NENA Technical Information Document on the Network Interface to IP Capable PSAP

NENA-08-501 Issued June, 2004

NENA Technical Information Document on the Interface between the E9-1-1 Service Provider Network and the Internet Protocol (IP) PSAP

Prepared by:

National Emergency Number Association (NENA) Migration Working Group of the Network Technical Committee

Published by NENA

Printed in USA

NENA

TECHNICAL INFORMATION DOCUMENT

NOTICE

This Technical Information Document is published by National Emergency Number Association (NENA) as technical information to guide providers of Emergency Service Networks and Data and their equipment suppliers, and for the designers and manufacturers of customer-premise systems that are used for the purpose of processing emergency calls at a Public Safety Answering Point (PSAP). It is not intended to provide complete design specifications or parameters nor to assure the quality of performance of such equipment.

NENA reserves the right to revise this Technical Information Document for any reason including, but not limited to, conformity with criteria or standards promulgated by various agencies, utilization of advances in the state of the technical arts or to reflect changes in the design of equipment or services described therein.

It is possible that certain advances in technology will precede these revisions. Therefore, this Technical Information Document should not be the only source of information used to implement network changes or to purchase Customer Premise Equipment (CPE). NENA members are also advised to contact their Telephone Company representative to ensure CPE compatibility with the Telco network.

The techniques or equipment characteristics disclosed herein may be covered by patents of some Corporations or others. No license expressed or implied is hereby granted. This document is not to be construed as a suggestion to any manufacturer to modify or change any of its products, nor does this document represent any commitment by NENA or any affiliate thereof to purchase any product whether or not it provides the described characteristics.

This document has been prepared solely for the voluntary use of E9-1-1 service providers, E9-1-1 equipment suppliers, and participating telephone companies.

By using this document, the user agrees that the NENA will have no liability for any consequential, incidental, special, or punitive damage that may result.

This draft document is based on the DRAFT NENA Standard for Creating Or Updating E9-1-1 Technical References developed by the NENA PSAP standards Committee and further developed by the NENA Technical Committee Chairs. The NENA executive board has NOT recommended that document for industry acceptance. This draft document is being proposed as a draft. Recommendations for changes to this document may be submitted to:

National Emergency Number Association
1700 Diagonal Road, Suite 500
Alexandria, VA 22314
202.466.4911
or commleadership@nena.org

Acknowledgments:

This document has been developed by the National Emergency Number Association (NENA) Migration Working Group.

The following industry experts and their companies are recognized for their contributions in development of this document.

Group Leader: Nathan Wilcox State of Vermont Enhanced 9-1-1

Members:	**Company**
Nadine Abbott	Telcordia
Anand Akundi	Telcordia
Spencer Angel	CML
Richard Atkins	Tarrant County 9-1-1 District
Chuck Bell	Sprint
Jim Beutelspacher	State of Minnesota
Eileen Boroski	Intrado
Tom Breen	BellSouth
Larry Ciesla	Intrado
Kevin Eckhardt	Zetron
Pete Eggiman	Metro 911 Board, St Paul, Mn
Richard Frye	Orbacom Systems
Jay Fuller	Plant Equipment
John Gerberg	SBC Pacific Bell
Steve Gillies	ACX
Roger Hixson	NENA
Bill Johnson	Orbacom Systems
Scott Keagy	Cisco Systems
Gordon Kelly	CML
Mark Knox	Intrado
Ron Mathis	Intrado
Robert Miller	RCC
Martin Moody	State of Minnesota
Mark Payne	Denco Area 9-1-1 District
Kantu Patel	SBC/Pacbell
Nancy Pollock	Metro 911 Board, St Paul, Mn
Keith Ritchie	Bell Canada
Jim Rusmisel	PSAP Data Resources
Joseph Sallak	J&J Consulting
Peter Schmidt	Intrado
Henning Schulzrinne	Columbia University
Steve Sipple	Nortel Networks
Allan Spivey	Zetron

Table of Contents

1 Executive Overview

1.1 Purpose and Scope of Document

This "NENA Technical Information Document on the Network Interface to IP Capable PSAP" document provides technical information to guide manufacturers of network equipment and Public Safety Answering Point (PSAP) Customer Premises Equipment (CPE) in the development of Internet Protocol based interfaces between the network and PSAP CPE and to assist E9-1-1 Network Service Providers and PSAP's in implementing such interfaces. It defines a service description for the capabilities that will need to be supported by the VoIP signaling on the interface, as well as the necessary network and CPE elements needed in the supporting architecture. The Appendices to this TID include specific assumptions/issues for individual candidate Voice over Internet Protocol (VoIP) signaling protocols, that will need to be considered in the specification of (separate) technical reference document(s) that provide signaling requirements for the individual VoIP protocol alternatives identified.

1.2 Reason to Implement

The NENA Technical Information Document on Network Interfaces for E9-1-1 and Emerging Technologies identified Voice over Internet Protocol (VoIP) as an emerging technology that needs to be considered for the interface between the E9-1-1 Service Provider's Network and the PSAP CPE. PSAP's are experiencing an increasing need to receive and share data related to emergency call handling. Many carriers and enterprise networks today are implementing broadband access and packet data networks that can support both voice and data traffic. Packet-based voice and data delivery may offer a more robust and diverse transport for emergency services, and can aggregate the numerous services required by PSAP's into a common broadband access. Several competing signaling technologies are being developed that support VoIP for normal call traffic. This TID identifies the signaling capabilities and interface requirements to support the special signaling needs of emergency call handling.

1.3 Benefits and Risks

Use of this NENA TID will promote a convergence toward VoIP signaling standards that can support the terminating functions of emergency call handling at PSAPs. A packet based network access from the PSAP to the PSTN (i.e., the E9-1-1 Service Provider's E9-1-1 Tandem Office(s)1) will:

- Allow voice and data, 9-1-1 and administrative lines to share common access reducing the number and types of interface devices to be supported. Common access will also allow for more flexibility and potential cost savings for alternate routing of calls in PSAP site emergency situations (accommodated as simply another type of call redirection).
- Allow for more flexibility in accommodating PSAP call-taking from remote sites. For example, if a PSAP were incapacitated, call-takers at an emergency back-up site could be registered remotely at shared VoIP network elements to receive emergency calls for that PSAP.
- Allow for the potential to improve call setup time performance. Existing MF (CAMA-like,

[1] An E9-1-1 Tandem Office is also referred to in NENA documents and in conventional circuit-switched E9-1-1 Service Provider Networks as an *E9-1-1 Control Office* or a *Selective Router*. The preferred is E9-1-1 Control Office.

(Centralized Automatic Message Accounting)) and E-MF (Enhanced Multi-Frequency) trunk access to PSAPs include a minimum delay in call setup time of approximately 2 to 4 seconds. If replaced by digital signaling (of which VoIP is one alternative), this delay could be almost completely eliminated. However, note that VoIP solutions that require a VoIP gateway conversion from MF/E-MF to digital/VoIP signaling will not eliminate the delay inherent in MF signaling.

- Allow for increased functionality. IP based networks have the potential to accommodate more flexibility in method and formats for delivery of callback and location information.
- Allow more flexibility to accommodate emerging technologies and needs. For example, as emerging technologies that support wireless text-based messaging proliferate (e.g., wireless Short Message Service and wireless PDAs), there will be an increasing demand for PSAPs to have an approach to receive and handle text-based emergency contacts. An IP-network based solution will more gracefully accommodate delivery of such contacts to PSAPs.
- Provide routing diversity
- IP based network solutions simplify the ability to support multi-media calling in the future. For example, an IP based network can be leveraged to support transfers of emergency calls, along with accumulated call information to a secondary PSAP. Similarly, Automatic Collision Notification calls could be supported with coordinated voice/data/video sessions.
- Provide call-processing flexibility.
- There is an opportunity to increase migration away from special purpose equipment toward E9-1-1 specific application software on standard equipment and interfaces.
- VoIP solutions leverage a mature data services solution. TCP/IP is a proven technology, standard off-the-shelf equipment is available and affordable, and many PSAP CPE vendors already support TCP/IP for data applications.
- Interoperability between competing application layer protocols supporting VoIP is a result of the relative immaturity of the technology. Many industry experts believe that these issues will be resolved in the near future.
- As E9-1-1 Service Providers migrate toward VoIP network architectures, and the functions currently provided by E9-1-1 Tandems migrate to other VoIP network elements, this interface document should also provide a basis to support this migration of functionality.
- IP-based architectures have a significant advantage in the ability to share/exchange data between two parties engaged in a voice call. For example, when a call is transferred between a PSAP and another public safety entity, large amounts of data could be transferred as well.

Developers who consider deploying IP to support voice should be aware of the potential pitfalls. These can include:

- Technology driven by “best-effort” does not always guarantee a solid quality of service (although this is slowly being addressed (e.g. ITU-T Recommendation I.350 for ATM))
- Voice Quality of Service (QoS) is an important consideration for emergency calls. QoS solutions are coming on the market; however, service providers will need to give careful attention to implementation to ensure voice QoS equivalent to the PSTN. QoS will also depend on the QoS provided by the originating IP network service provider.
- One of the potential advantages of VoIP is in improved efficiency (reduced cost) that can be

achieved with compression and silence suppression techniques. However, these techniques may not be appropriate for emergency calls in which "background noise" can be an important part of the call (both for the call-taker and for logging recording purposes). It may not always be possible to suppress these techniques, for example, if they are invoked by an emergency caller's VoIP equipment/applications.

- The initial availability of VoIP providers and vendors may create concern among customers. It will be desirable to leverage standard VoIP equipment and interfaces wherever possible; however, some E91-1 specific functions may require special applications and functions. Equipment interoperability will be a concern that can be mitigated by aggressive attention to incorporating support for E9-1-1 PSAP needs and functionality in VoIP standards.
- The perceived immaturity of the technology
    - TCP/IP was created in 1982 and packet switched networks have been around since 1968
    - VoIP is now in use at approximately 70% of the Fortune 1000 companies
- When expanding overlying private VoIP 9-1-1 networks, security concerns at one location will affect all participant networks.
    - Require conformity to accepted security certifications as defined by a nationally recognized 9-1-1 authority (i.e. NENA)
- TTY/TDD communications may be negatively impacted by packet loss.
    - Refer to section 2.4 for a possible resolution.

However, if history proves true, much like the development of circuit switched technology; the industry interest in VoIP networks will eliminate the pitfalls that are prevalent in development of this technology.

