defined to drive toward consistency of geodetic protocols among service providers and users. Basic recommendations in this area are covered in NENA data standards documents. NG9-1-1 efforts nationally should further evaluate the potential for inaccuracies related to use of conflicting geospatial data sets before, within, and beyond NG9-1-1, and establish recommendations on accuracy requirements and minimum geospatial data source consistency.

Section 6: NG9-1-1 Network

As discussed earlier, the NG9-1-1 System is designed as a "system of systems" that can use a variety of network topologies that provide the telecommunications infrastructure to support IP-based communications. The NG9-1-1 System is typically defined as an IP network that is created through common data communications standards, protocols, and tools. Most legacy networks have used traditional analog telecommunications facilities for the network design, while focusing on data standards to create a virtual network. The NG9-1-1 System is not unlike that type of network. Traditional circuits can be used to build a dedicated network on which the IP network service can be built. The NG9-1-1 network architecture has three primary goals:

- Determining and validating location
- Routing the call to the appropriate interconnection point
- Providing IP interconnection between legacy and NG9-1-1 networks.

The actual communications network for the NG9-1-1 System, as defined by NENA, requires IP communications features, and

Introduction
Arch. Analysis Approach
Architecture Definition
Key Arch. Considerations
NG9-1-1 DB Services
NG9-1-1 Network
NG9-1-1 PSAP
IP Call Origination
Architecture Summary
Source References
Appendices

protocols. NENA has recommended, through the i3 documentation as well as the IETF through the ECRIT[1] and Network Reliability and Interoperability Council (NRIC) documentation, that an IP network is the desired platform for the NG9-1-1 System. This NG9-1-1 platform will rely on common data communication standards to ensure and protect delivery of information. The physical network will also use telecommunications standard configurations that are made up of the wires, gateways, routers, and equipment to transmit and receive traditional communications signals. Commonly, the topology is a distribution of physical telecommunications wires with a higher level "logical" overlay network.

In NG9-1-1 System networking, the core platform is the IP network. This enables the entire NG9-1-1 network to use IP-based communications from end to end. Specifically, IP transport through the network ensures that traffic can be delivered seamlessly through the network across whatever physical network is available. Virtual connections are also required to improve access to the network and secure the traffic across all connections.

The entire NG9-1-1 architecture will be based on IETF-ratified standards throughout the design. This ensures a standardization of network structures, data, and routing protocols.

The core elements making up the topology of the NG9-1-1 network include—

- **NG9-1-1 IP Routing.** The core of the NG9-1-1 network, as defined in i3, is based on IP routing. Essentially, the NG9-1-1 architecture is a WAN that provides transparent delivery across the network. The core of the network will leverage dynamic routing protocols to ensure that the network can provide automated path detection. Routing protocols used for the NG9-1-1 System will need to provide the scalability and security to meet the requirements of applications traversing the system.
- **Emergency Service Routing Proxy.** The ESRP manages the routing policy surrounding the access to the IP network from legacy E9-1-1 networks. It is essentially a separate proxy server that allows a legacy PSAP to receive calls from an IP-based client and the NG9-1-1 network. Acting as a proxy for a traditional call, the ESRP can deliver a legacy 9-1-1 PSAP call to an NG9-1-1 based PSAP through the NG9-1-1 IP-enabled network. There will be multiple ESRPs throughout the NG9-1-1 network. The primary goal will be to pair ESRPs with each other to create a mesh of ESRPs so that no single point of failure is present within the network.
- **IP Automatic Call Distributor.** The IP ACD feature delivers calls over the IP network back to NG9-1-1 IP-based PSAPs. The IP ACD function is described in Section 7.1, IP Call Distribution.

This NG9-1-1 platform is known as the ESNet. Its primary goal is to provide a standardized backbone facility to interconnect multiple PSAPs without limiting the communications facility. As identified earlier, the ESNet is designed as a system of systems based on IP networking. The ESNet will bridge all traffic from the legacy network through to IP-enabled PSAPs. ESNet is a network of shared communications facilities that can provide for private, secure access across a WAN. The ESNet will contain all of the necessary gateway functions, and the border control mechanisms will manage security across the entire platform. All connections to the ESNet will be routed over IP.

6.1 Network Structure

6.1.1 Description

As participating NG9-1-1 networks become more common, the ability to connect seamlessly across several diverse backbone connections is paramount in providing an end-to-end solution. A network built on the concept of an IP-enabled system of systems will provide flexibility in connecting NG9-1-1 partners and will efficiently route information across the system.

[1] *The IETF ECRIT working group seeks to identify and describe the Internet technologies available to indicate an Internet caller's location and to manage call routing for emergency calls. More information about ECRIT can be found here at: http://www.tschofenig.com/twiki/bin/view/EmergencyServices/*

The NG9-1-1 network is designed to be an IP-enabled network built on a flexible, robust platform with built-in security to mitigate system risks. The typical NG9-1-1 network can be configured as an IP-based mesh type solution in which 9-1-1 calls are routed across a WAN. In addition routing of this information across such an advanced network to the correct PSAP depends on the interconnection of network elements.

Interconnection across the NG9-1-1 System is quite complicated. Various networks must be interconnected across a common backbone to provide a transparent and seamless transport facility. This requires the NG9-1-1 internetwork to be able to provide connection to the legacy 9-1-1 network as well as the IP access network.

The overarching structure of the NG9-1-1 network structure will follow the guidelines outlined in NENA TRD 08-751 (also referred to as NENA i3). In addition, the Federal Communications Commission (FCC) NRIC IV will also be used as a guide for maintaining a cohesive network topology.

Many access methods are available within the structure, and the NG9-1-1 network will continue to rely on these elements. The creation of an IP-wide area network is introduced as a general “overlay” to the existing access methods in order to allow creation of the VPNs within the system. The IP-WAN will use the available physical network facilities but will rely on standard routing protocols to maintain the IP portion of the system. This allows use of a variety of access methods and will allow the network to operate as an “any-to-any” converged system.

Six common connections will be required of the NG9-1-1 platform:

- IP Access Network
- NG9-1-1 PSAP
- Legacy Access Network
- Legacy PSAP
- NG9-1-1 Internetwork
- Database Services.

Connections must be made to the IP access network in order to deliver IP-based calls. Calls will be in a number of formats. Data, video, voice, and text converged into an IP signal will use the IP network. The network will function as the transport mechanism to deliver calls to the IP gateway device at the NG9-1-1 network edge.

In the NG9-1-1 System, the network must be capable of providing bandwidth as well as transport facilities to deliver calls to the correct PSAP. The concept is to provide enough bandwidth to allow traffic to enter the IP Network BCF so that calls are not blocked. NG9-1-1 network PSAPs will be equipped with the capabilities to support converged traffic. Each PSAP will be able to terminate data, voice, video, and text on a single connection while routing the call to the correct answering point. The call detail record will provide more information to the call taker prior to call treatment.

Interconnection to the legacy 9-1-1 access network is also a requirement. Legacy 9-1-1 networks will continue to produce traffic and must be connected to the NG9-1-1 network to allow for transparent interconnection between basic and enhanced 9-1-1 callers and the NG9-1-1 network. The Legacy Access Network is primarily made up of centralized automated message accounting (CAMA) trunks that are configured to directly access the PSAP from a tandem office. The legacy network is built with traditional telecommunications (i.e., PSTN) based circuits. The addition of a Selective Router that serves to route calls to the correct PSAP creates an E9-1-1 system. Selective Routers are owned and maintained by individual telecommunications companies and are typically assigned to large geographic areas. In the NG9-1-1 System, the network must be able to support legacy as well as IP communications.

In the NG9-1-1 network, the selective routing function as a telecommunications service will not be required. Using network gateways and standard routing protocols, the network will enable quick routing of calls across the system to the correct PSAP. All routing in the NG9-1-1 network will be based on common standard protocols.

The connections from the NG9-1-1 platform are key connections within the network. All of the routing, data, and information attached to the call are obtained through these connections. The ANI/ ALI database, MSAG, SRDB, EPAD, and LoST database will all be outside the NG9-1-1 network. A connection must be configured over a private or virtually private network to access System data. In addition, links to the VPC, ERDB, and MPC will be required across the same IP platform. Finally, interconnection to the authentication and authorization data stores will also be required.