1.4 Terms and Definitions

TBD – See master glossary – Section 3

1.5 Effective Date

1.6 Document Terminology

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

1.7 Reason for Reissue

Document Number	Approval Date	Reason For Changes
NENA 08-501	June 2004	Initial Document
NENA 08-501.1	06/19/2015	Update web page links

1.8 Date Compliance

All systems that are associated with the 9-1-1 process shall be designed and engineered to ensure that no

detrimental, or other noticeable impact of any kind, will occur as a result of a date/time change up to 30 years subsequent to the manufacture of the system. This shall include embedded application, computer based or any other type application.

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

1.9 Major Initiatives:

The evolution of 9-1-1 call and data delivery from analog to IP will include the following initiatives that can be executed in any order:

PSTN to PSAP interface. Equipment at the edge of the PSTN will be needed to translate terminating calls to a VoIP format that will then traverse a packet-capable transport mechanism to the PSAP. The protocols used in a VoIP environment must meet certain criteria to be considered for use in a 9-1-1 environment (refer to appendix D for a blank checklist of VoIP capabilities versus specifications outlined in this T.I.D.). This document will consider the interface between the E9-1-1 Tandem and the PSAP over a VoIP Network. (The interface between a Local End Office and the PSAP is beyond the scope of this document.)

VoIP Network to PSAP interface. As E9-1-1 Network Service Provider functions migrate into elements within VoIP networks, the interface from the VoIP network to the PSAP must provide at least equivalent functionality to be considered for use in a 9-1-1 environment.

Network/ALI database. Modifications must occur to the equipment that will allow it to operate in a "native IP" environment. In the VoIP network, network elements may initiate retrieval of ALI information and deliver it with the call to the appropriate PSAP. Retrieval of ALI information may also continue to be initiated by the PSAP, e.g., while a voice call is in progress. The second aspect is beyond the scope of this document.

PSAP CPE. The equipment at the PSAP must be capable of viewing and utilizing packet data and/or voice in a native IP environment. This process is outside the scope of this document as well.

Figure 1-1 shows the various migration strategies that can be deployed for VoIP within an existing 9-1-1 network.

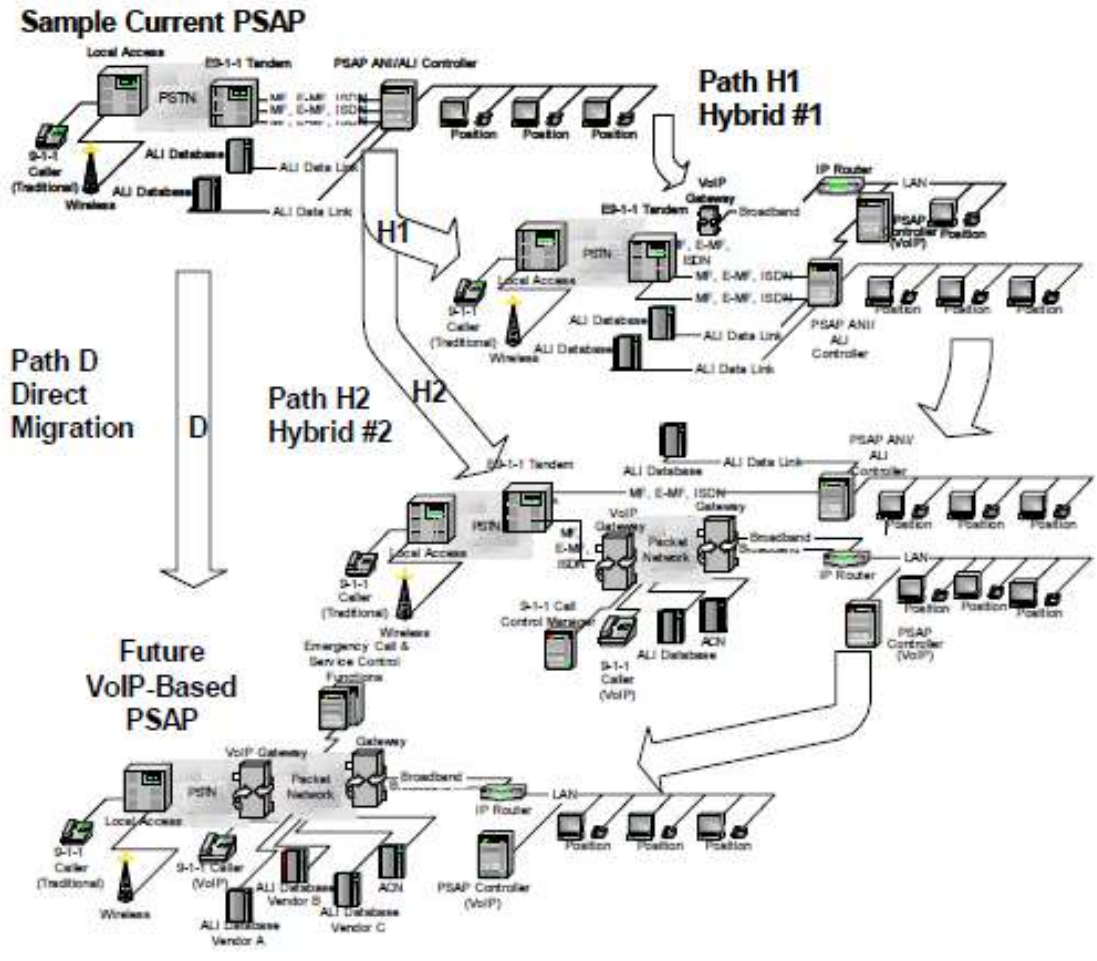


Figure 1-1 VoIP Migration Strategies

The following paragraphs describe the steps in the various migration paths.

Hybrid 1: Before IP service is available, one or more MF trunks (especially new trunks) or ISDN lines can be converted to broadband access with VoIP Gateways (Gwy). The PSAP can retain existing interfaces during a transition period. The advantage of this step is to provide additional capacity without additional MF trunks or ISDN lines at the PSAP.

Hybrid 2: After IP packet based access is available, one or more MF trunks (especially new trunks) or ISDN lines can be converted to broadband access. This step requires VoIP capable CPE. The advantages of this step are to provide a more robust, diverse access to the PSAP, and to reduce the number of different trunk/line groups that need to be supported between the PSTN and the PSAP. The PSAP can leverage VoIP capabilities, while keeping legacy trunks during transition, or to support non-VoIP service providers. This may be a final configuration for many PSAPs.

Direct: After VoIP service is available; this is the most direct path to a VoIP-based PSAP. This is most appropriate for new PSAPs that have IP packet-based access available. MF trunks or ISDN lines have either all been replaced or were never used.

2 Technical Description

This document, Network to IP PSAP Interface, will be one document in a set that will describe migration of emergency calling to use Voice over Internet Protocol (VoIP) on a variety of different access data transports from the PSTN. Emergency call information associated with the caller will also be transmitted sharing the same IP network resources. The Internet Protocol (IP) forms the common protocol foundation of the (public) Internet as well as many private data networks. IP is a connectionless protocol where each IP packet is self-contained; setting up a "circuit" or "call" or "session" is not required to establish and maintain communications.

For voice calls originated in the PSTN, (IP telephony) gateways translate the caller's voice into IP packets and then send them towards their destination IP address. Once the packets reach their intended destination, they may be rendered into audio by IP-capable end systems or translated back, by another gateway, into a circuit-switched bit stream or analog voice circuit.

In E9-1-1 VoIP Networks, functions formerly provided by E9-1-1 Tandems in the PSTN will be provided by a collection of **Emergency Call and Service Control** functions implemented in the VoIP network.

Emergency call data and emergency calls can be delivered together, without the delays that may be engendered by waiting for PSAP data queries after calls are delivered to the PSAP. Data associated with the call will also be transmitted using the Internet Protocol (IP). Generally speaking, the IP access bandwidth will be larger than today's ALI access, thus speeding up ALI data delivery. Data sources will either be co-located with Emergency Call and Service Control functions in the VoIP network or, remotely located and interconnected via IP capable links.

When PSAPs are interconnected using VoIP networks, voice calls and data sessions will be established virtually simultaneously, and PSAP agents will be enabled to exchange call related information more easily.

Any new packet-based system for 9-1-1 must have equivalent functionality and reliability as today's circuit-switched technology. Most of the call features today are provided by signaling protocols supported between an E9-1-1 tandem in the PSTN and the PSAP. The PSTN to PSAP interface is significantly affected by this transition and has been chosen as the place to start defining the required functionality.

2.1 Network to PSAP Interface Overview

2.1.1 Architecture

Currently, multiple trunk groups and protocols are required between the E9-1-1 Service Provider and the PSAP to provide the necessary voice and data services. Separate trunk groups/interfaces may be needed to terminate emergency calls from different E9-1-1 control offices, for administrative calling via the local serving office, and for data connectivity.

This document proposes to support all voice and data services, with a common IP-based interface to the PSAP, using VoIP signaling to support voice calls. The network infrastructure needs to be a MANAGED IP NETWORK to provide appropriate security and quality of service.

The first two architecture diagrams illustrate packet-based access to a legacy E9-1-1 tandem from both a legacy PSAP and a VoIP capable PSAP. The E9-1-1 tandem may be connected, via a gateway, to a PSAP via a point-to-point high-speed dedicated data link or packet-based access. The E9-1-1 tandem is likely to have a MF (CAMA-like), Enhanced MF or ISDN circuit-switched interface. The VoIP gateway connects

to this interface and converts circuit-switched voice and signaling into their packet equivalents. (Note that the E9-1-1 tandem may also integrate the VoIP gateway function, removing altogether the delays due to MF signaling.) Legacy PSAP's that do not support IP on their CPE may employ another gateway that reverses the translation, turning packet-based protocols and data into suitable circuit-switched ones.

Both the VoIP PSAP and the E9-1-1 tandem may be connected to the same packet network operated by a service provider (refer to Figure 2-1). This diagram also includes depiction of a legacy PSAP served directly by the E9-1-1 tandem using conventional signaling (e.g., MF (CAMA-like), Enhanced MF). Some E9-1-1 related call control and service functions may continue to be provided by the E9-1-1 tandem in the PSTN; some of these functions may migrate to elements on the IP packet-based network. These functions are represented in the diagram as "9-1-1 Call and Service Control functions." Examples of these Emergency Call and Service Control functions include selective routing, call redirection, call distribution, and conferencing functions. Depending on the VoIP protocol(s) implemented in the IP packet network, these functions may be provided by different types of elements.

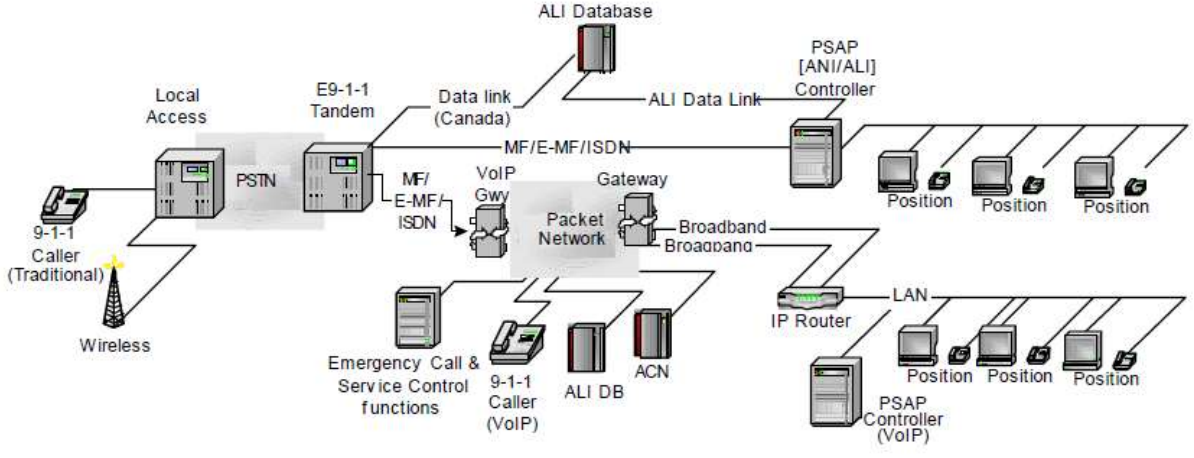


Figure 2-1 Legacy E9-1-1 Tandem Conventional and VoIP Packet-Baseed Access to PSAPs

The next architecture diagram illustrates packet-based access between an IP-based network and both a legacy PSAP and VoIP capable PSAP (refer to Figure 2-2). In this architecture, a VoIP gateway is shown (integrated with the PSAP Controller function in this example) at the PSAP to provide protocol interworking between the VoIP and media protocols supported by the packet-based access network and the conventional voice signaling at the legacy PSAP. If the VoIP protocols supported by the packet-based access network and the VoIP PSAP were different, a VoIP gateway would also be needed in this case to provide the inter-working between VoIP protocols for the VoIP PSAP. In both cases, IP-based signaling over the common broadband access is assumed for data exchanges, e.g., ALI queries/responses. In this example, 9-1-1 Call and Service Control functions have migrated to the VoIP network.

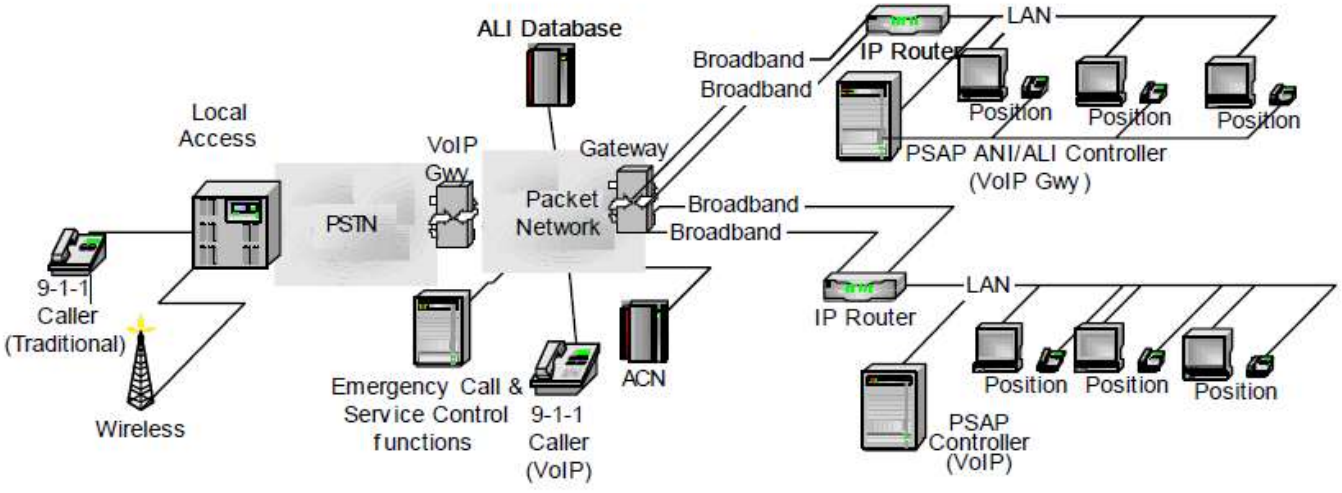


Figure 2-2 VoIP Network Support for Both Legacy and VoIP PSAPs

In this TID, some features and capabilities are described as "network" features. These may be capabilities supported in the E9-1-1 Tandem, or supported by new E9-1-1 Call and Service Control elements in the IP packet-based network. This TID identifies the signaling functions that would need to be supported by the VoIP protocols for the PSAP to be able to receive, control, invoke, cancel, and modify these network-based features.

Some of these network features may alternatively be provided by functions internal to the PSAP Customer Premises Equipment (CPE). The VoIP signaling capabilities required to support such features within the PSAP CPE architecture are outside the scope of this TID (although they might be analogous to VoIP signaling capabilities described for access to similar features provided by the network-based versions).

The VoIP signaling capabilities described here shall include at a minimum the functions necessary to support PSAP interactions with the E9-1-1 Tandem (via VoIP gateways). Additional functionality may also be included that can be supported by VoIP signaling interactions between the VoIP PSAP and the VoIP E9-1-1 Call and Service Control network elements in the packet-based access network. These will be identified as additional desirable functionality.

Centralized vs. Distributed Architectures

In PSAPs today, typically the voice telephony services are provided using a centralized architecture, where dumb endpoints (telephones) are served by a switch, whether using E9-1-1 Tandem/Centrex functionality or using an on-premise PBX. IP data network architectures, on the other hand, tend to be more distributed, with functionality and control distributed among peers. Depending on the choice of VoIP protocols, VoIP technology allows more choices about the centralization/distribution of functionality and the balance of simplified management versus endpoint innovation. (Refer to Section 2.1.4 for more background on these protocols: Media Gateway Control Protocol [MGCP] and H.248 (Megaco), H.323, and Session Initiation Protocol [SIP].)

In general, MGCP and H.248/Megaco protocols are associated with centralized architectures, with a centralized media gateway controller or call connection agent—that handles switching logic and call control.

The media gateway controller communicates with media gateways, providing instructions for the media gateway to route and transmit the audio/media portion of a call. Endpoints (gateways/telephones) are relatively dumb, with limited functionality. It is also possible to build centralized networks with SIP or H.323 protocols.

The advantages of a centralized VoIP architecture for a service provider are centralized (simplified) management, provisioning, and call control, and simplified support of legacy voice features. Disadvantages include reduced flexibility for innovation by intelligent endpoints.

Distributed architectures are generally associated with H.323 and SIP protocols. These protocols allow network intelligence to be distributed between endpoints and call management devices. Examples of network intelligence include awareness of call state, feature operation, call routing, provisioning, measurements for performance, or any other aspect of call handling. Endpoints can be VoIP gateways, IP phones, media servers, or any device that can initiate and terminate a VoIP call. In an H.323 network, the call management devices are called gatekeepers, and proxy or redirect servers in a SIP network.

One advantage of distributed architecture is flexibility. VoIP applications can be treated like any other distributed IP application, and the intelligence for new capabilities can be added to either endpoints or call-control devices, depending on business and technology needs. Disadvantages are that distributed networks tend to be more complex.

VoIP protocols can also be used in combination, for example, with H.248 (Megaco) being used to control media access gateways and provide some functionality, and SIP used between endpoints to provide additional functionality.

2.1.2 Internet Protocol Stack

In order to understand how VoIP works, it is necessary to understand the model on which all IP reliant applications are designed upon or molded around. The Internet Protocol Stack is a multi-layered model in which each layer is dependent on its neighboring layers for consistent handoffs of information, because of this; a great deal of flexibility can be exerted within the layer itself. The Internet protocol stack is customarily divided into the physical, data link, network, transport and application layers, briefly described below.

2.1.2.1 Physical Layer – Layer 1

The physical layer encompasses the electrical or optical transmission mechanisms used to communicate bits between two or more points. This layer includes the modulation schemes needed to convey data across fiber optic links, coaxial cable, twisted pairs, radio spectrum or other transmission media. The Internet architecture is designed to shield upper layers from changes in the physical layer. Routers process packets at layers 1 through 3, while end systems (“hosts”) process all layers.

2.1.2.2 Data Link Layer – Layer 2

The data link or media access control layer (MAC) is responsible for converting bit streams provided by the physical layer into packets, discovering transmission bit errors and, where applicable, establishing and terminating logical links. Ethernet, frame relay and ATM are examples of common data link layers. At this layer, hosts are typically identified by a MAC address (colloquially known as “Ethernet address”).

2.1.2.3 Network Layer – Layer 3

The network layer provides a method of transmitting packets provided by higher layers over the network to a specified destination. In the Internet architecture, the Internet Protocol (IP) provides this service. The Internet network layer delivers packets on a "best-effort" basis, i.e., there is no guarantee when and if a packet might reach its destination. Packets may arrive out of order. The Internet Protocol architecture currently supports two versions of IP, namely IPv4 and IPv6, with the latter meant to replace the former. End points and routers are identified at the network layer by IP addresses, bit strings that are globally unique within a network.

2.1.2.4 Transport Layer – Layer 4

The transport layer is primarily responsible for flow control of data between communicating end points. The data must not only be delivered error-free but also properly sequenced. The transport layer also sizes the packets so they are in a size required by the lower layer of the protocol stack. Proper packet sizing is dictated by the network architecture.

2.1.2.5 Application Layers

Application-layer protocols provide services specific to one type of application. The most relevant protocols for this document are HTTP (for web services), SMTP (for email delivery), RTP (for packet audio and video), SIP, H.248 and H.323 (for VoIP signaling). There are numerous other application-layer protocols, both proprietary and standardized.

2.1.3 Video Media Protocols

Audio (and video) packets used for VoIP are transported using Real-time Transport Protocol (RTP) packets. RTP is described in IETF RFC[2] 1889 and 1890, while a large number of other RFC's describe how audio and video data for specific codec's is encapsulated for transmission.