6.1.2 Benefits

The benefits of using a mesh network for NG9-1-1 topology are that a mesh design is aware of all of the paths available throughout the network. This enables transparent connections to be built as a virtual network throughout the entire system. The virtual nature of these networks can result in several network benefits:

- **Dynamic Routing of Traffic**—Through the ability to re-route traffic quickly without administrator intervention, congestion can be averted.
- **Redundancy**—A mesh topology can provide network redundancy on top of physical redundancy common in survivable circuit based networks.
- **Transparent Networking**—Virtual tunnels can be created to segment traffic using a shared backbone.
- **Survivability**—With the ability to reroute traffic to a resource on the network that is not out of service, a level of failover or survivability can be achieved.
- **Metering and Monitoring**—Measurements on the network can be performed to ensure that the entire platform is operating efficiently.
- **Traffic Policing**—Traffic can be policed according to type, class, tags, or other features as determined by the policies assigned for each packet.
- **Interoperability**—A mesh network with the tools included in this list can offer a high level of interoperability and convergence.

A mesh topology deployed in the NG9-1-1 System can use traditional telecommunications circuits for transmission. Typically, a Synchronous Optical Network (SONET) or ring-based physical network will provide the backbone and deliver the connectivity to the routers required for IP networking. A mesh operating on top of the ring network enhances the diversity and overall redundancy of the NG9-1-1 platform.

Because a mesh network appears as a WAN platform, several data communications features can be added to enhance the delivery of calls. Quality of Service (QoS) is a method of placing a threshold on the overall network to ensure reliability of the network.

Quality of Service

QoS is a mechanism used throughout the network to offer a level of assurance for delivering communications during periods of congestion. Jitter, latency, and delivery are all variables that determine QoS parameters across a network. A feature of most IP networks is an ability to maintain a specific routing table. The table identifies all the particular routes available in the network, while maintaining all of the potential destinations. When a network applies QoS to the virtual network, thresholds can be assigned according to criteria specified. Each network that bridges to the NG9-1-1 network will require its own IP connectivity. Each must meet the minimum QoS requirements to ensure delivery across the entire system.

6.1.3 Considerations

Redundancy will be provided through a series of diversely positioned devices. Multiple routers, servers, gateways, and physical equipment will be required. Connections will be provided over a redundant network, enabling each device to remain survivable in the event of a failure. To prepare the network to be as redundant and survivable as possible, there should be no single point of failure throughout the design.

NG9-1-1 networks must be as resilient and survivable as possible. Diverse network connections and fault tolerant redundant equipment must be accounted for throughout the network design. Therefore, a mesh or hybrid design offers the best option for minimizing outage risks. The routers in the network are capable of redistributing routes when failures occur. The preferred NG9-1-1 IP network also logically separates the functions of the physical network and the logical system design of the NG9-1-1 System.

The hybrid network design will use the available network facilities in a given geography. Some may have only private line type services, while others could operate on a Multi Protocol Label Switching (MPLS) network. A mesh network will allow use of the physical network and can be created on top of almost any available facility. The mesh design will be delivered as Layer 3 IP-based connections. The mesh overlay is important in order to continue to use existing equipment in a particular physical network. Ultimately, the ability to build a mesh overlay while using the available underlying physical network allows for individual networks to remain flexible over the long term.

Within the NG9-1-1 mesh network, several business rules will be defined to determine the best possible solution for addressing each scenario.

- Calls must route to one or more backup PSAPs when a failure occurs.
- Alternate or backup PSAPs must be designated.
- Recovery must be seamless when a PSAP comes back online.
- Security measures must be functional across the primary and backup PSAPs.
- Calls must be able to be transferred from the backup PSAP with the same amount of information that the primary PSAP could.
- No location preference to the PSAP should be made.

Risks to the NG9-1-1 IP mesh network include the possibility of the network being compromised either unintentionally or by malicious users. These risks can be limited through the implementation of security controls to mitigate risks to the NG9-1-1 IP network. Other potential risks to the NG9-1-1 System include—

- Denial of Service Attacks
- Misrepresentation
- Eavesdropping
- Call Pattern Tracking
- Malformed Requests
- QoS Abuse
- Spoofed Messages
- Call Hijacking.

Security will need to be built into the design of the entire system, including authentication and authorization, filtering, monitoring, auditing, and incident response capabilities.

NG9-1-1 networks must have a BCF to minimize access to the network. At the most rudimentary level, strict user authentication must be adhered to that will limit a user's rights to access network resources. Filtering capabilities will also limit outside attacks and entry into the NG9-1-1 network without proper authentication.

6.2 Border Control Function

6.2.1 Description

The NG9-1-1 IP network will require that BCFs are present at the ingress and egress of all interconnections within the network. The primary goal of the BCF is to manage the boundaries of the legacy PSTN, the NG9-1-1 network, IP networks, and the PSAPs to which the traffic must be delivered. In addition, BCFs allow VoIP traffic to navigate the firewalls and network security appliances within the NG9-1-1 network. They also assure that each session is maintained to complete a call.

By employing BCFs at the edge of each divergent network, the entire NG9-1-1 platform can maintain strict access control. At a very basic level, Access Control Lists can deny access to the network resources before allowing entry into the network. This allows all systems inside the network to operate with minimum levels of security while securing the entire architecture.

Session Border Control provides assurance that SIP-based voice traffic can keep a session active without re-registration to the server. This function enables SIP calls to operate as if they were dialed from a dedicated telecommunications circuit. Media Validation is another aspect of the BCF. Each BCF will maintain connections to various media types throughout the network and allow access to those as necessary.

Because the BCFs operate at the edge of the network, they can allow internetworking to occur. A transparent “bridge” is created through the access links in the BCF that performs dedicated circuit-like networking. Although these connections are dynamic, their ability to operate without a dedicated connection allows internetworking to occur without intervention through a manual setup.

6.2.2 Benefits

The NG9-1-1 IP network will deploy BCFs at various levels throughout the NG9-1-1 network to ensure all of the network boundaries are accessible and functional. Emergency information from any network, device, or type of system can be transmitted through the network. The BCF manages the access through the network.

BCFs at multiple levels offer greater session control and assurance that calls will be delivered properly. Data (including SMS/text messages), video, and voice traffic will all be appropriately delivered through the BCF to the destination as defined through the NG9-1-1 network. SIP trunking and VPNs will also be tunneled through the NG9-1-1 network to limit latency and maintain a session. Traffic can be optimized and congestion minimized through the BCF distributed network. A BCF platform will also help minimize costly equipment replacements.

The design of the NG9-1-1 network requires broadband IP networking to deliver the features, protocols, and security necessary to handle calls across the network. The most efficient topology is a mesh architecture that can be built on traditional telecommunications facilities. Within the NG9-1-1 IP platform, various network controls will be engaged to assure that traffic congestion is minimal. IP features such as QoS will be used to maintain the threshold necessary to transport calls. Call delivery must be assured through all network devices. Therefore an IP mesh network offers an unprecedented set of tools to maintain and assure communications. These include BCFs as well as redundancy measures and security assurance.

6.2.3 Considerations

Deploying BCF tools in a WAN helps maintain a very reliable and consistent network platform. The ability to control access at the edge of the network while allowing access to the resources within any network connected to the backbone is vital. BCFs allow for every network in a system to be versatile to meet local needs while not limiting the flexibility, reliability, security, and scalability of the entire network. The BCFs will engage in Session Border Control as well as provide the ability to control the boundary of the network.

6.3 Media Gateways

6.3.1 Description

The mesh NG9-1-1 IP network will require the use of gateways to deliver specific functions. When a legacy 9-1-1 network is connected to an NG9-1-1 IP network, the gateway function allows all traffic to be configured for IP transport. Each gateway will be used as the ingress to the NG9-1-1 network. In addition, a comparable function must exist at the IP network entry point. The IP Network BCF will operate in similar fashion to a gateway but will offer more robust control. The IP Network BCF will use more Access Control Lists to assure that traffic from a specific location will be able to access only those resources to which it is entitled. This will create a more hierarchical network and minimize direct service attacks.

In the NG9-1-1 network, a gateway is the primary interface to the network. The gateway collects all traffic from each network and distributes it to the IP-based NG9-1-1 backbone. Typically, the gateway device connects networks using different data protocols so that information can be passed between them. In the NG9-1-1 architecture, three specific gateways perform network functions as well as transfer data to other NG9-1-1 platforms. Gateways can be integrated, allowing for greater functionality and security features in one platform. A separate gateway operates in conjunction with other hardware to perform other network functions such as proxy server, firewalls, and enterprise support.