2.1.4 VoIP Signaling Protocols

VoIP signaling protocols establish, modify and terminate multimedia sessions. The most common ones, H.323, SIP and H.248, are described below.

2.1.4.1 H.323 Protocol Overview

H.323 is a standard developed by the ITU-T to define the operation of multimedia systems over packet-switched networks. Originally developed as a network architecture and protocol applicable to Local Area Networks (LANs), this standard has developed into a protocol suitable for many environments, including VoIP.

H.323 is an umbrella standard for a family of related and interdependent standards that define the multimedia system: H.323 defines the overall architecture, H.225 defines protocols for registration, admission and status (RAS) and call setup, and H.245 defines protocols for media or bearer capabilities

[2] The Requests for Comments (RFC) document series is a set of technical and organizational notes. Memos in the RFC series discuss many aspects of computer networking. RFCs can be found at http://www.rfc-editor.org and the mirror sites listed on that web site.

exchange. The call setup protocol in H.225.0 is very similar to Q.931 signaling used in ISDN and somewhat similar to the ISDN User Part (ISUP) in SS7.

In general, a multimedia system can consist of terminals, gateways, multipoint control units, and gatekeepers. A particular network may have some or all of these elements depending on the application being addressed. H.323 can support distributed architectures that allow the intelligence for call handling and feature processing to be distributed among call management and feature servers and end user devices.

2.1.4.2 H.248 (MEGACO) Protocol Overview

ITU H.248, also known as Megaco (Media Gateway Control Protocol) in the IETF, is a standard protocol for handling the signaling and session management during a VoIP call. It defines a means of communications between a media gateway (slave), which converts data from a circuit switched network to a packet switched format and the media gateway controller (master). H.248 is an enhanced version of the earlier Media Gateway Control Protocol (MGCP).

2.1.4.3 Session Initiation Protocol (SIP) Overview

The Session Initiation Protocol (SIP) is a signaling protocol standardized by the Internet Engineering Task Force (IETF), the standardization body for Internet protocols. SIP is specified in RFC 3261 and related documents. SIP allows user agents to set up, modify and tear down sessions. The sessions themselves are described using the Session Description Protocol (SDP) (RFC 2327). A VoIP call and a multimedia conference are examples of sessions.

SIP systems are primarily composed of user agents and proxies. SIP end systems are called user agents. They periodically register their current network location, described by their IP address, with registrars. Proxy servers use the information in registrars to route messages to end systems. Typically, each domain has its own proxy server or set of redundant proxy servers. Proxy servers perform call routing functions, but do not process any voice or other media streams. Proxies do not modify request bodies and do not originate new requests (calls). Proxies can, but do not have to, keep track of call state. Often, they only remember the current pending transaction, i.e., a single request and its responses. Proxies are often only needed for the initial call setup messages, but may request to be in the path of all session signaling messages. An end system receiving a request can inspect the request to discover the identity of all proxy servers. Proxies implement services such as conditional and unconditional call forwarding, call filtering and “find me” services.

User agents can perform all of the functions that a proxy is not allowed to do, such as originating requests or inspecting message bodies; they are generally origination or termination points. In other words, the caller cannot “see” what is behind the user agent. IP telephones are examples of user agents, but a “bridge” (conference server) also acts as a SIP user agent.

SIP systems are identified by SIP Uniform Resource Indicators (URI), such as sip:alice@example.com, or telephone URIs, such as tel:+1-212-555-1234. A single SIP or telephone URI can refer to any number of end systems, which can be located anywhere in the network. In order to reach a particular SIP URI, only a Domain Name System (DNS) entry for the domain is needed. In other words, the origin and destination of a call do not need to make prior arrangements to exchange messages.

2.2 Call capacity management – Bandwidth management

When conventional trunks are used to provide the network to PSAP access, the access capacity for different types of calls (e.g., terminating 9-1-1 calls, other emergency call terminations, call originations, and administrative line calling) is managed by the number of trunks/lines engineered for each type of call. If VoIP network to PSAP access is provided with a common broadband access interface used to support all call types, a mechanism needs to be provided to control the amount of bandwidth that can be used for each type of service. This will prevent all available capacity from being allocated to any one particular service. For VoIP calls this might be implemented as min/max restrictions on the number of simultaneous calls, for some service types (similar to the concept of Simulated Facility Groups used to control the number of trunks in a trunk group that are allocated to a particular service.) or by min/max restrictions on the bandwidth for other service types. It is desirable for such min/max restrictions to be managed by day or time of day, and to be configurable in real time by an authorized agent of the PSAP to allow for special circumstances (e.g., the temporary need to allocate administrative capacity in favor of accepting more than the usual number of emergency calls).When a common broadband access from the VoIP network to the PSAP is used to support multiple services, the bandwidth capacity should be engineered following guidelines recommended by NENA in the appropriate documents. This bandwidth engineering should also reflect any additional requirements imposed by specification of the minimum number of simultaneous calls that must be able to be supported for particular service type(s). It may be desirable for the VoIP network to PSAP interface to support automatically invoked dynamic adjustment of bandwidth. This would allow for the bandwidth allocated to existing calls to be adjusted so that additional calls can be supported on the interface. However, if such dynamic bandwidth adjustment capabilities are supported, the governing policies should not permit automatic bandwidth reduction for emergency calls.

2.3 Voice Call Functionality

2.3.1 Terminating Emergency Calls

2.3.1.1 Network Call Distribution Functions (optional)

The interface between the PSTN and the PSAP must support the capability to

- Simultaneously alert a given set of call takers of the incoming call;
- Award the call to the first call taker to answer;
- Allow other call takers to join the call, bridging (conferencing) all participants and also allow call takers to drop off the call.

This interface may support additional capabilities traditionally provided by automatic call distribution[3] systems (ACDs), such as the following:

- Calls may be routed to call agents based on policies and different distribution algorithms (e.g., least busy).
- Agents must be able to be assembled into multiple groups according to policies specified by PSAP

[3] Refer to NENA Recommended Generic Standards for E9-1-1 PSAP Equipment (04-001) section 3.15 for a further description of ACD functionality.

authorities. These groupings must be changeable by the PSAP authority.

- Callers may receive automated announcements or other indications of call status.
- Protocol support for agent logon/logoff functions is required and workstation status conditions should include at least "ready", "not ready", and "busy" at a minimum. The Emergency Call and Service Control functions must monitor the state of PSAP ACD workstations and be able to address the individual workstations, e.g., with individual unique IP addresses.
- Supervisors can manage call queues.
- Supervisors and/or agents can measure call delays and other performance metrics. (This may require additional capabilities in Emergency Call and Service Control functions and the exchange of data between these functions and the PSAP, but it does not affect VoIP signaling or processes.)
- Agents must be able to indicate their availability. Calls must be routed only to agents that are available and not busy with other calls.
- It must be possible to queue calls, either in answered or unanswered state. Queued calls must be able to receive recorded announcements. PSAP personnel, as directed by policy, should be able to modify the announcements.
- Systems should provide a display to individual agents as well as to common areas, e.g., via a "reader board". Information typically includes the number of calls in queue, the length of time the longest call has been in queue, and the number of agents available. Such information may be made available in areas such as break rooms and cafeterias so that call takers can be alerted to return to duty. This information should also be recorded for resource management purposes. The VoIP network to PSAP interface needs to support signaling of the required information. PSAP displays are beyond the scope of this document.
- Audio logging systems must be able to record calls while the calls are in queue and while they are being answered. The logging system must record information about the call taker identity or position.
- Supervisors must be able to monitor/bridge onto the audio stream of on-going calls for training and quality management.
- Call takers must be able to add supervisors to an existing call to help with difficult calls.
- PSAPs need to be notified of abandoned calls, i.e., 9-1-1 calls that are dropped by the caller before being answered by a call taker.
- The same group of call takers should be able to handle both 9-1-1 and 10-digit emergency calls.
- The call queue should allow automatic or manual transfer to another location of calls that exceed a particular expected waiting time.

2.3.1.2 Type of Call

To differentiate services, the interface must provide a way to distinguish the following call types. The call type information should be derivable from information carried in the VoIP signaling delivered to the PSAP with the emergency call. Call types include:

- Emergency 9-1-1 calls
- Non-selective routed emergency calls (e.g., direct 7-digit or 10-digit emergency calls)
- Transfers from other PSAPs
- Anonymous calls
- Administrative calls

2.3.1.3 Delivery of Emergency Call Related Information

Each call setup request must deliver the following essential (tier 1 - refer to section 2.5.1) data, either embedded in the call-signaling message or by a separate mechanism that unambiguously associates this data with the call.

- Called Party Number (to identify PSAP and or type of call)
- Calling Party Number, including any numbering plan digits (the "I" digit for MF (CAMA-like trunks)
- Delivery of Indication of Caller ID Blocking for non-9-1-1 calls
- Location information or lookup keys
- Delivery of ANI on abandoned calls
- Ability to deliver an indication that a terminating emergency call has been alternate routed from another PSAP[4]. Delivery of this indication could be arranged in one of [at least] two ways:
    - It could be delivered along with ANI to the PSAP.
    - Alternatively, this information could be provided to an E9-1-1 Server function in the network which could prepare and include this information along with information retrieved from the ALI database for download to the PSAP.
- Provide a general use legacy "flash" indication

Additionally, the following items should be included with delivery of Emergency Call Related Information outside of the parameters established for tier 1 information in the future path plan:

- Call origination information: wireline, wireless, TDD/TTY, other…
- Default routed calls (These are calls for which selective routing information was unavailable, resulting in the call being routed to a "default" PSAP based on other criteria.)

[4] When interworking with CAMA/Enhanced MF trunks from an E9-1-1 Tandem/Control Office, this indication is provided in the first "I" or "II" digits out-pulsed after the MF ST (Start) pulse. Traditionally, this indication has been used to indicate whether the accompanying ANI information is to be presented as a "flashing ANI" display (as opposed to "steady on"), and the meaning of the "flashing ANI" has varied from PSAP to PSAP. Increasingly, the other meanings of "flashing ANI" can be supported by other data that resides at the PSAP CPE (e.g., identification of special sites, like power plants). However, whether a call has been alternate routed may only be known by elements in the network. Therefore, it is useful to support signaling of this information on the network to PSAP interface.

2.3.1.4 Alerting

The VoIP interface shall provide signaling to support an indication that a call is being offered at the PSAP.

2.3.1.5 Answer

The VoIP interface shall provide signaling to support an indication that a call has been answered at the PSAP.