Four primary gateways are identified within the network that interconnect the various networks that must access the NG9-1-1 System. Each gateway will provide boundary management features at the interface to the networks. Although integrated gateways offering multiple functions in one system are available, the NG9-1-1 network will use gateways to operate a single process at the access point. Therefore, four standalone single-function units will be deployed in the network that have specific rules and interfaces but that also offer more traffic consolidation tools.

The benefits of an integrated gateway in an NG9-1-1 network would not be as great as when such a gateway is used in a normal WAN. With an integrated gateway, a single piece of network equipment is used to perform multiple functions across the platform. An integrated gateway can also offer specific telephony features while decreasing the equipment required. This method eliminates several points of failure within the network. However, a separate (i.e., un-integrated) gateway allows delivery of the gateway functions through other devices. Routers, firewalls, and other network security devices must be attached to the gateway to provide their services across the network. A separate gateway is very efficient and common in most networks.

The NG9-1-1 network will deploy several gateways throughout the design to provide a flexible solution capable of interconnecting various networks. Consequently, the model also allows for a high level of reliability when transferring information from end to end.

6.3.2 Benefits

The benefit of an architecture using a gateway inside the NG9-1-1 network is primarily to allow reconfiguration of traffic into IP format. However, gateways also offer a collection point for all traffic within the system. In short, all points attached to the network are aware of all other points across the backbone—including legacy 9-1-1 PSAPs. This all-points awareness uses the capability of gateway architectures to maintain all of the necessary network elements to deliver calls accurately and in a timely fashion to their destination. In an NG9-1-1 network, three specific gateways will be deployed to allow the completion of calls:

- **Selective Router Gateways**—A Selective Router gateway is the interface to the existing legacy selective router. This gateway functions as a repository for all traffic originating from the Selective Router and transfers those calls to the IP network BCF. Once into the BCF, the calls will be shaped for transmission across the NG9-1-1 network.

- **Legacy PSAP Gateways**—Legacy PSAP gateways are used to join the NG9-1-1 network to a legacy PSAP. Calls are sent from the NG9-1-1 IP-enabled network back through the legacy gateway into the telephony switch at the PSAP.
- **Legacy Responder Gateways**—Legacy Responder gateways enable the NG9-1-1 network to transfer traffic through the IP network back to the responders.
- **PSTN Gateways**—PSTN gateways connect the PSTN to transfer legacy E9-1-1 traffic through the NG9-1-1 IP network back to a legacy PSAP, or to NG9-1-1 PSAP.

6.3.3 Considerations

The use of gateways in the NG9-1-1 architecture aids the BCF by segmenting and directing the traffic to the correct system. Each gateway is responsible for a particular network segment, which helps maintain the divergent access beyond the backbone. Using an architecture with several layers of BCFs through separate gateways ensures that all network resources are shared equally.

All architectural considerations should be based on current security standards and common protocol framework. It is recommended that the following standards[2] be used to ensure network security is enabled across all network elements.

- A Framework for IP-based Virtual Private Networks [RFC 2764]
- The Internet IP Security Domain of Interpretation for ISAKMP (Internet Security Association and Key Management Protocol) [RFC 2407]
- Session Initiation Protocol (SIP) [RFC 3261]
- RTP (Real-Time Protocol): A Transport Protocol for Real-Time Applications [RFC 3550]
- Analysis of the Security of Border Gateway Protocol (BGP)/Multi Protocol Label Switching (MPLS) IP Virtual Private Networks (VPNs) [RFC 4381].

6.4 Network Interconnections

6.4.1 Description

The most effective configuration for the NG9-1-1 network is through a private network when available. However, a virtual network designed across a shared infrastructure can also be viable. A VPN is designed to secure communications through a shared network. Traditionally, this is done by creating a secure tunnel through the Internet or other network facility. While typically designed for enterprise systems, VPNs can function at multiple layers within a network. At Operating System Interface (OSI) Layer 2, VPNs can be delivered using Ethernet, Frame Relay, or Asynchronous Transfer Mode (ATM) technology. Within OSI Layer 3, a VPN can be created through Transmission Control Protocol (TCP)/IP. Both types of VPNs are functional in the context of the overall NG9-1-1 system. VPNs can be built on many common telecommunications arrangements while achieving the benefits of both physical and logical networking.

While the underlying network can be a multitude of point-to-point systems or a hub and spoke design, the VPN service allows each type to be configured seamlessly. A virtual mesh network can be configured through the VPN across the hub and spoke circuit switched networks. The creation of a mesh network relies more on the enabling equipment than the architecture of the physical connection.

Within a mesh network, traffic types (data, voice, video, and text) are combined within the virtual framework. However, they can be separated for transmission across the single IP network. Each communications type may require a specific VPN-based tunnel to connect from end-to-end within the network.

Because a VPN over a mesh platform can allow for traffic separation, delivery of each traffic type can be designed for efficiency. For example, video traffic must be highly reliable with low latency. However, text may not need to be reliable

[2] *The standards specified here include industry-accepted best practices and are accessible via the IETF at: http://www.ietf.org/rfc.html*

and can handle a small amount of latency. In the normal circuit-switched environment, this would require a dedicated connection for the duration of the call. However, using an IP network, the traffic may be able to burst to a size consistent with that required for only the time it needs to transmit the packets of information. This bursty capability, along with the ability to privatize the network tunnels securely, is big benefit for a VPN.

A hub and spoke network architecture refers to the physical point-to-point connections between equipment. These point-to-point networks can be used as the "highway" connecting a larger network deployment. Hub and spoke networks can be configured into survivable ring architecture with the deployment of SONET type equipment to allow redundancy and survivability. A mesh can be built across the point-to-point network using the benefits of both architectures.

Building a hub and spoke architecture can add redundancy across all links in the system. The hubs represent the equipment termination nodes. The nodes typically will be a multiplexer that can connect the circuits/spokes between the nodes. The hub and spoke network is a common telecommunications network design.

The most common form of NG9-1-1 topology will be an IP-based VPN design. This topology uses the physical network as a highway and the upper layer IP network through the NG9-1-1 network. The configuration of virtual paths will enable the NG9-1-1 network to choose the best path for transmission. Routers can be connected to each neighboring router, which creates a decentralized distributed network. Such a deployment enables VPN configurations across the entire network and increases the redundancy throughout the architecture.

Common network deployment strategies include traditional telecommunications services, Metro Ethernet, IP networks, and MPLS. MPLS uses both Layer 2 and Layer 3 to build a layered and meshed network. By using MPLS tags instead of standard IP routing, MPLS can operate more efficient than standard IP networking. MPLS can deliver packets through the network based on the tag alone instead of reading each IP address at each hop through the network. Using MPLS allows VPN networks to be configured faster and more frequently than normal IP networking. VPN networks will be configured across the MPLS network, focusing on securing the paths through the network.

An NG9-1-1 network based on IP has the flexibility obtained by merging two network platforms. On the physical side, a hub and spoke design can be enhanced by using a mesh network that acts as an overlay. The overlay is created through a series of routers connected to the hub and spoke network. The routers create a transparent virtual network that can be configured to reroute traffic in the event of a network outage. A mesh network can offer a high level of security and redundancy without relying on the physical connections to create survivability. Some of the benefits of a hub and spoke design with a mesh overlay are—

- Greater redundancy
- Survivability
- Physical diversity.

A number of VPN technologies exist today, each with different benefits. Technologies that would need to be considered include IP Security (IPSec) VPNs, and Secure Socket Layer (SSL) VPNs. A benefit of a VPN is the additional security through forced authentication. A user must authenticate to the VPN before being allowed access to the resources located within the VPN. Another benefit of a VPN is the ability to allow sharing of resources across the network. This model essentially creates a virtual mesh when interconnecting across a WAN. VPNs can deliver an "any-to-any" connection to resources that are present on the VPN itself. For example, when a user authenticates to a particular network, all the resources attached to that network can be made available to that user. Theoretically, local rights for each resource will further secure the network.

When interconnecting to these other networks, a WAN model is the best overall solution. The advantages of a WAN are that the networks can be bridged or interconnected without relying on the physical plant each time. The ability to dynamically allocate bandwidth along with the flexibility of the IP network is crucial to delivering calls.

The most cited benefits are—

- Reduced call-setup time
- Improved QoS
- Efficient use of resources
- Preparation of PSAPs for future technologies
- Disaster recovery
- Greater security
- Minimization of points of failure
- Interoperability
- Ability to transfer calls over a wider area
- Call integrity
- Data transfer
- No geographic restriction on calls.

When a mesh network is used to overlay a circuit-based architecture, each VPN that is created operates at a higher layer. This enables the entire NG9-1-1 architecture to remain failsafe and redundant. Redundancy through routing protocols can be effective at the VPN, and network redundancy through diversity of facility arrangements is available at the physical level. In addition, redundancy must be designed to support—

- Identification of calls as failover when transmitted to another PSAP
- Capability of a PSAP for immediate takeover of a call.

Physical access to outside plant facilities should be limited and require security access procedures. Network security is often a function of logins, passwords, and access rights. Furthermore, network security can be a function of Administration, Accounting, and Authentication (AAA) type functions. Applying the standards of AAA can aid in supplying a very functional network access security platform.

The NG9-1-1 IP infrastructure requires 24/7 monitoring of the network. The NG9-1-1 network should have monitoring, maintenance, repair, and upgrade/replacement agreements in place. Any agreements should outline minimal repair times, on-site spare equipment, replacement schedule, and detailed reporting of network usage. Care should be taken regarding the type of monitoring being provided.

As described in Section 7 of NENA 03-501, the Disaster Recovery Plan should address full or partial PSAP outages, E9-1-1 network failures, serving/E9-1-1 Control Office switch failures, and natural or manmade disasters that affect any portion of the 9-1-1 system. The first objective of the Disaster Recovery Plan should be to route the voice call to the PSAP that the local jurisdiction designates, with delivery of ALI and ANI as secondary objectives.

6.4.2 Benefits

Among the benefits is that every resource connected to the network will be visible to every other resource. The ability to create a transparent system of systems without relying on a particular type of equipment, device, or protocol is very beneficial in the NG9-1-1 design. The primary focus is to be able to allow access into the network from any device and transfer that information through the system to a call taker. Using the NG9-1-1 system of systems approach with the elements described here, a WAN designed using standard IP routing can offer a resilient private network capable of any-to-any connectivity. The NG9-1-1 network intends to offer interoperability among PSAPs, radios, video, voice, text, and data. Development of applications for such a network is only the beginning. As the network evolves, the system of systems approach to the NG9-1-1 System will enable more development of public safety specific applications that have not been available.

6.4.3 Considerations

The entire network is to be constructed as a transparent system of systems allowing for interconnection to all of the elements required to deliver an emergency call. Therefore, the WAN approach to routing traffic to the PSAP will greatly enhance the ability to transfer critical information from a variety of devices. The NG9-1-1 system of systems infrastructure will allow for any-to-any communications across the platform. This overarching structure will enable the platform to grow as the bandwidth needs dictate without limiting traditional telecommunications facilities.

A VPN architecture is included in this analysis to create a seamless, transparent yet flexible alternative to dedicated architectures. The VPN model is typically able to conform to IP-based communications without relying on specific physical telecommunication bandwidth limitations.

VPNs should be considered where available. However, this does not to imply that implementing a VPN is the only acceptable way to build an NG9-1-1 network. VPNs allow high-level security than common IP networks and continue to support the standards mentioned earlier.

Notes

Section 7: NG9-1-1 PSAP

The current E9-1-1 system relies on the telecommunications network to transport calls to the appropriate PSAP. The telecommunications network(s) of the NG9-1-1 System will be critical for transporting information from multiple sources to PSAPs. The telecommunications networks, although actually associated with a variety of media, can logically act as a common logical network interconnecting a nationwide system of PSAPs. Developing the NG9-1-1 network will require a network architecture consisting of communication requirements and an interconnection topology. Requirements to satisfy the communication needs of the system, include, but are not limited to, transport media (wired/wireless), interfaces, devices, protocols, service level agreements, routing, and topology. As a next generation system, NG9-1-1 will use the IP and routing capabilities to transform and link the existing public safety systems.

Introduction
Arch. Analysis Approach
Architecture Definition
Key Arch. Considerations
NG9-1-1 DB Services
NG9-1-1 Network
NG9-1-1 PSAP
IP Call Origination
Architecture Summary
Source References
Appendices

7.1 IP Call Distribution

7.1.1 Description

The transformation and integration of IP technology with NG9-1-1 is a major change from traditional E9-1-1. The impetus for the use of IP is its widespread and increasing standardization as the communication protocol for wired and wireless networks. The NG9-1-1 System must be able to interface with multiple systems and to transport traffic using a common protocol to achieve end-to-end interoperability. IP will be the enabling distribution protocol for NG9-1-1. Traditional E9-1-1 evolved toward a data traffic routing scheme based on small streams typically consisting of 10 numeric digits within the call stream (but sometimes including as many as 20). The structure of IP enables call distribution to the appropriate destination on a transport network. Each IP packet provides a destination and source header before the data payload. Consequently, IP packets can distribute calls across a nationwide system to the exact address and deliver the emergency call information.

The transition from the legacy 9-1-1 system to an IP-based network will require a complex planning effort and detailed architecture. The architecture should include multiple tiers of topologies with increasingly more distribution detail. At the highest level, the nationwide architecture will provide the IP transport backbone to which all PSAPs and public safety organizations will connect. The regional, state, and local public safety agencies will then define the physical and logical connectivity to the national transport network. Each of the PSAP connectivity and distribution functions must include detailed infrastructure design, routing, and interoperability. Because location and other data is part of the call stream, the system will enable call routing functionalities, including call distribution, based on established processes and business rules. A key design component is the integration of data pointers and triggers that can be defined, configured, and dynamically changed by system and PSAP data management. In E9-1-1 routing, the actual call entry point to the network can be critically important to determine distribution. In an IP network, however, call distribution is driven by the call's attached data rather than the network entry point of the stream. The call distribution/routing software analyzes this data and determines distribution/routing paths.

Customized PSAP-Based Call Distribution Versus Modified IP ACD Services

Once calls are received at the PSAP, they are recorded with the caller location (i.e., ALI). The ACD functionality that was typically provided as a separate component from the primary 9-1-1 equipment is now being included with the PSAP customer premise equipment (CPE). In traditional 9-1-1 systems, the ACD functions are primarily off-the-shelf features like those offered in standard commercial call centers. ACDs are most often used in medium-to-large PSAPs where there are high call volumes. This current PSAP functionality and operation will change dramatically in NG9-1-1 through the expanded use of software to perform many of the key functions, which in the current system, are highly dependent on hardware/physical equipment. Many hardware functions currently in place in the PSAP will be integrated into software. Emerging requirements have also warranted the integration of additional key ACD features and functions.

IP ACD services are currently using caller input to determine proper call distribution and treatment within virtual call centers. It is a strong possibility that IP ACD vendors could modify existing software to perform similar call distribution and treatment functions using call stream data for an NG9-1-1 PSAP. The calls would be handled by the IP ACD based on the information within the call data. IP ACD will determine the caller location, caller preferences, and other details specific to the type of call center involved in order to complete the call. Alternatively, another approach would be for vendors to develop customized PSAP-based call distribution processes within existing PSAP CPE, which currently may route and distribute calls based on incoming 9-1-1 trunk group or similar data. While it is premature to determine the best approach, it is clear that the necessary changes to fully realize NG9-1-1 will have a significant impact on the PSAP environment.

Data redundancy can be delivered via separate and dual dynamic processing; however, any pointer/trigger to a PSAP network or call taker position, must have a redundant physical path in case of failure of components at the time of the call. This redundant path pointer/trigger may be to the same PSAP/call taker or it may be a backup path. This will enable the system to immediately redirect calls when path failures occur at the network and PSAP level.

Secure IP distribution must be incorporated into the design and include a secure login and access process for defining call routing data pointers and triggers. Physical security must be provided for various components employed for call distribution, ranging from routing equipment to the actual cable throughout the distribution path. The design needs to ensure that those who can establish or dynamically update pointers/triggers can only do so within their own realms of responsibility; others must not have access.