2.3.2 Alternate Routing Control and Notification

Alternate Routing is the capability for the network to temporarily re-route calls to a different PSAP because the selected PSAP is not available to take calls, or if connectivity to the selected PSAP is not available in a network failure scenario. This capability is invoked/cancelled by the PSAP that receives the alternate routed calls. Notification that Alternate Routing has been invoked/cancelled is provided to the PSAP from which calls have been redirected. Alternate Routing can only be invoked for a particular PSAP by a PSAP that is authorized by previous policy agreements to receive calls for that PSAP. Alternate Routing can only be cancelled by the PSAP that has previously invoked it.

PSTN to PSAP signaling capabilities that shall be supported include:

- Alternate Routing Control and Notification
- Activation/Deactivation of Alternate Routing
- Acknowledgment of Permission for Activation of Alternate Routing
- Notification of Alternate Routing Activation

It is desirable to have these capabilities in a VoIP network implementation also. An authenticated party should be provided the ability to invoke or cancel alternate routing for a particular PSAP. It should be possible to specify the alternate routing destination and time constraints when re-routing should occur. A rerouting indication at the PSAP should occur as soon as alternate routing is invoked. This can be controlled through the use of predetermined policies that can be changed as the situations creating the alternate routing scenario dictate.

2.3.3 Network Call Forwarding Features

There are circumstances under which a PSAP may wish to have calls rerouted to another PSAP through the use of policy agreements, e.g. for handling overflow when all call-takers are busy. Call forwarding can occur either by requesting that the PSTN perform this function or calls can be redirected directly by the PSAP to other IP-enabled PSAP's via VoIP signaling protocols. PSTN network to PSAP signaling should support invocation and cancellation of call redirection by request, on busy, don't answer after a configured delay, time-of-day, equipment or connectivity failure at PSAP. The PSAP should be able to specify the destination(s) to which calls should be redirected. The receiving and redirecting PSAP should be notified that calls are being redirected. This signaling may also be used to invoke redirection capabilities supported by Emergency Call and Service Control functions in the VoIP network, if applicable.

2.3.4 Network Call Transfer

PSAP's shall be able to transfer emergency calls to other PSAPs. The transferring PSAP should have control over when to disconnect (remain connected to the call until they disconnect).

The E9-1-1 tandem-to-PSAP signaling shall be able to support:

- Procedures for invocation of Network Call Transfer
- Choice of Caller ID to be provided with transferred call: PSAP ID or Emergency caller ID
- Inclusion of original emergency caller information (refer to Section 2.5.1).
- The transferring PSAP should be able to initiate an associated data session to provide information already collected by the transferring PSAP agent including ALI information (refer to Section 2.5.4, Transfer of Emergency Call Related Information with Voice Call Transfer).

The Network Call Transfer capabilities should include:

- Ability to provide emergency caller ID on transferred call
- Inclusion of an indication of an emergency call with the transferred call
- Selective routing of transferred call based on original caller location information
- Transfer to announcements.

VoIP signaling to support transfer of a call from one PSAP to another destination should also be supported by Emergency Call and Service Control functions in the VoIP Network.

2.3.5 Network Call Conferencing

There are circumstances in which a PSAP may wish to have additional parties participate in an emergency call, e.g., other PSAPs, language translation services, special purpose emergency response centers (e.g., poison control), etc. Conferencing can be provided as an IP service or by the PSTN. To support this, the PSTN to PSAP signaling should be able to support:

- Ability to conference at least six or more parties
- Add/drop control of the primary (controlling) PSAP (to add/drop other parties)
- Transfer of Control of Conference to another party
- Automatic conference of caller on multi-way connections

2.3.6 Other PSAP Call Control Features

Other Network features that should be supported by signaling capabilities on the Network to PSAP interface include:

- Hold
    - Hold - This is the ability for the PSAP call taker to be able to place a call in a status that allows him/her to handle other calls without disconnecting from the caller. A visual/audible

notification should be available for the call taker to alert them that a call is on hold. The call should continue to be recorded and an optional voice message should be made available for the caller so they are aware of the status of their call.

- Consultation hold – This places the caller in a hold status automatically (as described above) during the transfer of a call. Using this method, the call taker is able to consult with the transfer destination before connecting the parties together. Like hold, the call should continue to be recorded and an optional voice message should be made available for the caller so they are aware of the status of their call.

- Forced Disconnect (of the caller)

  This will allow the PSAP call taker to disconnect a call when the call is in an off hook status at the calling party's end. This eliminates the possibility that 9-1-1 resources are needlessly tied up by 9-1-1 calls made and then left off hook.

- Called Party Hold

  This feature allows a call taker to continue to stay connected to the calling party even if the calling party attempts to place their phone in an on-hook status.

- Caller Ring Back

  This will allow the call taker to be able to ring a phone back even if the destination phone is in an off-hook status.

- Automatic Bridging

  This allows for a call to be automatically connected to two separate answering points when alerting. When one called party picks up the alerting stops but the other automatically bridged party still has the option of picking up and participating on the call.

2.3.7 Network Control Features

The control features include:

- Alternate Routing Control

  This is the control capability required by the "Alternate Routing Control and Notification" section (2.3.2). This requires the ability to define alternate routing based on all circuits busy to a PSAP and "time of day" or "night service" routing.

- Call Forward Control

  This requires the ability of the PSAP to set the forwarded number(s) and turn forwarding on or off manually or for preset times.

- Bandwidth Control

  VoIP bandwidth can support a number of calls depending on the Quality of Service (QoS) and Service Level Agreement (SLA) requirements. The PSAP will require the ability to set the number of calls to be carried by the available bandwidth.

  The ability to separate bandwidths for various call types will be required to prevent one call type from swamping the PSAP to detriment of other call types. These call types are;

- 911 (separate wireline and wireless bandwidth)
- Administration calls
- ACN

- QoS and SLA Control

  The PSAP will require the ability to measure the QoS of calls (refer to section 2.7) to ensure that the SLA is being met. Some of these measurements would be, delay, packet loss and jitter. Where possible, degradation of voice quality should not be introduced by the PSAP or 9-1-1 networks voice CODEC scheme.

2.3.8 Administrative Call Handling

An administrative call is any call that has not been dialed as 9-1-1 or not otherwise presented as a 9-1-1 call to the call taker. These calls are handled by an ACD function that supports different call queues with precedence given to 9-1-1 calls.

2.4 Text-based Emergency Contacts

The VoIP Network to PSAP interface shall support methods for text-based contacts to support the needs of text-based users, including Telecommunications Devices for the Deaf/Teletype (TDD/TTY) and their successors. Other text-based means include wireless short message service (SMS), email, and instant messaging.

The reliability of information exchange using TDD/TTY equipment can be negatively impacted by the transmission and audio encoding techniques used on a VoIP system. Use of an appropriate signaling protocol and the G.711 type codec should yield acceptable performance with existing equipment. However, there is some debate among industry members as to the maximum total character error rate (TCER) allowable. The VoIP TTY (VTTY) Forum of the Alliance for Telecommunications Industry Solutions (ATIS) is currently addressing how to determine this specification limit. The target for resolution is mid-year, 2003.

Instant messaging from cell phones, alphanumeric pagers, PDA's and PC's has been growing in popularity. A native IP infrastructure provides a more seamless integration for applications associated with these devices.

Any text based emergency contact device should be implemented through the use of 9-1-1 as a destination address; e.g. SOS devices in SIP environments.

Other groups within NENA are developing TID's (i.e. Data Only Technology Working Group) to address the specifics of these types of devices.

2.5 Emergency Call Related Data Functionality

2.5.1 Emergency Call Related Data

The NENA Future Path Plan describes three types of information related to an emergency call that are either delivered with the emergency call or that can be made available to the PSAP either through a query/response method initiated by the PSAP or as initiated by the network or a third-party. These sets of

data include essential data, supportive data and supplemental data. An example of essential data would be the callers ANI and few crucial data items from the callers ALI. An example of supporting data would be an ALI record. (Refer to "Future E9-1-1 and Emergency Telecommunications Evolution – NENA's Technical Path Plan Concept for the New 9-1-1" located at www.nena.com.

2.5.1.1 Enhanced Data (Tier 1)

Voice and Essential Data should be provided on a single primary path. On the VoIP interface, essential data is provided as part of the VoIP signaling required to establish the call, or in a related data session.

This should include Essential Data that supports call delivery and adequate response capability if all other sources of information fail. (For each type of Essential Data, "alternate" information may be provided in the event that the Essential Data is not available) These might include:

Essential-Description	**Example**	**Alternate Information – Description**	**Example**
Callback Information on how to re-contact the caller.	NPA-NXX-YYYY Sip:alice@anywhere.net	Default information – Used to identify the origin of the call.	NPA-911-ESCO
Fixed Caller location MSAG/GIS-validated address information	Doe, John 123 Main St Anywhere, VT	Caller Location Key / ID – Used to obtain the location information from a known source (i.e. call back number).	NPA-NXX-YYYY
Non-fixed Caller Location	Wireless Caller X: 43.66297 Y: -73.32248	Caller Location Key / ID – Used to obtain the location information from a known source.	444-555-1010
Call routing code ESRK or ESRD – used for routing the call through the network	802-511-1234	N/A	N/A
Origination code Represents where the call comes from (e.g., cell site or cell sector) more discrete than the trunk group – may also be used to potentially control congestion dynamically that is not network based.	444-555-1010	N/A	N/A
DB routing access code Code indicating where to retrieve the data.	784569	Type of call	Default: ALI DB

Information necessary for trouble shooting (analogous to current information, plus additions based on new technology; i.e., ESCO, new origination code, CoID, error codes) should be available in the PSTN so that the PSAP can retrieve it in the event of failures and/or call delivery problems. The PSTN to PSAP interface should support a method for query/response to retrieve this information.

2.5.1.2 Supportive Data (Tier 2)

Supportive Data is analogous to ALI data. It may be delivered with a call or requested by the PSAP during an on-going call. An example is a detailed street address or geodetic location information.

ALI data exchange formats and protocols are described in NENA Technical Reference 02-010. The VoIP interface has to support the ability for the PSAP to query a separate entity for supportive data based on essential information delivered to the PSAP.

2.5.1.3 Supplemental Data (Tier 3)

Supplemental Data is data that can assist the emergency responder(s) in preparing to respond to the emergency. It may include for example:

- Medical records
- Motor vehicle records
- Vehicle collision information
    - Video information
    - Occupant information.
    - Delta-V Information

The VoIP interface has to support the ability for the PSAP to query a separate entity based on essential information delivered to the PSAP.