Applicable standards include the NENA i3, which describes various architectural components relevant to call distribution, and NENA 58-001, which specifies various operational requirements of call distribution. There are also other NENA standards that were originally created for traditional E9-1-1, but that include generic requirements and recommendations that can also be followed in NG9-1-1 call distribution—these latter include NENA data standards 02-010 and 02-011, NENA 03-005 Generic Requirements for an Enhanced 9-1-1 Selective Routing Switch, NENA 03-006 Standards for E9-1-1 Call Congestion Management, and NENA 04-001 Generic Standards for E9-1-1 PSAP Equipment. In addition, other relevant documents, while they are not standards, include NENA 04-502 E9-1-1 PSAP Site Characteristics, NENA 04-503 Network/System Access Security, and NENA 08-501 Interface between the E9-1-1 Service Provider Network & IP-PSAP.

Additional research is needed regarding existing ACD standards that address technical, operational, and security issues, such as IP NG9-1-1 call distribution, which can take advantage of considerably more features, such as call stream data. This research may allow leveraging of architecture design and other work that has already been done.

IP-based call distribution in an NG9-1-1 environment is a considerable leap forward from what is offered via existing ACD features and capabilities. Because of this major shift/change, the architectural design is critical to NG9-1-1 operation. The design will provide the actual implementation of NG9-1-1 call distribution based on such factors as the caller's location, caller's language preference, medical and other data being transported with call stream, and many other possibilities.

7.1.2 Benefits

PSAP-based IP call distribution enables the determination of the route of the call to a call taker (or even to another PSAP or other entity) based on various factors contained in data found within the call stream, coupled with availability of call taker positions and groups.

This data-driven routing can include routing to specific position(s) based on the caller's location, device type, language preference, and/or other information in the call stream. It can permit the matching of call taker skill sets with appropriate calls and also allow geographic-specific knowledge to be included.

7.1.3 Considerations

Because customized dynamic call distribution is a new concept for those who manage 9-1-1 networks and PSAPs, the possibility exists that the data triggers and pointers could be established or dynamically updated poorly and/or inappropriately, possibly resulting in negative consequences.

For NG9-1-1 features and functions to be realized within several months, rather than several years, for at least some 9-1-1 entities, it is important that the appropriate entities (IP ACD and/or PSAP CPE vendors) have either already begun product/service development or that they begin quite quickly and, hopefully, with a clear understanding of what NG9-1-1 call distribution means and includes.

7.2 PSAP User Interface (Human Machine Interface)

7.2.1 Description

The information currently available to the PSAP operator is voluminous and has the potential to inundate and confuse. This issue will be exacerbated with the influx of next-generation capability within the NG9-1-1 System. Video streams, static imagery, and advanced routing capabilities can enhance situational awareness and emergency resolution only if they are integrated into a human machine interface (HMI) that allows the operator to quickly and intuitively interpret the data and forward as appropriate. It is therefore paramount that the HMI be designed with this issue in mind to effectively deliver the requisite information and access to operators based on the circumstances of each individual call.

The NG9-1-1 PSAP HMI should be capable of displaying and otherwise making available all data relevant to a given call. The interface should correlate and aggregate the data automatically without intervention by the call taker. The aggregation of call data should be performed consistent with the nature of the inbound call; calls established with text messages, photos, and/or video will cause the HMI to display additional data areas containing those transmissions and the controls to interact with that data. The controls to interact with the data will, in turn, depend on the nature of the data itself—text message elements should allow the operator to scroll through inbound message content as a conversation and should also allow the operator to respond via text messaging; video controls should allow pause, replay, etc.

Despite the influx of next-generation media and content, the HMI will simplify the operator’s experience by intelligently correlating data from disparate sources and databases and selectively including data in the display based on call contents. This integrated approach will mitigate the need for call takers to switch between applications and windows and the need to manually correlate the displayed data—dramatically increasing efficiency.

Multiple views of the total call data should be created such that core mandatory call data is visible at all times while still allowing display of non-mandatory data from other sources. As an example, there may be views that allow an operator to view and browse geospatial data from external systems, or perhaps an interface through which the operator can coordinate the distribution of collected call information to first responders via next-generation channels (e.g., e-mail, text messaging).

7.2.2 Benefits

The benefits gained through the incorporation of video, image, and multidirectional text messaging are tremendous and will enable a level of support and service unprecedented in current 9-1-1 implementations. Using such a broad range of information effectively in emergency response could potentially require a call taker to have a large number of applications open and ready to receive and transmit information. Not only is it time consuming and difficult to navigate numerous applications to view call data, it becomes exponentially difficult to correlate the data from one application to another. The added complexity in a next-generation environment would confound even the best and brightest of call takers or at least mire them in time-consuming manual data correlation at times when their attention should be focused on the caller.

A “single pane of glass” approach would dramatically increase operational efficiency compared with the model described above. Through the integration and correlation of the disparate data sources and applications into a single role and call-based view, call takers would no longer need to manipulate several applications to gain situational awareness. Training too can be simplified because call takers no longer need to master the individual applications to obtain relevant information. This effect has been proven and observed in other high-pressure, quickly evolving environments such as tactical elements of the military where accurate and timely situational awareness is imperative in support of decision making for command and control operations.

At the system level, a web-based HMI simplifies workstation configuration and deployment. Workstations no longer require buildout and configuration of a variety of software packages to enable the user to do his/her job—access to all application functionality and external systems is served by a cluster of servers via the user's web browser. This simplifies the subsequent rollout of new versions of the HMI because the software that handles the integration and display of data resides on a single cluster of servers instead of many workstations; installation occurs once, and all workstations can automatically use the new version immediately.

At the network level, the HMI will reside on infrastructure capable of addressing IP-based traffic, which not only fundamentally enables the integration of next generation data and content, but positions the NG9-1-1 System for simplified integration with additional future content. The telecommunications industry is moving toward an intersection of analog and IP-based transports. VoIP, SMS, and consumer-driven cellular device functionality are all serving as catalysts for progress toward this point. The NG9-1-1 System will fully use the SIP, which itself is IP based and is serving as the basis for the expansion of IP-based telecommunications capability, including the areas of VoIP, streaming video (3GPP), and H.323, which addresses a variety of audiovisual communication mechanisms. The result of this architectural direction is that the environment will be highly extensible because of its alignment with the pervasive enabling technologies that are being developed to drive the future of telecommunications.

7.2.3 Considerations

The HMI portion of the NG9-1-1 system will have to account for a variety of accessibility considerations as mandated by Section 508 of the Disability Act. Further detail regarding these requirements can be found at—http://www.section508.gov /index.cfm?FuseAction=Content&ID=12.

As the deployment of IP-based capability expands within the 9-1-1 environment, it may be prudent to consider the integration of all communications—analog, digital, or otherwise—into the application/workstation portion of the HMI. This approach would offer efficiency in terms of centralized data recording and playback, warehousing and archiving, and automated correlation across data types within the NG9-1-1 System. In this scenario, inbound calls and associated content would be automatically routed to the appropriate call taker's workstation, which would offer audio, visual, and textual capability in a single package. The call taker would then have the capability to share or re-route the inbound data to other call takers or PSAPs, which would prove vitally important in large-scale disaster scenarios where local PSAPs are unable to respond.

More traditional workstation integration approaches are discussed within NENA-04-004: NENA Recommended Generic Standards for E9-1-1 PSAP Intelligent Workstations.

Although there are a variety of additional considerations when discussing the PSAP User Interface/HMI, two particularly significant topics are outlined here in more detail:

- Developing software using open source or proprietary tools
- Leveraging COTS products or developing a proprietary tool.
- Open Source Versus Proprietary Tools

Traditionally, views on this topic have been polarized. Open source software development typically offers the benefit of source code access and a supporting community that is eager to refine its product. Alternatively, proprietary tools offer the benefit of assured support, albeit at a cost, and the backing of a corporate entity.

In recent times, and in the context of enterprise application development and integration, a new phenomenon has appeared—intermingling of open source and proprietary technologies. In particular, data interchange standards and the mechanisms that support them have been developed and refined within an open community, and developers of proprietary solutions have embraced these standards, enabling a wide range of integration options. Standards already defined in sources such as NENA 02-010 NENA Standard Data Formats for ALI Data Exchange & GIS Mapping and the NENA XML Repository will facilitate data integration through prescribed, agreed-upon information formats. Other standards that enable communication, such as SMS and video streaming (notably, those being developed by and for 3GPP2), will also play an important role in facilitating the integration of next-generation media and capabilities within the NG9-1-1 System.

All of the capabilities discussed in the preceding sections can be implemented within and supported by a number of commonly used application platforms. Enterprise applications have evolved over the years from mainframe and terminal-based tools to client-server implementations and, more recently, to web-based technologies. The advent of AJAX (Asynchronous JavaScript and XML) and related technologies have spawned a generation of applications that look and feel very much like traditional client-server or desktop applications while operating natively within a simple web browser. The capability to provide users with an interface experience consistent with the desktop applications that they are accustomed to using while maintaining a zero-footprint installation is particularly powerful as workstation configuration and new software release deployment become a non-issue. Development and integration of a web-enabled AJAX interface appear particularly applicable because the underlying XML and supporting services operate very similarly to the way modern integration platforms operate—the granular, low-level technologies are the same (XML, web services, etc.). Ultimately, this means that the commoditization and encapsulation of remote system data can easily be fully exploited by the presentation layer portion of the application because it is designed to consume data in the format the integration points already produce.

The body of work already established by NENA is a significant step in the right direction in terms of a standardized information model. In order for the NG9-1-1 System to be successful as an integrated solution, and in the interest of maintaining flexible, simplified integration with future technologies, new information model standards need to be integrated into a baseline of data interchange standards. The baseline NENA XML repository should be augmented to include standards for each of the next generation content types and communication channels. In some cases, information models may already exist and are accepted as industry standards. In other cases, there may be a variety of information models represented across the industry with no clear front-runner. In still other cases, there may be no pervasive information model at all. In lieu of an approved standard for data interchange, a joint industry and government consortium should be considered to identify standards for information models and integration points. This approach will also ensure progressive development and adoption of standards to support emerging communication mechanisms.

COTS Versus Custom-Developed Tools

The reliability of the HMI will depend largely on the technology and integration approach used for the infrastructure on which it resides. In an environment in which timeliness and accuracy of data can affect a person's welfare, data integration features such as assured message delivery become vitally important. While modern relational database management systems (RDBMS) generally support standard interfaces (e.g., ODBC, OLEDB) for interaction and integration, those interfaces rarely provide for assured message delivery. This feature becomes increasingly important as the number of integrated external systems increases; the more systems integrated in the solution, the more important a centralized integration mechanism becomes.

Creating this type of functionality from scratch would be costly and error-prone. There are a wide variety of COTS and open-source products and technologies that enable this type of system-to-system communication. These products range from enterprise-class integration engines such as Microsoft's BizTalk to open-source components such as the Java Message Service (part of J2EE) and proprietary components such as Microsoft's

Message Queue. The latter two components would require custom development to place messages in a queue and receive and process on the opposite end of the integration, whereas products such as BizTalk are designed to handle the receipt and delivery of messages as well as perform complex transformations and business logic. Moreover, these enterprise-class solutions typically have "adaptors" available for purchase that allow them to integrate with other enterprise solutions such as SAP, PeopleSoft, and others in a turn-key fashion. An enterprise integration platform offers the capability to commoditize heterogeneous data sources and formats so that they can be transformed into any other configured format and relayed to any attached system. In terms of scalability, clustering capabilities are also common among these products, which means that after initial deployment, scaling the platform's capability is as simple as adding additional hardware to the mix.

Notes

Introduction
Arch. Analysis Approach
Architecture Definition
Key Arch. Considerations
NG9-1-1 DB Services
NG9-1-1 Network
NG9-1-1 PSAP
IP Call Origination
Architecture Summary
Source References
Appendices

Section 8: IP Call Origination/IP Access Network

With the advent of the IP telephony and voice/video/data convergence, providing IP-based access to the NG9-1-1 network is a critical requirement. It offers flexibility to the end users to initiate emergency calls using multimedia handheld devices such as mobile phones, PDAs, etc. In addition, because traditional telephony users are fast migrating to VoIP service, it is imperative that the NG9-1-1 architecture support emergency calls that originate from IP UAs, sensors, and telematics devices.

The NG9-1-1 architecture should be able to effectively and efficiently accept emergency calls from the Internet and other IP-based networks and terminate the calls to an appropriate PSAP. End-to-end IP-based calls (i.e., emergency calls originating from an IP end system and terminating in an IP-capable PSAP), conveyed entirely over an IP network is a critical operational scenario for the NG9-1-1 architecture.

8.1 IP-based Access to NG9-1-1

8.1.1 Description

Supporting IP-based calls will require PSAPs to transition from traditional circuit-switched interfaces to packet-switched technology. Key elements required to provide IP-based access to the NG9-1-1 environment are mechanisms to—

- Identify origin and location of emergency IP calls
- Route emergency IP calls to the PSAP that has jurisdiction over the location.

Section 3 of this document outlines both a high-level and detailed view of key architectural components required to support IP-based emergency calls. However, because of the technical advantages of IP-based multimedia applications, the current emergency calling architecture must be further refined. The IETF has created the ECRIT working group to address issues associated with routing emergency calls over the Internet. The ECRIT effort will result in several changes to the existing 9-1-1 architecture and will require retrofitting existing IP networks to be able to determine the location of the IP-based 9-1-1 calls and deliver them to the appropriate PSAP.

The purpose of this section is to provide guidance in developing key architectural components for providing IP-based access to the NG9-1-1 systems. This section discusses in detail the following sub-components required to support IP-based calls:\

- IP emergency call origination and location determination
- IP emergency call routing/signaling.

It also identifies risks, benefits, and security considerations associated with providing IP-based access to the NG9-1-1 environment. In addition, all applicable standards and guidelines have been leveraged to ensure compliance with industry best practices.

8.1.2 Benefits

Enabling IP-based access to NG9-1-1 systems provides several benefits. Most IP endpoints have the capability to connect to the Internet. Using this feature, endpoints can connect to the Internet and other IP networks, allowing the caller to send voice, video, and text messages to the NG9-1-1 System. The IP technology efficiently transmits these multimedia messages over service providers' networks to the appropriate PSAPs. This constitutes an important benefit to the NG9-1-1 architecture because the call taker at the PSAP is presented with both audio and visual information pertaining to the emergency situation. The call taker can also forward these messages to the first responders, which allows them to prepare in advance. Another benefit of this architecture is that it leverages current IP infrastructure deployed by service providers and organizations to facilitate end-to-end communications between IP endpoints.

8.1.3 Considerations

Currently, standards do not exist for providing IP-based access to the NG9-1-1 systems. IETF has established a working group for identifying technical solution for supporting emergency calls on IP networks such as the Internet. The effort is called the ECRIT working group. The working group has developed several Internet drafts for supporting emergency calling using IP-based multimedia applications. The proposed architecture leverages activities currently being conducted by ECRIT.

While IP-based access to 9-1-1 is the primary focus of this and other documents within the NG9-1-1 Initiative, there are non-IP issues that will also need to be resolved. For example, devices that transmit SMS and text messages do not currently support location determination when sending messages. Providing that important feature requires changes outside of NG9-1-1 and needs further investigation.

8.2 IP Call Origination

8.2.1 Description

The next generation architecture supports origination of IP calls using IP UAs such as IP phones, laptops, and IP-enabled wireless devices. IP/SIP UAs should register with a Call/SIP Register server so that emergency calls can be registered within the call originating network, enabling the PSAP to call back after the call is completed, if required. The UA can either have a static IP address provided by a service provider or can acquire dynamic IP address using the Dynamic Host Configuration Protocol (DHCP). The UA should be able to detect emergency dial-strings and perform translation to an emergency Uniform Resource Name (URN) internally or by using a proxy server, as defined in the ECRIT working group drafts.

Identifying the location of the emergency call origination is important to ensure that PSAPs provide the right location information to the emergency responders. The proposed architecture recommends three modes for providing the location information as defined in the IETF's ECRIT requirements. These are—

1) Inserted by the endpoint—The endpoint inserts into the call signaling protocol the location information provided by the GPS, a third-party tool, call server, or any other mechanism.
2) Endpoint referenced—The endpoint provides an identifier to the location information stored in a server.
3) Inserted by a proxy—An intermediary device (e.g., LoST) provides the location information. See Section 8.3 for more information on LoST.

The location information must include the source of data such as the GPS, manual entry, or access network. Once the location has been identified and validated, the information should be included in the signaling protocol and will be used by other entities in the call path to perform call processing to establish an emergency call to the appropriate PSAP.