2.5.2 Automatic Delivery of Emergency Call Related Data

The PSTN-to-PSAP interface should support delivery of Essential Data to the PSAP with the Emergency Call. When Essential Data cannot be provided, “alternate” information should be included to allow default action/processing by the PSAP (as described in section 2.5.1.1).

It is desirable that the interface should support automatic delivery of Supportive Data to a PSAP, initiated by a network element or third-party user agent, e.g., an Emergency Service Database. The Network to PSAP interface should support a method for this data session to be associated with a previously terminated voice call.

It is desirable that the Network should support automatic delivery of Supplemental Data to a PSAP, initiated by a network element or third-party user agent, e.g., an Automatic Collision Notification (telematics) service provider or Medical Call Center. The Network to PSAP interface should support a method for this data session to be associated with a previously terminated voice call.

2.5.3 Retrieval of Emergency Call Related Data

The Network to PSAP interface should provide a method to retrieve Supportive Data from Emergency Services Databases (e.g., ALI) based on “retrieval key” information provided in the Essential Data.

The Network to PSAP interface should support a method to retrieve Supplemental Data from Third Party Service Providers, based on "retrieval key" information available in the Essential and/or Supportive Data.

These methods should include the capabilities to support:

- Queries
- Responses
- Error Recovery
- Requests for Location Updates

Essential Data should be available during the duration of the call with a key for retrieval of Supportive Data. Supportive Data should provide a key for long-term retrieval of Supplemental Data.

2.5.4 Transfer of Emergency Call Related Information with Voice Call Transfer

The PSAP should be able to establish a data session to another PSAP, and be able to associate this data session with a voice call transferred to that PSAP.

2.6 Remote Log-In

Some PSAP solutions support a remote Log-In capability for their call takers. This capability allows a call taker to access a PSAP using a remote workstation, typically through a broadband connection. This would allow a remote call taker to be treated as if they were physically at the PSAP location. The call taker can, in this situation be assigned calls by the PSAPs ACD or KTS functionality. All the capabilities needed such as CAD, logging recorder, etc. are accessible to the remote call taker. This capability could be used in cases where the PSAP has to be evacuated but the equipment at the PSAP can still function at the PSAP.

When this capability is used for work force augmentation and handling overflow then, the remote workstation must have the full functionality of the workstations at the PSAP. However when used for disaster recovery applications, a lesser degree of feature functionality may be used at the workstation as determined by local requirements.

Figure 2-3 depicts a next generation PSAP solution that employs the use of remote call takers.

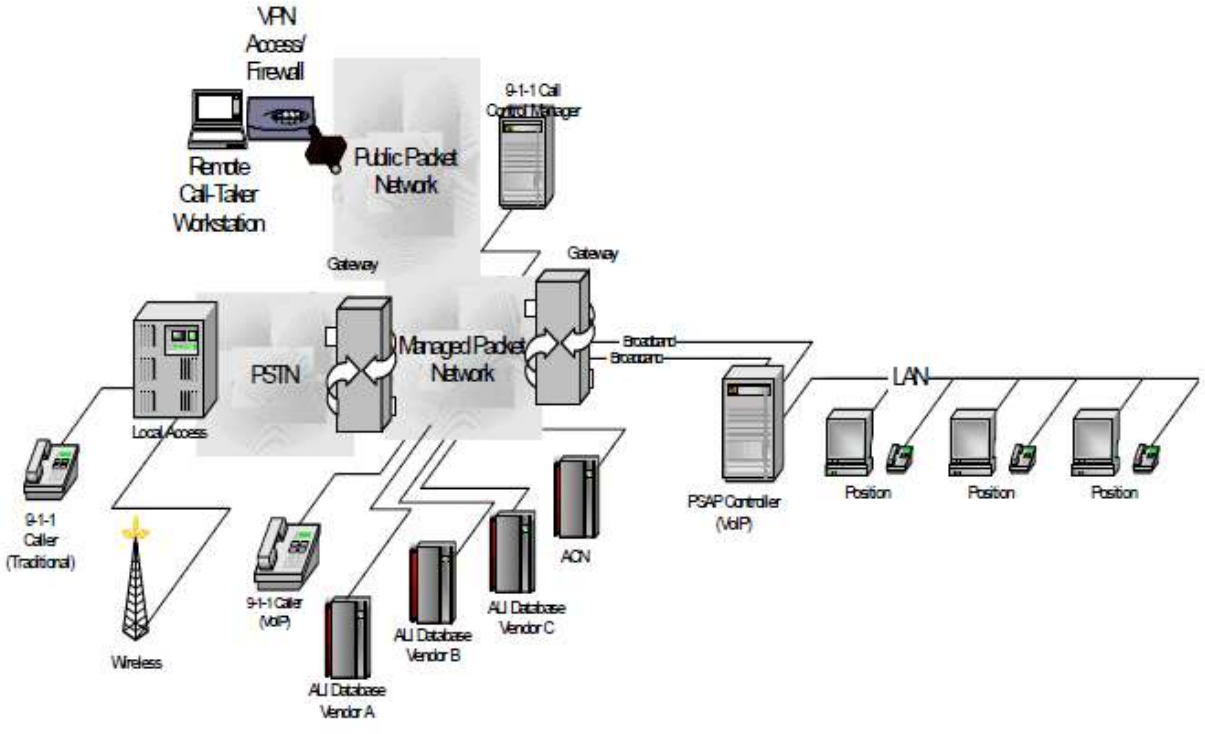


Figure 2-3 PSAP Solution with Remote Call Taker

2.7 Performance

2.7.1 Quality of Service (QoS)

The packet-based access network shall be managed to provide a QoS for Voice Calls that can be measured to be equivalent to carrier-grade circuit-switched calling. The 9-1-1 facilities should not degrade the audio quality of the call through the use of compression. Voice compression should not be used for emergency calls on the interface that directly supports the PSAP.

The packet-based access network shall be managed to provide delay and packet loss performance equivalent to legacy based access to ALI systems for mission-critical data to support E9-1-1.

2.8 Security

At a minimum, consideration should be made in the following areas:

Channel security – every packet between two end points gets encrypted and is from a trusted source.

Application security – individual authentication for applications that ride on the upper layers occurs and this may also include encryption at the lower layers.

These should be deployed to meet the highest level of security of every application that is utilized on the system.

The packet-based access network shall be able to provide confidentiality, integrity and authentication for voice calls and data transactions to and between PSAPs and other entities that are connected to the network.

The packet-based access network shall be able to provide confidentiality, integrity and authentication for mission-critical data sessions between two PSAPs, and between PSAPs and Emergency Service database and server elements on the packet network.

Further consideration for specific security applications will be described in later iterations of this documentation series.

3 Glossary

This section defines terminology used in this document. Some terms are specific to particular signaling architecture arrangements, as noted. Subsections provide background on several signaling architecture alternatives for Voice over Packet (VoP) networks. This information is supplemental to the NENA Recommended Technical Standard 01-002, Master Glossary of 9-1-1.

Call Management Server (CMS) – An intelligent packet based device that is capable of routing calls and perhaps providing services for end users. It does not handle the bearer switching, but it does interact with the network edge devices that perform the bearer switching. An NGN Call Agent is an example of a CMS.

Gateway – A device that supports at least one of the following interworking functions:

Interworking of two networks

Interworking of two different media flows

Interworking of two different signaling flows.

An example of a gateway is a device that supports an analog line and therefore provides circuit to packet interworking for the voice call. In addition, this gateway will provide signaling interworking from the analog line to the packet network signaling. For example, an off-hook signal may be translated into an off-hook indication sent to a call agent.

VoIP Gateway – Protocol independent gateway

H.248/MGCP Access Gateway – Provides access to conventional PSTN lines and/or trunks for a packet network. Typically the Access Gateway is located within the network.

Customer Gateway – Similar to Access Gateway with two differences. A customer gateway is located on the customer's premises and it may support access to IP Phones and customer LANs.

H.248/MGCP Trunk Gateway – A Trunk Gateway typically performs media mapping from circuit based trunks to packet media flows.

H.248/MGCP Signaling Gateway – A Gateway that simply performs signaling interworking from one type of signaling to a given packet based signaling. An SS7 Signaling gateway may receive SS7 signaling and terminate the lower layer SS7 functions (e.g., MTP2) and transport the upper layer signaling to a Call Agent or other device for call processing.

H.323 Gatekeeper (GK) – An element in an H.323 network that at a minimum handles user registration and address resolution. In addition, a Gatekeeper can perform call control, signaling mediation and mapping functions, provide services, perform call admission control, and provide bandwidth modification

control.

H.323 Gateway – A Gateway in an H.323 network that interfaces to another network or that serves users with non-packet interfaces (e.g., analog lines). H.323 Gateways that interface to another network typically perform signaling interworking and media interworking.

SIP Gateway – A Gateway in a SIP network that interfaces to another network or that serves users with non-packet interfaces (e.g., analog lines). SIP Gateways that interface to another network typically perform signaling interworking and media interworking.

SIP Proxy Server – A SIP server that locates the called user and routes the session request to the called user on behalf of the calling user. A SIP proxy server may also perform signaling mediation.

SIP Redirect Server– A SIP server that performs real-time address resolution and returns a routable address for the called user to the calling user. The calling user then initiates a SIP session to the current location of the called user.

Selective Routing Function (SRF) – is a network element/function that provides routing functions to deliver emergency calls to the appropriate PSAP.

Emergency Services Server – is a network element/function that provides network assistance to support PSAP emergency call handling and features.

RTP – Real Time Transport Protocol is a protocol developed by the IETF for the transport of real-time media (i.e., data that typically has stringent requirements on the tolerability of delay and loss characteristics). Examples of real-time media include a voice call and a videoconference.

RTCP – Real Time Control Protocol is a protocol developed by the IETF for providing control and feedback information related to an associated media flow occurring via RTP.

Router, IP –

Router, Selective –

IP – Internet Protocol is a network layer protocol with its own global addressing space developed by the IETF for routing packets in a network. Most current implementations support IP version 4 while plans are being made to develop and deploy IP Version 6.

SCTP – Stream Control Transmission Protocol is a transport protocol recently developed by the IETF for carrying user data packets and provides improved and more efficient operation when compared to TCP by allowing multiple streams in a single connection and providing a mechanism to avoid/minimize head of line blocking.

SIP – Session Initiation Protocol

TCP – Transmission Control Protocol is a transport protocol developed by the IETF for carrying user data packets where reliable delivery of information is important. This widely deployed protocol provides a connection-oriented service above the IP layer.

UDP – User Datagram Protocol is a widely deployed transport protocol developed by the IETF for carrying user data packets where reliable delivery of the information is not critical. With UDP there is no acknowledgement of the delivery of the protocol, no transport layer mechanism exists for recovery of lost packets. The application layer needs to take this into account.