8.2.2 Benefits

The ability to originate and deliver emergency calls using IP UAs such as IP phones, laptops, and IP-based wireless devices is an important benefit of the NG9-1-1 architecture. It provides flexibility to the end users to originate emergency calls using common consumer devices that can connect to the Internet. Using these devices the end user can transmit voice, video, and data messages to the service provider or to a PSAP's IP-enabled CPE device. The NG9-1-1 architecture leverages this capability to capture and provide the emergency call taker with vital information concerning the emergency situation. This will help the first responders to better prepare themselves prior to reaching the emergency location.

The past several years have seen increased deployment of IPBXs. Most organizations are upgrading their PBX to IPBX to leverage features and functionalities of the IP. The call origination component of the NG9-1-1 architecture provides the capability for the IP UAs to interface with the IPBX. End users can leverage this capability to connect their IP devices to their organizations IPBX and originate emergency calls, if required.

The NG9-1-1 architecture also includes support for telematics and IP-based sensor devices. Security cameras and sensor devices can initiate emergency calls if any security breach/emergency situation is detected by them. Using IP networking, they can transmit statistics and data through NG9-1-1 to an IP endpoint located at a PSAP or an emergency call center. The NG9-1-1 architecture thus broadens the scope of devices/endpoints that could originate emergency calls.

8.2.3 Considerations

Supporting emergency calls over IP networks introduces security issues. Emergency service is an obvious target for deliberate attack, specifically denial of service (DoS) attack. The architecture should incorporate adequate security measures to detect and mitigate such attacks while continuing to provide seamless and efficient service to genuine callers. However, security measures should not become an impeding factor for establishing end-to-end emergency calls over IP networks. Data confidentiality and integrity should be maintained at all times, and technologies such as digital certificates should be used to validate users. In order to prevent fraudulent calls to PSAPs, features such as authentication should be provided to identify source provider legitimacy.

Adequate redundancy should be built into the architecture to ensure that emergency calls are not dropped in the event of equipment failure or path congestion. All infrastructure associated with location identification, service mapping, and call routing should be redundant. PSAPs should have redundant edge routers and circuits connected to multiple Internet service providers (ISP) to ensure high availability and path redundancy. Call routing protocols should be able to establish multiple paths to the PSAP edge routers and route calls using secondary path in case the primary path becomes unavailable.

8.3 IP Call Routing/Signaling (LoST/SIP)

8.3.1 Description

Call routing based on location information should be conducted using either the LoST protocol or other similar protocols. The ECRIT working group has published detailed drafts describing ECRF and functions of the LoST protocol. In the past year, significant progress has been made to develop features and functionality within the LoST protocol. LoST provides a number of operations, focused on mapping locations and service URNs to service URLs and associated information.

The ECRIT working group defines a database query (called a “mapping”), which contains location information and a “service;” the response is a URL indicating where to deliver the call—this is the ECRF process. The call would then be routed using normal SIP (or other protocols supported) to the indicated destination. The protocol defined by the IETF that provides the mapping is called the LoST.

The NENA i3 architecture envisions that, in many cases, the route taken as a result of ECRF mapping will not be directly to a PSAP. Instead, calls will be routed to an ESRP. This element, which might be operated on behalf of, for example, a state agency, would take all calls for that state and make another routing decision to send them to the appropriate PSAP. The reason for deploying an ESRP is to position robust firewalls and other protective devices (such as the BCF), with large amounts of IP bandwidth between the sources of calls and the PSAP. This provides an outer defensive perimeter to protect the PSAP from malicious calls or DoS. i3 envisions that the same ECRF, using LoST as the interface protocol, will be able to be queried by the ESRP to determine how to route the call onward to the PSAP.

Similarly, the ECRF mechanism may be used by the PSAP to determine how to route a call to the correct responder. The ECRF will allow storage of civic and geo boundaries for PSAPs (and ESRPs) as well as any number of responders. This allows any

PSAP to route a call to any responder based on the location of the caller. This mechanism directly encodes service boundaries. Given a location and a desired service (police, fire, mountain rescue, etc.), the mechanism returns the URI of the appropriate responder. As with the PSAP routing, the call may traverse one or more ESRPs.

The LoST protocol provides several other important functions used for emergency calling. LoST will supply the local dial string (9-1-1) for a location. This is used by the endpoint or proxy to differentiate an emergency call from other calls. LoST also is used for the Location Validation Function. If a route exists for a location, that location is valid, and thus LoST can report which locations are valid using the same database as the routing function. This is similar to the current MSAG that supplies the "route" (that is, the ESN) as well as the validation data.

LoST is proposed to use 9-1-1 Authority managed, GIS-based map layers of validated civic addressing or geodetic boundary data for PSAP jurisdictions and emergency responders in order to determine how to route a caller or emergency location to the appropriate PSAP or other entity destination. It can cache individual mapping information, which provides robustness against network failures. In addition, LoST messages are sent using Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS) protocols, which enables use of TLS to protect the integrity and confidentiality of the requests and responses.

The routing protocol must also ensure that all emergency calls are prioritized as they move through IP networks to avoid the possibility of dropped calls. At the time of emergency calling, the IP endpoint should attempt to validate the caller's location using its location acquisition function or cached values. During the location to service mapping process, the protocol should determine the service boundary and identify services available for a particular location. Based on the information obtained by the protocol, the call should be routed to the PSAP that has jurisdiction over the location. ESRP servers should be used to make routing decisions based on PSAP state and location of the caller to identify the appropriate PSAP. An ESRP primary role is to invoke the location-to-PSAP URI mapping function and to return an appropriate PSAP URI or the URI for another ESRP.

Signaling protocols such as SIP should be used to resolve URIs to a next hop destination, if required. As mentioned in the ECRIT drafts, signaling information should be protected using the TLS or GeoPriv protocol to meet privacy requirements for geospatial data. Appropriate authentication mechanisms should be used to validate the caller and to ensure that the PSAP's IP devices are not subject to DoS attacks. Secure VPNs can be established between edge routers to provide network layer security, if required.

Emergency calls routed over IP networks should be prioritized using existing queuing technologies such as LLQ to ensure that calls are not dropped because of link congestion. LLQ is the preferred queuing mechanism to prioritize VoIP traffic over IP networks. Queuing mechanisms and traffic policies currently used by ISPs and service providers must be refined to ensure that 9-1-1 calls are effectively prioritized and routed to the NG9-1-1 network.

8.3.2 Benefits

Routing emergency calls over IP networks is an important benefit of the NG9-1-1 architecture. Convergence of voice, video, and data technologies have resulted in a ubiquitous architecture based on IP. IP gateways have become an important component in facilitating convergence of these technologies. Thus, encapsulating the emergency location information and using IP to route the information to the PSAPs is an important advantage of the NG9-1-1 architecture. The IP protocol also supports QoS features for reserving bandwidth end-to-end and to prioritize mission-critical traffic over both public and private networks. The IP Access component of the NG9-1-1 architecture can leverage both of these features to guarantee delivery of emergency information to the appropriate PSAPs.

IP routing protocols can automatically choose alternate path from source to destination in case of the primary path failure. This feature of the IP routing protocols is an important benefit to the NG9-1-1 architecture because IP will ensure that multiple paths are available to route emergency calls to the PSAP.

8.3.3 Considerations

IP networks can also connect to non-IP networks using gateways. IP gateways allow flexibility in connecting to non-IP endpoints such land mobile radios (LMR) and analog phones. The architecture proposes using standard IP gateways to connect to non-IP networks. Most communications product vendors currently market IP gateways as part of their product line. Based on individual requirements, service providers and PSAPs should select and deploy appropriate gateways to interface with their IP and non-IP networks.

IP is considered a connectionless protocol. It does not guarantee end-to-end packet delivery. The primary risk of using IP technology for establishing emergency calls is that IP alone cannot be trusted to set up the call. Other signaling, transport, and applications layer protocols are required to set up the call over IP networks. This could potentially lead to interoperability and integration issues in some cases.

Providing IP-based access to the NG9-1-1 network is an enormous step toward defining the NG9-1-1 architecture. It provides flexibility to callers to generate emergency calls using IP endpoints, such as soft phones and PDAs, that are already part of their daily activities. With current wireless technology enabling Internet access from handheld devices, it has become critical that IP networks support and route emergency calls efficiently and effectively to the appropriate PSAPs. PSAPs must upgrade their infrastructure to support calls routed over IP networks. Current interfaces and applications must be upgraded to support functionality such as IP routing, automatic call distribution, and call termination.