WAN – Wide Area Network

948 **URI** – Uniform Resource Indicator – A SIP system or resource identifier. A single SIP or telephone URI
949 can refer to any number of end systems, which can be located anywhere in the network

950 **URL** – Universal Resource Locator is a generic address that can refer to entities such as a server or host.
951 In communications, a URL is generally translated into an IP address and port number since network based
952 routing occurs on IP addresses and not URL's.

953 # 4 References

954 1. "Understanding Packet Voice Networks". The International Engineering Consortium.
955 http://www.dt.fee.unicamp.br/~motoyama/ee981/aulas/voiceOver
956
957 2. "The role of Megaco/H.248 in media gateway control: A protocol standards overview"
958 Nortel Networks, December 2000
959
960 3. "Megaco/H.248: A New Standard for Media Gateway Control"
961
962 4. "H.248 Information Site" http://www.packetizer.com/iptel/h248/

963

964

Appendix A: H.323 Protocol Considerations

H.323 is a standard developed by the ITU-T to define the operation of multimedia systems over packet based networks. Originally developed as a network architecture and protocol applicable to Local Area Networks (LANs), this standard has developed into a protocol suitable for many environments.

The term H.323 is an umbrella standard for a family of related and interdependent standards that define the multimedia system. In general, a multimedia system can consist of terminals, gateways, multipoint control units, and gatekeepers. A particular network may have some or all of these elements depending on the application being addressed. For example, to design a simple closed system, an implementation may include just terminals. This presumes that each terminal will know the transport address of all other terminals it wants to access. These terminals will not be able to call anyone outside of the system since the system is closed and has no gateways to reach the external world.

A more sophisticated network may consist of all of the elements mentioned above. In such a network, the gatekeeper will provide address resolution for its served terminals and gateways. The terminals and gateways register with the gatekeeper. In performing the registration, the terminal/gateway provides the gatekeeper with its call signaling transport address (to which call signaling should be sent when the gatekeeper sends messages to the terminal/gateway).

Three main components of signaling and system control include:

- Registration, Admission, and Signaling (RAS) Control
- Call Control
- Bearer Control

RAS is described in H.323 at a systems level and in more detail in H.225 at a protocol level. RAS supports the following major capabilities:

- Discovery of the Gatekeeper by a terminal or gateway
- Registration with the serving GK
- Admissions Request - requesting permission from the GK to make or answer a call
- Bandwidth Modification Request - Requesting more or less bandwidth for a call from the GK

H.323 also defines a zone that consists of a set of terminals and gateways that are governed by one and only one Gatekeeper. Of course, backup gatekeepers are possible, but not yet addressed.

A RAS Control mechanism is provided by H.323 for a terminal to “discover” its serving gatekeeper (GK). This mechanism is useful when the terminal does not have a priori knowledge of its GK. In this case, the terminal sends out a message asking “Who is my gatekeeper?”. This message is sent on a well-known multicast address and port number that all gatekeepers should recognize. When the appropriate gatekeeper sees this message, it responds with a confirmation message.

Once the terminal knows who its GK is, the terminal then proceeds to register with that GK. The terminal provides its alias address (an address that others would use to call it) as well as its call signaling transport address.

When making or answering a call, the terminal shall receive permission to do so from its GK. During the

registration process, the GK may provide the terminal with a blanket approval for certain type of calls so that permission does not need to be requested for each call. Once permission is granted for setting up the call, the terminal uses H.225 signaling to set up the call.

Call Control is performed using the H.225 standard that is based on ITU-T Recommendation Q.931 (the standard for ISDN signaling). The extensions are made to accommodate the fact that the underlying network is a packet-based network rather than a circuit based network.

H.323 allows terminals to use:

- Direct call setup (call setup end to end without assistance of a Gatekeeper).
- Call Setup with address resolution by the Gatekeeper followed by direct call setup procedures
- Call Setup with call signaling routed via the Gatekeeper

Bearer control is the ability to establish, maintain and release the number of virtual bearer associations for carrying media (e.g., speech) and their support characteristics (e.g., whether compression is to be used and what codec type will be used). With H.323, bearer control is performed using ITU-T Recommendation H.245. Originally, bearer control involved end to end signaling that was performed after the completion of call signaling via H.225. However, the invocation of bearer control signaling procedures after the completion of call signaling procedures introduced call setup delays. To minimize these delays, two techniques were developed:

- Fast Connect (inclusion of special parameters in H.225 signaling to perform bearer negotiation).
- Encapsulation of H.245 messages in H.225 call control signaling.

For a single call, multiple bearer associations can be established depending on the desired end to end application. For example, for a simple voice call, a single bearer association is sufficient. For a video conference call, a voice and video bearer might be necessary. In addition, to support white boarding (sharing of text/diagrams prepared in real time), a data bearer might also be necessary.

H.323 systems were initially used for wireline type applications, but have since expanded to include wireless access users and applications as well.

Appendix B: H. 248 (MEGACO) Protocol Considerations

The H.248/MEGACO protocol is the result of a cooperative effort between the ITU-T Study Group 16 and the IETF MEGACO working group. This protocol is based on a Master and Slave relationship where there is centralized intelligence in the form of Media Gateway Controllers (MGC). MGC's not only communicate between each other but also manage numerous Media Gateways using H.248/MEGACO. The Gateways interface the packet protocols to PSTN trunks, analogue or digital lines as well as video and other facilities, including IP phones. The call control communications between MGC's can be protocols such as;

- SIP-T: Encapsulating PSTN signaling protocol across IP networks
- ISUP/H.323 encapsulating ISUP in H.323 across digital networks
- ISUP over IETF SIGTAN between MGC's and SS7 signaling gateways.

An item is Network Magazine5 on 10/05/00 positions MEGACO with respect to E911.

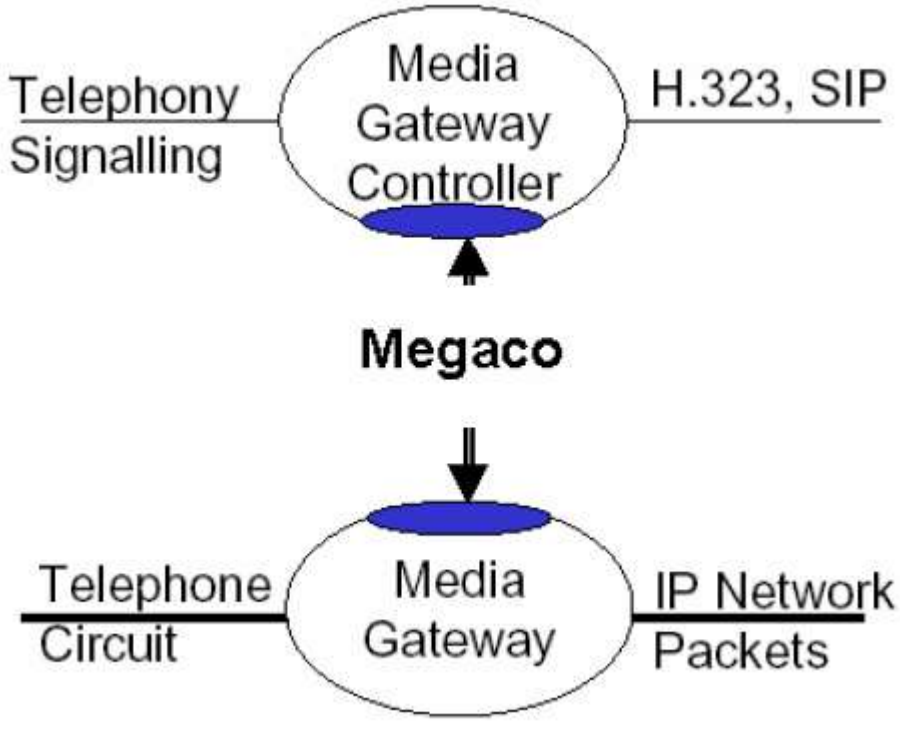
> "Right now, many vendors consider it more practical to build large gateways that separate the signaling from the media-handling because of the density of the interconnections (which may have OC-3 or even OC-12 connections). Removing the signaling to a fast server is more practical than trying to integrate it into the MG. Also, by removing the signaling from a residential gateway, network operators retain a higher degree of control, **which many believe will result in more reliable networks-vital if VoIP systems support lifeline/emergency services."**

This protocol and architecture bears a resemblance to the SS7 PSTN network where call control is separate from the call "connections" which is seen by the Internet based thought as being typically a Telco protocol.

This protocol can also be used in conjunction with SIP and/or H.323; e.g. a MGC will use H248 to control the media gateways (MG's) but communication between the gateways may occur using SIP or H.323.

The following diagram (B-1) represents the MEGACO protocol and its relationship with various PSTN and VoIP network elements.

1070



1071
1072
1073 **Diagram B-1 MEGACO's Relationship with MG's and MGC's**
1074
1075

Appendix C: Session Initiation Protocol (SIP) Considerations

C.1. Naming

SIP URIs can identify users at devices (sip:alice@128.59.16.1) and abstract users (sip:alice@psap.co.bergen.nj.us) that are not tied to any particular device.

It is recommended that each PSAP acquire a domain name, such as psap.co.bergen.nj.us and assign a common user name as the externally visible identifier, e.g., sip:emergency@psap.co.bergen.nj and sip:business@psap.co.bergen.nj. Each call taker is then assigned an identifier. Call takers can use SIP registration to associate their name (e.g., sip:mary.jones@psap.co.bergen.nj for call taker Mary Jones) with the emergency identifier. Multiple call takers can register under the same external identifier and then rely on SIP sequential or parallel searches as a simple automatic call distribution mechanism. Alternatively, a SIP proxy or B2BUA can keep track of call taker status and route calls. The call taker identifier may or may not share the same domain name as the PSAP itself.

SIP INVITE requests may contain tel URIs (RFC 2806) that describe telephone numbers, for example: tel:+1-201-555-1212. These numbers may appear in the destination and source header (To and From, respectively). The tel context parameter may be used to label the realm of the number. A mechanism exists to label tel URIs with ISUP call type information.

The SIP asserted identify mechanisms can be used for the PSTN to indicate the calling number and any privacy indications.

C.2. Call Routing

SIP proxies and user agents can route pending calls to any other PSAP, either directly if the PSAP is IP-enabled or indirectly, by having the IP telephony gateway perform a call transfer based on the SIP 3xx redirection response. SIP user agents, such as the conferencing server, can transfer active calls to other PSAPs using the SIP REFER mechanism.

The SIP history mechanism may be used to indicate the call routing history of a call.

C.3. Reliability and Scaling

Multiple proxies and end systems can respond to the same SIP URI, by using appropriate Domain Name Service (DNS) mechanisms. This supports redundancy and load balancing.

C.4. Text Messaging

Instant messages and email messages can use the same identifier. Instant messages may use SIMPLE, the SIP-based instant messaging and presence protocol.

C.5. Call Monitoring

A standard SIP/RTP media mixer can be used to provide supervisor listening and conferencing. No additional protocol features are necessary.

SIP call status subscriptions can be used to monitor the status of calls from any location, including the status of pending calls.

C.6. Call Data

Location information or other caller information can be included in the Caller-Info header field, either by value or by reference to a database record. (Such references would typically use URIs, e.g., an HTTP query URI.) The detailed format has not been standardized yet.

C.7. Automatic Call Distribution

Automatic call distribution in SIP can be implemented in several ways, depending on the type of functionality desired. If calls are only queued in the "ringing" (pending) state, a proxy can queue up calls and deliver them to the first available call taker. This mode of operation does not support announcements. Alternatively, ACD functionality can be implemented by a B2BUA. The caller-facing side of the B2BUA answers the call and plays announcements. The call taker-facing side keeps track of agent status, possibly using SIP presence notification, and initiates calls to available call takers.

The ACD function can reside either in the PSAP network or on the network (provider) side of the PSAP access link. Placing the ACD function on the provider side has the advantage that queued calls do not consume access network resources. However, this requires cooperation by the gateway provider or the network service provider. If the ACD functionality is located on the PSAP network, a proxy should be on the provider side, to allow routing calls to a backup PSAP in case the access links for the primary PSAP fail.

SIP provisional responses may be used to update the gateway on call status without consuming access link (bandwidth) resources. The PSTN-facing gateway may then translate such information into spoken status messages.

1134 # Appendix D: Functional Considerations Checklist

	Functionality	VoIP Support & Standards Reference						Other Protocol	Std / Ref.
		H.323	ITU Ref.	SIP	IETF Ref.	H.248/ Megaco	ITU/IETF Ref.		
	Bandwidth Control (Section 2.2)								
1.	Mechanism to control bandwidth allocated to different services (emergency calling, administrative calling, etc.)								
2.	Ability to disallow compression of emergency calls								
	Key Telephone Service (Section 2.3.1.1)								
3.	Simultaneously alert a given set of call takers of the incoming call								
4.	Award the call to the first call taker to answer								
5.	Allow other call takers to join the call, bridging (conferencing) all participants								
	Automatic Call Distribution (Section 2.3.1.1)								
6.	Routing of calls to agents based on policies and different distribution algorithms (e.g., least busy).								

	Functionality	VoIP Support & Standards Reference						Other Protocol	Std / Ref.
		H.323	ITU Ref.	SIP	IETF Ref.	H.248/ Megaco	ITU/IETF Ref.		
7.	Agents must be able to be grouped into multiple according to policies specified by PSAP authorities.								
8.	Agent groupings must be changeable by an authority designated by the PSAP.								
9.	Ability to route calls to automated announcements or other indications of call status								
10.	Supervisors can manage call queues								
11.	Supervisors and/or agents can measure call delays and other performance metrics.								
12.	Agents can indicate their availability to receive calls. Calls must be routed only to agents that are available and not busy with other calls.								
13.	Capability to queue calls, either in answered or unanswered state. Answered, but queued calls must be able to receive recorded announcements. The announcement should be changeable by authorized PSAP supervisors.								

	Functionality	VoIP Support & Standards Reference						Other Protocol	Std / Ref.
		H.323	ITU Ref.	SIP	IETF Ref.	H.248/ Megaco	ITU/IETF Ref.		
14.	Reports to PSAP of emergency call queue information, including: number of calls in queue length of time the longest call has been in queue number of agents available.								
15.	Capability to conference audio logging systems with emergency calls while in queue and after answer. Information to uniquely identify agent identity or position must be available to audio logging system.								
16.	Supervisors must be able to monitor/bridge onto the audio stream of on-going calls.								
17.	Call takers must be able to add supervisors to an existing call to help with difficult calls								
18.	PSAPs need to be notified of abandoned calls, i.e., 9-1-1 calls that are dropped by								

	Functionality	VoIP Support & Standards Reference						Other Protocol	Std / Ref.
		H.323	ITU Ref.	SIP	IETF Ref.	H.248/ Megaco	ITU/IETF Ref.		
	the caller before being answered by a call taker								
19.	The same group of call takers should be able to handle both 9-1-1 and 10-digit emergency calls.								
20.	The call queue should allow automatic or manual transfer to another location of calls that exceed a particular expected waiting time.								
	Ability to distinguish various call types (Section 2.3.1.2)								
21.	Emergency 9-1-1 calls								
22.	non-selective routed emergency calls (e.g., direct 7-digit or 10-digit emergency calls)								
23.	Transfers from other PSAPs								
24.	Anonymous calls								
25.	Administrative calls								
26.	Call origination information: wireline, wireless, TDD/TTY, other…								
27.	Indication of a call that has been routed to an alternate PSAP								

	Functionality	VoIP Support & Standards Reference						Other Protocol	Std / Ref.
		H.323	ITU Ref.	SIP	IETF Ref.	H.248/ Megaco	ITU/IETF Ref.		
28.	Indication of default routed call								
	Delivery of Call Related Information to PSAP with the call (Section 2.3.1.3) **Essential (Tier 1) Information:**								
29.	Called Party Number								
30.	Calling Party Number, including any numbering plan digits (the "I" digit for CAMA trunks)								
31.	Delivery of Indication of Caller ID Blocking for non-9-1-1 calls								
32.	Location information or lookup keys								
33.	Delivery of Calling Party Number on abandoned calls								
34.	Ability to deliver an indication that a terminating emergency call has been alternate routed from another PSAP (note this is same as above in 2.3.1.2)								
	Alternate Routing Functionality (Section 2.3.1.4)								
35.	Ability to invoke/revoke Alternate Routing for particular PSAP by authorized party.								

	Functionality	VoIP Support & Standards Reference						Other Protocol	Std / Ref.
		H.323	ITU Ref.	SIP	IETF Ref.	H.248/ Megaco	ITU/IETF Ref.		
36.	Ability to specify the alternate routing destination and time constraints on alternate routing, if desired.								
37.	Notification of Alternate Routing to designated PSAP(s)								
	Call Forwarding Features (Section 2.3.1.5)								
38.	Invocation and cancellation of call redirection by request, on busy, don't answer after a configured delay, time-of-day, equipment or connectivity failure at PSAP.								
39.	PSAP should be able to specify the destination(s) to which calls should be redirected.								
40.	Receiving and redirecting PSAP should be notified that calls are being redirected.								
	Call Transfer Features (Section 2.3.1.6)								
41.	Invocation/cancellation of Network Call Transfer								
42.	Choice of Caller ID to be provided with transferred call: PSAP ID or Emergency caller ID								
43.	Inclusion of original emergency caller Information								

	Functionality	VoIP Support & Standards Reference						Other Protocol	Std / Ref.
		H.323	ITU Ref.	SIP	IETF Ref.	H.248/ Megaco	ITU/IETF Ref.		
44.	Inclusion of an indication of an emergency call with the transferred call								
45.	Transferring PSAP should be able to initiate an associated data session to provide information already collected by the transferring PSAP agent (see also Section 2.5.4).								
46.	Indication of kind of transfer: e.g., Selective routing of transferred call based on original caller location information								
47.	Transfer to announcements.								
	Call Conferencing Features (Section 2.3.1.7)								
48.	Ability to conference four or more parties								
49.	Add/drop control of the primary (controlling) PSAP (to add/drop other parties)								
50.	Transfer of Control of Conference to another party								
51.	Automatic conference of caller on multi-way connections.								
	Other PSAP Call Control Features (Section 2.3.6)								
52.	Hold (PSAP places caller or other party on Consultation Hold)								

	Functionality	VoIP Support & Standards Reference						Other Protocol	Std / Ref.
		H.323	ITU Ref.	SIP	IETF Ref.	H.248/ Megaco	ITU/IETF Ref.		
53.	Forced Disconnect (of the caller)								
	Network Control Features (Section 2.3.7)								
54.	?								
	Administrative Call Handling (Section 2.3.8)								
55.	?								
	Text-Based Emergency Contacts (Section 2.4)								
56.	Methods for delivery of text-based contacts, e.g., Telecommunications Devices for the Deaf/Teletype (TDD/TTY), wireless short message service (SMS), email, and instant messaging.								
	Emergency Call Related Data (Section 2.5)								
57.	Essential data (Sections 2.5.1.1 and also 2.3.1.3)								
58.	Supplemental data (Section 2.5.1.2)								
59.	Supplemental data (Section 2.5.1.3)								
60.	Delivery of Essential data (Section 2.5.1) with call								

	Functionality	VoIP Support & Standards Reference						Other Protocol	Std / Ref.
		H.323	ITU Ref.	SIP	IETF Ref.	H.248/ Megaco	ITU/IETF Ref.		
61.	Automatic delivery of emergency call related Supportive data (Section 2.5.2). Desirable to support automatic delivery of Supplemental data.								
62.	Ability to support PSAP queries for Supportive data and Supplemental data (Section 2.5.3). • Queries, responses, error recover, requests for Supportive data updates.								
·	**Remote Log-In (Section 2.6)**								
63.	Ability for PSAP agent to register from a remote location to receive calls.								
	Performance (Section 2.7)								
64.	Quality of Service for Voice Calls that can be measured to be equivalent to carrier-grade circuit-switched calling.								
65.	Delay and packet loss performance better than legacy based access to ALI systems for mission-critical data to support E9-1-1.								
	Security (Section 2.8)								
66.	Channel security – every packet between two end points gets encrypted and is from a trusted source.								

	Functionality	VoIP Support & Standards Reference						Other Protocol	Std / Ref.
		H.323	ITU Ref.	SIP	IETF Ref.	H.248/ Megaco	ITU/IETF Ref.		
67.	Application security – individual authentication for applications that ride on the upper layers.								
68.	Encryption at the lower layers.								
69.	Provide confidentiality, integrity and authentication for voice calls and data transactions to and between PSAPs and other entities that are connected to the network.								
70.	Provide confidentiality, integrity and authentication for mission-critical data sessions between two PSAPs, and between PSAPs and Emergency Service database and server elements on the packet network.								

1135