Section 9: Architecture Summary

The high-level NG9-1-1 System architecture analysis has been developed by evaluating various source documents and leveraging the experience and knowledge of public safety and IP networking subject matter experts, along with a careful consideration of emerging and accepted technologies and standards. This resulting document describes the approach, methodology, and initial recommendations for the NG9-1-1 architecture. These initial recommendations should be used as a flexible system framework (how it **could** be built) and *not* a blueprint for how NG9-1-1 **must** be implemented.

It is expected that 9-1-1 authorities throughout the nation will evaluate this proposed structure and, based on the content of this report, make decisions that fit their individual needs. A "best-of-breed" concept will emerge, and although the NG9-1-1 networks will be implemented with different hardware and software, the systems will be interoperable because of the established connectivity and communications standards. System components will change and improve as technology matures and as important lessons are learned from other initiatives (similar to NG9-1-1) that are implemented.

With the proposed architecture as a guide, 9-1-1 authorities can identify their specific system and functional requirements. Once the requirements have been gathered, they can be mapped to the architecture, ensuring that the system hardware and software will meet the baseline needs of the Authority.

A number of significant architectural considerations must inform the identification of specifications for an NG9-1-1 network. One major consideration is how the NG9-1-1 network will interface with other NG9-1-1 networks and the ESNet. Although the ESNet will provide a standardized backbone to interconnect PSAP and NG9-1-1 networks, the NG9-1-1 System must adhere to those standards identified to ensure compatibility among the connected entities.

Another significant architectural consideration is how the system will be secured. Protecting the integrity of the system is of paramount importance for all involved stakeholders. Security must be multifaceted and implemented at multiple levels. Industry best practices will help determine the intrusion protection, firewall, and identity management products to employ to protect the NG9-1-1 System.

This NG9-1-1 Architectural Analysis document is the first iteration of the NG9-1-1 design framework. Future design versions may incorporate new technologies, including access devices, networking, and system components. System designs will also improve based on lessons learned from similar implementations, the NG9-1-1 Initiative Task 3 (PoC phase), as well as a broader review by various stakeholders and other industry professionals.

Section 10: 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.

Introduction
Arch. Analysis Approach
Architecture Definition
Key Arch. Considerations
NG9-1-1 DB Services
NG9-1-1 Network
NG9-1-1 PSAP
IP Call Origination
Architecture Summary
Source References
Appendices

- *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.

- The ATIS-ESNet Next Generation Emergency Services (NGES) Subcommittee will define a new messaging and interaction protocol between PSAPs and Emergency Services Networks to significantly expand the paradigms that provide those services today. Various summaries and briefing materials are available at the NGES Subcommittee website at http://www.atis.org/esif/nges.asp. The NGES messaging and interaction protocol will be specified as an American National Standard (ANS). Messaging interfaces have been adopted for trial use.

- *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 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 VDB, ERDB, and system administrator to maintain the 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 foreseeably 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.

- *NENA Operations Information Document (OID) on Video Relay Service & IP Relay Service PSAP Interaction*. [NENA 52-5xx—Pre-publication] NENA Operations Development Committee. Document is not currently available to the public. This OID will provide information to PSAPs and telecommunications relay service providers about how to best manage the operational interface between PSAP call takers and service providers that will be forwarding calls from the deaf and hearing-impaired community.

- *NENA TID on Emergency Services IP Network Design*. [NENA Document Number TBD—Pre-publication] NENA VoIP/Packet Technical Committee. This document is not currently available to the public. This TID will provide information for PSAPs in developing IP networks for emergency communication use.

NOTES

Appendix A: Acronyms

AAA	Administration, Accounting and Authentication
ACD	Automatic Call Distributor
ACN	Automatic Collision Notification
AJAX	Asynchronous JavaScript and XML
ALI	Automatic Location Information
ANI	Automatic Number Identification
ANS	American National Standard
ATM	Asynchronous Transfer Mode
BCF	Border Control Function
BGP	Border Gateway Protocol
CAMA	Centralized Automatic Message Accounting
CMRS	Commercial Mobile Radio Service
COI	Community of Interest
COOP	Continuity of Operations
COTS	Commercial Off-the-Shelf
CPE	Customer Premises Equipment
DB	Database
DBMS	Database Management System
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DoS	Denial of Service
DR	Disaster Recovery
DRM	Data Rights Management
E9-1-1	Enhanced 9-1-1
ECRF	Emergency Call Routing Function
ECRIT	Emergency Context Resolution with Internet Technologies
EMS	Emergency Medical Services
EPAD	Emergency Provider Access Directory
ERDB	Emergency Services Zone Routing Database
ESAR	Enterprise Segment Activity Roadmap
ESGW	Emergency Services Gateway
ESN	Emergency Services Number
ESNet	Emergency Services Network
ESRP	Emergency Service Routing Proxy
ESZ	Emergency Service Zone
FCC	Federal Communications Commission
GIS	Geographic Information System
GPS	Global Positioning System
HMI	Human Machine Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IdAM	Identity and Access Management
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPBX	IP-based Private Branch eXchange
IPSec	Internet Protocol Secure
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
ITU	International Telecommunications Union
LDT	Location Determination Technology (synonymous with Position Determining Entity [PDE])
LEC	Local Exchange Carrier
LIS	Location Information Server
LLQ	Low-Latency-Queuing
LMR	Land Mobile Radio
LoST	Location-to-Service Translation
MPC	Mobile Positioning Center
MPLS	Multi Protocol Label Switching
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
NGES	Next Generation Emergency Services

NRIC	Network Reliability and Interoperability Council
OID	Operational Information Document (NENA)
OSI	Operating System Interface
PBX	Private Branch eXchange
PCS	Personal Communications Services
PDA	Personal Digital Assistant
PDE	Position Determining Entity (synonymous with Location Determination Technology [LDT])
PoC	Proof-of-Concept
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RDBMS	Relational Database Management System
RTP	Real-Time Protocol
SIP	Session Initiation Protocol
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SOA	Service-Oriented Architecture
SONET	Synchronous Optical Network
SRDB	Selective Router Database
SSL	Secure Socket Layer
SSO	Single Sign-On
TCP	Transmission Control Protocol
TIA	Telecommunications Industry Association
TID	Technical Information Document (NENA)
TLS	Transport Layer Security
TTY/TTD	Teletype/Telecommunications Device for the Deaf
UA	User Agent
URI	Uniform Resource Identifier
URL	Universal Resource Locator
URN	Uniform Resource Name
USDOT	U.S. Department of Transportation
VDB	Validation Database
VoIP	Voice over Internet Protocol
VPC	VoIP Positioning Center
VPN	Virtual Private Network
WAN	Wide Area Network
WiMAX	Worldwide Interoperability for Microwave Access

Notes

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.
Activity	See “Functional Activity.”
Analog	Continuous and variable electrical waves that represent an infinite number of values; as opposed digital.
Association for Public-Safety Communications—International (APCO)	A not-for-profit organization established in 1935 and the world’s largest organization dedicated to public safety communications. Members rely on APCO for their professional needs—from examining standards and issues to providing education, products and services, and frequency coordination services.
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 Collision 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.
Commercial Mobile Radio Service (CMRS)	A category of wireless telephone service regulated by the Federal Communications Commission (47 CFR 20.9). It includes both cellular and Personal Communications Services (PCS) telephone service.
Configurability	Property of a system that supports the rearrangement of interfaces and functionalities.
Continuity of Operations (COOP)	A system's ability to prevent critical system failures (e.g., via component redundancy) and to seamlessly conduct updates and repairs.
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.

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.”
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.
Session Initiation Protocol (SIP)	A signaling protocol used to exchange data (including voice, video, and text) among an association of participants. [RFC 3261]
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.

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. 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.
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 Agent (UA)	Typically used to describe a SIP-based phone; however, for this document, used to generically describe a call origination device.
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.
Worldwide Interoperability for Microwave Access (WiMAX)	A standards-based technology that enables delivery of “last mile” wireless broadband access, WiMAX includes fixed, nomadic, portable, and soon, mobile wireless broadband connectivity.
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. See Commercial Mobile Radio System (CMRS).
Wireline	Standard telephone and data communications systems that use in-ground and telephone pole cables. Also known as landline or land-based.

Notes